CHUBB®

Le frontiere del rischio tecnologico

Consapevolezza dei rischi cyber per le aziende del settore IT

CHUBB®

Consapevolezza dei rischi cyber per le aziende del settore IT

Autori

Barry Schütte
Manager Industry Practices Benelux, Chubb

Wouter Wissink
Senior Principal Cyber Risk Engineer e Technology Industry Practitioner, Chubb

La sicurezza informatica è un'area di rischio che richiede un'attenzione enorme. Secondo Cybersecurity Ventures, costi della criminalità informatica previsti su scala mondiale ammonteranno a circa 10,5 trilioni di dollari all'anno entro il 2025. Le aziende del settore Information Technology sono particolarmente esposte a tali rischi, poiché il loro ruolo di software/service providers le rende un potenziale veicolo per la diffusione di malware o ransomware a più aziende con un solo attacco.

Gli attacchi Kaseya e SolarWinds sono due esempi di alto profilo dei danni che possono essere provocati da organizzazioni criminali sempre più sofisticate. Gli hacker organizzati sono sempre più motivati dalla monetizzazione delle loro attività, non a caso i ransomware sono ormai la maggiore minaccia informatica, come segnalato dall'Agenzia dell'Unione europea per la cibersicurezza.

Per porre fine ai crimini informatici occorrono solide soluzioni di sicurezza e un'attenzione continua ai controlli. I rischi possono essere notevolmente mitigati osservando alcune misure di *cyber hygiene*. Ma, tenuto conto degli attacchi sempre più mirati e avanzati, come possono tutelarsi le aziende del settore Information Technology?

Esposizioni comuni

Queste aziende fanno i conti con due rischi principali, estremamente interconnessi: gli attacchi ai propri sistemi e gli attacchi che colpiscono i clienti. Un attacco informatico a uno sviluppatore o a un distributore di software può tradursi nel furto di dati riservati, che potrebbero essere usati in modo improprio dagli hacker per accedere direttamente ai sistemi di un cliente. In caso di attacco ransomware, un'azienda del settore IT potrebbe non essere in grado di fornire servizi di supporto cruciali per i clienti. Così come è possibile che i clienti acquistino inconsapevolmente software compromessi da malware di tipo "backdoor", agevolando così un attacco a centinaia o migliaia di aziende.

I criminali informatici possono inoltre causare danni ottenendo l'accesso ai clienti tramite i Managed Service Provider (MSP), ovvero i fornitori di servizi gestiti, avverte Wouter Wissink, Senior Principal Cyber Risk Engineer e Technology Industry Practitioner di Chubb.

Le conseguenze finanziarie e reputazionali per le aziende operanti nel settore Information Technology possono essere immense, ha dichiarato Barry Schutte, Industry Practices Manager di Chubb. E ha aggiunto: "La preoccupazione dei clienti potrebbe spingerli a passare alla concorrenza, con forti ripercussioni sui profitti."

Decisioni aziendali difficili

Cosa possiamo imparare dalle crisi di Kaseya e SolarWinds? Nel caso della multinazionale statunitense Kaseya, a luglio 2021 un gruppo di hacker ha sfruttato le vulnerabilità nel suo software di Virtual System Administrator (VSA), fornito al provider di servizi gestiti e al team IT, per sferrare un attacco zero-day.

Checklist delle best practice di *cyber hygiene*

- **Puoi identificare i rischi a cui la tua azienda e i tuoi clienti sono esposti?**
- **Sai cosa fare per prevenire queste esposizioni?**
- **Sono utilizzati strumenti efficaci per individuare le minacce informatiche?**
- **È presente un piano chiaro su come reagire in caso di attacco?**

“In quanto “intermediari”, i Managed Service Provider sono esposti a rischi informatici concreti”

“Questa fase intermedia è molto difficile da proteggere”, ha spiegato Wissink. “Alle società di software occorre una settimana o più per risolvere questo tipo di problema e nel frattempo gli sviluppatori sono estremamente vulnerabili.”

Le perdite di Kaseya sono state limitate a circa 50 clienti, ma sembra che il ransomware sia riuscito a colpire fino a 1.500 aziende a valle a livello mondiale.

L’esposizione a questo tipo di attacchi è in aumento. Secondo quanto riferito in un rapporto di Rapid7, nel 2021 gli attacchi zero-day sarebbero raddoppiati. “Si tratta dell’area di rischio più critica in quanto è molto difficile da gestire”, ha affermato Wissink. Il quale incita le società interessate a informare i clienti il giorno stesso dell’attacco, a mettere tempestivamente offline i sistemi e a tenere aggiornati gli utenti.

“Per alcune aziende può essere molto difficile”, avverte. “In pratica stai dicendo ai clienti che il tuo modello di business non è più sicuro e che si ritroveranno offline.”

La tattica della “backdoor”

Sei mesi prima dell’episodio di Kaseya ha avuto luogo il cosiddetto Solorigate, un attacco alla supply chain con il quale un gruppo di criminali informatici ha inserito un malware negli aggiornamenti del sistema software SolarWinds Orion, ampiamente usato dalle società che gestiscono risorse IT.

“Gli hacker sono riusciti ad accedere all’ambiente di sviluppo”, ha spiegato Wissink. Il malware si è diffuso indisturbato nell’ambito dei consueti aggiornamenti software per i clienti, creando una “backdoor” ai loro sistemi informatici. Circa 18.000 clienti si sono trovati esposti, incluse agenzie del governo statunitense e aziende multinazionali. Secondo Wissink, “l’adozione di misure basilari di *cyber hygiene* avrebbe potuto prevenire questo attacco”.

Trend emergenti

Quali sono le tendenze riscontrate oggi dagli assicuratori? Poiché le aziende migliorano progressivamente i propri livelli di protezione, i criminali informatici puntano sempre di più a colpire venditori e fornitori, ha affermato Schütte. In quanto “intermediari”, i Managed Service Provider sono esposti a rischi informatici concreti, infatti l’espansione costante di questo segmento è accompagnata da un incremento dei sinistri.

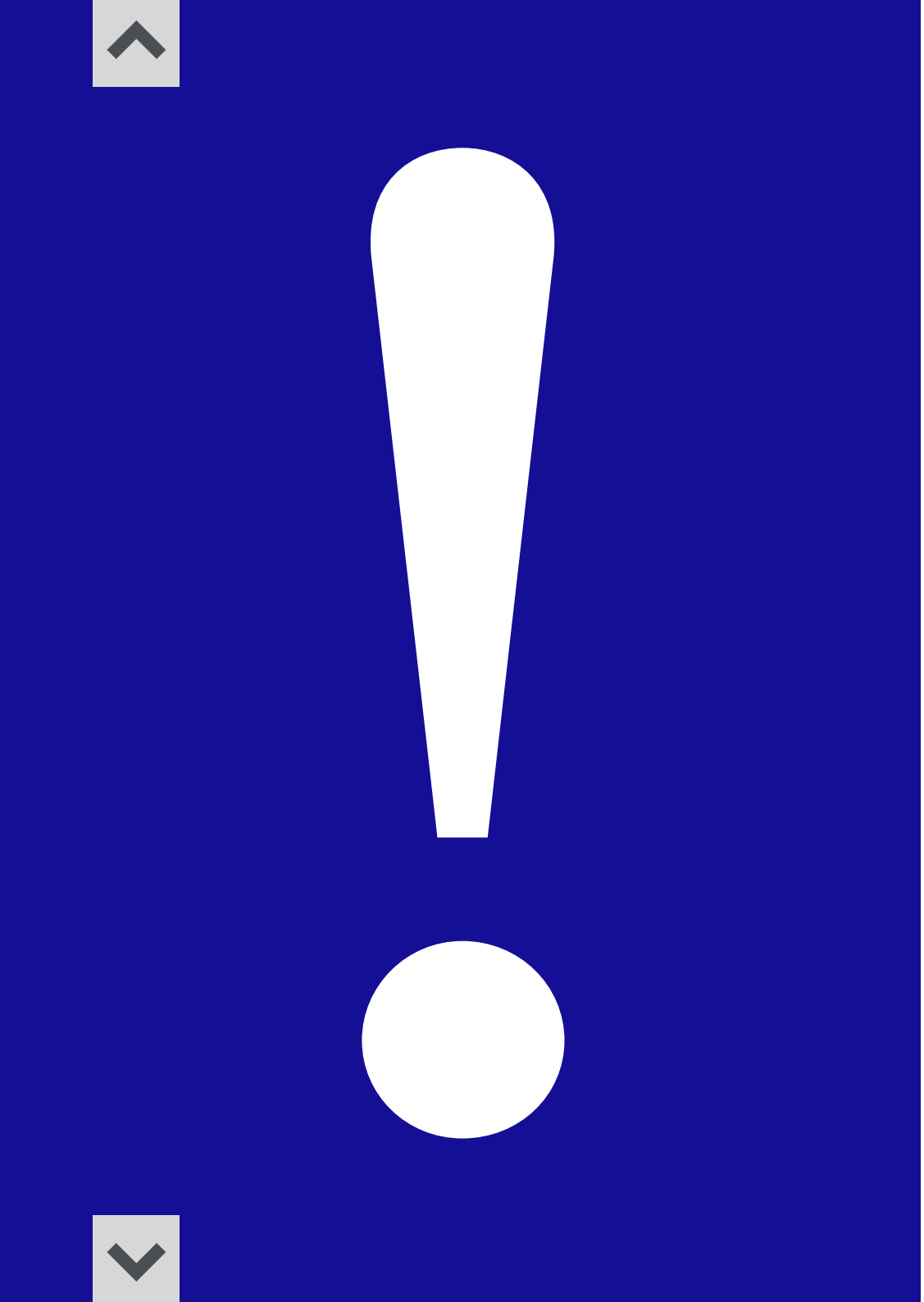
“Anche i sistemi Platform as a Service (PaaS) e Software as a Service (SaaS) sono più esposti”, aggiunge. “Insomma, il profilo di rischio è aumentato notevolmente con l’allontanamento dalle soluzioni software on-premise a favore di modelli basati su piattaforme o sul cloud.”

Un’altra area di rischio emergente riguarda il Duty of Care. Nell’ambito di una relazione tra fornitore e cliente, in genere una società che opera nel settore IT è considerata l’esperto, spiega Schütte. “Spesso le sue responsabilità vanno oltre il contratto scritto, e quindi i rischi connessi alla responsabilità possono moltiplicarsi.” Un fornitore consiglia a un cliente di adottare misure di sicurezza supplementari, senza però mettere per iscritto il suggerimento. Successivamente il cliente subisce un attacco ransomware e fa causa al fornitore di servizi IT, che viene ritenuto responsabile.

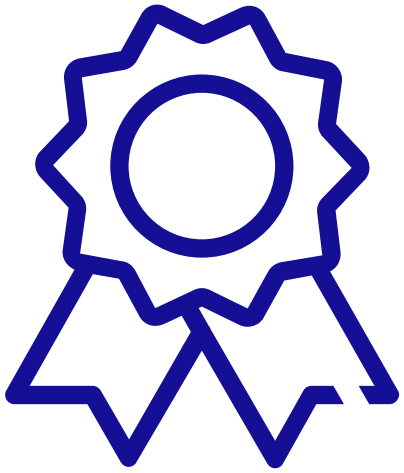
Quindi, in che modo è possibile mitigare questi rischi attraverso una buona *cyber hygiene*? Analizziamo le best practice per le aziende del settore Information Technology in base a quattro azioni: identificare, prevenire, rilevare e reagire.

Identificare i rischi

La definizione dei rischi cyber dipende semplicemente da un’efficace gestione del rischio, spiegano Wissink e Schütte. Le aziende del settore IT devono identificare con esattezza i prodotti e i servizi che forniscono in modo da valutare cosa può potenzialmente tradursi in un rischio. Producono software o si limitano a distribuirli? Sono un Managed Service Provider? Memorizzano password per i clienti?



“Anziché un unico rischio generalizzato, ora assistiamo a diverse esposizioni significative. Il rischio per le aziende del settore IT è quindi di gran lunga superiore rispetto a 10 o 15 anni fa”



Un Sistema di gestione per la sicurezza delle informazioni (ISMS) consente alle aziende di determinare tali dati. Questo sistema amministrato a livello centrale permette di gestire, monitorare e rivedere le prassi connesse alla sicurezza delle informazioni.

Benché in genere gli sviluppatori di software dedichino "notevoli sforzi" alla creazione di prodotti sicuri, Wissink sostiene che spesso mancano protezioni analoghe per i propri ambienti. Ad esempio, ai clienti viene chiesto regolarmente di scaricare il software da un sito web poco protetto.

Rafforzare le difese

Per fermare gli attacchi informatici occorrono, come minimo, misure standard di *cyber hygiene*, tra cui l'autenticazione a più fattori, un'adeguata formazione per il personale, i firewall, la scansione delle e-mail di phishing e il filtraggio dei siti web.

"Ad ogni modo, le società operanti nel settore Information Technology dovrebbero necessariamente mettere in atto le migliori best practice possibili in termini assoluti, considerando il rischio di rilevanti perdite causate da eventi di ampia portata e le accresciute responsabilità connesse al Duty of Care", suggerisce Wissink. E aggiunge che esse necessitano di un sistema di Privileged Access Management (PAM). Lo strumento di gestione degli accessi privilegiati (PAM) preserva le identità con accessi privilegiati o funzionalità supplementari rispetto a quelle degli utenti comuni. Questo è particolarmente importante per i Managed Service Provider, dove molti utenti hanno bisogno di accedere a più programmi attraverso un pacchetto software centrale.
Le società di sviluppo di software devono anche isolare le proprie reti e proteggerle con strumenti aggiuntivi a cui solo gli sviluppatori possono accedere, aggiunge Wissink. "Questo ambiente di sviluppo non dovrebbe avere una connessione automatica al resto dell'azienda."

Tra le altre misure di buona amministrazione per ridurre l'esposizione e contribuire alla continuità aziendale figurano i test continui dei backup e la loro archiviazione offline, nonché un'attenzione particolare alla crittografia delle password e degli altri dati. Un'altra ottima mossa è assumere un responsabile della sicurezza informatica dedicato.

"Le aziende devono proteggere questi dati ma dovrebbero anche avere adeguati accordi contrattuali con i clienti sulle modalità di archiviazione ed elaborazione dei loro dati", ha affermato Schütte.

Tuttavia prevenire non significa solo adottare misure di prevenzione tecnica, bensì anche comunicare adeguatamente e stabilire accordi contrattuali sul livello di servizio e sulla protezione dei dati. "Una società operante nel settore IT, e in special modo un Managed Service Provider, ha il dovere di avvertire e istruire i clienti sul livello di protezione potenzialmente scarso di un particolare ambiente", ha aggiunto Wissink. "I clienti dovrebbero essere informati per iscritto e, per tutelarsi dal punto di vista della responsabilità, tutto questo processo andrebbe documentato."

Secondo Schütte, molte aziende del settore Information Technology sono indietro nell'elaborare procedure di sviluppo sicure, ad esempio in termini di test di penetrazione e vulnerabilità, ma anche di revisione di codice e formazione sulla scrittura di codice (il documento OWASP Top Ten può fornire informazioni utili).

Aggiunge che gli sviluppatori di software impegnati nella creazione di software non critici non dovrebbero trascurare l'importanza di queste procedure.

"Nel contesto odierno, ricco di minacce, qualunque azienda rappresenta un potenziale bersaglio", avverte Wissink.

Conclusioni

- **Gli attacchi ai Managed Service Provider costituiscono il maggiore** trend emergente a livello di sinistri
- **Le aziende del settore IT devono gestire in modo strutturato** gli attacchi zero-day
- **I rischi legati al Duty of Care sono in aumento** e devono essere considerati dalle aziende
- **Applicare un Sistema di gestione per la sicurezza delle Informazioni (ISMS)** per identificare i rischi
- **Utilizzare uno strumento di gestione degli accessi privilegiati (PAM)** per contribuire a bloccare gli hacker
- **Isolare il proprio sistema software** dal resto dell'azienda
- **La comunicazione con i clienti è un altro fattore chiave** per prevenire attacchi informatici
- **Adottare politiche di secure coding** in materia di sviluppo software
- **Avviare un sistema di monitoraggio della rete** (monitorato 24/7)
- **Non ignorare i piani formali di incident response** e di continuità operativa
- **Testare costantemente i backup** e archiviarli offline

Individuare le violazioni informatiche

I software di monitoraggio e rilevamento, quali EDR (Endpoint Detection and Response), sono imprescindibili per le aziende operanti nel settore IT, come anche i firewall efficaci e i sistemi di monitoraggio della rete, tenuti sotto osservazione 24 ore su 24, 7 giorni su 7 da un centro operativo di sicurezza interno o esterno. "Nel momento in cui un hacker entra in un sistema, è fondamentale scoprirlo in tempo", sottolinea Wissink.

Domare l'incendio

Wissink e Schütte concordano entrambi che uno degli aspetti più cruciali per le aziende nella gestione degli attacchi cyber sia la presenza di un piano di incident response ben definito. Un'attenta pianificazione anticipata permette alle aziende di reagire in modo idoneo e tempestivamente in caso di attacco. Per le società di software, questo piano va ben oltre il proprio ambiente IT e dovrebbe includere una procedura di comunicazione con i clienti e di gestione delle crisi. Secondo la loro esperienza, molte aziende non sono preparate. "Gran parte delle volte non sanno come reagire", spiega Schütte.

In caso di violazione dei sistemi IT, le aziende devono garantire che i sistemi siano sicuri e che il ripristino delle loro funzionalità avvenga il prima possibile, oltre alla capacità di assistere i clienti in modo competente nel lasso di tempo intermedio.

Il futuro dei rischi cyber nell'era del digitale può intimidire, ma la mancata adozione di misure preventive per proteggere la propria azienda equivale un po' a lasciare costantemente spalancata la porta di casa e sperare che nessuno rubi niente. In un'ottica aziendale, ha molto più senso formarsi sul tema della *cyber hygiene* e predisporre misure adeguate per proteggere la propria attività e i propri clienti.

Contatti

Barry Schütte
Manager Industry Practices Benelux, Chubb
bschutte@chubb.com

Wouter Wissink
Senior Principal Cyber Risk Engineer e Technology Industry Practitioner, Chubb
wwissink@chubb.com

Chubb. Insured.℠

IT8218-WA02/23