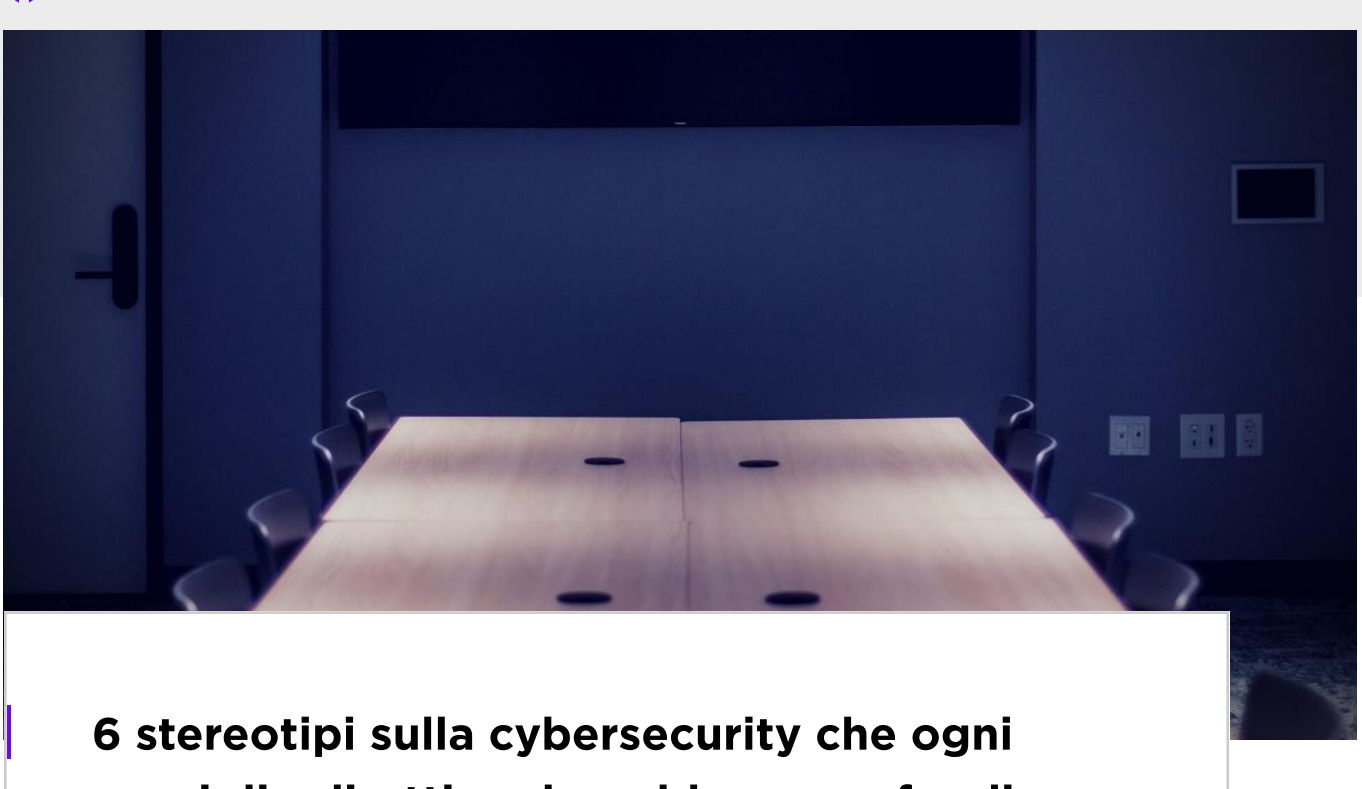
Avete subito una violazione? Ricevi una demo



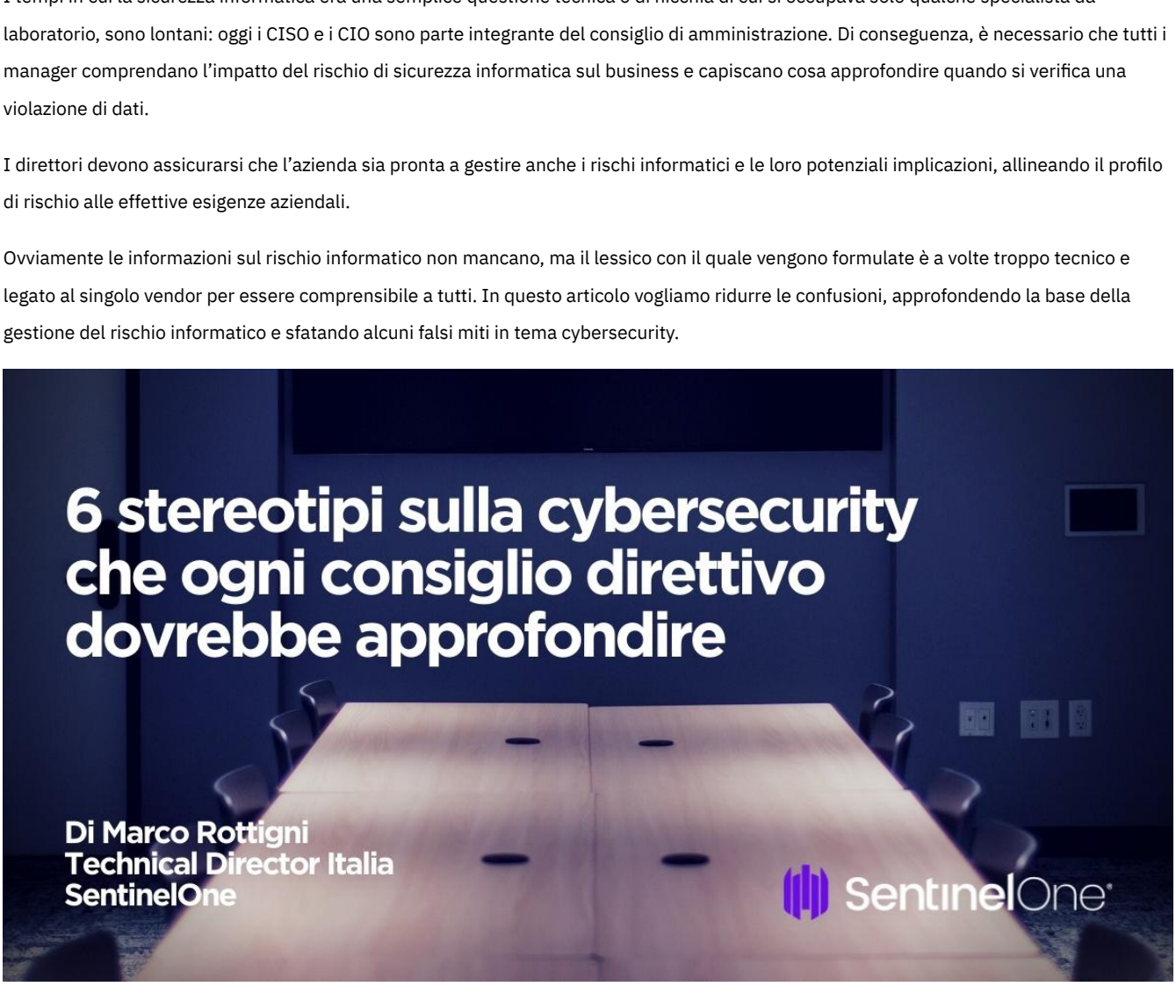
6 stereotipi sulla cybersecurity che ogni consiglio direttivo dovrebbe approfondire

Giugno 23, 2022
by Marco Rottigni, Technical Director Italia di SentinelOne

I tempi in cui la sicurezza informatica era una semplice questione tecnica o di nicchia di cui si occupava solo qualche specialista da laboratorio, sono lontani: oggi i CISO e i CIO sono parte integrante del consiglio di amministrazione. Di conseguenza, è necessario che tutti i manager comprendano l'impatto del rischio di sicurezza informatica sul business e capiscano cosa approfondire quando si verifica una violazione di dati.

I direttori devono assicurarsi che l'azienda sia pronta a gestire anche i rischi informatici e le loro potenziali implicazioni, allineando il profilo di rischio alle effettive esigenze aziendali.

Ovviamente le informazioni sul rischio informatico non mancano, ma il lessico con il quale vengono formulate è a volte troppo tecnico e legato al singolo vendor per essere comprensibile a tutti. In questo articolo vogliamo ridurre le confusioni, approfondendo la base della gestione del rischio informatico e sfatando alcuni falsi miti in tema cybersecurity.



1: La sicurezza informatica è indispensabile solo per alcune tipologie di aziende

Molti ritengono che solo alcuni tipi di aziende necessitino di sicurezza informatica e che, se non si rientra in tale elenco, la sicurezza informatica non sia una priorità. La cybersecurity è fondamentale per tutte le organizzazioni, indipendentemente dal loro settore. La continua ondata di attacchi ransomware dimostra che gli hacker prendono di mira qualsiasi impresa che disponga di dati preziosi o sistemi da poter sfruttare.

Anche le aziende che non conservano dati sensibili (Personally Identifiable Information – PII) possono essere violate o infettate da ransomware se i propri sistemi non sono adeguatamente protetti; e i PII non sono gli unici item che possono essere rubati o compromessi in un attacco. Le imprese possono anche perdere denaro, subire danni alla reputazione e altre conseguenze negative a seguito di una violazione informatica.

Analogamente, le dimensioni non sono un fattore significativo nella valutazione del rischio. Le piccole imprese vengono spesso considerate bersagli più facili perché si stima che non abbiano le stesse risorse da dedicare alla sicurezza come le grandi imprese e, il livello di rischio cresce se l'azienda non prende le precauzioni necessarie a proteggersi.

> Tutte le aziende, a prescindere da dimensioni, settore o fatturato, dovrebbero disporre di un piano di sicurezza informatica completo per proteggersi dai potenziali attacchi.

2: Un software di sicurezza è ciò di cui un'azienda ha bisogno per sentirsi al sicuro

Nell'arsenale di difesa della cybersecurity ci sono molti strumenti di precisione. Strumenti come SIEM, SOAR, Firewall, Anti Virus e molti altri hanno dimostrato negli ultimi anni di non essere sufficienti a tenere le aziende fuori dalle notizie negative di cronaca. L'ambiente di lavoro moderno offre ai dipendenti una libertà mai vista prima, con la possibilità di installare software e accedere alle risorse aziendali dall'endpoint, ovunque si trovino fisicamente. Lo sforzo di rimanere al sicuro dai rischi informatici può iniziare con l'ottenere lo strumento giusto per controllare tutto, ma non finisce qui. Con la continua evoluzione del quadro della cybersecurity, anche le capacità di difesa devono restare al passo.

> L'idea di una protezione totale dalle minacce informatiche non è realistica. Tuttavia, le imprese sono agevolate quando il consiglio direttivo promuove una cultura di consapevolezza informatica e integra gli investimenti in resilienza informatica con la visione strategica generale dell'organizzazione.

3: Le vulnerabilità del software non sono un problema per il consiglio direttivo

Ogni software utilizzato da un'organizzazione può introdurre vulnerabilità che facilitano gli attacchi nella rete aziendale. Alcuni esempi recenti includono CVE-2022-30190 (nota come vulnerabilità Follina), che consente agli attaccanti di compromettere un computer Windows semplicemente inviando un testo Word dannoso; oppure CVE-2021-44228 (nota come Log4Shell), una vulnerabilità nella libreria Log4j di Apache di cui la maggior parte delle aziende non si era nemmeno resa conto di avere. Purtroppo, l'origine delle vulnerabilità software può essere collegata al sistema operativo stesso. Ecco alcune statistiche sconfortanti:

- nel 2020, Microsoft ha confermato 1.220 nuove vulnerabilità collegate ai propri sistemi, con un aumento del 60% rispetto l'anno precedente;
- 807 delle 1.220 vulnerabilità erano associate a Windows 10, di cui 107 riguardavano l'esecuzione di codice, 105 l'overflow, 99 l'acquisizione di dati e 74 i maggiori privilegi;
- nel 2021 sono state confermate 836 nuove vulnerabilità, 455 delle quali riguardano Windows 10 e 107 consentono l'esecuzione di codice dannoso.

Sebbene la gestione delle patch sia responsabilità del team IT, il direttivo aziendale deve capire che nessuna quantità di patch può annullare il rischio di sicurezza collegato al sistema operativo stesso. Ciò significa che le organizzazioni dovrebbero collaborare con i vendor capaci di assicurare un approccio olistico alla sicurezza. Occorre evitare di affidarsi unicamente al fornitore del sistema operativo per applicare le patch, o per adottare componenti aggiuntivi di sicurezza necessari a colmare le lacune.

> Sviluppare una strategia che miri a ridurre i rischi, diminuendo le dipendenze e integrando facilmente la soluzione di sicurezza con il resto dello stack software.

4: Non è necessario preoccuparsi degli attacchi alla supply chain

Anche se un'organizzazione riesce a tenere al sicuro il proprio software, qualsiasi altro fornitore di servizi può inconsapevolmente facilitare l'accesso degli hacker alla rete. È notizia abbastanza recente l'attacco alla supply chain di SolarWinds, dove gli attaccanti sono stati in grado di compromettere le reti attraverso l'aggiornamento del software SolarWinds. E' stato rilevato anche l'incidente di Kaseya, dove gli hacker hanno preso di mira i server Kaseya VSA, comunemente utilizzati dagli MSP e dalle società di gestione IT, per infettare i clienti con il ransomware. Questi attacchi sono molto redditizi per gli hacker perché la compromissione di un anello debole consente l'accesso a un portfolio completo di clienti che utilizzano lo stesso software.

> Assicurarsi che la strategia del consiglio direttivo includa aspetti quali l'implementazione della giusta soluzione di sicurezza, lo sviluppo di un piano di risposta agli incidenti (IR), la garanzia che le policy di integrità delle applicazioni consentano l'esecuzione solo delle applicazioni autorizzate e la promozione di una cultura incentrata sulla cybersecurity.

5: Non si può fare nulla contro le minacce alla sicurezza informatica

Anche se è vero che alcune minacce sono fuori controllo, ci sono molte iniziative da implementare per proteggere l'azienda dagli attacchi informatici. L'implementazione di solide misure di sicurezza informatica può contribuire a ridurre il rischio di essere presi di mira dagli hacker. È inoltre importante ricordare che esistono misure che le organizzazioni possono adottare per rendersi il più sicure possibile contro gli attacchi più probabili. Nella stragrande maggioranza dei casi, gli hacker hanno motivazioni economiche e sono alla ricerca di "vittorie facili".

> L'implementazione di un piano di cybersecurity completo, che includa diversi livelli di sicurezza, aiuterà a proteggere la vostra organizzazione dalla maggior parte degli attacchi.

6: E' impossibile educare i dipendenti in tema di sicurezza informatica

Sebbene i dipendenti siano una parte fondamentale della strategia di sicurezza informatica di qualsiasi impresa, non ci si può aspettare che ognuno sia esperto di sicurezza e ogni azienda deve fornire formazione e risorse adeguate. Questo include una regolare sensibilizzazione sui tipi di minacce che l'organizzazione deve affrontare, semplici indicazioni per identificare le e-mail di phishing o le richieste più strane, o ancora per segnalare attività sospette. L'ingegneria sociale, più comunemente nota come la sottile arte di convincere le persone a fare clic sulle e-mail di spear phishing, rimane uno dei modi più comuni con cui i criminali informatici operano oggi.

> I dipendenti devono aiutare le difese informatiche: serve assicurarsi che non solo abbiano i mezzi per segnalare qualsiasi cosa sospetta, ma che si sentano sicuri e fiduciosi nel farlo.

Conclusioni

La sicurezza informatica consiste nel gestire il rischio nel modo più efficace possibile. Non esiste un'organizzazione al mondo che sia immune dalle minacce informatiche: nello scenario attuale è fondamentale che la sicurezza informatica sia considerata un fattore strategico, che deve essere pianificato dai vertici dell'organizzazione. Il rischio per l'azienda è troppo grande se si pensa di sottovalutare la sicurezza informatica.

Per ulteriori informazioni consultate www.it.sentinelone.com

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Come difendersi da misconfiguration, vulnerabilità e minacce in cloud
- Come anticipare gli hacker nel 2022: vademecum per la cybersecurity
- Difendere l'impresa nel 2022 dai rischi della Digital Supply Chain
- Status sulle minacce informatiche: le tecniche di attacco alle reti cloud
- Come misurare l'efficacia dei controlli di sicurezza in 4 step
- SentinelOne indica le più grandi falsità sulla cybersecurity raccontate ai CISO

©2022 SentinelOne, tutti i diritti riservati.
Informativa sulla privacy Condizioni del servizio