SUPPLY CHAIN SECURITY

L'importanza di conoscere e gestire i rischi della catena di fornitura

Clusit Community For Security

Supply Chain **Security**

Questo libro evidenzia l'importanza della gestione della sicurezza della catena di fornitura cercando di farne comprendere la magnitudine e di dare un aiuto pratico ai decisori e agli operativi. È un tema complesso non solo per i clienti ma anche per i fornitori e per le varie autorità che devono vigilare sul sistema. È una nuova frontiera dell'information security, cybersecurity e della sicurezza ICT che si aggiunge a quella della continuità operativa.

Alessandro Vallega
Founder e chairman della Clusit Community for Security

SOMMARIO

1. INTRODUZIONE, EXECUTIVE SUMMARY

La supply chain (“catena di fornitura”) è una rete di organizzazioni coinvolte nelle attività di produzione o di erogazione di servizi fino al cliente o utente finale. Le attività possono includere, per esempio, processi di messa a disposizione di materie prime e la logistica distributiva.

Il mondo delle forniture e delle supply chain, fino al recente passato, era considerato di minor rilevanza strategica, per le organizzazioni, rispetto alla vendita di prodotti e servizi. Ultimamente però, a seguito della rilevanza crescente della disponibilità e dei prezzi delle forniture in logica di sostenibilità del business, il *customer relationship management* (di seguito CRM) e il supply *chain management* (di seguito SCM) sono entrati a far parte delle discipline strategiche per il successo del business aziendale.

La presente pubblicazione è stata concepita proprio su questi presupposti. Le organizzazioni non dispongono internamente di tutte le risorse necessarie (materie prime, strumenti e servizi) per gestire l'intero ciclo di vita di un prodotto o di un servizio ed è per questo motivo che fanno ricorso a fornitori.

Nessuna organizzazione realizza totalmente in casa ogni parte dei propri prodotti e servizi: esistono sempre fornitori di materie prime, prodotti, strumenti e servizi che concorrono alla realizzazione del prodotto finale e alla sua commercializzazione.

Per questo motivo è necessario, anche se rappresenta una sfida complessa per una qualunque organizzazione, privata o pubblica, avere il controllo completo su tutta la supply chain.

I crescenti requisiti di qualità e sicurezza imposti o comunque attesi (anche implicitamente per la normativa cogente, o legati alla notorietà del marchio) da parte dei clienti, anche sotto forma di certificazioni di qualità e di prodotto, creano la necessità per le organizzazioni di assumersi l’onere della responsabilità sull’intera supply chain.

Queste condizioni introducono inevitabilmente un rischio, minimo o grande che sia, legato al livello di sicurezza della fornitura.

Dai dati del Rapporto Clusit 2021[1] sulla sicurezza ICT in Italia e nel mondo, emerge che nessun settore è immune dai cyberattacchi: solo nel 2020, infatti, sono stati registrati, a livello globale, 1.871 attacchi gravi di dominio pubblico, ossia con un impatto sistemico in ogni aspetto della società, della politica, dell'economia e della geopolitica.

Il report evidenzia un incremento di attacchi veicolati sfruttando vulnerabilità della supply chain, che consente ai criminali informatici di colpire tutti i soggetti in essa coinvolti (clienti, altri fornitori e soggetti terzi). Questo perché la supply chain moderna presenta una struttura e un grado di complessità superiore rispetto alle filiere di qualche anno fa. Ciò è dovuto alla globalizzazione dei mercati, all'intensificarsi dei flussi di materie prime, ai cambiamenti nelle abitudini dei consumatori e, soprattutto, alla crescente digitalizzazione e alla sempre più ampia esternalizzazione di servizi, inclusi quelli informatici (p.e. cloud computing, servizi esternalizzati e consulenza).

Alcune dinamiche emergenti o recentemente consolidatesi evidenziate dal report sono:

- incremento della superficie di attacco;
- mutamento delle strategie dei cybercriminali attraverso una semplificazione degli attacchi e un orientamento verso i soggetti deboli della supply chain;
- investimenti in sicurezza informatica disomogenei, con le grandi realtà che detengono strumenti, risorse e conoscenze, mentre le PMI, per mancanza di budget, scarsa formazione, consapevolezza e sensibilità, ne rimangono scarsamente dotate;
- permanenza di un problema culturale, dove microimprese e PMI ritengono erroneamente di non essere un bersaglio, dotandosi conseguentemente di un livello di sicurezza inadeguato al contesto attuale.

Purtroppo la crescente interconnessione tra le varie organizzazioni fa sì che la debolezza di un solo anello della catena potenzialmente violabile apra un'autostrada di accesso ai dati e alle reti dei committenti e di tutta la filiera.

Il presente libro tratta i rischi relativi alla sicurezza della supply chain ICT. Il termine *supply chain* sarà dunque normalmente riferito, in modo implicito, a quella ICT, pur estendendo talvolta la trattazione, più in generale, a quegli oggetti digitalizzati la cui sicurezza è fortemente correlata a quella dei loro fornitori. Va comunque precisato che, come recentemente sottolineato anche dal NIST[2], i rischi di cybersecurity

1 https://www.mmn.it/wp-content/uploads/2021/05/Rapporto-Clusit_03-2021-web.pdf.

2 NIST SP 800-161r1 - Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, May 2022

possono manifestarsi in tutte le *supply chain* di prodotti e servizi, includendo quindi sia quella ICT sia quelle non legate alla fornitura di tecnologie digitali (si ricordi ad esempio il caso del famoso data breach subito da Target nell'ormai lontano 2013[3]).
La supply chain relativa ai servizi ICT ha subito nel tempo profonde trasformazioni, passando da soluzioni gestite nei data center interni all'outsourcing e al cloud, interessando non solo la classica informatica di base, ma anche l'automazione degli impianti con soluzioni OT (operational technology) e IoT (Internet of things). L'esternalizzazione dei servizi ha inoltre come conseguenza che sempre più fornitori accedono ai sistemi informatici dell'organizzazione cliente. Esempi di rischi si trovano, per esempio, nel settore della sanità, dove alcuni sistemi informatici interagiscono con il paziente e li espongono ai rischi derivanti dal loro uso, manutenzione e aggiornamento, introducendo quindi rischi di sicurezza fisica (safety) e delle informazioni (security).

La sicurezza della supply chain assume una rilevanza crescente anche per l'impatto dei recenti eventi geopolitici, della globalizzazione e della digitalizzazione.

Diviene perciò fondamentale per il management comprendere come lo scenario descritto possa interessare la propria organizzazione e a quali rischi essa è esposta, considerando tutte le tipologie di servizi ICT interni o esternalizzati.

Importanti sono anche le normative dedicate a settori regolamentati, alle organizzazioni che erogano servizi essenziali (oltre 500 identificate in Italia) e alle organizzazioni rientranti nel perimetro della sicurezza nazionale cibernetica. È ragionevole ipotizzare la presenza di un numero ancor più significativo di fornitori, anche PMI, che erogano servizi ICT e fanno parte delle supply chain delle organizzazioni citate.

Ne deriva che i rischi delle supply chain assumono una dimensione sistemica e che, per le organizzazioni che non garantiscono adeguate misure di sicurezza informatica, sarà sempre più difficile operare sul mercato.

Un'autorevole conferma allo scenario ipotizzato arriva anche da un report di Gartner[4]. In sintesi ha sottolineato, fra l'altro, che gli attacchi alle supply chain ICT hanno generato un grande ritorno sugli investimenti (...dei criminali), e che "nel 2025 il 45% delle organizzazioni di tutto il mondo subirà attacchi alle proprie supply chain, con un incremento triplo rispetto al 2021".
Si preannuncia pertanto una situazione potenzialmente critica, che può esse-

3 https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

4 Executive IT, "Risk management. Quali saranno le principali tendenze per quanto riguarda sicurezza e gestione del rischio". Pag. 85 e 88. Marzo-Aprile 2022.

re affrontata anche con interventi normativi specifici. In questa prospettiva è da segnalare l'avvenuta pubblicazione della Direttiva NIS2 destinata alle organizzazioni private e alle pubbliche amministrazioni che operano nei servizi fondamentali e nelle infrastrutture critiche e ai loro fornitori, cioè alla loro supply chain. Tale Direttiva stabilisce i requisiti in materia di sicurezza dei dati, di valutazione dei rischi di sicurezza ICT, di gestione degli incidenti, di business continuity, di test periodici relativi alla sicurezza delle infrastrutture ICT e all'efficacia delle misure di mitigazione del rischio adottate (inclusi vulnerability assessment e penetration test), sia per l'organizzazione interessata che per tutta la supply chain. Questo orienterà sempre più le grandi organizzazioni nel selezionare i propri fornitori, che dovranno adottare misure efficaci di sicurezza informatica. Neanche le medie, piccole e micro organizzazioni possono però sentirsi esonerate dal mettere in campo opportune azioni di controllo delle loro supply chain, visti i loro impatti.

Oltre alle organizzazioni citate, se consideriamo i rischi operativi e di compliance, nessuna organizzazione dovrebbe sottovalutare i rischi derivanti dalla supply chain. Ciò vale sia per le organizzazioni che adottano sistemi informativi di base sia per le realtà con un forte orientamento alla digitalizzazione e ai sistemi di business intelligence. Si pensi ancor di più a chi opera nelle nuove frontiere della robotica e dell'intelligenza artificiale. Oggi una supply chain ICT vulnerabile non è più accettabile.

La necessità di perseguire questo approccio è dimostrata anche da alcuni incidenti dovuti a errori, leggerezze e mancati controlli da parte dei subfornitori della supply chain, i cui impatti si sono propagati poi sino al cliente finale, con conseguenze anche gravi per il business.

Alla luce delle considerazione sopra riportate, La Clusit Community for Security si propone, in questo libro, di fornire alcuni suggerimenti di taglio interfunzionale.

Questo libro si propone quindi di:

- approfondire quali rischi devono essere esaminati nella gestione della supply chain nei diversi contesti;
- esaminare come le criticità e le vulnerabilità della supply chain possano propagarsi;
- suggerire come intervenire presentando controlli per prevenire o almeno limitare la propagazione delle criticità;
- approfondire gli aspetti legali e contrattuali.

Lo scopo non è soltanto quello di aiutare i clienti a comprendere cosa chiedere ai

propri fornitori, ma anche quello di aiutare i fornitori a prepararsi a sostenere le possibili (e sempre più probabili) richieste dei propri clienti.

2. PER CHI ABBIAMO SCRITTO QUESTO LIBRO

A beneficiare della lettura di questo libro saranno certamente i vertici delle organizzazioni (p.e. componenti dei CdA, CEO e CFO). Essi infatti giocano un ruolo fondamentale nella definizione delle strategie di sicurezza e di esternalizzazione, potranno sviluppare la consapevolezza sul tema e richiedere un adeguato monitoraggio della supply chain.

Il libro sarà inoltre un'utile lettura per le altre figure con responsabilità più operative e di supporto al vertice. Ad esempio i risk manager, i CIO, i CISO, i DPO e, nell'ambito pubblico, i responsabili per la transizione al digitale, i responsabili degli acquisti, i project e product manager.

La lettura di questo libro non presuppone competenze pregresse approfondite: si assumerà per il lettore almeno una sensibilità verso i processi critici di un'organizzazione e un'attenzione a cosa è esternalizzato.

3. COMMUNITY E LICENZA

Trattando il tema del rischio della supply chain, la Clusit Community for Security arriva alla sua quattordicesima pubblicazione.

Quelle precedenti, anche loro liberamente scaricabili dal sito **http://c4s.clusit.it**, sono:

- ROSI - Return on Security Investments: un approccio pratico. Come ottenere Commitment sulla Security;
- Fascicolo Sanitario Elettronico: il ruolo della tecnologia nella tutela della privacy e della sicurezza;
- Privacy nel Cloud: Le sfide della tecnologia e la tutela dei dati personali per un'organizzazione italiana;
- Mobile e Privacy: Adempimenti formali e misure di sicurezza per la conformità dei trattamenti di dati personali in ambito aziendale;
- La sicurezza nei Social Media: guida all'utilizzo sicuro dei Social Media per le aziende del Made in Italy;
- I primi 100 giorni del responsabile della Sicurezza delle Informazioni: Come affrontare il problema della Sicurezza informatica per gradi;
- Le frodi nella rete: il duplice ruolo dell'ICT;
- Mobile Enterprise: sicurezza in movimento;
- SOC e Continuous Monitoring faccia a faccia con la Cybersecurity;
- Consapevolmente Cloud. Guida per l'azienda che deve affrontare l'innovazione con le idee chiare;
- IoT Security e Compliance. Gestire la complessità e i rischi;
- Intelligenza artificiale e sicurezza: opportunità, rischi e raccomandazioni;
- Rischio digitale, Innovazione e Resilienza: Conoscere, affrontare e mitigare il rischio digitale.

Gli autori svolgono il lavoro di preparazione tramite un confronto multidisciplinare e multisettoriale. Li motiva la consapevolezza del grande bisogno di sicurezza e compliance delle organizzazioni italiane e un forte senso di responsabilità verso la nostra società. La Community opera dal 12 settembre 2007 e permette la collaborazione di alcune centinaia di professionisti, che operano negli ambiti della sicurezza, dell'audit, della conformità, dell'ethical hacking, della consulenza, dell'integrazione dei sistemi e delle certificazioni basate su norme internazionali. Partecipano alla Community

i responsabili della sicurezza del mondo della domanda e dell'offerta di servizi e tecnologie correlati a questi ambiti. Il lavoro verte su molteplici aspetti: culturale, organizzativo e tecnologico.

La Community riceve il sostegno di prestigiose associazioni professionali e industriali che collaborano attivamente tramite i loro membri, come ad esempio: ABI Lab, ACFE, AIEA, AISIS, ANDIP, ANRA, ANORC, APIHM, AUSED, BCI Italy Chapter, CSA Italy, ISACA VENICE, ISC2.

Le pubblicazioni sono il frutto del lavoro di almeno 50 persone e consistono in 100-200 pagine di materiale. Consci che tutto è migliorabile, e nel pieno spirito della Community, le rendiamo disponibili con una licenza "Creative Common, Attribuzione e Condividi nello stesso modo" (**https://creativecommons.org/licenses/by-sa/4.0/**). La licenza permette a chiunque di usare il nostro prodotto per crearne una sua evoluzione a condizione che citi gli autori originali riportando la nostra URL **http://c4s.clusit.it** e utilizzi a sua volta lo stesso tipo di licenza.

4. L'IMPORTANZA DELLA SUPPLY CHAIN

È cambiato lo scenario di riferimento per le organizzazioni in termini di mercati e modelli operativi, indotti dalla globalizzazione. Assume crescente rilevanza la necessità di rimanere competitivi offrendo beni e servizi a prezzi più bassi o a maggior valore aggiunto, sfruttando anche l'accesso ai mercati esteri, che possono rendere conveniente ripartire le risorse su una più ampia area geografica.

Oggi la diffusione di Internet rende possibile una forte interconnessione tra tutte le aziende che operano come fornitori di prodotti o servizi: ciò consente di migliorare e velocizzare la risposta alle esigenze dei clienti razionalizzando i costi, riducendo il time-to-market e assicurando un'opportuna differenziazione rispetto ai concorrenti.

Il ruolo della supply chain è quindi determinante nell'ottimizzare il livello di servizio ai clienti, sempre attraverso un attento controllo dei costi e dell'impiego di risorse, impianti e materie prime. In altre parole, la supply chain diviene sempre più strategica nei piani di sviluppo a breve e a lungo termine delle organizzazioni in contesti estremamente dinamici e sfidanti.

Un'applicazione molto rilevante in termini di supply chain è l'outsourcing, ossia la completa esternalizzazione di servizi. Di seguito verranno descritte in maggior dettaglio le caratteristiche più significative e gli scenari di sviluppo futuro dell'outsourcing.

4.1 Un po' di terminologia

È utile chiarire alcuni termini spesso utilizzati nell'ambito della supply chain a partire proprio da quest'ultimo.

La **supply chain** è una rete di organizzazioni coinvolte nelle attività di produzione o di erogazione di servizi fino al cliente o utente finale. Le attività possono includere, per esempio, processi di messa a disposizione di materie prime e la logistica distributiva.

Quando un'organizzazione ingaggia un'altra entità, acquista beni e servizi, o in generale stipula con essa un contratto per una fornitura, ci si riferisce a tale entità

con termini vari, quali: supplier, vendor, terze parti, contractor, reseller, provider, merchant, partner, outsourcer e, in italiano, fornitore o appaltatore. Non esistendo per essi definizioni universalmente riconosciute, a volte sono utilizzati in modo del tutto equivalente, mentre in altri casi si fanno delle distinzioni. È questo, ad esempio, quello che avviene con i termini "*vendor*" e "*supplier*", che alcuni definiscono come segue:

- **Supplier**: una terza parte che fornisce beni e servizi di valore chiave nella produzione dell'organizzazione. Ad esempio, una casa automobilistica non produce in proprio gli pneumatici per le auto che produce, ma li acquista da un produttore specializzato.
- **Vendor**: una terza parte che fornisce beni e servizi ausiliari, comunque importanti per garantire l'operatività dell'organizzazione, ma che non influiscono direttamente su quanto prodotto. Ad esempio, i venditori di software commerciali sono comunemente definiti vendor.

I termini *reseller* e *merchant* sono alternative a *vendor*, mentre *provider*, *partner*, e *outsourcer* possono essere utilizzati invece di *supplier*. Viceversa, il termine *contractor* sostituisce indistintamente *vendor* e *supplier*.

Il termine **terze parti** è un termine generico, più ampio, utilizzato per descrivere ogni entità con cui l'organizzazione interagisce oltre ai fornitori (p.e. organizzazioni partner di vario tipo e organismi di regolamentazione; al limite, anche gli stessi clienti, che a rigore sono definiti come "seconde parti") e che possono comunque esporla a rischi significativi, in quanto a essa collegate.

Nell'ambito della gestione del rischio, è evidente la necessità di focalizzare l'attenzione sui fornitori più critici.

4.2 Supply chain e outsourcing

È possibile individuare una serie di vantaggi derivanti da un percorso di *business outsourcing*:

a. concentrazione sul "core business" e i relativi processi abilitanti;
b. modelli economici prevalenti che privilegiano la OpEx (*operational expenditures*), costi necessari per gestire un prodotto, un business o un sistema, verso la CapEx (*capital expenditures*), costi per sviluppare o fornire asset durevoli per il prodotto o il sistema, per avere prodotti e servizi meno statici e prevedibili;
c. riduzione del *time-to-market* per prodotti e servizi non in regime di mono-

polio (vedere il modello giapponese e quello sud-coreano per l'elettronica di consumo);

d. globalizzazione dei mercati con la creazione di campioni planetari specializzati (effetto "massa critica", per cui l'incremento di produttività porta la riduzione dei costi unitari di produzione mentre la maggior dimensione consente maggiori investimenti in automazione e innovazione);
e. incremento della qualità e della specializzazione dei processi, per la costruzione di un prodotto o servizio;
f. affermazione di un modello organizzativo, mutuato dal settore automotive, di cooperazione federata non competitiva di organizzazioni, ciascuna fortemente specializzata, finalizzata alla creazione di un prodotto o servizio;
g. concentrazione sulla CX (*customer experience*) come fattore chiave per la creazione di valore per l'organizzazione (*customer first*).

Oggi, quindi, il mondo della produzione e dei servizi è estremamente interconnesso e quasi nessuna organizzazione, incluse aziende e pubbliche amministrazioni, è in grado di raggiungere i propri obiettivi senza il ricorso a fornitori esterni.

Il fenomeno ha raggiunto dimensioni economiche significative a livello globale, anche per quanto riguarda nello specifico il mercato dei servizi in outsourcing, come sintetizzato nella tabella seguente:

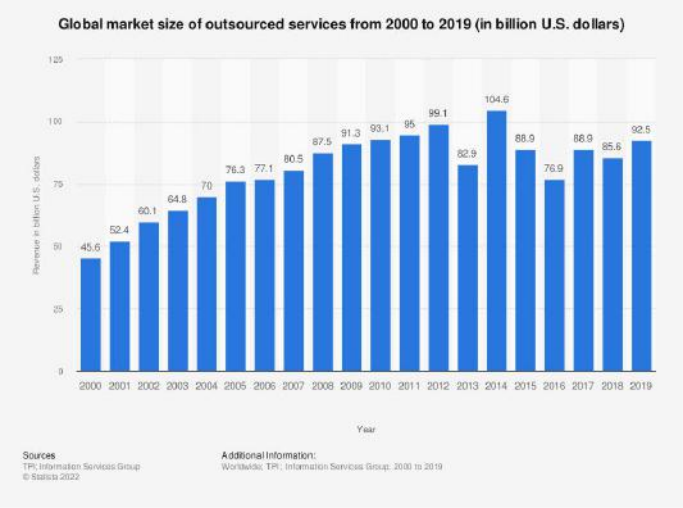


Figura 1 – Mercato globale dei servizi in outsourcing dal 2000 al 2019[5]

5 Fonte in figura.

4.2.1 I processi affidati in outsourcing

I processi o servizi solitamente affidati in outsourcing sono:

a. HR operations (p.e. contabilità e buste paga);
b. legal, compliance e audit;
c. customer experience multimediale (come evoluzione del call center);
d. marketing e telemarketing;
e. magazzini e logistica;
f. servizi di assistenza e supporto all'infrastruttura (mail, connettività, spazio di archiviazione).

Prendendo come esempio il settore finanziario, questo fenomeno sta avendo un forte sviluppo anche in ragione dell'avvento del Fintech, dove organizzazioni specializzate offrono al mercato e a terzi prodotti o servizi, primariamente in forma digitale e gestiti integralmente, secondo il modello *white-label*, che ne permette il *rebranding* da parte di altre organizzazioni per offrirlo, a loro volta, come se fosse realizzato e gestito da loro. Un esempio sono le carte di pagamento, i cui operatori hanno da tempo smesso di offrire il prodotto alla clientela finale, concentrandosi sul modello B2B offrendo a banche e operatori finanziari il servizio in modalità *white-label*.

Tale modello operativo richiede che tra l'emittente (la banca) e il gestore della carta, sia mantenuto uno scambio di informazioni costante, affidabile e regolamentato. Tale requisito richiede un'adeguata struttura contrattuale, con le responsabilità degli attori, i livelli di servizio e i relativi sistemi condivisi di controllo (ad esempio KPI).

Sempre nel settore bancario sono presenti altri esempi:

a. bancassurance: la banca come erogatore di servizi assicurativi ramo vita e danni;
b. la rateazione puntuale (BNPL, *buy now pay later*) o strutturata (credito al consumo) di acquisti di beni e servizi: la banca si propone come singolo punto di contatto per il cliente.

4.2.2 L'outsourcing dell'ICT

L'infrastruttura ICT, in considerazione della sua pervasività operativa, della sua crescente complessità e della velocità dell'innovazione tecnologica e dei nuovi modelli di offerta, è divenuta sempre più decentralizzata.

Di seguito, in particolare, sono elencate le principali motivazioni della decentralizza-

zione:

a. evoluzione del mercato dei fornitori che, spinti dalla concorrenza storica e dallo sviluppo di nuove funzioni o applicativi, cercano di creare portafogli di prodotti e servizi sempre più completi e quindi economicamente più vantaggiosi per i clienti;
b. aumento della complessità delle architetture ICT, che il fornitore può integrare con un approccio "a mattoncini", con architetture finali componibili e modificabili nel tempo, proporzionalmente al mutare dei bisogni dei clienti;
c. aumento della richiesta, in numero e competenze, di specialisti ICT necessari per gestire e governare l'ICT in tutti i suoi domini;
d. evoluzione delle architetture ICT per il supporto dei nuovi modelli abilitati dal digitale (anytime, anywhere, any media);
e. bilanciamento in termini di costi-benefici, a condizione che le prestazioni, la disponibilità e la sicurezza dei sistemi siano garantite secondo standard predeterminati e condivisi.

Questi fattori di evoluzione appesantiscono il budget dell'organizzazione per il mantenimento delle risorse tecniche e la gestione di personale qualificato, rendendo necessaria la ricerca di nuovi modelli operativi dotati di maggiore duttilità ed efficienza.

Una risposta è la ricerca di "concentrazione" di risorse omogenee, sfruttando l'effetto "massa critica". Proprio per questo, il ricorso all'outsourcing è la miglior risposta ai problemi evidenziati.

L'outsourcing riguarda tutti i domini ICT (alcuni dei quali possono essere fruiti secondo il paradigma cloud, come illustrato al paragrafo 5.1), tra cui:

a. gestione delle risorse tecnologiche fisiche e infrastrutturali (presso il data center del fornitore o del cliente, in presenza o da remoto):
    1. infrastrutture elaborative;
    2. infrastrutture di memorizzazione dati;
    3. reti ed infrastrutture di comunicazione;
    4. apparati per la sicurezza;
    5. infrastrutture per disaster recovery;
b. protezione delle informazioni e delle risorse tecnologiche:
    1. monitoraggio dei componenti hardware e software di base;
    2. supporto alla gestione dei cambiamenti;

3. backup e restore;
4. disaster recovery (DRaaS o disaster recovery as a service);
5. autenticazione e gestione delle identità digitali;
6. gestione delle componenti di sicurezza (SECaaS o security as a service);
7. verifiche di sicurezza (ad esempio penetration testing);

c. processi di gestione del software di sistema e applicativi:
    1. installazione e gestione del software di sistema;
    2. sviluppo del software applicativo;
    3. messa a disposizione temporanea di specialisti ICT (time & material);
    4. utilizzo di app store e di marketplace per la distribuzione o l'acquisizione di software;
d. gestione del rapporto con le terze parti:
    1. architetture di contract automation;
e. sistema dei controlli (terzo livello):
    1. ICT audit;
f. formazione.

Altro dominio è quello della fornitura di hardware, che include server, dispositivi IoT, dispositivi medici e di diagnostica in vitro, sensori e attuatori utilizzati in larghissima misura in qualunque ambito produttivo, e il relativo firmware.

Per quanto riguarda i dati, il solo mercato dell'outsourcing dei processi è destinato a crescere in valore di circa l'8,5% tra il 2021 e il 2028[6]. Ecco alcuni punti chiave:

- il 45% delle organizzazioni ha pianificato di aumentare l'outsourcing dopo la pandemia, spesso concentrandosi sulla ricerca di competenze non accessibili internamente.
- Il cloud permette alle organizzazioni di abbracciare più opportunità di outsourcing, consentendo loro di coinvolgere una gamma più ampia di professionisti distribuiti.
- La ragione principale per l'esternalizzazione è la riduzione dei costi, in quanto per il 70% delle organizzazioni l'outsourcing riduce i costi associati all'assunzione di personale interno.

L'indagine Deloitte sull'outsourcing del 2020[7] indica che circa il 90% delle organizzazioni ritiene il cloud uno dei principali fattori abilitanti nel loro percorso di outsour-

6 https://www.grandviewresearch.com/industry-analysis/business-process-outsourcing-bpo-market.
7 "How much disruption? Deloitte Global Outsourcing Survey 2020".

cing (gli altri sono il *robotic process automation*, o RPA, e l'uso di ERP senza client).

Deloitte, nel 2020, riteneva che la crisi COVID-19 avrebbe spinto maggiormente l'adozione del cloud e avrebbe aumentato ulteriormente le opportunità di outsourcing.

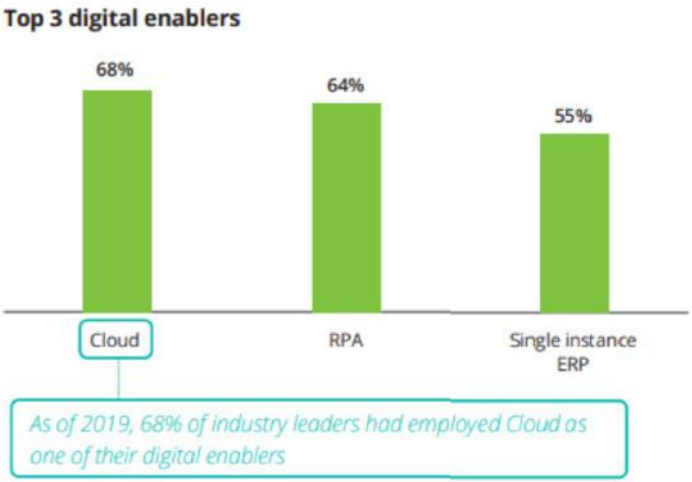


Figura 2 – Gli abilitatori principali per il digitale[8]

Un rapporto di Aptude[9] sul mercato globale dell'outsourcing indica che le organizzazioni stanno esternalizzando circa il 68% della loro forza lavoro, con circa 300.000 posizioni attualmente trasferite all'estero, per un valore di circa $85,6 miliardi nel mercato globale.

Aptude rileva inoltre che il motivo principale per cui le organizzazioni esternalizzano è la riduzione delle spese e la gestione di un ambiente complesso. Tuttavia, le organizzazioni si rivolgono all'outsourcing anche per garantire che le loro attività possano funzionare in modo più efficiente in un ambiente che richiede servizi attivi 24/7.

Secondo i rapporti pubblicamente disponibili di Statista[10], il mercato dell'outsourcing dei servizi ICT dovrebbe essere in rapida crescita. Entro il 2022, il mercato avrà un valore di circa 1.280 miliardi di dollari a livello mondiale. L'aumento della domanda

8 Fonte: "How much disruption? Deloitte Global Outsourcing Survey 2020"
9 https://aptude.com/outsourcing/entry/what-you-need-to-know-about-outsourcing-which-outsource-service-is-right-for-you/.
10 https://www.statista.com/.

di soluzioni SaaS e cloud nell'ambiente di lavoro moderno è destinato a far crescere ulteriormente questa domanda. Entro il 2023, si prevede che il mercato raggiungerà un valore di circa 1.392 miliardi di dollari per l'outsourcing ICT a livello mondiale.

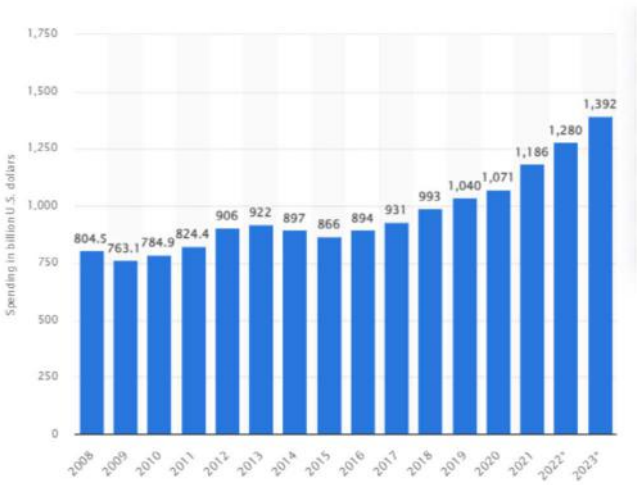


Figura 3 – Mercato dell'outsourcing dei servizi ICT[11]

Secondo un rapporto di Clutch del 2019 e aggiornato nel 2022[12], circa un terzo delle piccole imprese (37%) attualmente esternalizza almeno un processo per ridurre i costi e migliorare le competenze disponibili. Le organizzazioni che hanno partecipato all'indagine esternalizzano più frequentemente attività tecniche come i servizi ICT (37%), la contabilità (37%) e il marketing digitale (34%).
Circa il 52% degli intervistati ha dichiarato di avere intenzione di aumentare il ricorso all'outsourcing. Inoltre, il 24% ha dichiarato di esternalizzare per migliorare l'efficienza, mentre il 18% ha dichiarato di esternalizzare per accedere all'assistenza di esperti.

4.3 Gli scenari del prossimo futuro

Le supply chain globali, in particolare delle tecnologie di valore strategico, stanno subendo fortemente l'impatto dei nuovi eventi geopolitici. Questo implica un ripensamento in termini di affidabilità, resilienza, ridondanza e capacità di adattarsi a

11 Fonte: https://www.statista.com/.
12 https://clutch.co/bpo/virtual-assistants/resources/small-business-outsourcing-statistics.

scenari caratterizzati da un livello elevato di incertezza[13]. In un mondo in rapido movimento, frammentato e consumer-centrico si impone la transizione da supply chain tradizionali, il cui obiettivo era la stabilità e la riduzione dei costi, a supply chain molto più dinamiche, in grado di prevedere, preparare e rispondere alla domanda in rapida evoluzione. In breve, le supply chain dovranno diventare "agili"[14].

Alcuni fenomeni relativi alla gestione della supply chain emersi negli ultimi anni:

- **Rivalutazione dell'integrazione verticale fra organizzazioni**: alcuni gruppi industriali hanno da tempo integrato, all'interno della propria attività, forniture di organizzazioni controllate (approccio seguito, ad esempio, dal Gruppo Fiat negli anni Settanta e, più recentemente, dal Gruppo Luxottica). Ora si assiste a un fenomeno analogo, teorizzato già nel 1992[15], realizzato fra imprese non appartenenti allo stesso gruppo, la cosiddetta Impresa 4.0, che adotta le nuove tecnologie per un migliore controllo lungo la supply chain[16].
- **Rivalutazione dell'approccio just in time**: a inizio millennio, i problemi economici delle industrie con elevati valori del circolante (in particolare delle scorte di materie prime) avevano spinto molte organizzazioni ad adottare l'approccio "just in time", nato negli anni 80, limitando i volumi delle materie prime nei magazzini adottando soluzioni che prevedevano il ricorso a fornitori che, di fatto, gestivano i magazzini dei clienti. Tale soluzione, valida in uno scenario di stabilità dei mercati, ora si presenta molto critica.
- **Digitalizzazione della supply chain**: è necessario fare riferimento alla digitalizzazione sia del processo di approvvigionamento (supply chain management) sia dei processi di produzione tramite impianti, spesso affidati a fornitori esterni.
- **Sistemi informatici e cybersecurity**: l'informatica, fin dagli anni Settanta del secolo scorso, con le applicazioni online dedicate ai processi di supporto al business (ad esempio ciclo attivo e produzione) e all'automazione dei processi di supporto (ad esempio HR, sistemi contabili e di controllo, ciclo passivo), era considerata il "tessuto connettivo" fra i processi interni. L'approccio "reti di impresa" ha esaltato tale ruolo ampliandolo alla interconnessione tra più organizzazioni, determinando anche un ripensamento radicale del sourcing verso i fornitori ICT, sempre più focalizzato su sistemi applicativi acquisiti sul mercato (Sap, per fare un semplice e diffuso esempio) e sui

13 CSIS, The Great Rewiring: How Global Supply Chains Are Reacting to Today's Geopolitics, https://www.csis.org/analysis/great-rewiring-how-global-supply chains-are-reacting-todays-geopolitics.

14 McKinsey, Future-proofing the supply chain, https://www.mckinsey.com/capabilities/operations/our-insights/future-proofing-the-supply chain.

15 Gianni Lorenzoni (a cura di) "Accordi, Reti e vantaggio competitivo. Le innovazioni nell'economia d'impresa e negli assetti organizzativi, Etas Libri 1992.

16 Mirella Castigli, 26 luglio 2021, https://www.industry4business.it/connected-enterprise/vertical-integration-significato-vantaggi-e-strategie/.

servizi cloud[17].

Lo scenario così delineato coinvolge evidentemente tutti i settori. Un esempio per tutti è la crisi di disponibilità dei chip registrata dal 2021, che ha costretto l'Unione europea ad approvare la prima decisione sugli aiuti di Stato nell'ambito dello **European Chips Act**, dando il via libera a un investimento da 730 milioni di euro da parte di una società franco-italiana per la realizzazione di un nuovo stabilimento in Sicilia[18].

Si osserva anche che lo sviluppo delle tecnologie digitali ha, da un lato, esacerbato alcune linee di frattura geopolitiche (si pensi alla rivalità Cina-USA-EU per la supremazia in settori quali l'intelligenza artificiale o i semiconduttori), ma, dall'altro, può costituire uno strumento estremamente efficace nella riprogettazione delle interdipendenze globali.

Si stanno sviluppando anche tecnologie per governare al meglio le interdipendenze. Un esempio riguarda il framework PEPPOL per i soggetti pubblici[19]. Esso è un insieme di specifiche per lo sviluppo di una rete globale per l'e-procurement di tipo federato, attraverso il quale le organizzazioni partecipanti possono scambiarsi documenti di gara, comprese le fatture elettroniche, in formato machine-readable.

I rapporti tra clienti e fornitori possono essere migliorati anche dall'utilizzo di credenziali verificabili. È in questa direzione il lancio, da parte della Commissione europea, di un'identità digitale europea insieme a una proposta di miglioramento dell'attuale regolamento eIDAS[20].

17 Osservatorio Polimi – 13 ottobre 2021, https://www.corrierecomunicazioni.it/digital-economy/cloud/cloud-in-italia-il-mercato-vale-a-38-miliardi-16-spinta-dai-servizi-paas-e-iaas/.

18 https://www.agi.it/economia/news/2022-10-10/von-der-leyen-sicilia-prima-produzione-ue-base-chip-18390477/.

19 https://peppol.eu/.

20 European Commission, eIDAS Regulation, https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation.

5. I RISCHI ICT DELLA SUPPLY CHAIN

Al giorno d'oggi, sempre più le tecnologie informatiche e operative (ICT e OT) si basano su un ecosistema di supply chain complesso, distribuito a livello globale e fortemente interconnesso per fornire soluzioni molto avanzate, economiche e riutilizzabili.

L'ambiente digitale distribuito si compone così di un numero importante di soggetti, operanti su diversi livelli di subfornitura, che utilizzano metodi di distribuzione e tecnologie diverse, soggetti a normative sempre più pervasive e variegate, a policy, procedure e pratiche di diversa natura, che interagiscono per progettare, produrre, distribuire, attuare, utilizzare, mantenere e gestire prodotti e servizi ICT o OT. Di conseguenza, l'integrità delle loro supply chain è sempre più di fondamentale importanza per la maggior parte delle organizzazioni, indipendentemente dal fatto che acquistino o vendano prodotti e servizi.

Uno scenario divenuto sempre più comune vede l'attaccante puntare ai fornitori spesso estremamente specializzati nel rispettivo campo applicativo, ma non nella cyber security, utilizzandoli quale punto di accesso per penetrare l'organizzazione obiettivo dell'attacco.

Una vulnerabilità in un fornitore può immediatamente tradursi in una vulnerabilità del prodotto o servizio realizzato con il suo supporto dall'organizzazione. Tale prodotto o servizio può essere a sua volta usato da innumerevoli utenti (potenziali vittime) non interessati alla complessità sottostante ma al risultato finale. Proprio quest'ultima caratteristica rende gli attacchi informatici alla supply chain particolarmente interessanti per i criminali con obiettivi economici, politici o strategici.

In questo capitolo sono presentati alcuni rischi di sicurezza della supply chain inerenti all'uso di tecnologie informatiche. In particolare, sono stati analizzati i rischi relativi a:

- servizi cloud;
- software;
- gestione del software;
- app per dispositivi mobili;

- OT e supply chain integrata;
- hardware;
- lock-in;
- continuità operativa;
- accesso remoto;
- intelligenza artificiale;
- clausole contrattuali.

Non sono trattate invece altre tipologie di rischio relativo alla supply chain, come l'affidabilità dei trasporti, la disponibilità delle materie prime, i rischi legati all'andamento dell'economia globale e quelli legati alla situazione geopolitica, poiché non strettamente legate all'ambito ICT.

Le pratiche di gestione dei fornitori comuni a tutti i settori sono riportate nel capitolo 10.

5.1 Servizi cloud

L'adozione dei servizi cloud presenta differenze rispetto a quelli on-premise (ossia su infrastruttura hardware e con software posizionati e gestiti all'interno dell'organizzazione). In generale, per i servizi erogati on-premise, le organizzazioni hanno il pieno controllo della propria infrastruttura tecnologica (p.e. il controllo fisico dell'hardware e della rete, il pieno controllo dello stack tecnologico in produzione), anche se in taluni casi ricorrono a servizi esterni per alcune o tutte le attività di gestione.

I servizi cloud possono basarsi su differenti modelli, solitamente riconducibili a[21]:

- Infrastructure as a Service (IaaS): è fornito ai clienti l'accesso con un metodo di pagamento PAYG (pay-as-you-go, pagamento a consumo) allo storage, alla connessione di rete, ai server e ad altre risorse di calcolo nel cloud.
- Platform as a Service (PaaS): è fornito l'accesso a un ambiente di lavoro, in cui gli utenti possono sviluppare e distribuire applicazioni.
- Software as a service (SaaS): sono forniti software e applicazioni. Gli utenti si abbonano al software e vi accedono tramite il web o le API del fornitore.

La scelta del modello di servizio cloud dipende dalle esigenze specifiche e dagli obiettivi economici dell'organizzazione, dal tipo di governance e compliance che si vuole mantenere, dal grado di responsabilità che si vuole demandare al provider. Con i servizi cloud, le organizzazioni utilizzano risorse e procedure messe a disposi-

21 https://www.ibm.com/it-it/cloud/learn/iaas-paas-saas.

zione dal cloud service provider (CSP). Di conseguenza, la gestione della sicurezza e della privacy è una **responsabilità condivisa** tra il cliente e il cloud provider. Il livello di responsabilità varia in base alla natura della tipologia del servizio cloud (IaaS, PaaS o SaaS) fornito dal CSP.

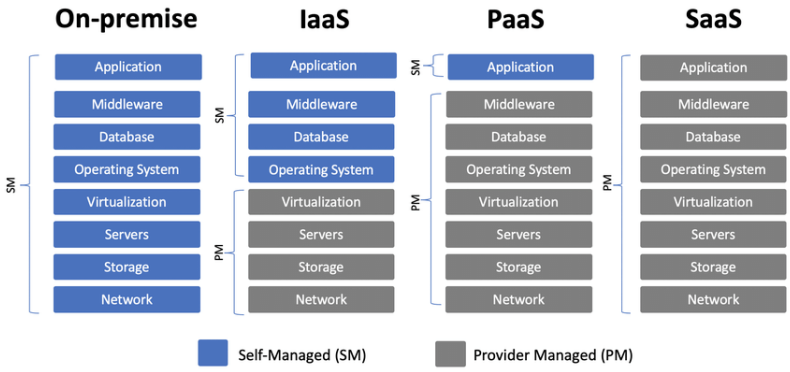


Figura 4 - Servizi on-premise, IaaS, PaaS, SaaS

La corretta comprensione del modello di responsabilità condivisa da parte delle organizzazioni è fondamentale per il ricorso ai servizi cloud in modalità sicura.
Il cliente che adotta servizi cloud, indipendentemente dal modello che utilizza (IaaS, PaaS, o SaaS), deve sempre ricordare che la sicurezza e la compliance sono anche sua responsabilità (come minimo perché deve verificare che il CSP abbia livelli di sicurezza adeguati, che questi siano effettivamente applicati e che il personale li usi correttamente).

5.1.1 Scenari di rischio

5.1.1.1 Governo e sovranità del dato, data protection e privacy

L'utilizzo di un servizio cloud per conservare dati personali può esporre l'organizzazione a rischi di violazione della normativa sulla privacy e, in particolare, del principio di sovranità digitale.
È importante quindi per un'organizzazione avere la piena consapevolezza della localizzazione geografica dei dati affidati al fornitore cloud (ossia della collocazione dei data center in cui essi vengono trattati). Infatti, il luogo dove si trovano fisicamente i dati ha conseguenze rilevanti ai fini della normativa applicabile per la loro protezione.

5.1.1.2 Vendor lock-in

Questa tipologia di rischio si presenta quando un'organizzazione desidera passare a un nuovo fornitore di servizi cloud, ma non può farlo, a causa della complessità, dei costi e del tempo necessari per effettuare tale passaggio (vedere paragrafo 5.7).

5.1.1.3 Errori di configurazione (misconfiguration)

Gli errori di configurazione avvengono quando un sistema o una risorsa in cloud non è configurata correttamente, mettendo così a rischio il sistema ed esponendola a un attacco o a furti di dati. I clienti dei servizi **IaaS** sono maggiormente esposti a questo rischio, dove gestiscono direttamente le configurazioni dell'infrastruttura e delle componenti applicative.

5.1.1.4 Indisponibilità del servizio

Il servizio potrebbe non essere disponibile per lunghi periodi.

5.1.1.5 Inadeguata formazione

L'organizzazione potrebbe non avere esperienza nella gestione e nell'assistenza di servizi cloud, in quanto è richiesta una formazione specifica e adeguata.

5.1.1.6 Vulnerabilità dei container

Una ricerca di Palo Alto ha mostrato che il 63% di template di terze parti utilizzati nella creazione dell'infrastruttura cloud ("infrastruttura as code") contenevano configurazioni non sicure e il 96% delle applicazioni container di terze parti distribuite nell'infrastruttura cloud conteneva vulnerabilità note[22].

5.1.1.7 Scarsa trasparenza contrattuale

La mancanza o la scarsa trasparenza di clausole contrattuali, che regolamentano la disponibilità del servizio, la chiara attribuzione di ruoli e responsabilità, gli eventuali risarcimenti in caso di incidenti di sicurezza o data breach, le modalità di protezione dei dati, le modalità di cancellazione degli stessi a seguito di rescissione o termine del contratto ecc, possono innalzare notevolmente il livello di rischio correlato all'erogazione del servizio da parte del cloud provider, anche in termini di compliance normativa.

5.1.2 Buone pratiche

Un'organizzazione che adotta servizi cloud deve selezionare il servizio, la soluzione e il fornitore che meglio garantiscono la copertura delle proprie esigenze, in ottemperanza alla normativa applicabile, in continua evoluzione.

22 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

Di seguito sono riportati, per macro-aree, i principali aspetti da tenere in considerazione nel processo di selezione del cloud provider:

- **Governance**: valutazione del cloud provider in tema di solidità finanziaria, cybersecurity e gestione dei rischi. Fanno parte di questo ambito: certificazioni (ad esempio ISO/IEC 27001, SOC 1, SOC 2, SOC 3), formazione del personale, adozione di framework di sicurezza informatica o di sicurezza delle informazioni, processi per la gestione dei rischi relativi alla sicurezza delle informazioni interni e legati alla propria supply chain.
- **Compliance**: valutazione della capacità del CSP di essere conforme alle normative di legge, ai regolamenti e agli standard di riferimento per il cliente. Sono inclusi: l'aderenza alle normative privacy, la gestione dei dati, l'ubicazione geografica dei data center, e di conseguenza dei dati, le modalità di comunicazione, le coperture assicurative nel caso di violazioni e incidenti e la disponibilità a fornire evidenze di conformità a standard e regolamenti. Occorre sempre determinare le norme applicabili, soprattutto quando si opera su scala globale: per esempio un'organizzazione che offre servizi cloud negli USA è soggetta anche per i server localizzati in Europa ad alcune norme USA (Cloud Act[23]).
- **Business continuity**: valutazione della capacità del provider di garantire la continuità dei servizi offerti e dei dati.
- **Sicurezza infrastrutturale**: politiche e gestione di sicurezza fisica e ambientale (dal controllo degli accessi fisici agli impianti antincendio e antiallagamento), distribuzione dei data center all'interno della stessa regione geografica.
- **Gestione delle identità e degli accessi ai servizi (IAM)**: controllo degli accessi logici a sistemi, apparati, servizi e applicazioni, sia da parte del personale del provider per finalità di gestione sia da parte degli utenti dei clienti per accedere a servizi e dati. Inoltre, le regole relative alle password, la disponibilità di meccanismi di SSO e di autenticazione a più fattori, il monitoraggio degli accessi logici, la connettività via VPN.
- **Protezione dei dati**: valutazione della capacità del provider di proteggere i dati dei clienti da accessi e modifiche non autorizzati, con misure organizzative e tecniche. Tra le organizzative: formazione e audit; tra le tecniche: la crittografia dei dati memorizzati, le procedure di gestione delle chiavi crittografiche, le soluzioni e le procedure di backup e ripristino e la gestione, inclusa la restituzione, dei dati alla cessazione dei contratti.
- **Host, middleware & application security**: misure per la sicurezza dei server

23 https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_en.pdf.

(hardening, patching, sistemi di intrusion detection e intrusion prevention ecc.), del middleware e delle applicazioni (ispezione del codice, adozione di politiche di sviluppo di codice sicuro, ecc.), verifiche periodiche attraverso VA (vulnerability assessment) e PT (penetration testing).

- **Operation & monitoring**: gestione delle patch anche di sicurezza, logging delle attività svolte sui sistemi, monitoraggio dei log e audit, antivirus, strumenti e procedure per la gestione e la notifica degli incidenti di sicurezza.

Sotto il profilo contrattuale e amministrativo, è opportuno valutare se l'offerta del CSP sia congrua con le esigenze del cliente e che i termini della stessa siano chiaramente esplicitati. A questo deve seguire la disponibilità di:

- strumenti di gestione della configurazione e dei servizi attivi;
- strumenti di monitoraggio e reportistica sull'uso effettivo di risorse;
- strumenti di monitoraggio e reportistica sul livello di servizio.

Questi elementi costituiscono il prerequisito per ottenere la trasparenza in fase di fatturazione e dunque abilitano il controllo delle risorse utilizzate e il relativo costo.

Relativamente ai rischi evidenziati nel paragrafo precedente, si suggeriscono nel seguito alcune misure di sicurezza.

5.1.2.1 Governo e sovranità del dato, data protection e privacy

I cloud provider devono offrire ai clienti trasparenza sulla localizzazione dei loro dati, sugli accessi da remoto a essi, sulle operazioni di trattamento eseguite per proprie finalità (p.e. fatturazione, miglioramento del prodotto) in qualità di titolare e su quelle condotte in qualità di responsabile[24] e fornire una vasta gamma di protocolli e standard di sicurezza dei dati in accordo con le normative applicabili. Solitamente la localizzazione fisica dei dati ("region") è scelta dal cliente, tra le opzioni disponibili, ed è contrattualizzata.

5.1.2.2 Vendor lock-in

Il rischio è mitigato mediante l'adozione di formati e standard aperti, più facilmente adottabili nel contesto **IaaS** e **PaaS**. Nel contesto **SaaS** vi possono essere difficoltà nella portabilità dei dati a causa dei differenti formati e modelli implementati dai vari fornitori.

5.1.2.3 Indisponibilità del servizio

I cloud provider dovrebbero assicurare: un ambiente sicuro per ogni cliente, data center distribuiti geograficamente, domini multipli, ecc.

24 https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf.

Nel contesto **IaaS**, il cloud provider può mettere a disposizione dei clienti specifici servizi, architetture di riferimento e funzionalità per erogare servizi a elevata disponibilità. In questo scenario il cloud provider è responsabile della disponibilità dell'infrastruttura fisica, mentre il cliente è responsabile dell'architettura e dell'implementazione del servizio.
In generale, nel contesto **PaaS** e in quello **SaaS**, la responsabilità della disponibilità del servizio e del rispetto degli SLA contrattualizzati è in carico al cloud provider. Il cliente dovrebbe accertare la presenza di soluzioni affidabili di disaster recovery.

5.1.2.4 Inadeguata formazione

Trasversalmente ai servizi **IaaS**, **PaaS** e **SaaS**, è richiesta una specifica e adeguata formazione del personale ICT al fine di mitigare i rischi di incremento dei costi di trasformazione dei servizi verso il cloud, di sicurezza (ad esempio per configurazioni insicure), di indisponibilità del servizio. Nel modello SaaS, i clienti possono essere PMI, professionisti o consumatori privati che, anche in questo caso, sono spesso non adeguatamente formati.

5.2 Software

Il software si può classificare in relazione ai modi di realizzazione, alle finalità, alle caratteristiche di aggiornamento e manutenzione, ecc. Per quanto attiene alle modalità di produzione, esso è disponibile nelle forme:

- Prodotto (o pacchetto): as-is, come ideato e sviluppato dal vendor, senza necessità di ulteriori sviluppi e personalizzazioni;
- Progetto: ad-hoc, appositamente sviluppato, eventualmente come adattamento di un prodotto.

Relativamente al livello di astrazione che esso implementa, si può distinguere in:

- software di base: finalizzato alla gestione delle risorse hardware (p.e. sistema operativo, firmware, driver, scheduler);
- middleware: costituente lo "strato di mezzo" cui, generalmente, sono relegati i compiti di trasporto delle informazioni;
- software applicativo: che costituisce l'interfaccia con l'utente finale, fornendo specifiche funzioni operative (es. emissione fatture, bonifici, contabilità, partita doppia).

Le relazioni tra hardware, software di base e software applicativo è illustrata in maniera molto semplificata in figura.

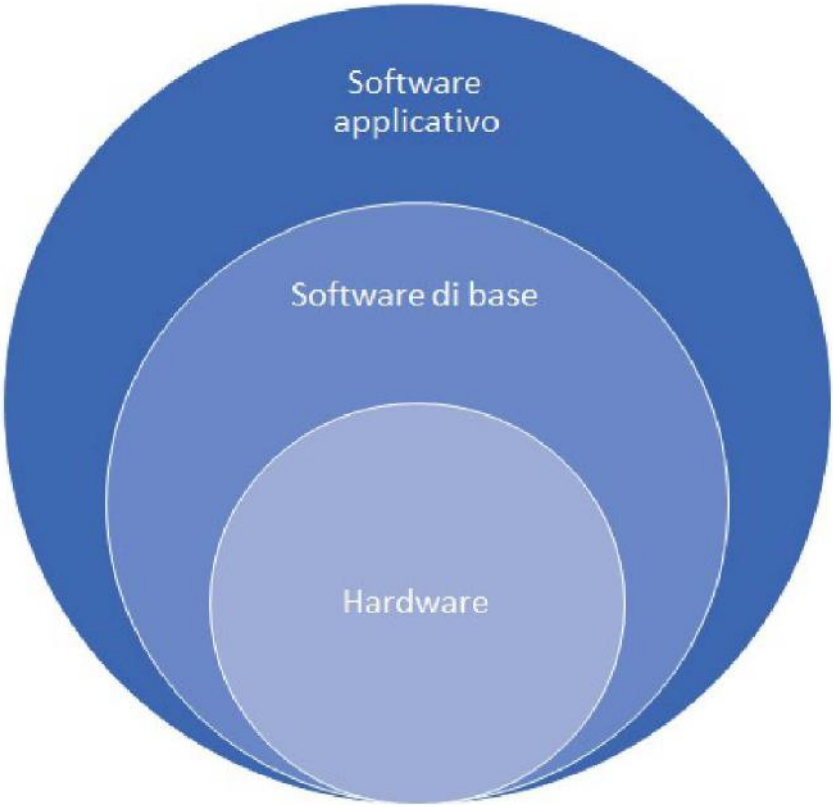


Figura 5 – Relazione tra hardware, software di base e software applicativo.

5.2.1 Scenari di rischio

In generale, per tutti i software (incluso il software di base per l'IoT) esiste una forte dipendenza dal produttore o dallo sviluppatore, dai suoi processi di sviluppo, di manutenzione e di distribuzione delle patch.

5.2.1.1 Inserimento di software dannoso durante lo sviluppo

I software potrebbero includere software dannoso o malware o non essere stati progettati o sviluppati in modo corretto e presentare quindi vulnerabilità o malfunzionamenti (questi, anche se non sono sfruttabili da malintenzionati, arrecano comunque danni all'organizzazione che li utilizza).

Oggigiorno le dipendenze software sono pervasive. In un progetto software si trovano in media 203 dipendenze da progetti open source[25]. Inoltre, i dati del settore suggeriscono che il 99% del software contiene codice open-source e che tra l'85 e il 97% dei software specifici di un'organizzazione provengono dall'open-source[26].

Essere in grado di sfruttare il lavoro di migliaia di sviluppatori open source significa che migliaia di estranei hanno lavorato sul codice. Questo costituisce un indubbio vantaggio in termini di efficienza e di tempi di sviluppo, di acquisizione di competenze spesso non disponibili in azienda: questo fatto ha portato all'adozione molto ampia di componenti sviluppati da terzi (sia aziende che community open source), accettando implicitamente i relativi rischi: si veda il caso di Log4j descritto di seguito.

Se una di queste dipendenze presenta una vulnerabilità, è molto probabile che i progetti che le utilizzano abbiano la stessa vulnerabilità. Inoltre, a peggiorare le cose è il fatto che una dipendenza potrebbe cambiare a insaputa degli utilizzatori e potrebbero essere introdotte nuove vulnerabilità.
L'elevata numerosità dei sistemi su cui sono spesso installati i pacchetti è un altro elemento significativo, visto che, in presenza di vulnerabilità, gli attaccanti hanno la possibilità di compromettere e di prendere il controllo di un gran numero di sistemi.

Un problema di sicurezza dei software è l'**utilizzo di librerie open source**. Tali librerie hanno in alcuni casi un utilizzo molto ampio, e sono integrate anche all'interno di software commerciale senza nessun contributo allo sviluppo da parte del vendor, e in maniera a volte non trasparente per gli utenti finali. La presenza di vulnerabilità su tali librerie può essere difficile da correggere da parte degli utenti anche in presenza delle patch, in quanto gli utilizzatori sono spesso inconsapevoli di quali siano i sistemi sui quali le librerie da aggiornare sono installate.

Un attacco alla software supply chain si verifica quando del codice dannoso è aggiunto intenzionalmente a un componente, utilizzando la supply chain di quel componente per distribuire il codice alle potenziali vittime (obiettivi). Esistono diversi metodi per attaccare una supply chain:

- accedere abusivamente al codice sorgente e modificarlo introducendo malware;
- partecipare a progetti open source cooperativi al fine di introdurre malware nel codice sorgente;

25 https://github.blog/2020-09-02-secure-your-software-supply-chain-and-protect-against-supply-chain-threats-github-blog/.
26 https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html

- acquisire l'account di un partecipante al progetto per introdurre malware nel codice sorgente a suo nome;
- compromettere una chiave di firma per distribuire software che non fa ufficialmente parte di un componente.

Famosi esempi di problemi di questo tipo sono la vulnerabilità della libreria Log4j[27], diventata di pubblico dominio a fine 2021, che potrebbe essere sfruttata per eseguire codice arbitrario sui sistemi, e quella della libreria OpenSSL (Heartbleed[28]) rilevata nel 2014, che potrebbe essere sfruttata per accedere a informazioni sensibili trasmesse nel canale cifrato.

Facendo invece riferimento al closed source (prodotti software i cui creatori limitano l'uso del codice sorgente), sono presenti rischi relativi alla presenza di backdoor o vulnerabilità note non mitigate. Esemplificativo è il caso delle soluzioni di sicurezza informatica fornite da organizzazioni legate alla Federazione Russa, a seguito della recente guerra in Ucraina. Sebbene non le citi esplicitamente, a inizio 2022 l'Agenzia per la Cybersicurezza Nazionale (ACN) ha ritenuto essere alto il corrispondente rischio per la sicurezza nazionale[29].

Relativamente al software di base, è necessario considerare l'ampio impatto di eventuali vulnerabilità che insistono su di esso. Infatti, operando a basso livello e interfacciandosi con l'hardware, gode generalmente di ampi privilegi: lo sfruttamento delle vulnerabilità può pertanto permettere agli attaccanti di guadagnare accessi privilegiati ai sistemi.

5.2.1.2 Qualità insufficiente

Per quanto la qualità non venga spesso associata alla sicurezza, un software sviluppato non correttamente (p.e. non seguendo standard di codifica sicura) o con funzionalità non adeguate può portare a problemi di integrità e disponibilità delle informazioni.

5.2.1.3 Compromissione della distribuzione del software

Altri scenari da tenere in considerazione sono quelli relativi alla **distribuzione del software** agli utilizzatori. In questo caso gli attaccanti possono provare a sfruttare le tattiche per compromettere il software e gli aggiornamenti mentre transitano nei sistemi di distribuzione; questi metodi sono simili agli attacchi man-in-the-middle

27 https://logging.apache.org/log4j/2.x/security.html.

28 https://heartbleed.com/.

29 https://www.csirt.gov.it/crisi-ucraina-analisi-del-rischio-tecnologico-e-diversificazione.

(MITM) sui canali di comunicazione, e tentano di iniettare codice dannoso o vulnerabilità per un successivo sfruttamento. Esiste inoltre la possibilità di compromettere direttamente il sistema di distribuzione: ciò può includere il repository, il gestore dei pacchetti e altri strumenti che consentono di consegnare il software ai clienti.

5.2.1.4 Difficoltà di aggiornamento

Ulteriori problemi si hanno in alcuni ambiti come quello industriale e dei dispositivi medici, dove l'installazione di patch del sistema operativo deve essere certificata dal vendor del software applicativo perché potrebbe comprometterne il funzionamento. Il processo di certificazione può richiedere diverso tempo e ciò può portare ad avere sistemi operativi a cui non sono state applicate patch di sicurezza o, peggio ancora, versioni di sistemi operativi obsolete e non più supportate dal produttore.

5.2.2 Esempi di attacchi ai pacchetti software

Di seguito sono presentati alcuni esempi di attacchi alla supply chain software.

5.2.2.1 Attacco alla libreria event-stream

La libreria event-stream[30] Node.js è ampiamente utilizzata. Essa è un progetto open source aperto alla comunità degli sviluppatori. Nell'autunno del 2018, un nuovo utente si offrì volontario per rilevare il flusso di eventi su GitHub[31]. Il gestore accolse con favore l'aiuto extra e concesse i diritti di pubblicazione al nuovo arrivato. Poche settimane dopo, il nuovo utente aggiunse una nuova dipendenza a event-stream, flatmap-stream. La settimana successiva, lo stesso utente riscrisse il codice per non richiedere più la dipendenza flatmap-stream e provò a rimuoverlo. Il codice malevolo aveva come target l'applicazione Copay per la gestione di portafogli bitcoin; era progettato per raccogliere dettagli degli account e delle relative credenziali che avessero un saldo maggiore di 100 bitcoin o di 1000 bitcoin cash.

5.2.2.2 Attacco a Codecov

Un altro esempio più recente è quello che colpì Codecov[32], strumento di code coverage che controlla quanto codice sorgente dell'applicativo analizzato è sottoposto a test. Nella figura successiva è rappresentato l'attacco. Il processo di creazione del container Codecov aveva un bug, presente nei container disponibili pubblicamente (1). Gli utenti malevoli riuscirono ad accedere al container e ottennero le credenziali Codecov per accedere al repository (2). Modificarono quindi lo script bash di Codecov (3) e la modifica fu propagata in tutti i client che utilizzavano lo strumento (4). Lo script bash malevolo aveva il compito di raccogliere le credenziali dei vari clienti in

30 https://github.com/dominictarr/event-stream.

31 https://blog.npmjs.org/post/180565383195/details-about-the-event-stream-incident.

32 https://about.codecov.io/.

modo tale da accedere ai dati degli stessi (ad esempio al codice sorgente) (6).

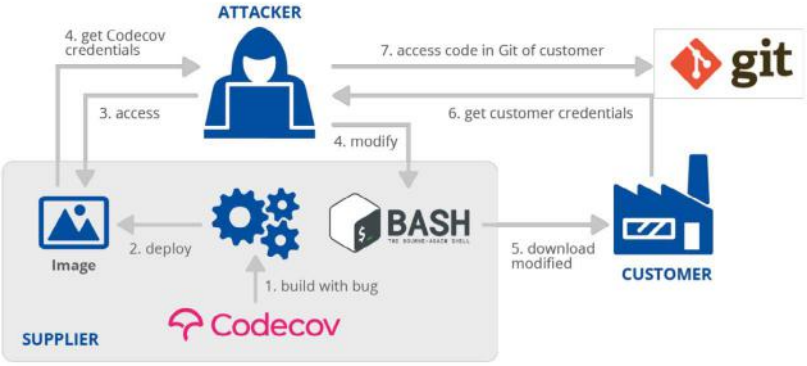


Figura 6 – Codecov supply chain attack[33]

5.2.3 Buone Pratiche

5.2.3.1 Inserimento di software dannoso durante lo sviluppo

Un aspetto chiave dell'open-source è la trasparenza, ovvero la possibilità di ispezionare il codice e le relative dipendenze. Proprio questo aspetto permette di mitigare il rischio di fornitura. Attraverso l'analisi del codice è infatti possibile:

1. identificare tutte le dipendenze software e la loro versione; questo permette di realizzare un inventario delle componenti (software composition analysis o SCA);
2. identificare le componenti dell'inventario obsolete o vulnerabili;
3. correggere o mitigare le vulnerabilità tramite l'aggiornamento delle componenti obsolete o vulnerabili.

Si possono prevedere analisi molto accurate del codice per identificare vulnerabilità nuove (ad esempio, tramite analisi statica o dinamica del codice, anche manuale, laddove si abbiano le competenze e le componenti siano particolarmente critiche).

Per i fornitori che sviluppano software ad hoc è possibile verificare se usano processi e regole di sviluppo e codifica sicura.

In alcuni casi l'approvvigionamento di beni, servizi e sistemi ICT è regolamentato per legge, nello specifico per i soggetti pubblici o privati che forniscono un "servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali

33 Fonte: https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply chain-security-attacks.

per gli interessi dello Stato", ossia facenti parte del PSNC (vedere paragrafo 8.3). Non si tratta quindi di soli operatori pubblici ma anche di privati o di privati a partecipazione statale. In questi casi, sono previste verifiche relative alla qualità tecnica e alla sicurezza, che includono l'analisi di possibili backdoor e vulnerabilità. Nel caso di dispositivi medici, le norme tecniche di attuazione delle indicazioni normative (su Regolamenti europei) richiedono che il fornitore documenti tutte le dipendenze e che, nelle attività seguenti l'immissione sul mercato, vigili sulle vulnerabilità e sui relativi aggiornamenti[34].

Tutte le maggiori piattaforme di collaborazione allo sviluppo software sono dotate di strumenti automatici capaci di supportare il processo o permettono l'integrazione con strumenti di terze parti dedicati a tale scopo. Ad esempio, GitHub supporta in maniera nativa la mitigazione da vulnerabilità note[35].

Quando però si usa software closed source, risulta impossibile ispezionare il codice e quindi di verificare l'assenza di backdoor o di funzionalità che permettano attacchi o monitoraggi esterni illeciti.

Il CERT-FR, in risposta al caso della backdoor GoldenSpy ha affrontato in un report dedicato[36] il tema dell'integrazione di software non affidabile. Esso indica raccomandazioni relative a:

- infrastruttura;
- accesso al software;
- mantenimento delle misure di sicurezza;
- detection.

Inoltre, nel report si raccomanda di aggiornare la mappa della rete, per facilitare la supervisione delle aree segmentate e l'identificazione di potenziali percorsi di compromissione.

È opportuno menzionare le piattaforme di *software composition analysis*. Esse consentono di ottenere visibilità sulla composizione di un software, generando una SBOM (Software bill of materials) con informazioni circa i moduli e le librerie incorporate, le versioni, le dipendenze e le configurazioni. Tali informazioni sono estremamente utili per identificare vulnerabilità già note e forniscono un contributo per individuare nuove vulnerabilità.

34 MDCG 2019-16 - Guidance on Cybersecurity for medical devices https://ec.europa.eu/docsroom/documents/41863.

35 https://docs.github.com/en/organizations/keeping-your-organization-secure/managing-security-settings-for-your-organization/managing-security-and-analysis-settings-for-your-organization.

36 https://cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-007/.

Per quanto riguarda software provenienti da Paesi potenzialmente insicuri, l'ACN, con l'emanazione della circolare n. 4336[37], ha ordinato alle amministrazioni pubbliche di "procedere alla diversificazione delle seguenti categorie di prodotti e servizi tecnologici di sicurezza informatica: prodotti e servizi della società Kaspersky Lab, Group-IB e Positive Technologies" e ha suggerito misure e buone prassi di gestione di servizi informatici e del cyber-rischio.

5.2.3.2 Qualità insufficiente

È evidente che, in questo scenario complesso, lo strumento di controllo principale risulta essere il contratto tra fornitore e committente.

Il contratto di sviluppo del software viene definito un contratto atipico volto a regolamentare il rapporto che si instaura tra il committente che richiede la realizzazione di un software personalizzato e il concedente (software house) che viene incaricato di mettere in atto il progetto[38].

Essendo il contratto di sviluppo del software atipico, la normativa italiana riconduce la sua disciplina al contratto di appalto dove si prevede che lo sviluppatore elabori il software sulla base delle esigenze manifestate dal cliente; la software house procede con lo sviluppo, organizzando i mezzi necessari e assumendosi la gestione a proprio rischio.

Più precisamente, il contratto di sviluppo del software è un accordo che ha come oggetto il custom-made software, ossia il programma informatico fatto su misura[39] per il cliente.

L'art. 105 del Codice dei contratti pubblici (D. Lgs. 50 del 2016) definisce il sub-appalto quale "contratto con il quale l'appaltatore affida a terzi l'esecuzione di parte delle prestazioni o lavorazioni oggetto del contratto di appalto".

Al subappaltatore è richiesto un coinvolgimento imprenditoriale e organizzativo in relazione all'esecuzione dell'appalto principale[40].

È opportuno stabilire regole di qualità e di sviluppo sicuro nei contratti. Si consiglia di fare riferimento a riferimenti comuni, evitando di indicare requisiti troppo specifici.

37 https://www.gazzettaufficiale.it/eli/id/2022/04/26/22A02611/sg.

38 https://www.iusinitinere.it/il-contratto-di-sviluppo-software-34736

39 https://www.to.camcom.it/sites/default/files/regolazione-mercato/11990_CCIAATO_832011.pdf.

40 https://www.lavoripubblici.it/documenti2021/lvpb4/vademecum-subappalto-ance-2021.pdf.

AgID ha dato diverse indicazioni in merito[41]. Anche il Cyber Security Framework nazionale[42] costituisce un utile modello, derivato dal NIST Cyber Security Framework[43]. Sono rilevanti anche altre pubblicazioni del NIST[44], quelle del CISA[45] e diverse iniziative di OWASP[46], tra cui un modello sulla maturità del ciclo di sviluppo[47] e altri progetti che coprono le diverse fasi[48] e tecnologie[49]. Per sistemi critici, vengono presi a riferimento i Common Criteria[50]. Significativi sono anche i contributi di Cloud Security Alliance[51] e di alcuni vendor[52]. Per applicazioni in contesti particolari (trasporti) in cui un errore potrebbe causare perdite di vite umane vi sono standard specifici[53].

Si rende innanzitutto necessaria una valutazione dei rischi per la sicurezza delle informazioni e una valutazione d'impatto per garantire la tutela dei dati sensibili[54].

In questo contesto possono risultare utili il documento di ENISA in merito agli standard[55] e alla certificazione dei prodotti[56] secondo il Regolamento (EU) 2019/881 (Cybersecurity Act[57]).

Il committente deve quindi stabilire processi per verificare la qualità e la sicurezza del codice, attraverso audit, un monitoraggio adeguato, test condotti direttamente o da altri fornitori con specifiche competenze, verifiche da parte di personale specializzato o attraverso l'analisi dei resoconti di test. Per i casi più critici, le attività di verifica indipendente di prodotto secondo lo standard ISO/IEC 17065 sono richieste normativamente e la Commissione europea mantiene un elenco di enti che possono certificare i prodotti.

41 https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict; https://www.agid.gov.it/it/infrastrutture/cloud-pa; https://docs.italia.it/AgID/documenti-in-consultazione/lg-procurement-ict/it/bozza/index.html; https://www.agid.gov.it/sites/default/files/repository_files/allegato_1_linee_guida_per_ladozione_di_un_ciclo_di_sviluppo_di_software_sicuro.pdf.

42 https://www.cybersecurityframework.it/.

43 https://www.nist.gov/cyberframework.

44 https://www.nist.gov/publications/system-development-life-cycle-sdlc e https://csrc.nist.gov/Projects/ssdf.

45 https://www.cisa.gov/uscert/sites/default/files/publications/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF.

46 https://owasp.org/.

47 https://owasp.org/www-project-samm/

48 https://owasp.org/www-project-web-security-testing-guide/ e https://wiki.owasp.org/index.php/Projects/OWASP_Development_Guide.

49 https://owasp.org/www-project-mobile-app-security/.

50 https://www.commoncriteriaportal.org/.

51 https://cloudsecurityalliance.org/artifacts/devsecops-pillar-4-bridging-compliance-and-development/.

52 https://www.microsoft.com/en-us/securityengineering/sdl.

53 https://dit.sa.gov.au/__data/assets/pdf_file/0009/667935/Safety_Assurance_Framework.PDF.

54 https://www.cybersecurity360.it/soluzioni-aziendali/la-sicurezza-informatica-nello-sviluppo-del-software-le-buone-regole-da-seguire.

55 https://www.enisa.europa.eu/publications/threat-landscape-for-supply chain-attacks.

56 https://www.enisa.europa.eu/topics/standards.

57 https://eur-lex.europa.eu/eli/reg/2019/881/oj.

5.2.3.3 Compromissione della distribuzione del software

Le organizzazioni possono innanzitutto utilizzare meccanismi di transito sicuro, sfruttare hashing e firme digitali sia a livello di prodotto che di componente software, nonché implementare sistemi di crittografia e controllo degli accessi al codice. Molte norme, come ad esempio la ETSI 303-645 (al punto 5.7) e la IEC 62443-4-1 (dal SM-6 al SM-10), richiedono sistemi di cifratura del codice, di avviso in caso di tentata modifica, di gestione della catena delle chiavi e dei certificati sia propri sia di terze parti fornitrici. In particolare, le firme digitali aiutano a proteggere l'integrità degli artefatti software e forniscono maggiori garanzie ai consumatori. Tuttavia, se il server di firma o il meccanismo stesso dovessero essere compromessi, tali assicurazioni non sarebbero più affidabili o utili perché la compromissione consentirebbe agli attaccanti di firmare legittimamente artefatti dannosi da loro prodotti. Per mitigare questo rischio si raccomanda l'adozione di controlli come un'efficace autenticazione multi-fattore (MFA) e il controllo dell'accesso fisico all'infrastruttura di firma; inoltre, la firma dovrebbe avvenire su segmenti di rete isolati e configurati appositamente per questo scopo, rafforzando in questo modo l'intera infrastruttura di firma.

5.2.3.3 Difficoltà di aggiornamento

Il cliente non deve limitarsi a richiedere a un fornitore il solo sviluppo o il solo prodotto, ma anche le indispensabili successive attività di aggiornamento. Pertanto deve valutare preliminarmente il fornitore e in particolare:

- disponibilità di un servizio di supporto e manutenzione;
- capacità dell'organizzazione di sopravvivere nel tempo, garantendo un adeguato supporto al componente;
- disponibilità del software bill of materials (SBOM), ossia la possibilità di individuare tutte le librerie esterne che sono integrate nel componente;
- velocità nel distribuire aggiornamenti per risolvere le vulnerabilità individuate;
- ampio livello di diffusione e utilizzo dei componenti;
- modalità sicura di distribuzione degli aggiornamenti software e tempi di rilascio in relazione alla pericolosità della vulnerabilità riscontrata.

Nel caso in cui, almeno temporaneamente, non siano disponibili patch o non siano installabili a causa di dipendenze, è comunque opportuno adottare adeguati controlli per mitigare il rischio conseguente al mancato aggiornamento (p.e. controllo del traffico con firewall).

5.2.3.5 Marketplace ufficiali

Una delle modalità con cui è possibile valutare il servizio offerto, in particolare da un fornitore di servizi cloud, è quello di avvalersi di un marketplace ufficiale. Esempi sono quelli usati dalle Pubbliche Amministrazioni, che valutano in modo oggettivo e secondo processi standard la qualità dei servizi offerti.

La prassi di utilizzare un servizio di questo tipo per rendere disponibili alle Pubbliche Amministrazioni un elenco di fornitori qualificati trova riscontro in diversi Paesi.

Questa prassi ha innumerevoli vantaggi. Ogni singolo ente avrebbe infatti difficoltà a valutare le capacità di un fornitore. Inoltre, valutazioni sullo stesso fornitore effettuate da enti differenti, senza uniformità nei criteri di audit, potrebbero portare a esiti completamente diversi, in funzione della metodologia utilizzata e della capacità degli auditor. In questo modo non si avrebbero risultati comparabili, comportando, da un lato, difficoltà nel riuso da parte di un ente di un'attività di verifica svolta da un altro ente. D'altro lato ripetute attività di verifica svolte da enti diversi comporterebbero un impegno che per il fornitore potrebbe risultare insostenibile sia in termini di tempo da dedicare agli auditor dei vari enti, sia per i rischi connessi all'attività di audit per gli altri clienti del fornitore.

A fronte degli indubbi vantaggi occorre considerare che le attività del gestore del marketplace sono principalmente di verifica formale di aderenza ai criteri di ammissione all'albo, basandosi in molti casi su verifiche di terze parti (certificatori di sistema di gestione) senza operare direttamente test di sicurezza (p.e. vulnerability assessment).
Un esempio particolarmente significativo di marketplace ufficiale è quello di FedRAMP[58] (Federal Risk and Authorization Management Program), ente USA il cui compito è "fornire un approccio standardizzato alle autorizzazioni di sicurezza per le offerte di servizi in cloud".

Anche la Pubblica Amministrazione italiana ha il suo marketplace per le soluzioni cloud[59]. Esso espone i servizi e le infrastrutture qualificate da AgID.

5.3 Gestione del software

Il software, oltre a essere sviluppato e acquisito, deve essere gestito. La sempre maggiore pervasività e integrazione del software in tutti gli ambiti, unita alla sua

58 https://www.fedramp.gov/.
59 https://catalogocloud.agid.gov.it/.

crescente complessità e alla specializzazione richiesta al personale che gestisce gli applicativi, porta a un uso massivo di fornitori, con una conseguente complessità delle pratiche e delle procedure che permettono una gestione sicura.
Questo caso è diverso da quello dei servizi SaaS, in quanto il software è maggiormente sotto il controllo dell'organizzazione.

Il controllo della supply chain può essere complesso se si considera che un'organizzazione può rivolgersi a un fornitore di servizi cloud IaaS, un altro che gestisce i servizi infrastrutturali (sistema operativo, qualche middleware e RDBMS), un altro per un determinato applicativo che, a sua volta, ha affidato i servizi di conduzione operativa (monitoraggio, assistenza, abilitazione degli utenti applicativi) a un suo subfornitore.

Nel caso invece di esternalizzazione di servizi non ICT (per esempio servizi di consegna, trasporto, noleggio di beni), i relativi fornitori potrebbero a loro volta avvalersi di fornitori ICT senza le necessarie competenze in materia di sicurezza.

5.3.1 Scenari di rischio

Nel seguito si riportano alcuni dei principali rischi relativi alla gestione del software, restando inteso che qui la trattazione è rivolta al caso in cui sia coinvolta una terza parte.

5.3.1.1 Inserimento di malware in esercizio

Un attaccante potrebbe riuscire ad inserire un malware attraverso un fornitore.
Come già in parte richiamato, l'inserimento di codice malevolo può provocare:

- data leakage: esfiltrazione di dati, anche sensibili, senza la consapevolezza dell'organizzazione;
- blocco o interruzione di funzionalità tecniche e operative, allo scopo di danneggiare l'organizzazione stessa o richiedere un riscatto;
- alterazione di codici o informazioni (p.e. IBAN), volte al furto attraverso la modifica di transazioni finanziarie;
- alterazione della capacità di presidio e monitoraggio dei processi per avviare tentativi di frode.

5.3.1.2 Compromissione dell'integrità dei dati

Si elencano nel seguito alcuni casi:

- perdita di dati, a causa del non corretto processo di memorizzazione;

- alterazione di dati, a causa del non corretto controllo formale e logico dei dati stessi;
- corruzione dei dati, a livello di modello logico.

5.3.1.3 Qualità insufficiente

La messa in esercizio di software non adeguatamente controllato a livello di qualità può:

- abilitare l'inserimento di malware;
- non garantire adeguatamente l'integrità dei dati;
- ridurre il livello di sicurezza dei dati e delle infrastrutture;
- non garantire il rispetto delle esigenze dell'organizzazione in termini funzionali, come il rispetto dei livelli di servizio richiesti;
- non abilitare adeguatamente gli strumenti di controllo e presidio (logging e monitoring).

5.3.1.4 Perdita di proprietà intellettuale

L'insieme delle conoscenze e dell'esperienza aziendale acquisite nello sviluppo interno di un software, che si configura come proprietà intellettuale, è frutto di investimenti di tempo, capacità, impegno del personale e risorse economiche. Qualora il coinvolgimento di un fornitore comporti la perdita di tali conoscenze, in toto o in parte, ne potrebbe derivare un danno all'organizzazione in termini di competitività.

5.3.1.5 Change management

Il ciclo di vita delle componenti software (requisiti, sviluppo, verifica e controllo, messa in esercizio) può evidenziare problematiche quali:

- introduzione di cambiamenti non previsti o non richiesti con scopo anche malevolo;
- non coerenza delle modifiche con i requisiti funzionali;
- non coerenza delle modifiche con i livelli di servizio richiesti;
- qualità non adeguata, possibile causa di incidenti;
- introduzione di carenze nei presidi di sicurezza dei dati e delle infrastrutture;
- mancata disponibilità.

5.3.1.6 Accesso da parte del gestore

I rischi relativi all'accesso remoto sono discussi in generale al paragrafo 5.9. Si rileva qui che le credenziali e gli strumenti di accesso remoto a disposizione del gestore

possono essere usati impropriamente da persone diverse rispetto a quelle inizialmente stabilite, soprattutto se i fornitori usano credenziali generiche e non personali o il processo di gestione delle credenziali non è sufficientemente efficiente (che sia gestito dal cliente o dal fornitore perché, per esempio, non sono cambiate le credenziali di un amministratore di sistema a seguito di dimissioni o licenziamento).

Su questo tema si osservi che, in caso di offshore, è necessario considerare le differenze culturali tra cliente e fornitori, non sempre consapevoli allo stesso modo dei rischi.

In ambito industriale, macchine e linee sono connesse in maniera più o meno occulta con il costruttore, o a tutte le possibili diramazioni e connessioni delle soluzioni multi-cloud presenti in ogni livello dell'organizzazione.

5.3.1.7 Perdita di competenze

Come già indicato al paragrafo 5.3.1.4, la perdita di conoscenza e di specializzazione è uno dei possibili rischi per l'organizzazione che esternalizza.

Tale perdita di know-how, ma anche di sensibilità, può portare in particolare ad una riduzione dei controlli su quanto si acquisisce, con una progressiva diminuzione della qualità del software e un aumento del rischio cyber.

5.3.2 Buone pratiche

Si forniscono a seguire alcune indicazioni su come trattare i rischi precedentemente evidenziati.

5.3.2.1 Inserimento di malware in esercizio

Il monitoraggio e il controllo delle vulnerabilità standard (CVE) o non ancora standardizzate (zero-days) dei software applicativi, delle librerie, dei sistemi operativi, dei dispositivi elettronici e in generale di ogni sistema informatico permette di abbattere sensibilmente i fattori di rischio, non necessariamente solo all'interno ma anche all'esterno del perimetro di rete.
Attraverso l'uso di adeguate tecnologie, che si appoggiano a database standard e laboratori specializzati, è possibile estendere il perimetro di analisi, con criteri predefiniti, su tutta la supply chain.

5.3.2.2 Compromissione dell'integrità dei dati

In generale, garantendo la qualità del software mediante la corretta gestione del processo di change management, si ha un buon presidio di tale rischio.

È inoltre opportuno valutare la possibilità di implementare sistemi di crittografia dei dati e di firma digitale dei log, in modo da prevenire qualsiasi tipo di manipolazione o di accesso non autorizzato ai dati, così come quella di avere un fornitore differente per il SOC.

5.3.2.3 Qualità insufficiente

Per assicurare un buon livello di qualità del software deve essere seguito un processo definito di sviluppo e manutenzione. Tale processo può basarsi su approcci cosiddetti waterfall (in cui a inizio progetto si completano l'identificazione dei requisiti e la pianificazione) o Agile (in cui i requisiti da sviluppare sono scelti all'inizio di ciascun "ciclo", la cui durata è costante per tutto il progetto ed è solitamente di 3 o 4 settimane).

A prescindere dall'approccio, è necessario che il software venga verificato attraverso test tecnici e funzionali, anche delle funzioni di sicurezza, in modo da verificarne la correttezza. L'esecuzione dei test dovrebbe essere svolta in ambiente distinto da quello di sviluppo (e, ovviamente, da quello di produzione) e anche da persone diverse dagli sviluppatori, in modo che non siano sottovalutati o, in caso di attacchi intenzionali, alterati fraudolentemente.

Tra le funzioni di sicurezza da verificare vanno ricordate quelle di identificazione, autenticazione, autorizzazione, logging e monitoring (o di interfacciamento con altri software che forniscono queste funzioni).

Nell'ambito delle supply chain, il cliente dovrebbe condividere con il fornitore le caratteristiche del processo e le modalità con cui può essere controllato (p.e. con strumenti di change management, con la condivisione dei rapporti di test, facendo svolgere i test da un'entità distinta dallo sviluppatore, utilizzando strumenti SAST e DAST di analisi del codice).

5.3.2.4 Perdita di proprietà intellettuale

La titolarità dei diritti d'autore sull'opera realizzata dallo sviluppatore rappresenta uno degli aspetti più critici di questa fattispecie.

La normativa ha ricondotto i software nella categoria delle opere coperte da diritto d'autore e pertanto ritenuti meritevoli di protezione dall'ordinamento italiano[60].

In particolar modo, il software trova riconoscimento normativo nella Legge n. 633/1941 in materia di diritto d'autore; il software si qualifica come opera di ingegno

60 https://legalfordigital.it/copyright/proprieta-intellettuale-software/.

a carattere creativo e trova tutela contro la riproduzione totale o parziale nella sua duplice forma del codice oggetto e codice sorgente.

Il contratto di sviluppo software non comporta per forza il diritto di acquisizione da parte del cliente dei diritti di proprietà intellettuale. Tutto ciò trova fondamento e conferma nell'art. 4 della Legge 81/2017[61], dove è stabilito che, in assenza di espressa pattuizione, i diritti rimangono in capo all'autore del software.

Nella redazione di un contratto di sviluppo software è importante capire quali sono le esigenze dei contraenti:

- il committente, se la software house non mantiene più il software (per chiusura completa o di una linea o per altri motivi), deve poter recuperare il codice; per questo si possono prevedere misure di code escrow;
- la software house, che realizza programmi simili per clienti differenti, può avere interesse nel mantenere integro il diritto di utilizzare porzioni dei codici, riservandosi i diritti di sfruttamento dei codici e limitando gli utilizzi consentiti del programma in relazione a ciò di cui ha realmente bisogno il committente;
- il committente potrebbe richiedere un periodo minimo di manutenzione (evolutiva e correttiva), per esempio 10 anni, del software sviluppato.

5.3.2.5 Change management

La gestione della configurazione, la corretta archiviazione così come l'inventario dei software applicativi sviluppati e in uso sono buone pratiche che permettono di innalzare il livello di protezione di tutti gli asset informatici a tutti i livelli dell'organizzazione e della supply chain. Queste attività sono richieste da diversi standard di settori quali ISO/IEC 20000, ISO/IEC 27001 e ISO 9001 e dalle buone prassi ITIL.

È opportuno conoscere esattamente la configurazione, intesa come l'elenco delle versioni o della tipologia di quanto sia caratterizzante di ciascun asset informatico. Questo permette di migliorare sensibilmente le attività (sviluppo, manutenzione, obsolescenza e dismissione) e la sicurezza delle informazioni. Di seguito un elenco di elementi da monitorare:

- software applicativi;
- sistema operativo;
- strumenti di sviluppo e debugging;
- middleware (RDBMS, application server, librerie, incluse quelle crittografi-

61 https://www.gazzettaufficiale.it/eli/id/2017/06/13/17G00096/sg.

che);
- patch o SIM installate;
- BIOS.

Esistono numerosi strumenti che possono supportare la gestione della configurazione di quasi tutti i tipi di asset informatici (dai server, ai portatili, sino ad arrivare ai dispositivi OT).

Si possono inoltre prendere in considerazione le seguenti ulteriori indicazioni:

- regolamentare il processo per gli aggiornamenti e assicurare che siano fatti con condizioni contrattuali e SLA;
- prevedere l'effettuazione di SAL periodici;
- richiedere un preavviso minimo per i futuri cambi, al fine di consentire un'adeguata pianificazione delle attività;
- precisare in dettaglio la documentazione (manuali) e i test che dovranno essere messi a disposizione.

5.3.2.6 Accesso da parte del gestore

La prima misura per controllare gli accessi da parte del gestore è attivare un processo robusto di gestione delle credenziali e delle autorizzazioni, che includa quindi le attività di registrazione, abilitazione e disabilitazione delle autorizzazioni del personale del gestore e di assegnazione dei permessi per svolgere specifiche operazioni e attività effettuate su un determinato asset.

In uno scenario in cui il concetto di perimetro di sicurezza informatica è sfumato o difficilmente delimitabile il modello che sembra prevalere è quello "zero trust" (ossia "non fidarsi mai, verificare sempre"), per cui i dispositivi non devono essere considerati attendibili per impostazione predefinita, anche se sono connessi a una rete autorizzata come una LAN aziendale e sono stati precedentemente verificati.

Zero Trust è implementato stabilendo una forte verifica dell'identità (ad esempio con un sistema multi-fattore), convalidando la conformità del dispositivo prima di concedere l'accesso, garantendo l'accesso con privilegi minimi solo alle risorse autorizzate in modo esplicito e continuando a monitorare la connessione per verificare eventuali modifiche al contesto.

Resta comunque evidente che, soprattutto per operazioni da remoto, il solo controllo degli accessi può risultare insufficiente per garantire un adeguato livello di sicurezza, soprattutto negli ambiti più critici.

Ad esempio, è possibile disabilitare la modifica o il salvataggio di una configurazione su uno specifico dispositivo, fare il download di una lista di set-point, spegnere un apparato e così via.

Inoltre, tutte le connessioni esterne che transitano su rete pubblica devono essere cifrate, tipicamente attraverso collegamenti di tipo VPN (virtual private network) possibilmente con controllo anti-malware e di anomaly detection in ingresso per mitigare gli effetti dell'accesso esterno di un dispositivo tipicamente "untrusted".

E' importante adottare il principio del privilegio minimo per l'accesso alle risorse di una organizzazione in tutta la supply chain con particolare attenzione agli amministratori di sistema (AdS). In questi casi bisogna applicare principi di separazione dei ruoli, tracciamento delle operazioni e autenticazione a più fattori con password complesse.

Ogni amministratore deve dunque avere un account univoco per la corretta attribuzione delle azioni e non deve poter disporre della capacità di modifica dei log. Inoltre, deve essere separato il personale che si occupa della sicurezza da quello che amministra il sistema per evitare che i controllati siano anche controllori. Chi si occupa di sicurezza deve infine monitorare le attività di rilascio delle credenziali per accesso locale e remoto e l'utilizzo delle stesse, anche con sistemi di rilevazione comportamentale ove necessario.

Il Garante già nel 2008 aveva posto l'attenzione sulla criticità di queste figure tramite il relativo Provvedimento.

5.3.2.7 Perdita di competenze

Per mitigare questo rischio è importante assicurare un'adeguata formazione del personale dell'organizzazione sulle competenze individuate come critiche per il business, pur in un contesto in cui la gestione del software è prevalentemente demandata a terze parti.

5.4 App per dispositivi mobili

Le app per dispositivi mobili possono essere considerate simili ai pacchetti software già affrontati nel paragrafo 5.2. Il loro utilizzo su strumenti personali e spesso non controllati, oltre che la loro facilità di installazione, rende necessaria un'analisi specifica.

5.4.1 Scenari di rischio

5.4.1.1 Malware e applicazioni malevole

Gli utenti fanno riferimento alle app presenti sui vari store. Gli store più noti sono quelli per Android e iOS. Esistono svariati altri store offerti dai produttori dei dispositivi mobili e altri di terze parti. Essi potrebbero differire notevolmente in termini di controlli di sicurezza e privacy.

Pochi utenti, così come le organizzazioni che le adottano, si interrogano sulla sicurezza delle app, ignorando il problema o confidando che qualcuno le controlli. La realtà però ci dice che è un mondo tutt'altro che sotto controllo, alcuni esempi su tutti:

- tra le 250 applicazioni più popolari di Android almeno il 70% consente a terzi non autorizzati di accedere ai dati personali degli utenti;[62]
- a causa della vulnerabilità zero-day, identificata come CVE-2022-32917[63], i prodotti Apple potrebbero permettere ad applicazioni dannose di eseguire codice arbitrario con privilegi del kernel;
- nel 2021 sono stati sottratti i dettagli di circa 380.000 carte di credito dall'applicazione mobile British Airways[64].

Le app possono avere comportamenti malevoli:

- accesso non supervisionato a dati personali e, in generale, riservati;
- upload non autorizzato di dati sensibili verso server esterni;
- violazione delle norme sulla localizzazione geografica dei dati;
- non corretta gestione della crittografia durante il salvataggio o l'invio di dati.

5.4.1.2 Rischi di repacking

Una delle principali caratteristiche del sistema operativo Android è la sua apertura, che gli ha consentito di guadagnare rapidamente quote di mercato ed essere adottato da sempre più organizzazioni.

Di conseguenza, anche lo store principale in cui sono distribuite le app, Google Play, è gestito in modo aperto. Chiunque può registrarsi come sviluppatore di app, acquisendo la possibilità di convalidarle e registrarle.

La distribuzione delle app può, però, avvenire anche in altri modi, incluso il download diretto da Internet del file APK.

62 https://www.hdblog.it/2017/06/02/android-problemi-privacy-app/.
63 https://nvd.nist.gov/vuln/detail/CVE-2022-32917.
64 https://www.wired.it/attualita/tech/2018/09/07/british-airways-carte-credito/.

Questo permette l'operazione di repacking: codice malevolo è inserito nel file APK delle app utilizzando tecniche di reverse engineering. I passi della procedura sono i seguenti:

- Decompilazione: lo strumento di decompilazione baksmali è utilizzato per creare il codice sorgente smali dopo aver estratto il file DEX dal file APK.
- Iniezione e modifica del codice: è aggiunto il codice contenente istruzioni Dalvik VM nel punto di modifica identificato, oppure è aggiornato il codice esistente.
- Modifica al manifesto dell'app: è modificato il nome del pacchetto, in modo da non avere conflitti quando l'app è registrata sullo store di Google.
- Autofirma: Per completare il repacking, l'app modificata è autofirmata.

5.4.1.3 Rischi relativi agli store di terze parti

È di fondamentale importanza per le organizzazioni stabilire lo store da cui scaricare le app sui dispositivi di sua proprietà.

Oltre agli store ufficiali di Google e Apple, che richiedono che le app aderiscano a rigide linee guida e quindi sono considerate a rischio relativamente basso, altri store possono essere creati da sviluppatori indipendenti e da aziende.

Le procedure di verifica della sicurezza e di autorizzazione di uno store potrebbero non essere sufficienti per gli standard stabiliti dall'organizzazione. Alcuni store permettono di distribuire app che forniscono agli utenti un accesso più ampio al sistema, di fornire contenuti rubati o copie gratuite contraffatte di software premium.

La pratica di installare app su dispositivi mobili utilizzando canali diversi rispetto agli store ufficiali è detta "sideloading". Per abilitare il sideloading, gli utenti devono modificare le impostazioni di sicurezza degli smartphone Android procedendo poi all'installazione dell'app attraverso l'interfaccia USB oppure utilizzando app store di terze parti come Amazon, Getjar, Mobogenie, Slideme e Appbrain. Sui dispositivi IOS occorre invece eseguire il jailbreak del dispositivo.

Questo tipo di operazione permette l'installazione di software potenzialmente pericolosi provenienti da fonti dubbie. Nonostante ciò, il sideloading è necessario per l'installazione di programmi sviluppati dall'organizzazione solo per il proprio personale e quindi non disponibili sugli store ufficiali.

5.4.2 Buone pratiche

5.4.2.1 Controlli in fase di sviluppo

Controllo delle vulnerabilità
Difficilmente gli utenti possono verificare la qualità e sicurezza delle app. Le organizzazioni che richiedono sviluppi a fornitori possono invece richiedere l'applicazione di norme di sviluppo sicuro, tra cui quelle OWASP[65].

Offuscamento del codice
L'offuscamento è una tecnica utilizzata per rendere più difficile il reverse engineering del codice sorgente o del codice macchina. L'offuscamento è diviso in due categorie principali: offuscamento del codice sorgente e offuscamento del codice binario. Lo strumento di offuscamento predefinito per sorgenti Java/Kotlin offerto da Android è Proguard.

La logica di controllo del programma, tuttavia, non cambia prima e dopo l'offuscamento, quindi l'attaccante può determinare i ruoli svolti da classi e metodi studiando la logica del software; in questo caso, tuttavia, l'analisi richiede una quantità superiore di tempo, dipendente dalla complessità dell'algoritmo di offuscamento. Per mitigare questo problema sarebbe necessaria una tecnica di offuscamento della logica, come l'offuscamento del controllo, sebbene questo abbia in genere lo svantaggio di ridurre le prestazioni di esecuzione del codice.

Certificazione del codice
Una delle protezioni di sicurezza più efficaci per le app per smartphone che trattano dati sensibili, comprese le app bancarie, è il Trusted Platform Module (TPM). Questo è un sistema su un chip (SoC) che consente l'esecuzione di attività di sicurezza come l'avvio certificato del kernel e del sistema operativo, l'isolamento di applicazioni e l'attestazione remota dell'integrità del dispositivo e del software caricato. In particolare, l'attestazione remota permette di determinare se l'app utente è stata contraffatta prima che i dati siano condivisi tra l'app utente e il server, Inoltre, uno smartphone può eseguire test di integrità statica del codice di esecuzione binario e l'attestazione remota può essere utilizzata per rilevare programmi dannosi mentre sono eseguiti. L'introduzione della verifica dell'integrità delle app basata su TPM, però, comporta costi aggiuntivi dovuti all'hardware necessario per il suo utilizzo.

5.4.2.2 Controlli in fase di acquisizione per gli utenti finali

Gli utenti finali possono verificare su Google Play se gli sviluppatori hanno completato una convalida effettuata da tester indipendenti, visualizzandone i risultati nella

65 https://owasp.org/www-project-mobile-top-10/.

sezione “Sicurezza dei dati”.

La valutazione include considerazioni sulla sicurezza lato client, l’autenticazione del servizio back-end sul cloud e la connettività.

Per quanto riguarda il rilevamento del malware, su Android, gli utenti hanno accesso alla funzione di verifica dell’app Google Play Protect (opzione preattivata).

5.4.2.3 Controlli in fase di acquisizione per le organizzazioni

Analisi delle app
In fase di acquisizione, le organizzazioni possono analizzare le app utilizzando due tipologie di tecniche: analisi statica e analisi dinamica. Per analisi statica si intendono tutte quelle tecniche che analizzano i file (APK o IPA) con l’obiettivo di individuare pattern di vulnerabilità, codice malevolo e informazioni hardcoded (ad esempio password). Le tecniche di analisi dinamica comprendono le tecniche che verificano l’app durante la sua esecuzione, dando visibilità sul traffico di rete generato e le interazioni con il sistema operativo con l’obiettivo di individuare perdite di dati, configurazioni insicure o vulnerabilità.

Per queste attività si possono usare strumenti commerciali o open source. Tra questi ultimi possiamo trovare **MobSF**[66] e, a livello nazionale, **Approver**[67].

OWASP ha pubblicato alcune guide per condurre test di sicurezza sulle applicazioni mobile[68] e le verifiche di sicurezza[69].

Si raccomanda anche la Special Publication 800-163r1[70] del NIST[71], denominata “Vetting the security of mobile apps”.

Filtro per gli app store
Per evitare l’uso di app store non ufficiali e salvaguardare la propria organizzazione, si rende necessario filtrare i contenuti accessibili via Internet.

Limitazione della firma automatica
Per contrastare gli attacchi di repacking, il modo più semplice è impedire la distribuzione dell’app senza firma, disabilitando dunque la funzione di auto-firma. Tale

66 https://github.com/MobSF/Mobile-Security-Framework-MobSF.
67 https://approver.talos-sec.com/.
68 https://github.com/OWASP/owasp-mstg.
69 https://github.com/OWASP/owasp-masvs
70 https://csrc.nist.gov/publications/detail/sp/800-163/rev-1/final.
71 https://csrc.nist.gov.

operazione, però, viola la politica di apertura di Android e il vantaggio dell'aggiornamento continuo andrebbe perso.

Questo approccio è impraticabile anche perché richiederebbe la sostituzione di tutti i software dei dispositivi con un nuovo software che non consente l'auto-firma. A causa di questa restrizione è necessario sviluppare un metodo per risolvere la vulnerabilità mantenendo la compatibilità con il sistema attuale. La strategia di firma delle app basata su più firme è uno di questi metodi, in grado di ridurre al minimo le modifiche al sistema corrente pur soddisfacendo il requisito di aggiornamento continuo.

5.4.2.4 Controlli in fase di utilizzo

Partizionamento
Per ridurre i rischi determinati dall'uso di dispositivi lavorativi a scopi personali (a cui spesso si affiancano comportamenti meno attenti) o per controllare il ricorso al BYOD, è possibile prevedere un partizionamento del dispositivo in parte personale e in parte lavorativa, in modo che errori, malfunzionamenti e attacchi a una parte non abbiano impatti sull'altra.

Malware
Per evitare infezioni da virus, per i dispositivi Android è possibile scaricare app anti-malware da sviluppatori affidabili tramite il Play Store. Per i dispositivi Apple, poiché l'App Store è utilizzato per installare tutti i programmi ed è privo di malware, si assume che il software antimalware non sia necessario per proteggere ulteriormente gli utenti.

Controllo dei dispositivi
Per il controllo dei dispositivi, molte organizzazioni si affidano a sistemi di mobile application management (MAM[72]). Tali sistemi consentono il pieno controllo (distribuzione, installazione, configurazione iniziale, aggiornamento e, alla fine, rimozione) sulle applicazioni mobili che accedono a servizi e dati dell'organizzazione. I sistemi di mobile device management (MDM[73]), che spesso includono funzionalità MAM, danno visibilità e possibilità di gestione del dispositivo.

Altri strumenti, come AWS AppConfig[74], permettono di configurare le app mobili, senza però offrire ulteriori funzionalità di MDM o MAM.
Alcune configurazioni suggerite per dispositivi e app che accedono a servizi e dati dell'organizzazione sono:

72 https://www.gartner.com/reviews/market/mobile-application-management.
73 https://www.gartner.com/en/information-technology/glossary/mobile-device-management-mdm.
74 https://aws.amazon.com/systems-manager/features/appconfig/.

- autenticazione locale (ad esempio con codice di sblocco, sensori biometrici) e remota (ad esempio tramite identity provider e accesso condizionale);
- protezione dalla compromissione del dispositivo (ad esempio rilevando jailbreak e rooting);
- blocco dell'accesso all'app in caso il dispositivo sia offline, sia collegato a reti Wi-Fi non conosciute oppure sia in roaming;
- analisi del traffico di rete generato dall'app (ad esempio per finalità di content filtering);
- protezione dalla perdita di dati sensibili con funzionalità di DLP;
- creazione di tunnel cifrati (VPN).

Gli strumenti MDM e MAM da soli non sono però sufficienti a coprire le varie casistiche di sicurezza. Essi non forniscono informazioni dettagliate sulle autorizzazioni delle app in tempo reale e sui controlli di accesso ai dati. Con i dispositivi personali non gestiti la visibilità è ancora minore.

Strumenti di mobile app reputation services (MARS) offrono una visibilità completa sui rischi posti dalle app e consentono agli amministratori di monitorare e impostare criteri di controllo.

5.5 OT e supply chain integrata

L'attenzione alla protezione dei sistemi di Operational Technology non è sicuramente materia nuova.
Lo scenario italiano è in rapida evoluzione anche sulla spinta delle agevolazioni Industria 4.0 (ora Transizione 4.0'), introdotte a partire dalla legge 232/16 dell'11 dicembre 2016.

5.5.1 Scenari di rischio

Lo scenario di rischio più comune è la **condivisione** di cartelle di rete o di tabelle di frontiera (tabelle usate per lo scambio di dati tra applicazioni) senza segmentazione o limitazione degli accessi dei vari utenti (inclusi fornitori del macchinario, fornitori di software CAD e CAM, fornitori dei sistemi gestionali e MES).

Relativamente al **controllo da remoto** lo scenario più comune è una connessione non presidiata attraverso sistemi quali Teamviewer, Anydesk, VNC. Molto frequente è anche l'utilizzo di servizi di connessione "blackbox" forniti da organizzazioni specializzate che permettono la connessione di sistemi inizialmente non predisposti con

sistemi esterni all'organizzazione.

Per quanto riguarda gli attacchi da parte di malintenzionati, i vettori di attacco principalmente sfruttati sono: i software rilasciati dalle software house ai propri clienti, i protocolli di comunicazione tra i diversi attori. I target principali cui puntano gli attaccanti sono l'integrità dei dati, l'accesso agli account chiave dell'organizzazione, l'accesso ai sistemi interni di produzione e l'ottenimento di risorse economico finanziarie.
Oltre all'utilizzo delle diverse tipologie di azioni malevole, dal ransomware, al malware, al phishing e così via, gli attaccanti, per portare a termine il proprio lavoro con successo, oggi sfruttano soprattutto il rapporto di fiducia che è alla base del buon funzionamento della supply chain.

5.5.2 Buone pratiche

Un particolare supporto lo fornisce lo standard IEC 62443. Esso permette di definire un sistema di gestione dei vari attori coinvolti nella fornitura di soluzioni OT, in particolare tra l'asset owner (che utilizza le soluzioni realizzate), il system integrator (che integra la soluzione) e il fornitore di prodotto (che sviluppa ed eventualmente certifica lo specifico componente).
Lo schema complessivo è indicato nell'immagine seguente

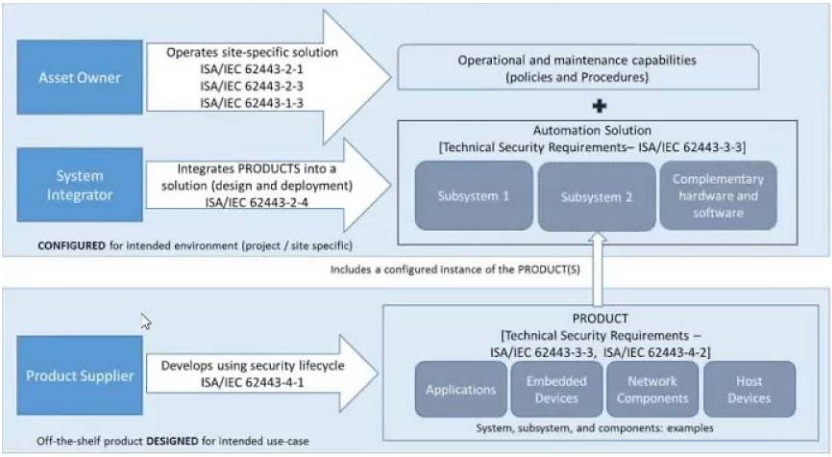


Figura 7 - Applicabilità della IEC 62443[75]

75 Fonte: rielaborazione dalla IEC 62443-2-4:2017

L'asset owner, per far fronte agli scenari di rischio, dovrebbe applicare alcuni controlli chiave:

- valutazione del livello di sicurezza informatica nei contratti con la supply chain;
- valutazione tecnica delle dipendenze del proprio processo produttivo dalla supply chain, relative misure di sicurezza ed eventuali certificazioni richieste ai fornitori;
- attuazione di processi di audit, monitoraggio, riesame periodico ed eventuale modifica dei fornitori e dei loro processi di sicurezza informatica;
- sviluppo di processi di continuità operativa in caso di blocco dell'attività di uno o più attori della supply chain;
- controllo degli accessi remoti (vedere paragrafo 5.9);
- controllo dei software acquisiti e gestiti e delle loro modalità di distribuzione (vedere paragrafo 5.2).

5.6 Hardware

L'enorme pervasività delle piattaforme e componenti hardware in tutti i campi della nostra esistenza unita alla crescente complessità delle funzioni gestite ha reso sempre più necessaria l'acquisizione di tali componenti da fornitori specializzati.

Peraltro, quando si effettuano considerazioni sulla sicurezza dei componenti che sono forniti, la distinzione fra componenti hardware e software è poco significativa perché un qualsivoglia componente hardware ha sempre una seppur minimale componente software. Nella migliore delle ipotesi si tratta di un software di basso livello (un firmware), utile a interagire con il componente e a governarlo. Sempre più di frequente, però, complice la disponibilità di potenza di calcolo a bassissimo costo e l'offerta di prodotti sempre più evoluti e ricchi di funzionalità, anche componenti o prodotti tutto sommato semplici possono essere dotati di software non di basso livello, come un sistema operativo o applicazioni web.

Basti pensare all'evoluzione che nel corso di pochi anni hanno subito i piccoli e grandi elettrodomestici e apparecchi domestici. Evidentemente, tutto questo solleva criticità sotto il profilo della sicurezza e apre scenari come quello che ha portato all'attacco contro DynDNS nell'ottobre 2016[76], un attacco DDoS che sfruttò dispositivi IoT e non computer.

76 https://mse238blog.stanford.edu/2018/07/clairemw/the-2016-dyn-attack-and-its-lessons-for-iot-security/

5.6.1 Scenari di rischio

Oltre ai rischi relativi alla sicurezza e qualità del firmware, già oggetto del paragrafo 5.2, sono da considerare le difficoltà nella fornitura di chip, necessari per la realizzazione di apparati (e da approvvigionare anche come parti di ricambio). Va tenuto in considerazione che fenomeni globali, come la pandemia o come tensioni geopolitiche tra i Paesi che estraggono e utilizzano le materie prime per la produzione di semiconduttori, hanno provocato fluttuazioni nella domanda e nell'offerta, non sempre prevedibili.

Questo rischio è tanto più significativo se si pensa che la carenza di hardware può avere impatti sui data center e sui fornitori di servizi cloud. I principali elementi di un data center da mettere in sicurezza (controllando quindi anche tutti gli aspetti della supply chain di prodotti e servizi ICT di terze parti che saranno utilizzati) sono:

- componenti core del data center: dispositivi hardware e software per ICT operation, storage di dati e di applicazioni (storage systems; servers; network infrastructure, switches routers; sistemi di sicurezza come i firewall);
- infrastrutture di supporto: generatori e sistemi di continuità (Uninterruptible Power Sources, UPS), sistema di riscaldamento, raffreddamento e ventilazione (HVAC systems), sistemi per la sicurezza fisica (biometrica, videosorveglianza).

Per ciascuna di queste componenti bisognerà considerare la specifica supply chain e i rischi che questa comporta.

Da considerare infine anche la possibilità di un fornitore di componenti hardware che cessa del tutto la propria attività (oggetto di trattazione nei paragrafi 5.6 e 5.8).

5.6.2 Buone pratiche

Tra le buone pratiche che si possono individuare in questo ambito, la via della standardizzazione del firmware è certamente quella che può portare ai migliori risultati. Essa permette di mantenere il controllo dell'elemento più critico di un hardware, anche se può limitare alcune scelte progettuali a causa dei vincoli sulle piattaforme o sui microprocessori da utilizzare. Negli ultimi anni si sono affermati alcuni esempi di standard intermedi (tra sistema operativo e firmware) come l'UEFI (Unified Extensible Firmware Interface) in ambito Intel anche se, in generale, può essere efficace semplicemente definire un insieme di regole e procedure da applicare come, ad esempio, la scelta di un limitato numero di piattaforme (microprocessore e componenti elettronici installati su una scheda elettronica con una determinata funzione), la gestione dei cambiamenti e del versionamento del firmware, la definizione di

modelli ben documentati per lo sviluppo e la manutenzione. Insomma l'acquisto a "scatola chiusa" in questo ambito è molto poco efficace.

Con riferimento alla mitigazione di rischi legati a difficoltà negli approvvigionamenti (chip e materie prime), nel periodo pandemico in molti settori si è reso necessario individuare possibili soluzioni. Il tema della carenza di risorse è diventato così grave da dar origine al concetto di una "shortage economy".
Tra le soluzioni emerse vi è quella di dotarsi di sistemi di e-procurement sempre più sofisticati, ampi, arricchiti da analisi predittive.

5.7 Lock in

5.7.1 Scenari di rischio

Il ricorso a un fornitore comporta inevitabilmente il cosiddetto rischio di lock-in, ossia quello relativo ai costi ("switching cost") da sostenere (in termini di risorse economiche, oneri amministrativi, organizzativi, formazione del personale, sicurezza delle informazioni, tempi di migrazione elevati, ecc.) in caso di una sua sostituzione o internalizzazione dei beni o servizi offerti da esso.

Il ricorso a fornitori "di fiducia" aggrava il rischio di lock-in, specie quando l'asimmetria informativa tra cliente e fornitore è molto sbilanciata in favore del secondo.

È opportuno considerare anche che il fornitore possa essere oggetto di restrizioni, ad esempio dovute a bandi internazionali di carattere geopolitico (ad esempio su fornitori cinesi o russi).

5.7.2 Buone pratiche

Il rischio di lock-in è una delle caratteristiche chiave su cui basare la scelta del fornitore e stabilire le relative clausole contrattuali o i bandi di gara. Per questo motivo è contemplato da molte norme, standard e linee guida settoriali, come, ad esempio, quelle bancarie (paragrafo 8.7 e 8.8), o quelle relative agli appalti pubblici con le linee guida della Commissione Europea[77], dell'autorità italiana anticorruzione[78] e AgID[79].

77 Commissione Europea. Contro il lock-in: costruire sistemi TIC aperti facendo un uso migliore degli standard negli appalti pubblici, Com (2013) 455 final del 25 giugno 2013. https://www.senato.it/web/docuorc2004.nsf/00672360b4d2dc27c1257690058cad9/e27b615813f0fafec1257b Commissione Europea. Contro il lock-in: costruire sistemi TIC aperti facendo un uso migliore degli standard negli appalti pubblici, Com (2013) 455 final del 25 giugno 2013. https://www.senato.it/web/docuorc2004.nsf/00672360b4d2dc27c12576900058cad9/e27b-615813f0fafec1257b

78Linee guida n. 8 <<Ricorso a procedure negoziate senza previa pubblicazione di un bando nel caso di forniture e servizi ritenuti infungibili>> approvate con Deliberazione n. 950 del 13.09.2017 dal Consiglio dell'Autorità Nazionale Anticorruzione. https://www.anticorruzione.it/-/linee-guida-n.-8

79 Linee guida AGID sull'acquisizione e riuso di software per le pubbliche amministrazioni del 9 maggio 2019, cap. 2 https://www.agid.gov.it/it/design-servizi/riuso-open-source/linee-guida-acquisizione-riuso-software-pa.

Esistono differenti pratiche per mitigare il lock-in. Queste possono essere di ambito:

- **tecnologico**; includono la verifica se il fornitore offre servizi interoperabili basati su standard e formati dati "aperti", ossia pubblici (non proprietari), documentati e universalmente disponibili;
- **contrattuale**, dove il cliente può verificare ed eventualmente richiedere al fornitore specifiche clausole relative al rischio di lock-in (p.e. uso di standard aperti, assistenza in caso di passaggio di consegne);
- **differenziazione** dei fornitori ICT, soprattutto in ambito cloud.

Per i prodotti software, AgID fa riferimento allo standard ISO/IEC 25010:2011. Esso definisce un modello di qualità del prodotto software sviluppato su diverse dimensioni, tra cui quella di portabilità. Allo stesso modo, la portabilità è prevista dal regolamento che disciplina le infrastrutture digitali e i servizi cloud della pubblica amministrazione[80].

5.8 Continuità operativa

I processi considerati critici ai fini della continuità operativa sono quelli che garantiscono il corretto funzionamento del business. Essi devono essere dotati di piani di ripristino in caso di interruzioni delle attività ordinarie.

5.8.1 Scenari di rischio

Quando i processi sono esercitati con il supporto di fornitori, diventa importante trasferire alla terza parte la stessa attenzione che si applica ai processi stessi.

Il fornitore di servizi infatti diventa parte integrante dell'operatività del cliente e problemi di continuità del servizio potrebbero mettere a rischio la continuità del business del cliente.

Il fornitore può:

- cessare le attività completamente (p.e. per fallimento) o parzialmente (p.e. dismettendo una linea di produzione o un servizio);
- sperimentare un incidente ai sistemi, al software o alle TLC;
- avere problemi di carenza di personale.

La decisione di avvalersi dei servizi di fornitura di un solo o di pochissimi fornitori

80 Regolamento AGID recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/213481843250O__ORegolamento+servizi+cloud.pdf.

può comportare una crescente dipendenza dal fornitore stesso, con impatti molto significativi.

L'analisi dovrebbe comprendere anche le dipendenze dei fornitori verso i subfornitori. Negli ultimi anni si sono evidenziati impatti generalizzati a causa, per esempio, della crisi per il rallentamento delle forniture di microchip (a seguito della pandemia e delle tensioni geopolitiche) e della crisi energetica.

5.8.2 Buone pratiche

L'organizzazione dovrebbe innanzitutto stabilire le proprie strategie:

- pianificando la continuità:
    - facendo ricorso a più fornitori contemporaneamente, in modo da ricorrere agli altri in caso di indisponibilità di uno di essi (caso tipico è l'uso di linee dati di fornitori distinti);
    - monitorando fornitori alternativi in modo da ricorrere ad essi in caso di indisponibilità del fornitore corrente (caso tipico riguarda i fornitori di hardware);
- richiedendo al fornitore selezionato di pianificare la continuità.

Nel secondo caso, in fase preliminare alla stesura del contratto è necessario verificare la capacità del fornitore in fatto di continuità operativa. Questa verifica è tipicamente svolta con il supporto di questionari da compilare in autodichiarazione, con la richiesta di certificazioni a copertura dei servizi oggetto della fornitura (p.e. ISO 22301) o con audit.

In fase di negoziazione e poi di redazione del contratto con il fornitore è decisivo esplicitare le aspettative del committente, alle quali la controparte dovrà attenersi.

In questa fase, per i servizi informatici, è fondamentale che il committente espliciti un recovery time objective (RTO) e un recovery point objective (RPO) che il fornitore dovrà garantire in caso di interruzione delle attività ordinarie. Sono necessarie anche garanzie circa le verifiche periodiche effettuate sulle soluzioni di continuità operativa e, se richiesto dal committente, sarà necessario garantire la possibilità di effettuare test congiunti, così da esercitare le capacità di ripristino del processo end-to-end.

In fase di monitoraggio periodico, è importante interagire con il fornitore per mantenere aggiornati i livelli di servizio fornito e, se necessario, procedere con un audit.

In particolare per i processi di business più critici, in cui le aspettative di ripristino si esprimono in poche ore dall'eventuale interruzione, risulta decisiva la capacità di coordinamento con il committente, avendo preventivamente definito un approccio e dei processi con l'intervento di figure precise.

5.9 Accesso remoto

Il fornitore, per accedere al perimetro ICT di un'organizzazione e poter operare, utilizza di solito l'accesso VPN.

La connessione VPN è considerata intrinsecamente sicura: si crea un tunnel tra il fornitore e l'organizzazione che, essendo cifrato, difficilmente consente l'intercettazione del traffico.

Sono invece molteplici i rischi legati all'uso di VPN da parte dei fornitori, soprattutto relativi alla gestione dell'utenza, all'autenticazione ai profili autorizzativi, al monitoraggio delle connessioni, alle attività svolte. Soprattutto nella configurazione "LAN-to-LAN", qualunque accesso indebito alle risorse del fornitore può facilmente implicare un accesso non autorizzato alle reti dei clienti.

5.9.1 Scenari di rischio

La Colonial Pipeline Company fu vittima di un attacco ransomware, che rapidamente interruppe la fornitura di carburante in un'ampia porzione del sud-est degli Stati Uniti, con una potenziale diffusione a nord, fino a New York. Gli attaccanti riuscirono a introdursi nella VPN dell'organizzazione piuttosto facilmente perché l'autenticazione a più fattori (MFA) non era attiva.

L'Azienda Socio Sanitaria Territoriale Fatebenefratelli Sacco di Milano fu colpita da attacco ransomware usando credenziali VPN in vendita sul darkweb. Altre aziende sanitarie sono state vittima di ransomware in circostanze analoghe.

Da questi casi si comprende l'importanza di considerare anche la sicurezza dei client VPN. Un client compromesso e vulnerabile potrebbe infatti rivelarsi un punto di debolezza che potrebbe aprire delle falle all'interno dell'infrastruttura. Però l'organizzazione difficilmente riesce ad avere il governo del client del fornitore e assicurare che rispetti tutti i requisiti minimi di sicurezza (patching, antivirus, utenze privilegiate, ecc.).

Di seguito riportiamo sinteticamente alcuni dei rischi relativi agli accessi remoti dei fornitori e legati al ciclo di vita delle utenze e dei profili autorizzativi:

- il fornitore può far accedere utenti differenti con le stesse credenziali o assegnare un'unica user-id e password a più persone;
- il fornitore non cambia (o non segnala a chi gestisce le autorizzazioni) le credenziali in caso di dimissioni di un AdS;
- il fornitore utilizza applicazioni non controllate o non presidiate attraverso sistemi quali Teamviewer, Anydesk, VNC e anche servizi di connessione "blackbox" come già indicato al paragrafo 5.5.1);
- il fornitore lascia attive connessioni "occulte".

5.9.2 Buone pratiche

Si forniscono nel seguito alcune indicazioni su possibili tecniche di mitigazione dei rischi sopra evidenziati.

Autenticazione a più fattori (MFA)
Richiedendo agli utenti di utilizzare due o più fattori diversi di autenticazione, prima di ottenere l'accesso a un file o sistema, l'MFA consente di innalzare significativamente il livello di sicurezza. L'uso di due o più fattori implica che, a differenza di quanto avviene con le normali password, le credenziali di accesso non possono essere facilmente condivise o utilizzate da più utenti.

Accesso alle risorse necessarie (need-to-know)
Bisogna concedere solo il giusto perimetro di azione al fornitore, dandogli accesso soltanto alle risorse e ai servizi necessari, avere un monitoraggio continuo degli accessi e richiedere l'utilizzo di VPN, impedendo collegamenti diretti. Il controllo sulle connessioni dei fornitori deve essere in ogni caso lasciato all'organizzazione. La micro-segmentazione della rete consente poi di limitare gli spostamenti "laterali" in caso di accessi indebiti.

Gestione e controllo degli accessi
Fondamentale importanza, oltre alla messa in sicurezza dell'accesso VPN, riveste la gestione degli accessi del personale dei fornitori ai sistemi dell'organizzazione sia in fase di fornitura delle utenze che di disabilitazione e controllo continuo.

L'organizzazione dovrebbe sempre fornire utenze nominative al personale del fornitore con necessità di accedere alle infrastrutture, in accordo con le politiche di sicurezza definite. Gli accessi del fornitore dovranno poter essere quindi tracciati,

verificati ed eventualmente bloccati se non previsti.
Le soluzioni di Identity and Access Management si stanno dotando di componenti sempre più sofisticati, che permettono l'accesso dinamico basato sul contesto e l'analisi del comportamento degli utenti. Tra queste vi sono:

- **Context-aware Access**: soluzioni con politiche di accesso automaticamente apprese e dinamicamente aggiornate al fine di adattarsi ai cambiamenti di contesto. Il sistema può determinare quali fattori di autenticazione applicare in una particolare situazione, considerando ad esempio i dispositivi usati, la posizione dell'utente, l'ora della connessione e il tentativo di accesso da una rete mai utilizzata in precedenza.
- **User Behavior Analytics**: Le soluzioni User and Entity Behavior Analytics (UEBA) utilizzano l'analisi dei dati e gli algoritmi di machine learning (ML) per creare un comportamento di base specifico per ciascun utente ed entità (host, indirizzi IP e applicazioni). Quando rilevano deviazioni da questa linea di base, possono applicare misure di sicurezza specifiche. Ad esempio, se è stato rilevato un numero eccessivo di accessi non riusciti entro un intervallo di tempo predefinito, possono arrestare un processo specifico, modificare le impostazioni del firewall, disabilitare l'account di un utente, chiudere l'intero server, inviare notifiche in caso di accesso a informazioni mai precedentemente richieste o comportamenti inusuali quali caricamenti o cancellazione massive di dati.

5.10 Intelligenza artificiale

5.10.1 Scenari di rischio

ENISA ha illustrato una tassonomia delle debolezze e vulnerabilità che possono affliggere sistemi di intelligenza artificiale[81], in particolar modo quelli legati all'uso di machine learning.

Come illustrato in figura, il ciclo di vita di un sistema basato su machine learning richiede diverse fasi, ognuna delle quali può essere demandata a un fornitore esterno. Si parla infatti di data collection (raccolta dati), data cleaning (pulizia dei dati), e data preprocessing (preparazione dei dati), ed è pratica comune acquistare dataset da fornitori esterni.

Per quanto riguarda il model design (progettazione del modello) e training (addestramento del modello), spesso si fa riferimento a strumenti di terze parti, ad esem-

81 Securing Machine Learning Algorithms, ENISA, 2021 https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms.

pio i framework per apprendimento di reti neurali scritti in Python.

Si deve procedere necessariamente all'addestramento, all'esecuzione di test, e all'ottimizzazione del modello, spesso utilizzando servizi di terze parti, solitamente ospitati nel cloud. La valutazione (evaluation) e il rilascio (deployment) del modello richiedono spesso integrazioni con software di terze parti, come ad esempio gli store dei vari sistemi operativi.

Infine, strumenti di terze parti potrebbero essere necessari per il monitoraggio e l'inferenza, al fine di monitorare l'uso e il valore aggiunto generato per gli utenti finali.

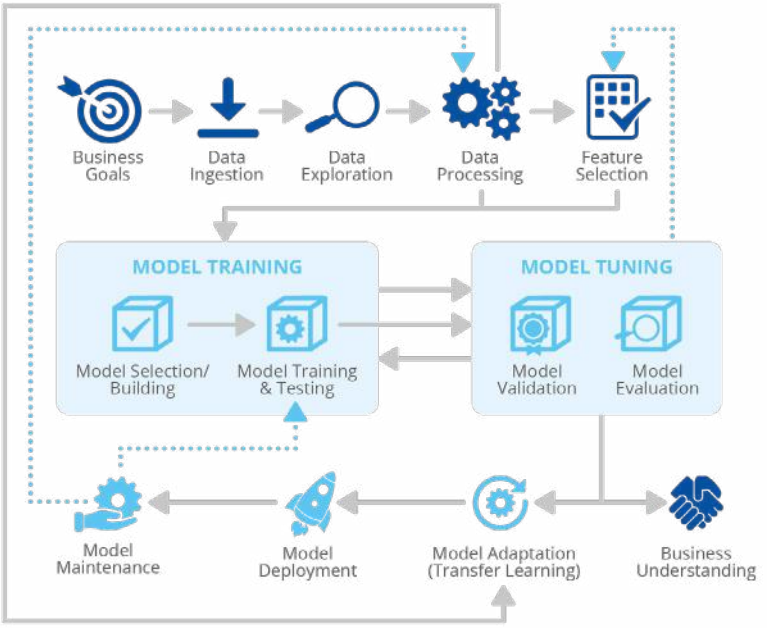


Figura 8 – Ciclo di vita di un'applicazione di machine learning[82]

Come evidenziato in altra sede[83], la principale difficoltà sta nel fatto che un attacco può essere difficile da riconoscere anche quando è in atto. Ad esempio un attacco che, manipolando il dataset utilizzato per l'addestramento del sistema, introduce

82 Fonte: European Union Agency for Cybersecurity (ENISA), 2021. Riproduzione autorizzata con riferimento alla sorgente. https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms.

83 Liberamente scaricabile all'indirizzo https://iasecurity.clusit.it/.

volontariamente un pregiudizio (bias), con lo scopo di favorire l'attaccante in qualche tipo di valutazione svolta dal sistema.
Analogamente, errori introdotti dal fornitore (ad esempio, pregiudizi introdotti involontariamente) possono essere difficili da riconoscere a posteriori.

Si presentano anche gli stessi problemi che si trovano in altre forniture in cui i requisiti di sicurezza debbano essere propagati attraverso una supply chain potenzialmente molto lunga, specialmente quando il componente di IA sia parte di un servizio più complesso offerto all'utente finale.

5.10.2 Buone pratiche

Per affrontare il rischio di pregiudizi introdotti involontariamente da un fornitore, vanno previsti requisiti di validazione sia dei dataset che del processo di apprendimento.

Si raccomanda di richiedere ai fornitori di applicare specifici controlli di sicurezza, associati alle diverse fasi del ciclo di vita degli algoritmi e alle minacce. Per questi è possibile fare riferimento, tra gli altri, al rapporto dell'ENISA "Securing Machine Learning Algorithms[84]".

Occorre inoltre prestare attenzione alle implicazioni sulla protezione dei dati personali, nelle diverse fasi dello sviluppo e manutenzione dei sistemi. I prodotti usati per l'addestramento spesso sono formati da dati personali pseudonimizzati da cui, con attacchi sofisticati, si possono ricostruire i dati personali o fare inferenze sui dati anche particolari di uno o più soggetti.

84 European Union Agency for Cybersecurity (ENISA), 2021. https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms.

6. SETTORI SPECIFICI

In questo capitolo sono affrontati aspetti relativi alla gestione della supply chain nei settori:

- Sanitario;
- Automotive;
- Auto elettriche e centraline di ricarica;
- Forniture di sicurezza informatica;
- Difesa e spazio;
- Telecomunicazioni;
- Trasporti;
- Pubblica amministrazione;
- Finanziario.

6.1 Settore sanitario

Nell'ultimo decennio il settore sanitario si è trasformato radicalmente grazie alle tecnologie digitali. La pandemia globale ha accelerato i processi e l'utilizzo dei dati, facendo emergere non banali carenze tecniche e culturali in tema di sicurezza informatica.

Eventuali carenze nella supply chain ICT per le strutture in ambito sanitario potrebbero avere ripercussioni significative sia in termini di continuità operativa che di protezione delle informazioni e dei dati.

Il danno per l'utenza potrebbe andare dal pericolo di sopravvivenza per il paziente (es. sistemi non funzionanti a seguito di un attacco ransomware), all'incapacità di effettuare diagnosi o somministrate farmaci (es. impossibilità di accedere al fascicolo del paziente), errori e/o sovrapposizioni della pianificazione operativa (es. errori di codice negli applicativi per la prenotazione dei servizi), fino all'esposizione di informazioni o dati e non conformità di norme cogenti quali il Regolamento UE 679/2016 GDPR, particolarmente significativo in ambito sanitario, vista la presenza in gran numero di dati personali particolari.

L'impatto della digitalizzazione in ambito sanitario è enorme: cliniche, ospedali, me-

dici utilizzano le cartelle cliniche elettroniche e software per il trattamento dei dati sanitari. L'enorme mole di dati generata dal comparto sanitario e la carente capacità di strutturare una cybersecurity adeguata, hanno reso questo settore uno degli obiettivi più appetibile per i criminali informatici, rendendo la sicurezza informatica nel settore sanitario una sfida importante.

Sono molte le applicazioni specifiche per gli ambiti sanitari e a titolo esemplificativo sono riportate in grafica quelle relative alla sola diagnostica.

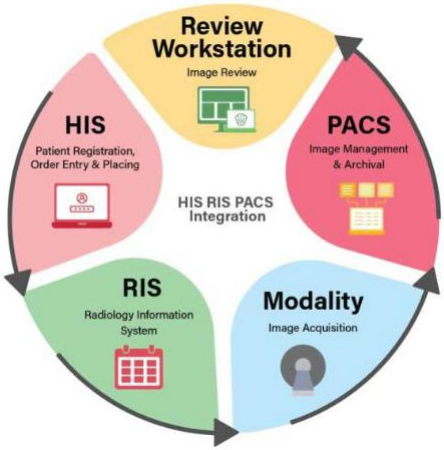


Figura 9 – Diagnostica per immagini: applicazioni e funzioni[85]

Altri elementi critici di questo settore sono i dispositivi medici, intesi come strumenti caratterizzati dalle interazioni dirette o indirette con esseri umani (pazienti ed operatori).

Anche le applicazioni client-server e le app per dispositivi mobili possono essere considerati dispositivi medici e possono sperimentare problemi di sicurezza come le altre (p.e. ransomware[86]): il criterio determinante di classificazione è il rischio di arrecare danni alla salute sia in termini di impatto che di probabilità.

In generale nel settore sanitario vi è un ricorso sempre più spinto all'esternalizzazione di servizi supportati da piattaforme ICT. Per esempio: trasporto dei pazienti presso i centri di cura con geolocalizzazione dei veicoli e previsioni sull'orario di arrivo, consegna di sussidi presso i pazienti, servizi di erogazione pasti, cure a domicilio,

85 Fonte: https://www.ramsoft.com/his-ris-pacs-integrations-workflow/.

86 https://www.cybersecurity360.it/nuove-minacce/ransomware/donna-morta-per-colpa-di-ransomware-la-sanita-non-cyber-sicura-uccide/.

prenotazione di visite specialistiche (CUP), ricerche cliniche.
Dal punto di vista normativo, viene richiesta la condivisione in rete di dati particolari su larga scala:

- tutti gli erogatori di prestazioni sanitarie, pubbliche e private, devono alimentare il Fascicolo sanitario elettronico (FSE) consentendo la consultazione dei referti prodotti da parte dei pazienti e di tutti i curanti da esso autorizzati;
- tutte le prescrizioni ed erogazioni di farmaci e prestazioni sono trasmesse in tempo reale al MEF.
- tutti gli episodi collegati alla pandemia COVID 19 (tamponi, contagio, contatti stretti, prenotazione ed effettuazione vaccinazioni, guarigioni) sono comunicati in rete tra una pluralità di soggetti (Medici di famiglia, Farmacie, ASL/ATS/ASST, Regioni, Comuni, Ministero)

6.1.1 Scenari di rischio

Le falle nei sistemi elettronici clinici mettono in pericolo la salute e potenzialmente anche la vita di un paziente.

Molte organizzazioni del settore sanitario si affidano a fornitori esterni. Se questi fornitori hanno livelli di sicurezza insufficienti, si possono avere problemi per l'organizzazione o l'ente sanitario. Ad esempio, il furto delle credenziali o la compromissione degli account di un fornitore possono portare gravi danni, soprattutto se il fornitore ha privilegi elevati nell'ambiente informatico dell'organizzazione sanitaria.

I cyber attacchi che sfruttano la supply chain costituiscono una minaccia crescente nel settore sanitario. Molto più che in altri settori, la supply chain nel mondo sanitario vede il coinvolgimento di una rete complessa di organizzazioni e fornitori interconnessi - anche tra di loro – che forniscono prodotti e servizi sanitari ai clienti-pazienti. Componenti principali di questa supply chain sono rappresentati dai produttori di farmaci o di apparecchiature mediche. Negli ultimi anni sono sempre più diffusi servizi di "Patient Engagement" e di "Digital Health" che si rivolgono direttamente al pubblico, ma si connettono ai sistemi di un'organizzazione sanitaria, ampliando così la superficie di attacco.

Un rischio comune per la sicurezza si verifica quando le organizzazioni sanitarie concedono permessi di accesso troppo generosi, che consentono a più utenti di accedere a grandi quantità di dati dei pazienti. Oltre ai difetti tecnici delle applicazioni, anche l'errore umano può essere un fattore di rischio.

Per quanto riguarda i dispositivi medici, la normativa vigente (vedere paragrafo 8.10) prevede che gli stessi siano classificati secondo classi di rischio basate sul possibile impatto nei confronti della sicurezza fisica delle persone: alcuni dispositivi, quali i sistemi di radioterapia e radiodiagnostica, possono facilmente uccidere o compromettere gravemente la salute delle persone, altri, quali sistemi di monitoraggio da remoto, possono presentare rischi fisici molto più bassi (reazioni allergiche, indurre il medico a prescrivere farmaci non adatti alla situazione reale clinica del paziente).

L'attuale sviluppo della digitalizzazione in sanità comporta poi che oggi molti dispositivi medici di natura informatica rimangono presso il fornitore o sono collegati, attraverso Internet, a servizi esterni (p.e. le app su smartphone). Potrebbero quindi essere installati in reti non dedicate o configurati con protocolli poco sicuri.

Gli impatti includono la trasmissione di dati personali e sanitari dei pazienti a persone non autorizzate e l'azionamento di macchinari da remoto da parte di malintenzionati con effetti potenzialmente anche letali.

6.1.2 Buone pratiche

In termini di migliori pratiche per la protezione delle applicazioni sanitarie rivolte ai pazienti, qui di seguito una lista delle più importanti:

- applicare sempre il principio del "least privilege": ovvero assegnare l'accesso minimo indispensabile per svolgere il proprio compito e non di più;
- adottare un approccio "zero trust": il modello di sicurezza deve verificare ogni azione per determinare se l'identità dell'accesso è autorizzata e se c'è un comportamento insolito che deve essere bloccato, quando si accede ai dati personali;
- mappare in modo puntuale l'intero sistema informatico e le relazioni con le terze parti;
- integrare l'analisi dei rischi relativi alla sicurezza delle informazioni e alla salute delle persone effettuata dai fornitori con la propria, considerando l'uso previsto del dispositivo;
- attivare l'autenticazione a più fattori (MFA);
- mantenere e verificare periodicamente il backup dei dati;
- formare il personale;
- assicurarsi che i fornitori dispongano di team esperti e competenti, che comprendano i rischi per la sicurezza e i requisiti normativi;

- assicurarsi che la normativa sia applicata.

Per quanto riguarda i dispositivi medici, l'attuale normativa (paragrafo 8.10) prevede che i software di tipo medical device siano di classe IIa, IIb o III: di conseguenza per ottenere la certificazione devono essere preventivamente sottoposti al controllo dei cosiddetti notified body, soggetti notificati dalla Commissione Europea. La normativa prescrive poi che siano messi in atto sistemi di sorveglianza dopo la messa in commercio per minimizzare i rischi derivanti dal loro utilizzo.

Sul mercato esistono strumenti che, attraverso sonde o apparecchi sviluppati ad hoc, permettono in modo passivo di monitorare, raccogliere informazioni tecniche e criticità di tutti i dispositivi medici presenti in una determinata rete senza creare disservizi. È così possibile avere una mappatura dei dispositivi clinici installati, in modo da poter effettuare analisi dei rischi con l'obiettivo di definire le migliori strategie per la gestione dei rischi, il piano di utilizzo e manutenzione degli apparati.

Si ricorda che i principali operatori sanitari sono soggetti al D.Lgs. 65/2018, recepimento della direttiva NIS, e devono quindi applicare il Cybersecurity framework nazionale.

6.2 Automotive

Ci sono molte sfide che l'industria automobilistica deve affrontare mentre cerca di essere competitiva sul mercato e produrre veicoli con un numero crescente di funzionalità.

6.2.1 Scenari di rischio

Più veicoli connessi sono prodotti, maggiori sono le possibilità per malintenzionati di sfruttare le vulnerabilità del software tramite connessioni wireless (Wi-Fi, GSM, Bluetooth...) e fisiche. L'auto di oggi può contenere fino a 150 centraline elettroniche (ECU) e oltre 100 milioni di righe di codice software. Ciò aumenta enormemente il numero di possibili difetti e di conseguenza il numero di potenziali vulnerabilità di sicurezza. Questa dipendenza da ECU e software è destinata a crescere nei prossimi anni, poiché i veicoli passeggeri e commerciali adotteranno gradualmente capacità di guida autonoma e sistemi avanzati di risparmio energetico.

L'industria automobilistica ha una supply chain estremamente complessa e articolata, composta dai produttori di veicoli (OEM) e molte terze parti che forniscono componenti hardware, software, firmware, ecc.

Gli OEM incontrano difficoltà nel controllare e garantire che l'intero processo produttivo sia regolato da adeguati requisiti di sicurezza informatica.

6.2.2 Buone pratiche

Per la corretta prevenzione e gestione dei rischi, sono state introdotte diverse normative. La più importante è la normativa UN ECE R155[87], in vigore in oltre 60 Paesi, che ha introdotto come obbligatori diversi requisiti di cybersecurity e l'implementazione di un sistema di governance dedicato (CSMS) atto a garantire una sicurezza by-design, ossia un approccio basato sul rischio che copra tutto il ciclo di vita dei veicoli a partire dalla fase di design fino alla dismissione.

Solo gli OEM dovranno ottenere una certificazione rispetto alla normativa, ma allo stesso tempo questi dovranno assicurarsi che i loro fornitori dimostrino capacità adeguate per la cybersecurity dei loro prodotti.

Di fatto sarà necessaria l'integrazione dei requisiti di cybersecurity nell'intera supply chain.

Ulteriori normative sono

- la ISO/SAE 21434, che prevede un sistema di controlli informatici;
- ISO 26262, che contempla la gestione della safety e della cybersecurity;.
- UN ECE 156 e la corrispettiva, ma immatura, ISO/DIS 24089 (in aggiornamento) in termini di aggiornamenti software;
- Tisax (Trusted Information Security Assessment eXchange) che fornisce misure di sicurezza riferite all'industria automobilistica;
- EN 50126, che si riferisce al settore ferroviario;
- CLC/TS 50701 (Railway applications – Cybersecurity), a sua volta basata sui requisiti proposti dalla IEC 62443-2-1.

6.3 Auto elettriche e centraline di ricarica

Negli ultimi dieci anni, i veicoli elettrici (EV) sono diventati una delle tecnologie primarie per aiutare la società a raggiungere ambiziosi obiettivi di energia pulita e decarbonizzazione. Il sistema che ne consegue, somma alle criticità poc'anzi viste per il comparto automotive, analogo per quello elettrico, nuove problematiche di sicurezza ICT per le stazioni di ricarica (EVCS), concepite in diverse modalità, e le reti

87 https://unece.org/sites/default/files/2021-03/R155e.pdf.

elettriche. Ne esce una complessa interdipendenza, che può essere sfruttata in modo malevolo per danneggiare ciascun elemento dell'insieme.

Mentre per i veicoli elettrici si hanno analogie con in paragrafo precedente e gli elementi minacciati a livello si sicurezza informatica possono essere sia hardware (es: batterie, adattatori, convertitori AC/DC), sia software, comprendendo le risorse di comunicazione e le interfacce del veicolo, che consentono l'interazione fra componenti interne e esterne (es: ECU, Control Gateway, Bus, FlexRay).

Le stazioni di ricarica e la rete elettrica analogamente si compongono di sistemi digitali e fisici.

6.3.1 Scenari di attacco

I **veicoli elettrici** possono essere sottoposti a minacce che emergono sfruttando vulnerabilità interne al veicolo (es. CAN BUS, TPMS) oppure esterne e di comunicazione (es. interfacce USB/Wi-Fi/Bluetooth, interfacce con EVCS, Internet Service Portal, OEM/Vendors, Roadside Infrastructure (V2I), Veicoli (V2V), Network (V2N)).

Le **stazioni di ricaric**a, come dimostrato da diverse ricerche[88], possono incorporare vulnerabilità interne sia per quanto riguarda le componenti digitali che le reti di comunicazioni (es: password e algoritmi di hashing deboli, software con flaw note, deboli sistemi di controllo di accessi, firmware non firmato) e vulnerabilità delle reti di comunicazione esterne (es: smartphone communication, OEM/Vendor Communication, Server communication).

Nel 2022, a seguito dell'invasione russa in Ucraina, le stazioni di ricarica sull'autostrada M11 che collega Mosca con San Pietroburgo sono state compromesse e disattivate da alcuni attivisti[89]. Sono state individuate nei dispositivi di ricarica diverse vulnerabilità critiche, in taluni casi dovute a una non corretta gestione della supply chain. Le vulnerabilità consentivano il controllo remoto di milioni di dispositivi, il furto di dati sensibili e l'intrusione nelle reti informatiche connesse ai caricatori.

Con riferimento alle vulnerabilità interne di seguito sono riportati alcuni scenari di attenzione: weak passwords and hashing algorithms, weak access control, unsigned firmware update process, hard-coded login credentials, remote code injections, SQL injections.

Con riferimento alle vulnerabilità esterne si possono considerare: man-in-the-

88 https://www.pentestpartners.com/security-blog/smart-car-chargers-plug-n-play-for-hackers/.

89 https://www.vice.com/en/article/akvya5/russian-electric-vehicle-chargers-hacked-tell-users-putin-is-a-dickhead.

middle cyberattacks on data privacy, message authenticity, message integrity, and non-repudiation a causa di mancanza di server/client certificates e end-to-end message encryption.

Gli impatti più significativi di un attacco alle centraline sono:

- furto di energia elettrica e frode finanziaria;
- denial of service;
- instabilità di porzioni di rete elettrica.

6.3.2 Buone pratiche

La UN ECE R155, già citata per il comparto Automotive, è applicabile ovviamente anche per i veicoli elettrici. È altresì vero che la cybersecurity dei dispositivi di ricarica e dell'infrastruttura connessa non sono oggetto del processo di omologazione relativo a tale normativa.

Bisogna quindi fare riferimento anche ad altre regolamentazioni e best practices come ad esempio:

- Cybersecurity for Electric Vehicle Charging Infrastructure[90];
- Regulations: electric vehicle smart charge points[91];
- Security requirements for procuring EV charging stations[92].

I requisiti includono l'implementazione di controlli negli ambiti della crittografia, della comunicazione di rete, del logging delle operazioni, oltre che dell' hardening dei sistemi.

Nello specifico sono elencati di seguito, suddivisi per ambito, i principali controlli da applicare per innalzare il livello di sicurezza complessivo:

- Autenticazione dell'operatore EV: adozione di meccanismi di autenticazione con OTP basati su funzioni unidirezionali, protocolli challenge-response su chiavi crittografiche o RFID basati su infrastruttura PKI e l'estensione delle capacità di audit e logging degli eventi.
- Hardening delle interfacce Internet dei server, con anche soluzioni crittografiche end-to-end basate su TLS, e, nel caso di presenza di APIs, sessioni di comunicazione sicure e autenticate tramite scambio di certificati; per contrastare attacchi di tipo Cross-Site Scripting (XSS) e Cross-Site Request Forgery (CSRF), sono necessarie la sanitizzazione dello user input e l'adozione

90 https://www.osti.gov/biblio/1877784.

91 https://www.gov.uk/guidance/regulations-electric-vehicle-smart-charge-points;

92 https://elaad.nl/wp-content/uploads/2022/05/security-requirements-for-procuring-ev-charging-stations.pdf.

di token random da utilizzare per ogni richiesta.

- Hardening delle interfacce di manutenzione, con soluzioni tamper protection e relativi allarmi per le interfacce seriali (ad esempio RS232, RS485, USB, etc...) o di rete, laddove non sia possibile la totale rimozione delle porte esterne di comunicazione, update packages firmati digitalmente e encryption del data-at-rest con cipher suites a 256 bit. Le schede all'interno dei dispositivi devono disporre di funzionalità secure boot, funzionalità non presente su schede Raspberry Pi il cui utilizzo è generalmente diffuso.

Gli sviluppatori di software per le stazioni di ricarica per veicoli elettrici potrebbero anche prendere spunto da quanto fatto dai produttori di veicoli autonomi: costruire dischi interni e software di controllo in ogni dispositivo, in modo che possano funzionare in modo indipendente anche in caso di malfunzionamenti della rete di ricarica.

6.4 Forniture di sicurezza informatica

Le forniture di sicurezza informatica includono un insieme variegato di soluzioni.

Le soluzioni di sicurezza possono essere classificate in base alla modalità di erogazione (servizi gestiti, soluzioni software installati su dispositivi gestiti dall'organizzazione, soluzioni erogate attraverso appliance fisiche o virtuali, soluzioni fornite in cloud e così via). Naturalmente non si tratta di categorie mutuamente esclusive; ad esempio, una soluzione anti-malware contiene una componente installata sui dispositivi dell'organizzazione (l'agente) e una componente centralizzata, che ne permette la gestione e il monitoraggio.

6.4.1 Scenari di rischio

A fronte degli evidenti benefici, le soluzioni di sicurezza introducono alcuni rischi derivanti principalmente dal tipo di informazioni, che tali soluzioni gestiscono, informazioni molto critiche che, se dovessero fuoriuscire, avrebbero impatti molto negativi per l'organizzazione, ad esempio esponendo il fianco ad attacchi mirati.

Un altro aspetto di rischio è rappresentato dalle posizioni cruciali in cui sono posizionate tali soluzioni e dagli ampi privilegi con cui sono eseguite.

Un fornitore con intenzioni malevole (o anche solo sospettato di averle, in base agli

scenari geopolitici del momento) o poco attento alla sicurezza (sembra paradossale trattandosi di software di sicurezza, ma capita), oppure semplicemente una vulnerabilità software critica come quelle rilevate giornalmente su tutte le tipologie di software, ma per il quale il fornitore non rilasci in tempi rapidi una patch, avrebbe un impatto molto elevato.

Ulteriori scenari di rischio sono quelli analizzati nel capitolo precedente.

6.4.2 Buone pratiche

Ognuna delle soluzioni offerte dal mercato ha pregi e difetti, per cui dovrebbe essere fatta un'attività di analisi, valutando attentamente le peculiarità delle soluzioni in relazione con le necessità dell'organizzazione. Esistono altri fattori che è bene tener presente.

Il primo punto d'attenzione è proprio nella valutazione, la quale deve portare alla scelta di un servizio che sia "completo". Un errore molto comune è quello di acquistare una soluzione molto "verticale", ossia, specifica per una determinata necessità, e ipotizzare che essa possa essere sufficiente per tutte le necessità di sicurezza. Ad esempio, l'acquisto di un firewall non ha lo scopo di individuare direttamente malware eseguiti sulle postazioni di lavoro. Come pure una soluzione anti-malware non è progettata per identificare attacchi agli applicativi web esposti su Internet. Una visione di insieme per un monitoraggio completo è più appannaggio di soluzioni MDR.

Ovviamente, una componente fondamentale delle soluzioni è la loro qualità. Tuttavia, la valutazione della qualità di tali soluzioni non è sempre facile. Nessuna organizzazione vuole arrivare a "provare con mano" la soluzione nel momento in cui sta subendo un attacco; bisognerebbe quindi organizzare, insieme al fornitore, le modalità corrette e opportune per effettuare delle verifiche che siano sia complete e coerenti con gli obiettivi che si vuole raggiungere con la soluzione. Errori comuni portano a scegliere scenari di test non adeguati; questo può portare all'acquisto di una soluzione errata o a scartare una soluzione che avrebbe risposto correttamente alle esigenze.

Oltre alle analisi tecniche occorre considerare gli aspetti di protezione dei dati personali: le soluzioni spesso prevedono che il fornitore tratti i dati personali (per esempio, le email ricevute per filtrarle con un sistema antispam) e questo potrebbe anche avvenire con servizi cloud, con potenziale accesso da parte di soggetti esterni allo spazio economico europeo. Occorre quindi predisporre tutti gli adempimenti previsti dalla normativa vigente.

Un punto fondamentale è l'osservazione di quali informazioni sono fornite alla soluzione e, quindi, al fornitore stesso.

Infine, per affrontare il rischio di lock-in, è opportuno assicurarsi che, in qualsivoglia momento, si possa sostituire la soluzione con un impatto minimo di tempo e costi.

6.5 Difesa e spazio

Gli operatori del settore difesa e spazio investono sempre più in tecnologie digitali per accelerare lo sviluppo di prodotti, ridisegnare i processi e aumentarne l'efficienza. Considerando l'avvento delle reti 5G, si avrà, anche nel settore della difesa e dello spazio, un'enorme proliferazione di dispositivi connessi e un ampliamento incontrollato della superficie d'attacco. Le società attive nei settori difesa e spazio hanno, rispetto ad altri, grandi responsabilità nella protezione di dati critici per la stessa sicurezza nazionale.

6.5.1 Scenari di rischio

Un'operazione che ha dimostrato la vulnerabilità dei sistemi spaziali è l'attacco attribuito ai russi ai sistemi di comunicazione dell'operatore satellitare Viasat (in data 24 febbraio 2022, quindi poche ore prima dell'ingresso delle truppe nei territori dell'Ucraina). Secondo fonti ufficiali americane, inglesi ed europee, sarebbero stati infatti hacker governativi russi a prendere di mira Viasat, procurando così un parziale arresto delle comunicazioni a danno dell'esercito ucraino, che utilizzava la rete satellitare per le proprie truppe. L'operazione, volta ad ottenere un'interruzione dei servizi di comunicazione Viasat, ha di fatto procurato la disconnessione di migliaia di utenti in Ucraina oltre che in altre aree d'Europa.

La supply chain dei settori difesa e spazio, con la globalizzazione e la virtualizzazione di molteplici processi, conta oggi molti attori che possono avere accesso alle reti, scambiare dati, condividere tecnologie, know how e proprietà intellettuale, anche relativa a sistemi di difesa e alla sicurezza nazionale[93].

In settori tecnologicamente avanzati come quelli della difesa e dello spazio, le terze parti acquistano un ruolo critico in attività come ricerca e sviluppo, produzione, ingegneria, logistica, testing e integrazione, oltre che nei servizi ICT associati all'operatività dei sistemi, all'archiviazione e alla condivisione di informazioni, alla collaborazione.

93 Third-party risk management. Cybersecurity in the Defense Industrial Base (DIB), Deloitte, 2019.

Gli impatti di un incidente alla supply chain possono essere molteplici. Tra questi:

- nazioni ostili o gruppi terroristici potrebbero entrare in possesso di capacità avanzate in campo militare o spaziale e possano produrre tecnologie e armi da rivendere sui mercati internazionali;
- Paesi nemici potrebbero essere in grado di infiltrare reti e sistemi della difesa o delle comunicazioni spaziali per svolgere azioni offensive in tempi di ostilità.

6.5.2 Buone pratiche

Recentemente, il Dipartimento della Difesa Americano (DoD) ha pubblicato[94] un rapporto in merito alle supply chains DIB (defense industrial base). Da questo documento emergono diverse raccomandazioni specifiche agli aspetti di sicurezza informatica:

1. incrementare le risorse per la sicurezza informatica;
2. sviluppare pratiche efficaci ed efficienti di C-SCRM (Cybersecurity-Supply Chain Risk Management);
3. migliorare lo svolgimento di attività di C-SCRM, in particolare per identificare i fornitori a maggiore priorità;
4. migliorare la qualità della Cyber Threat Intelligence (CTI) fornita ai vari decisori nei processi di supply chain;
5. espandere la condivisione di informazioni — classificate o meno — relative a problemi di sicurezza informatica;
6. assicurare l'uso di pratiche di sicurezza informatica mature e assodate;
7. migliorare l'approccio alla sicurezza informatica delle compagnie fornitrici critiche, richiedendo incident reporting tempestivi, condivisione di CTI, ecc...

Nel rapporto sulla sicurezza delle reti 5G militari e della loro supply chain, presentato dal NATO CCDCOE[95], si discute ampiamente della necessità di un C-SCRM, notando come la maggior parte dei Paesi che aderiscono alla NATO stiano sviluppando leggi, linee guida, e sistemi in tale direzione. Ciò dovrebbe mitigare i rischi legati a fornitori non fidati, manipolazione del codice software, furto e scarsa qualità nella produzione degli artefatti, principalmente tramite la raccolta di CTI, l'implementazione di mitigazioni basate sull'analisi del rischio e il continuo monitoraggio. Il NIST 800-161 è citato come documento di riferimento.

94 DoD, Securiing Denese-Critical Supply Chains, Febbraio 2022, https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY CHAINS.PDF.

95 P. Pernik, et al. Research Report Supply Chain and Network Security for Military 5G Networks, NATO CCDCOE, 2021, https://ccdcoe.org/uploads/2021/10/Report_Supply_Chain_and_Network_Security_for_Military_5G_Networks.pdf.

È raccomandato di avere la supply chain il più possibile integrata e verticale, con una relazione win-win tra committente e fornitore, cioè creare un network collaborativo. Se la supply chain non è integrata e non si ha uno scambio fedele di informazioni tra i vari attori, si corre il rischio di subire l'effetto Forrester (ossia l'effetto frusta, ossia un'incertezza previsionale proporzionale all'aumento della lunghezza della supply chain).

6.6 Settore delle telecomunicazioni

La sicurezza delle reti di telecomunicazione è un tema divenuto progressivamente sempre più rilevante non solo per gli impatti economici e sociali, ma anche per le implicazioni di carattere strategico e di sicurezza nazionale: le reti di telecomunicazione sono infatti considerate, a buon titolo, parte delle infrastrutture critiche.

La supply chain costituisce un tassello critico dei servizi di telecomunicazione (di rete fissa o mobile). Essa è composta da fornitori di apparati tecnologici, infrastrutture, servizi di manutenzione e supporto.

6.6.1 Scenari di rischio

Rischi relativi al settore delle TLC sono:

1. standard e prassi obsoleti, con scarsa attenzione alla sicurezza;
2. scarsa protezione di apparati e software da cyberattacchi;
3. dipendenza da uno o da un numero molto limitato di fornitori (vedere paragrafi 5.7 e 5.8);
4. volatilità delle forniture di chipset (vedere paragrafo 5.6);
5. compromissione degli accessi amministrativi remoti (vedere paragrafo 5.9).

Il 5G è importantissimo nella gestione della logistica e della supply chain. Infatti, la centralità del consumatore e delle sue preferenze sta comportando un ripensamento delle catene di logistica tradizionali, come evidenziato nella figura sottostante: la logistica sta evolvendo, infatti, da un modello di retail logistics a una smart logistics: cioè da uno schema "lineare" a uno schema "circolare".

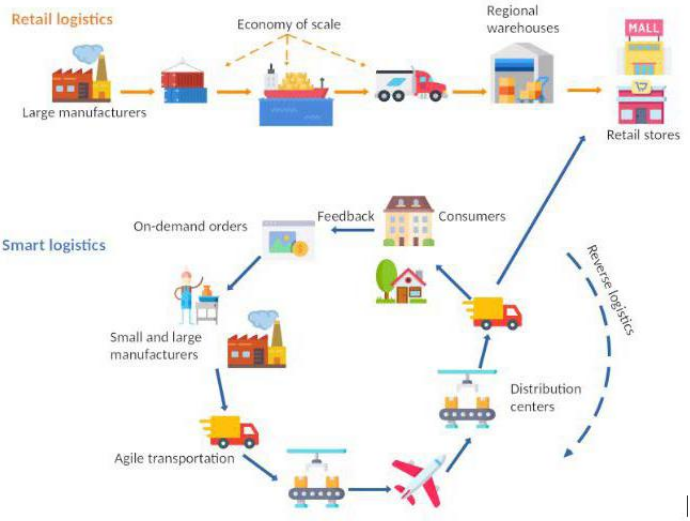


Figura 10 – Evoluzione della logistica da "lineare" a "circolare"[96]

Quindi la supply chain sarà resa più veloce e più orientata verso il consumatore finale: i passaggi di merci lungo la supply chain diverranno interamente tracciabili, grazie all'utilizzo di sensori e di tecnologie RFID e NFC; sia i siti produttivi che i centri di distribuzione opereranno in ambienti fortemente automatizzati e dotati di sistemi di videosorveglianza.

Questa progressiva ed accellerata trasformazione è possibile grazie al 5G, che insieme a nuove e significative opportunità introdurrà nuovi scenari di rischio per i cyber attacchi e e conseguentemente allo sviluppo di nuove misure per la mitigazione dei rischi, innescando quella che potrebbe divenire una nuova battaglia globale strategica ed economica per la supremazia del 5G e alla conseguente corsa a realizzare le nuove infrastrutture necessarie.

Questo ha offerto agli attaccanti l'opportunità per condurre campagne di spionaggio informatico, interferenze esterne e altre attività pericolose. I ricercatori hanno evidenziato che la supply chain è esposta a rischi come "software e hardware dannosi, componenti contraffatti, e progetti, processi di produzione e procedure di manutenzione inadeguati". In aggiunta, i miliardi di dispositivi 5G connessi (IoT e IIoT)

96 Fonte: Khatib, Barco, Optimization of 5G Networks for Smart Logistics, "Energies", 2021.

aggravano ulteriormente il problema. Un singolo atto di manomissione in qualsiasi punto della supply chain 5G potrebbe avere un enorme effetto a cascata. A solo titolo di esempio, strumenti come router, smartphone e dispositivi IoT potrebbero essere compromessi in massa, mentre i Paesi che acquistano attrezzature 5G da aziende con supply chain compromesse potrebbero essere vulnerabili all'intercettazione, manipolazione, interruzione o distruzione dei dati[97].

6.6.2 Buone pratiche

Pratiche specifiche per il settore delle telecomunicazioni sono riportate dal "UK Telecoms Supply Chain Review Report" del 2019, in cui si dà ampio spazio ad aspetti come l'aderenza a framework regolamentari per la riduzione del rischio (sono indicate pratiche di sicurezza che gli operatori devono, a livello contrattuale, estendere ai propri fornitori critici); i test di sicurezza dei prodotti adottati seguendo metodi comuni codificati; la collaborazione con l'agenzia centrale di cybersecurity per una continua valutazione dei rischi posti dai diversi fornitori.

In particolare, il Regno Unito è stato uno dei primi Paesi europei a valutare la possibilità che il fornitore cinese Huawei potesse rappresentare un rischio per la sicurezza delle reti nazionali. Un tema entrato nell'agenda politica italiana per la sovranità tecnologica e il golden power sul 5G.

Altre raccomandazioni specifiche per la sicurezza delle supply chain nel settore delle telecomunicazioni sono contenute nel white paper "Supply Chain Security for Telecom Operators[98]". In esso si sottolinea l'importanza, sia per gli operatori di telecomunicazioni sia per i loro fornitori, di investimenti specifici per aumentare la trasparenza e la condivisione di informazioni sui rischi lungo l'intera supply chain di sviluppo e fornitura di software.

È raccomandato un approccio multilivello ai test di sicurezza attraverso la supply chain, utilizzando ove possibile l'automazione per rendere il tutto più efficace.

Come riporta la figura successiva, sono molti gli aspetti critici da considerare nell'ambito di forniture complesse di software (si pensi ad esempio al ruolo del software open source), se si vuole ridurne vulnerabilità e rischi.

97 https://www.mdpi.com/2079-9292/9/11/1864.

98 https://www.hardenstance.com/white-paper-supply chain-security-for-telecom-operators/.

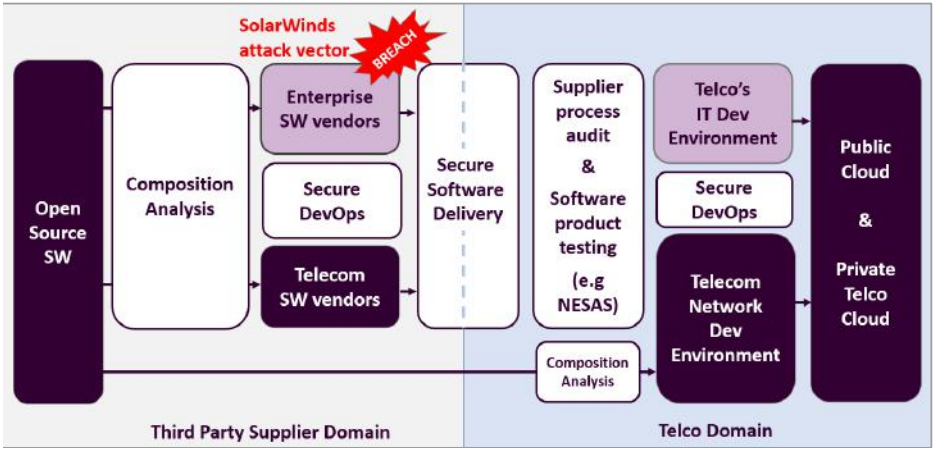


Figura 11 – Gestire le vulnerabilità software nella supply chain[99]

6.7 Trasporti

Da molto tempo i trasporti (aerei, navi, treni e camion) stanno effettuando un percorso di forte integrazione digitale delle flotte con l'obiettivo di ridurre i costi e aumentare l'efficienza. Inoltre, la stessa pandemia ha imposto nuove sfide tecnologiche per gestire problematiche impensabili sino a qualche anno fa, quali ad esempio la catena del freddo necessaria per distribuire capillarmente un'enorme quantità di vaccini.

6.7.1 Scenari di rischio

È doveroso sottolineare che la crescente integrazione e la digitalizzazione del settore ha, come contropartita, un aumento esponenziale del rischio di sicurezza informatica. Il trasporto aereo e marittimo di merci, ad esempio, è stato vittima di un numero sempre maggiore di attacchi, basti pensare a quelli perpetrati ai danni di principali vettori marittimi o aerei (ad esempio Maersk, MSC, COSCO, Swissport). Questi attacchi hanno reso inutilizzabili i sistemi e un impatto negativo sui clienti, sulle entrate e sulla reputazione del marchio. Il software di gestione della flotta ShipManager di DNV, che serve 13.175 navi e unità mobili offshore (MOU) con un volume totale di trasporto merci fino a 265,4 milioni di tonnellate, ovvero il 21% dell'intero

99 Patrick Donegan. "Supply Chain Security for Telecom Operators". Luglio 2021. https://www.hardenstance.com/white-paper-supply chain-security-for-telecom-operators/.

mercato mondiale. Più di 300 clienti utilizzano le soluzioni software ShipManager e Navigator per la gestione dei porti e dell'equipaggio[100].

Secondo il Supply Chain Resilience Report 2021 di BCI, quasi il 30% delle organizzazioni di trasporto e logistica ha segnalato più di 20 interruzioni della supply chain tramite attacchi informatici, rispetto al solo 4,8% che ha riportato lo stesso numero nel 2019.

Inoltre, secondo altre fonti, il settore dei trasporti si distingue per essere uno dei settori in più rapida crescita con attacchi che sono già aumentati di quasi il 150% tra gennaio 2020 e oggi.

Di seguito sono riportati alcuni degli impatti degli attacchi informatici nel settore dei trasporti:

- Il trasporto su binari, ferrovie e metropolitane, è estremamente fragile ad attacchi di qualsiasi tipo compresi quelli cyber. La cronaca offre spesso prova di come sia facile interrompere il servizio con manomissioni fisiche di apparati dislocati lungo l'estesa rete ferroviaria. L'interruzione operativa del servizio con migliaia o milioni di passeggeri impossibilitati a utilizzare il servizio può divenire più frequente e massiva, violando i sistemi ITC di operatori di gestione delle rete e/o del materiale circolante. La Metropolitan Trasportation Authority di New York nel giugno 2021 ha subito un attacco cyber che, sfruttando uno zeroday, ha violato 18 sistemi per diversi giorni[101].
- Il trasporto su strada, oltre ad incamerare un rischio cyber sui mezzi, già descritto nella sezione dedicata all'automotive, potrebbe essere compromesso nei suoi innumerevoli impianti di gestione dei flussi: interruzione nei servizi semaforici, dei caselli autostradali e di segnalazione elettronica stradale.
- Biglietterie: l'interruzione nel servizio delle biglietterie automatiche, potrebbe essere di pregiudizio per ogni tipo di trasporto, sia esso aereo, marittimo, su strada o ferro. La violazione dei sistemi potrebbe andare dall'esfiltrazione di informazioni relative la compagnia o i passeggeri, sino al blocco operativo dei sistemi e all'impossibilità di "staccare i tagliandi di viaggio" sia in loco che da remoto, con siti ed app che diverrebbero inutilizzabili, e enormi disservizi per l'utenza.
- Furto e/o impossibilità di accesso ad informazioni critiche, con potenziali ricadute sulla continuità del servizio. Matson compagnia di trasporto marittimo è stata colpita da un attacco con Windows REvil che ha esfiltrto e criptato

100 https://www.insicurezzadigitale.com/guerra-al-settore-marittimo-circa-mille-navi-dnv-colpite-da-attacco-ransomware/
101 https://cybersecurityguide.org/industries/transportation/

un terabyte di dati. Il riscatto è stato fissato alla considerevole somma di 2 migliardi di dollari.

6.7.2 Buone pratiche

Sono state pubblicate diverse regolamentazioni atte a garantire la resilienza del settore dei trasporti e della logistica.

Al fine di rispondere alle problematiche evidenziate, si suggerisce l'adozione e la predisposizione di politiche, standard e procedure che riguardino i seguenti ambiti: attivazione di SOC dedicati agli incidenti con impatto sui veicoli (da affiancare o integrare con SOC ICT e SOC OT), valutazione del rischio dedicata ai veicoli e infine conformità con le normative relative all'automotive.

Per il settore ferroviario, ENISA ha pubblicato alcuni documenti che fanno riferimento alla CLC/TS 50701:

- Building cyber secure Railway Infrastructure[102];
- Railway Cybersecurity - Good Practices in Cyber Risk Management[103];
- Railway Cybersecurity[104].

6.8 Pubblica amministrazione

Nella Pubblica amministrazione, l'acquisizione di beni e servizi, tra cui rientrano, ovviamente, anche i servizi ICT e il software, è regolata in maniera molto dettagliata da una serie di fonti normative, la principale delle quali è il Codice dei contratti pubblici (D.lgs 18 aprile 2016, n. 50). Per quanto riguarda l'acquisizione di programmi informatici e servizi di telecomunicazione, è fondamentale il Codice dell'amministrazione digitale (D.lgs 7 marzo 2005, n. 82, noto anche come CAD), il quale, agli artt. 68 e 69, disciplina la materia.

Alle norme generali si aggiunge la disciplina in tema di obblighi di utilizzo di strumenti di acquisto e di negoziazione previsti dalle disposizioni in materia di contenimento della spesa e le norme in tema di acquisti ICT introdotte dalla decretazione d'urgenza durante la pandemia, in attuazione dei contratti PNRR. In estrema sintesi, ogni acquisizione per la PA di beni e servizi deve, in generale, essere effettuata rispetto dei principi di economicità, efficacia, imparzialità, parità di trattamento, trasparenza, proporzionalità, pubblicità, tutela dell'ambiente ed efficienza energetica.

102 https://www.enisa.europa.eu/news/building-cyber-secure-railway-infrastructure.

103 https://www.enisa.europa.eu/publications/railway-cybersecurity-good-practices-in-cyber-risk-management/.

104 https://www.enisa.europa.eu/publications/railway-cybersecurity.

6.8.1 Scenari di rischio

La cronaca riporta diversi episodi di incidenti di sicurezza collegati alla supply chain.

Tra i casi più significativi:

- Regione Lazio: è da notare che la Regione fu danneggiata da un fornitore (LazioCrea) ma causò interruzioni di servizio alle sue aziende sanitarie in quanto in sussidiarietà amministrativa ospita alcune applicazioni sanitarie quali il CUP;
- Maggioli, fornitori di servizi prevalentemente software e gestionali per la P.A., la cui infrastruttura cloud fu oggetto di un attacco ransomware (5 diverse serverfarm) che causò disservizi a molti Comuni clienti, per diverse applicazioni che risultarono indisponibili per alcuni giorni. Fortunatamente i backup furono gestiti correttamente e non vi fu perdita di dati.

6.8.2 Buone pratiche

Le "Linee guida sicurezza nel procurement ICT" di AgID[105] propongono uno schema che esemplifica il procurement ICT (AP1 nella figura), suddivisi sulla base del livello di criticità complessiva (LCC).

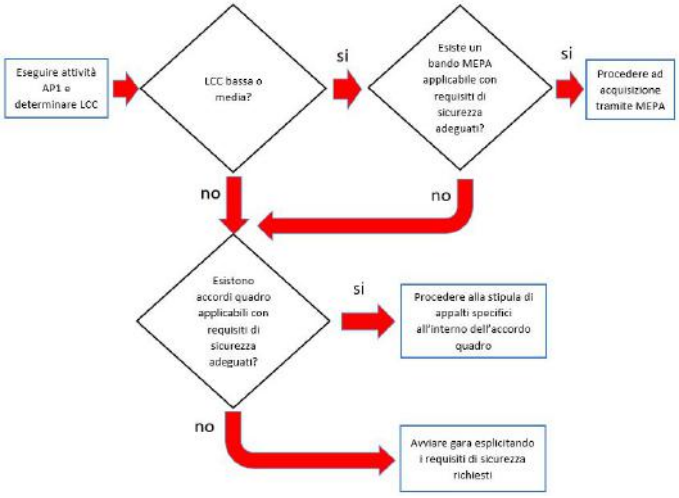


Figura 12 – Procurement ICT[106]

105 https://docs.italia.it/AgID/documenti-in-consultazione/lg-procurement-ict/it/bozza/indicazioni-per-le-amministrazioni.html.

106 Fonte: AgID.

Il documento fornisce una utilissima guida su tutte le fasi della supply chain nella PA, individuando le attività da svolgere prima dell'acquisizione, nel corso del procedimento di acquisizione, e dopo la stipula del contratto.

Il Piano Triennale per l'informatica nella Pubblica Amministrazione, aggiornamento 2021-2023[107], dedica un intero capitolo alla sicurezza informatica, e sottolinea che "sono necessarie infrastrutture tecnologiche e piattaforme in grado di offrire ai cittadini e alle imprese servizi digitali efficaci, sicuri e resilienti."

L'efficacia, sicurezza e resilienza dei servizi digitali passa, imprescindibilmente, attraverso:

- l'organizzazione di strumenti, metodologie, competenze e politiche di sicurezza;
- l'inserimento, nei bandi, nei capitolati, nei disciplinari e nei contratti, dei requisiti di sicurezza adeguati al rischio;
- l'implementazione dei necessari controlli volti a verificare che i requisiti siano adottati e rispettati per tutta la durata dell'erogazione dei servizi stessi.

Le "Linee guida sicurezza nel procurement ICT", peraltro, sono rivolte non soltanto alla PA, ma anche agli operatori di mercato e ai fornitori, per i quali è assai opportuno "essere a conoscenza delle problematiche legate alla sicurezza nel procurement ICT delle pubbliche amministrazioni, in modo che siano pronti a recepire le richieste dei committenti senza impatti rilevanti sulle negoziazioni, e anzi con spirito di collaborazione".

Le azioni da svolgere prima dell'acquisizione, indicate come azioni di carattere generale e strategico, che regolamentano tutti i futuri procedimenti di acquisizione, possono essere sintetizzate facendo riferimento a checklist suggerite dalle Linee guida.

Le Linee guida descrivono poi in dettaglio le azioni da svolgere nel corso del procedimento di acquisizione dei servizi ICT, che, sinteticamente, consistono in:

- analisi della fornitura e classificazione in base ai criteri di sicurezza;
- scelta dello strumento di acquisizione più adeguato, tenendo appunto conto della sicurezza;
- scelta dei requisiti di sicurezza da inserire nel capitolato, distinguendo i requisiti obbligatori (a pena di esclusione), da quelli opzionali, che invece possono rilevare ai fini del punteggio tecnico - l'appendice A contiene un elenco

107 https://www.agid.gov.it/sites/default/files/repository_files/pianotriennaleinformaticapa2021-2023.pdf.

dei requisiti di sicurezza che possono essere inseriti nei capitolati stessi;
- individuazione, all'interno della commissione di valutazione, di almeno un soggetto che abbia specifiche competenze in materia di sicurezza

Non bisogna poi dimenticare che, qualora si svolgano attività che importino il trattamento di dati personali, occorrerà rispettare il dettato dell'art. 28 GDPR, con conseguente necessità di individuazione di un fornitore che presenti garanzie sufficienti, e stipula di un apposito accordo sulla protezione dei dati personali.

Le linee guida, molto opportunamente, contengono anche l'elencazione delle azioni da svolgere dopo la stipula del contratto, che possono essere riassunte nei seguenti punti:

- gestione delle utenze, dei dispositivi, dell'accesso alla rete e degli accessi ai server e database, e loro monitoraggio; si tratta, in considerazione del moltiplicarsi degli attacchi supply chain, di raccomandazioni assai importanti;
- stipula di accordi di autorizzazione e riservatezza;
- verifica del rispetto delle prescrizioni di sicurezza nello sviluppo applicativo;
- verifica della documentazione finale di progetto;
- rimozione dei permessi al termine di ogni progetto e distruzione del contenuto logico dei dispositivi che dovessero venire sostituiti;
- manutenzione e aggiornamento dei prodotti;
- vulnerability assessment (sui beni e servizi critici ed esposti sul web).

Tali linee guida vanno poi affiancate dalle Misure minime ICT per le PA di AgID.

6.9 Settore finanziario

Nel settore finanziario il problema della gestione della sicurezza delle terze parti è affrontato sia per gli aspetti di rischio operativo che di compliance alle regole.

Il settore finanziario è caratterizzato dalla presenza di organizzazioni di differente dimensione economica e strutturale. Convivono istituzioni finanziarie ed assicurative molto grandi, vigilate a livello europeo, con organizzazioni locali o neonate, assimilabili alle PMI.

Di conseguenza sono diverse le capacità e le risorse disponibili per un corretto governo dell'operatività e dei rischi associati alle terze parti.

6.9.1 Scenari di rischio

Il sistema di regole imposto dalla BCE richiede che siano svolti degli assessment tecnologici su tutti i fornitori, che possano avere un qualsiasi impatto sulle infrastrutture tecnologiche dell'istituto committente.

Lo scenario cambia per i cosiddetti "small ticket", o progetti o servizi dell'ordine di qualche decina di migliaia di euro, ma a potenziale rischio in quanto comunque integrati nella filiera tecnologica; il costo di un assessment può superare il valore dell'intera fornitura! Ciò rende le istituzioni finanziarie essenzialmente "non compliant" rispetto alle regole BCE.

A rincarare la dose, il regolamento europeo DORA obbligherà, da fine 2024, tutti gli operatori del settore finanziario (non solo banche ed assicurazioni, ma qualunque soggetto gestisca in qualsivoglia maniera del denaro), a svolgere periodicamente assessment tecnologici finanche al terzo livello di sub fornitura.

Per questi segmenti di attività integrata della supply chain, gli assessment tradizionali, oltre a essere insufficienti e difficilmente praticabili, non saranno nemmeno possibili, considerata la quantità di soggetti da verificare continuamente.

6.9.2 Buone pratiche

L'introduzione di piattaforme e strumenti software, basati su questionari organizzativi e tecnologici semplici, comprensibili anche dai responsabili delle PMI, correlati con altri strumenti di investigazione tecnologica, inizialmente outside-in, successivamente anche inside-outside, potrà contribuire colmare il gap esistente tra la norma e la sua applicazione.

Per migliorare la sicurezza, una rete coordinata di solution provider territoriali potrà contribuire ad aumentare la resilienza delle PMI europee e consentire di creare filiere di servizi adeguate alla trasformazione digitale in atto.

7. RISCHI: RICERCHE ED ESEMPI

7.1 Ricerche sugli incidenti

Gli attacchi alla supply chain sono in continua evoluzione e in costante crescita. Nel seguito sono descritti i dati raccolti da alcune ricerche.

7.1.1 Ricerca dell'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano

Nel 2020 la ricerca dell'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano ha coinvolto 651 CISO, CSO, CIO, Compliance Manager, Risk Manager, Chief Risk Officer e DPO di imprese italiane. In particolare, sono state coinvolte 151 grandi organizzazioni (con più di 249 addetti) e 500 PMI (tra 10 e 249 addetti).

7.1.1.1 Le sfide per la sicurezza della supply chain

Tra le sfide che le organizzazioni si trovano ad affrontare nell'ambito della gestione della sicurezza lungo la supply chain, la principale (indicata dall'86% delle organizzazioni coinvolte nella ricerca) è rappresentata dai tradizionali rischi informatici, che sfruttano l'anello più debole della catena, con l'obiettivo di provocare ripercussioni a cascata anche sugli altri attori che costituiscono la filiera.

La seconda sfida riguarda gli accessi da remoto, concessi a terze parti per svolgere attività di gestione, manutenzione o supporto: oltre un'organizzazione su due (53%) testimonia difficoltà nel gestire tali politiche in maniera efficace.

La terza sfida (per il 45% delle organizzazioni) riguarda il nuovo contesto di trasformazione digitale, con il ricorso massivo ad ambienti cloud, la crescente automazione e il cambiamento delle modalità di lavoro, che impongono alle organizzazioni di superare il concetto tradizionale di difesa del perimetro.

Un punto di attenzione significativo, segnalato dal 37% delle organizzazioni, riguarda il ricorso a filiere sempre più estese a livello globale, che possono generare ripercussioni legate a turbolenze del contesto geo-politico.

7.1.1.2 Le tecnologie introdotte e il presidio organizzativo

Le sfide individuate si traducono sempre più spesso in un pericolo concreto per le

organizzazioni: quasi un'organizzazione su quattro (24%) ha dichiarato di aver subito negli ultimi 12 mesi un incidente di sicurezza legato a una violazione delle proprie terze parti.

Soluzioni di sicurezza per la supply chain includono il monitoraggio delle terze parti attraverso uno scoring basato su dati di cyber threat intelligence, la mappatura delle relazioni con i fornitori lungo tutta la supply chain e la virtualizzazione di rete e desktop per permettere l'assistenza remota, oltre a soluzioni di autenticazione multi-fattore e connessioni sicure.

Figura 13 – Le soluzioni tecnologiche adottate per la sicurezza della supply chain[108]

Secondo quanto emerge dalla ricerca, solo nel 33% delle organizzazioni esiste un presidio formale della supply chain, che non implica necessariamente la presenza di una figura dedicata.

La responsabilità in materia di sicurezza della supply chain è gestita in maniera piuttosto eterogenea: nella maggior parte dei casi è demandata alla funzione IT (54%) o, se presente, a una specifica funzione Security (31%); in altre la responsabilità è affidata a operations, procurement, risk management, legal e compliance o altre.

108 Fonte: Report "Supply Chain Security: la gestione della sicurezza nell'ambito del rapporto con le terze parti", Osservatorio Cybersecurity & Data Protection, School of Management Politecnico di Milano.

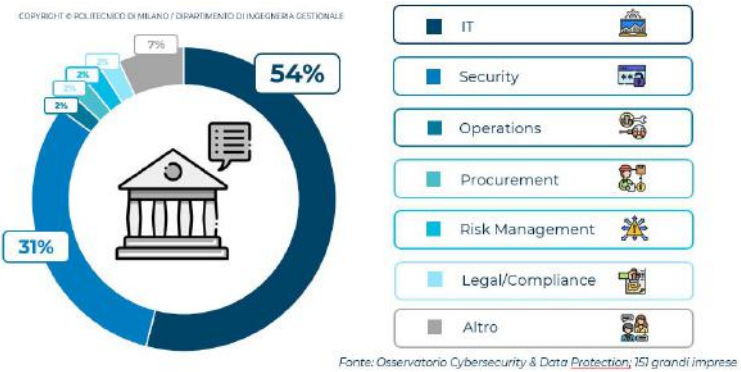


Figura 14 – La responsabilità di gestione della sicurezza della supply chain[109]

Il quadro complessivo che emerge dalla ricerca denota un livello di maturità e consapevolezza dei rischi in materia di sicurezza della supply chain ancora molto scarso: solo il 13% delle imprese del campione analizzato ha previsto l'utilizzo di strumenti tecnici specifici e un presidio organizzativo formale in materia.

7.1.2 Ricerca di ISACA

Per comprendere meglio quanto le organizzazioni siano sensibili riguardo alla sicurezza della propria supply chain, ISACA ha intervistato più di 1.300 professionisti ICT in tutto il mondo con esperienza nella supply chain[110]. Nel seguito se ne riportano i risultati principali.
La ricerca evidenzia i rischi percepiti come più importanti da parte degli intervistati.

Figura 15 – I rischi principali di supply chain[111]

109 Fonte: Report "Supply Chain Security: la gestione della sicurezza nell'ambito del rapporto con le terze parti", Osservatorio Cybersecurity & Data Protection, School of Management Politecnico di Milano.

110 "ISACA – Supply Chain Security Gaps: A 2022 Global Research Report".

111 Report "ISACA – Supply Chain Security Gaps: A 2022 Global Research Report".

Meno della metà degli intervistati ha fiducia nella sicurezza della supply chain, come indicato nella figura di seguito.

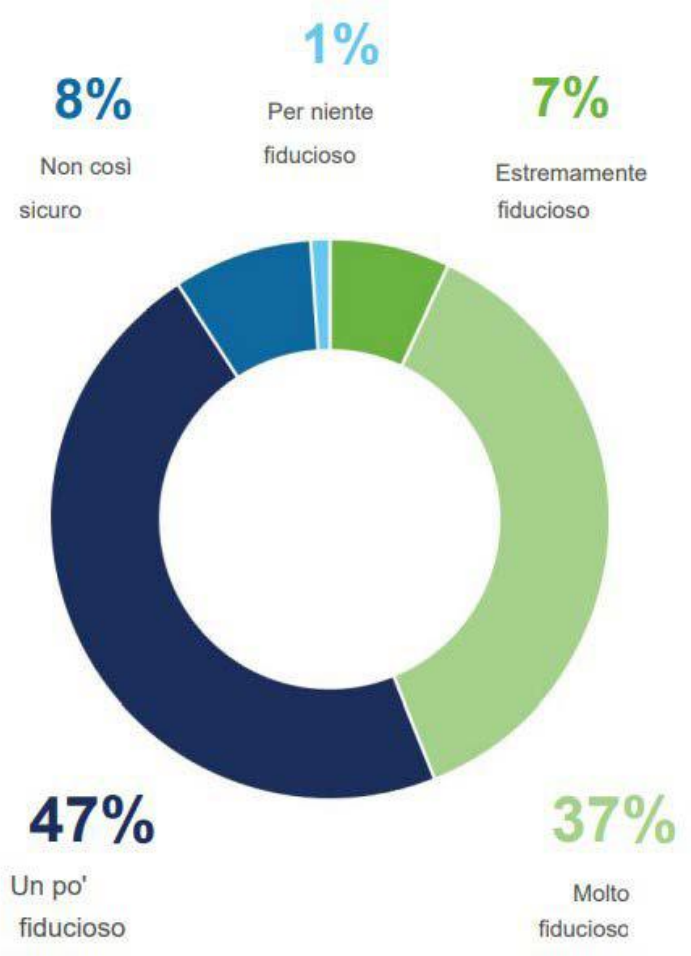


Figura 16 – Fiducia nella sicurezza della supply chain[112]

Il 25% delle organizzazioni riferisce di aver subito un attacco alla supply chain nei 12 mesi precedenti e il 53% pensa che nei successivi 6 mesi i problemi alla supply chain

112 Report "ISACA – Supply Chain Security Gaps: A 2022 Global Research Report".

peggioreranno.
Le vulnerabilità all'interno della supply chain possono manifestarsi in modi diversi, da quelli economici a quelli ambientali, il che rende la gestione di tutti i rischi, o anche il solo esserne consapevoli, molto impegnativa. La ricerca di ISACA mostra che sono necessari miglioramenti significativi quando si tratta di eseguire i test e gli audit necessari in modo da identificare e risolvere gli attacchi prima che inizino, come riepilogato nelle figure seguenti.

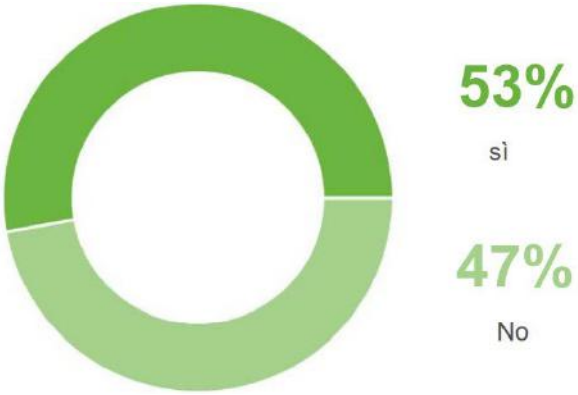


Figura 17 – L'organizzazione esegue VA e PT sulla sua supply chain? [113]

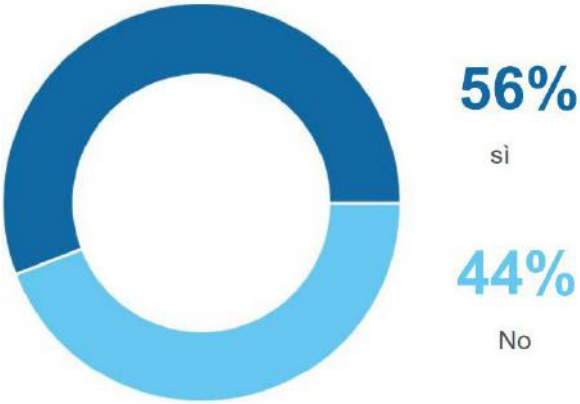


Figura 18 – Sono effettuate attività di audit? [114]

113 Report "ISACA – Supply Chain Security Gaps: A 2022 Global Research Report".
114 Report "ISACA – Supply Chain Security Gaps: A 2022 Global Research Report".

La ricerca evidenzia 5 rischi principali, elencati in ordine di rischio percepito:

- compromissione da ransomware;
- poche informazioni sulle pratiche di sicurezza utilizzate dai propri fornitori;
- vulnerabilità di sicurezza presenti nei software acquistati o sviluppati;
- archiviazione dei dati di terze parti;
- fornitori con accesso fisico o virtuale ai sistemi informativi o al codice software.

La ricerca mostra che sono necessari miglioramenti significativi al governo della supply chain. Di seguito gli aspetti più interessanti:

- il 20% afferma che il proprio processo di valutazione dei fornitori non include la sicurezza informatica o la privacy;
- il 39% non ha sviluppato piani di risposta agli incidenti con i fornitori in caso di un evento di sicurezza informatica;
- il 49% afferma che non sono eseguiti VA o PT sulla filiera;
- il 61% afferma che le proprie valutazioni del rischio non includono i rischi della supply chain.

In sintesi, l'84% afferma che la supply chain della propria organizzazione ha bisogno di una governance migliore rispetto a quella attuale.

7.1.3 Ricerca Verizon

Giunta ormai alla quindicesima edizione, la pubblicazione Verizon Data Breach Investigations Report[115] porta alla luce dati e statistiche utili per gli specialisti nella gestione degli incidenti.

Nell'edizione 2022 sono stati aggregati e analizzati i dati relativi a 23.896 incidenti di sicurezza che hanno comportato 5.212 data breach nel periodo compreso tra il 1 novembre 2020 ed il 31 ottobre 2021.

Occorre soffermarsi sulla terminologia: per "incidente" si intende la compromissione potenziale dei parametri fondamentali di sicurezza (riservatezza, integrità e disponibilità), mentre con il termine "data breach" si fa riferimento alla compromissione di tali informazioni confermata da parte dell'organizzazione colpita dall'attacco.

Estraendo dal report i dati che riguardano esclusivamente gli attacchi che hanno coinvolto a vario titolo i partner delle organizzazioni, ossia i fornitori che hanno un ruolo attivo nella supply chain ICT, risulta che i casi in cui tali soggetti sono stati,

115 https://www.verizon.com/business/resources/reports/dbir/.

loro malgrado, vettori di attacco nel caso di incidenti di sicurezza sono stati 3.403.

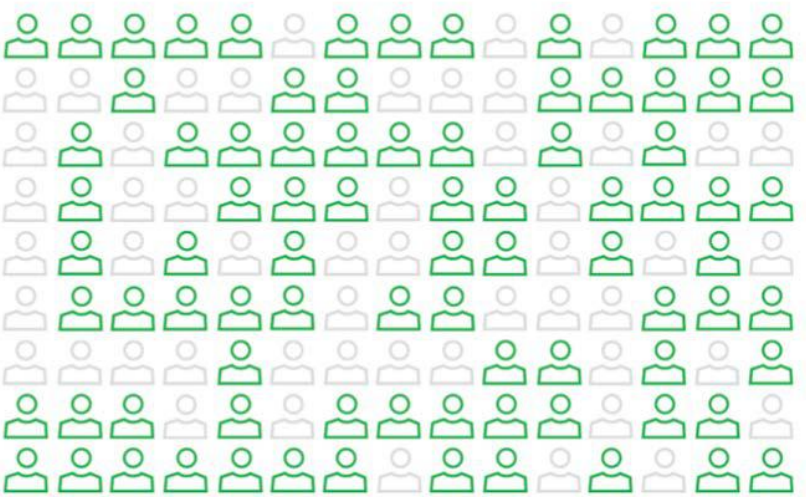


Figure 7. Partner vector in System Intrusion incidents (n=3,403)
Each glyph represents 25 incidents.

Figura 19 – Fornitori vettori di attacco[116]

Considerando la categoria di incidente "intrusione", il 60% dei dati analizzati indica i fornitori come vettore di attacco.

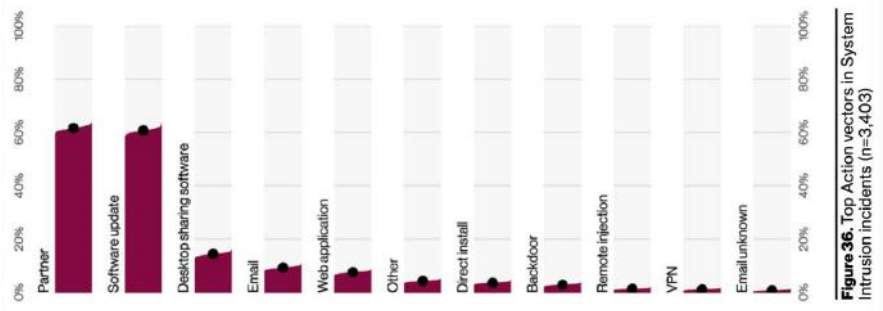


Figura 20 – Vettori di attacco degli incidenti[117]

116 DBIR – Verizon Data Breach Investigations Report.
117 DBIR – Verizon Data Breach Investigations Report.

Va comunque specificato che tali statistiche sono in parte non significative, considerando l'attacco del 2020 a Solarwinds, che ha coinvolto un numero rilevante di clienti finali.

7.1.4 Rapporto di ENISA

Il rapporto ENISA del 2021[118] sulle minacce informatiche alla supply chain si focalizza sugli incidenti rilevati tra gennaio 2020 e luglio 2021.

Si tratta di **24 attacchi**, di cui 8 avvenuti nel 2020 e 16 nei primi 6 mesi del 2021. Gli attacchi sono aumentati in numero e sofisticazione nel 2020 e la tendenza è continuata nel 2021, con un conseguente aumento del rischio per le organizzazioni.

Gli attacchi alla supply chain si confermano una minaccia rilevante anche nel rapporto pubblicato a novembre 2022[119] (dedicato alle minacce informatiche in generale) rientrando a pieno titolo tra le principali 8 minacce.

A livello di trend nel report vengono citati i seguenti dati, ripresi da altre ricerche, che testimoniano la gravità della situazione: tra il 39%[120] e il 62%[121] delle organizzazioni ha sofferto degli impatti di un incidente di cyber-sicurezza occorso a un fornitore.

Secondo il report Mandiant M-Trends[122] le compromissioni alla supply chain sono state il secondo prevalente vettore di infezione rilevato nel corso del 2021, che hanno caratterizzato il 17% delle intrusioni rilevate rispetto all'1% del 2020.

Circa la metà degli incidenti indicati nel report del 2021 ha avuto un impatto su scala globale (si veda la figura seguente).

118 ENISA, Threat Landscape for Supply Chain Attacks, 2021, https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

119 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

120 WEF Global Cybersecurity Outlook 2022 https://www.weforum.org/reports/global-cybersecurity-outlook-2022/.

121 Anchore 2022 Security Trends: Software Supply Chain Survey https://anchore.com/blog/2022-security-trends-software-supply-chain-survey/.

122 Mandiant M-TRENDS 2022 https://www.mandiant.com/resources/m-trends-2022.

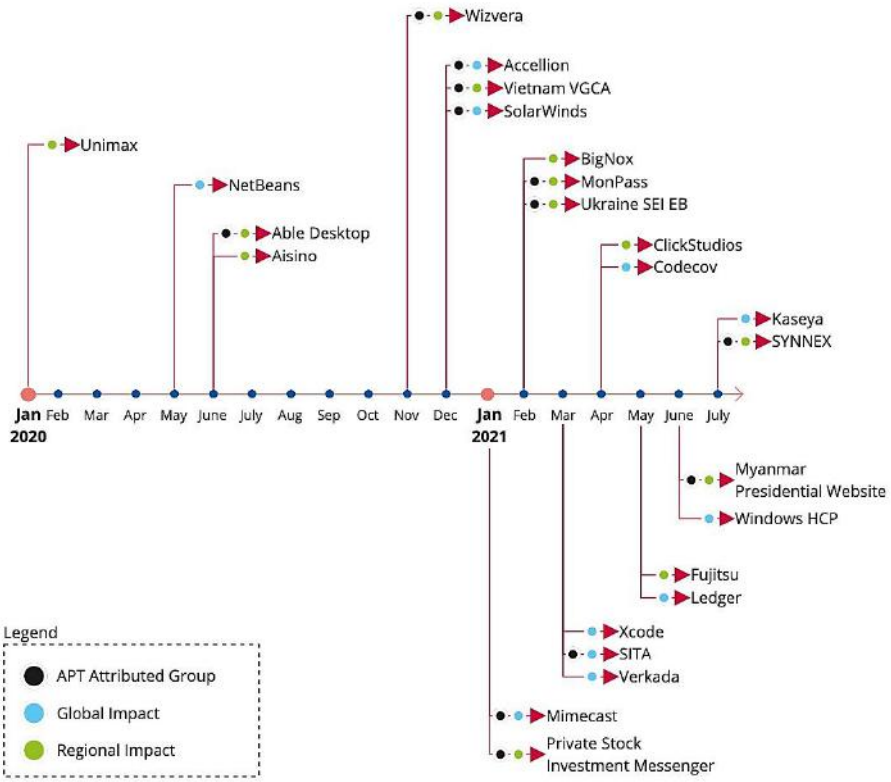


Figura 21 – Timeline di attacchi a supply chain riportate da gennaio 2020 a luglio 2021. [123]

Il rapporto ENISA fornisce una tassonomia per classificare gli attacchi alla supply chain e un'analisi specifica dei 24 attacchi segnalati.

Secondo la ricerca, un attacco a una supply chain deve necessariamente considerare tutti e quattro gli elementi di una supply chain e in particolare:

- tecniche di attacco usate per compromettere la supply chain;
- asset del fornitore che sono stati target di attacco;
- tecniche di attacco usate per compromettere il cliente a cascata;
- asset del cliente che sono stati target di attacco.

Se nessun fornitore o nessun cliente è attaccato, probabilmente non ci troviamo di

123 https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

fronte a un attacco alla supply chain. La tassonomia evidenzia quindi **come** il fornitore è attaccato, e **quale è stato l'oggetto** di tale attacco. In modo speculare, la tassonomia evidenzia anche **come** il cliente è stato attaccato, e **quale è stato l'oggetto** di tale attacco per il cliente.

La tassonomia risulta particolarmente utile per identificare i passi di un attacco attraverso la supply chain. Ad esempio, la figura seguente permette di descrivere il caso SolarWinds (paragrafo 7.2.1) con la tassonomia proposta da ENISA.

SUPPLIER		CUSTOMER	
Attack Techniques Used to Compromise the Supply Chain	Supplier Assets Targeted by the Supply Chain Attack	Attack Techniques Used to Compromise the Customer	Customer Assets Targeted by the Supply Chain Attack
Exploiting Software Vulnerability, Brute-force attack, Social Engineering	Processes, Code	Trusted Relationship [T1199], Malware Infection	Data

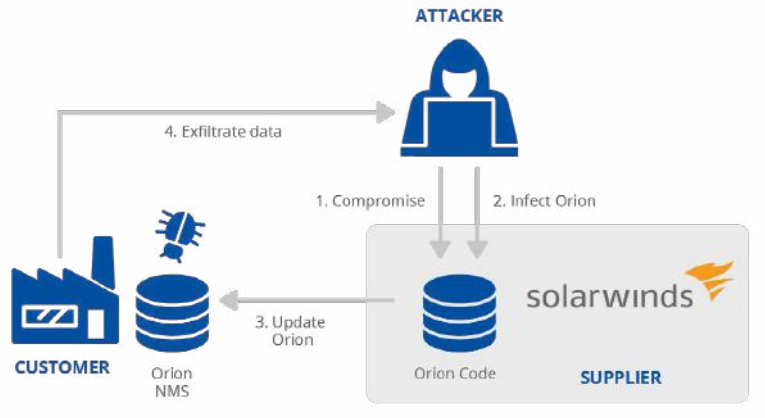


Figura 22 – Attacco a SolarWinds analizzato secondo la tassonomia proposta da ENISA. [T1199] si riferisce all'identificatore della tecnica utilizzata nel framework MITRE ATT&CK®.[124]

124 https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

Dall'analisi dei 24 attacchi, emergono alcune evidenze:

- nella maggior parte dei casi (66%), non è stato possibile determinare le tecniche di attacco usate per compromettere il fornitore; nel 16% dei casi si tratta invece di sfruttamento di vulnerabilità del software;
- relativamente agli asset del fornitore, il 66% degli incidenti ha avuto come obiettivo il codice del software sviluppato dal fornitore per compromettere clienti specifici;
- gli asset compromessi lato fornitore sono usati come vettore di attacco per compromettere il cliente; in questi casi, le tecniche usate più spesso sono l'abuso della fiducia del cliente nei confronti del fornitore (62%) oppure il malware (62%);
- indipendentemente dalle tecniche utilizzate, la maggior parte degli attacchi ha lo scopo di guadagnare l'accesso ai dati del cliente (58%).

Al di là delle azioni che singoli clienti e fornitori possono intraprendere, il report ENISA evidenzia l'iniziativa SLSA (supply chain levels for software artifacts[125]) che ha come obiettivo quello di assicurare l'integrità di artefatti software attraverso la supply chain.

7.1.5 Ricerca di Hackmanac

Hackmanac[126], da oltre dieci anni, analizza e classifica cyberattacchi internazionali andati a buon fine e di pubblico dominio.

Questi dati sono significativi in quanto trattano incidenti con impatto su tutti i settori, riguardano numerose tecniche, consentono di ricavare i trend globali di anno in anno.

In base ai dati raccolti, i cyberattacchi perpetrati ai danni di supply chain nel periodo 2019-2021, il cui numero annuo totale è riportato nella figura seguente, risultano così suddivisi:

- Attacchi totali a livello globale: 260;
- Attacchi critici: 85;
- Attacchi verso infrastrutture critiche: 173;
- Attacchi registrati in Italia: 3.

125 https://security.googleblog.com/2021/06/introducing-slsa-end-to-end-framework.html.
126 https://hackmanac.com/it. https://hackmanac.com/it.

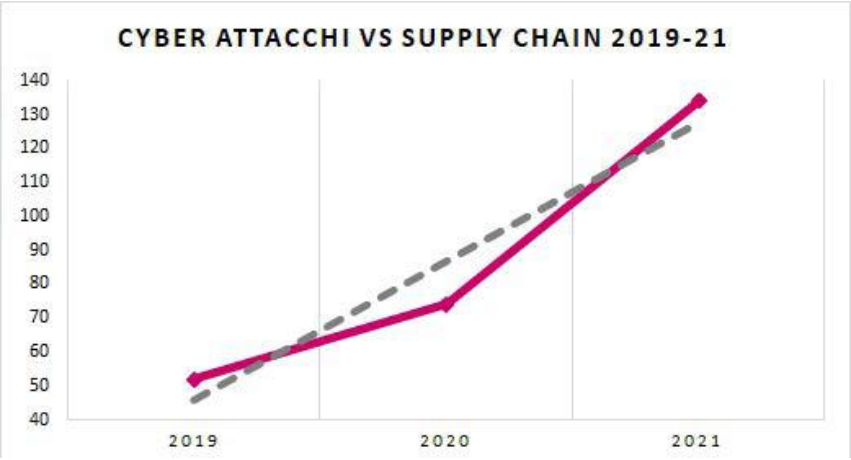


Figura 23 cyberattacchi alla supply chain 2019-2021[127]

È doveroso evidenziare come tali attacchi siano stati perpetrati soprattutto ai danni del settore sanitario, istituzioni governative e PA.

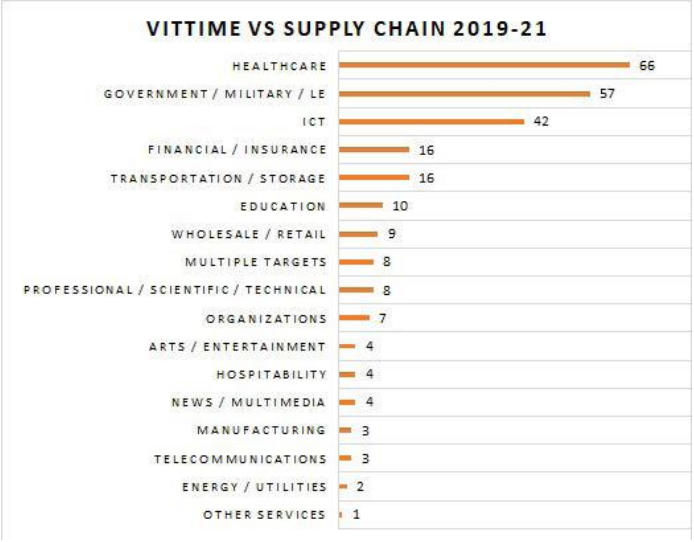


Figura 24 - Numero totale di cyberattacchi per settore nel 2019-2021[128]

127 Fonte: Hackmanac Global Cyber Attacks Report 2019-2021.

128 Fonte: Hackmanac Global Cyber Attacks Report 2019-2021.

L'America e l'Europa occupano rispettivamente la prima e la seconda posizione della classifica di cyberattacchi alla supply chain come indicato nella figura a sinistra, mentre a destra è evidenziata la gravità degli attacchi.

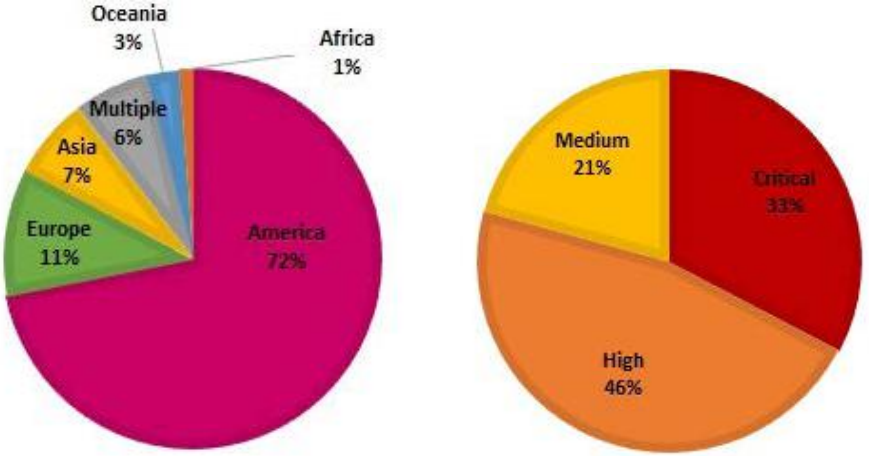


Figura 25 – Distribuzione geografica dei cyberattacchi alla supply chain e loro gravità[129]

Lo scenario non cambia significativamente se volgiamo la medesima analisi alle infrastrutture critiche.

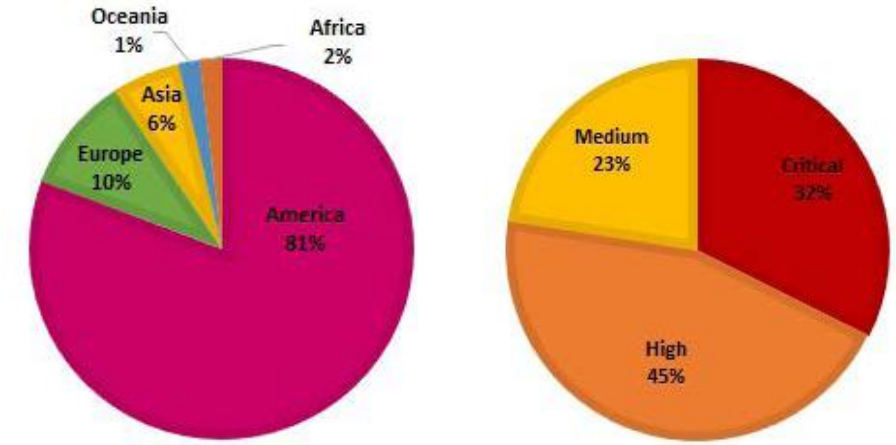


Figura 26 – Distribuzione geografica dei cyberattacchi alla supply chain delle infrastrutture critiche nel 2019-2021 e lo classe di gravità[130]

129 Fonte: Hackmanac Global Cyber Attacks Report 2019-2021.

130 Fonte: Hackmanac Global Cyber Attacks Report 2019-2021.

7.2 Esempi di incidenti di sicurezza

Nel seguito sono riassunti alcuni dei casi più eclatanti verificatisi negli ultimi due anni.

7.2.1 Il caso SolarWinds

SolarWinds è un'azienda che fornisce software di gestione e monitoraggio a circa 300.000 clienti – molti dei quali presenti nella classifica Forbes 500.

Nel dicembre 2020 fu compromessa la suite Orion, uno dei prodotti più venduti dalla società, che permette di supervisionare le risorse di rete, le applicazioni e gli storage. Gli aggressori, dopo aver ottenuto l'accesso alla rete della società – probabilmente sfruttando una vulnerabilità 0-day di un'applicazione o dispositivo di terze parti – modificarono il codice sorgente del software inserendo una backdoor nota come Sunburst. L'aggiornamento del software compromesso, scaricato dai clienti, consentì agli attaccanti l'accesso alla loro rete interna e la raccolta di informazioni in modo del tutto "invisibile".
L'attacco ebbe impatto su 18.000 utenti[131] e fu attribuito al gruppo APT29.

7.2.2 Il caso SITA

SITA è un'azienda specializzata nello sviluppo di soluzioni per compagnie aeree e aeroporti, per acquisire e gestire informazioni sui passeggeri.
Nel marzo 2021 l'azienda identificò una violazione con impatto sul servizio passeggeri (Passenger Service System - PSS) ospitato all'interno del suo data center situato ad Atlanta, Stati Uniti[132].
Si trattò di un chiaro attacco alla supply chain in quanto la violazione del sistema PSS colpì direttamente tutte le compagnie aeree membri della Star Alliance e della One World Alliance[133]. Analisi approfondite sull'incidente dimostrarono che l'attacco comportò il furto di dati dei passeggeri. Inoltre fu appurato che l'attacco si prolungò per oltre tre settimane prima che fosse individuato e bloccato dagli esperti di sicurezza della società[134].
Non si è avuta alcuna informazione sull'attore di minaccia.
Air India riportò di aver registrato la violazione del database dei clienti[135], ma ulteriori indagini rivelarono che in realtà si trattava di un altro attacco distinto, di tipo state-sponsored, di un gruppo collegato al governo di Pechino e conosciuto con il

131 https://blog.checkpoint.com/2021/04/05/supply chain-attacks-what-we-know-about-the-solarwinds-sunburst-exploit-and-why-it-still-matters/.

132 https://www.sita.aero/pressroom/news-releases/sita-statement-about-security-incident/.

133 https://heimdalsecurity.com/blog/outspread-sita-security-breach-exposes-more-airlines/.

134 https://asianaviation.com/sita-falls-victim-to-cyber-attack/.

135 https://blog.group-ib.com/colunmtk_apt41.

nome di APT41 o anche come Wicked Spider (Panda), Winnti Umbrella e Barium[136].

7.2.3 Il caso Carnival Maritime

La Carnival Corporation, società anglo-statunitense, è il più grande operatore al mondo nel settore delle crociere. Gestisce nove dei principali marchi di compagnie da crociera al mondo, compresa l'italiana Costa Crociere.
Il Gruppo Carnival fu vittima di due attacchi ransomware nell'agosto e nel dicembre 2020. Quello di dicembre fu originato da una violazione alla controllata AIDA Cruises che subì un considerevole problema informatico[137]. Le navi persero la connessione a Internet e di conseguenza tutti i servizi a bordo cessarono di funzionare, così come la sede centrale di Rostock non risultò raggiungibile né per telefono né per e-mail da parte dei clienti. I problemi riscontrati ai sistemi ICT della compagnia comportarono la cancellazione di alcune crociere, tra cui quelle previste per Capodanno. L'attacco si estese anche a Costa Crociere, la quale, fino ai primi giorni del 2021, riportava problemi di connettività.
Questo attacco non è collegato a un fornitore ma a una tipologia diversa di terza parte: la violazione alla compagnia AIDA colpì direttamente altre compagnie del Gruppo.

7.2.4 Il caso Kaseya

Kaseya è una società statunitense, leader mondiale nella fornitura di servizi di gestione di sistemi da remoto.
A luglio 2021 scattò l'allarme di un attacco informatico presso i server di Kaseya. Gli aggressori sfruttarono una vulnerabilità 0-day nel prodotto VSA - Virtual System/Server Administrator - per aggirare l'autenticazione ed eseguire comandi da remoto. Ciò consentì agli aggressori di sfruttare una funzionalità di VSA per distribuire ransomware verso tutti i VSA dei clienti.
Vittime, oltre alla società stessa, furono gli utilizzatori diretti dei servizi di Kaseya e i fornitori terzi di servizi ICT, erogatori a loro volta dei servizi della società.
L'attacco è stato rivendicato dal gruppo ransomware REvil/Sodinikibil.

7.2.5 Il caso di Coop Sweden

Un altro caso interessante di incidente con impatto sulla disponibilità dei dati e sistemi è quello occorso a Coop Sweden, quando circa 800 dei supermercati della catena furono costretti a chiudere per un'intera giornata a causa di un attacco informatico, avvenuto il 3 luglio 2021, conseguenza dell'attacco a Kaseya, già descritto in precedenza.
In tale data, tutti i registratori di cassa e le casse self-service della catena Coop smi-

136 https://www.securityweek.com/researchers-attribute-sita-cyberattack-chinese-hackers.
137 https://www.cruiselawnews.com/2020/12/articles/cyber-attacks/aida-cruise-ships-under-cyber-attack-are-costa-ships-also-affected/.

sero di funzionare costringendo alla chiusura di tutti i supermercati. Il servizio iniziò a risultare indisponibile in un gruppo limitato di negozi già a partire dalla serata del 2 luglio 2021, per poi espandersi a tutti i principali punti vendita.

7.2.6 Il caso Mimecast

Altro evento ben noto è quello subito da Mimecast[138], non solo per la sua portata ma perché a sua volta derivante dall'attacco a SolarWinds.
Mimecast è una delle principali aziende americane fornitrici di servizi di sicurezza informatica basati su cloud.
Nei primi mesi del 2021 si scoprì che un certificato di connessione ai server Mimecast per il servizio di gestione in cloud degli account email Microsoft 365, rilasciato dalla società, era stato compromesso: un gruppo di attaccanti era riuscito a intercettare le connessioni di rete, inserirsi nel processo e penetrare negli account Microsoft 365 dei clienti della società, accedendo a tutte le loro informazioni. La porta di accesso ai sistemi di Mimecast era stata, a sua volta, aperta dall'attacco che nel 2020 aveva colpito SolarWinds descritto in precedenza.

7.2.7 Il caso Log4Shell

Nel dicembre 2021 fu il turno di Log4Shell, una vulnerabilità 0-day della libreria Java Log4j, tra le più utilizzate dagli sviluppatori di tutto il mondo per scrivere i file log e registrare i messaggi di errore delle applicazioni.
Questa libreria conteneva, già da diverso tempo, una vulnerabilità, classificata con il livello più alto di gravità (10 su 10 CVSS), che permetteva a qualunque malintenzionato l'accesso e la possibilità di scrivere una riga di programma per far eseguire all'applicazione prescelta, che utilizzasse la libreria, qualsiasi azione desiderata. In breve, una porta aperta potenzialmente a chiunque per inserire software malevoli, installare codici o realizzare attacchi di cyberspionaggio. Scoperta la vulnerabilità, fu rilasciata una nuova versione della libreria, ma non fu aggiornata da tutti i milioni di utilizzatori.

7.2.8 Il caso del Consorzio Asti DOCG

L'Italia non è da considerarsi indenne da attacchi informatici rivolti alla supply chain. Esempio ne è l'attacco che prese di mira il Consorzio Asti Docg, reso noto nell'aprile 2021, che bloccò per alcune ore le attività di imbottigliamento di Docg Asti e Moscato d'Asti. L'evento fu provocato dal blocco di un server di proprietà del fornitore esterno presso cui il Consorzio appoggiava i suoi sistemi.
Per far fronte alla situazione, gli esperti ICT dell'organizzazione ricrearono il data-

138 https://threatpost.com/mimecast-certificate-microsoft-supply chain-attack/162965/.

base su un server interno e solo in questo modo fu possibile riprendere le attività di assegnazione e consegna delle fascette Docg alle aziende di imbottigliamento e di inserimento dei dati di commercializzazione, minimizzando i danni dell'interruzione.

7.2.9 Il caso della sanità della Regione Lazio

Il caso italiano più eclatante, balzato alle cronache nell'estate 2021, è l'attacco alle infrastrutture sanitarie della Regione Lazio, che portò gravi conseguenze non solo ai servizi legati al settore sanitario, ma anche a molti altri servizi rivolti a cittadini e organizzazioni.
Sembrerebbe (secondo le indagini di Cnaipic, Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche) che siano state sfruttate le credenziali di un dipendente in smartworking di LazioCrea, rubate e poi pubblicate sul Dark Web. Pare fosse stato utilizzato il ransomware RansomEXX, spesso veicolato dal noto gruppo di cybercriminali Sprite Spider.
Sono ancora molte le domande senza una chiara risposta: a chi attribuire le responsabilità dell'attacco? Come fu possibile ottenere l'accesso al terminale del dipendente di LazioCrea: direttamente o tramite altri anelli della supply chain? Come fu possibile ripristinare i servizi? Ci fu realmente un' esfiltrazione di dati sensibili? Sarebbe bastato qualche minimale accorgimento in termini di sicurezza (l'autenticazione a due fattori, ad esempio) per evitare, o quantomeno contenere, gli effetti dell'attacco?
Invece molto chiari e tangibili sono le conseguenze dell'attacco: oltre al blocco del sistema di prenotazione dei vaccini e di erogazione dei green pass, rimasto inattivo per qualche giorno in una fase molto delicata, si registrarono disservizi in molti settori, alcuni durati per mesi (come il sistema di rilevazione delle liste di attesa per visite ed esami e il sito web di Cotral).

7.2.10 Altri casi significativi

Ulteriori esempi di attacchi alla supply chain ICT:

1. *Dependency Confusion*, 2021: Alex Birsan, un ricercatore di sicurezza, fu in grado di compromettere Tesla, Apple, Netflix, Uber e Microsoft. Birsan inviò pacchetti di dati falsi, ma definiti come sicuri a utenti grazie alle dipendenze richieste dai software[139];
2. *Asus*, 2018: I ricercatori di Symantec affermano che l'attacco tramite malware ad Asus colpì almeno 500.000 PC, utilizzando la funzione di aggiornamento automatico[140];
3. *GitHub*, 2018: GitHub fu infettato da malware come parte di un attacco più

139 https://owasp.org/www-project-top-10-ci-cd-security-risks/CICD-SEC-03-Dependency-Chain-Abuse.
140 https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/asus-supply chain-attack.

generale, e un numero imprecisato di software ebbe accesso, tramite dipendenza, al repository che ospitava il malware[141];

4. MPS, 2022: Nel mese di giugno 2022 toccò ai sistemi della banca Monte dei Paschi di Siena. Attraverso un attacco strutturato gli attaccanti avevano come obiettivo gli indirizzi email dei clienti.
5. *Aisino*, 2020: Per l'elaborazione digitale delle dichiarazioni IVA, il governo cinese sviluppò il programma Golden Tax. Questo programma fu distribuito da due aziende, Baiwang e Aisino, e integrato nei loro prodotti. Il 25 giugno 2020, la società di sicurezza informatica di Singapore Trustwave rivelò che il prodotto di Aisino includeva una backdoor (soprannominata "GoldenSpy"). Due ore dopo l'installazione del software di gestione IVA, i codici della backdoor erano scaricati ed eseguiti all'insaputa degli utenti. Questo codice comunicava con un server remoto ad una frequenza casuale e consentiva l'esecuzione di codice arbitrario con privilegi di amministratore di sistema senza interazione dell'utente. GoldenSpy permaneva sui sistemi anche quando il software di Aisino veniva disinstallato.

141 https://www.cshub.com/attacks/news/github-supply chain-attack-could-affect-83-million-developers.

8. NORMATIVE DI RIFERIMENTO

Se anni fa l'individuazione di un fornitore avveniva in base a valutazioni basate sulla fiducia e sulla convenienza economica, oggi l'imposizione di molteplici normative richiede che il committente, ossia il soggetto che affida la fornitura, debba valutare l'idoneità del fornitore rispetto a molteplici ambiti (protezione dei dati, cybersecurity, sicurezza sul lavoro, previdenza, ecc.) e verificare periodicamente il permanere di tale "idoneità".

L'importanza della sicurezza nell'ambito della supply chain ha comportato la necessità, recepita dagli organi di governo nazionali e internazionali e da istituti di ricerca sulla cybersecurity ed enti regolatori, di definire e regolare la sicurezza informatica nei contesti propri della supply chain. Allo scopo, da un lato sono stati sviluppati framework e standard di sicurezza della supply chain che possono essere presi come importante riferimento dalle organizzazioni per costruire adeguatamente la propria strategia su questo ambito e, dall'altro lato, sono state emanate leggi e regolamenti specifici (compliance normativa) che dettano requisiti e obbligano le organizzazioni di determinati settori a seguire regole e approcci omogenei di cybersecurity con un occhio di riguardo alla supply chain.

Riportiamo qui di seguito un elenco di leggi, direttive, regolamenti e standard più conosciuti e consolidati che trattano il tema della sicurezza della supply chain.

Nel capitolo successivo sono presentati standard e framework internazionali.

8.1 GDPR

Il GDPR (come previsto dall'Art. 28 paragrafo 1 e dal Considerando 81) permette di ricorrere solamente a responsabili che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative adeguate che soddisfino i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

L'Art. 28 paragrafo 2 richiede che il responsabile del trattamento non ricorra a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del

titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

L'Art. 28 paragrafo 3, insieme al Considerando 81, richiede che l'esecuzione dei trattamenti da parte di un responsabile del trattamento sia disciplinata da un contratto o da altro atto giuridico (detto DPA – Data processing Agreement) a norma del diritto dell'Unione o degli Stati membri che vincoli il responsabile del trattamento al titolare del trattamento, in cui, tra gli altri, siano inclusi la materia disciplinata e la durata del trattamento, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, tenendo conto dei compiti e responsabilità specifici del responsabile del trattamento nel contesto del trattamento da eseguire e del rischio in relazione ai diritti e alle libertà dell'interessato. L'art. 28 riporta ulteriori elementi da includere.

Nell'ambito della regolazione del rapporto di responsabilità e sub responsabilità, il DPA è uno strumento ormai consolidato. Va valutata con attenzione però la sua applicazione e la sua efficacia. Il titolare infatti tende a inviare lo stesso DPA a tutti i responsabili senza operare nessun tipo di controllo relativo all'effettivo utilizzo dei dati personali da parte degli stessi. Al contempo, soprattutto in responsabili o sub responsabili con scarsa attenzione alle tematiche della protezione dei dati, si tende a dare risposte affermative ai requisiti richiesti per non incorrere in eventuali grattacapi o approfondimenti.

Si raccomanda quindi di svolgere audit sui fornitori e sub-fornitori. Gli audit dovrebbero essere anche eseguiti in caso di eventuali segnali di un problema (ad esempio ritardi di fornitura e data breach).

Il GDPR non pone requisiti ai fornitori di sistemi ed applicazioni, tranne indirettamente il Considerando 78 che incoraggia l'attenzione alla protezione dei dati. Rimane quindi al titolare (tipicamente il cliente) il totale onere della conformità al Regolamento, mentre il responsabile (fornitore) ha "solo" l'obbligo di proteggere i dati con misure tecniche ed organizzative adeguate al rischio.

Le autorità di controllo possono comunque pubblicare orientamenti, linee guida e buone prassi. Su questo argomento, il Garante tedesco del Baden-Württemberg ha pubblicato nel 2022 un codice di condotta ("Trusted Data Processor"[142]).

142 https://www.verhaltensregel.eu/wp-content/uploads/2022/11/Verhaltensregel_Trusted_Data_Processor_V1.pdf.

8.2 NIS e NIS 2

La Direttiva (UE) 2016/1148 (Direttiva NIS – Network and Information Security) è stato il primo atto legislativo adottato per migliorare la cybersecurity di soggetti pubblici e privati all'interno dell'UE.

Il rapido sviluppo del mondo digitale, il nascere di normative specifiche nei singoli Paesi sulla sicurezza nazionale (in Italia il PSNC, descritto al paragrafo successivo), nonché la pandemia di COVID-19, hanno evidenziato l'importanza e la necessità di rafforzare ulteriormente il quadro normativo, tanto da indurre la Commissione UE a proporre un aggiornamento della Direttiva NIS al fine di fornire risposte adeguate e innovative al nuovo panorama e alle sue sfide[143].

La Direttiva NIS 2 che è stata approvata e pubblicata nella Gazzetta Ufficiale come Direttiva (UE) 2022/2555[144], delinea alcune novità importanti, tra le quali:

1. elimina la distinzione tra fornitori di servizi essenziali e fornitori di servizi digitali, classificando le organizzazioni in "essenziali" o "importanti" a seconda della criticità dei servizi che offrono;
2. amplia il suo ambito d'applicazione, in quanto sono inclusi ulteriori servizi, come la produzione di prodotti farmaceutici e di dispositivi medici;
3. rafforza la sicurezza informatica lungo la supply chain.

In merito alle criticità legate alla supply chain, la direttiva impone agli Stati membri di adottare una strategia nazionale che tenga in considerazione le vulnerabilità dei fornitori e di:

- adottare misure relative alla cybersecurity della supply chain dei servizi delle tecnologie dell'informazione (TIC) utilizzati dai soggetti essenziali e importanti;
- provvedere affinché i soggetti essenziali e importanti adottino misure tecniche e organizzative adeguate per gestire i rischi di sicurezza relativi ai fornitori, quali quelli di servizi di conservazione ed elaborazione dei dati o di servizi di sicurezza gestiti.

143 https://www.cybersecurity360.it/cybersecurity-nazionale/direttiva-nis-2-gli-sviluppi-attuali-e-gli-scenari-futuri-il-punto/.
144 https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32022L2555

8.3 PSNC

Il D.L. 21 settembre 2019 n. 105, convertito con modificazioni dalla Legge n. 133 del 2019, istituisce il perimetro di sicurezza nazionale cibernetica con l'obiettivo di tutelare la sicurezza dello Stato e garantire un elevato livello di sicurezza delle reti, dei sistemi e dei servizi informatici da cui dipende l'esercizio di una funzione essenziale o l'erogazione di un servizio essenziale dello Stato.

I soggetti inclusi nel perimetro, individuati dal DPCM n. 131 del 2020 hanno determinati obblighi, tra cui:

- predisposizione e trasmissione dell'elenco delle reti, dei sistemi informativi e dei servizi informatici (i cosiddetti "beni ICT");
- valutazione dell'impatto di un incidente sui beni ICT in termini di limitazione della sua operatività, nonché di compromissione della disponibilità, integrità, o riservatezza dei dati;
- notifica al CSIRT degli incidenti aventi impatto sui beni ICT (DPCM n. 81 del 2021);
- adozione di misure di sicurezza per i beni ICT (DPCM n. 81 del 2021);
- comunicazione al Centro di valutazione e certificazione nazionale (CVCN) dell'intenzione di procedere all'affidamento di forniture di beni, sistemi e servizi informatici, appartenenti a categorie specifiche, destinati a essere impiegati sui beni ICT, per una valutazione tecnologica degli stessi (DPR n. 54 del 2021).

8.3.1 CVCN – Centro di valutazione e certificazione nazionale

In caso di comunicazione al CVCN dell'intenzione di acquisire da terze parti beni, sistemi e servizi ICT, il CVCN avvia e completa il procedimento di verifica e valutazione del bene ICT attraverso l'analisi della documentazione ricevuta e la predisposizione di un provvedimento con il quale indica al soggetto incluso nel perimetro eventuali condizioni a cui i fornitori dovranno attenersi e i test di hardware e software da eseguire.

Con il DPCM del 15 giugno 2021 sono stati definiti i criteri per individuare le categorie e i beni ICT per i quali i soggetti inclusi nel perimetro dovranno necessariamente effettuare la comunicazione al CVCN.

Le categorie sono quattro:

1. Componenti hardware e software che svolgono funzionalità e servizi di rete di telecomunicazione (accesso, trasporto, commutazione). Esempi: router, switch, gateway wi-fi.
2. Componenti hardware e software che svolgono funzionalità per la sicurezza di reti di telecomunicazione e dei dati da esse trattati. Esempi: firewall, security gateway, VPN, IDS, IPS.
3. Componenti hardware e software per acquisizione dati, monitoraggio, supervisione controllo, attuazione e automazione di reti di telecomunicazione e sistemi industriali e infrastrutturali. Esempi: sistemi SCADA, sistemi di artificial intelligence, sistemi 5G.
4. Applicativi software per l'implementazione di meccanismi di sicurezza. Esempi: PKI, SSO, web service con API.

Secondo quanto previsto dal DPR n. 54 del 2021, l'approvvigionamento dei beni ICT si articola in tre fasi:

1. verifiche preliminari;
2. fase di preparazione all'esecuzione dei test;
3. esecuzione dei test di hardware e di software.

8.3.2 Misure di sicurezza per i beni ICT

Il DPCM 81 del 14 aprile 2021 richiede che siano implementate misure di sicurezza. Relativamente alla supply chain, l'organizzazione deve:

- avere definito, implementato e documentato i processi atti a identificare, valutare e gestire il rischio legato alla supply chain;
- valutare regolarmente i fornitori e i partner terzi utilizzando audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali;
- utilizzare un processo di valutazione dell'affidabilità tecnica dei fornitori e dei partner terzi, con riferimento alle migliori pratiche in materia e tenendo conto almeno:
    - della qualità dei prodotti e delle pratiche di cybersecurity del fornitore e dei partner terzi, anche considerando il controllo degli stessi sulla propria supply chain e la priorità data agli aspetti di sicurezza;
    - della capacità del fornitore e dei partner terzi di garantire l'approvvigionamento, l'assistenza e la manutenzione nel tempo.

8.4 PCI DSS

Il Payment Card Industry Data Security Standard (PCI DSS) è stato sviluppato per incoraggiare e migliorare la sicurezza dei dati degli account delle carte di pagamento[145].
La PCI DSS è giunta alla versione 4.0, pubblicata a marzo 2022, e si compone di 12 requisiti minimi da rispettare per rafforzare la sicurezza degli account dei titolari di carta.
Il tema della sicurezza nella supply chain è affrontato nei requisiti 12.8 e 12.9.

8.4.1 Requisito 12.8

Il requisito prevede che: "Risk to information assets associated with third-party service provider (TPSP) relationships is managed".

Un'entità (denominata "cliente" in questa sezione) potrebbe scegliere di utilizzare un fornitore di servizi di terze parti (TPSP) per archiviare, elaborare o trasmettere dati dell'account o per gestire i componenti del sistema in ambito per conto del cliente. L'uso di un TPSP può avere un impatto sulla sicurezza dei sistemi informatici del cliente.

Esistono molti scenari diversi in cui un cliente potrebbe utilizzare uno o più TPSP. In tutti gli scenari, il cliente deve gestire e supervisionare lo stato di conformità PCI DSS di tutti i propri TPSP che:

- hanno accesso ai sistemi informatici del cliente;
- gestiscono i componenti del sistema in ambito per conto del cliente;
- possono influire sulla sicurezza dei sistemi informatici del cliente.

La gestione dei TPSP in conformità con il Requisito 12.8 include l'esecuzione della due diligence, l'adozione di accordi appropriati, l'identificazione di quali requisiti si applicano al cliente e quali si applicano al TPSP e monitorare lo stato di conformità dei TPSP almeno annualmente. Il requisito 12.8 non specifica che i TPSP del cliente devono essere conformi a PCI DSS, ma solo che il cliente monitori il proprio stato di conformità.

8.5 Requisito 12.9

Il requisito prevede che: "Third-party service providers (TPSPs) support their customers' PCI DSS compliance".

145 Payment Card Industry Data Security Standard: Requirements and Testing Procedures, v4.0.

Questo requisito ha lo scopo di promuovere un coerente livello di comprensione tra TPSP e i clienti sulle responsabilità del mantenimento dello standard PCI DSS. I TPSP, ad esempio, confermano per iscritto ai clienti che sono responsabili della sicurezza dei dati dell'account che possiedono o memorizzano, elaborano o trasmettono per conto del cliente, o nella misura in cui potrebbero avere un impatto sulla sicurezza dei sistemi informatici del cliente.

8.5 Direttiva dei sistemi di pagamento PSD2

La Direttiva dei sistemi di pagamento (Direttiva UE 2015/2366, PSD2) è stata sviluppata dal legislatore europeo per migliorare il quadro normativo dei servizi di pagamento e dei gestori dei servizi di pagamento.

La Direttiva rafforza le procedure di sicurezza che le istituzioni finanziarie devono rispettare per l'accesso al conto online e per i pagamenti elettronici e impone (art. 95) l'attuazione di un *quadro di misure di mitigazione e meccanismi di controllo adeguati per gestire i rischi operativi e di sicurezza, relativi ai servizi di pagamento che prestano.*

La gestione di tali rischi non può pertanto prescindere dal valutare le criticità legate ai fornitori terzi, a cui le istituzioni finanziarie fanno ricorso per implementare e integrare i propri sistemi ICT.

L'ABE (Autorità Bancaria Europea), coerentemente a quanto stabilito dall'art. 95 della PSD2, ha fornito alcune linee guida (l'ultima del 2019) per gestire e mitigare i rischi operativi e di sicurezza legati ai servizi di pagamento, suggerendo una serie pratiche da adottare:

- stabilire un quadro d'azione per perseguire l'obiettivo indicato dalla strategia ICT (tali piani dovrebbero essere comunicati a tutti gli interessati, compresi i fornitori);
- mantenere aggiornato l'inventario delle risorse informatiche che supportano le funzioni dell'organizzazione e i loro processi, nonché i soggetti terzi e le dipendenze da altri sistemi interni ed esterni;
- effettuare periodicamente un'analisi di impatto sull'operatività (cosiddetta BIA o business impact analysis), tenendo in considerazione anche i fattori esterni, quali ad esempio le criticità dei fornitori;
- valutare la capacità dei "piani di continuità operativa" in relazione alla loro

capacità di sostenere la redditività in seguito a un incidente e fino a quando le criticità non saranno risolte;

- accertarsi che le politiche di sicurezza dei fornitori siano conformi alle proprie politiche interne e garantire la propria capacità di comunicare in modo tempestivo e appropriato un eventuale incidente informatico a tutti gli interessati rilevanti, compresi i fornitori[146];
- garantire l'efficacia delle misure di sicurezza in caso di esternalizzazione delle funzioni operative dei servizi di pagamento, compresi i sistemi informatici;
- garantire che i contratti e gli accordi di livello del servizio conclusi con i prestatori ai quali hanno esternalizzato tali funzioni contemplino obiettivi, misure e prestazioni adeguate e proporzionate in materia di sicurezza;
- monitorare e ottenere garanzie per quanto riguarda il livello di conformità dei fornitori agli obiettivi, alle misure e alle prestazioni di sicurezza[147].

8.6 DORA – Digital resilience operational act

Alla data del 11 maggio 2022, il Consiglio e il Parlamento europeo hanno raggiunto l'accordo provvisorio sul Digital operational resilience act (DORA). Il 28 novembre 2022 il Consiglio ha approvato formalmente DORA.

Aggiornamenti sullo stato di DORA (testo da aggiornare): pubblicato il 27 novembre 2022 ed entrerà in vigore a gennaio 2023 (da usare il passato a questo punto, visto che questo libro verrà presentato a marzo) ed avrà applicazione a partire dal 17 Gennaio 2025. Titolo per benino è REGOLAMENTO (UE) 2022/2554 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011

Link: **https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32022R2554?**

DORA ha lo scopo di mettere in atto un quadro completo sulla resilienza operativa digitale per le entità finanziarie dell'UE e di consolidare e aggiornare i requisiti di rischio ICT.

146 EBA/GL/2019/04 – Orientamenti dell'EBA sulla gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (information and Communication Technology – ICT) e di sicurezza. https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/Updated%20Translations/880818/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management_COR_IT.pdf.

147 Orientamenti sulle misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento ai sensi della direttiva (UE) 2015/2366 (PSD2 EBA/GL/2017/17)" del 12/01/2018.

DORA richiede che EBA (European Banking Authority) stabilisca indirizzi in materia di gestione del rischio ICT, segnalazione degli incidenti, test di resilienza operativa digitale, misure per una sana gestione da parte delle entità finanziarie del rischio di terze parti ICT e un nuovo ruolo di supervisione dell'ESA (European Supervisory Authorities, le autorità di vigilanza) sui fornitori critici di ICT.

Viene definito un quadro di requisiti per l'includere i fornitori critici di servizi ICT (CTTPs) all'interno del perimetro normativo e nelle strategie di ICT third party risk management.

Negli ultimi anni si era assistito ad una convergenza della disciplina con la definizione di un complesso di norme comunitarie e di recepimenti a livello nazionale, con un quadro regolamentare composto principalmente dagli Orientamenti EBA in materia di esternalizzazione[148] e di ESMA (European Securities and Markets Authority) in materia di esternalizzazione dei servizi cloud[149].

Agli orientamenti precedenti si affianca il DORA Framework che orienta verso modelli di gestione del rischio in logica di accrescimento della resilienza dei processi, con un focus specifico su:

- testing della resilienza dei sistemi;
- classificazione degli eventi di perdita;
- gestione del rischio derivante dalle terze parti;
- condivisione delle informazioni tra i player.

Il framework indica una gestione del rischio ICT che include i servizi gestiti dalle terze parti e richiede di definire una strategia, approvata dal CdA, multi-vendor per i servizi ICT, in grado di evidenziare le dipendenze chiave per ciascuna entità.

In questo quadro sono risultati particolarmente significativi i suggerimenti forniti da EBF (European Banking Federation), che, ai fini della gestione dei rischi e di sicurezza e della vigilanza su terze parti (articoli da 25 a 28 di DORA), ha proposto di fare riferimento al documento di EBA "Guidelines on ICT and security risk management" (EBA/GL/2019/04).

148 https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2761380/1c9aaefc-e10d-45a6-8a51-1fb450814a29/EBA%20revised%20Guidelines%20on%20outsourcing_IT.pdf.

149 https://www.esma.europa.eu/sites/default/files/library/esma_cloud_guidelines_it.pdf.

8.7 Circolare 285 Banca d'Italia

Nel settore bancario, Banca d'Italia, attraverso la circolare n. 285/2013, fornisce la definizione di esternalizzazione precisando che si tratta dell'accordo tra la banca ed un fornitore di servizi in base al quale quest'ultimo realizza, su base continuativa o ripetitiva, un processo, un servizio o un'attività che rientrano tra quelli tipici e normalmente svolti dalla banca stessa.

In coerenza con l'approccio fondato sull'identificazione, la gestione e la mitigazione del rischio che è tipico del mondo bancario, con la già citata circolare n. 285, Banca d'Italia ha imposto, a tutti gli intermediari che intendano ricorrere ad una esternalizzazione, di valutare tale scelta considerandone attentamente tutti i rischi operativi, organizzativi e legali e di mettere in atto le idonee misure di contenimento del rischio.

Quando a essere esternalizzata è una componente critica del sistema informativo (vale a dire, secondo la definizione datane dalla circolare, "il sistema o l'applicazione per i quali un incidente di sicurezza informatica può pregiudicare il regolare e sicuro svolgimento di funzioni essenziali o importanti per l'intermediario, tra cui l'efficace espletamento dei compiti degli organi dell'organizzazione e delle funzioni di controllo") o l'intero sistema informativo, stante l'accrescimento del rischio, Banca d'Italia richiede cautele ulteriori.

Sotto questo profilo, un'importanza particolare è data al contratto, quale strumento di mitigazione e governo del rischio insito nell'esternalizzazione.

Oltre ai contenuti contrattuali previsti dagli orientamenti dell'EBA (European Banking Authority) in materia di outsourcing (cui la circolare n. 285 di Banca d'Italia, dopo i più recenti aggiornamenti, fa richiamo integralmente), il cap. 3, sezione VI della Circolare prevede che nell'accordo scritto tra la banca e i fornitori di servizi ICT debbano essere definiti e chiaramente formalizzati almeno i seguenti aspetti:

- le misure di attenuazione dei rischi garantite dal fornitore dei servizi, che devono essere conformi con il quadro di riferimento per la gestione del rischio della banca, con particolare riguardo a quello ICT e di sicurezza;
- le misure idonee a garantire l'accountability e la ricostruibilità delle operazioni effettuate, almeno con riferimento alle operazioni critiche e agli accessi a dati personali o sensibili;
- l'obbligo per il fornitore di servizi, una volta concluso il rapporto contrattuale e trascorso un periodo di tempo concordato, di eliminare – facendo uso di

opportuni strumenti e soluzioni tecniche, debitamente documentati – qualsiasi copia o stralcio di dati personali o sensibili presente su propri sistemi o supporti in ragione dei servizi in precedenza esternalizzati dalla banca, in modo da escludere qualunque accesso successivo da parte del proprio personale o di terzi;

- la ripartizione dei compiti e delle responsabilità attinenti all'attuazione della politica di sicurezza delle informazioni della banca;
- il raccordo con i ruoli e le procedure dell'intermediario attinenti al processo di analisi dei rischi ICT e per il sistema di gestione dei dati (cfr. Sezione V).

Una meticolosa analisi precontrattuale, unitamente a un'eventuale integrazione in via negoziale dei testi proposti dai fornitori, dovrebbe quindi precedere la conclusione degli accordi e costituire un presupposto indispensabile per garantire la conformità dell'intermediario alla normativa di vigilanza prudenziale dettata da Banca d'Italia.

Per l'esternalizzazione in cloud è richiesto il monitoraggio dei requisiti di sicurezza dei dati e dei sistemi da prevedere nel contratto.

8.8 Regolatori UE in ambito finanziario

Le Linee guida e gli Orientamenti emanati da EIOPA (European insurance and occupational pension authority), EBA (European banking authority), ESMA (European security and market authority), come misure di terzo livello, sono volti a promuovere un approccio convergente nell'Unione europea e sono direttamente applicabili alle Autorità di vigilanza di settore di ciascun Paese aderente all'UE e ai soggetti destinatari della relativa sorveglianza. Le Linee guida sono soggette a un meccanismo di comply or explain in base al quale l'Autorità di vigilanza nazionale deve dichiarare pubblicamente se intende aderire o indicare le ragioni per la mancata adesione. I Regolatori europei definiscono anche delle disposizioni di più generale orientamento su tematiche specifiche, non soggette alla procedura di comply or explain volte ad accrescere la convergenza delle pratiche di vigilanza (ad esempio Opinion, decisioni e protocolli di collaborazione, esiti delle peer review).

I riferimenti principali relativamente alla sicurezza della supply chain sono:

- Orientamenti EIOPA (Guidelines) in materia di cloud outsourcing;
- Orientamenti ESMA in materia di esternalizzazione a fornitori di servizi cloud (ESMA 50-164-4285, pubblicati il 10 maggio 2021);

- l'Orientamento EBA in materia di esternalizzazione (EBA/GL/2019/02).

Tali orientamenti forniscono raccomandazioni in merito all'identificazione, gestione e monitoraggio dei rischi derivanti dagli accordi di esternalizzazione di attività e servizi a società erogatrici di servizi cloud, con riferimento particolare a:

1. la valutazione del rischio e la due diligence da effettuare sui fornitori di servizi cloud;
2. i requisiti di governance, vigilanza e controllo da mettere in atto per monitorare le prestazioni dei fornitori di servizi cloud, nonché le modalità di uscita da tali accordi di esternalizzazione senza interruzione delle proprie attività;
3. i requisiti contrattuali fra le parti (imprese e fornitori di servizi cloud), ivi inclusi i rispettivi diritti e doveri;
4. i requisiti di sicurezza informatica e le strategie di uscita dagli accordi di esternalizzazione;
5. i requisiti da rispettare qualora il fornitore di servizi cloud per conto di un'impresa ricorra ad altri soggetti per l'esecuzione di determinate funzioni (o parti di esse) critiche o importanti (c.d. sub-esternalizzazione); (vi) le informazioni da notificare alle autorità competenti.

8.9 IVASS – Regolamento n.38/2018 – Capo VIII

Nell'ambito assicurativo, la disciplina dell'outsourcing – a partire dal Reg. Isvap n. 20 del 26 marzo 2008 sino al Reg. IVASS n. 38 del 3 luglio 2018, che ha dato attuazione a quanto previsto al riguardo dalla cosiddetta Direttiva Solvency II – deve essere letta in stretta correlazione a quella della governance e dei presidi organizzativi di cui le imprese di assicurazione devono dotarsi per garantire quella sana e prudente gestione che ne deve caratterizzare l'attività.

Il concetto di esternalizzazione in ambito assicurativo è stato definito dapprima dall'articolo 2, comma 1, lettera f) del regolamento ISVAP n.20 del 2008 come «l'accordo tra un'impresa di assicurazione e un fornitore di servizi, anche se non autorizzato all'esercizio dell'attività assicurativa, in base al quale il fornitore realizza un **processo**, un **servizio** o un'**attività** che verrebbero altrimenti realizzati dalla stessa impresa di assicurazione».

La definizione è stata poi rivista e integrata nel CAP (Codice delle assicurazioni private) come «l'accordo concluso tra un'impresa di assicurazione o di riassicurazione

e un fornitore di servizi, anche se non autorizzato all'esercizio dell'attività assicurativa o riassicurativa, in base al quale il fornitore di servizi esegue una **procedura**, un **servizio** o un'**attività**, direttamente o tramite sub esternalizzazione, che sarebbero altrimenti realizzati dall'impresa di assicurazione o di riassicurazione stessa».

Si passa, dunque, dal concetto di processo al concetto di procedura che seppur simili hanno significati differenti (dalla Legge 241 del 1990):

- «procedura»: *come un insieme di attività sequenziali e condivise per lo svolgimento di un'attività, potendo indicare un'attività messa in atto dall'autorità di vigilanza o una regolamentazione interna ad un'impresa di assicurazioni posta sotto la verifica dell'autorità di vigilanza stessa*;
- «processo»: *come un insieme di risorse strumentali e di comportamenti volti ad attuare una determinata procedura, termine che quindi identifica meglio un intero settore o attività produttiva di una qualsiasi impresa, anche assicurativa.*

Avendo i due termini significati differenti, si sono creati potenziali problemi interpretativi risolti con l'entrata in vigore del nuovo Regolamento 38/2018. Quest'ultimo, non contemplando nel testo una definizione di esternalizzazione e abrogando il Regolamento 20/2008, fa sì che l'unica definizione a cui si può far riferimento è quella contenuta nel CAP.

Definito il concetto di "esternalizzazione" e il campo applicativo, occorre porre particolare attenzione alle attività che possono rientrare tra le attività esternalizzabili, ossia:

- «attività o funzioni essenziali o importanti» (comma 1 dell'articolo 2 del Regolamento 38, alla lettera c): *attività o funzione la cui mancata o anomala esecuzione comprometterebbe gravemente la capacità dell'impresa di continuare a conformarsi alle condizioni richieste per la conservazione dell'autorizzazione all'esercizio, oppure i risultati finanziari, la stabilità dell'impresa o la continuità e qualità dei servizi verso gli assicurati*;
- «funzioni essenziali»: *sottoinsieme rispetto alle funzioni essenziali e importanti appena definite, identificate dal legislatore* (articolo 30 del CAP, comma 2, lettera d):
    - funzione di revisione interna (c.d. Internal auditing);
    - funzione di verifica alla conformità (c.d. Compliance);
    - funzione di gestione dei rischi (c.d. Risk management);
    - funzione attuariale.

Nel Regolamento 38 vi è un intero capo dedicato alla definizione dei requisiti di professionalità, onorabilità e indipendenza richiesti ai soggetti che rivestono la carica di esponenti aziendali e di titolari e a coloro che svolgono funzioni fondamentali, delineando anche le disposizioni valide nel caso queste funzioni vengano esternalizzate.

8.9.1 Politica di esternalizzazione

L'azienda deve definire una politica secondo quanto definito dall'articolo 5, comma 2, lettera n), attraverso la quale l'impresa, nella figura dei suoi amministratori, definisce i processi per «*l'identificazione e la valutazione del possesso dei requisiti di idoneità alla carica, in termini di onorabilità, professionalità e indipendenza di coloro che svolgono funzioni di amministrazione, direzione e controllo nonché, anche in caso di esternalizzazione o sub esternalizzazione, dei titolari e di coloro che svolgono funzioni fondamentali e dell'ulteriore personale in grado di incidere in modo significativo sul profilo di rischio*». La definizione di questa policy deve tener conto non solo delle disposizioni sopra richiamate, ma anche alla dimensione, ambito e complessità dell'attività esercitata e dell'impresa (secondo il principio di proporzionalità) e deve contenere alcuni punti minimi che vengono descritti dall'allegato 1 al Regolamento 38.

Di seguito i requisiti richiesti ai vari soggetti a seconda della funzione e se questa viene esternalizzata oppure no.

- **Funzione fondamentale non esternalizzata**: il titolare della funzione fondamentale deve rispondere ai requisiti del decreto ministeriale e a quelli della policy e si deve provvedere alla segnalazione di questi all'IVASS (art. 76, comma 1-bis, CAP). Il personale e i responsabili di più alto livello che svolgono tale funzione (escluso il titolare della funzione) devono soddisfare unicamente i requisiti previsti dalla policy interna.
- **Funzione fondamentale esternalizzata**: il titolare interno ha gli stessi obblighi previsti quando la funzione non è esternalizzata. Il responsabile della funzione individuato presso il fornitore, ai sensi dell'articolo 68 primo comma, deve possedere i requisiti previsti dalla sola policy e il nominativo deve essere comunicato all'IVASS come previsto dall'articolo 68 stesso. Per quanto riguarda il personale di più alto livello che svolge le attività collegate alle funzioni essenziali presso l'outsourcer, rispondono anch'essi ai requisiti della politica.
- **Attività o funzione essenziale o importante (non fondamentale) non esternalizzata**: il responsabile e il relativo staff devono rispondere a quanto previ-

sto dalla policy senza alcun obbligo di segnalazione a carico dell'impresa.

- **Attività o funzione essenziale o importante (non fondamentale) esternalizzata**: devono essere individuati un responsabile per l'attività di controllo sulle attività o funzioni esternalizzate che deve rispondere ai requisiti della policy, così come lo staff dedicato all'interno dell'outsourcer.

8.9.2 Scelta dei fornitori

L'azienda deve adottare idonei criteri di selezione dei fornitori, un processo di verifica, metodi per la valutazione dei risultati e delle prestazioni del fornitore (service level agreement) e indicare la frequenza delle valutazioni.

Inoltre deve dotarsi di un piano di emergenza in cui sono incluse le strategie di uscita e di eventuale nuova assegnazione in esternalizzazione.

Il regolatore prevede obblighi di comunicazione differenziati a seconda che il contratto di esternalizzazione riguardi attività essenziali o importanti, funzioni fondamentali o altre attività e se questo siano svolte all'interno o extra SEE.

8.10 Dispositivi medici

8.10.1 Le norme di legge e gli standard di riferimento

La messa in commercio di dispositivi medicali ("DM" o "medical device", "MD") è regolamentata da tempo in Europa. La normativa europea di riferimento ha ricevuto un aggiornamento che, pur risalendo al 2017, ha visto l'applicabilità del relativo Regolamento in fasi successive, a seconda della categoria di rischio, a partire da maggio 2021. L'Italia ha adeguato la propria normativa interna con il D.lgs. 5 agosto 2022, n. 137.

Come detto, il quadro attuale di riferimento è rappresentato, a livello europeo, da:

- il Regolamento (UE) 2017/745 (MDR, Medical device regulation), relativo ai dispositivi medici;
- il Regolamento (UE) 2017/746, relativo ai dispositivi medico-diagnostici in vitro.

Di particolare rilevanza per l'argomento d'interesse, sono le disposizioni di cui all'articolo 25, in merito alla tracciabilità, e all'Allegato I del Regolamento MDR "Requisiti generali di sicurezza e prestazione".

Nell'ambito di applicabilità del MDR, si evidenziano i documenti adottati dal Gruppo di coordinamento per i dispositivi medici (MDCG), come previsto dall'articolo 103 del Regolamento stesso. Tra i documenti adottati dal MDCG si segnalano le MDCG 2019-16, "Linee guida sulla *cybersecurity* nei DM".

Sempre in materia di dispositivi medici, si richiama l'attenzione alla norma tecnica ISO 13485. Essa si basa sulla ISO 9001, norma relativa ai sistemi di gestione per la qualità, e si applica alla produzione e all'immissione in commercio dei dispositivi medici.

Per la distribuzione sul mercato USA, gli operatori devono adeguarsi alla norma FDA 21 CFR 820 la cui applicazione, a differenza della ISO 13485 in Europa, è obbligatoria.

Merita una citazione anche il HIPAA (Health Insurance Portability and Accountability Act). La conformità ad esso non è strettamente rivolta ai produttori e distributori di DM, tuttavia può essere di supporto nella creazione, ricezione, manutenzione e trasmissione sicure dei dati di salute tra le strutture e i fornitori di servizi medici. La sua conformità persegue due finalità:

1. identificare quali informazioni del paziente dovrebbero essere protette;
2. fornire istruzioni per la gestione delle informazioni sulla salute del paziente.

8.10.2 Il modello proposto

Il modello proposto è quello di una responsabilità condivisa, simile ma duale rispetto a quello previsto nel cloud (sicurezza del cloud e sicurezza nel cloud):

- Sicurezza del prodotto: il fabbricante analizza i rischi e, in forza delle norme tecniche di attuazione (MDCG 16-2019), deve valutare gli impatti sulla salute. Il documento citato, richiamando lo standard ANSI/NEMA HN 1-201[150], chiede di riportare le misure di sicurezza adottate, le misure da adottare e quelle da non adottare per non creare rischi ulteriori. Il fabbricante è responsabilizzato nella gestione della supply chain, in particolare dei software of unknown provenance (SOUP), cioè dei software non sviluppati secondo il ciclo di vita richiesto per i MD, e deve vigilare sull'evoluzione delle relative vulnerabilità. Le informazioni sono anche dettagliate nel manuale di utilizzo e installazione.
- Sicurezza dei servizi sanitari erogati: l'organizzazione che fornisce servizi sanitari deve valutare se le sue condizioni di utilizzo (ambiente, rete, ecc.) sono compatibili con quanto indicato dal fabbricante e deve gestire i propri rischi, tenendo conto di quanto comunicato dal produttore.

150 https://www.nema.org/Standards/view/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.

Una figura specifica (risk manager clinico), prevista dalla Legge Gelli Bianco (L. 24/2017), sorveglia la corretta erogazione delle prestazioni sanitarie gestendo anche i "near miss", cioè eventi che potenzialmente avrebbero potuto compromettere la salute dei pazienti ma che non lo hanno fatto concretamente. Questa figura dovrebbe collaborare con altri soggetti, quali il DPO e il CISO, per assicurare che le prestazioni sanitarie siano sicure e rispondenti alle diverse normative.
A riprova del coinvolgimento dei DM nell'ambito della gestione del rischio clinico, si veda l'immagine che segue.

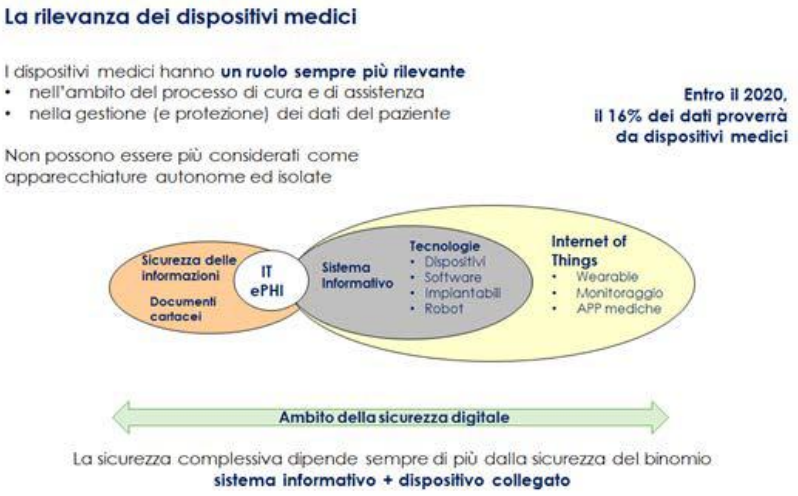


Figura 27 – Dispositivi medici e sicurezza digitale[151]

8.11 Codice etico e modello 231

Il Decreto Legislativo 8 Giugno 2001, n. 231 ha introdotto nel nostro ordinamento la responsabilità amministrativa degli enti, la quale si accompagna alla responsabilità penale della persona fisica che commette un reato a vantaggio o nell'interesse del medesimo. L'estensione della responsabilità all'ente mira a punire, oltre alla persona fisica che ha commesso il fatto, anche il patrimonio dell'ente.

In quest'ottica per gli operatori economici è diventato sempre più necessario adottare un Modello di organizzazione e gestione (MOG) ex art. 6 del D.Lgs. 231/2001, in grado di esimere l'ente da responsabilità attraverso l'applicazione delle migliori

151 https://d2pbnl7qikcego.cloudfront.net/wp-content/uploads/2020/03/word-image-7.png.

conoscenze consolidate nel momento storico in cui la condotta lesiva si è posta in essere. Pertanto, l'ente in grado di adottare e attuare un Modello di organizzazione e gestione apporterà migliorie all'interno del sistema organizzativo, monitorando i processi a presidio delle aree più a rischio al fine di non incorrere in sanzioni pecuniarie e interdittive talora gravose.

Il progetto di gestione del rischio volto alla costruzione del modello si compone inizialmente di una fase di analisi del rischio[152]. In questa sede viene mappato il contesto al fine di identificare le aree rischiose e le modalità con cui gli eventi pregiudizievoli si potrebbero astrattamente verificare. Conseguentemente si procede alla progettazione del sistema di controllo preventivo, ossia alla redazione dei protocolli[153] disciplinati dall'art. 6 comma 2 – lettera b; questi analizzano le aree di rischio individuate nella prima fase di analisi, prevedendo ruoli e responsabilità nelle diverse aree del processo e identificando le modalità di espletamento delle attività più sensibili. Infine si valutano i rischi residui, ossia quelli non coperti da controlli preventivi.

Contestualmente al MOG, per un ente è fondamentale dotarsi di un Codice etico, ossia di un documento contenente un insieme di principi e valori (tra cui la professionalità, la lealtà, l'onestà, la legalità e la correttezza e trasparenza) a cui l'impresa deve conformarsi.

Volgendo l'attenzione alla supply chain, il primo passo fondamentale che un'impresa deve compiere è quello di mettere a conoscenza dei fornitori il Codice etico, quale presupposto necessario per iniziare il rapporto di collaborazione. Infatti, il Codice etico dedica una sezione apposita alla disciplina dei rapporti con i fornitori; un'impresa dovrebbe impegnarsi a ricercare fornitori non solo dotati di forte professionalità ma anche disposti a condividere i principali valori su cui si fonda l'attività.

Inoltre, a tutela dell'integrità della sostenibilità della supply chain e del rispetto dei principi considerati irrinunciabili, l'impresa dovrebbe predisporre un "Patto etico e di integrità[154]" che ciascun fornitore e subappaltatore dovrebbe sottoscrivere per poter ricevere incarichi, impegnandosi così a conformare i propri comportamenti al rispetto dei principi previsti dal Codice Etico.

Sebbene la professionalità e le competenze siano caratteristiche necessarie, un'organizzazione deve selezionare i potenziali fornitori attraverso un'attività costante di monitoraggio, di audit e di valutazione delle prestazioni. In particolare, gli elementi

152 https://www.epc.it/contenuti/modello231_sito.pdf, pp. 136-137.

153 https://www.italiaonline.it/wp-content/uploads/2017/02/LINEE-DEL-MODELLO-231.pdf, p. 39.

154 Microsoft Word - Patto etico e di integrità (aggiornamento del 23 dicembre 2014) (snam.it).

su cui si deve fondare la valutazione del fornitore sono:

- capacità tecniche;
- affidabilità finanziaria;
- possesso di requisiti etici;
- tutela dell'ambiente;
- lotta alla corruzione;
- promozione di condizioni di lavoro salubri a tutela dei lavoratori.

Una volta individuato il fornitore ideale, quest'ultimo deve attestare di aver preso conoscenza del MOG, del Codice etico e del Patto etico mediante la sottoscrizione di tutte le clausole contrattuali a questi fini rilevanti.

8.12 Principi giuridici relativi alla fornitura

Nel diritto italiano il contratto si caratterizza per essere l'incontro tra due o più parti, la cui volontà è quella di stipulare un accordo volto a "*costituire, regolare o estinguere tra loro un rapporto giuridico patrimoniale*" (art. 1321 c.c.).

L'autonomia e la volontà delle parti sono quindi fondamentali per la sussistenza del negozio giuridico in questione.

Pur dovendo rispettare la normativa vigente, sono le parti, infatti, a determinare la tipologia e lo scopo dell'accordo, il contenuto delle rispettive obbligazioni, le tempistiche di adempimento, così come scegliere e decidere autonomamente con quale soggetto concludere il contratto.

Quest'ultimo elemento rappresenta un aspetto di particolare pregnanza, poiché, in determinati rapporti giuridici, estende le responsabilità per la parte che ha l'onere di effettuare una scelta adeguata della controparte (*culpa in eligendo*) e di vigilare sulla conformità dell'operato di quest'ultimo in base a quanto stabilito nel contratto (*culpa in vigilando*). E ciò, conformemente a quanto stabilito dal generale principio del neminem laedere, al fine di tutelare adeguatamente eventuali terze parti che, seppur estranee all'accordo, potrebbero subire lesioni ai propri diritti e interessi.

In altri termini, la **culpa in eligendo** comporta responsabilità connesse a un dovere di adeguata scelta del contraente, mentre la **culpa in vigilando** estende le responsabilità per tutta la durata del rapporto contrattuale, sulla base del dovere di controllo gravante su colui che ha effettuato la scelta.

Nel panorama giuridico italiano, diversi sono gli esempi in cui trovano applicazione i principi sopra esposti, basti pensare al dovere di scelta e vigilanza gravante sul datore di lavoro per le azioni commesse dai propri dipendenti. Si veda anche l'art. 2049 del Codice civile, applicabile alle istruzioni fornite dal committente al fornitore.

La *culpa in eligendo* e *culpa in vigilando* assumono poi grande rilevanza in tutti i casi in cui un soggetto, tenuto a svolgere un certo adempimento, decide (per ragioni organizzative o di competenza) di avvalersi di altro soggetto: in questo caso il soggetto tenuto all'adempimento risponderà in via contrattuale degli atti posti in essere dal soggetto terzo che lui ha scelto.

In alcuni casi - considerati di maggior impatto - il legislatore è poi intervenuto a dettare regole precise per disciplinare questa situazione giuridica.

È il caso - ma solo perché è l'esempio più conosciuto - del Regolamento UE 679/2016 (altrimenti noto come "GDPR") e in particolare nei rapporti che possono instaurarsi tra titolare, responsabile e sub-responsabile del trattamento.

9. STANDARD E FRAMEWORK INTERNAZIONALI

Occorre rilevare come i principali framework di riferimento in ambito cybersecurity dedichino specifiche categorie di controllo sulla supply chain.

9.1 Standard ISO

L'Organizzazione internazionale per la standardizzazione attraverso i propri standard ha trattato in molteplici occasioni il tema della supply chain, sia normandola all'interno di sistemi di gestione aventi finalità specifiche differenti (ad esempio qualità, protezione dei dati personali, continuità operativa, erogazione dei servizi ICT) sia, vista la criticità del tema, producendo standard ad hoc.

ISO 28001:2020 Sistemi di gestione per la sicurezza della catena logistica - Migliori pratiche per l'attuazione della sicurezza della catena logistica, valutazioni e pianificazioni - Requisiti e linee guida
L'obiettivo di questo standard è quello di stabilire e documentare un livello minimo di sicurezza all'interno della supply chain o di suoi segmenti. Lo scopo è quello di permettere alle organizzazioni che vi fanno ricorso di soddisfare i criteri degli operatori economici autorizzati (AEO), che sono stabiliti nel Framework of standards dell'Organizzazione Mondiale delle Dogane, e di conformarsi ai programmi nazionali di sicurezza della supply chain.
Le organizzazioni possono così:

- definire il settore di una supply chain internazionale all'interno della quale desiderano assicurare la sicurezza, rispettandone la conformità normativa;
- eseguire valutazioni di sicurezza su quel settore della supply chain e sviluppare adeguate contromisure;
- sviluppare e attuare un piano di sicurezza della supply chain ;
- formare il personale addetto alla sicurezza nei suoi compiti attinenti la sicurezza.

L'organizzazione deve adottare un processo che consenta, periodicamente, l'identificazione delle aree di rischio e dell opportune azioni di mitigazione, minimizzando così probabilità e impatto, fornisca uno schema di risposta tempestiva degli eventi,

definendo procedure di segnalazione, di comunicazione e di formalizzazione di piani e di strategie per il ripristino.

UNI EN ISO 9001:2015 Sistemi di gestione per la qualità - Requisiti
"La qualità", come è comunemente soprannominato questo standard, è il sistema di gestione largamente più diffuso in Italia. La norma specifica i requisiti che un'organizzazione dovrebbe adottare per fornire con regolarità prodotti o servizi in linea con le richieste del cliente, accrescendone il livello di soddisfazione.

La ISO 9001 dedica una corposa sezione al controllo dei fornitori. Inoltre, anche se non con un focus specifico, indica gli elementi necessari per la gestione del rischio della supply chain, come si evince al punto 8.4.2: "*L'organizzazione deve assicurare che i processi, prodotti e servizi forniti dall'esterno non influenzino negativamente la capacità dell'organizzazione di rilasciare con regolarità, ai propri clienti, prodotti e servizi conformi… L'organizzazione deve: … c) tenere in considerazione: 1) l'impatto potenziale dei processi, prodotti e servizi forniti dall'esterno sulla capacità dell'organizzazione di soddisfare con regolarità i requisiti del cliente e quelli cogenti applicabili; 2) l'efficacia dei controlli attuati dal fornitore esterno;*"

ISO/IEC 27001:2022 Tecnologie Informatiche - Tecniche di sicurezza - Sistemi di gestione della sicurezza dell'informazione - Requisiti

Lo standard specifica i requisiti di un sistema di gestione della sicurezza delle informazioni e include i requisiti per la valutazione e il trattamento dei rischi per la sicurezza delle informazioni.

La ISO/IEC 27002:2022, che riporta i controlli di sicurezza, si preoccupa significativamente del ruolo delle terze parti e vi dedica ampio spazio, in particolar modo a:

- selezione del fornitore secondo un processo controllato, in funzione di specifici requisiti;
- contrattualizzazione di accordi in grado di assicurare la sicurezza del patrimonio informativo e degli asset correlati; tali requisiti devono essere applicati anche ai sub-fornitori;
- audit e monitoraggio periodico;
- regole di change management (ad esempio valutazione dei rischi connessi alla sostituzione di un fornitore, ecc.) per la gestione dei cambiamenti nei rapporti di fornitura.

ISO/IEC 27017:2021 Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services

La norma ISO/IEC 27002 viene integrata da questa linea guida dedicata alla sicurezza delle informazioni nell'erogazione e utilizzo di servizi cloud.

ISO 22301:2019 Sicurezza e resilienza - Sistemi di gestione per la continuità operativa - Requisiti
La norma specifica i requisiti di un sistema di gestione per la continuità operativa, per cui l'identificazione e l'analisi dei fornitori critici per l'erogazione dei processi e dei servizi critici è parte integrante delle attività di business impact assessment svolte dall'organizzazione.

ISO/IEC 20000-1:2018 Tecnologie informatiche - Gestione del servizio - Parte 1: Requisiti per un sistema di gestione del servizio
La norma specifica i requisiti di un sistema di gestione dei servizi ICT. Ciò implica:

- la definizione di regole per la valutazione e la selezione dei fornitori che concorrono all'erogazione dei servizi ICT dell'organizzazione;
- la mappatura dei processi, dei servizi o delle componenti di servizio erogati o gestiti da soggetti terzi;
- la definizione di procedure per la gestione dei rapporti di fornitura, tra cui:
    - designazione di ruoli e responsabilità interne per la gestione dei rapporti, dei contratti e delle performance dei fornitori;
    - sottoscrizione di accordi contenenti clausole in tema di qualità dei servizi ICT (ad esempio requisiti che il fornitore deve rispettare, obiettivi e obblighi contrattuali);
    - definizione di accordi contrattuali tra il fornitore ed eventuali sub-fornitori;
    - monitoraggio delle performance dei fornitori coerentemente con gli SLA sottoscritti, identificando eventuali azioni correttive;
    - riesame periodico dei contratti con i fornitori in funzione dell'evoluzione dei requisiti di qualità dei servizi ICT erogati dall'organizzazione.

ISO/TS 22318:2022 Sicurezza della società - Sistemi di gestione per la continuità operativa - Linee guida per la continuità della supply chain
Lo standard include 3 appendici con esempi pratici:

- Appendice A - Esempio di domande generali da inviare ai fornitori strategici;
- Appendice B - Gestione delle interruzioni dei fornitori strategici;
- Appendice C - Esempi di esercitazioni congiunte con i fornitori.

Il fine è quello di incoraggiare l'apertura tra l'organizzazione e i propri fornitori critici, fornendo una migliore comprensione delle priorità e dei rischi reciproci e una pianificazione integrata della continuità, in un'ottica di miglioramento continuo e di riduzione del rischio.
Particolare attenzione è posta sia agli attori a monte (upstream) sia su quelli a valle (downstream) della supply chain, considerando non solo l'analisi del primo livello (Tier 1), ma anche di tutti gli altri livelli (Tier 2 e successivi).

9.2 NIST 800-161

Il Framework NIST 800-161 descrive le regole per l'implementazione di un cybersecurity supply chain risk management (di seguito C-SCRM), definito come un processo sistematico per la gestione dei cyber-rischi lungo tutta la supply chain e lo sviluppo di strategie, politiche, processi e procedure di risposta appropriati.

Il C-SCRM è basato su una serie di principi chiave:

- riservatezza, integrità e disponibilità delle informazioni trattate dalla supply chain (ad esempio sicurezza delle informazioni e dei dati personali);
- resilienza della supply chain anche in condizioni critiche;
- affidabilità dei prodotti e dei servizi che devono funzionare come definito per un determinato periodo di tempo e in modo prevedibile;
- sicurezza delle forniture che devono evitare di causare morte, lesioni, malattie professionali, danni o perdita di attrezzature o proprietà o danni all'ambiente;
- garantire che i prodotti e servizi siano autentici, inalterati e che funzionino secondo le specifiche e senza funzionalità indesiderate;
- rispetto delle specifiche prestazionali, tecniche e funzionali, garantendo l'attenuazione delle vulnerabilità che possono limitare la fornitura di un servizio, portare al guasto di un componente e essere sfruttate da potenziali attaccanti.

L'adozione di un C-SCRM richiede:

- mappatura dei rischi e valutazione dei rischi;
- identificazione di misure di mitigazione (controlli proposti da NIST 800-161);
- monitoraggio dei rischi e dell'efficacia delle misure di mitigazione dei rischi.

In fase di acquisizione dei fornitori sono importanti le politiche, le strategie e un inventario puntuale dei fornitori, delle forniture e dei contratti in essere. La mappatura consente di classificare i fornitori in categorie (ad esempio strategici innovativi,

di supporto, non essenziali, critici) per facilitare le analisi.

- Le condizioni contrattuali verso il fornitore devono includere:
- soddisfazione dei requisiti di sicurezza applicabili;
- requisiti di controllo dei subappaltatori;
- obiettivi di performance e piano di sorveglianza;
- validazione periodica della conformità del fornitore ai requisiti di sicurezza;
- comunicazione di vulnerabilità, incidenti e altre interruzioni dei servizi.

Il sistema funziona correttamente se sono presenti adeguati flussi informativi, se le persone sono opportunamente sensibilizzate e formate, se la direzione mette a disposizione le risorse necessarie per il corretto funzionamento del sistema stesso.

Insieme, SP 800-53 e SP 800-161 presentano un quadro completo per identificare valutare, trattare e monitorare i rischi della supply chain ICT. I controlli sono articolati come nella figura seguente.

Figura 28 – I controlli proposti da NIST 800-161[155]

155 Immagine autoprodotta.

9.3 NIST CSF

Il NIST Cybersecurity Framework v.1.1 riporta controlli specifici per i rischi di cybersecurity, come illustrato nella figura seguente.

Category	Subcategory
Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-1**: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders
	ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process
	ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.
	ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
	ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers

Figura 29 – Controlli specifici relativi alla supply chain riportati dal NIST Cybersecurity Framework v.1.1[156]

9.4 CIS CSC

Il CIS CSC (Center for Internet Security Critical Security Controls), sviluppato nel 2008 a seguito di una perdita di dati in una base industriale della difesa degli Stati Uniti, è un framework largamente riconosciuto.

Consiste in 18 categorie di controlli di sicurezza a loro volta composte da 153 controlli, riferiti con il termine "Salvaguardie".

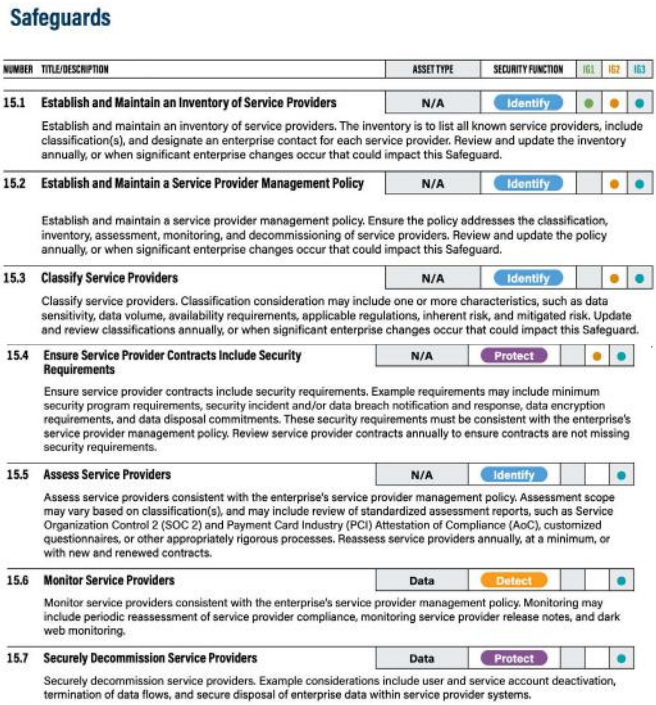
- Il CIS CSC è suddiviso in tre macrocategorie, denominate Implementation

156 https://www.nist.gov/cyberframework.

Group:

- I primi 56 controlli sono quelli fondamentali: fanno parte dell'Implementation Group 1 e sono definiti anche come "Basic Cybersecurity Hygiene";
- Altri 74 controlli di sicurezza da adottare in modo incrementale rispetto ai precedenti consentono alle organizzazioni la gestione di profili di rischio diversificati cosi' da affrontare in modo strutturato situazioni in cui la complessità tecnologica diventa rilevante;
- Infine, l'adozione di ulteriori 23 controlli consente l'adeguata protezione di informazioni caratterizzate da un elevato livello di sensibilità, oltre a poter rispondere in modo efficace ad attacchi informatici di natura sofisticata riducendone gli impatti.

I controlli del CIS CSC v.8 relativi alla tematica della supply chain sono riportati nella tabella seguente.



Safeguards

NUMBER	TITLE/DESCRIPTION	ASSET TYPE	SECURITY FUNCTION	IG1	IG2	IG3
15.1	**Establish and Maintain an Inventory of Service Providers** Establish and maintain an inventory of service providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Identify	●	●	●
15.2	**Establish and Maintain a Service Provider Management Policy** Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Identify		●	●
15.3	**Classify Service Providers** Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.	N/A	Identify		●	●
15.4	**Ensure Service Provider Contracts Include Security Requirements** Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. These security requirements must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.	N/A	Protect		●	●
15.5	**Assess Service Providers** Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Reassess service providers annually, at a minimum, or with new and renewed contracts.	N/A	Identify			●
15.6	**Monitor Service Providers** Monitor service providers consistent with the enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.	Data	Detect			●
15.7	**Securely Decommission Service Providers** Securely decommission service providers. Example considerations include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.	Data	Protect			●

Figura 30 – Controlli specifici relativi alla supply chain del CIS Critical Security Controls v.8[157]

157 https://www.cisecurity.org/controls/v8

9.5 COBIT

Un altro framework largamente riconosciuto in ambito IT è il COBIT (Control Objectives for Information and related Technology)[158] , creato nel 1996 da ISACA (Information Systems Audit and Control Association) e ITGI (IT Governance Institute), attualmente giunto alla versione COBIT 2019.

La documentazione disponibile per la precedente versione 5[159] è utilizzabile anche per l'attuale. Sono disponibili anche guide complementari per l'audit a terze parti e la "Vendor Management: Using COBIT 5".

I controlli specifici, ognuno declinabile in attività, per la supply chain sono:

- APO10.01 Identify and evaluate vendor relationships and contracts;
- APO10.02 Select vendors;
- APO10.03 Manage vendor relationships and contracts;
- APO10.04 Manage vendor risk;
- APO10.05 Monitor vendor performance and compliance.

158 https://www.isaca.org/resources/cobit.

159 https://www.researchgate.net/publication/281380010_The_effectiveness_of_COBIT_5_Information_Security_Framework_for_reducing_Cyber_Attacks_on_Supply_Chain_Management_System.

10. MISURE DI SICUREZZA COMUNI

A fronte di un'analisi del rischio relativa alla fornitura e dei requisiti di conformità, si identificano le misure di sicurezza da richiedere ai fornitori e nel tempo se ne valuta la corretta applicazione.

I momenti essenziali di questo processo sono tre:

- in fase di qualifica del nuovo fornitore;
- in fase di negoziazione (o rinnovo) contrattuale;
- a scadenze prefissate.

La periodicità delle scadenze (ad esempio ogni 12 mesi nello svolgimento di un contratto triennale) dovrebbe essere stabilita considerando i rischi della fornitura.

Tra le buone pratiche è opportuno segnalare le misure segnalate da ISACA[160] per migliorare il governo della supply chain:

- sviluppare e mantenere un inventario dei fornitori e delle capacità che ciascuno di essi fornisce;
- condurre un'analisi delle vulnerabilità delle terze parti considerate strategiche per l'organizzazione;
- creare un addendum contrattuale per misure tecniche e organizzative che hanno un impatto sulla supply chain;
- "trust but verify": condurre audit e riesami raccogliendo elementi di prova.

La valutazione del rischio, la richiesta di misure di sicurezza ai fornitori e la valutazione continua del loro operato sono processi molto onerosi dal punto di vista organizzativo per via della numerosità dei soggetti da coinvolgere e la distanza relativa delle organizzazioni.

Evidenziamo due aspetti molto rilevanti a favore di una relazione positiva tra il cliente e il fornitore a vantaggio di tutti:

- le misure di sicurezza richieste devono essere proporzionate e, soprattutto, relative al servizio / prodotto che ci si procura. Per fare un esempio estremo ma chiaro: è ridicolo chiedere al fornitore come gestisce il logging delle operazioni dei suoi amministratori di sistema se l'acquisto riguarda un software

160 "ISACA – Supply Chain Security Gaps: A 2022 Global Research Report".

in licenza d'uso (mentre non lo è affatto se si acquista un servizio SaaS in cloud);

- si deve cercare di utilizzare fonti autorevoli e best practice internazionali per la definizione e la richiesta di controlli.

In attesa dell'affermazione di uno standard utile, ampio, flessibile e dettagliato al giusto livello, abbiamo visto proliferare in questi anni decine di checklist variamente derivate da best practice differenti e liberamente adattate dalle aziende. La terminologia utilizzata a volte è scarsa e complica ulteriormente la difficoltà gestionale lato fornitore che si trova ad interagire con una molteplicità di diversi clienti con molteplici check list tutte diverse le une dalle altre.

10.1 Misure tecniche e organizzative

Premesso quanto precede e avvisando il lettore di non usare quanto segue come un'ulteriore nuova check list (ma meglio riferirsi alle best practice illustrate nel capitolo precedente), riportiamo di seguito alcune considerazioni in merito a diverse misure di tipo tecnico e organizzativo da considerare[161]. Il nostro scopo è quello di far comprendere a chi non voglia approfondire in questo momento di cosa si stia parlando. Si segnalano quindi le seguenti misure:

- Business continuity: è importante che il fornitore garantisca la continuità del servizio anche in caso di incidenti o situazione di crisi (ad esempio per indisponibilità di un sub-fornitore o indisponibilità di personale).
- Disaster recovery: nel caso in cui l'oggetto del contratto sia un sistema informatico, è fondamentale che il fornitore garantisca RTO (recovery time objective) e RPO (recovery point objective) in linea con le esigenze del cliente.
- Restituzione e cancellazione dei dati: è buona norma, a meno di vincoli normativi, che alla fine del contratto il fornitore restituisca al cliente tutti i dati trattati fino a quel momento e che ne dimostri poi la cancellazione dai propri sistemi (incluse eventuali copie di backup eseguite nel tempo).
- Controllo accessi: misure di segregazione tra i sistemi e servizi dei diversi clienti.
- Cifratura dei dati: la cifratura dei dati è importante per ridurre l'accesso indesiderato agli stessi; è altresì importante avere la possibilità, se lo si desidera, di gestire internamente le chiavi di cifratura.
- Formazione del personale: il fornitore si deve avvalere di manodopera qualifi-

161 Nel GDPR, per proteggere i dati personali, si prevede la necessità di "misure" tecniche e organizzative, mentre la ISO/IEC 27002:2022 categorizza i "controlli" in 4 temi: people, physical, technological e organizational. Oltre che la diversa tassonomia, si noti anche l'uso delle due diverse parole.

cata e formata.

- Segregazione dei compiti: le diverse fasi dei processi più critici devono essere assegnate a persone diverse.
- Privilegio minimo ("need to do", "need to know"): le autorizzazioni concesse alle persone devono essere ridotte il più possibile.
- Gestione dei log: i log con valore di prova devono essere inalterabili e il tempo di conservazione (retention) deve essere adeguato.
- Backup dei dati: i dati (incluso il software, le configurazioni ecc.) devono essere automaticamente salvati in copie periodiche, locali e remote e il sistema deve essere protetto e sicuro, monitorato e regolarmente testato.
- Sviluppo sicuro e accesso al codice sorgente: il fornitore deve adottare tecniche di sviluppo sicuro. In certi casi il cliente deve poter accedere al codice sorgente.
- Cifratura selettiva e/o separazione logica o fisica degli ambienti destinati a clienti diversi per evitare accessi abusivi o errori che causino la commistione di dati tra "tenant" diversi e per garantire che i dati non possano essere utilizzati per finalità diverse da quelle previste dal rapporto di fornitura, venduti o ceduti.
- Verifica e risoluzione di vulnerabilità: il fornitore deve eseguire verifiche ricorrenti in merito alla presenza di vulnerabilità e provvedere alla loro soluzione in tempi brevi.

Altre misure e controlli da svolgere riguardano:

- La presenza di un processo di gestione del rischio relativo alla sicurezza delle informazioni.
- La presenza e l'implementazione di policy e procedure in ambito sicurezza delle informazioni, tra le quali quelle per la gestione degli incidenti, la gestione delle vulnerabilità e la gestione dei cambiamenti e la comunicazione ai clienti;
- La definizione dei ruoli e responsabilità;
    - il cliente dovrebbe stabilire chiaramente le responsabilità interne (acquisti, CISO, ICT, business, HR, ecc.), anche con una procedura acquisti che preveda l'indicazione dei ruoli di coordinamento e dei criteri da adottare per affrontare i rischi di fornitura;
    - il fornitore dovrebbe indicare chi è il suo riferimento per tematiche di sicurezza informatica a cui rivolgersi in caso di necessità.

- La presenza di programmi di formazione e sensibilizzazione del personale (inclusi collaboratori ed eventuali sub-fornitori) in ambito sicurezza delle informazioni.
- La capacità di estendere ai subfornitori quanto stabilito negli accordi contrattuali.
- Il possesso di certificazioni di sicurezza come ad esempio la ISO/IEC 27001 e le altre elencate nel seguito.
- La diversificazione dei fornitori, soprattutto per i servizi critici, individuando più fornitori, intercambiabili e facilmente sostituibili. In tal senso potrebbe anche essere utile ragionare su strategie di reshoring (riavvicinamento delle fonti di approvvigionamento), internalizzazione, mitigazione o altre strategie volte a minimizzare le potenziali ricadute sull'organizzazione.
- Adottare un processo di acquisto che veda coinvolte tutte le funzioni dell'organizzazione interessate per la scelta dei fornitori e l'identificazione delle specifiche dei prodotti e servizi richiesti.

Visto che il cliente e il fornitore sono persone giuridiche differenti, è evidente che la relazione tra cliente e fornitore dovrebbe essere formale e basata su evidenze contrattuali e documentali. Quindi, quando si negozia e ci si accorda su un certo insieme di misure di sicurezza, bisogna produrre e acquisire la documentazione relativa. La valutazione di un fornitore deve anche tenere in conto della sua capacità di dar prova del modo in cui svolge le attività richieste.

10.2 Certificazioni e attestazioni di sicurezza

La complessità di quanto detto sopra trova una parziale soluzione nelle certificazioni e attestazioni di sicurezza. In loro presenza, per i clienti è più facile ridurre e selezionare i controlli da fare e per i fornitori dare prova della loro capacità di gestire il rischio.

Le attestazioni di terze parti autorevoli irrobustiscono la fiducia nelle procedure di un'organizzazione e hanno anche un ruolo importante per le organizzazioni quando devono decidere a quali fornitori rivolgersi.

È importante prestare attenzione alle *certificazioni accreditate*, per cui gli *enti di accreditamento* riconosciuti verificano che gli enti di certificazione adottino adeguati processi di verifica, che garantiscono, tra l'altro, che i controlli siano in qualche modo

omogenei in ugual misura per ogni Paese e per ogni organizzazione certificata.

È buona norma verificare il certificato e in particolare i seguenti punti:

- l'ambito della certificazione deve essere pertinente con il servizio o il sistema che il fornitore eroga all'organizzazione;
- la certificazione deve essere attiva e il fornitore deve impegnarsi contrattualmente a mantenerla attiva durante tutta la durata del contratto.

Vi è una continua evoluzione delle certificazioni, attestazioni e standard di conformità. Di seguito viene riportato una lista di quelli, ad oggi, maggiormente richiesti:

- Certificazioni Globali
    - ISO 9001: Quality Management Systems
    - ISO/IEC 20000-1: Service Management Systems
    - ISO/IEC 22301: Business Continuity Management
    - ISO/IEC 27001: Information Security Management Systems
    - ISO/IEC 27701: Privacy Information Management
    - SOC 1, 2 e 3: System and Organization Controls 1, 2 e 3
- Certificazioni specifiche per specifici settori
    - PCI-DSS: Payment Card Industry Data Security Standard (per il settore finanziario)
    - TISAX: Trusted Information Security Assessment Exchange (per il settore automobilistico)
- Certificazioni specifiche e codici di condotta per l'erogazione di servizi cloud:
    - ISO/IEC 27017: Cloud Specific Controls
    - ISO/IEC 27018: Personal Information Protection Controls
    - EU Cloud CoC: European Union (EU) Cloud Code of Conduct
    - Cloud Infrastructure Services Providers in Europe (CISPE) Code of Conduct
- Certificazioni in contesto US:
    - DoD DISA SRG: Department of Defense, Defense Information Systems Agency, Systems Requirement Guide
    - FedRAMP: Federal Risk and Authorization Management Program
    - FIPS 140: Federal Information Processing Standards Publication 140
    - HITRUST CSF: Health Information Trust Alliance Common Security

Framework

- HIPAA: Health Insurance Portability and Accountability Act
- NIST SP 800-171: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

Le autocertificazioni invece partono dal presupposto che non esista una terza parte che certifichi l'organizzazione, il servizio o il prodotto, ma che sia l'organizzazione stessa ad effettuare un'autovalutazione. Un esempio è la CSA (Cloud Security Alliance) STAR (Security, Trust, Assurance and Risk) livello 1 che è una semplice autocertificazione a differenza di quella di livello 2 che prevede invece un controllo di terze parti.

11. I CONTRATTI

Da circa 30 anni a questa parte stiamo progressivamente facendo i conti con l'effetto rivoluzionario della trasformazione digitale, il cui successo poggia principalmente sulla pervasività della rete e il crescente uso del web da parte delle organizzazioni, anche grazie ad un accesso sempre più semplificato ed economico alle risorse informatiche.

In questo contesto di profondo cambiamento, il contratto, tradizionalmente inteso come lo strumento giuridico in cui far convergere domanda e offerta delle parti, si è ineluttabilmente trasformato: le organizzazioni infatti sono chiamate a rapportarsi al mercato con una pressione in termini di competitività senza paragoni, con il venire meno dei limiti della territorialità e della presenza fisica oggi superati dalla dimensione liquida della rete. Tali mutamenti hanno cambiato anche gli "equilibri" dei contratti.

Secondo questi nuovi paradigmi, dettati dalla straordinaria accelerazione tecnologica, anche le relazioni commerciali hanno subito una metamorfosi radicale, talvolta svuotando di senso alcuni dei principi chiave del nostro ordinamento civilistico, come, ad esempio, quello dell'equità, il quale ha da sempre avuto come obiettivo l'equilibrio di potere tra le parti contraenti.

È noto che l'equità sia concetto ontologicamente connesso a quello di giustizia contrattuale, posto che l'esigenza primaria - tutelata tradizionalmente dal sistema più o meno in ogni parte del mondo, pur con differenti approcci - è quella di evitare la sproporzione tra prestazione e controprestazione e squilibri tra le forze contrattuali delle parti. L'intera disciplina contrattualistica ha, da sempre, come obiettivo, quello di preservare l'equità dei rapporti contrattuali e, dunque, garantire la proporzionalità tra le prestazioni, non solo dal punto di vista del loro valore economico ma anche per quel che riguarda l'assegnazione dei rispettivi diritti e doveri, obblighi, oneri e rischi tra le parti.

Ma se solo pensiamo al gigantismo giocato dalle Big Tech nei confronti della propria utenza, capiamo subito che la rivoluzione digitale ha pressoché sovvertito queste logiche tradizionali: le condizioni contrattuali imposte dalle *Over the top*, prevedono infatti esenzioni di responsabilità di ogni tipo, tetti risarcitori, limiti di utilizzo, nonché oneri di vario genere a carico del cliente.

Ugualmente, i rimedi giuridici volti a tutelare il principio della proporzionalità quali quello della rescissione o della risoluzione (art. 1447-1448-1453 c.c.), sono divenuti in certi contesti non esperibili: nella realtà concreta infatti, pur dando atto della sussistenza di condizioni inique, pericoli o disservizi, il mercato non offre alternative a questo o a quel provider (ad esempio la casella mail di Google, la messaggistica di WhatsApp, la presenza e lo scambio sui social). Ciò obbliga l'utente ad accettare un contratto in cui è "parte debole", pagando, spesso, per la prestazione ricevuta non solo attraverso un corrispettivo in denaro ma anche (o esclusivamente) con la cessione più o meno consapevole dei propri dati generati sulla rete.

Con l'avvento della digital economy, infatti, l'incontro tra domanda e offerta si perfeziona sempre più frequentemente "per adesione": la fase preparatoria della trattativa, degli accordi precontrattuali, la discussione e il confronto sugli obiettivi dell'accordo (in buona sostanza la fase dei preamboli negoziali) è stata via via soppiantata da stipule istantanee, velocissime, fatte sul modello *pay per click* e sulle logiche del as it is, ossia sull'accettazione di condizioni e clausole prestabilite dal fornitore e messe in vetrina sulla rete da sottoscrivere "così come sono" con ben poche (se non nulle) possibilità di modifica o margini di trattativa.

Anche nel settore della supply chain, la crescente capacità del digitale di mettere in connessione informazioni, luoghi e persone attraverso dispositivi intelligenti, come sensori, telecamere, robot, cobot e chatbot, ha parallelamente disegnato innovative geometrie di mercato e generato forti pressioni in termini di concorrenza, ma ha anche reso disponibile un'incalcolabile flusso di dati indispensabili per automatizzare e ottimizzare moltissimi processi produttivi a vantaggio degli operatori del settore. Il ricorso massivo al cloud computing tipico di questi anni, l'impiego della blockchain e dell'IA hanno ulteriormente interessato questo comparto: basti pensare all'impatto dell'IA sui processi decisionali, sulla formazione e la collaborazione dei dipendenti, sull'analisi dei flussi della merce e del suo tracciamento o alla certificazione delle materie prime e dei processi di lavorazione delle stesse.

In questo contesto di epocale cambiamento, lo strumento del contratto nella filiera della supply chain merita di essere analizzato sia dal punto di vista formale (le innovative formule di incontro tra domanda e offerta abilitate dalle piattaforme di nuova generazione), sia dal punto di vista sostanziale (la gestione automatizzata del rapporto contrattuale con il cliente dall'onboarding, alle possibili situazioni di patologia del contratto, fino alla cessazione del rapporto), insieme a tutti i conseguenti rischi legati alla sicurezza informatica, che vanno necessariamente identificati, compresi e governati.

11.1 Strumenti contrattuali di tutela

In linea generale la relazione committente-fornitore comporta, in capo al primo, obblighi di vigilanza e controllo sull'operato del secondo, tali da giustificare costantemente (per tutta la vigenza del rapporto) la scelta della nomina effettuata. E ciò al fine di evitare che possano sorgere in capo al committente responsabilità collegate alla cosiddetta "*culpa in eligendo e culpa in vigilando*".

Attualmente però, proprio in ragione dello sviluppo della tecnologica sopra illustrata e dei conseguenti mutamenti negli equilibri contrattuali, l'indipendenza e l'autonomia del fornitore nello svolgere i compiti e le attività oggetto del contratto con il committente, rendono spesso difficile la parificazione del sinallagma[162] contrattuale, creando situazioni di asimmetria che possono comportare un reale ed reale ed importante squilibrio tra le parti.

Per tali ragioni, ove possibile, è sempre opportuno intervenire contrattualmente, mediante la sottoscrizione di specifiche clausole che possano bilanciare la relazione tra le parti.

In particolare tra gli strumenti contrattuali di tutela da tenere in considerazione possono essere annoverate, a titolo esemplificativo e non esaustivo, le seguenti clausole:

- **Controllo delle modifiche al servizio**: i fornitori si riservano generalmente il diritto di introdurre modifiche unilaterali, ossia non subordinate al consenso dell'utenza e a prescindere da eventuali problemi, disfunzioni o difficoltà causate all'utenza stessa. Quest'ultima dovrebbe però avere diritto a un servizio di assistenza specifico, possibilmente non a pagamento, per passare - nel caso - a una tecnologia alternativa.
- **Penale contrattuale**: tale clausola non ha natura punitiva o sanzionatoria, bensì è anticipatoria di tutela, assolvendo alla funzione di rafforzare il vincolo contrattuale, stabilendo in via preventiva il quantum del risarcimento della parte inadempiente. Più precisamente attraverso tale clausola può essere stabilito che, qualora si verifichino inadempienze alle obbligazioni contrattuali o ritardi nell'esecuzione delle stesse, il contraente inadempiente dovrà corrispondere all'altro una somma di denaro predeterminata, senza alcuna necessità di attivare azioni giudiziarie. Attenzione, però, a determinare equamente l'importo posto a penale: alternativamente, nei casi di abuso o

162 Più comunemente definibile "rapporto" o "relazione" tra le parti, giuridicamente individua il nesso di reciprocità che lega le prestazioni corrispettive tra le parti all'interno di un vincolo contrattuale (o, in altri termini, la "posizione" giuridica delle parti all'interno del contratto).

sconfinamento dell'autonomia negoziale privata, la stessa potrà essere riparametrata secondo il discrezionale apprezzamento del giudice eventualmente adito.

- **Recesso unilaterale e risoluzione contrattuale**: anche tali due clausole assolvono alla funzione di riequilibrare il sinallagma contrattuale tra cliente e fornitore. Con il recesso unilaterale, infatti, si prevede espressamente la possibilità per una delle parti (in questo caso il cliente) di "svincolarsi" dalle obbligazioni assunte unilateralmente: tale istituto si rivela importante soprattutto nei contratti a prestazioni corrispettive e periodiche. Qualora, ad esempio, la struttura organizzativa del fornitore o l'esecuzione delle attività poste a contratto non garantiscano più il vincolo iniziale, il cliente potrà recedere unilateralmente dal contratto. La risoluzione contrattuale, invece, presuppone l'inadempimento contrattuale di una delle parti (nel nostro caso, del fornitore) o circostanze tali da far divenire la prestazione contrattuale eccessivamente onerosa o impossibile da realizzare. In tali casi, salvo ogni opportuna valutazione in merito al risarcimento del danno, il cliente potrà risolvere il vincolo sinallagmatico instaurato con il fornitore.
- **Accordo di riservatezza**: si tratta della clausola che riguarda segreti industriali del cliente e del fornitore. Occorre prestare attenzione alla circostanza che i dati e le informazioni che si possono qualificare oggi come segreti industriali sono quelli che rispondono ai requisiti dell'art. 98 del Codice della Proprietà industriale.
- **Accordo sul trattamento dei dati personali**: per garantire l'aderenza alle normative sulla protezione dei dati personali. Molto importante che tale clausola definisca con chiarezza i ruoli privacy di committente e fornitore, tenuto conto in particolare che l'art. 82 del GDPR stabilisce oggi la responsabilità solidale del Titolare e del Responsabile ex art. 28.
- **Assicurazione**: in ottica di mitigazione e trasferimento del rischio e di equilibrio contrattuale tra le parti, può essere utile inserire una specifica clausola che obblighi il fornitore alla stipula di una polizza assicurativa dedicata alla copertura del cyber-rischio. In tal senso, il cliente riceverà maggiori garanzie di affidabilità da parte del fornitore, il quale si impegna a tenere indenne il cliente da eventuali pretese risarcitorie che possono essere liquidate dalla compagnia designata. Sul punto sarà importante verificare il testo della copertura assicurativa stipulata, prestando attenzione soprattutto a massimali, franchigie, scoperti ed esclusioni di garanzie.
- **Subfornitori**: per un maggior controllo della supply chain, è opportuno che il cliente obblighi contrattualmente il fornitore a vigilare sui fornitori scelti

da quest'ultimo. In tal senso, oltre a definire direttamente a contratto la lista dei sub-fornitori nominati dal fornitore, quest'ultimo dovrà impegnarsi a far rispettare agli stessi le medesime previsioni contrattuali siglate con il cliente.

- **Audit di seconda parte**: tale clausola riveste particolare importanza, poiché consente al cliente di vigilare concretamente sull'operato del fornitore. Con tale strumento, infatti, si prevede una sorta di "ispezione" periodica del cliente (solitamente semestrale o quantomeno annuale), il quale, determinate congiuntamente le tempistiche e modalità di esecuzione, effettua un vero e proprio audit sulle attività e sull'organizzazione del fornitore. Si dovrebbe anche richiedere l'impegno esplicito da parte del fornitore a eseguire eventuali piani di rientro delle carenze segnalate. Appare inoltre opportuno - nell'ipotesi di forniture critiche - inserire la possibilità di audit a sorpresa, allo scopo di verificare in maniera molto più incisiva l'aderenza del fornitore agli obblighi contrattuali, regolatori o legislativi ai quali è tenuto.
- **Legislazione applicabile**: ai contratti stipulati in Italia trova applicazione la legge italiana. Ove invece il contratto sia stabilito con un soggetto che ha sede fuori dal nostro territorio (i c.d. contratti internazionali) è possibile per la parti scegliere la normativa applicabile: tale scelta può essere molto rilevante in caso di conflitto tra i contraenti.
- **Foro competente**: clausola di "chiusura", poiché solitamente posta al termine del contratto tra le parti. Mediante tale clausola, in deroga a quanto normativamente previsto, le parti hanno facoltà di determinare il giudice adito a dirimere giudizialmente l'eventuale insorgenza di controversie tra loro. In tal senso, il cliente potrà scegliere un foro più conveniente per la trattazione e risoluzione di eventuali liti con il fornitore, vuoi per convenienza di luogo geografico, vuoi per giurisdizione o competenza di un determinato ufficio.

Ove poi lo squilibrio di forza tra le parti non consenta modifiche contrattuali, è sempre opportuno prestare attenzione alle clausole di cui sopra per avere anche solo consapevolezza dei contenuti delle stesse e gestire al meglio le situazioni di debolezza del contratto.

11.2 Clausole contrattuali tecniche

I contratti stipulati con terze parti sono fondamentali per obbligarle a garantire un adeguato livello di sicurezza informatica rispetto agli standard adottati dal cliente. Ciò in particolare, laddove il servizio erogato dal fornitore o dall'appaltatore prevede anche il trattamento di dati personali, i livelli di sicurezza minima sono definiti dal

cliente stesso (eventualmente considerando quelli stabiliti a sua volta dal suo cliente). Alcuni dei temi più importanti che dovrebbero essere inseriti nella clausole contrattuali sono riportate nei capitoli precedenti.

12. VALUTAZIONE DEL RISCHIO FORNITORI

Il cliente non può attivamente operare all'interno della realtà del fornitore stesso. Tecnologie, infrastrutture, procedure, policy, tutto è di appannaggio del fornitore e, spesso, il cliente non ha modo nemmeno di verificare il livello di sicurezza adottato dal fornitore stesso su questi aspetti.

Tuttavia, come si è detto, il fornitore, nel momento in cui opera con un cliente, diventa una sua estensione e, conseguenza di questa estensione, sono anche tutte le minacce e gli attacchi che quest'ultimo potrebbe subire. Tali attacchi, pertanto, sarebbero subiti anche dal cliente in termini di compromissione di informazioni e servizi.

Diventa quindi essenziale valutare il livello di rischio o di esposizione alle minacce dei fornitori, al fine di poter avere la consapevolezza e la capacità di agire preventivamente a fronte di possibili attacchi.

12.1 Approcci di analisi

Al fine di effettuare una tale analisi possono essere perseguite diverse strade. Una di queste consiste nella raccolta delle informazioni relative ai sistemi, procedure e policy afferenti alla sicurezza, direttamente dal fornitore stesso. Spesso questo si traduce in interviste con le figure responsabili del fornitore in merito ai vari ambiti che possano impattare la sicurezza del cliente. Questo approccio può risultare molto completo, ma richiede un impegno importante di risorse e tempo sia da parte del fornitore che del cliente.

Un altro approccio è possibile attraverso l'esecuzione, da parte del cliente che effettua le verifiche, di attività tecnologiche e di intelligence per stimare un livello di sicurezza. Tali verifiche possono essere eseguite in modalità completamente "passiva" o, in alternativa, con la collaborazione da parte del fornitore. Queste attività possono evidenziare problemi di sicurezza come vulnerabilità presenti sui sistemi del fornitore esposte su Internet. Questo approccio è più economico del precedente per il fornitore, ma richiede comunque un certo impegno da parte del cliente per le analisi svolte direttamente o con l'ausilio di terze parti.

12.2 Complessità della supply chain ICT

Relativamente all'analisi del rischio, il punto focale consiste nell'**attribuzione delle responsabilità** per poter identificare prontamente e agire puntualmente ed efficacemente nel caso di mancanze o di criticità di sicurezza.
In una realtà complessa, varie responsabilità possono essere suddivise su vari ruoli. Questo comporta che un soggetto possa, o debba, essere insignito di diversi ruoli.

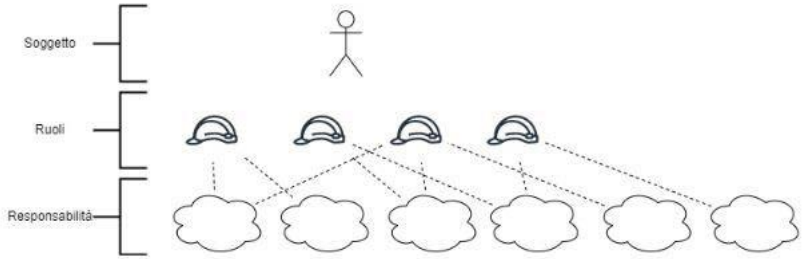


Figura 31 – Relazioni tra soggetti, ruoli e responsabilità[163]

Questa matrice di soggetti, ruoli e responsabilità diventa talvolta estremamente complessa.

Altro elemento di complessità è la **presenza di uno o più subfornitori** nell'ambito del rapporto di fornitura. Questo può causare in generale una aumentata esposizione a rischio tanto per il cliente, quanto per lo stesso fornitore.

Nell'ottica del primo, infatti, il rischio è che il ricorso alla subfornitura massiccia possa tradursi in una sostanziale elusione, da parte del fornitore, delle garanzie e delle responsabilità previste dal contratto, il quale, intercorrendo formalmente con una entità diversa da quella che sostanzialmente vi darà adempimento, rischia di svuotarsi di contenuto.

Dal punto di vista del fornitore, invece, il rischio insito nel ricorso alla subfornitura è quello di esporsi personalmente e direttamente verso il cliente, accollandosi la responsabilità del corretto adempimento e della dovuta diligenza da parte di un terzo.

La supply chain potrebbe essere costituita da un gran numero di **organizzazioni di piccola dimensione,** che collaborano in sistemi complessi e multilivello. Questo è particolarmente vero, per fare un esempio, nel settore manifatturiero, in cui si stima che il 95% del volume globale produttivo sia attribuibile a PMI. Nel mondo indu-

163 Immagine autoprodotta.

striale, a fronte di alcune grandi imprese che guidano l'intera produzione, la catena del valore vede un contributo importante di PMI a qualsiasi livello, e non solo nella fornitura, ma anche nella sotto-fornitura, con ecosistemi complessi, interconnessi e a più livelli.

Le PMI, solitamente, non hanno livelli di sicurezza comparabili a quelli delle grandi imprese committenti. Le dimensioni minori rendono problematica l'acquisizione di risorse e di competenze per far fronte a possibili attacchi e incidenti di cybersecurity. Essendo connesse, tra loro e con altre realtà, rappresentano una possibile "backdoor" per attaccanti interessati a prendere di mira organizzazioni di dimensione maggiore.

In aggiunta a questa complessità, va osservato che alcune PMI, pur avendo dimensioni ridotte, possono essere responsabili della gestione di grandi moli di dati, in proprio o per conto di loro clienti.

Il problema di garantire la sicurezza nelle PMI – prima che queste diventino la piattaforma ideale per la distribuzione di malware e cyberattacchi verso altri player – è quindi un tema di primaria importanza che deve essere affrontato sia da chi dipende da erze parti, sia anche dai regolatori. Si tratta infatti di un problema sistemico che va affrontato nel suo complesso più che con approcci puntuali.

A questo si aggiunge un ulteriore livello di complessità nel momento in cui vi è una **distribuzione su Paesi o continenti** differenti dei fornitori. In questi casi, infatti, bisogna anche tener conto delle implicazioni legali derivanti dalla sovrapposizione di diverse legislazioni e regolamentazioni.

Nel **caso dei software** va inoltre osservato che non sono quasi mai sviluppati da zero senza l'ausilio di librerie terze. Sono noti casi nei quali in tali librerie sono state identificate vulnerabilità, anche gravi (come i citati casi Heartbleed e Log4j). Sfruttando tali vulnerabilità, gli attaccanti sono stati in grado di compromettere in modo grave intere infrastrutture.

12.3 Valutare il rischio di fornitura

In generale, quando si parla di rischio si intende il prodotto tra la probabilità che un evento accada e la quantificazione del suo impatto nel caso in cui l'evento si realizzi.

Per la valutazione del rischio, si utilizzano i termini:

- **VRM** (vendor risk management) e SRM (supplier relationship management) per la gestione del rischio di fornitori;
- **TPRM** (third parties risk management) per la gestione del rischio di terze parti, che include i fornitori;
- **SCRM** (supply chain risk management), per la gestione del rischio della supply chain.

I programmi di VRM, SRM, TPRM e SCRM possono considerare rischi come quelli legati al tema della produzione etica e al consolidamento della spesa.

I programmi di VRM, SRM e TPRM si occupano del monitoraggio del rischio per l'intera durata del ciclo di vita della relazione. Nel caso esteso di TPRM, si deve però tener conto di una limitazione: mentre si possono selezionare i fornitori, non sempre è possibile scegliere tutte le altre terze parti (ad esempio, i clienti e gli organismi di regolamentazione).

L'SCRM si occupa di valutare l'intera supply chain e richiede una chiara comprensione dei partner da cui si sta acquistando materiali, manodopera e altri componenti.

Nel seguito si è scelto di usare il termine TPRM.

Il processo di gestione del rischio di fornitura dovrebbe prevedere procedure, responsabilità dichiarate, attività calendarizzate sia di esecuzione che di verifica. L'organizzazione dovrebbe verificare se il proprio TPRM è integrato con le proprie politiche di gestione del rischio.

La gestione del rischio inizia anche prima dell'inizio del rapporto. Ad esempio, un'organizzazione può valutare la concentrazione geografica dei fornitori per limitare i rischi conseguenti a un disastro naturale.

Sommariamente, le attività di gestione del rischio relativo alla supply chain sono riportate nei paragrafi successivi.

12.3.1 Organizzazione interna

Prima di procedere è doveroso definire le esigenze dell'organizzazione in termini chiari e inequivocabili.

La prima linea di difesa è lo staff interno all'organizzazione, il quale svolge un ruolo fondamentale nell'identificazione, valutazione, gestione e controllo dei rischi associati al fornitore, in quanto più vicini alle dinamiche operative e relazionali, all'insor-

gere di eventuali problemi e incidenti.

Il modello, così come necessita di una piena consapevolezza dal basso, parimenti ha bisogno di una governance forte e chiara da parte dell'alta direzione. Solitamente le funzioni dedicate all'applicazione del TPRM sono l'Ufficio conformità oppure, qualora non vi fosse, gli Acquisti. In qualsiasi caso, si necessita di una sinergia fra diverse aree quali Acquisti, Rischio, Legale, Compliance, ICT.

13.3.2 Mappare e classificare

Vanno individuati i diversi soggetti che compongono il contesto in cui opera l'organizzazione. Una criticità spesso difficile da superare è la **piena conoscenza di quanto la filiera sia ramificata e di quali rapporti di fornitura sussistano nelle singole ramificazioni**. Spesso un'organizzazione conosce il primo livello di fornitura, composto da quei soggetti terzi con i quali si ha un rapporto contrattuale in essere, ma raramente ha conoscenza di quali siano i subfornitori e gli ulteriori subfornitori.

Le attività di mappatura sono riportate nei paragrafi successivi.

12.3.2.1 Identificare le terze parti e i loro referenti all'interno dell'organizzazione

Le organizzazioni che non dispongono di un inventario e si stanno adoperando per predisporne uno, possono sfruttare i dati esistenti e distribuiti fra le diverse funzioni, che di volta in volta si sono attivate per l'individuazione del fornitore o che ne gestiscono i rapporti.

Un aiuto lo può fornire l'ufficio acquisti anche se spesso l'autonomia organizzativa di alcuni uffici, l'iniziativa di alcuni collaboratori o la contingenza di situazioni emergenziali potrebbe avere introdotto all'interno del perimetro organizzativo servizi non correttamente censiti, talvolta anche gratuiti o privi di una corretta contrattualizzazione.

Ulteriore supporto alla mappatura viene dall'analisi della spesa: estraendo i dati dal gestionale si ha evidenza dei fornitori verso cui si ha una maggiore esposizione finanziaria e quindi indirettamente una maggiore dipendenza. Dettagliato il primo livello di fornitura non resterà che approfondire quali sono i subfornitori da cui dipende il funzionamento critico del fornitore.

Le organizzazioni hanno già sovente delle mappature pensate per altri scopi (rispondere a requisiti dei sistemi di gestione, tra i più diffusi la ISO 9001) e queste potreb-

bero essere un primo punto di partenza. L'alberatura di un ERP di o di un gestionale potrebbe fornire spunti per iniziare a costruire la propria mappatura dei processi.

12.3.2.2 Classificare i fornitori

Non tutte le terze parti sono uguali. Per questo motivo le organizzazioni dovrebbero valutare le terze parti secondo criteri specifici, attraverso una descrizione dettagliata del servizio e una valutazione sulla sua criticità, la data di inizio del servizio, informazioni di costo, vincoli contrattuali in essere, referenti del fornitore, subfornitori (anche detti quarte parti) e un riepilogo dei principali rischi associati a ciascun fornitore.

In un secondo tempo si dovrebbe redigere una seconda classificazione, questa volta sul rischio intrinseco associato al singolo fornitore. Questo considerandone la solidità economico-finanziaria, le dimensioni, la presenza di strutture operative e di supporto adeguate, le referenze, la criticità di fornitura (quanto l'interruzione del servizio possa impattare sulla propria organizzazione e quanto velocemente possa essere rimpiazzato), la possibilità di sostituirlo, le condizioni socio-politiche delle zone geografiche in cui opera, se opera su processi critici dell'organizzazione, ecc.

Il risultato dell'analisi è un elenco dei fornitori e del loro livello di criticità, affinché l'organizzazione sia perfettamente consapevole dell'impatto che un fornitore può avere sulla propria operatività.

12.3.2.3 Aggiornamento in tempo reale dell'inventario

L'inventario deve essere costantemente aggiornato, accurato e completo.

12.3.3 Individuare i rischi

Esistono infatti diversi tipi di rischi: strategici, geopolitici, reputazionali, finanziari, digitali, operativi, normativi e di compliance, informatici e di privacy, di continuità operativa e resilienza, pandemici, sociali. Il livello di esposizione a questi rischi è ovviamente influenzato dall'estensione e dalla complessità della supply chain. Un'organizzazione, ad esempio, potrebbe ritenersi immune da rischi geopolitici e sociali, avendo le proprie attività prevalentemente all'interno di un contesto stabile quale è l'UE, ma indirettamente avere cali di prestazione dei propri servizi per difficoltà di un subfornitore, non correttamente mappato, nel garantire i livelli prestazionali minimi previsti, a seguito di tumulti socio-politici all'interno del Paese in cui è ubicato.

La valutazione del rischio di fornitura, quale metodologia utilizzare, su quale framework fare affidamento o quale strumento software acquistare sono spesso gli

elementi su cui si concentra l'attenzione dei più.

Una mappatura delle minacce o una sua elencazione come da tabella aiuterà il processo di classificazione poc'anzi menzionato.

Categorie	Minacce su cliente
Prodotti	Indisponibilità di materie prime, alterazioni o perdite di prodotti durante il trasporto (ad esempio per danneggiamento, contaminazione, furti), furto di proprietà intellettuale, ritardi (di produzione, sviluppo, aggiornamento), obsolescenza, esposizione a minacce digitali (ad esempio IoT).
Sistemi informatici	Interruzione nel corretto funzionamento di sistemi, servizi e reti, incompatibilità dei sistemi, vulnerabilità agli attacchi informatici, rischi associati ai sistemi di e-commerce, problemi ed errori nello scambio di informazioni relative a prodotti e servizi, violazioni di dati personali.
Logistica	Piattaforme di scambio dati per l'erogazione del servizio, interruzione della catena dei trasporti, complessità o lunghezza della catena dei trasporti, ritardi o danneggiamenti dei prodotti durante il trasporto.
Fattori economici e finanziari	Fragilità economica del fornitore (esposizione finanziaria, situazione debitoria, sanzioni, insolvenza), difficoltà di accesso al credito (ad esempio per la scalabilità del servizio), fluttuazione di prezzi o tassi, tasse e imposte impreviste.
Impianti produttivi o sviluppo	Malfunzionamenti dei sistemi, scioperi del personale, limiti di produzione o sviluppo, aumento del costo del lavoro, produzione non flessibile, instabilità dei processi, interruzione delle attività.
Processo di approvvigionamento	Interruzione delle attività, costi o tempi di sostituzione del fornitore eccessivi (vendor lock-in), incapacità di risposta dei fornitori al mutare di scenari o necessità.
Processo di produzione	Interruzione della fornitura (ad esempio a causa di eventi naturali, malfunzionamenti, attacchi informatici, attacchi terroristici, epidemie, interruzioni elettriche), capacità produttiva insufficiente.

Categorie	Minacce su fornitore
Socio – politiche	Governi instabili o potenzialmente instabili (ad esempio autoritari o repressivi), problemi di sicurezza interna (ad esempio disordini civili), corruzione, crisi economiche finanziarie (ad esempio crisi del debito sovrano).
Economici	Inadeguate infrastrutture, crisi energetiche, alti livelli di povertà, rilevante disoccupazione o ricorso al lavoro in nero.
Reputazionali	Sfruttamento del lavoro (ad esempio ricorso al lavoro minorile), divieto di partecipazione ad associazioni politiche e sindacali, discriminazione contro donne e minoranze, problemi etici e di corruzione.
Ambientali	Processi produttivi che richiedono un eccessivo utilizzo di risorse (ad esempio energia elettrica, acqua), rumore e inquinamento ai danni della popolazione locale, espropriazione dei terreni.
Demografici	Flussi migratori, malfunzionamenti nel mercato del lavoro, differenze culturali.
Lavorativi	Predominanza di lavoratori con basse competenze, rischi di salute e sicurezza dei lavoratori, insoddisfazione dei dipendenti, incidenti o malattie correlate all'attività lavorativa, turnover dei dipendenti, mancanza o perdita di lavoratori con competenze.

Il **monitoraggio delle fonti di rischio** permette all'organizzazione di mantenere la propria valutazione dei rischi nel tempo.

Oggi esistono servizi specializzati di intelligence che forniscono aggiornamenti continui, sfruttando molteplici fonti informative e algoritmi di intelligenza artificiale per collegarle e interpretarle. In questo modo è possibile non solo identificare le fonti di rischio, ma anche accorgersi tempestivamente di avvenimenti che potrebbero portare a problemi di fornitura nel prossimo futuro per cercare di adottare rapidamente contromisure adeguate.

La valutazione dei rischi dovrebbe essere svolta prima dell'acquisizione di un fornitore ed ogni qualvolta vi siano rilevanti variazioni nel contesto interno ed esterno.

Inoltre, i risultati delle attività dovrebbero essere comparabili anno su anno, anche al fine di creare serie storiche per una migliore comprensione dell'evoluzione del proprio profilo di rischio.

12.4 Trattare i rischi

La fase successiva richiede di **individuare opportune misure di mitigazione dei rischi.** Gli interventi cautelativi potranno essere richiesti al fornitore o essere adottati direttamente dall'organizzazione.

Una valutazione delle misure di mitigazione in termini di efficacia (idoneità della contromisura a ridurre il rischio inerente) permette all'organizzazione di calcolare un valore di *rischio residuo*, ossia il rischio che permane dopo l'applicazione delle misure di prevenzione e protezione.

Per semplificare, i rischi residui possono essere distinti in due categorie:

1. rischi che dovranno essere sottoposti a trattamento, solitamente perché di livello alto considerato non tollerabile, indipendentemente dai benefici realizzati attraverso l'attività rischiosa;
2. rischi che non necessitano di trattamento, solitamente perché di livello basso e considerato accettabile o che non necessita di misure di controllo aggiuntive.

12.4.1 Mitigare il rischio

Nei capitoli precedenti sono state presentate molte buone pratiche per mitigare il rischio, da quelle più tecnologiche a quelle contrattuali e quelle di organizzazione interna.

L'organizzazione dovrebbe pertanto predisporre, a fronte di ciascun rischio identificato, le misure già previste e quelle da prevedere, in modo da predisporre un piano d'azione con precise responsabilità e scadenze. Il piano dovrebbe essere oggetto di riesame periodico in modo da monitorare lo stato di avanzamento delle azioni.

12.4.2 Evitare il rischio

Il rischio di supply chain potrebbe essere evitato internalizzando le attività o non esternalizzandole. Evidentemente, questa opzione comporta la necessità di gestire altri rischi, ossia quelli relativi alle attività interne.

12.4.3 Condividere il rischio con le assicurazioni

Nel medio termine, il trasferimento del rischio attraverso **polizze assicurative** ad hoc sarà una ulteriore misura. Diffusasi recentemente, si ritiene che la misura possa consolidarsi anche indipendentemente dal momento storico che sicuramente ne enfatizza l'esigenza.
Tra i benefici anche l'aumento della consapevolezza del rischio a livello apicale attraverso la valutazione dei premi (in vertiginoso aumento) e di conseguenza l'attenzione del management alla gestione delle security operation.

Il percorso di valutazione di una polizza può consentire di avere una valutazione del rischio condotta da operatori economici estranei al mondo ICT, ma abili nel definire algoritmi che "pesano" le variabili rilevanti per la continua misurazione del rischio stesso. Questo consente di dare priorità alle azioni anche sulla base di indici di rischio non tipici del mondo ICT.

Al fine di valutare il rischio derivante da soggetti terzi, le compagnie di assicurazione hanno elaborato metodologie di assessment che indagano il modello di TPRM adottato dal proponente.

L'esposizione al rischio terze parti è verificata dall'assicuratore mediante questionario tecnico assuntivo, interviste al cliente e utilizzo di tool che eseguono ricerche OSINT automatiche sia nella rete pubblica che nel cosiddetto "dark web", con il fine di contestualizzare l'ambito di fornitura, la tipologia di servizio erogato, l'affidabilità del fornitore, i presidi contrattuali richiesti dal committente e, più in generale, le misure organizzative e di governance assunte dal committente e dal fornitore, nonché le misure tecniche e infrastrutturali che è in grado di garantire il fornitore.

In particolare, viene verificato: il processo di selezione dei fornitori, il censimento della supply chain ICT, la definizione di ruoli e di responsabilità, la richiesta di una copertura di responsabilità civile, eventuali limitazioni della responsabilità imposte dal vendor, la riserva del diritto di audit da parte dell'acquirente, le misure per il controllo degli accessi (tramite VPN, MFA, rispetto del principio del "least privilege", riesame dei diritti di accesso, monitoraggio), le certificazioni ottenute dalla terza parte (ad esempio ISO/IEC 27001), gli SLA garantiti (fra cui RPO e RTO), la possibilità di ricorso alla subfornitura, l'approccio zero trust, altre misure tecniche e infrastrutturali e, in definitiva, le garanzie del fornitore riguardo ai requisiti minimi di sicurezza (back-up, crittografia, ecc.).

Tali indagini si rendono indispensabili per quantificare in termini di severità e

frequenza l'esposizione al rischio a cui è soggetto l'assicurato in caso di esternalizzazione di servizi, specialmente qualora ricorra ad un full outsourcing dei servizi informatici.

Gli impatti considerati riguardano la possibile perdita di disponibilità del servizio erogato al committente, la compromissione dell'integrità dei dati che implica attività di ripristino e costi di gestione della crisi, la violazione della riservatezza dei dati del committente che potrebbe comportare azioni di responsabilità civile da parte di terzi.

Non ultimo, bensì fra i primi timori degli assicuratori, si pone il tema della gestione del rischio di cumuli, legato all'erogazione di servizi da parte di un singolo fornitore in favore di una pluralità di assicurati che potrebbe comportare contemporaneamente impatti sistemici e l'attivazione di una molteplicità di coperture assicurative (si veda, per esempio, il caso SolarWinds).

Per offrire una soluzione di trasferimento del rischio idonea agli scenari fin qui descritti, oggi il mercato assicurativo nazionale e internazionale propone di integrare la classica cyberpolizza con la garanzia di *cyber contingent business interruption* (cyber CBI), volta ad assicurare i danni patrimoniali derivanti da un evento che colpisce il sistema informatico del fornitore, ICT o non ICT, da cui l'assicurato dipende.

Quando l'assicurato valuta se attivare la garanzia cyber CBI deve porre attenzione alla tipologia di clausola che gli viene proposta: quali fornitori sono coperti? Fino a che livello contrattuale di fornitura è estesa la clausola? Sono oggetto di copertura solo fornitori nominati in polizza? Quali sono i trigger di attivazione della clausola? Sono previsti sottolimiti o franchigie monetarie e temporali diverse rispetto a quelli generali di polizza? Sono richiesti requisiti minimi di sicurezza informatica ai fornitori affinché si attivi l'operatività della clausola?

Innanzitutto è d'obbligo definire la tipologia di fornitore cui si fa riferimento. La copertura assicurativa può infatti far riferimento al solo fornitore di prodotti e servizi informatici che supportano l'operatività. In questo caso i protagonisti sono i dati e i sistemi informatici di proprietà dell'assicurato ma posti presso la sede del fornitore esterno. L'oggetto di copertura è l'interruzione dell'attività che deriva all'assicurato in seguito a un evento che colpisce il proprio fornitore informatico. Solitamente questa estensione è già prevista nelle cyberpolizze tradizionali per i fornitori diretti dell'assicurato.

Fondamentali per la continuità operativa sono, anche, i fornitori di beni e servizi non

informatici. La clausola CBI può essere estesa all'interruzione dell'attività dell'assicurato in seguito ad un evento che colpisce uno di questi attori. Si tratta di una condizione solitamente non inclusa nelle polizze standard ma valutabile in fase di sottoscrizione con condizioni dedicate e spesso limitata ai soli fornitori nominati in polizza.

Nella visione di supply chain quale complesso sistema rientrano, poi, le infrastrutture critiche esterne, ossia quei servizi essenziali per il mantenimento delle funzioni vitali: elettricità, acqua, gas, internet, telecomunicazioni. Tale tipologia di fornitura è caratterizzata a livello intrinseco dal principio secondo cui da pochi attori dipende l'operatività della quasi totalità delle organizzazioni e da un funzionamento il cui controllo è posto al di fuori del perimetro d'azione dell'assicurato. Tali fattori fanno sì che ogni interruzione dell'infrastruttura critica è sempre esclusa dalle polizze standard sul mercato per ragioni di sostenibilità del mercato assicurativo stesso.

Altro elemento chiave da non sottovalutare nella valutazione di un'estensione cyber contingent business interruption è il trigger di attivazione della clausola.

Nella versione base della clausola CBI il trigger di attivazione è il *security failure*, ossia una falla di sicurezza nel sistema informatico del fornitore. In questo caso l'evento assicurato è un evento che colpisce il sistema informatico o i dati sul sistema del fornitore causando un'interruzione dell'attività all'assicurato.

L'operatività della cyber CBI può essere estesa anche al *system failure*, estendendo la copertura a ogni altra interruzione non pianificata o non intenzionale del sistema informatico del fornitore da cui derivi un'interruzione all'attività del soggetto assicurato.

Restano ferme le definizioni e le restanti condizioni specificate nella polizza di partenza, tra cui l'esclusione, quasi sempre confermata, dei danni materiali, che è principio cardine della moderna cyberpolizza volta ad assicurare i soli danni immateriali derivanti da un cyberincidente.

In entrambi i casi, ciò che la compagnia indennizza sono l'impatto economico negativo subito dall'assicurato derivante dalla riduzione o interruzione della sua attività caratteristica e i costi che la stessa organizzazione deve sostenere per recuperare l'operatività dei sistemi e ripristinare l'integrità dei dati impattati dall'evento.

Infine conviene prestare attenzione al tier di fornitura incluso in polizza, ossia il livello di dipendenza contrattuale con il fornitore che definisce se sono considera-

ti i soli fornitori con rapporto direttamente regolato da un contratto scritto tra il fornitore e l'organizzazione (*first tier*) o include i sub-fornitori, il cui contratto non è direttamente regolato dall'assicurato (*second tier o multi tier*). Le clausole più diffuse oggi sul mercato prevedono la copertura dei fornitori di primo livello, perimetro in cui il rischio che ne deriva è ancora valutabile e misurabile secondo le modalità che abbiamo già descritto.

Quanto fin qui presentato, ci fa intendere che il trasferimento del rischio residuo prevede, da parte dell'organizzazione, un esame attento e trasparente del proprio profilo di rischio e il mercato assicurativo deve essere valutato come tassello integrato nel processo di TPRM.

Si tenga presente che le proposte del mercato assicurativo relative alla supply chain ICT sono in costante aggiornamento, in quanto devono garantire l'allineamento della sostenibilità del mercato assicurativo globale a un contesto in cui numero e gravità degli attacchi è in costante aumento e anche le soluzioni e gli attori.

12.4.4 Accettare il rischio

Considerando che non è possibile avere un rischio zero, i rischi residui possono essere accettati se molto bassi.

È possibile accettare anche i rischi non trascurabili per molti motivi. Tra questi: il fatto che azioni di mitigazione potrebbero introdurre ulteriori rischi più elevati, il costo delle azioni di mitigazione superiore a quello dei possibili benefici, la necessità di adeguarsi a precise esigenze contrattuali dei clienti, la presenza di controlli compensativi (p.e. di monitoraggio).

L'accettazione del rischio deve essere esplicitata dall'organizzazione, in modo da poterla riesaminare periodicamente per verificare se è possibile modificare l'opzione scelta.

12.5 Prodotti per l'analisi del rischio di fornitura

Il presente paragrafo prende spunto dal lavoro fatto dal gruppo di lavoro "Rischio digitale Innovazione e Resilienza" del 2021 in cui sono stati analizzati gli strumenti per l'analisi del rischio e, inoltre, dalle indicazioni ricevute dalle società di valutazione come Gartner e Forrester e dalle indicazioni del mercato.

Abbiamo quindi cercato prodotti le cui caratteristiche ci sembrassero funzionali per la valutazione del livello di maturità digitale dei fornitori e sono stati selezionati se (1) sono utili per valutare il rischio (2) di cybersecurity (3) di un soggetto coinvolto nella supply chain.

I parametri di riferimento utilizzati sono stati i seguenti:

- disponibilità di funzionalità di analisi del rischio di fornitura e misurazione del livello di maturità digitale di un fornitore,
- disponibilità di funzionalità specifiche per misurare il livello di rischio di una singola transazione all'interno del processo di supply chain.

Con questi criteri abbiamo identificato alcuni prodotti censiti da Gartner e da Forrester (vedi tabella successiva) e tre altri che non essendo in Gartner o Forrester abbiamo descritto con più dettaglio in seguito.

La lista seguente risulterà non esaustiva e velocemente superata dal progredire dei prodotti, ma in ogni caso rappresenta un utile punto di partenza per chiunque avesse la volontà di migliorare il proprio processo di valutazione dei fornitori e della supply chain.

Prodotto	URL	Forrester	Gartner
Allgress	https://allgress.com/	Not rated	Aspiring
Aravo	https://aravo.com/	Strong Performers	Strong Performer
Archer	https://www.archerirm.com/	Strong Performers	Aspiring
BitSight	https://www.bitsight.com/	Not rated	Customer's Choice
Black Kite	https://blackkite.com/	Not rated	Customer's Choice
Coupa	https://www.coupa.com/	Contenders	Not rated
CyberGRX	https://www.cybergrx.com/	Not rated	Strong Performer
Cyber Quant (MasterCard)	https://www.mastercard.	Not rated	Not rated
Diligent (Galvanize)	https://www.diligent.com/	Strong Performers	Strong Performer
Logic Manager	https://www.logicmanager.com/	Contenders	Not rated

LogicGate	https://www.logicmanager.com/	Strong Performers	Not rated
MetricStream	https://www.metricstream.com/	Strong Performers	Not rated
NAVEX	https://www.navex.com/	Strong Performers	Not rated
OneTrust	https://www.onetrust.com/	Leaders	Customer's Choice
Panorays	https://panorays.com/	Not rated	Strong Performer
Prevalent	https://www.prevalent.net/	Strong Performers	Customer's Choice
ProcessUnity	https://www.processunity.com/	Leaders	Customer's Choice
Red Piranha	https://redpiranha.net/	Not rated	Strong Performer
RiskRecon	https://www.riskrecon.com/	Not rated	Aspiring
SCORE (Rexilience)	https://score.rexilience.eu/	Not rated	Not rated
Security Scorecard	https://securityscorecard.com/	Not rated	Customer's Choice
ServiceNow	https://www.servicenow.com/	Leaders	Established
Swascan	https://www.swascan.com/it	Not rated	Aspiring
UpGuard	https://www.upguard.com/	Not present	Established

La tabella sintetizza quanto indicato nei report 2022 sul Third-Party Risk Management di Forrester Research[164] e di Gartner[165].

Il report di Forrester Research valuta i top vendor presenti sul mercato usando le quattro classificazioni decrescenti: **Leaders, Strong Performers, Contenders e Challengers**. L'analisi è svolta utilizzando 21 indicatori che valutano Offerta Corrente, Strategia e Presenza di Mercato.

Il report "Voice of the Customer" di Gartner aggrega le recensioni dei decisori ICT sui vari prodotti. Le recensioni sono riclassificate come:

- **Customer's Choice**: soddisfa o supera sia la valutazione complessiva media del mercato sia l'interesse e l'adozione media degli utenti del mercato.

164 "The Forrester Wave™: Third-Party Risk Management Platforms, Q2 2022. The 12 Providers That Matter Most and How They Stack Up", May 16, 2022.

165 "Gartner Peer Insights 'Voice of the Customer': IT Vendor Risk Management Tools", March 2, 2022 – ID G00763741.

- **Established**: soddisfa o supera la media di mercato dell'interesse e dell'adozione degli utenti, ma non soddisfa la media di mercato della valutazione complessiva.
- **Strong Performer**: soddisfa o supera la valutazione complessiva media del mercato ma non soddisfa l'interesse e l'adozione media degli utenti del mercato.
- **Aspiring**: non soddisfa né l'interesse e l'adozione media degli utenti né la valutazione complessiva media del mercato.

Di seguito vi è una descrizione sintetica dei prodotti non valutati da Forrester o Gartner di cui abbiamo ricevuto segnalazione. Uno di essi è una soluzione internazionale e due sono stati realizzati in Italia.

12.5.1 Master Card – Cyber Quant

Nome: Cyber Quant

Nazionalità produttore: Israele

Descrizione:
Cyber Quant, sviluppato in Israele e acquisito da MasterCard, è una piattaforma che misura i rischi per la sicurezza informatica di un'organizzazione, segnala le lacune e stima l'impatto dei nuovi controlli considerando le minacce, creando risultati e raccomandazioni personalizzate. Cyber Quant calcola diverse misure da cui emerge un insieme quantitativo di metriche. La metodologia alla base del sistema si basa sul modello TARA (Threat agent risk assessment) di Intel e sul modello FAIR (Factor analysis of information risk), derivato dal framework Value at Risk (VaR) per la cybersecurity e il rischio operativo.

Vantaggi per la Supply Chain:
Permette non solo di valutare un fornitore attraverso le risposte ad un questionario che viene erogato on line, ma anche e soprattutto di valutarne la security posture attraverso un'analisi delle configurazioni locali effettuata attraverso un agent da scaricare ed eseguire temporaneamente sulle postazioni del fornitore. In questo modo, Cyber Quant effettua una misurazione della Security Posture del fornitore e valuta il livello di cyber-rischio per il contraente. Le analisi possono essere ripetute e confrontate in tempi diversi.

12.5.2 SCORE – Rexilience

Nome: SCORE

Nazionalità produttore: Italiana

Descrizione:
SCORE (Security and Compliance Overall Risk Evaluation) nasce con l'intento di effettuare la valutazione "oggettiva" del cyber-rischio delle piccole organizzazioni. Fornito come servizio SaaS, realizza delle valutazioni automatizzate esclusivamente tramite algoritmi e scale quantitative, e fornisce utili indicazioni per ridurre drasticamente il rischio e migliorare la propria valutazione.
SCORE si basa su:

- un questionario di raccolta dati a domande chiuse per valutare la postura dell'organizzazione;
- diversi servizi integrati di scansione di internet e di analisi delle vulnerabilità e diverse basi dati internazionali per la valutazione delle vulnerabilità e della loro gravità attivati sulla base delle risposte del questionario;
- estese ricerche di informazioni nel dark web relativamente agli elementi emersi come compromessi dalla fase di analisi.

SCORE produce due output:

- un punteggio tra zero e cento che rappresenta il livello di rischio tecnico e organizzativo;
- un report che indica a quali cose è più urgente porre rimedio.

Vantaggi per la Supply Chain:
Oltre a semplificare e rendere accessibile la valutazione di cybersecurity alle PMI, SCORE offre alle grandi imprese uno strumento che consente loro di valutare in modo oggettivo e non invasivo la cybersecurity di tutte le PMI che costituiscono la loro supply chain.
Il modello di SCORE basato su un semplice questionario a domande chiuse e strumenti automatici di scansione delle vulnerabilità e di raccolta di dati OSINT consente ad una grande organizzazione di misurare ad un costo estremamente contenuto e con risultati confrontabili qualsiasi organizzazione della sua supply chain indipendentemente dalla sua dimensione.

12.5.3 Swascan

Descrizione:
Swascan offre un apposito servizio per la difesa informatica della supply chain. Uno strumento finalizzato alla verifica dei rischi connessi alla gestione del portafoglio fornitori. Il Supply Chain Risk Indicators di Swascan permette di identificare e individuare le informazioni pubbliche e semi-pubbliche a rischio, le vulnerabilità disponibili pubblicamente relative al dominio indicato e di scoprire le email compromesse del fornitore.

Inoltre, permette di verificare l'esposizione al rischio di attacchi informatici tramite la supply chain e di rispondere agli obblighi previsti dalla GDPR relativi alle attività di controllo a carico del Titolare nei confronti dei Responsabili del Trattamento. Il tutto rientrando nei requirement previsti dalla ISO/IEC 27001.

Vantaggi per la Supply Chain:
Il Supply Chain Risk Indicators si avvale della tecnologia piattaforma Software as a Service Swascan – fornendo:

- La superficie d'attacco: mappatura degli asset potenzialmente a rischio
- Il livello di Rischio Tecnologico: individuazione delle potenziali vulnerabilità lungo tutta la filiera
- Il livello di Rischio Umano: rischio collegato al social engineering
- Il livello di Rischio GDPR: verificando, tramite vaglio delle fonti OSINT e CLOSINT, la confidenzialità, integrità e disponibilità delle informazioni.

Erogato come servizio mensile e abbinato al centro di competenze verticali Swascan.

Intervista
La gestione delle terze parti in UniCredit

Di Gianbattista Piacentini, Head of Digital Security Validation at UniCredit.

Nell'ambito del complesso contesto politico ed economico in cui le banche e le istituzioni finanziarie operano attualmente, i rischi generati dagli accordi di outsourcing e non-outsourcing con terze parti sono considerati tra i più rilevanti e più difficili da controllare.

Questo vale ancor di più nell'ambito più specifico della cyber security: se oggi il rischio cyber è considerato uno dei rischi operativi più rilevanti per le banche, il

rischio cyber collegato alle terze parti emerge come uno dei “top risk” dell’area cyber nel suo complesso.

UniCredit ha ben chiara la rilevanza di questi temi e da alcuni anni ha definito e progressivamente consolidato un framework specifico per la gestione delle terze parti, con l’obiettivo di assicurare l’efficace identificazione, valutazione, mitigazione e monitoraggio dei rischi generati dagli accordi con terze parti.

Dal punto di vista organizzativo è stata creata una struttura ad hoc “Group Third Parties Management” che coordina a livello di gruppo la gestione complessiva delle terze parti, dalla definizione delle linee guida e dei processi di funzionamento alla verifica della implementazione nelle diverse società del gruppo, con team specializzati nella gestione degli accordi di outsourcing e nella gestione di accordi di non outsourcing.

Il processo di gestione del rischio di terze parti prevede diverse fasi nell’ambito delle quali sono coinvolti più attori: oltre alla struttura di Group Third Parties Management che agisce da centro di coordinamento, sono coinvolte le strutture di business che propongono accordi con terze parti e i Centri di competenza responsabili di presidiare le dimensioni di rischio relative alla propria area di competenza, ad esempio Cyber Security, Business Continuity, Data Protection Office e ICT.

Nei prossimi paragrafi ci soffermiamo in particolare sulle attività svolte dal Competence Center Cyber Security.

12.5.4 La gestione del rischio cyber di terze parti

Il Competence center Cyber Security viene coinvolto in tutti i casi in cui la relazione con la terza parte comporti un rischio cyber ossia è definita “Cyber Relevant”.
Le macro fasi del processo più rilevanti in cui è previsto il coinvolgimento di Cyber Security sono due:

- pre-contract;
- monitoring.

12.5.5 La fase di pre-contract

Nel ciclo di vita della relazione con la terza parte, la fase di pre-contract è la fase in cui si effettuano tutte le attività di analisi dei rischi propedeutiche alla finalizzazione di un accordo tra la banca e la terza parte per la fornitura di un servizio, sia esso in outsourcing o non outsourcing.

Dal punto di vista cyber security lo scopo di questa fase è valutare i rischi cyber relativi al servizio offerto dalla terza parte e definire con essa le misure di sicurezza che dovrà osservare in modo che tali rischi siano correttamente mitigati.

La fase di pre-contract si articola nelle seguenti attività:

- viene identificato l'ambito e le peculiarità del servizio offerto dalla terza parte e il livello di rischio inerente cyber associato;
- vengono identificati i requisiti di sicurezza che la terza parte è tenuta a osservare;
- viene effettuato l'assessment ovvero la valutazione di quanto la terza parte soddisfi i requisiti di sicurezza identificati. Durante questa fase vengono valutati tutti gli elementi che contribuiscono a ridurre e mitigare il rischio cyber: le policy adottate, le evidenze tecniche (ad esempio i vulnerability assessment e i penetration test effettuati), i processi e i controlli posti in essere dalla terza parte, applicati anche a eventuali suoi sub-fornitori;
- nel caso in cui emergano dei gap nei requisiti di sicurezza, viene definito con la terza parte un piano di rimedio;
- infine viene calcolato il rischio residuo cyber, che tiene conto dei risultati dell'assessment e dell'eventuale piano di rimedio. Il calcolo del rischio residuo cyber viene effettuato utilizzando un'apposita metodologia definita da UniCredit in linea con le best practice di mercato, le normative in essere e le linee guida dei regulator.

Va aggiunto che sulle modalità di applicazione delle misure di sicurezza o sui tempi di implementazione del piano di rimedio possono in alcuni casi emergere punti di vista differenti tra la banca e la terza parte, che vengono però di norma risolti in fase di negoziazione contrattuale.

In ogni caso, affinché l'accordo con la terza parte possa essere finalizzato, è necessario che il rischio residuo cyber risulti minore o uguale a un valore soglia predefinito in accordo con le funzioni di Risk Managament di UniCredit.

Il risultato finale della fase di pre-contract cyber è un allegato tecnico che diventa parte integrante del contratto con la terza parte. Tale allegato include i requisiti di sicurezza che la terza parte è tenuta a soddisfare e l'eventuale piano di rimedio che la terza parte si impegna a realizzare.

La fase di monitoring

La fase di monitoraggio inizia dopo la firma del contratto, ossia da quando la strut-

tura di business che è responsabile del contratto inizia a monitorare la qualità del servizio fornito dalla terza parte. Lo scopo della fase di monitoraggio è quello di garantire che la terza parte e i servizi da essa forniti seguano le disposizioni del contratto attraverso revisioni e controlli periodici.

Dal punto di vista cyber security le attività di controllo sugli accordi di outsourcing e non outsourcing sono svolte al fine di verificare che il soggetto terzo stia attuando le azioni concordate nella fase di pre-contract, ad esempio le misure di sicurezza contenute nell'allegato tecnico siano correttamente applicate e i piani di rimedio (nel caso in cui siano stati individuati rilievi di sicurezza) vengano eseguiti.

I controlli periodici sono sempre previsti in caso di contratti di outsourcing, mentre per i contratti di non outsourcing vengono effettuati sulla base di criteri basati su una logica "risk based", ad esempio se il contratto ha una durata limitata nel tempo, il monitoring non è strettamente necessario.

Gli elementi rilevanti da valutare nella fase di monitoring sono i cambiamenti intercorsi dal momento in cui l'accordo con la terza parte è stato effettuato. Tali cambiamenti possono essere dovuti a modifiche del servizio offerto dalla terza parte, ad aggiornamenti del quadro regolamentare o dei regolamenti interni, a modifiche degli scenari di rischio cyber, tutti elementi che possono modificare i livelli di rischio originariamente valutati.

Di conseguenza la fase di monitoring cyber prevede di:

- rivalutare il rischio cyber inerente al servizio offerto dalla terza parte;
- verificare l'adeguatezza delle misure di sicurezza contenute nell'allegato tecnico e degli eventuali piani di rimedio;
- ricalcolare il rischio cyber residuo e verificare che sia ancora minore o uguale al valore soglia definito da UniCredit.

Il risultato finale della fase di monitoring cyber è un eventuale aggiornamento dell'allegato tecnico in termini di requisiti di sicurezza che la terza parte è tenuta a soddisfare e dell'eventuale piano di rimedio che la terza parte si impegna a realizzare.

Conclusioni

In un mondo sempre più interconnesso, il rischio di terze parti è un tema di grande rilevanza e molto difficile da controllare. UniCredit ha sviluppato un'organizzazione e una serie di processi specifici, strutturati e pragmatici, con l'obiettivo di gestire in modo efficace il rischio di terze parti e allo stesso tempo essere pronta a evolvere velocemente in un contesto che cambia in modo rapido e poco prevedibile.

FineIntervista

Intervista

Piattaforma integrata di vendor risk management di InfoCert

Di Giovanni Belluzzo, InfoCert, Head of Cyber Security & Management System, Chief Information Security Officer.

In InfoCert, nell'ambito delle attività di definizione del Piano Strategico Cyber Security 2022, è stata identificata la necessità di ottimizzazione del processo finalizzato alla **classificazione dei fornitori e partner** sulla base del **rischio cyber intrinseco**.

Sin dalle prime fasi di progettazione del processo si è evidenziata la necessità di una **Piattaforma Integrata di Vendor Risk Management (VRM)** che rispondesse ai seguenti requisiti:

1. Misurazione preventiva della **Cyber Risk Exposure** mediante indicatori automatici non invasivi (report cyber threat intelligence, ecc.);
2. **Questionari di self-assessment** da sottoporre ai vendor, profilati (numero di controlli) in base al livello di rischio rilevato al punto 1;
3. **VRM dashboard** sul livello di rischio globale del vendor (VRM Score), derivante dall'integrazione fra indicatori automatici e risultati dei questionari di self-assessment; il VRM Score permette la prioritizzazione delle attività di audit di 2° parte presso i vendor.

In figura una rappresentazione concettuale della piattaforma.

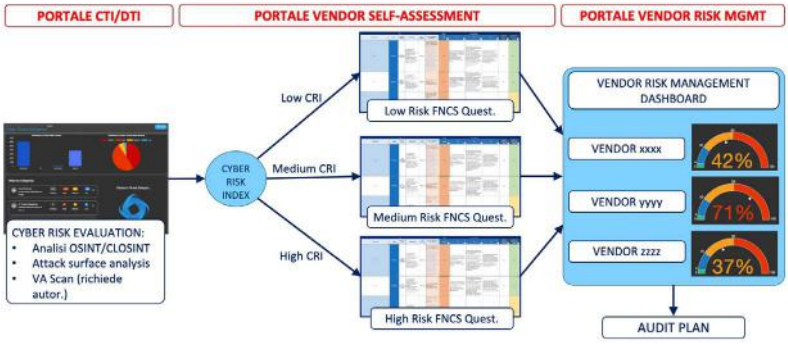


Figura 32 – Schema concettuale della piattaforma integrata VRM

Procedendo nell'analisi tecnica sono state individuate le componenti fondamentali rappresentate nella figura seguente.

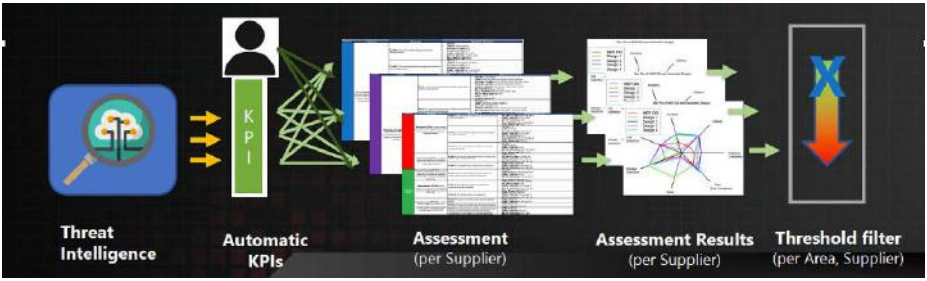


Figura 33 – Componenti piattaforma integrata VRM

In dettaglio:

- **Threat Intelligence**: le attuali metodologie di cyber threat intelligence permettono l'estrazione di indicatori sintetici quali:
  - N. IP;
  - N. sottodomini;
  - N. vulnerabilità (distinte per high, medium e low);
  - N. email compromesse;
  - altre breach.
- **Automatic KPI**: dai dati ottenuti dagli strumenti di threat intelligence possono essere estratti una serie di indicatori "normalizzati" da confrontare con soglie di riferimento, ad es.:
  - vulnerabilità per IP;
  - email compromesse per sottodominio.
- **Assessment (per supplier)**: il questionario valutativo è basato su una selezione di blocchi di domande specifiche per fornitore (o – per generalità – di singole domande); dovrà essere possibile decidere (per singole domande o macro-categorie) di eliminare alcuni set di domande (p.e.. a fronte di certificazioni presentate), oppure di forzarne alcune anche se escluse dall'analisi automatica di threat intelligence (p.e. a fronte di informazioni offline riguardo la non attendibilità del fornitore su specifiche aree).

	Q1	Q2	...	Qn
Supplier 1	X			X
Supplier 2	X	X		
...				
Supplier m		X		X

- **Assessment results (per supplier)**: parte integrate del questionario valutativo è la produzione di indicatori di sintesi (p.e. per area) che permettano il ranking dei fornitori:
    - grafici multidimensionali (es. radar) per la valutazione di più componenti;
    - indicatori e grafici di sintesi.
- **Threshold filter** (per area, supplier): dagli indicatori di sintesi, sono segnalati i fornitori che non rispetteranno soglie minime in specifiche aree.

Dal punto di vista dell'utilizzo, la piattaforma VRM prevede utenze con profilazione basata sul ruolo:

- **Amministratore**: effettuano la valutazione dei fornitori;
- **Referente fornitore**: dipendente di un fornitore, assegna le parti di questionario ad altri colleghi;
- **Fornitore**: rappresenta l'insieme dei dipendenti del fornitore interessato dal processo valutativo.

Nella tabella seguente vengono sintetizzati i permessi per ogni ruolo.

	Gestione fornitori	Visione report	Personalizzazione questionari	Assegnazione parti questionario	Compilazione questionario
Amministratore	X		X	X	
Referente fornitore				X	
Fornitore					X

La piattaforma VRM, attualmente in fase avanzata di realizzazione, verrà testata su un numero limitato di fornitori critici pilota nel corso dell'ultimo trimestre 2023; dopo questa fase pilota si procederà con un utilizzo massivo su tutto il catalogo fornitori e partner.
FineIntervista

13. GESTIRE LA SUPPLY CHAIN

13.1 Il processo di acquisizione

Del processo di acquisizione tipicamente si occupa la funzione acquisti, talvolta è formalizzato altre volte no. Si preoccupa prevalentemente di verificare elementi di conformità e chiaramente di economicità, analizza gli elementi funzionali e prestazionali della fornitura, spesso con il supporto del reparto più direttamente interessato dalla tipologia di fornitura.
Il processo di acquisizione, se pur spesso capitanato dall'Ufficio acquisti, necessita per sua natura del coinvolgimento di più funzioni e di competenze sempre più specifiche. La digitalizzazione spinta di beni e servizi necessita del coinvolgimento della funzione ICT. La trasversalità e mutevolezza degli scenari e delle normative suggerisce di attivare anche nel processo di acquisizione figure con competenze di analisi del rischio e adeguamento normativo.

13.2 La raccolta di informazioni e di offerte

Il processo di acquisizione del fornitore, dovrebbe prevedere una specifica e puntuale articolazione, affinché tutti gli elementi, controlli e requisiti siano verificati dal personale dedicato. Il processo potrà articolarsi su quattro macro fasi:

- RFI (request for information): indagine aperta che ha l'obiettivo di raccogliere informazioni su diversi fornitori in modo da poter effettuare comparazioni, in preparazione di una RFQ, o di una RFT o di una RFP. L'ambito di indagine può riguardare i fornitori (ad esempio strutture e solidità finanziaria), lo stato del mercato, strategie di prezzo e la gamma di prodotti e servizi per fornitore.
- La fase di RFI dovrebbe incorporare i criteri sull'esposizione al rischio dei fornitori (ad esempio geolocalizzazione del fornitore e sua esposizione a fenomeni socio-politici). Questo permette di escludere dal processo di fornitura soggetti con un'esposizione al rischio ritenuta inaccettabile.
- RFQ (request for quotation): primo contatto con i potenziali fornitori, a cui segue la richiesta di formalizzare un'offerta economica per i beni o i servizi oggetto della fornitura. Tale richiesta dovrebbe includere la descrizione della fornitura e le specifiche tecniche, i requisiti qualitativi, i termini contrattuali e di pagamento. La fase di RFQ potrebbe includere un primo ed iniziale

questionario ove richiedere la presenza di certificazioni, di piani di continuità operativa, il rispetto delle principali normative impattate dalla fornitura, l'esistenza di processi di gestione del rischio e monitoraggio dei propri fornitori. Questo permette di filtrare i fornitori e inserirli in un graduale processo di verifica di esposizione al rischio del fornitore. Nel paragrafo 13.3 questa è indicata come fase di qualifica.

- RFT (request for tender): invito aperto rivolto a tutti i potenziali fornitori, ai quali è richiesto di presentare un'offerta a fronte di una richiesta dettagliata (ad esempio bando di gara).
- RFP (request for proposal): richiesta di offerta in cui l'organizzazione comunica la disponibilità di risorse disponibili per un particolare progetto, ne descrive le caratteristiche e sollecita i potenziali fornitori a presentare offerte per il completamento delle attività progettuali.

La fasi di RFT e RFP, ancor più di quanto previsto dalla fase di RFQ, dovrebbero dettagliare puntualmente i requisiti imprescindibili per l'organizzazione non solo come già avviene sotto l'aspetto funzionale ma anche e sempre più sotto l'aspetto di sicurezza della fornitura e della sua esposizione ai rischi.

Si raccomanda anche di verificare che il fornitore abbia eseguito una propria valutazione del rischio e abbia attivato un programma di TPRM, in modo da assicurarsi che sia esso stesso attento al rischio di fornitura.

Alcuni requisiti di sicurezza da considerare sono poi da riportare nel contratto e sono riportati nel capitolo 11.

13.3 Verifiche di sicurezza

Durante la **fase di qualifica**, ogni fornitore, indipendentemente dalla dimensione e dal valore della fornitura, deve essere sottoposto a valutazioni in ambito sicurezza delle informazioni. Da queste dovrà emergere la capacità (o l'incapacità) della terza parte di soddisfare i requisiti minimi di sicurezza.

Le organizzazioni, prima di qualificare un nuovo fornitore dovrebbero assicurarsi che esso abbia:

- adottato buone pratiche al fine di garantire la protezione dei dati personali in accordo con la normativa vigente;
- definito ruoli e responsabilità nella gestione della sicurezza delle informazioni;

- identificato i dati sensibili dell'organizzazione a cui fornisce servizio;
- attuato adeguate misure di sicurezza per prevenire o contenere le conseguenze di un incidente di sicurezza informatica;
- attuato misure appropriate per identificare il verificarsi di un evento di sicurezza nella propria organizzazione e nell'infrastruttura informatica.

La **verifica tecnica preliminare** è un'analisi più approfondita del servizio di fornitura e dovrebbe essere svolta prima o nel primissimo periodo dall'avvio del rapporto di fornitura. Questa ulteriore analisi è attivabile per le forniture più critiche, più esposte a rischio, con forte componente tecnologica o di complessità intrinseca.

Le verifiche tecniche preliminari possono essere di diversa natura e variare a seconda del servizio e prodotto.

Lo scopo è di acquisire una significativa conoscenza delle misure tecniche implementate, siano esse funzionali che di sicurezza. Alcuni elementi possono riguardare:

- certificazioni possedute;
- modalità di autenticazione e tracciamento dei log;
- gestione delle vulnerabilità e degli aggiornamenti;
- attività di VA e PT;
- formazione del personale tecnico nell'ambito della rete, dei sistemi e dello sviluppo sicuro;
- processo di sviluppo del codice sicuro (SDLC);
- applicazione dei principi di security by design[166];
- code review;
- monitoraggio delle minacce anche con tecniche OSINT (open source intelligence[167], ossia l'analisi di fonti aperte, da clear e dark web a materiale pubblicato in qualunque formato e accessibile — incluso a pagamento — a qualunque privato cittadino).

Le attività di verifica devono anche aiutare a comprendere l'estensione e ramificazione della supply chain.

Alcuni elementi potrebbero apparire ridondanti rispetto ad alcuni requisiti verificati in fase di acquisizione. La differenza nella fase di verifica tecnica preliminare è

166 https://www.paconsulting.com/insights/five-steps-to-make-your-supply chain-secure-by-design/.

167 Yuxuan (Cicilia) Zhang, Richard Frank, Noelle Warkentin, Naomi Zakimi, Accessible from the open web: a qualitative analysis of the available open-source information involving cyber security and critical infrastructure, Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac003, https://doi.org/10.1093/cybsec/tyac003.

la profondità del controllo, l'oggetto (non tanto il fornitore ma la fornitura stessa) e soprattutto la puntualità della verifica (verificata oggettivamente).

13.4 Contratto

Una volta selezionato il fornitore, all'interno del contratto devono essere inserite le **clausole contrattuali** relative ai requisiti minimi di sicurezza, al loro mantenimento nel tempo, riportanti istruzioni precise per la terza parte. L'integrazione delle clausole contrattuali specifiche deve consentire di attribuire correttamente ruoli e responsabilità in ambito sicurezza e delle informazioni.
Per maggiori dettagli, vedere il capitolo 11.

13.5 Monitoraggio e audit

È fondamentale prevedere una fase di audit e di messa a disposizione di elementi di accountability, partendo già dalle verifiche di qualifica e preliminari. Nelle fasi successive è raccomandato di condurre verifiche del rispetto dei vincoli contrattuali e delle misure di sicurezza applicate, sia tramite dichiarazioni del fornitore (ad esempio descrizione delle misure attuate) sia con audit da remoto o in presenza.

Il monitoraggio e gli audit sono fondamentali perché le iniziali risultanze del processo di acquisizione non siano statiche e vengano superate dall'evolversi degli eventi.

Il monitoraggio e gli audit sono utili per un'attività puntuale di revisione contrattuale perché forniscono all'organizzazione un quadro entro cui muoversi nei rapporti con le terze parti.

L'organizzazione stabilisce tempi e modalità di monitoraggio e audit, tenendo conto del livello di rischio e della criticità della fornitura.

13.5.1 Monitoraggio

Le attività di monitoraggio, siano esse automatizzate attraverso strumenti software o manuali e condotte mediante audit, sono importanti per la gestione dei fornitori e subfornitori, sui quali la capacità di controllo e verifica è evidentemente più flebile essendo esterne al perimetro organizzativo.

Il processo di monitoraggio dovrebbe in particolar modo includere:

- Monitoraggi dello scenario di rischio associato al fornitore, prendendo in

considerazione fonti di informazioni interne ed esterne. Lo scenario di rischio potrebbe mutare significativamente e un fornitore ritenuto affidabile divenire improvvisamente critico.

- Monitoraggi automatizzati con l'uso di software di analisi e segnalazioni di eventuali anomalie riscontrate sulle prestazioni del fornitore in modo da individuare tempestivamente situazioni critiche.
- Sensibilizzazione del proprio personale sul rischio di fornitura in modo che possano segnalare anomalie e criticità (ad esempio il calo delle prestazioni potrebbe essere dovuto alla presenza di spyware).
- Audit (vedere paragrafo successivo) per verificare i requisiti della fornitura, identificando quelli che, se non rispettati, potrebbero pregiudicare il rapporto stesso di fornitura e la fiducia fra le parti.

13.5.2 Audit

Il controllo dei fornitori attraverso audit costituisce il modo migliore per ottenere un quadro completo delle regole e procedure del fornitore e per ricevere tutte le informazioni necessarie per intraprendere eventuali azioni correttive, laddove si rendessero necessarie.

Gli audit ai fornitori possono essere eseguiti sulla base di standard internazionali e delle procedure dell'organizzazione.

In un contesto con un numero elevato di fornitori, il programma di audit va definito anche tenendo conto del livello di rischio associato ai fornitori stessi.

Dal punto di vista contrattuale, è importante aver disciplinato la possibilità di svolgere audit e la modalità di gestione e attuazione delle eventuali misure e azioni di miglioramento che possono emergere dagli audit. Laddove il fornitore agisce come responsabile al trattamento, trova applicazione anche l'articolo 28 del GDPR che dà diritto al titolare del trattamento a effettuare audit ai responsabili.

13.5.2.1 La delega dell'audit a terzi

Si possono utilizzare audit e lavori di verifica di terze parti come quelli condotti a scopo di certificazione. Questo è molto utile in contesti che presentano numerosi fornitori che a loro volta utilizzano subfornitori in supply chain.

L'auditor può utilizzare il lavoro di terzi in tutta la supply chain, ma deve comunque formulare un'opinione propria. Questo anche in presenza di certificazioni.

13.5.2.2 Conduzione degli audit

Le modalità di gestione e conduzione degli audit sono oggetto di numerose pubblicazioni. Tra queste:

- ITAF 4 di ISACA[168];
- prassi di internal audit di AIIA[169], disponibili sul suo sito web;
- ISO 19011 e, per la sicurezza delle informazioni, ISO/IEC 27007 e ISO/IEC 27008;
- principi di intervento di IOSCO (International Organization Of Securities Commissions), che ha considerato anche gli audit in ambienti multivendor e terziarizzati[170] nell'ambito delle agenzie di rating del credito (sono però validi anche in altri settori).

ISACA[171] permette di accedere a pubblicazioni e strumenti per programmare e condurre audit.

Con il framework COBIT 2019 di ISACA sono disponibili guide complementari per l'audit a terze parti e la "Vendor Management: Using COBIT 5".

ISACA mette anche a disposizione i documenti "Outsourced IT Environments Audit/Assurance Program" e "IS Audit/Assurance Program for Cloud Computing", con check list degli elementi di verifica. Sono acquistabili anche documenti per ambienti specifici (p.e. MS Azure e AWS).

13.6 Chiusura del rapporto

Importante è gestire la dismissione del fornitore, sul quale andrebbe eseguita una valutazione di chiusura per comprendere il livello di esposizione al rischio che la cessazione della terza parte comporta per l'organizzazione.

Intervista

Intervista a Sergio Insalaco di UnipolSai

Sergio Insalaco è Head of IT Governance Security & Continuity at UnipolSai e membro del Comitato scientifico CLUSIT.

In quale modalità il processo aziendale di gestione dei rischi integra e tratta il

168 ISACA IT Audit Framework (ITAF™): A Professional Practices Framework for IT Audit, 4th Edition.

169 https://www.aiiaweb.it/international-professional-practices-framework-new-ippf.

170 FR07/2021 "Principles on Outsourcing Final Report". https://www.iosco.org/library/pubdocs/pdf/IOSCOPD687.pdf.

171 https://www.isaca.org/resources/insights-and-expertise.

rischio di sicurezza nella supply chain?

Qualsiasi organizzazione, indipendentemente dalle sue dimensioni, opera ormai in un ambiente estremamente complesso, dinamico e interconnesso, con collegamenti a livello di sistemi informatici e dati che abbracciano diverse tipologie di terze parti, in particolare fornitori, outsourcer, reti di vendita, partner.

La tutela dai rischi provenienti dalle terze parti, e in particolare dai fornitori, è un tema sempre esistito, almeno per quanto riguarda i tradizionali rischi legati a solidità economica e finanziaria, capacità operativa, conformità normativa, concentrazione, possibili conflitti di interesse, e tuttora questi rimangono rischi di cui tenere conto nei rapporti contrattuali.

Negli ultimi anni, tuttavia, è notevolmente aumentata anche l'importanza di verificare l'esposizione di una terza parte al rischio di sicurezza ICT, possibilmente secondo un approccio olistico che ricomprenda diversi filoni: governance, cyber security, protezione dei dati (personali e non), business continuity e resilienza. Infatti, un attacco cyber su una terza parte può comportare l'indisponibilità del servizio per un tempo prolungato o un impatto su riservatezza o integrità dei dati o ambedue, con conseguenze anche rilevanti di tipo economico, reputazionale e normativo per l'organizzazione committente.

Per questo, anche sul fronte metodologico e normativo, le best practice e gli standard internazionali quali l'ISO/IEC 27001, esistenti ormai da diversi anni e che comprendono controlli sulle terze parti, da qualche tempo vengono affiancate da un numero crescente di nuove raccomandazioni, orientamenti, direttive e regolamenti delle autorità, in particolare europee, sia trasversali (p.e. GDPR, Cyber Resilience Act) sia verticali (p.e. DORA e orientamenti EBA-EIOPA-ESMA per il mondo finanziario), con impatti che in qualche modo ricadono su tutte le organizzazioni coinvolte nella supply chain.

La valutazione e gestione del TPRM non è un percorso facile e lineare, perché è un tema nuovo non ancora standardizzato, caratterizzato da una forte dinamicità digitale tecnologica, architetturale e procedurale che consente alle varie best practice e normative di indicare alle aziende "cosa va fatto" ma non "come va fatto".

Di conseguenza è un tema molto attuale, rispetto al quale le organizzazioni, in particolare quelle più grandi, si sono già mosse, implementando sistemi di verifica concettualmente simili, spesso basati su questionari di assessment, declinati però secondo diverse modalità proprietarie che comportano effort di risorse e tempisti-

che non trascurabili.

Quali metodologie vengono utilizzate nel ciclo di procurement per la qualificazione del fornitore e per valutazione preventiva della sicurezza dei prodotti e servizi?

La qualificazione del fornitore in fase pre-contrattuale prevede la fornitura da parte dello stesso alla nostra azienda di una serie di informazioni e relative evidenze documentali, che consentano di stabilire o confermare il suo livello di affidabilità e conformità rispetto ai requisiti richiesti. Il dossier contrattuale condiviso con il fornitore comprende, tra l'altro, clausole con specifici requisiti e obblighi in relazione alla sicurezza dei dati e dei sistemi, ai livelli di servizio, ai diritti di accesso e audit e alla exit-strategy, nonché l'accettazione di un elenco di requisiti di sicurezza e privacy, e la compilazione di un questionario di sicurezza e di un modulo specifico per la gestione di dati personali ai sensi del GDPR. Il fornitore è tenuto contrattualmente a fornire informative periodiche sull'andamento dei servizi erogati e a segnalare tempestivamente l'insorgenza di eventuali incidenti di sicurezza o data breach.

La compilazione del questionario è articolata in due parti: la prima parte chiede di fornire la descrizione del servizio oggetto del contratto, i nominativi di riferimento e le eventuali certificazioni in vigore (ISO/IEC 27001 ed estensioni cloud ISO/IEC 27017 e 27018 o privacy ISO/IEC 27701, ISO 22301, ISAE 3402, SOC2, PCI/DSS, CISPE-CLOUD, CSA STAR, ecc.), la seconda parte richiede una risposta esplicita di adozione o meno di misure di sicurezza fisica, logica, perimetrale, di protezione dei dati, di tracciatura degli accessi, e di gestione incidenti e piani di recovery, ecc. secondo uno schema assimilabile ai domini ISO/IEC 27001. Particolare importanza e attenzione rivestono i contratti che contemplano l'esternalizzazione di servizi.

Le risposte a tale questionario vengono verificate con il supporto del nostro team di Sicurezza, incrociandole con le specifiche della fornitura e le eventuali tematiche GDPR coinvolte, e se necessario integrate con la richiesta di evidenze documentali (politiche, procedure, piani di continuità, penetration test o vulnerability assessment recentemente effettuati, ecc.), con incontri di approfondimento con il fornitore e con l'attivazione di ulteriori assessment specifici.

La presenza di certificazioni di sicurezza costituisce un elemento preferenziale nella valutazione rispetto ai fornitori che non ne possiedono, in quanto, ancorché non costituisca una completa garanzia, testimonia il fatto che il sistema di gestione della sicurezza è strutturato secondo standard internazionali e i suoi controlli sono sottoposti ad audit annuali sia interni sia effettuati da revisori esterni.

Quali processi di monitoraggio dei fornitori vengono attuati in fase di esercizio?

In fase di esercizio, si possono individuare diversi processi di monitoraggio e controllo delle terze parti, svolti in parallelo da settori aziendali diversi.

Il fornitore innanzitutto viene monitorato nel continuo dal nostro referente interno definito contrattualmente, riguardo soprattutto al rispetto dei livelli di servizio erogati, della disponibilità e della qualità della fornitura e del relativo supporto in caso di problemi.

Ulteriori segnalazioni su possibili anomalie relative al fornitore e ai servizi da esso erogati possono derivare anche da analisi effettuate dal nostro team di Sicurezza con strumenti finalizzati al monitoraggio applicativo, all'intrusion prevention e detection, alla threat intelligence e all'OSINT (open source intelligence), ad esempio relativamente a vulnerabilità zero-day (quali ad esempio Log4J e Solarwinds), a data leak di informazioni su open e dark web o a data breach non ancora comunicati. Ovviamente tali segnalazioni devono essere tempestivamente approfondite e verificate con il fornitore.

Ai due processi di monitoraggio nel continuo citati si aggiungono anche attività di audit puntuali sulle terze parti, che prevedono da parte dell'azienda cliente una verifica più approfondita dei controlli di sicurezza implementati dal fornitore e delle relative evidenze, con l'eventuale successiva condivisione di un piano di remediation per le misure che non sono ritenute all'altezza dei requisiti del cliente.

Quali sono le possibili evoluzioni future dell'approccio TPRM?

Un'evoluzione interessante del processo di monitoraggio nel continuo è quella di poter abbinare alle attività già previste anche l'interrogazione di servizi di security rating (BitSight, SecurityScorecard, RiskRecon, UpGuard, solo per citarne alcuni). Questi servizi consentono di avere una quantificazione della postura cyber di una realtà aziendale partendo dalla raccolta e analisi nel continuo di dati pubblici in relazione agli asset digitali e alle informazioni esposte in Internet (vulnerabilità presenti sui domini Internet, assenza o mancato aggiornamento di certificati di crittografia dei siti, segnalazioni data breach, infezioni malware o data leak subiti dall'azienda, ecc.). Queste soluzioni, potranno migliorare molto i programmi di TPRM, ma non sostituirli, in quanto non coprono alcuni aspetti di indagine (legati ad esempio alla security governance) e le fonti informative da cui raccolgono le informazioni possono essere non aggiornate o insufficienti, come in alcuni casi di PMI italiane.

Il mio auspicio è comunque che si proceda a livello internazionale verso una standardizzazione del framework di controlli TPRM e l'obbligo per i fornitori di conseguire specifiche certificazioni, onde permettere alle varie organizzazioni di semplificare almeno in parte le verifiche necessarie, riducendo complessità, tempi e costi.
FineIntervista

Intervista
Intervista a Alessandro Maria Manfredini e Alessandro Marzi di A2A

Alessandro Maria Manfredini è Direttore di Group Security e Cyber Defence del Gruppo A2A e Presidente dell'associazione AIPSA, Associazione Italiana Professionisti della Security Aziendale; Alessandro Marzi è A2A Group Cyber Defence e CISO.

In quale modalità il processo aziendale di risk management integra e tratta il rischio di sicurezza nella supply chain?

Il rischio di sicurezza nella fornitura (soprattutto in ambito digital) è sicuramente un tema di grande attualità e interesse e che è inserito nelle agende non solo dei Chief Risk Officer ma anche dei professionisti della security. Le minacce che gravano sulle forniture digital riguardano la scarsità di materie prime, dovute al concentramento in poche aree del mondo di componentistiche fondamentali; anche la scarsità di manodopera qualificata è sicuramente una tematica che potrebbe generare problemi alle forniture in senso lato, soprattutto se pensiamo ai professionisti della cyber security che in Italia sono nettamente inferiori rispetto alla domanda. Il rischio di sicurezza nella fornitura dovrebbe poi essere gestito in ottica preventiva e proattiva durante la qualifica del fornitore e in modo dinamico nel corso del mantenimento della qualifica e del contratto attivo, poiché gli scenari – come abbiamo visto – sono in continuo cambiamento è opportuno avere sempre una visione aggiornata dello status quo.

Il rischio della sicurezza della fornitura è quindi strettamente associato al concetto, caro ai professionisti della sicurezza, che dice che il grado di sicurezza è direttamente proporzionale a quello del suo anello più debole.

Nel Gruppo A2A questa tipologia di rischio è gestita dai nostri risk owner che si avvalgono del supporto dei risk specialist (la Direzione Digital & Innovation per la parte legata alle forniture IT, la Supply Chain per la parte di procurement e la Direzione Group Security &Cyber Defence per la parte relativa ai rischi appunto di security) il tutto in modo coerente con il nostro modello di Enterprise Risk Management (ERM).

In qualità di responsabile di tutto il processo di security di Gruppo riferisco al nostro Comitato Controllo Rischi l'andamento dell'esposizione alle minacce rispetto agli asset e ai processi e do una sintesi dei piani di mitigazione del rischio in modo da consentire di avere al nostro board aziendale una vista coerente alla strategia aziendale.

Quali metodologie vengono utilizzate nel ciclo di procurement per la qualificazione del fornitore e per valutazione preventiva della sicurezza dei prodotti e servizi?

Ogni organizzazione adotta il modello più congeniale al proprio business e in generale alle proprie esigenze per qualificare il proprio fornitore di beni e servizi in ambito digital (IT e OT) per garantire livelli di sicurezza adeguati al grado di rischio misurato dall'organizzazione stessa. Occorre individuare a priori alcuni indicatori che devono essere utilizzati per misurare il prospect che chiede di qualificarsi per una determinata fornitura di beni o di servizi: si può partire dalla compliance normativa e tecnica per clusterizzare alcuni requirement. Apparentemente più semplice potrebbe essere direttamente "certificare" i prodotti, sicuramente più impegnativo e sfidante invece qualificare i servizi.

In questo senso, A2A estende e adegua il proprio processo di risk management integrandolo anche nell'ambito della supply chain. Le valutazioni sono incrementali, seguono il processo di acquisti con verifiche specifiche per ogni fase, dalla qualifica del fornitore sino alle successive eventuali fasi di gara per l'acquisto di prodotti o servizi, e inoltre sono adeguate al contesto di fornitura stessa.

L'obiettivo è duplice, da un lato qualificare il fornitore che si appresta ad avviare una partnership con A2A in termini di maturità della sicurezza, avendo una ragionevole certezza che sia gestita secondo i principi definiti nelle nostre policy aziendali e non vi siano rischi o addirittura minacce attive che possano "trasferirsi" o rappresentare una vulnerabilità per l'azienda. Questi sono controlli "all'ingresso" su specifiche classi merceologiche e continuativi a campione. In secondo luogo, all'interno delle specifiche gare è previsto il supporto secondo il principio della security by design con requisiti tecnologici e clausole di sicurezza. Queste ultime rappresentano anche la base degli audit verso i fornitori svolti a campione sui contratti in essere.

Quali processi di monitoraggio del fornitore vengono attuati in fase di esercizio?
Poiché, come abbiamo anticipato, gli scenari sono mutevoli, occorre prevedere un monitoraggio continuo del fornitore (e/o della fornitura) durante la fase di esercizio, durante il normale svolgimento della fornitura. Va da sé che bisognerebbe aver previsto alcune clausole nel contratto che garantiscano questo monitoraggio in continuum in modo che il rapporto tra cliente e fornitore sia sempre improntato

alla massima trasparenza e ad un fruttuoso e costruttivo scambio di informazioni. Occorre definire i parametri, ad esempio, la cui variazione entro certe soglie, scateni un processo di confronto ed analisi della situazione (in questo caso anche la gestione dei cosiddetti near miss può essere un elemento interessante da adottare).

In A2A, verifichiamo l'adeguatezza della sicurezza e la conformità alle clausole all'interno di attività di audit e assessment specifiche a campione e sulla base dell'importanza del servizio o prodotto in termini di business impact analysis. Oltre a ciò, un secondo aspetto fondamentale sono le attività svolte dal nostro Cyber Defence Center che ci permette di avere una fotografia sul grado di rischio attuale della nostra catena attraverso le sue analisi continuative di Intelligence svolte con duplice modalità ad ampio spettro e sui fornitori in perimetro. Questo è ciò che intendiamo in A2A per approccio preventivo e proattivo.

E' possibile avere una visione generale del processo strutturato di "third party risk management -TPRM" che integra la raccolta delle informazioni nell'intero ciclo di vita della fornitura?

Molte organizzazioni mature, il più delle volte già soggette a compliance normative molto stringenti, hanno adottato, o stanno per farlo, un processo strutturato di TPRM, che rappresenta un buon presidio preventivo e proattivo per la sicurezza delle forniture di beni e servizi.

Nel Gruppo A2A, sfruttando le potenzialità di piattaforme informatiche di raccolta di informazioni, si mettono a fattor comune le evidenze per andare ad approfondire nel caso di necessità quanto rilevato. Ripeto, è più facile se si tratta di prodotti, diventa più difficile analizzare una fornitura di servizi in assenza di indicatori predefiniti.

Quali sono le principali strutture organizzative e quali sono i ruoli interni coinvolti nel processo TPRM?

Il processo di TPRM vede interagire diverse funzioni e presidi aziendali: in primissima battuta il modello deve essere conforme all'ERM, pertanto deve essere condiviso con il Chief Risk Officer aziendale (laddove previsto organicamente). Inoltre tale valutazione deve essere fatta in strettissima collaborazione con il procurement aziendale e il business (o comunque la funzione che normalmente richiede l'acquisto della fornitura o servizio).

Nel Gruppo A2A la gestione del processo è curata da una funzione indipendente e che esprime controlli di secondo livello all'interno dell'organizzazione, al fine di

garantire la corretta segregazione dei compiti: la Direzione Group Security & Cyber Defence ha proprio il compito di orchestrare queste attività.

Ritengo che in una azienda complessa e articolata (come un gruppo), il naturale presidio dovrebbe essere quello della Corporate Security, massima espressione della governance e del monitoraggio dei processi funzionali a garantire la sicurezza e la continuità del business.
FineIntervista

14. CONCLUSIONI

Le best practice nella gestione del rischio legato ai fornitori raccomandano attività di controllo preventivo, monitoraggio, diffusione di notifiche di sicurezza e richiesta di scambio di informazioni. L'ideale sarebbe essere in grado – anche quando la supply chain è lunga e variegata – di attivare le giuste contromisure ogni qualvolta si identifichi una vulnerabilità, anche in prodotti o servizi di terzi, attraverso un monitoraggio continuo e un sistema di risposta quanto più possibile immediato ed esteso a tutti i livelli. A causa però di diversi livelli di maturità dei diversi attori, oltre che per la loro numerosità, può diventare uno sforzo immane, soprattutto nel caso di PMI.

L'iniziativa non può quindi più essere demandata al singolo: serve uno sforzo collettivo, azioni di sistema, un coordinamento più ampio con forti responsabilità da parte delle istituzioni. Interessanti a questo fine alcuni suggerimenti dell'OECD[172] che segnala le seguenti misure per incrementare la sicurezza informatica e la protezione dei dati personali nelle PMI:

- Iniziative guidate da associazioni di settore e dall'industria di riferimento;
- aggiornamento della sicurezza sfruttando le stesse supply chain, con il coinvolgimento diretto di grandi organizzazioni e multinazionali;
- nuove norme e regolamenti ad opera dei governi nazionali;
- utilizzo di soluzioni di mercato in ambito cybersecurity;
- campagne d'informazione.

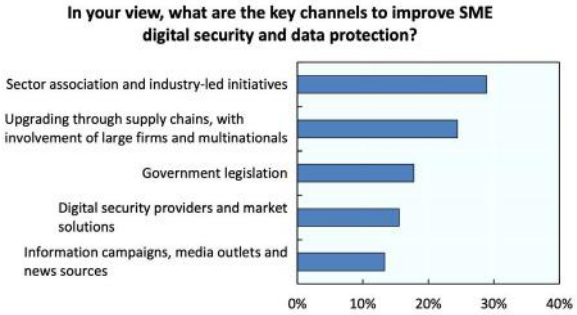


Figura 34 – Digital Security and Data Protection in SMEs[173]

172 Fonte: OECD, ottobre 2020 – https://www.oecd.org/going-digital/sme/.

173 Fonte: OECD, ottobre 2020 – https://www.oecd.org/going-digital/sme/.

A livello europeo, da segnalare anche le raccomandazioni dell'European DIGITAL SME Alliance e ECSO del 2017[174]:

- stabilire a livello europeo centri specializzati per le PMI (Hub di cybersecurity) perché possano collaborare su specifici progetti in questo ambito;
- individuare modalità perché l'offerta di soluzioni sicure fornite da PMI europee sia ben visibile agli acquirenti;
- sviluppare strategie nazionali di cooperazione territoriale, tema cruciale per aiutare le PMI ad accedere alle misure di cybersecurity;
- una revisione dei meccanismi di finanziamento di H2020, per renderli più adeguati alle necessità delle PMI.

Al riguardo può essere opportuno accennare anche alla NIS2 (paragrafo 8.2), che orienterà sempre più le grandi organizzazioni nel selezionare fornitori, comprese le PMI[175].

È necessario ricordare che un fornitore è da ritenersi un importante alleato, un'opportunità, un investimento. La scelta dei fornitori più adatti alla propria organizzazione permette di migliorare i processi, sia di business sia per fronteggiare i rischi di sicurezza informatica.

Affinché ciò si possa tradurre in una vera e propria cooperazione finalizzata, l'organizzazione deve impostare il rapporto con il fornitore non come mera relazione commerciale, bensì come partnership strategica. A maggior ragione in una realtà come quella italiana, ove i fornitori sono in genere delle micro e piccole imprese, strategiche per l'organizzazione, ma senza grosse capacità di investimento nella sicurezza delle informazioni.

L'organizzazione dovrà quindi far evolvere il suo approccio alla *supply chain*, non pretendendo che i fornitori rispettino, o meramente dichiarino di rispettare, i requisiti di sicurezza previsti, ma coinvolgendoli nella definizione della strategia da adottare per porre in sicurezza l'intera supply chain. La sinergia deve far sì che la cultura sulla sicurezza informatica nelle piccole e medie organizzazioni possa crescere, diffondersi e diventare un ulteriore aspetto strategico del rapporto cliente-fornitore, peraltro ad investimento zero, essendo attività che l'organizzazione già pone in essere al suo interno.

La collaborazione con i fornitori, però, non deve limitarsi ai soli aspetti procedurali e contrattuali, ma dovrebbe estendersi agli aspetti tecnologici e organizzativi. In tal

174 https://www.cyberwatching.eu/news-events/news/european-cybersecurity-strategy-fostering-sme-ecosystem.
175 ITimpresa, 9 agosto 2022, https://www.it-impresa.it/blog/nis2-sicurezza-dei-dati/.

senso, si potrebbe pensare a delle partnership con i propri fornitori di soluzioni di sicurezza informatica (siano esse di natura tecnologica o organizzativa) così da rendere, da un lato, più appetibili e sostenibili gli investimenti in soluzioni di sicurezza da parte dei fornitori, che potrebbero godere di prezzi vantaggiosi derivanti da tale partnership, e dall'altro avere la certezza che le soluzioni adottate dall'intera *supply chain* siano coerenti con la strategia di sicurezza delle informazioni congiuntamente definita.

15. GLOSSARIO

Asset: tutto ciò che ha valore per l'organizzazione. [Fonte: ISO/IEC 27002:2022]

Cloud service provider (CSP): fornitore di servizi cloud

Disponibilità (availability): garanzia di un accesso e un utilizzo tempestivi e affidabili delle informazioni. [Fonte: FIPS 200 NIST]

Evento: il verificarsi o modificarsi di un particolare insieme di circostanze. Un evento può consistere in uno o più episodi e può avere una pluralità di cause e di conseguenze. Un evento può essere anche qualcosa che ci si attende che non accada, oppure qualcosa che non ci si attende che accada. Un evento può essere una fonte di rischio. [Fonte: Guida ISO/IEC 73]

Incidente: un evento che è stato valutato come avente un effetto effettivo o potenzialmente negativo sulla sicurezza o sulle prestazioni di un sistema. [Fonte: ENISA]

Information security: conservazione della riservatezza, integrità e disponibilità delle informazioni. [Fonte: ISO/IEC 27000:2018]

Integrità (integrity): protezione contro la modifica o la distruzione impropria delle informazioni e include la garanzia del non ripudio e dell'autenticità delle informazioni. [Fonte: FIPS 200 NIST]

Minaccia (threat): un evento che può non essere dannoso all'origine ma che può danneggiare o compromettere un'attività a seguito di un attacco. [Fonte: AGID]

Mitigazione del rischio: strategia di gestione del rischio che prevede di ridurre le vulnerabilità mediante l'applicazione di una o più misure di sicurezza.

NIS (network and information systems): Direttiva europea (2016/1148) sulla sicurezza delle reti e dei sistemi informativi adottata nel 2016. Trattandosi di una direttiva, ogni Stato membro dell'UE ha successivamente emanato una legislazione nazionale di recepimento della direttiva. Tale recepimento nazionale da parte degli Stati membri dell'UE è avvenuto nel 2018. [Fonte: ENISA]

NIS2: Direttiva europea che, una volta definitivamente adottata, sostituirà l'attuale

Direttiva NIS. [Fonte: ENISA]

Operational technology (OT): Sistemi o dispositivi programmabili che interagiscono con l'ambiente fisico (o gestiscono e controllano dispositivi che interagiscono con l'ambiente fisico). Ne sono un esempio i sistemi di controllo industriale, i sistemi di gestione degli edifici, i sistemi di controllo antincendio e i meccanismi di controllo degli accessi fisici. [Fonte: NIST SP 800-37 Rev. 2]

Operatori di servizi essenziali (OSE): soggetti pubblici o privati, tenuti all'adeguamento ai requisiti della Direttiva NIS, che soddisfano criteri specificati dalla stessa Direttiva. [Fonte: Decreto Legislativo n. 65 del 2018 di attuazione della direttiva (UE) 2016/1148]

OSINT (Open Source Intelligence): attività di raccolta e analisi di dati, pubblicamente disponibili, per scopi di intelligence

Procedura: modo specificato per svolgere un'attività o un processo [Fonte: ISO 9000:2015]

Processo: insieme di attività correlate o interagenti che utilizzano input per fornire un risultato previsto [Fonte: ISO 9000:2015]

Processo di gestione del rischio (risk management process): l'applicazione sistematica di politiche, procedure e pratiche di gestione alle attività di comunicazione, consulenza, definizione del contesto e identificazione, analisi, valutazione, trattamento, monitoraggio e riesame del rischio. [Fonte: ISO Guide 73:2009 e ISO/IEC 27000:2018]

Propensione al rischio: (o amore per il rischio) se un agente preferisce sempre una data quantità aleatoria rispetto a ottenere il suo valore atteso con sicurezza. [Fonte: Wikipedia]

Progetto: sforzo temporaneo per raggiungere uno o più obiettivi definiti [Fonte: ISO 21502:2020]

Rischio accettabile: il livello di rischio residuo che è stato valutato essere un livello ragionevole di potenziale perdita o interruzione per un sistema specifico. [Fonte: Critical Infrastructure Assurance Office USA]

Riservatezza (confidentiality): Preservazione delle restrizioni autorizzate all'accesso e alla divulgazione delle informazioni, compresi i mezzi per proteggere la privacy e le

informazioni proprietarie. [Fonte: FIPS 200 NIST]

Rischio residuo: parte di rischio rimanente dopo l'applicazione delle misure di sicurezza. [Fonte: NIST]

Sistema di gestione (management system): insieme di elementi interconnessi o interagenti di un'organizzazione per stabilire politiche, obiettivi e processi per raggiungere tali obiettivi. [Fonte: ISO/IEC 27000:2018]

SolarWinds (caso): azienda USA di cybersecurity, nel 2020 ha subito un attacco hacker, caso di "supply-chain attack" realizzato con strumenti avanzati.

Stakeholder: qualsiasi individuo, gruppo o organizzazione che può influenzare, essere influenzato da, o percepire di essere interessato da un rischio. [Fonte: Guida ISO/IEC 73]

Supply chain: rete di organizzazioni coinvolte nelle attività di produzione o di erogazione di servizi fino al cliente o utente finale. [Fonte: ISO/TS 22318:2015, con modifiche]

Supply chain attack: attacco che prevede di attaccare un obiettivo utilizzando asset di un suo fornitore, precedentemente compromessi.

Threat intelligence: Informazioni sulle minacce che sono state aggregate, trasformate, analizzate, interpretate o arricchite per fornire il contesto necessario ai processi decisionali. [Fonte: NIST SP 800-150]

Titolare del rischio (risk owner): persona o entità con la responsabilità e l'autorità per gestire un rischio. [Fonte: ISO Guide 73:2009]

Vulnerabilità: l'esistenza di una debolezza, un errore di progettazione o di implementazione che può portare ad un evento imprevisto ed indesiderato che compromette la sicurezza del sistema informatico, della rete, dell'applicazione o del protocollo coinvolto. [Fonte: ITSEC]


ARISK


CASSA
CENTRALE
BANCA
CREDITO COOPERATIVO
ITALIANO


CBA


ConsAL
di Longhi Andrea
Consulting Services


CSI
your digital partner


CSQA


CYBER PARTNERS


CYBERTECH
ENGINEERING GROUP


DI.GI. Academy


DITEN


eni


plenitude

Supply Chain Security


GODOLI
RAS


PKF


Pluribus One
pioneers on adversarial machine learning


PQE GROUP
GLOBAL QUALITY SOLUTIONS


Qualys
Continuous Security


REXILIENCE
#BEYOND_CYBERSECURITY


S2E
business & technology consultants


sernet
MANAGEMENT
ADVISORY


ServiTecno


STELLA McCARTNEY


LA&P
legal and tax counsel


vmware

16. AUTORI, CONTRIBUTORI E RINGRAZIAMENTI

16.1 Editor e team leader

- Orlando Arena - Consulente, Cyber Risk Management & Digital Innovation
- Fabrizio Bulgarelli - PKF GODOLI RAS, Partner
- Andrea Cabras - Webuild S.p.A., Cyber Security Expert
- Cesare Gallotti - , Consulente di sicurezza delle informazioni, qualità e privacy
- Francesca Gatti - CLUSIT
- Valeria Lazzaroli - Arisk, Chief Risk Officer
- Alberto Leporati - Università degli Studi di Milano-Bicocca, Professore Associato; Comitato Scientifico Clusit
- Paola Meroni - Whirlpool Corporation, Global Privacy Manager
- Roberto Obialero - CLUSIT, Consiglio Direttivo; Membro di ECSO-CISO European Community; S2E, CISO & Manager BL Cybersecurity Advisory & Compliance
- Manuel Angelo Salvi - GRC Team, ISO 27001 e GDPR Consultant, DPO
- Silvia Stefanelli - Studio Legale Stefanelli & Stefanelli, Avvocato
- Mario Testino - ServiTecno, COO e Consigliere
- Alessandro Vallega - CLUSIT, Coordinatore Community for Security

16.2 Autori

- Riccardo Abeti - EXP Legal, Founding Partner, specializzato in “Privacy e diritto delle nuove tecnologie”
- Davide Agostinello - Comparto sanitario pubblico, Collaboratore Tecnico
- Davide Ariu - Pluribus One, CEO
- Andrea Arrigoni - Sanofi S.r.l, IT Country Leader
- Giovanni Belluzzo - InfoCert, Head of Cyber Security & Management System, Chief Information Security Officer

- Manfredi Blasucci - Qualys Inc., Senior Security Solution Architect
- Milena Boetti - Cassa Centrale Banca, IT Security Governance Specialist
- Raffaele Borrelli - Revo Insurance SpA, Cyber & Technology Underwriter
- Angelo Bosis - Oracle, Technology Architect Director
- Giuseppe Brando - ENI, Head of Cyber Threat Analysis and Research
- Fabio Bucciarelli - Cybertech - Engineering Group, Solution Architect Master
- Giancarlo Butti - Esperto privacy e sicurezza
- Dario Carnelli - Codd&Date Suisse, IT Strategy & GRC Advisor
- Andrea Castello - CSQA Certificazioni, Digital Improvement and Development Executive Manager
- Marco Ceccon - Deloitte Risk Advisory, Director
- Federico Cerutti - Università degli Studi di Brescia, Ricercatore Rita Levi-Montalcini e Professore Associato
- Mauro Cicognini - CLUSIT, Founding Partner
- Coreena Corgado - Unicredit, Cyber Security Specialist
- Igino Corona - Pluribus One, Chief Technology Officer
- Rita Eva Cresci - IUSINTECH, Innovation Lawyer
- Giuseppe Cusello - Cyber Partners S.p.A. (Gruppo RINA), GRC Director
- Carlo Di Giangiacomo - Unicredit, Head of Group BC & Resilience Methodology
- Giorgia Dragoni - Politecnico di Milano, Researcher at Osservatori Digital Innovation
- Elenio Dursi - CLUSIT, IT project manager and Scientific Committee Board Member at Clusit
- Ambrogio Ferretti - A2A, Senior IT Auditor
- Enrico Ferretti - Protiviti, Managing Director
- Giovanni Battista Gallus - Array studio legale, Avvocato; Fellow Centro Nexa su Internet e Società; membro Advisory Board Osservatorio Droni Polimi
- Chiara Gatti - UnipolSai Assicurazioni s.p.a., Responsabile Sottoscrizione Rischi Cyber (head of cyber risk underwriting)
- Patrizia Gona - Cybertech - Engineering Group, Presale Manager Security Architect
- Carlo Guastone - Sernet spa, Vicepresidente Business Development
- Anna Iorio - CBA Studio Legale e Tributario, Avvocato – Privacy & Intellectual

Property and Technology

- Anna Italiano - Partners4Innovation, Avvocato - Senior Legal Consultant
- Lorenzo Ivaldi - DITEN. Università di Genova, SysAdmin (funzionario tecnico), docente a contratto
- Franco Lazzari - IBM Italia, Cybersecurity Consultant
- Veronica Leonardi - Cyberoo S.p.A., Executive Board Member and Chief Marketing Officer
- Federica Maria Rita Livelli - Business Continuity & Risk Management Consultant; ANRA - Board Member; BCI ITALY CHAPTER - Board Member; CLUSIT Scientific Committee
- Marco Locatelli - Rexilience, CEO
- Andrea Longhi - ConsAL, Consulente Direzionale
- Lorena Manco - UnipolSai Assicurazioni s.p.a., Sottoscrittore Rischi Cyber (Cyber risk underwriter)
- Davide Manconi - Plenitude, Cyber Security Manager
- Franco Marconcini - Electrolux Professional, CISO
- Andrea Mariotti - EY, Associate Partner Cybersecurity & Digital Protection
- Stefano Mastella - Studio ing. Stefano Mastella, Titolare
- Luigi Mauro - Protiviti, Manager
- Savino Menna - Studio LA&P, Avvocato Senior Partner - Head of Tech Law, Cybersecurity & Data Protection Department
- Riccardo Modena - Sernet spa, Manager delle Lines of Business “ICT Governance” e “ICT Security”
- Enzo Mudu - IBM Consulting, Business Sales & Delivery Executive - Security & Privacy e Chief Information Security Officer presso DOCK (an IBM Company)
- Raffaele Munari - MM spa, Responsabile ICT Governance
- Michele Onorato - Westpole, CISO & Security BU Manager
- Paolo Ottolino - ISC2 Chapter-Italy, PMP CISSP-ISSAP CISA CISM OPST ITIL
- Enrico Palmerini - Università degli Studi “G. d’Annunzio” Chieti-Pescara, Responsabile Settore Help Desk Informatico
- Gian Fabio Palmerini - Webuild S.p.A., Information & Cyber Security Senior Manager
- Ignazio Parrinello - Mead Informatica, Responsabile Compliance

- Maurizio Pastore - Liguria Digitale, Responsabile servizi Privacy
- Maria Roberta Perugini - IUSINTECH, Avvocato
- Pieraldo Pistocchi - MM spa, CISO
- Riccardo Ranza - , Consulente IT e Security
- Roberto Raspatella - Oracle, Senior Technology Specialist
- Roberto Reale - Agenzia per l'Italia Digitale, Project Manager
- Andrea Rui - CLUSIT, CISA, CBCP, CCSK, Consulente IT e Security
- Corrado Salvemini - Stella McCartney, Head of IS&T Security
- Martina Santi - PKF Godoli Ras Srl , Assistente legale
- Sofia Scozzari - HACKMANAC, CEO & Founder - CLUSIT, Membro del Direttivo
- Eliana Sessa - MunichRe, Cyber Underwriter
- Mattia Spagnoli - VMware, Lead Solution Engineer, Security
- Giulio Spreafico - AIEA, Auditor di Sistemi Informativi e Consulente Rischi ICT, Sicurezza e Privacy
- Claudio Telmon - CLUSIT, Membro del Direttivo Clusit
- Andrea Tomassi - Di.Gi. Academy, Cyber Security Manager
- Guglielmo Troiano - Grant Thornton, Manager Data Protection Services
- Elena Vaciago - THE INNOVATION GROUP, Research Manager
- Roberto Veca - Cyberoo S.p.A., Head of Cybersecurity
- Enzo Veiluva - CSI Piemonte, DPO
- Luca Verderame - Talos Security,
- Sylvio Verrecchia - Supply Chain Cyber Security Risk Manager
- Gianfranco Vinucci - PCAutomotive, Chief Operating Officer
- Luca Zammarchi - PQE Group, Digital Governance International Delivery Director
- Fabrizio Zarri - Oracle, Cloud Security Advisor

16.3 Contributori

- Sergio L. Insalaco - UnipolSai, Responsabile Governance Standard, Continuità e Sicurezza dei servizi informatici

- Alessandro Maria Manfredini - Direttore di Group Security e Cyber Defence del Gruppo A2A e Presidente dell'Associazione AIPSA Associazione Italiana Professionisti della Security Aziendale
- Alessandro Marzi - Responsabile Cyber Defence e CISO del Gruppo A2A
- Gianbattista Piacentini: Head of Digital Security Validation at UniCredit

16.4 Ringraziamenti

Ha aiutato nella realizzazione di questo libro Sara Obialero per la grafica, impaginazione e per il logo e la copertina.

Il perché di questo libro

Negli ultimi mesi è emerso con grande evidenza il problema della sicurezza della catena di fornitura. Sono innumerevoli e in crescita gli attacchi veicolati alle aziende e organizzazioni pubbliche e private che sfruttano la connessione digitale tra i diversi soggetti e la scarsa comprensione della responsabilità reciproche in merito alla sicurezza delle informazioni e della cybersecurity.
Alcune dinamiche emergenti sono:

- incremento della superficie di attacco;
- mutamento delle strategie dei cybercriminali attraverso una semplificazione degli attacchi e un orientamento verso i soggetti deboli della supply chain;
- investimenti in sicurezza informatica disomogenei, con le grandi realtà che detengono strumenti, risorse e conoscenze, mentre le PMI, per mancanza di budget, scarsa formazione, consapevolezza e sensibilità, ne rimangono scarsamente dotate;
- permanenza di un problema culturale, dove microimprese e PMI ritengono erroneamente di non essere un bersaglio, dotandosi conseguentemente di un livello di sicurezza inadeguato al contesto attuale.

Purtroppo, la crescente interconnessione tra le varie organizzazioni fa sì che la debolezza di un solo anello della catena permetta l'accesso ai dati e alle reti dei committenti e di tutta la filiera. Diviene perciò fondamentale per il management comprendere come lo scenario descritto possa interessare la propria organizzazione e a quali rischi essa è esposta, considerando tutte le
tipologie di servizi ICT interni o esternalizzati.
Lo scopo di questo libro non è soltanto quello di aiutare i clienti a comprendere cosa chiedere ai propri fornitori, ma anche quello di aiutare i fornitori a prepararsi a sostenere le possibili (e sempre più probabili) richieste dei propri clienti.

Prima edizione: marzo 2023

https://supplychainsecurity.clusit.it/

SUPPLY CHAIN SECURITY

L'importanza di conoscere e gestire i rischi della catena di fornitura

Supply Chain **Security**

TOP