NTT DATA
Trusted Global Innovator

Quanto sono sicuri i tuoi fornitori?

Una breve guida al Supply Chain Risk Management:
che cos'è e perché è importante per la tua cybersecurity.

WHITE PAPER / CYBERSECURITY

Indice dei contenuti

Introduzione

Gli ultimi decenni sono stati caratterizzati da un rapido e significativo sviluppo tecnologico che ha comportato cambiamenti radicali nei processi organizzativi e nella modalità di erogazione dei servizi da parte delle aziende. In particolare la collaborazione con fornitori terzi specializzati è diventata essenziale, perché i fornitori rappresentano un mezzo immediato per poter conoscere e implementare soluzioni innovative, estendere la copertura geografica, gestire e ottimizzare carichi di lavoro con competenze specialistiche, nonché snellire i processi garantendo vantaggi competitivi.
Secondo una ricerca condotta da Gartner (Stay Ahead of Growing Third-Party Risk) nel 2019, il 71% delle organizzazioni dichiara che il proprio **network di fornitori** è **nettamente superiore** rispetto ai 3 anni precedenti. La stessa percentuale di organizzazioni (71%) dichiara una prevedibile **crescita del proprio network** nei successivi tre anni.
L'ecosistema aziendale è quindi in continua evoluzione e il tema del Supply Chain Risk Management è più che mai attuale:
le organizzazioni devono adottare nuovi approcci per la gestione del rischio, tenendo in considerazione i **rischi derivanti dalle terze parti** in relazione alle attività e ai dati scambiati. In poche parole **le aziende devono assicurarsi che i propri fornitori gestiscano nel migliore dei modi i dati e le informazioni** a loro affidati, garantendo altresì i livelli di servizio concordati nel pieno rispetto dei principi di cybersecurity e conformità normativa. Una violazione della sicurezza delle terze parti può causare danni con impatto elevato e i risvolti potrebbero essere molteplici. Non sarebbe nuova la casistica in cui, ad esempio, un attacco cyber venga pianificato non solo per colpire uno specifico target (e quindi una specifica azienda), ma anche per colpire tutte le altre aziende con le quali sussistono accordi commerciali.
I rischi di cybersecurity non sono, però, relativi esclusivamente agli attacchi cyber, ma possono derivare anche da altri eventi che espongono il sistema a diversi tipi di "failure", come errore umano, frode, malfunzionamento.

QUALI IMPATTI POSSONO ESSERE GENERATI DA UN FAILURE DELLA SICUREZZA DEI PROPRI FORNITORI?

1

Impatti finanziari che spesso sono la tipologia di impatto più documentata e derivano principalmente dall'impossibilità di eorgare i servizi ai propri clienti, dai costi per ripristinare le attività operative, dalle penali contrattuali e da frodi subite. In realtà una violazione subita non è limitata ad una mera perdita economica;

2

Impatti di non conformità, relativi alla non conformità a normative di legge che impongono requisiti di protezione dei dati (es. GDPR, PCI-DSS, HIPPA) o relativi alla proprietà intellettuale;

3

Impatti sull'immagine pubblica e sulla reputazione, spesso dovuti alla divulgazione di informazioni riservate dei clienti, ad una perdita di fiducia da parte dei clienti o dei partner societari, o ancora al loro malcontento.
Gli impatti reputazionali possono derivare anche da un'errata gestione della violazione subita e/o delle comunicazioni effettuate verso l'esterno/nei confronti dei soggetti interessati dalla violazione.

È evidente che il processo di **Supply Chain Risk Management dovrebbe essere una delle priorità nei programmi di cyber security aziendali.**

Cosa significa gestire i fornitori?

La gestione dei fornitori non si limita alla sottoscrizione di un contratto di servizio, bensì richiede il controllo su molti aspetti rilevanti che i fornitori potrebbero compromettere, quali ad esempio: **la resilienza del business, la continuità dei servizi e l'integrità e la confidenzialità delle informazioni e dei dati trattati.**

Una relazione con un soggetto terzo all'azienda implica una serie di rischi che non si limitano esclusivamente alla cybersecurity. Si pensi ad esempio ai rischi operativi (il rischio che una terza parte possa causare l'interruzione del business o di un processo critico), al rischio reputazionale (il rischio che l'operato di una terza parte possa influire negativamente sull'opinione pubblica), al rischio strategico (il rischio che, a causa di una terza parte, non si possano raggiungere i propri obiettivi di business) e così via.

Come si può operare implementando una gestione efficace ed efficiente del rischio derivante da terze parti?

La gestione dei fornitori è sempre più spesso affiancata al concetto di *"Supply Chain Risk Management*.
Gartner definisce il Supply Chain Risk Management come: **"il processo atto a garantire che i fornitori di servizi e i fornitori IT non creino una potenziale interruzione del business o un impatto negativo sulle prestazioni aziendali. Il Supply Chain Risk Management è a supporto delle aziende che devono valutare, monitorare e gestire la propria esposizione al rischio derivante da terze parti che forniscono prodotti o servizi IT o che abbiano accesso alle informazioni aziendali"[2].**
L'implementazione di un programma ben strutturato di Supply Chain Risk Management consente di identificare e mitigare tempestivamente i rischi sopra menzionati.

[2] Gartner Glossary - https://www.gartner.com/en/information-technology/glossary/vendor-risk management

In che cosa consiste un programma di Supply Chain Risk Management? Di seguito i 4 punti cardine da considerare:

1. **"FARE ORDINE"**

È fondamentale sapere "chi" c'è all'interno della nostra azienda e a "cosa" accede: si tratta del primo e imprescindibile step per sapere quali fornitori accedono a quali dati personali e/o riservati e come possono operare con essi.

2. **CLASSIFICARE I FORNITORI**

Ogni fornitore precedentemente identificato dovrà essere classificato, almeno, in base alla tipologia di:

- **servizio offerto** (es. outsourcer, service provider)
- **informazioni/dati trattati**
- **tipologia e modalità di accesso a sistemi e/o reti proprie e/o del committente**.

La classificazione consentirà di **associare a ciascun fornitore il livello di rischio** a cui si sta esponendo l'azienda committente. Ad esempio un fornitore che in qualità di outsourcer gestirà l'intero processo dei pagamenti di una grande banca, verrà molto probabilmente classificato come fornitore ad alto rischio, poiché sarà responsabile di un intero processo, trattando dati personali e informazioni confidenziali.

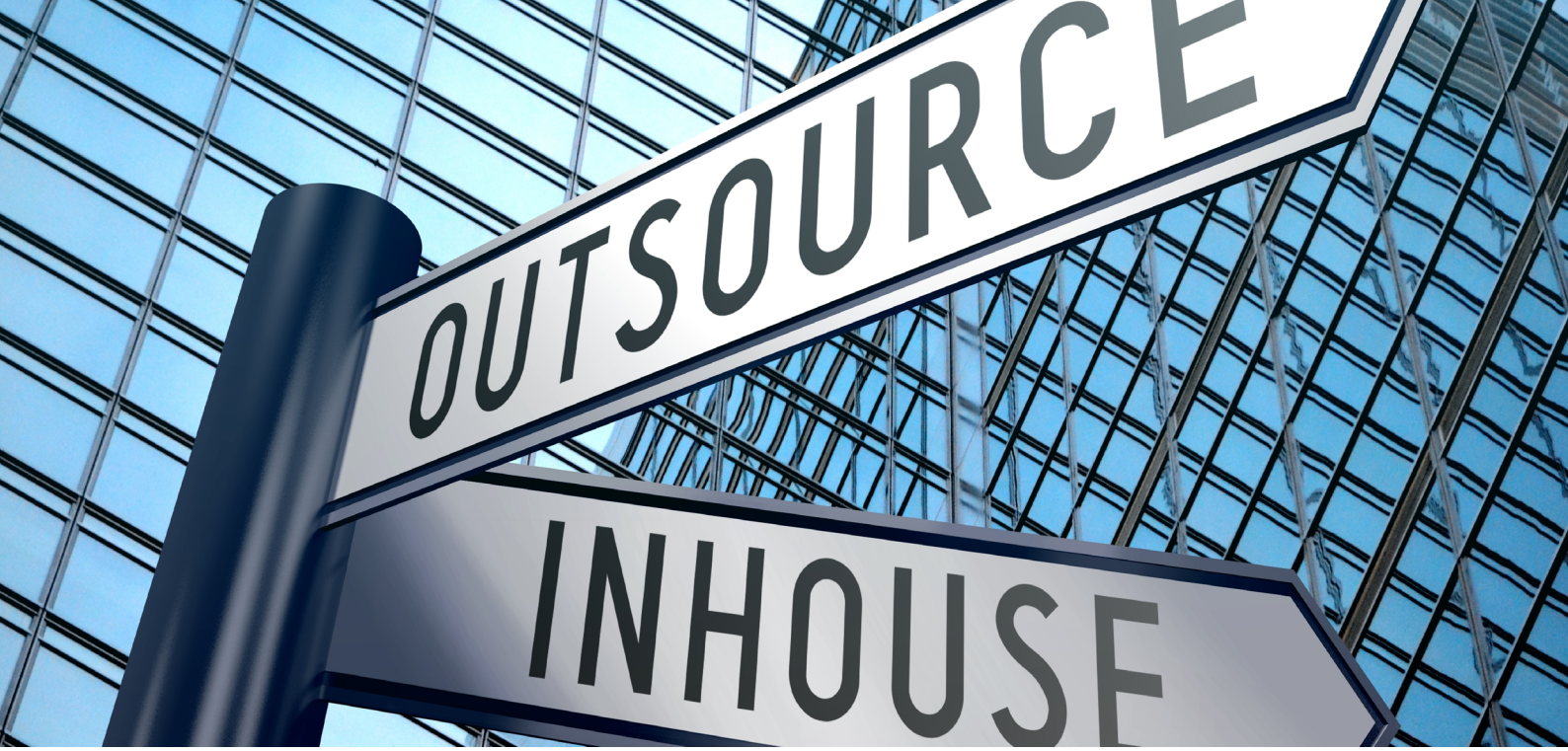
3. **VALUTARE LA SICUREZZA DEI FORNITORI (SECURITY RISK SCORING)**

È fondamentale sapere come le terze parti p**roteggano i dati e le informazioni** che trattano durante l'erogazione di un servizio. L'esecuzione della "**Supply Chain Risk Assessment**" su ciascun fornitore (o almeno sui fornitori con un alto **livello di esposizione al rischio**) consente di raccogliere informazioni circa le modalità attuate, le best practice adottate e gli standard di sicurezza implementati dalle terze parti. In questa fase sono indagati tutti gli aspetti relativi alle **misure di protezione dei dati e sicurezza** adottate per **garantire l'integrità, la sicurezza e la riservatezza dei dati.**

Tutte le attività relative alla valutazione dei fornitori potrebbero essere racchiuse in **un piano di Supply Chain Risk Management**: un documento usufruibile da entrambe le parti e che mira a definire misure di sicurezza, tipologie di accessi, SLA e altri elementi concordati tra cliente e fornitore.

Il piano deve essere strutturato facendo in modo che possa contenere:

- **le informazioni principali del fornitor**e (es. punti chiave, anagrafica);
- le **modalità** attraverso cui l'azienda si riserva la possibilità di effettuare le **analisi** e le **verifiche** (es. checklist o requisiti di cybersecurity e data protection);



- le **modalità** attraverso cui il fornitore intende **rimediare a eventuali scoperture**.

4. **PRENDERE DELLE DECISIONI IN BASE AL PROPRIO MODELLO DI VALUTAZIONE DEL RISCHIO**

Dopo un'attenta valutazione dei fornitori è molto probabile che segua una fase di **"remediation".** Al fornitore verrà chiesto di **migliorare e/o implementare** alcune **misure tecniche/ organizzative** e, sulla base dei **risultati e benefici ottenuti**, l'azienda committente potrà decidere di rinnovare o meno il contratto stipulato.
Un aspetto importante, spesso sottovalutato, riguarda il principio che la valutazione e gestione dei rischi potenzialmente derivanti dai propri fornitori non è limitata ad un momento unico e specifico della relazione cliente-fornitore, ma si classifica come **attività ciclica e periodica**.

Il processo di gestione e valutazione del fornitore è sicuramente da applicare all'inizio di ogni collaborazione o rinnovo della stessa, ogni qualvolta ci siano dei cambiamenti anche in ottica di **Security-by-design, ma deve essere** soprattutto un **processo continuo nel tempo**.

Tutte le organizzazioni, attraverso un approccio proattivo, dovrebbero assicurarsi che le richieste fatte ai fornitori siano in linea con le proprie aspettative e con i propri requisiti di sicurezza. L'efficacia di un programma di Supply Chain Risk Management è maggiore se integrato nel modello organizzativo aziendale, quindi se tutte le strutture impattate dal processo sono consapevoli della sua importanza (es. IT, Security, HR, Legal&Compliance, Procurement).

SE SI UTILIZZA IL TERMINE "FORNITORE", A CHI CI SI RIFERISCE?

Il **fornitore** rappresenta una persona fisica o un'azienda che **eroga servizi e/o prodotti** verso le aziende che ne fanno richiesta (clienti). Si considerano fornitori almeno le seguenti categorie:

- Produttori di beni
- Fornitori di servizi (inclusa la consulenza)
- Outsourcer
- Appaltatori (sia a breve che a lungo termine)
- Eventuale personale esterno

Perché è importante applicare un programma di Supply Chain Risk Management?

La gestione dei fornitori, come premesso, non riguarda solo la cybersecurity. È piuttosto un processo molto ampio e complesso che abbraccia le aziende in tutta la loro interezza. Definire un programma e favorirne la realizzazione e l'implementazione richiede tanti sforzi da parte delle aziende, sia in termini economici che di competenze da impiegare; tuttavia i vantaggi e i benefici che ne derivano superano di gran lunga i possibili danni (economici e non) che potrebbero verificarsi a seguito di una gestione inadeguata o del tutto assente dei fornitori.

Nella pratica, in cosa si traducono i benefici dell'avere un programma di Supply Chain Risk Management e quindi del gestire efficacemente i fornitori? Di seguito qualche esempio:

- Miglioramento del livello di sicurezza, in termini di **protezione end-to-end sui fornitori**
- Maggiori **controlli sugli accessi a dati e informazioni**
- Indirizzamento degli **audit sui fornitori** sulla base di criteri di rischi effettivi
- Maggiore tutela attraverso **clausole contrattuali** mirate per la gestione dei rischi di sicurezza
- Ottimizzazione della **gestione del rischio**: in futuro, i rischi già gestiti, richiederanno meno tempo e risorse
- **Aumento delle responsabilità** (sia da parte dell'azienda che del fornitore)
- Possibile **riduzione di costi**
- Miglioramento della **disponibilità dei servizi**

Secondo la ricerca "The 2020 Third-Party Risk Management Study" (Prevalent), le motivazioni per le quali le aziende intervistate effettuano il Supply Chain Risk Assessment sono:

PERCHÉ ESEGUIRE DEGLI ASSESSMENT SUI FORNITORI?

36 %
Ottemperamento a richieste da parte di specifici **Regulator/ Framework di settore/Normativa**

36 %
Mitigazione dei **rischi di cybersecurity** derivanti dai fornitori

17 %
Miglioramento e ottimizzazione del processo di **valutazione** dei fornitori in termini di risorse e tempo impiegati

10 %
Strategie di business

2 %
Altro

CASE STUDY 1

Data Breach BlueLeaks: online 269 GB di informazioni riservate di agenzie governative degli Stati Uniti

Il 19 giugno 2020 il noto gruppo di attivisti **Distributed Denial of Secrets** (DDoSecrets), impegnati nella diffusione di "Hacked material" dichiara con un tweet di aver reso pubblici 269 GB di dati riguardanti **rapporti di polizia ed FBI**, immagini e **video di sospettati, nomi, indirizzi, numeri di telefono, coordinate IBAN** e molto altro. I dati sarebbero stati forniti a DDoSecrets da parte del gruppo attivista Anonymous, il quale avrebbe compromesso e prelevato materiale da più di **250 siti web** sviluppati e ospitati sui **server del fornitore Netsential**, società di Houston attiva nel campo dello sviluppo web.
Secondo quanto emerso dalle indagini, tutto il materiale compromesso sembrerebbe provenire dai cosiddetti "Fusion Center", una sorta di hub telematico creato dall'amministrazione statunitense con la funzione di agevolare la comunicazione tra le agenzie governative in merito a potenziali minacce alla sicurezza nazionale.

Gli hacker avrebbero identificato una vulnerabilità in uno dei siti web, la quale gli avrebbe permesso di scaricare i dati e di compromettere consequenzialmente anche tutti gli altri siti collegati al medesimo Fusion Center.

BlueLeaks è stato definito come uno dei più **grandi attacchi hacker nei confronti delle forze dell'ordine e agenzie governative degli Stati Uniti**. Stando a quanto dichiarato da DDOSecrets, **la violazione ha permesso l'acquisizione e la pubblicazione di dati altamente confidenziali** (riguardanti stati, agenzie federali e locali USA) compromettendo di conseguenza la **sicurezza di numerosi cittadini**. È importante infatti considerare che tra le **informazioni rese pubbliche** vi sono anche **indagini in corso, operazioni sensibili ad alto rischio, civili sotto copertura con nuove identità, ma anche agenti**.
Il volume del materiale compromesso è direttamente proporzionale al rischio della sua divulgazione. Un esempio potrebbero essere le organizzazioni criminali del paese, le quali potrebbero entrare in possesso dei fascicoli a loro riguardo, stesso rischio per i soggetti indagati e quelli sotto processo.
Allo stesso tempo è significativo considerare che il materiale compromesso potrebbe anche essere fonte di grandi scandali o prova di discutibile condotta delle forze dell'odine americane, specialmente in un periodo storico di alta tensione come il medesimo.

CASE STUDY 2

Data Breach BlueLeaks: online dati di pazienti positivi al Covid-19 in Sud Dakota

Il 19 giugno 2020, il **Fusion Center del Dipartimento di Pubblica Sicurezza del Sud Dakota** è stato informato dal suo fornitore **Netsential, presso il quale deteneva informazioni altamente riservate relative a pazienti affetti da COVID-19, di essere stato vittima del Data Breach BlueLeaks**.
Come anticipato nel precedente case study, lo scorso giugno Anonymous ha attaccato i server di Netsential, società di sviluppo web e fornitore di agenzie governative degli Stati Uniti, impossessandosi di circa 269 GB di dati altamente confidenziali riguardanti dipartimenti di polizia, agenzie federali/locali e altre risorse di formazione delle forze dell'ordine USA.

A differenza di quanto accaduto nel caso precedente, dove i dati sono stati resi pubblici nell'immediato, **le informazioni confidenziali e di tipo sanitario con riferimento al COVID-19, non risultavano essere state compromesse, convinzione tuttavia svanita nel mese di agosto, quando il gruppo Hacker ha dichiarato di essere in possesso di informazioni riservate su numerosi pazienti affetti da COVID-19.**
Durante la scorsa primavera, nel pieno dell'emergenza COVID-19, numerosi **Law Enforcement Fusion Centers** hanno **sviluppato**, con il **supporto di Netsential**, un **portale online utile ad identificare e assistere gli individui positivi al virus** durante la loro situazione di degenza. Le informazioni sono state mantenute sui server sicuri di Netsential limitando l'accesso a un numero selezionato di funzionari del Dipartimento di Pubblica Sicurezza. Tuttavia, durante l'elaborazione di questi dati, **Netsential ha attribuito alcune etichette utili a ricondurre i pazienti al loro stato COVID-19**, permettendo così a terzi non autorizzati di associare facilmente i dati dei pazienti con il relativo stato di salute.

In accordo con quanto presente nella lettera pubblicata dal Dipartimento di Pubblica Sicurezza del Sud Dakota in data 17 Agosto[3], il dati compromessi a seguito della violazione potrebbero essere ancora disponibili sul Web e riguarderebbero: anagrafiche, indirizzi di residenza e stato COVID-19 dei pazienti. Inoltre, secondo quanto dichiarato dal Dipartimento, ai pazienti, i cui dati personali sono attualmente di pubblico dominio, non è ancora stata fatta una comunicazione ufficiale circa la compromissione dei dati subita dalla società Netsential.

Il sito web della società Netsential è stato reso fin da subito inaccessibile ed è la Società stessa a dichiarare che "i propri server sono stati recentemente compromessi e che attualmente è impegnata in una collaborazione con le autorità competenti al fine di risolvere la situazione". In aggiunta, la Società dichiara che, "per via delle investigazioni in corso e la confidenzialità delle informazioni coinvolte, non verrà rilasciata alcuna dichiarazione".

QUAL È IL SETTORE PIÙ COLPITO DA DATA BREACH DI TERZE PARTI?

Secondo una **ricerca** condotta dall'**Istituto Ponemon** (Michigan)[4], nel 2020 le **organizzazioni** sanitarie hanno subito, per il decimo anno consecutivo, il più **alto danno associato ai Data Breach** per un costo di $7.1M, in netto incremento rispetto a quello del 2019 di $6.45M.

Secondo quanto dichiarato dalla ricerca il valore dei **fascicoli sanitari** di un paziente è, per gli hacker, **tre volte più redditizio rispetto** a quello dei dati relativi alle **carte di credito.**

[3] South Dakota Department of Public Safety –Netsential Notification Letter - 2020
[4] Ponemon Institute - Cost of a Data Breach Report 2020 - 2020

Dai case study alle possibili strategie di mitigazione e prevenzione del rischio

BlueLeaks è stato definito come uno dei più grandi e impattanti data breach perpetrato nei confronti di Agenzie Governative Americane. Come si evince dalla descrizione dei due case study, il gruppo attivista Anonymous, attaccando il fornitore Netsential, ha creato ingenti danni a numerose agenzie governative USA, divulgando prima dati strettamente confidenziali di polizia e forze dell'ordine e successivamente informazioni riservate e relative a pazienti affetti da COVID-19.

In numerose interviste, sia il Dipartimento di Pubblica Sicurezza del Sud Dakota che le agenzie governative hanno **puntato il dito contro il fornitore Netsential scaricandosi** da qualsiasi tipo **di responsabilità** in termini di inadeguatezza a **standard di cybersecurity e protezione dei dati**. Tuttavia, data la presenza di più attori coinvolti, sorge spontaneo domandarsi:

"A chi deve essere attribuita la responsabilità? Possono questi due case study essere considerati come un esempio di inadeguata gestione della sicurezza informatica?"

In situazioni simili, si dovrebbe parlare di **duplice responsabilità**, quindi sia del cliente che del fornitore. Infatti, sebbene il cliente si sia affidato al suo fornitore per la gestione sicura dei suoi dati, si sarebbe dovuto comunque impegnare nel verificarne le modalità e la relativa applicazione delle stesse.
Come testimoniano i casi presentati, **ancora troppo di consueto si tende a sottovalutare l'importanza della sicurezza informatica e di quanto sia necessario al giorno d'oggi essere aggiornati su quelle che possono essere le minacce cyber, le loro conseguenze e quelli che invece sono gli strumenti necessari per contrastarle e ridurle al minimo.**

Qui emerge l'importanza del **Supply Chain Risk Assessment** che, all'interno del programma di **Supply Chain Risk Management**, permette di attuare un'**analisi del rischio dei fornitori** prima e durante il rapporto di business, mantenendo un monitoraggio costante nel tempo.

Il programma di Supply Chain Risk Management consente molti vantaggi, poiché permette ai clienti di gestire in sicurezza i propri fornitori, garantendo una conoscenza trasparente della loro security posture e di conseguenza anche i rischi derivanti dai propri fornitori.

Ricollegandosi al concetto di duplice responsabilità dei due case study in analisi, si può affermare che se fosse stato implementato un programma di gestione dei fornitori e un conseguente Supply Chain Risk Assessment, sarebbe stato possibile individuare la presenza di vulnerabilità significative a livello di sicurezza di sistemi, network e dati, e quindi la richiesta dell'implementazione di un piano di remediation da parte del fornitore, avrebbe potuto far evitare la violazione e i conseguenti danni.

BEST PRACTICE:
La top 10 suggerita da NTT DATA

Che cosa avrei potuto fare meglio? A cosa non ho pensato? Come faccio a coinvolgere le altre strutture? Quali e quanti fornitori lavorano con me e come faccio a controllarli? I dubbi e le domande sono sempre molti, così come le "soluzioni".

Di seguito si propone una sintesi di quelle **best practice** che, se implementate, hanno la funzione di contribuire alla creazione di un **efficace programma di gestione sicura dei fornitori,** come dimostrato dall'esperienza sul campo di NTT DATA:

1 **investire** maggiormente **nei processi di sicurezza**, sia in termini di **miglioramento** di quelli già in essere, sia di **integrazione** di quelli non attualmente presenti;

2 mettere in atto un **programma proattivo di sicurezza**, implementando, aggiornando e migliorando policy e procedure di sicurezza;

3 mantenere un'**elevata attenzione e conoscenza in materia di data protection**, così da evitare la compromissione delle informazioni di una singola azienda e di tutte quelle a essa collegate;

4 predisporre e mantenere aggiornato nel tempo un **inventario** di tutti i **fornitori** con cui l'organizzazione ha un rapporto di business, indicando a cosa ciascuno di essi accede e attraverso quali modalità;

5 **catalogare i rischi di sicurezza informatica** ai quali le terze parti potrebbero esporre l'organizzazione;

6 **classificare i fornitori** sulla base del loro **livello di criticità**, derivante dalla tipologia di dati trattati, le relative modalità di trattamento e il conseguente livello di esposizione al rischio da parte dell'azienda committente;

7 sviluppare un **sistema di controlli** utili a valutare la qualità con cui le terze parti gestiscono la **sicurezza dei dati dei committenti**;

8 garantire che tutti i **contratti** con le terze parti godano di un diritto di verifica, in termini di **controlli e requisiti di sicurezza** che i fornitori hanno in atto;

9 definire dettagliatamente l'**attività di monitoraggio** dei fornitori in termini di: tempistiche, modalità di conduzione delle **revisioni/feedback, identificazione e mitigazione di rischi**;

10 **collaborare attivamente** con le altre **funzionali aziendali coinvolte nel programma** di gestione dei fornitori (es. Audit, Procurement, Compliance, IT).

Conclusioni

In conclusione, è importante che ogni azienda inserisca all'interno della propria strategia un approccio strutturato alla valutazione dei rischi della Supply Chain.

Infatti, ogni azienda opera all'interno del proprio ecosistema che comprende i fornitori. È evidente che un qualsiasi evento negativo che impatta anche solamente uno dei fornitori, potrebbe causare un degrado del livello di efficienza e di resilienza dei servizi dell'azienda.
È opportuno, quindi, presidiare l'intero ecosistema, al fine di verificare che i fornitori garantiscano un livello di sicurezza ritenuto appropriato, in relazione al loro ruolo all'interno dell'ecosistema stesso e in base ai servizi e ai prodotti erogati.
Di conseguenza l'approccio proposto è di tipo end-to-end durante l'intero ciclo di vita del rapporto con i fornitori: dalla selezione, alla negoziazione contrattuale fino al monitoraggio costante nel tempo e al termine della collaborazione.

Key takeway

1 Una violazione della sicurezza delle terze parti può causare danni con impatto elevato; spesso la finalità di un attacco cyber è colpire l'anello debole della catena: colpendo uno specifico target, si potrebbero colpire le altre aziende con le quali sussistono accordi commerciali.

2 I rischi derivanti da una relazione con un soggetto terzo all'azienda potrebbe implicare non solo impatti sulla sicurezza ma anche impatti operativi, reputazionali ed economici.

3 L'approccio di NTT DATA al Supply Chain Risk Management consente di monitorare i fornitori affinché sia garantito il livello di sicurezza ritenuto adeguato.

4 Il processo di Supply Chain Risk Management di NTT DATA prevede la classificazione dei fornitori e la relativa differenziazione dei controlli, in relazione ai dati gestiti dai fornitori e alla tipologia del servizio erogato.

NTT DATA
Trusted Global Innovator

Daniela Mazzarone
Director

Head of Cyber Security Strategy & Governance Practice | Security

Fabiola Giambattista
Manager

Cyber Security Strategy & Governance Practice | Security

Martina Belli
Consultant

Cyber Security Strategy & Governance Practice | Security

NTT DATA aiuta le organizzazioni a orientarsi nella rapida evoluzione delle tecnologie, a rispondere alle crescenti aspettative dei clienti e, attraverso l'innovazione e la profonda esperienza nel settore, mette a disposizione le competenze e le risorse per guidare lo sviluppo digitale. Offriamo consulenza in ogni fase di progetto, da una prima fase di strategia e concept, passando dagli impatti sui processi, per arrivare all'implementazione finale. Advisory, Design, Tecnologia e Operation sono solo alcune delle nostre aree di competenza. NTT DATA ha sede a Tokyo con oltre 123.000 professionisti in oltre 50 Paesi in tutto il mondo. www.nttdata.com/it

NTT DATA