Il cyber risk management della supply chain

a cura di Francesco Calì, Alessandro Lamesa, Domenico Ricco, Enrico Fazio

Il caso di questo articolo affronta un progetto che mira a proporre una concreta soluzione su come affrontare e gestire il rischio cyber della Supply Chain: dalla qualificazione dei fornitori all'assegnazione delle forniture.

L'intervista ad Alessandro Lamesa e Domenico Ricco di ELETTRONICA S.p.A. permetterà di illustrare gli obiettivi, le attività, le fasi del progetto e i risultati ad oggi ottenuti.

PRESENTAZIONE SOCIETÀ

Elettronica fondata nel 1951 è tra i principali leader mondiali nel settore della difesa elettronica. Fornisce attualmente 3000 sistemi ai governi di 30 paesi nei 5 continenti, ed è a bordo dei principali programmi della Difesa europei, tra cui l'Eurofighter. Con sedi di rappresentanza in Europa, Medio Oriente e Asia, Elettronica combina l'eccellenza italiana con una visione internazionale. Ha tra i propri pilastri il people care e l'innovazione permanente. Investe volontariamente ogni anno circa 13 milioni di euro in R&S. Negli ultimi 5 anni ha conseguito la certificazione Great Place to Work ed è entrata tra le Best Workplaces, la classifica delle migliori aziende in cui lavorare in Italia e anche in Europa, unica società della Difesa italiana mai menzionata in questa classifica.

È inoltre nella classifica dei Most Attractive Employers italiani del 2022, stilata da

Francesco Calì
Managing director
Valeo-in

Alessandro Lamesa
Head of Indirect Sourcing
Elettronica S.p.A.

Domenico Ricco
Head of Quality & Performance Sourcing
Elettronica S.p.A.

Universum Global, società leader mondiale dell'Employer Branding. Fa parte di Elettronica Group a cui appartengono anche, CY4GATE, specializzata in Cyber security e Cyber Intelligence, Elettronica Gmbh, controllata tedesca centro di eccellenza europeo nella Homeland Security e EltHub specializzata in R&D e fast prototyping.

DESCRIZIONE DEL PROGETTO

In questi anni è diventato sempre più strategico garantire la continuità di business dei principali fornitori chiave. Per raggiungere questo obiettivo è fondamentale poter gestire proattivamente il potenziale rischio dell'acquisto e a consuntivo attivare un piano di risposta e risoluzione dello stesso. Tra tutti i principali rischi legati alla supply chain di natura economica, politica, sociale, tecnologica, ambientale, etica e legale, il rischio cyber sta ottenendo sempre più attenzione. La sicurezza cibernetica è infatti uno dei fondamentali ambiti sui quali il Piano Nazionale di Ripresa e Resilienza (PNRR) si è concentrato.

Il DPCM del 30 luglio 2020, n.131, ha fornito i criteri per l'individuazione dei soggetti inclusi nel Perimetro Nazionale di Sicurezza Cibernetica (PNSC): «Qualunque soggetto pubblico o privato che fornisca un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato».

Tutte le attività di compliance, richiedono la redazione di programmi di prevenzione e risk management, aggiornamenti periodici degli stessi, corsi di formazione per il personale, training specifici e attività pratiche come ad esempio il red teaming, con simulazioni di attacchi cibernetici reali posti in essere all'insaputa dell'utente e i penetration test, con l'obiettivo di individuare le vulnerabilità dei sistemi e testarne la resilienza.

I soggetti rientranti nel PNSC devono essere tenuti ad un meticoloso controllo relativo alla qualificazione dei beni, dei servizi oggetto e dei propri contratti di fornitura al fine di adempiere agli obblighi. Diventa quindi fondamentale, per tutti i soggetti pubblici o privati, implementare il controllo, la qualificazione e il monitoraggio costante della propria catena di fornitura.

Elettronica ha già da anni in essere un robusto e complesso sistema di gestione dei rischi della propria supply chain basato sul calcolo dell'affidabilità del fornitore e del rischio di fornitura. L'attuale sistema riceve come input molte informazioni provenienti dai questionari di accreditamento/qualifica (che valutano la compliance rispetto a normative vigenti, etica, lavoro, personale), dal Vendor Rating Qualità e Temporale, dal risultato degli Audit di qualifica, da questionari di gradimento interni, dai report di solidità finanziaria.

Tuttavia, nel contesto e per le ragioni sopra riportate, Elettronica, essendo soggetto incluso nel perimetro del PNSC, ha deciso di promuovere iniziative di valutazione delle terze parti dal punto di vista del rischio di sicurezza informatica così da arrivare ad un numero sempre più ristretto di cosiddetti "high risk cyber-supplier".

Per tale valutazione Elettronica ha deciso di avvalersi del supporto della sua consociata CY4GATE S.p.A., società quotata a Euronext Growth Milano, operante nel mercato cyber a 360 gradi e capace di soddisfare le più particolari esigenze di Cyber Intelligence & Cyber Security. Il caso specifico vede l'attuazione di ProntoCyber® che rappresenta la concreta risposta a queste tre principali esigenze:

- Visione d'insieme dello stato di esposizione ai «cyber risk» dei fornitori chiave di Elettronica;
- Monitoraggio costante della cyber posture dei suoi fornitori;
- Implementazione di attività di sicurezza ed irrobustimento cyber della sua supply chain.

Il contesto in cui questa soluzione si innesta è caratterizzato da uno scenario in cui:

• I fornitori saranno obbligati ad essere conformi tecnicamente e negli elementi di mitigazione del rischio basati su contratto con una sicurezza che supporti gli scopi dell'impresa;

• Gli attori pubblici e privati dovranno quindi promuovere iniziative di valutazione della supply chain dal punto di vista del rischio di sicurezza informatica così da arrivare a un numero sempre più ristretto di cosiddetti "high risk cyber-supplier".

In breve, la soluzione adottata da Elettronica è una piattaforma para-assicurativa di pronto intervento digitale contro attacchi cyber e violazione dei dati.

La piattaforma è dedicata a professionisti, PMI e Corporate e garantisce un supporto rapido ed efficace nella gestione dei cyber-incidenti (sia dal punto di vista cyber che legale). In caso di incidente, il cliente abbonato potrà usufruire immediatamente di un supporto altamente qualificato, tecnico, cyber o legale.

L'idea di ProntoCyber® è semplice: sottoscrivere un abbonamento in «tempo di pace» permette di essere coperto in «tempo di guerra».

Oltre al supporto nella gestione degli incidenti informatici, la piattaforma prevede la fornitura di tutto il ventaglio di servizi per la cyber security.

OBIETTIVO DEL PROGETTO

Misurare, gestire e prevenire il rischio cyber della supply chain, supportare i fornitori nel miglioramento continuo, utilizzare il dato di cyber resilience nel calcolo del rischio globale fornitore, incorporare il Cyber Risk Management nelle strategie di sourcing.

Elettronica ha tradotto questo obiettivo in una soluzione che sfrutta la piattaforma la quale, grazie ad una gestione a "silos di dati" dedicati a ciascun cliente, ha permesso ad Elettronica di disporre della piena osservabilità centralizzata della propria supply chain.

Elettronica ha di fatto costruito un osservatorio diretto sul suo parco fornitori, sulla loro misura di rischio in ogni momento, sulle azioni di contenimento che intraprendono, sulle misure di rientro che attivano.

Di pari importanza è, in ottica di approccio win-win per Elettronica ed i propri fornitori, l'ampio ventaglio di misure di protezione, miglioramento della sicurezza e irrobustimento della cyber resilience che la piattaforma offre agli attori della supply chain.

Infatti, i fornitori di Elettronica accedono facilmente a servizi per aumentare la propria cyber resilience, con evidenti ricadute positive sulla riduzione del rischio e sulla continuità del business di Elettronica stessa.

LE FASI DEL PROGETTO

Il processo di gestione dei rischi **(Fig.1)**, ha permesso di definire le fasi per l'identificazione del potenziale rischio sui singoli fornitori, identificando le strategie e la definizione delle azioni preventive per la mitigazione del rischio identificato, valutato come probabilità di accadimento e magnitudo.

La piattaforma mappa le esigenze di gestione del rischio in ogni fase del processo, individuando le azioni più adatte per garantire protezione e resilienza all'intera catena di approvvigionamento. Non solo un approccio post-incident, ma un servizio esteso che va dalla Cyber Education alle attività di valutazione delle vulnerabilità.

INSTANT RESCUE
Pronto intervento digitale
- Cyber Expertise
- Consulenza legale

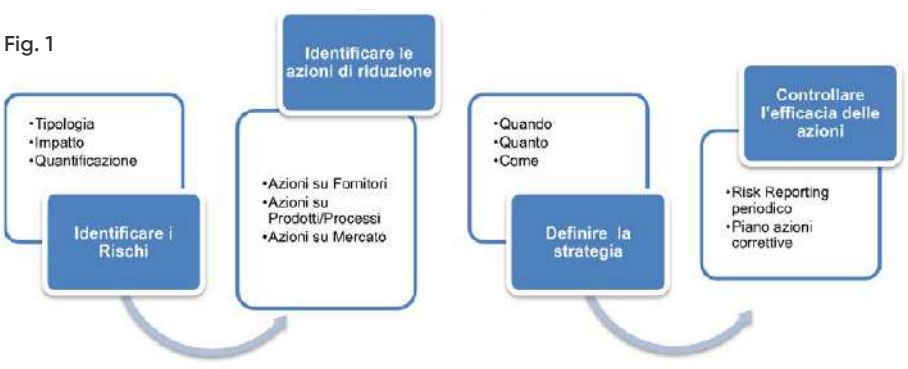
ADJACENT
Cyber Resilience
- Vulnerability Assessment
- Penetration test

ADJACENT
Cyber Awareness
- Cyber Education
- Campagne Phishing

TRANSFORMATIONAL
Policy & Procedures
- Consulenza Policy di sicurezza
- Consulenza per progettazione Architetture Cyber Resilient

TRANSFORMATIONAL
Sicurezza Gestita
- Monitoriaggio Sicurezza e gestione incidenti (SOC)
- Reportistica

Fig. 1



È stato identificato un primo set di circa 30 fornitori potenzialmente «critici» per tipologia di fornitura (business continuity) e/o per tipologia di informazioni gestite (privacy e riservatezza).

Il loro coinvolgimento è stato fatto attraverso una comunicazione che indicava la necessità di un self-assessment specifico sul cyber risk, mediante la compilazione del Risk Evaluation Form disponibile sulla piattaforma. Questo assessment è particolarmente utile per osservare e monitorare la postura di cyber risk della propria supply chain e suggerire o raccomandare azioni correttive volte a migliorarne la resilienza, attivabili velocemente e facilmente attraverso la piattaforma ProntoCyber®.

I principali risultati ottenuti

I principali benefici ottenuti sono:

• Tutti i fornitori critici monitorati in un singolo punto di osservazione che funge da centro di monitoraggio dell'intera supply chain;

• Input puntuali sulle azioni di recupero per ridurre il rischio cyber dei partner che hanno evidenziato carenze;

• Implementazione operativa delle azioni di remediation, riducendo drasticamente il cyber risk per Elettronica e per tutti i partner della sua supply chain;

• Garanzia di maggior efficacia nell'eventuale risposta agli attacchi grazie alla centralizzazione dell'informazione sulle minacce.

Alessandro Lamesa e Domenico Ricco rispondono alle domande sull'implementazione del Progetto e i risultati ottenuti:

Quali sono state le motivazioni che hanno portato ad implementare il Progetto?

Il driver principale è quello dell'irrobustimento della resilienza della supply chain. In uno scenario a complessità crescente (numerosità e intensità/magnitudo degli attacchi cyber) cresce anche il rischio indotto dalla rete di approvvigionamento che funge spesso da veicolo nella rete di attacco.

Il caso specifico di Elettronica vede l'attuazione di un prodotto, ProntoCyber®, ideato e realizzato all'interno del nostro gruppo, che rappresenta la risposta a queste esigenze:

• Visione d'insieme dello stato di esposizione ai «cyber risk» dei fornitori chiave;

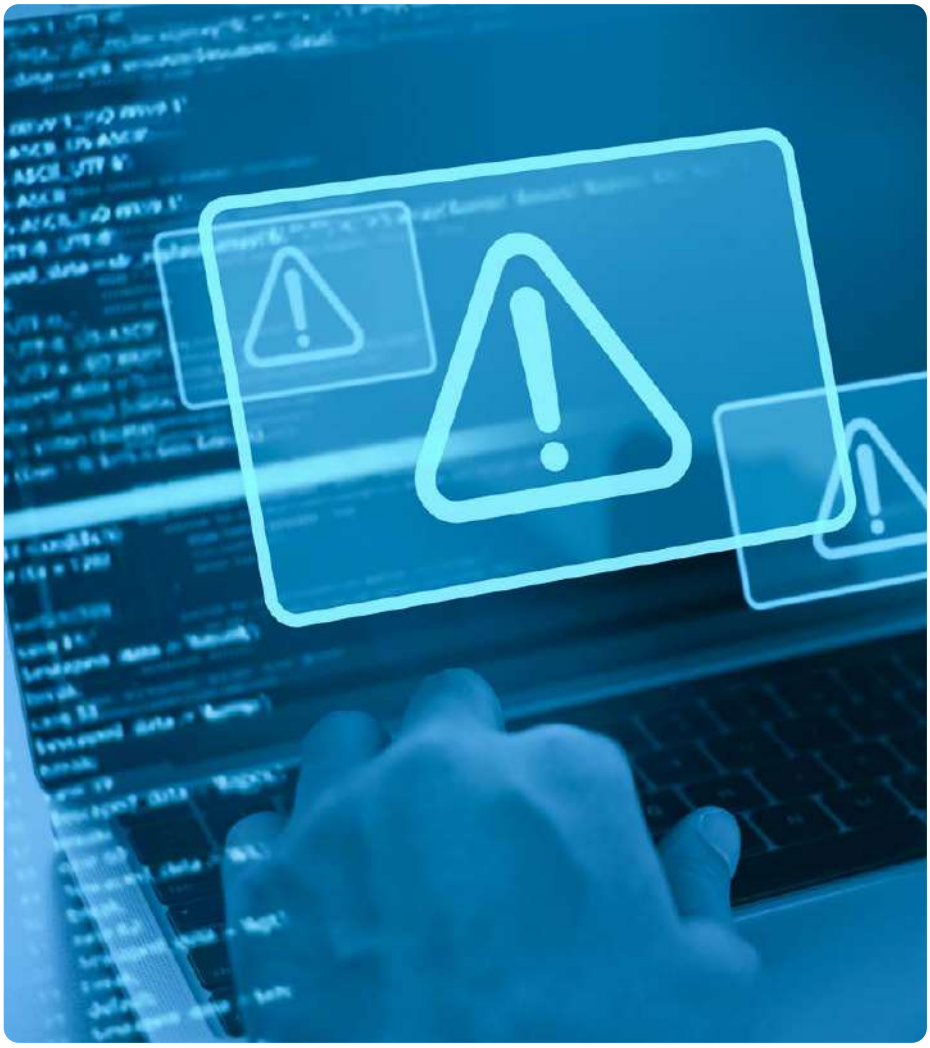
• Monitoraggio costante della cyber posture dei fornitori;

• Implementazione di attività di sicurezza ed irrobustimento cyber della supply chain.

Quali obiettivi vi siete posti con questo Progetto?

Il principale obiettivo del progetto è fornire ad Elettronica la piena osservabilità centralizzata della propria supply chain in chiave di postura del cyber rischio e relative misure di rientro per i suoi partner.

La soluzione proposta fornisce un osservatorio diretto sul parco fornitori, sulla loro misura di rischio in ogni momento, sulle misure di contenimento del rischio che possono intraprendere e sulle azioni che mettono in campo. Infatti, i fornitori di Elettronica accedono facilmente a servizi per aumentare la propria cyber resilience, con evidenti ricadute positive sulla riduzione del rischio e sulla continuità del business di Elettronica stessa.



Quali sono state le valenze del Progetto?

Il Progetto si traduce in un concreto vantaggio sia per Elettronica che per i suoi fornitori in ottica win-win:

1. La riduzione del rischio per l'interruzione delle forniture critiche a causa di un attacco cyber grazie al supporto immediato e qualificato in caso di attacco:

→ a. Con ProntoCyber® si annulla il tempo tra l'individuazione dell'attacco e l'ingaggio dei tecnici per la risposta all'incidente.

→ b. Assistenza altamente qualificata derivante da expertise ad oggi al servizio delle più grandi corporate italiane e internazionali con un team di Incident Response con un'esperienza decennale nel settore specifico.

2. Un incremento degli strumenti di difesa messi in opera da parte dei fornitori, grazie alla sostenibilità economica del modello e-commerce;

3. Un singolo gestore dell'intera rete di sicurezza per la supply chain. Questo elemento permette non solo una pronta risposta estesa, ma anche la capacità di intercettare ed anticipare potenziali eventi malevoli che verificatisi su un singolo nodo della rete potrebbero essere veicolati sull'intera rete.

Le competenze di Cyber Threat di Cy4gate a servizio di ProntoCyber® permettono di intercettare in tempo utile potenziali minacce prima che si traducano in pericolosi attacchi distribuiti sull'intera rete di approvvigionamento.

Quali sono stati i principali insegnamenti chiave tratti dal Progetto?

Il mercato necessita di soluzioni semplici, immediate ed efficaci per rispondere ad esigenze caratterizzate da una sempre maggior complessità e dinamismo: distribuzione geografica, complessità dei processi, piena ed immediata osservabilità sulla rete, Threat model in continua evoluzione. Il tutto in ottica win-win tra cliente e i suoi fornitori per garantire una adoption estesa ed a valore aggiunto per l'intera rete.

Quali sono i prossimi step che avete previsto per la gestione del Cyber Risk?

A seguito della prima fase pilota intrapresa si è deciso di:

1. Estendere la valutazione del cyber risk index a tutta la supply chain potenzialmente critica per aspetti di privacy, riservatezza e business continuity;

2. Incorporare il Cyber Risk Management nel processo di accreditamento/qualifica di nuovi fornitori, stabilendo livelli minimi di accettabilità per categorie merceologiche al processo di selezione;

3. Avviare azioni di mitigazione del rischio promuovendo formazione alle PMI ed estendere maggiormente l'adozione dei servizi ProntoCyber® offerti da Cy4gate (miglioramento continuo);

4. Includere il rischio cyber nel calcolo dell'indice di affidabilità del fornitore in modo da includerlo di conseguenza nel processo di valutazione e assegnazione delle forniture.

PROBLEMATICHE WORST PRACTICES

Principali problematiche emerse durante il progetto, soluzione implementata e suggerimenti per evitare lo stesso problema su progetti successivi.

Descrizione progetto	Principali problematiche	Soluzione implementata
Data l'importanza attuale nella gestione preventiva degli attacchi hacker sui principali dati sensibili aziendali, ELETTRONICA che opera nella progettazione, sviluppo e fornitura di sistemi di sorveglianza strategica, autodifesa e attacco elettronico per uso navale, aereo e terrestre, ha deciso di monitorare e gestire preventivamente il rischio di attacchi cyber presso tutti i principali fornitori che gestiscono dati sensibili di Elettronica e che sono strategici per la continuità di fornitura.	Il DPCM del 30 luglio 2020, n.131, ha fornito i criteri per l'individuazione dei soggetti inclusi nel Perimetro Nazionale di Sicurezza Cibernetica (PNSC): «Qualunque soggetto pubblico o privato che fornisca un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato». Tutte le attività di compliance, richiedono la redazione di programmi di prevenzione e risk management, aggiornamenti periodici degli stessi, corsi di formazione per il personale, training specifici e attività pratiche come ad esempio il red teaming, con simulazioni di attacchi cibernetici reali posti in essere all'insaputa dell'utente e i penetration test, con l'obiettivo di individuare le vulnerabilità dei sistemi e testarne la resilienza. Diventa quindi fondamentale, per tutti i soggetti pubblici o privati, implementare il controllo, la qualificazione e il monitoraggio costante della propria catena di fornitura. Elettronica ha già da anni in essere un robusto e complesso sistema di gestione dei rischi della propria Supply Chain basato sul calcolo dell'affidabilità del Fornitore e del rischio Fornitura, che non comprende il RIschio di Cyber Attack.	Elettronica, essendo soggetto incluso nel perimetro del PNSC, ha deciso di promuovere iniziative di valutazione delle terze parti dal punto di vista del rischio di sicurezza informatica così da arrivare ad un numero sempre più ristretto di cosiddetti "high risk cyber-supplier". Elettronica ha deciso di avvalersi del supporto della sua consociata CY4GATE S.p.A., società quotata a Euronext Growth Milano, operante nel mercato cyber a 360° e capace di soddisfare le più particolari esigenze di Cyber Intelligence & Cyber Security. Il caso specifico vede l'attuazione di ProntoCyber®.

IDEE DI MIGLIORAMENTO BEST PRACTICES

Idee di miglioramento (relative a tempi, costi e qualità) identificate e applicate con successo durante il Progetto e che possono essere estese ad altri progetti.

Obiettivi del progetto	Idee di miglioramento – Best Practice	Risultato ottenuto
• Misurare il rischio cyber della supply chain, supportare i fornitori nel miglioramento continuo, utilizzare il dato di cyber resilience nel calcolo del rischio globale fornitore.	**1. Estendere** la valutazione del cyber risk index a tutta la supply chain potenzialmente critica per aspetti di privacy, riservatezza e business Continuity. **2. Incorporare** il Cyber Risk Management nel processo di accreditamento/qualifica nuovi fornitori stabilendo livelli minimi di accettabilità' per categorie merceologiche al processo di selezione. **3. Avviare** azioni di mitigazione del rischio promuovendo formazione alle PMI ed estendere maggiormente l'adozione dei servizi ProntoCyber® offerti da Cy4gate (miglioramento continuo). **4. Includere** il rischio cyber nel calcolo dell'indice di affidabilità del fornitore in modo da includerlo di conseguenza nel processo di valutazione e assegnazione delle forniture.	• Tutti i fornitori critici monitorati in un singolo punto di osservazione che funge da centro di monitoraggio dell'intera supply chain. • Input puntuali sulle azioni di recupero per ridurre il rischio cyber dei partner che hanno evidenziato carenze. • Implementazione operativa delle azioni di remediation, riducendo drasticamente il cyber risk per Elettronica e per tutti i partner della sua supply chain. • Garanzia di maggior efficacia nell'eventuale risposta agli attacchi grazie alla centralizzazione dell'informazione sulle minacce.