di F. De Luca
General Manager DuskRise Italia spa

CYBERSECURITY: rischi, impatti e nuovi modelli di prevenzione per aziende e istituzioni

Nel contesto attuale, caratterizzato da una progressiva e inarrestabile digitalizzazione, il panorama della sicurezza informatica si sta evolvendo in modo complesso e sfidante. Le soluzioni avanzate di cybersecurity, tradizionalmente progettate per soddisfare le esigenze di clienti ad alto profilo come grandi aziende e istituzioni, sono diventate sempre più sofisticate e specifiche. Queste soluzioni verticali sono indispensabili per enti che gestiscono enormi volumi di dati sensibili e infrastrutture critiche, richiedendo un livello di protezione e di personalizzazione che va oltre le capacità standard di sicurezza.

Tuttavia, un aspetto critico che emerge in questo scenario è la crescente incidenza di violazioni
della sicurezza originate da errori umani o da falle all'interno di entità collegate, ma esterne al perimetro di sicurezza principale dell'ente. Questo fenomeno evidenzia una realtà in cui le minacce non si limitano ai confini di una singola organizzazione, ma si diffondono attraverso l'intera rete di partner, fornitori e altre entità collegate. Inoltre, l'interconnessione tra diverse organizzazioni e il crescente ricorso a servizi di terze parti espandono il campo d'azione delle potenziali minacce, rendendo ancora più complessa la gestione della sicurezza informatica.

Nel frattempo, le piccole e medie imprese (PMI), che costituiscono una parte significativa dell'ecosistema economico, si trovano spesso in una situazione di vulnerabilità a causa della mancanza di risorse e competenze per accedere a soluzioni di sicurezza avanzate.
Questa disparità non solo espone le PMI a rischi maggiori, ma rappresenta anche un punto debole nell'intero tessuto economico, dato che le vulnerabilità in un'entità possono facilmente
trasformarsi in rischi per l'intera rete di cui fa parte.
Di conseguenza, la necessità di democratizzare l'accesso alla sicurezza informatica diventa imperativa.

È fondamentale che le soluzioni avanzate di cybersecurity non siano prerogativa esclusiva delle
grandi entità, ma siano rese accessibili anche alle PMI. Questo passaggio verso la democratizzazione non solo aiuterà a proteggere le PMI stesse, ma rafforzerà anche la sicurezza dell'intero ecosistema digitale, riducendo i punti deboli che possono essere sfruttati dagli attaccanti. In sintesi, l'evoluzione del panorama della sicurezza informatica richiede un

nuovo approccio che non si limiti a fornire soluzioni avanzate solo alle grandi entità, ma che estenda la protezione a tutto il tessuto economico, includendo PMI e altre organizzazioni collegate.
Una strategia olistica e inclusiva è fondamentale per costruire un ambiente digitale sicuro e resiliente, capace di affrontare le sfide di un mondo sempre più connesso e interdipendente.

1. I Rischi e gli Impatti delle Minacce Informatiche Variazione e Portata dei Rischi

Le minacce informatiche rappresentano un problema complesso e sfaccettato. Oltre ai danni finanziari diretti, come la perdita di ricavi e il costo di ripristino dei sistemi, questi attacchi portano con sé gravi conseguenze reputazionali. Un'azienda che subisce una violazione di dati può perdere la fiducia dei suoi clienti e partner, il che può avere un impatto duraturo sulla sua
posizione nel mercato. Inoltre, vi sono implicazioni legali, specialmente nel contesto di normative come il GDPR, che impone severe penalità per la non conformità nella gestione e protezione dei dati personali.

Rischi Trasversali: Un Fenomeno Pervasivo

La natura trasversale delle minacce informatiche significa che nessun settore è immune.
Ad esempio, nel settore sanitario, un attacco ransomware può bloccare l'accesso ai sistemi di record medici, mettendo in pericolo la vita dei pazienti e ostacolando le operazioni quotidiane. Nel campo dell'istruzione, le violazioni dei dati possono esporre informazioni personali di studenti e docenti, con ripercussioni che vanno ben oltre la perdita di dati. Le PMI, in particolare, si trovano in una posizione vulnerabile. Mancando spesso delle risorse finanziarie e tecniche per implementare sistemi di sicurezza sofisticati, queste aziende possono diventare bersagli facili per gli attacchi informatici, con conseguenze che possono essere disastrose sia a livello operativo che di immagine.

Impatto delle Regolamentazioni: Il Caso della NIS2

Le recenti evoluzioni nelle regolamentazioni europee, come la Direttiva NIS2, ampliano il campo di applicazione delle misure di sicurezza obbligatorie. Questa direttiva mira a rafforzare la resilienza complessiva dei sistemi informativi all'interno dell'UE, richiedendo a un più ampio
spettro di enti, inclusi fornitori di servizi essenziali e fornitori di servizi digitali, di adottare misure di sicurezza robuste. La conformità alla NIS2 richiede un'analisi approfondita dei rischi, la realizzazione di sistemi di sicurezza adeguati e l'implementazione di procedure di notifica degli incidenti. Le sanzioni per la non conformità possono essere significative, ma ancora più
importanti sono le potenziali ripercussioni di un attacco su larga scala che potrebbe paralizzare
infrastrutture critiche o esporre dati sensibili.

... continua a pag. 33

... continua da pag. 24

L'Interdipendenza nell'Ecosistema Digitale

Nell'odierno ecosistema digitale interconnesso, la sicurezza di un'entità è spesso legata a quella
dei suoi partner e fornitori. Un attacco riuscito contro un singolo elemento della catena di fornitura può avere un effetto domino, influenzando tutte le organizzazioni collegate. Questa interdipendenza rende fondamentale non solo la sicurezza interna di un'organizzazione, ma anche la sicurezza del suo network esterno.
La comprensione e la gestione di questo rischio richiedono un approccio olistico alla sicurezza, che consideri tutti i potenziali punti di vulnerabilità, sia interni che esterni.

In sintesi, il panorama delle minacce informatiche è complesso e in continua evoluzione, richiedendo un approccio multidimensionale che consideri aspetti finanziari, reputazionali, legali e operativi. La diffusione di queste minacce attraverso vari settori e la crescente interconnessione tra diversi attori economici sottolineano l'importanza di un approccio integrato e globale alla sicurezza informatica.

2. Strumenti di Prevenzione e Democratizzazione della Sicurezza Informatica

La democratizzazione della sicurezza informatica è un processo cruciale nell'odierno panorama digitale. Questo concetto non solo enfatizza l'importanza di rendere la sicurezza informatica accessibile a tutti, ma sottolinea anche la necessità di adottare un approccio inclusivo che copra entità di diverse dimensioni e competenze tecniche.

Accesso Esteso alla Threat Intelligence

La threat intelligence rappresenta un pilastro fondamentale nella prevenzione degli attacchi informatici. Tradizionalmente, l'accesso a queste informazioni vitali era riservato a grandi organizzazioni che potevano permettersi di investire in risorse e strumenti avanzati. Tuttavia, con la democratizzazione, si intende estendere questo accesso anche alle PMI.

Importanza per le PMI

Per le piccole e medie imprese, l'accesso a informazioni aggiornate sulle minacce informatiche
può significare la differenza tra la prevenzione di un attacco e il subirne le conseguenze. Con l'aiuto di servizi di intelligence adeguati, le PMI possono anticipare e prepararsi contro le minacce emergenti, adattando le loro strategie di sicurezza in tempo reale.

Personalizzazione e Scalabilità

Questi servizi di intelligence devono essere personalizzabili per soddisfare le esigenze specifiche di ogni azienda, tenendo conto del loro settore, dimensione e risorse. La scalabilità è un altro aspetto cruciale, permettendo alle PMI di adeguare il livello di servizio in base alla loro crescita e ai cambiamenti nel paesaggio delle minacce.

Soluzioni Basate su Abbonamento

Le soluzioni di sicurezza basate su abbonamento offrono un approccio flessibile e conveniente
per le organizzazioni di tutte le dimensioni.

Vantaggi del Modello di Abbonamento

Questo modello consente di ridurre notevolmente i costi iniziali, rendendo la sicurezza informatica un servizio continuo piuttosto che un prodotto una tantum. Le aziende pagano per ciò di cui hanno bisogno e possono aggiornare o modificare il loro piano in base all'evoluzione delle minacce e alla crescita aziendale.

Copertura Completa

Le soluzioni offerte in questi piani possono variare da semplici servizi di monitoraggio e allerta a soluzioni più complesse che includono analisi delle vulnerabilità, supporto nella gestione degli incidenti e consulenza in materia di sicurezza. Per le PMI, ciò significa avere accesso a un range di strumenti che un tempo erano prerogativa delle grandi corporazioni.

Importanza della Semplificazione

Uno degli obiettivi principali della democratizzazione è rendere questi strumenti intuitivi e facilmente gestibili, anche per chi non possiede una profonda conoscenza tecnica. Ciò implica
interfacce utente semplici, report comprensibili e un supporto clienti efficace per guidare gli utenti attraverso le varie funzionalità.
In sintesi, la democratizzazione della sicurezza informatica è un processo vitale per garantire che tutte le organizzazioni, indipendentemente dalla loro dimensione o dalla loro esperienza tecnica, abbiano l'opportunità di proteggersi efficacemente dalle minacce informatiche. Con l'adozione di soluzioni basate su abbonamento e l'accesso esteso alla threat intelligence, le organizzazioni possono non solo proteggersi meglio, ma anche contribuire a creare un ecosistema digitale più sicuro e resiliente.

3. L'Importanza della Formazione

L'educazione e la formazione giocano un ruolo cruciale nella creazione di una cultura della sicurezza informatica. Attraverso la formazione, gli individui possono sviluppare la consapevolezza necessaria per identificare e reagire alle minacce in modo efficace.

Programmi Educativi

Programmi di formazione nelle scuole, università e ambienti lavorativi sono essenziali per sviluppare una comprensione profonda delle minacce informatiche e delle strategie per affrontarle.

Simulazioni e Workshop

L'uso di simulazioni di phishing e workshop pratici può aiutare le persone a riconoscere e reagire a tentativi di attacco, incrementando le loro capacità di difesa.

Conclusioni

In un'era definita dalla rapida evoluzione tecnologica e dalla crescente interconnessione digitale, la sicurezza informatica non è più solo una questione di protezione individuale, ma si configura come un imperativo collettivo che abbraccia un ampio spettro di entità, dalle grandi aziende e istituzioni alle piccole e medie imprese (PMI).

L'adozione di soluzioni di sicurezza informatica avanzate e altamente personalizzate da parte delle grandi organizzazioni rappresenta solo una parte della soluzione. È fondamentale che queste misure di protezione si estendano oltre i confini tradizionali, includendo la vasta rete di
partner, fornitori e altre entità interconnesse che costituiscono l'ecosistema digitale globale. La
sicurezza di un'organizzazione è intrinsecamente legata a quella delle entità con cui interagisce;
pertanto, la protezione contro le minacce informatiche deve essere considerata una responsabilità condivisa.
La democratizzazione della sicurezza informatica, che mira a rendere gli strumenti e le conoscenze di protezione accessibili a tutti, è un passo essenziale verso la creazione di un ambiente digitale più sicuro e resiliente. Fornendo alle PMI l'accesso a soluzioni di sicurezza avanzate e a informazioni di threat intelligence, si riducono non solo i loro rischi specifici, ma si rafforza anche la sicurezza dell'intero tessuto economico.

Inoltre, la formazione e l'educazione continua in materia di sicurezza informatica sono fondamentali per sviluppare una comprensione profonda delle minacce e delle strategie per contrastarle. Questo aspetto è cruciale non solo per gli addetti IT, ma per ogni individuo che opera nell'ambiente digitale, indipendentemente dal suo ruolo o settore.

In conclusione, l'approccio alla sicurezza informatica nel mondo contemporaneo richiede un cambio di paradigma: da una visione isolata e segmentata a una strategia olistica e inclusiva.
Solo attraverso un impegno congiunto e una responsabilità condivisa tra tutte le entità coinvolte nel panorama digitale, è possibile garantire un livello di protezione efficace e adeguato alle sfide sempre più complesse del cyberspazio.