La prevenzione prima di tutto:

Come la difesa proattiva può ridurre al minimo la superficie di attacco e colmare le lacune di conformità

Digital Security
Progress. Protected.

Contenuti

Adottare una protezione multilivello contro i diversi vettori d'attacco 4

Andate oltre la protezione degli endpoint con XDR 9

Il potere dell'MDR 10

Conclusione: Perché la prevenzione è importante 11

Introduzione

Il seguente documento analizza esattamente i rischi a cui le organizzazioni sono esposte attraverso molteplici vettori di minacce. Inoltre, si illustra una strategia di prevenzione a più livelli dal punto di vista pratico.

Dato il costante aumento della complessità dell'IT, nonché la continua crescita in volume e sofisticazione delle minacce, il modo migliore per gestire queste sfide è una piattaforma unica e unificata. Quando il cambiamento è l'unica costante, trovare un partner di cybersecurity affidabile è fondamentale.

Il mondo cambia velocemente. E la tecnologia è l'agente di questo cambiamento: sta trasformando il modo in cui le aziende globali lavorano e interagiscono con i loro clienti. In quasi tutti i settori, la direzione di marcia è quella dei servizi, delle applicazioni e dell'infrastruttura cloud-first. Si tratta di ambienti IT concepiti per supportare il lavoro remoto agile. E sempre più spesso si tratta di innovazioni guidate dall'intelligenza artificiale, progettate per ottimizzare la produttività e offrire esperienze eccezionali ai clienti.

Ma il costo di questa trasformazione digitale si paga allargando rapidamente la superficie di cyberattacco. Le caselle di posta elettronica, gli endpoint, le applicazioni SaaS, i dispositivi mobili, le reti e altre risorse sono bersagli crescenti per gli attori delle minacce. Molte organizzazioni fanno fatica a gestire l'insieme dinamico di rischi. Secondo una stima, nel 2023 una risorsa su 10 aperta a Internet presentava una vulnerabilità senza patch e 70 miliardi di file erano esposti a potenziali furti o ransomware. Un'altra rivela che oltre la metà (52%) delle organizzazioni non sa quanto sia protetta la propria superficie di attacco e **nessuna è sicura di avere il pieno controllo di tale superficie.**

Oltre il

52%

delle aziende

non conosce il grado di protezione della propria superficie di attacco.

Gli attori delle minacce prosperano in queste condizioni. Solo cinque anni fa, i cyberattacchi più gravi venivano sferrati tramite payload software completamente automatizzati. Tuttavia, con l'evolversi delle difese, si sono evolute anche le tattiche offensive. Oggi le minacce più dannose sono gli attacchi "hands-on-keyboard", che possono coinvolgere sofisticati sistemi di social engineering, malware fileless e altro ancora. **I responsabili IT devono evolvere le loro attività di protezione, rilevamento e risposta alle minacce, di pari passo con la loro evoluzione.**

COSA SIGNIFICA IN PRATICA?

Un approccio a più livelli orientato alla prevenzione ridurrà le probabilità che un avversario riesca a penetrare nella rete aziendale e limiterà i danni che potrebbe causare in caso di successo. Ciò **sposta l'attenzione** dei team di sicurezza **dalla fase di remediation al monitoraggio proattivo della rete**, nonché al rilevamento delle intrusioni e alla gestione del rischio della superficie di attacco.

Un approccio proattivo e orientato alla prevenzione aiuterà le organizzazioni a:

- **Mitigare il rischio di minacce avanzate come ransomware e minacce zero-day.**
- **Identificare e neutralizzare le minacce emergenti prima che possano essere eseguite.**
- **Gettare le basi ad un approccio zero-trust**
- **Ridurre i costi e l'impatto di potenziali violazioni di dati**
- **Ridurre al minimo il tempo che i team di sicurezza dedicano alla risposta agli incidenti e alla risoluzione**
- **Colmare le lacune di conformità e soddisfare i rigorosi requisiti assicurativi**
- **Garantire la conformità aziendale**

Adottare una protezione multilivello contro i diversi vettori d'attacco

Le organizzazioni devono affrontare ogni giorno tentativi di furto di dati sensibili interni, dei clienti o dei dipendenti, di dirottamento di risorse IT o di criptazione di sistemi critici. Con l'aiuto di piattaforme cloud unificate, devono mitigare queste minacce informatiche su più aspetti della loro superficie di attacco.

ENDPOINT L'endpoint rappresenta l'intersezione tra uomo e macchina. Pertanto si tratta di uno degli obiettivi principali degli attacchi informatici, in quanto gli attori delle minacce cercano di sfruttare le vulnerabilità nei dispositivi/macchine endpoint o la fallibilità umana (tramite il phishing) per ottenere un punto d'appoggio nelle reti. Le minacce informatiche fileless sono particolarmente pericolose in quanto, non sfruttando i tradizionali file eseguibili, non esiste una firma per il rilevamento da parte dell'antivirus tradizionale. Uno studio del 2023 ha riscontrato un aumento del 1400% di questi attacchi in un periodo di sei mesi.

1 PROTEZIONE A LIVELLO DI ENDPOINT

La protezione degli endpoint deve andare oltre l'antivirus tradizionale e includere l'analisi comportamentale basata sull'intelligenza artificiale per bloccare gli exploit fileless eseguiti tramite script. Questa tecnologia è in grado di analizzare e classificare i campioni sospetti per ottimizzare la prevenzione delle minacce. Cercate soluzioni che **si aggiornino continuamente in tempo reale** per offrire protezione dalle nuove minacce e che **applichino più livelli di protezione**, tra cui la scansione del traffico di rete e il blocco delle minacce sulle unità rimovibili. La protezione degli endpoint deve inoltre funzionare su più sistemi operativi e tipi di macchine o dispositivi, tra cui desktop, laptop e server.

L'individuazione delle vulnerabilità e la loro eliminazione o mitigation attraverso l'installazione delle patch più recenti per le applicazioni e i sistemi operativi restano misure di prevenzione cruciali. Tracciare e correggere attivamente le vulnerabilità su tutti gli endpoint è un'attività che richiede molto tempo e i team IT tendono a rimanere indietro con le patch. Le organizzazioni devono prevenire qualsiasi rischio potenziale causato dal rinvio del patching e **cercare una soluzione automatizzata** che rilevi continuamente le vulnerabilità e semplifichi il processo di patching dando priorità alle risorse critiche in tutte le applicazioni e i sistemi operativi.

LA RISPOSTA DI ESET *ESET offre diverse funzionalità di sicurezza degli endpoint di nuova generazione. ESET LiveGuard® Advanced offre una difesa proattiva contro i tipi di minacce zero-day e mai viste prima, sfruttando il sandboxing nel cloud per analizzare e isolare i file sospetti in massa e in velocità. ESET Endpoint Security funziona su Windows, macOS e Linux, prevenendo gli attacchi malware basati su file, rilevando le attività dannose e fornendo attività di indagine e remediation per una risposta rapida agli incidenti di sicurezza dinamici. ESET Vulnerability and Patch Management tiene attivamente traccia delle vulnerabilità nei sistemi operativi e nelle applicazioni, fornendo patch automatiche o manuali su tutti gli endpoint per colmare le lacune di sicurezza e soddisfare i requisiti di conformità.*

DISPOSITIVI MOBILI

Il trend del lavoro ibrido e remoto fa sì che un numero sempre maggiore di utenti acceda alle risorse aziendali dai propri dispositivi mobili. Tuttavia, essi sono sempre più di frequente il bersaglio di attacchi di phishing e malware mobile, oltre al maggior rischio di perdita o furto cui sono esposti. Un rapporto del 2023 ha rivelato la presenza di malware su 1 dispositivo Android su 20 affermando che attualmente l'80% dei siti di phishing prende di mira i dispositivi mobili.

2 PROTEZIONE A LIVELLO MOBILE

Le organizzazioni hanno bisogno di una protezione a più livelli che funzioni su tutti i dispositivi aziendali. Ove possibile, dovrebbe includere la funzionalità anti-furto (compresi la cancellazione e il blocco da remoto), il **controllo delle app**, la **sicurezza web** e l'**anti-phishing**, nonché la possibilità di **applicare** da remoto **i criteri per le password** e altro ancora. Tutto questo deve essere gestibile da un'unica console per una maggiore visibilità e controllo.

LA RISPOSTA DI ESET *ESET Mobile Threat Defense funziona su Android e iOS e offre una prevenzione del malware basata sul cloud e difese multilivello potenziate dall'intelligenza artificiale, il tutto gestito da un unico punto con prestazioni senza precedenti. È inoltre disponibile la funzionalità di Mobile Device Management (MDM) per semplificare l'onboarding e la protezione dell'intera flotta.*

APP IN CLOUD PER OTTIMIZZARE LA PRODUTTIVITA' E SISTEMI DI POSTA ELETTRONICA

La posta elettronica continua a essere il canale principale per la diffusione di minacce quali attacchi di phishing, ransomware avanzato, compromissione della posta elettronica aziendale (BEC) e altro ancora. Di fatto, il phishing è stato il vettore di accesso iniziale più comune nelle violazioni dei dati nel 2023.

Le piattaforme di posta elettronica e le app di produttività in cloud più diffuse, come Microsoft 365 e Google Workspace, includono una serie di applicazioni in cloud a supporto della produttività, come le app di archiviazione e di collaboration, che possono essere prese di mira per il furto di dati e l'estorsione.

Le organizzazioni non dovrebbero affidarsi solo ai controlli di sicurezza nativi dei fornitori di cloud per la loro sicurezza.

3 PROTEZIONE DELLE APP IN CLOUD E DEI SISTEMI DI POSTA ELETTRONICA

Le best practice impongono di potenziare i controlli integrati di Microsoft 365 o Google Workspace con una protezione dedicata e a più livelli per la posta elettronica, le app di collaboration e lo storage ospitati nel cloud. **La sicurezza integrata delle e-mail nel cloud** o una soluzione di sicurezza delle e-mail cloud-native, abilitata alle API, dovrebbe includere il **filtraggio dello spam**, la **scansione anti-malware**, l'**anti-phishing** e l'**analisi comportamentale**. Esegue automaticamente la scansione di tutti i file nuovi e modificati nell'archivio condiviso per impedire l'esecuzione o la diffusione di malware. Idealmente, dovrebbe essere gestibile da un'unica console centralizzata.

LA RISPOSTA DI ESET *ESET Cloud Office Security offre una protezione avanzata per le app di Microsoft 365 e Google Workspace. I nuovi utenti sono automaticamente protetti da scansioni adattive avanzate, machine learning all'avanguardia, sandboxing nel cloud e analisi comportamentale approfondita.*

4 PROTEZIONE DEI SERVER DI POSTA ON-PREMISE

Le organizzazioni che, per vari motivi, utilizzano ancora server di posta on-premise devono implementare protezioni complete anti-phishing, anti-spam e anti-malware **per filtrare i messaggi indesiderati o dannosi**. Inoltre, devono proteggere il server come host. Le soluzioni migliori combinano l'intelligenza artificiale con l'esperienza umana e supportano il clustering, che consente ai prodotti di comunicare tra loro e di scambiarsi configurazioni, notifiche, greylisting e altro ancora, per una protezione di livello enterprise.

LA RISPOSTA DI ESET *ESET Mail Security offre una protezione avanzata per i server MS Exchange grazie alla tecnologia a 64 bit per una prevenzione accelerata delle minacce e-mail. Supporta anche le aziende che utilizzano Microsoft Exchange in una configurazione ibrida.*

HARDWARE E DISPOSITIVI Con la proliferazione degli endpoint, aumenta anche la superficie di attacco. E molto spesso ciò che gli attori delle minacce cercano sono i dati aziendali. Possono tentare di compromettere le macchine sfruttando le vulnerabilità o, più frequentemente, utilizzando credenziali legittime. Oggi una violazione di questo tipo potrebbe costare, in media, 4,5 milioni di dollari, oltre a causare grossi problemi con le autorità di regolamentazione.

5 PROTEZIONE A LIVELLO HARDWARE

Le organizzazioni possono mettere in atto una protezione stratificata, ma non è infallibile al 100%. Nel caso in cui si verifichi lo scenario peggiore, è necessaria una **forte crittografia dei dati** per renderli inutilizzabili da qualsiasi ladro. Ciò contribuirà anche a garantire la conformità al GDPR, al CCPA e ad altre normative e ai requisiti delle polizze di assicurazione informatica. Le organizzazioni dovrebbero cercare una soluzione che applichi l'Advanced Encryption Standard (AES) a 256 bit ai dischi di sistema, alle partizioni e alle intere unità, garantendo che nulla sia esposto. Per facilitare i compiti amministrativi e d'uso, la soluzione dovrebbe funzionare su Windows/macOS e consentire la gestione di più dispositivi da un'unica console.

LA RISPOSTA DI ESET *ESET Full Disk Encryption offre un potente AES a 256 bit convalidato FIPS 140-2 per dischi di sistema, partizioni o intere unità. L'implementazione con un solo clic e la gestione centralizzata alleggeriscono il lavoro dei team IT e garantiscono la massima tranquillità.*

IDENTITÀ

Sempre più spesso gli attori delle minacce rinunciano del tutto al malware e allo sfruttamento delle vulnerabilità e utilizzano credenziali legittime per impersonare gli utenti ed eludere le difese degli endpoint. Un rapporto rileva un aumento annuale del 71% del volume di attacchi che utilizzano credenziali e account validi in questo modo.

Queste credenziali sono spesso acquistate sul dark web o rubate con un malware apposito. Secondo lo stesso rapporto, nel 2023 si è registrato un aumento del 266% nell'uso di questo tipo di malware. Il lavoro degli attori delle minacce è facilitato dal riutilizzo delle password e dalla loro cattiva gestione.

6 PROTEZIONE DELLE IDENTITÀ

L'autenticazione a più fattori (MFA) è essenziale per prevenire l'uso improprio delle credenziali, soprattutto per gli account privilegiati o amministrativi. Le soluzioni devono supportare l'**autenticazione mobile, con un solo tocco**, che funziona senza problemi su dispositivi Android e iOS, integrandosi con la biometria e supportando l'autenticazione push per migliorare l'esperienza dell'utente. Il supporto nativo per l'accesso alla rete, VPN, Remote Desktop Protocol (RDP), Outlook Web Access, VMware Horizon View e servizi basati su RADIUS migliorerebbe inoltre l'efficienza del back-end. Le soluzioni MFA complete dovrebbero funzionare anche con i token hardware, se l'organizzazione li utilizza.

LA RISPOSTA DI ESET *ESET Secure Authentication offre una soluzione MFA one-touch basata su dispositivi mobili. L'installazione è semplice, poiché non è necessario alcun hardware. Sono supportati diversi metodi di autenticazione, tra cui applicazioni mobili, notifiche push, token hardware, chiavi di sicurezza FIDO e metodi personalizzati.*

Andate oltre la protezione degli endpoint con XDR

Oltre alla protezione in ciascuno di questi punti della superficie di attacco, le organizzazioni dovrebbero considerare il valore dell'Extended Detection and Response (XDR). Contrariamente a quanto si pensa, queste funzionalità non sono pensate solo per accelerare il rilevamento e la risposta agli incidenti. Possono anche far parte di un approccio proattivo e orientato alla prevenzione. Infatti, sono in grado di individuare sistemi mal configurati, vulnerabilità sprovviste di patch e minacce nascoste, consentendo alle organizzazioni di intervenire tempestivamente e di rafforzare la resilienza informatica. I vantaggi di una soluzione XDR sono:

- **Maggiore visibilità della rete aziendale**
- **Indagini più approfondite sugli incidenti di sicurezza, le minacce avanzate e gli attacchi mirati**
- **Monitoraggio più efficiente di incidenti e attività insolite e sospette**
- **Esecuzione più accurata della risposta agli incidenti**
- **Supporto del rilevamento proattivo delle minacce, per bloccare gli attacchi prima che il malware venga distribuito**

LA RISPOSTA DI ESET ESET Inspect offre un rilevamento unico basato sul comportamento e sulla reputazione, fornendo ai team di sicurezza informazioni in tempo reale sulle minacce fornite dal sistema globale ESET LiveGrid® Reputation System. È in grado di rilevare e bloccare minacce persistenti avanzate, attacchi fileless, minacce zero-day, ransomware e violazioni dei criteri aziendali.

Il potere dell'MDR

I servizi di Managed Detection and Response (MDR) consentono ai team IT presenti all'interno delle aziende di poter dedicare le risorse limitate a disposizione ad attività di maggior valore. In questo modo, supportano non solo le attività di rilevamento e risposta alle minacce, ma possono anche attuare una strategia di prevenzione, rivelando i punti deboli dell'infrastruttura di sicurezza e bloccando i comportamenti e le applicazioni sospette. I servizi MDR aiutano le organizzazioni a:

- **Rafforzare la capacità di risposta dell'infrastruttura di sicurezza aziendale, garantendo capacità di rilevamento immediato delle minacce, di indagine e di risposta agli incident**
- **Ottenere il rilevamento delle minacce efficiente dal punto di vista dei costi, attivo 24 ore su 24, 7 giorni su 7, grazie alla presenza di un team di esperti di cybersecurity**
- **Ridurre i costi di mantenimento di personale specializzato interno, riducendo a pochi minuti i tempi di risposta agli incidenti**
- **Essere preparati a soddisfare i requisiti di conformità; l'EDR/XDR e MDR sono sempre più spesso requisiti critici delle polizze di assicurazione informatica, nonché requisiti normativi.**

LA RISPOSTA DI ESET ESET offre servizi gestiti per PMI e clienti Enterprise. ESET MDR e ESET Detection & Response Ultimate sono servizi di gestione delle minacce operativi 24 ore su 24, 7 giorni su 7, che utilizzano l'intelligenza artificiale e l'esperienza umana per offrire una protezione ransomware di livello enterprise senza la necessità di assumere specialisti di sicurezza interni. A seconda del livello di servizio richiesto, ESET mette a disposizione esperti nei servizi proattivi di Threat Hunting e Threat Monitoring.

Conclusione: Perché la prevenzione è importante

Le organizzazioni globali fanno fatica a contenere i rischi su una superficie di attacco estesa, in continua crescita per effetto del lavoro ibrido e degli investimenti nella trasformazione digitale. La risposta è **concentrarsi in modo proattivo sulla prevenzione**. Perché? Essa riduce infatti al minimo i costi operativi associati al rilevamento delle minacce o alla risposta agli incidenti e ottimizza la produttività dei team operativi di sicurezza.

> **Quando un attacco viene impedito dalla piattaforma di protezione degli endpoint, gli analisti possono dedicare il loro tempo a indagare su come la minaccia sia penetrata nelle altre linee di difesa, invece di ripulire l'endpoint.**

Fonte: *Forrester: The Forrester Wave™: Endpoint Security, Q4 2023.* Paddy Harrington, 19 ottobre 2023.

Il modo migliore per rendere operativa la cybersecurity orientata alla prevenzione è attraverso un'unica piattaforma. Ciò garantirà:

- **Meno compartimenti stagni nella sicurezza dei prodotti e meno potenziali lacune nella protezione**
- **Risparmio sui costi delle licenze**
- **Minore onere amministrativo per i team di sicurezza (poiché c'è un solo prodotto/UI da imparare)**
- **SecOps più efficienti (meno lavoro manuale ripetitivo)**

ESET PROTECT Platform offre esattamente questi vantaggi grazie a una gamma completa di funzionalità di prevenzione delle minacce di nuova generazione unificate in un'unica offerta.

Si basa su tre decenni di esperienza di ESET nella ricerca e sviluppo nel campo della cybersecurity e su informazioni all'avanguardia sulle minacce globali per fornire **una protezione continua e automatizzata su più vettori di attacco**. Coniuga alti tassi di rilevamento con bassi falsi positivi e un impatto IT minimo, per **ridurre al minimo la superficie di attacco e il rischio normativo,** oltre a migliorare la continuità aziendale.

Scoprite perché **la piattaforma ESET PROTECT** è perfetta per la vostra azienda.

SCOPRI DI PIÙ

ESET

Difesa proattiva. Il nostro obiettivo è ridurre al minimo la superficie di attacco.

Rimanete un passo avanti rispetto alle minacce informatiche note ed emergenti con il nostro **approccio prevention-first**, **basato sull'intelligenza artificiale e sull'esperienza umana**.

Avvalendovi del nostro supporto potrete beneficiare di una protezione best-in-class, basata su un'**intelligence interna sulle minacce informatiche** globali maturata in oltre 30 anni all'interno della nostra rete di ricerca e sviluppo sotto la guida di **ricercatori rinomati nel settore**. ESET protegge la vostra azienda per consentirvi di sfruttare appieno il potenziale della tecnologia.

Tecnologia multilivello

L'Intelligenza Artificiale incontra l'esperienza umana

In prima linea nella ricerca sulla cybersecurity

Assistenza personalizzata e locale

ESET
Digital Security
Progress. Protected.