HP WOLF SECURITY

Revisione della strategia di sicurezza degli endpoint

Gli endpoint: l'elemento chiave per la sicurezza

I dispositivi endpoint svolgono un ruolo cruciale ai fini della sicurezza informatica perché, essendo il punto di incontro fra dati, utenti e Internet, costituiscono il bersaglio principale degli attacchi. Le aziende lo sanno e, proprio per questo, investono in soluzioni di sicurezza degli endpoint nel tentativo di contenere il rischio. Ma poiché alcuni attacchi, come quelli di phishing e ransomware, riescono ancora a colpire nel segno, significa che è necessario cambiare approccio.

Perché gli attacchi agli endpoint riescono ancora

La maggior parte delle architetture di sicurezza degli endpoint si basa su due soluzioni. La prima è costituita dal software NGAV (Next Generation Antivirus), che viene utilizzato per contrastare le minacce note e alcune varianti di tali minacce. La seconda è costituita dalle soluzioni EDR (Endpoint Detect and Response), che vengono installate in molti ambienti. Le soluzioni EDR tentano di rilevare le tracce degli attacchi che hanno eluso il software NGAV, ma possono fare ben poco per bloccarli. Forniscono dati forensi utili per difendersi da attacchi simili in futuro, ma non sono in grado di prevenire l'infezione iniziale.

PIATTAFORME DI PROTEZIONE DEGLI ENDPOINT (EPP, ENDPOINT PROTECTION PLATFORMS)

- Note come Antivirus (AV) o Next Gen Antivirus (NGAV)
- Bloccano efficacemente le minacce note o i file che mostrano comportamenti anomali

SOLUZIONE EDR (ENDPOINT DETECT AND RESPONSE)

- Rileva le attività sospette e fornisce consigli per la correzione
- Ideale per il rilevamento delle nuove minacce o delle varianti di quelle esistenti

Visti i presupposti, si può intuire facilmente perché gli attacchi vanno ancora a segno. Gli hacker si avvalgono infatti di tecniche di offuscamento per eludere NGAV ed EDR, inoltre sfruttano l'ingegneria sociale per indurre gli utenti ad agevolare l'attacco, facendo clic su determinati collegamenti e aprendo determinati documenti. Serve pertanto un approccio intrinsecamente più protettivo, capace di isolare i dati e il sistema operativo, per evitare che un eventuale vettore di attacco al PC riesca a sottrarre informazioni o a insediarsi permanentemente nel sistema.

Contenimento delle minacce – Protezione intrinseca a livello di endpoint

HP ha sviluppato un approccio unico alla protezione degli endpoint, che riesce dove le soluzioni NGAV ed EDR falliscono. Tale approccio, denominato "Contenimento delle minacce", sfrutta la tecnologia di isolamento per eseguire ogni singola operazione potenzialmente rischiosa (come l'apertura di un'allegato a un messaggio e-mail) in un'area isolata. E poiché l'isolamento viene applicato dall'hardware della CPU, non può essere eluso da alcun tipo di malware presente nel sistema. Al termine dell'operazione l'area isolata viene distrutta, e con essa l'istanza del malware.

CONTENIMENTO DELLE MINACCE

- Usa una micro-macchina virtuale (µVM) per proteggere le singole operazioni
- Blocca il malware, indipendentemente dal comportamento o dall'identificazione, e fornisce le prove forensi necessarie per colmare le lacune nella sicurezza degli endpoint

Il concetto di isolamento utilizzato dalla tecnologia di contenimento delle minacce è simile a quello utilizzato dagli hypervisor in un data center, che consentono di eseguire più applicazioni sullo stesso hardware impedendo a ciascuna di esse di accedere direttamente all'hardware, al kernel dell'hypervisor o ad altre applicazioni. HP ha esteso questa architettura collaudata ai PC endpoint, ottimizzando prestazioni e risorse come necessario per garantire un'esperienza utente coerente. Il nostro approccio basato sulla "micro-virtualizzazione" evita di imporre i requisiti di CPU e memoria degli hypervisor tradizionali ed è espressamente ottimizzato per i vettori di attacco più diffusi, ovvero i documenti di Office, i file PDF e i collegamenti Web.

La tecnologia di contenimento delle minacce integra le soluzioni NGAV ed EDR in modo da formare un'architettura esaustiva per la protezione degli endpoint. Il software NGAV blocca le minacce note più evidenti, mentre la soluzione EDR fornisce prove forensi affidabili ai fini della ricerca sulle operazioni di sicurezza. La tecnologia di contenimento delle minacce fornisce pertanto l'anello mancante: uno schermo protettivo zero-trust a livello di singola attività che isola, in fase di apertura, i documenti e i collegamenti non affidabili, presupponendo che potrebbero essere compromessi.

Vantaggi della soluzione per tutti gli stakeholder

La tecnologia di contenimento delle minacce non si limita a utilizzare un approccio tecnico esclusivo, ma offre una vasta gamma di vantaggi all'intera azienda.

GESTIONE DEL RISCHIO

- Approccio zero-trust
- Protegge sia le operazioni personali che quelle aziendali
- Garantisce una protezione intrinseca

VISIBILITÀ

- Offre un'area sicura per l'osservazione del malware
- Riproduce l'ambiente, per garantire una threat intelligence di altissimo livello
- Effettua un'analisi storica basata su cloud

ESPERIENZA UTENTE

- Nessuna modifica al flusso di lavoro degli utenti
- Nessuna correzione necessaria
- Serenità dei lavoratori
- Nessun calo di prestazioni

EFFICIENZA OPERATIVA

- Numero minimo di strumenti di sicurezza
- Riduzione dei ticket di supporto
- Riduzione dei falsi positivi
- Riduzione degli interventi correttivi sugli endpoint

CONFORMITÀ E AUDIT

- Raggiungimento degli obiettivi di controllo
- Controllo compensativo per la gestione delle patch

SOLUZIONI HP PER IL CONTENIMENTO DELLE MINACCE: SURE CLICK ENTERPRISE[1] E WOLF PRO SECURITY[2]

Sure Click Enterprise è la soluzione HP di contenimento delle minacce concepita per le grandi imprese. Supporta le policy flessibili e offre ampie possibilità di integrazione come necessario in questo tipo di ambiente. La gestione centralizzata può essere implementata on-premise o nel cloud, mentre la protezione delle credenziali viene fornita gratuitamente. Le piccole aziende possono invece considerare Wolf Pro Security, che fornisce una tecnologia di contenimento delle minacce facile da gestire, con un software NGAV opzionale.

Riepilogo

Quando si definisce la strategia di sicurezza degli endpoint, è necessario scegliere soluzioni efficienti allo scopo di minimizzare il rischio e le esigenze di gestione della soluzione di sicurezza. Le soluzioni EPP ed EDR tradizionali non bastano più. La nuove minacce sono in grado di eluderle, generando allarmi che assorbono buona parte del personale IT. Introducendo una tecnologia di contenimento delle minacce, l'azienda può aumentare la propria efficienza operativa grazie alla possibilità di adottare un approccio di sicurezza zero-trust, che ottimizza la protezione degli endpoint e al tempo stesso riduce i costi, senza interferire con la produttività dei dipendenti, riempiendo i vuoti lasciati dalle soluzioni EPP ed EDR.

[1] HP Sure Click Enterprise è in vendita separatamente. Gli allegati supportati includono Microsoft Office (Word, Excel, PowerPoint) e i file PDF, se sono installati Microsoft Office o Adobe Acrobat. Per i requisiti di sistema completi, visitare il sito System Requirements for HP Sure Click Enterprise, che contiene informazioni dettagliate.

[2] HP Wolf Pro Security è disponibile solo per alcuni dispositivi HP, su abbonamento o come licenza a tempo determinato. Per ulteriori informazioni, contattare il proprio responsabile vendite HP.

4AA8-2074ITE, maggio 2023