

Third parties, che ruolo giocano nella sicurezza aziendale e la necessità di definire una nuova metodologia a livello di industry sulla supplier security

La gestione del rischio relativo alle terze parti sta diventando un aspetto sempre più importante e delicato per chi si occupa di Cyber Security.

Il motivo è molto semplice: la gestione del rischio sugli asset interni al proprio perimetro seppur molto complessa, anche in realtà molto strutturate e di grandi dimensioni ha raggiunto un approccio consolidato.

Aziende che hanno una solida cultura di Cyber Security sono infatti in grado di portare all'approvazione del Board investimenti, anche molto importanti, per implementare soluzioni di sicurezza che controllino la corretta configurazione degli stack SW e/o soluzioni di logging e monitoring che siano in grado di intercettare la maggior parte degli attacchi in una fase preliminare, limitando impatti più ampi.

Il rischio derivante da "soggetti terzi", quindi esterni rispetto alla propria azienda, è molto più difficile da inquadrare e gestire.

Fino ad oggi, l'approccio di molte aziende è stato e continua ad essere quello di demandare ad aziende terze l'esecuzione di

interi processi aziendali, senza però tenere nel debito conto le ripercussioni che un incidente Cyber o più in generale di un data leak occorso sulla terza parte può avere sul proprio contesto aziendale.

Detta in altri termini, c'è la tentazione di considerare un incidente di una terza parte meno grave di un incidente sulla propria infrastruttura, anche in virtù di clausole contrattuali che trasferiscono la responsabilità sulla protezione dei dati e implementazione di presidi Cyber.

Tuttavia, una terza parte può avere all'interno della propria infrastruttura dati personali/critici di cui l'azienda committente è comunque responsabile, nonché avere interconnessioni con la stessa che portano con sé anche il rischio di una propagazione delle minacce sulle infrastrutture e sui servizi, con un possibile impatto sulla continuità del business aziendale.

Nell'RSA Conference del 2023 [1] è stato condiviso uno studio molto interessante condotto dalla Difesa Statunitense che denota un marcato trend che dal 2008 al 2020 evidenzia una sempre maggiore rilevanza degli incidenti di sicurezza relativi alle terze parti.

A ciò si aggiunge al fatto che il livello di rischio Cyber sta aumentando globalmente ed in particolare nel mondo delle Telco:

- Un report di Zayo illustra una crescita di attacchi DDOS del 200% anno su anno globalmente ma con una crescita degli attacchi del 1175% nell'industry delle Telco tra il Q1 e il Q2 del 2023
- La situazione geopolitica a livello mondiale rende le Telco, in quanto infrastruttura critica del paese, un obiettivo rilevante per attori in grado di utilizzare ingenti risorse in attacchi su larga scala, come la disruption operata verso l'operatore ucraino Kyivstar

tristemente conferma

- Un trend di crescita di aziende compromesse nei data leak forum delle varie “ransomware” gang. La fine del secondo quarter del 2023 ha visto circa 1350 organizzazioni vittime di ransomware con un increase di circa il 66% rispetto al primo quarter secondo studi di settore

Ma perché vediamo un trend così netto verso le terze parti negli incidenti relativi alla sicurezza informatica?

In una società sempre più digitalizzata, gli attacchi informatici sono diventati più sofisticati e attraggono molti più attori del passato, anche in virtù di una “democratizzazione” dei tool che consentono anche ad attori con poca esperienza di far leva su strumenti o servizi estremamente avanzati, quali ad esempio Ransomware as a Service (RaaS), Phishing as a Service (PhaaS) o DDOS as a Service (DaaS).

Da un lato realtà con una rilevante dimensione, spesso guidate anche da tematiche regolatorie, hanno intrapreso un percorso di incremento della resilienza Cyber sui propri asset primari.

Dall'altro lato, l'ecosistema delle terze parti, spesso fatto da aziende di dimensioni molto più contenute e con una limitata capacità di investimento, hanno faticato a definire piani ugualmente efficaci e si stanno dimostrando come l'anello debole della catena.

Risulta facilmente intuibile come per un attaccante sia meno oneroso e probabilmente altrettanto redditizio compromettere una terza parte per entrare in possesso dei dati delle aziende appaltatrici o da lì, trovare accesso alle loro reti.

Di seguito alcuni spunti di riflessione non esaustivi, che possono aiutare ad avviare un percorso di migliore gestione del rischio:

Valutare l'opportunità di un outsourcing esplicitandone e accettandone il rischio implicito:

Come chiarito sopra, il controllo di una terza parte non può essere mai equivalente al controllo sugli asset presente nell'organizzazione interna ed è necessario prenderne esplicitamente coscienza. Non sempre demandare processi all'esterno è un vantaggio nel momento in cui si prende coscienza dei rischi e delle necessarie azioni da mettere in campo per mitigarli. L'opportunità va esplicitamente valutata in termini di costi/benefici e se l'outsourcing rimane comunque l'opzione migliore, è importante fare una attenta analisi dei dati che si rende necessario esportare verso la terza parte e degli eventuali impatti di business nel caso di interruzione del servizio a causa di incidenti.

Identificare un robusto framework contrattuale:

Avere una resilienza nella Cyber Security ha un costo ed è necessario proteggere gli investimenti internamente alla terza parte rendendoli parte del framework contrattuale, non solo in termini di controlli ma anche di eventuali penali/rescissione del contratto nel caso si verificano eventi non correttamente gestiti.

Assicurarsi che la terza parte implementi i controlli più rilevanti, entrando nel merito della qualità implementativa:

La maggior parte degli incidenti hanno le stesse cause, ad esempio assenza di MFA, assenza di WAF/IPS, Vulnerability critiche esposte sul perimetro esterno, attacchi di social engineering, assenza di anti-malware/EDR sugli asset, assenza di logging e monitoring. Identificare i controlli prioritari e

fare un deep dive della loro implementazione con la terza parte sia in termini di adeguatezza di funzionalità che di copertura degli asset ha un enorme valore in termini di prevenzione rispetto ad un self assessment su un numero ampio a piacere di controlli generici spesso fatto all'unico scopo di rispettare processi di compliance.

Supportare le terze parti con rilevanti feed di Threat Intelligence:

La lotta tra chi difende e chi attacca è per definizione impari. Un attaccante ha mesi/anni per preparare un attacco, mentre chi difende si trova spesso a disperdere energie su più fronti e a dover reagire in tempi molto stretti. In questa situazione, è fondamentale l'apporto della Threat Intelligence, che consente di focalizzare gli sforzi nelle aree più critiche sia in termini di vulnerabilities che di tecniche usate dagli attaccanti per compromettere asset. Difficilmente aziende piccole sono in grado di avere una capability di Threat Intelligence matura, pertanto fornire alle proprie terze parti informazioni rilevanti per aiutarle a direzionare gli sforzi è sicuramente un approccio da valutare.

È chiaro dagli spunti sopra citati che si tratta di una tematica articolata e che non esiste una unica ricetta per far fronte a questa tipologia di rischio la cui gestione ha un costo sia in termini di complessità che di budget.

Per questo motivo, anche in considerazione delle implicazioni di business che ne possono conseguire, il rischio delle terze parti e la sua conseguente gestione è uno dei temi più importanti da riportare quando si parla di rischio Cyber. Renderlo evidente al Board e definire un approccio strutturato sono un ottimo punto di partenza per iniziare ad affrontarlo nel modo più corretto.

Note

[1]: How Top CISOs Are Transforming Third-Party Risk Management (rsaconference.com)

Articolo a cura di **Luigi Iaccarino**

Profilo Autore



Laureato in Ingegneria delle Telecomunicazioni, ha iniziato a lavorare nella consulenza nel 1999 ricoprendo diversi ruoli nei sistemi IT, nelle tecnologie di rete e nel broadcasting in Italia e all'Estero. Entrato in Vodafone nel 2012 come Responsabile delle Architetture e in seguito del Delivery dell'IT, ha ricoperto ruoli di crescente responsabilità fino a diventare nel 2015 responsabile della Cyber Security in Vodafone Italia, ruolo esteso nel 2019 anche a livello Europeo andando a coprire il ruolo di Responsabile della Cyber Security dell' EU Cluster. Da Maggio 2023 ha la responsabilità del team di Cyber Defence del Gruppo Vodafone, mantenendo la guida della Cyber Security di Vodafone Italia.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/articoli/third-parties-che-ruolo-giocano-nella-sicurezza-aziendale/>