SOPHOS

Protezione Contro Le Minacce Informatiche Avanzate Per Il Settore Finanziario

Sophos MDR È Il Servizio Di Managed Detection And Response Più Apprezzato Dal Settore Finanziario

I fornitori di servizi finanziari sono uno dei bersagli più desiderabili per i cybercriminali. Gli avversari informatici sono attirati dal fatto che queste organizzazioni custodiscono dati preziosi, che offrono ai malintenzionati l'opportunità di estorcere pagamenti con strategie come il ransomware e la minaccia di rilasciare pubblicamente i dati sottratti durante la violazione.

Con l'incremento inarrestabile sia della quantità, sia della complessità delle cyberminacce, molti fornitori di servizi finanziari scelgono di affidarsi al servizio Sophos Managed Detection and Response (MDR) per proteggersi dagli attacchi più avanzati che le tecnologie, da sole, non sono in grado di prevenire. Questo briefing sulla soluzione esplora le sfide di sicurezza affrontate da questo settore e offre una panoramica di Sophos MDR: la scelta numero uno per l'MDR, a sostegno dei moderni fornitori di servizi finanziari.

Whitepaper Sophos. Febbraio 2023

La Sfida Di Cybersecurity Per Il Settore Finanziario

I fornitori di servizi finanziari sono uno dei bersagli più desiderabili per le cyberminacce

Più della metà (55%) delle organizzazioni che operano nel settore finanziario è stata colpita dal ransomware nel 2021, una percentuale più alta rispetto al 34% del 2020[1]. Questo incremento del 62% in un solo anno dimostra la rapida evoluzione del problema delle cyberminacce per il settore finanziario.

Più generalmente, l'anno scorso gran parte dei responsabili IT che lavorano nel settore ha riscontrato un aumento significativo in termini di volume (55%), complessità (64%) e impatto (55%) degli attacchi informatici. Nel frattempo, i cybercriminali continuano a sfruttare l'automazione e il modello "malware-as-a-service" nei loro attacchi. E si prevede che queste statistiche non faranno altro che aumentare.

55% Organizzazioni colpite dal ransomware nel 2021

55% Organizzazioni che hanno registrato un incremento del volume degli attacchi

64% Organizzazioni che hanno notato un aumento della complessità degli attacchi

55% Organizzazioni che hanno segnalato un aumento dell'impatto degli attacchi

L'Impatto Delle Cyberminacce Avanzate Sul Settore Finanziario È Molto Forte

Un incidente di cybersecurity molto grave implica conseguenze finanziarie e operative molto serie per le organizzazioni che operano nel settore finanziario. Nel 2021, il costo medio necessario per rimediare ai danni causati da un attacco ransomware ha raggiunto gli 1,59 milioni di $, con molto più di un terzo (37%) di casi in cui i dati cifrati non sono risultati recuperabili dopo l'incidente.

I costi di riparazione dei danni sono solo parte della storia. Quasi tutti (91%) i fornitori di servizi finanziari che sono stati colpiti dal ransomware sostengono che l'attacco ha avuto ripercussioni sullo svolgimento delle loro attività, mentre l'85% delle vittime nel settore privato afferma che l'attacco ha causato perdite commerciali e di fatturato. Se i sistemi informatici diventano inutilizzabili, la capacità di questi fornitori di offrire i propri servizi può diventare estremamente limitata e ciò può avere ripercussioni molto gravi per i clienti.

Il processo di ripristino dei sistemi può richiedere diverso tempo: più di un quarto (26%) delle vittime del ransomware nel settore finanziario ha avuto bisogno di più di un mese per tornare a svolgere regolarmente le proprie attività dopo l'attacco.

$ 1,59 Mio Costo medio di riparazione dei danni

91%
Percentuale di attacchi che hanno avuto ripercussioni sullo svolgimento delle attività

85%
Percentuale di attacchi che hanno causato perdite commerciali e di fatturato

1 La Vera Storia Del Ransomware Per Il Settore Finanziario, 2022, Sophos. Un sondaggio indipendente condotto tra 5.600 professionisti dell'IT, inclusi 444 che lavorano nel settore finanziario. Con il termine "colpito dal ransomware" si intende uno scenario in cui l'attacco ha avuto un impatto su uno o più dispositivi, senza includere necessariamente attività di cifratura.

Il Settore Finanziario Fa Fatica A Tenere Testa A Criminali Ben Finanziati

Di fatto, da sole le tecnologie non sono in grado di prevenire tutti gli attacchi informatici. Molti cybercriminali riescono infatti a eludere le soluzioni di sicurezza e conducono attacchi sfruttando vari strumenti IT legittimi, credenziali e autorizzazioni di accesso rubate, nonché vulnerabilità per le quali non sono state applicate le giuste patch. Emulando gli utenti autorizzati e approfittando delle debolezze nei sistemi di difesa delle organizzazioni, gli hacker possono evitare di farsi notare dalle tecnologie di rilevamento automatico.

L'unico modo per rilevare accuratamente e neutralizzare certi cybercriminali è con un servizio di monitoraggio completo e operativo 24/7, a cura di tecnici esperti che sfruttano avvisi di sicurezza e dati di intelligence sulle minacce provenienti da varie origini per identificare e bloccare le minacce prima che possano causare danni irreversibili.

Tuttavia, la complessità dei moderni ambienti operativi e la rapida evoluzione delle minacce informatiche costituiscono un ostacolo sempre più insormontabile per la maggior parte delle organizzazioni, che fanno fatica a gestire autonomamente le attività di rilevamento e risposta agli incidenti.

Le organizzazioni di ogni settore, incluso quello dei servizi finanziari, stentano a tenere il passo con avversari ben finanziati, che continuano a innovarsi e a industrializzare la loro capacità di eludere le tecnologie di difesa.

Sophos MDR: Protezione Per I Fornitori Di Servizi Finanziari

Con l'aumento costante dei problemi di cybersecurity, le organizzazioni del settore finanziario decidono sempre più frequentemente di affidarsi al servizio Sophos MDR per tenere testa alle cyberminacce avanzate che caratterizzano gli ambienti informatici moderni.

Servizio Di Prevenzione Contro Ransomware E Violazioni, Operativo 24/7

Sophos Managed Detection and Response (MDR) è un servizio completamente gestito, a cura di esperti che rilevano e rispondono agli attacchi informatici che colpiscono i tuoi computer, server, reti, workload del cloud, account di posta elettronica e altro.

- **Rilevamento:** monitoriamo il tuo ambiente 24/7, raccogliendo, contestualizzando e mettendo in correlazione i dati di sicurezza prelevati dal Sophos Adaptive Cybersecurity Ecosystem e dagli altri prodotti di cybersecurity in cui hai già investito, al fine di identificare eventuali tracce di attività sospetta
- **Indagine:** i potenziali incidenti vengono analizzati da operatori umani con elevate competenze tecniche, sfruttando la nostra conoscenza approfondita degli ambienti informatici delle organizzazioni che operano nel settore finanziario, unita alla nostra esperienza in tema di cyberminacce, per individuare proattivamente qualsiasi traccia di attività dei criminali
- **Remediation:** gli analisti intervengono rapidamente su tutti gli attacchi nel tuo intero ambiente, prima che si trasformino in un pericolo molto più devastante, come il ransomware o una violazione dei dati su vasta scala
- **Revisione:** Root Cause Analysis completa degli incidenti, controlli di integrità a intervalli regolari, più report settimanali e mensili per permetterti di migliorare il tuo profilo di sicurezza e prevenire gli attacchi futuri

Con un tempo medio di soli 38 minuti per i processi di rilevamento, indagine e remediation, la rapidità di Sophos MDR supera di 5 volte qualsiasi team operativo di cybersecurity interno.

Con Sophos MDR, puoi contare sul nostro team di oltre 500 tecnici operativi specializzati in cybersecurity, che mettono a tua disposizione le loro competenze in tutti gli ambiti del ciclo di rilevamento e risposta, da threat hunting e neutralizzazione, fino a progettazione delle difese antimalware e automazione della sicurezza. Con Security Operations Center (SOC) situati in Australia, India, Europa e Nord America, garantiamo monitoraggio 24/7, ogni giorno dell'anno.

Un Servizio Progettato In Base Alle Tue Esigenze

Sappiamo che ogni organizzazione che opera nel settore finanziario è un caso a sé, con tecnologie di sicurezza, team di cybersecurity/IT e ambienti informatici unici. Sophos MDR viene incontro alle tue esigenze: sei tu a scegliere il livello di supporto che ti serve, sia che tu voglia semplicemente ricevere notifica di eventuali minacce, lasciando la remediation al tuo team interno, che tu desideri affidare a noi la responsabilità di isolare le minacce, o che tu preferisca usufruire del nostro servizio completo di risposta agli incidenti e Root Cause Analysis. I nostri specialisti di protezione collaboreranno a stretto contatto con te, per identificare l'approccio giusto per la tua organizzazione.

Eleva La Protezione, Sfruttando I Tuoi Investimenti Attuali

Le moderne cyberminacce avanzate possono avere varie origini e spesso i cybercriminali sfruttano diversi strumenti, tattiche e procedure per sferrare i loro attacchi. Gli analisti del team Sophos MDR rilevano e rispondono anche agli attacchi più evoluti nell'intero ambiente di sicurezza, utilizzando gli strumenti Sophos e quelli di terze parti già implementati nel tuo ambiente. Possiamo utilizzare le tue soluzioni di:

- **Telemetria Endpoint:** per identificare le attività dannose e i comportamenti tipici degli hacker
- **Raccolta di dati del Firewall:** per rilevare i tentativi di intrusione e i beacon
- **Telemetria di Rete:** per identificare risorse non autorizzate, dispositivi non protetti e attacchi mai osservati prima
- **Avvisi Email:** per individuare il punto iniziale di ingresso nella rete e i tentativi di prelevare illecitamente i dati di accesso
- **Raccolta di Dati sull'Identità:** per identificare gli accessi alla rete non autorizzati e i tentativi di privilege escalation
- **Avvisi Cloud:** per identificare gli accessi alla rete non autorizzati e i tentativi di furto dei dati

Più vediamo, più velocemente agiamo. Rilevando e rispondendo agli attacchi più avanzati con gli strumenti di sicurezza che già usi, Sophos MDR riduce il rischio informatico e incrementa il tuo ritorno sull'investimento per le tecnologie di cybersecurity che hai già acquistato.

Sophos MDR: Il Servizio MDR Numero 1 Per Il Settore Finanziario

Sophos è il fornitore di servizi MDR numero 1 al mondo: difende più organizzazioni di qualsiasi altro vendor, proteggendo le infrastrutture informatiche da ransomware, violazioni dei sistemi e altre minacce che le tecnologie, da sole, non sarebbero in grado di bloccare.

Sophos MDR difende più di 500 fornitori di servizi finanziari. E proprio per questo motivo possiamo vantare competenze di un'ampiezza e una profondità imbattibili in tema di minacce che colpiscono il settore finanziario. Questa telemetria estremamente ricca ci permette di raggiungere "l'immunità della comunità", poiché ci consente di applicare tutto ciò che impariamo da un'organizzazione a qualsiasi altro cliente che opera nello stesso settore. Il risultato è un sistema di difesa più elevato per tutti.

Naturalmente, il nostro obiettivo principale sono i risultati di cybersecurity che possiamo garantire ai nostri clienti. Sophos è la soluzione MDR con le valutazioni più alte e con il maggior numero di recensioni in Gartner® Peer Insights™, con un punteggio pari a 4,8/5 ottenuto in 271 recensioni (dati aggiornati al 20 dicembre 2022) e con il 97% dei clienti che afferma che consiglierebbe Sophos. Inoltre, Sophos è stata valutata come Top Vendor nella 2022 G2 Grid® per i servizi MDR per le aziende di medie dimensioni; è anche stata nominata Leader per l'MDR da G2 nei segmenti Overall (generale), Midmarket (medie dimensioni) ed Enterprise (grandi imprese).

Numero 1 Per Il Settore Finanziario

- ✓ **Più Affidabile:** oltre 15.000 organizzazioni utilizzano Sophos MDR (1° trimestre del 2023)
- ✓ **Migliore Valutazione:** il 97% dei clienti consiglia Sophos
- ✓ **Maggior Numero Di Recensioni:** 271 recensioni su Gartner Peer Insights nel 2022

Cosa Dicono I Nostri clienti Nel Settore Finanziario

★★★★★

"La qualità della sicurezza ci garantisce la massima tranquillità, nella consapevolezza che abbiamo un team che vigila sui nostri sistemi e che non siamo da soli nel garantire la sicurezza dei dati della nostra azienda e dei nostri clienti."

Azienda con un fatturato di 50-250 milioni di USD, Nord America. Recensione completa su Gartner Peer Insights

★★★★★

"Usiamo il servizio da qualche mese e sono molto felice del ritorno sull'investimento riscontrato. Anche se non lavoro nel reparto IT, i report mensili includono risultati straordinari... Rispettiamo completamente la conformità ai nostri standard di settore, ed è grazie a Sophos MDR."

Azienda con un fatturato di meno di 50 milioni di USD, Asia Pacifico. Recensione completa su Gartner Peer Insights

★★★★★

"L'azione tempestiva del servizio ci ha aiutato a ripristinare la rete a uno stato di normalità, senza perdita di dati. Inoltre, il team ci ha fornito un ottimo report con tutti i dettagli di come si è verificato l'incidente."

Azienda con un fatturato di 1-3 miliardi di USD, zona EMEA. Recensione completa su Gartner Peer Insights

Cosa Fare Ora

Per scoprire di più su Sophos MDR e su come possiamo aiutare la tua azienda, parla con un referente commerciale Sophos oggi stesso o visita www.sophos.it/mdr

"Il team IT ha risparmiato almeno 40 ore alla settimana di attività SecOps."

AAVAS Financiers Limited

"Sophos MDR ci ha aiutato a contrastare minacce informatiche sempre più prolifiche e sofisticate, senza dover ampliare il nostro team SecOps."

Tourism Finance Corporation of India Limited

MDR Sophos

- Monitoraggio e risposta 24/7 alle minacce in tempo reale
- Threat hunting con supervisione di esperti umani
- Unione e correlazione dei dati sugli eventi di sicurezza provenienti da più prodotti (Sophos e di terze parti)
- Incident response gestita e completa (numero illimitato di ore; nessun costo aggiuntivo o anticipato)
- La migliore garanzia in assoluto per la protezione contro la violazione dei sistemi
- Contatto dedicato per l'incident response
- Supporto dedicato con linea diretta ai Security Operations Center di Sophos (6 SOC a livello globale)
- Report settimanali e mensili sulle attività
- Briefing mensile di intelligence
- Root Cause Analysis per migliorare il tuo profilo di sicurezza e impedire che le stesse minacce si ripresentino in futuro
- Sophos Account Health Check svolto regolarmente, per una revisione delle configurazioni e per garantire livelli ottimali di performance

27/02/2023 (WP-NP)

SOPHOS