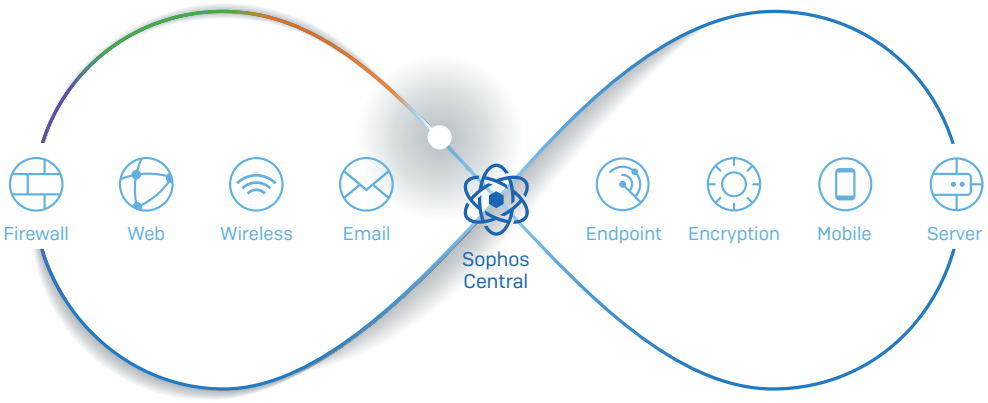
SOPHOS
Security made simple.



Sicurezza Sincronizzata: una rivoluzione nella protezione contro le minacce

Whitepaper Sophos Febbraio 2017

Sezione 1: L'attuale mondo del cyber-rischio

Gli attacchi sono sempre più numerosi, complessi e sofisticati

Tutte le aziende, che siano di grandi, piccole o medie dimensioni, devono sopravvivere e imparare a crescere in un mondo in cui il cyber-rischio è una minaccia sempre più preoccupante. I motivi alla base dell'aumento di questi rischi sono diversi, e variano dall'incremento della superficie di attacco, alla presenza di attacchi sempre più complessi e sofisticati.

Dispositivi mobili e servizi cloud sono risorse sempre più comuni per i dipendenti, e le infrastrutture virtuali e basate sul cloud vengono implementate da aziende di qualsiasi dimensione. La conseguenza è stata la drastica crescita dell'area definita come "superficie di attacco".

Si consideri quanto segue:

- **Dispositivi:** Al giorno d'oggi, il tipico consumatore digitale possiede tre dispositivi connessi[1].
- **App:** Al lavoro, i dipendenti adoperano in media 16 app, e le più frequentemente usate sono Box, SalesForce e Microsoft Office 365[2].
- **Internet of Things:** Gartner prevede che quasi 21 miliardi di 'apparecchi' di vario genere saranno connessi a Internet entro il 2020[3].

Il costante incremento dei vettori utilizzati ha causato un aumento della quantità degli attacchi, con un maggior numero di incidenti relativi alla perdita dei dati e casi di violazione andati a segno.

La presenza di toolkit di malware dotati di ottime risorse commerciali (disponibili sul mercato grigio e nero) consente ai cybercriminali di sferrare attacchi sempre più sofisticati, con un bisogno sempre minore di competenze tecniche specifiche.

Inoltre, i cybercriminali copiano i modelli imprenditoriali delle organizzazioni legittime, offrendo malware-as-a-service (ad es. ransomware) con tanto di garanzia soddisfatti o rimborsati. Ciò riduce ulteriormente le competenze tecniche necessarie per condurre un attacco informatico, e garantisce il continuo aggiornamento degli strumenti forniti.

Lo spiacevole risultato di tutti questi sviluppi è che ora i cybercriminali si muovono più rapidamente delle aziende, la maggior parte delle quali non riesce a tenere il passo. Secondo il Data Breach Investigation Report di Verizon per il 2016:

- Hackeraggio e malware sono le due principali cause di violazione dei dati.
- Gli autori degli attacchi compromettono i sistemi delle vittime con sempre maggiore rapidità: in quasi tutti i casi l'attacco va a segno nel giro di pochi giorni o meno, e talvolta occorrono solo pochi minuti o persino meno.
- Il ritardo di rilevamento (ovvero il periodo di tempo che intercorre tra compromissione e rilevamento) diventa sempre più grande, e occorre più tempo per identificare gli attacchi.

Inoltre, il report di Verizon indica che nell'80% dei casi, la motivazione principale degli attacchi è il lucro. Per le piccole e medie imprese, l'impatto finanziario può essere catastrofico.

Panorama delle minacce

Ci si trova ad affrontare attacchi in costante in aumento, maggiore complessità delle strategie, e perdite più elevate come loro conseguenza. Occorre chiedersi: cosa dobbiamo cambiare nelle nostre strategie?

Poco personale disponibile, risorse sfruttate al limite, difficile mercato del lavoro

È normale pensare che la reazione più naturale all'aumento degli attacchi debba essere un maggiore dispiego di personale: più assunzioni e un incremento dei livelli di sicurezza. Tuttavia, siccome nelle aziende il personale dedicato alla sicurezza informatica è limitato, espandere o ridistribuire le risorse non è un'opzione fattibile per la maggior parte delle piccole e medie imprese.

Come mostra la Figura 1, in qualsiasi azienda che non sia di grandi dimensioni i team dedicati alla sicurezza informatica sono composti da pochi dipendenti, e hanno a disposizione risorse limitate.

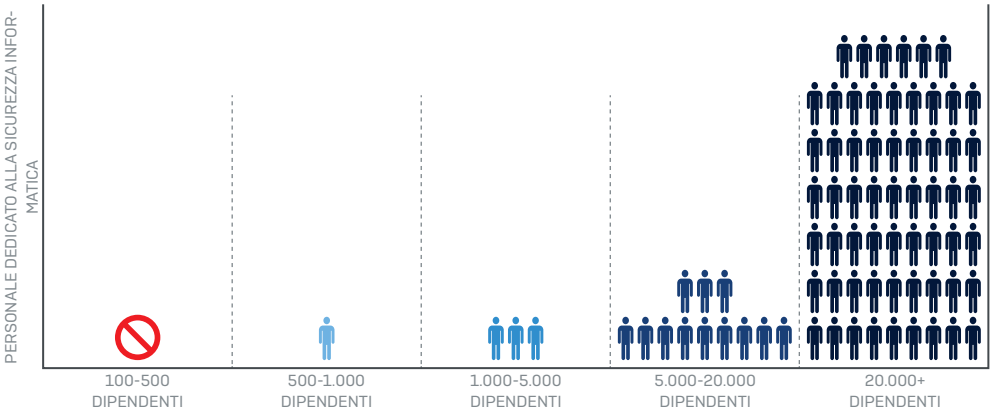


Figura 1: Le strutture di sicurezza informatica delle aziende appartenenti alla fascia media del mercato sono limitate in termini di dimensioni e risorse (Fonte: U.S. Department of Homeland Security, 2014)

Anche se i dirigenti aziendali desiderassero espandere i team dedicati alla sicurezza, si troverebbero pur sempre ad affrontare un altro ostacolo: la preoccupante carenza di risorse di sicurezza informatica. Una ricerca condotta da Enterprise Strategy Group indica che una percentuale molto elevata, il 46%, delle aziende ritiene di avere una carenza critica di competenze di cybersecurity[4]. Ciò rappresenta un ulteriore peso per i team IT attuali, che sono costretti a dover fare di più, con meno risorse.

Nonostante l'enorme quantità di attacchi sempre più sofisticati (ed efficaci), non si dispone di abbastanza personale qualificato. Doversi affidare alle risorse disponibili significa per le aziende esporsi a livelli di rischio inaccettabili.

Sezione 2: Gli attuali approcci alla sicurezza

A vari livelli, con poca integrazione. Complessi e senza visione. Indipendenti dal proprio contesto. Decisioni isolate. Tutte queste descrizioni sono applicabili agli attuali approcci alla sicurezza.

Gli autori degli attacchi sferrano attacchi coordinati contro interi ecosistemi informatici, non contro singoli prodotti di sicurezza.

Osservando il modo in cui il settore della sicurezza informatica si è evoluto, è facile capire perché. Le aziende di sicurezza hanno concentrato le proprie attività sullo sviluppo di prodotti individuali che fossero in grado di risolvere problemi in punti specifici della catena di attacco, invece di cercare di realizzare una soluzione olistica per combattere le minacce informatiche che tutti noi ci troviamo ad affrontare. Di conseguenza, la responsabilità di armonizzare l'integrazione di prodotti di sicurezza completamente diversi è ricaduta sulle spalle del personale IT, già oberato di lavoro. Praticamente, è come se una casa automobilistica vendesse le singole parti di un veicolo e chiedesse ai clienti di assemblarle e realizzare l'automobile.

I professionisti della sicurezza informatica hanno cercato di "unire i puntini" tra le varie fonti di dati, utilizzando motori di correlazione, warehouse di big data, Security information and Event Manager (SIEM), programmi di condivisione delle nuove informazioni quali STIX e OpenIOC, e decine e decine di analisti umani. Tuttavia, anche con gli strumenti più avanzati, comprendere i dati provenienti da un'ampia varietà di prodotti di punta per rilevare ed eliminare rapidamente il rischio e bloccare la perdita dei dati può risultare altrettanto difficile quanto "rimettere in piè" l'Humpty Dumpty della filastrocca.

Il processo di correlazione di eventi e log dipende ancora dall'impostare e gestire complesse regole di correlazione, dal mappare un infinito numero di campi, e dall'impostare altrettante definizioni per i filtri, per non parlare di ore e ore di tempo e lavoro di analisti altamente specializzati ed estremamente difficili da reperire. I SIEM richiedono un considerevole investimento di capitale e continue spese operative. Inoltre la condivisione delle informazioni, sebbene non vi sia alcun dubbio che rappresenti un fattore essenziale per il futuro della sicurezza, non è ancora abbastanza matura per consentirne un'adozione universale e semplice.

I risultati, o meglio la mancanza degli stessi, parlano da soli. I rischi e la perdita dei dati sono in costante aumento, senza mostrare alcun cenno di diminuzione, e il personale non è abbastanza. Secondo un recente report del Ponemon Institute, il 74% delle violazioni passa inosservato per più di sei mesi. E il fatto più preoccupante è che, per quanto riguarda la mitigazione dei rischi, le aziende di medie dimensioni sembrano trovarsi in maggiore difficoltà rispetto a quelle più grandi, che dispongono di risorse migliori. Ovviamente la risposta non è l'ennesimo prodotto di punta non integrato, e neppure ulteriori console, più personale o altri SIEM con poca flessibilità. Questi approcci hanno avuto un effetto deludente. Occorre trovare un approccio migliore e più efficace.

Sezione 3: Un nuovo approccio alla sicurezza informatica

Per decine e decine di anni, il settore della sicurezza ha considerato la sicurezza della rete, degli endpoint e dei dati come entità ben distinte. La situazione è paragonabile all'avere tre guardie di sicurezza in un edificio (una fuori dalla porta di ingresso, una all'interno dell'edificio, e una davanti alla cassaforte), senza concedere loro la possibilità di comunicare l'una con l'altra.

Ma con la crescente complessità delle minacce, e il sempre maggiore carico di lavoro affrontato dal personale IT, non è più possibile mantenere questo approccio senza che la sicurezza ne risenta.

La **Sicurezza Sincronizzata** è un sistema di sicurezza di primissima categoria, nel quale prodotti integrati condividono in maniera dinamica informazioni relative a minacce, stato di integrità dei dispositivi e sicurezza. Il risultato: una protezione più rapida e di migliore qualità contro le minacce avanzate. È come dotare ciascuna di queste guardie di uno smartphone per consentirne la comunicazione e la coordinazione delle attività, al fine di prevenire le minacce.

È un concetto tanto semplice quanto rivoluzionario. Per implementare una sicurezza sincronizzata, occorrono tre elementi:

1. **Un sistema di sicurezza centrale**
   Al cuore dell'approccio sincronizzato vi è una piattaforma di sicurezza centrale, con una visuale completa sulle minacce e sul contesto di sicurezza su tutti i dispositivi e i dati. Deve essere semplice da usare, e in grado di permettervi di gestire tutti i componenti della protezione da un unico pannello. Non si sarà più costretti a passare ripetutamente da una console a un'altra: questo sistema aiuta a risparmiare tempo e fatica nelle attività quotidiane.

2. **Tecnologia next-gen**
   La Sincronizzazione non deve influire negativamente sull'efficacia della protezione. Ciascun componente di sicurezza deve includere le più recenti tecnologie di prevenzione delle minacce, per garantire sempre e comunque la sicurezza più avanzata.

3. **Protezione intelligente**
   Il sistema di sicurezza deve essere in grado di consentire alle tecnologie di protezione di condividere le informazioni e automatizzare la risposta agli incidenti; inoltre, deve offrire la possibilità di isolare in tempo reale qualsiasi dispositivo infettato, per prevenire sia la perdita dei dati che ulteriori casi di infezione all'interno dell'azienda. Il risultato è una protezione senza eguali contro minacce avanzate e complesse.

Attuali soluzioni di sicurezza a livelli multipli	Sicurezza Sincronizzata
Basate sulle minacce, agiscono indipendentemente da oggetti ed eventi vicini	Basata sull'ecosistema, agisce in piena consapevolezza degli oggetti e degli eventi vicini
Prodotti di punta specializzati e isolati	Prodotti coordinati
Efficacia tramite l'aggiunta di personale	Efficacia tramite automatizzazione e innovazione, non richiede personale aggiuntivo
Gestione indipendente della cifratura	Protezione con cifratura integrata, in grado di rispondere automaticamente alle minacce
Complesso	Semplice

Figura 2: Le soluzioni attualmente disponibili richiedono un cambiamento radicale

Sezione 4: La strategia Sophos

Sophos si è affermata come pioniere dell'approccio della sicurezza sincronizzata. Secondo IDG, "le altre aziende non riescono neppure ad avvicinarsi a questo livello di comunicazione tra endpoint e prodotti di sicurezza della rete". Come funziona, quindi, la nostra soluzione?

Sophos Central, la nostra pluripremiata piattaforma di sicurezza, consente di gestire l'intero sistema di protezione Sophos da un unico centro di comando per: endpoint, dispositivi mobili, server, web, e-mail, wireless, cifratura e firewall. La differenza tra la sicurezza sincronizzata e una console digestione centralizzata è immensa. Gartner definisce la sicurezza sincronizzata come l'"integrazione a livello dei criteri", mentre una console centralizzata è semplicemente un'"integrazione nei pannelli di controllo".

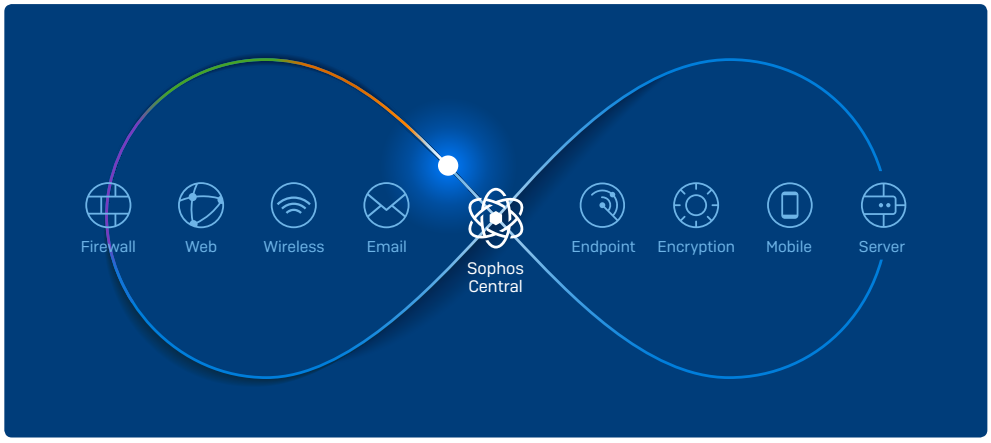


Figura 3: La Sicurezza Sincronizzata con Sophos

Nei nostri prodotti sono integrate tecnologie next-gen, per cui tutti i dispositivi e i dati godono sempre e comunque della protezione più recente contro ransomware, malware e ATP. Recenti premi e riconoscimenti degli analisti di settore includono:

- Unico vendor a essere nominato Leader nei Quadranti Magici di **Gartner** per piattaforme di protezione degli endpoint e UTM.
- **Computing**: Best Firewall 2016
- 'Breakout Star' nella **Forrester** Encryption Wave 2016
- **SC Magazine**: Excellence Award per Cifratura e Firewall di rete
- **AV Test**: Best Android Security 2016

La Sicurezza Sincronizzata viene resa possibile dalla nostra tecnologia brevettata Security Heartbeat™: un sistema che connette e abilita la comunicazione sicura tra i prodotti Sophos, permettendone la condivisione di informazioni relative a minacce, stato di integrità e sicurezza, con l'automatizzazione della risposta alle minacce. Decine di tecnologie diverse agiscono in sincronia per garantire la migliore protezione al mondo contro gli attacchi coordinati. Sophos Security Heartbeat riduce a pochi secondi i tempi necessari per i processi di rilevamento delle minacce, protezione dei sistemi e risposta agli incidenti: tutte operazioni che di solito possono richiedere ore, giorni o addirittura settimane.

Sezione 5: Sicurezza integrata: Blocco delle minacce più recenti

Per offrire una migliore dimostrazione dell'efficacia della sicurezza sincronizzata, diamo un'occhiata a come agisce in esempi tratti da situazioni reali, con due delle minacce più comuni dei nostri tempi: le botnet e il ransomware.

Botnet

Le botnet sono reti nelle quali gli hacker controllano il traffico dei dispositivi arruolati, all'insaputa dei loro proprietari, al fine di lanciare cyberattacchi coordinati; sono attualmente una delle cinque principali minacce di sicurezza a livello internazionale. Vengono utilizzate per diversi attacchi, che includono:

- Generazione di cryptocoin, per attività di mining di nuove valute on-line
- Hacking di dati tramite sistemi POS, come è successo ai negozi Target
- Attacchi di DDoS o di DNS amplification, come la botnet Mirai, che è riuscita a mettere fuori uso vari siti web in tutto il mondo
- Hacking delle password tramite attacchi di tipo brute-force e spam

Le informazioni relative a stato di integrità e minaccia botnet vengono inviate, tramite Security Heartbeat, al Sophos XG Firewall, che procede isolando automaticamente il dispositivo compromesso tramite la rimozione del suo diritto di accesso alla rete. In questo modo, viene impedito al malware delle botnet di comunicare con il proprio server di comando e controllo per ricevere ulteriori istruzioni, prevenendo la generazione di altre infezioni per mezzo del dispositivo iniziale.

Security Heartbeat condivide queste informazioni anche con Sophos Encryption, che revoca le chiavi di cifratura del dispositivo interessato fino a quando non viene risolto il problema, per prevenire un eventuale tentativo di furto di dati.

L'intero processo, da rilevamento a isolamento e rimozione della chiave, avviene in maniera immediata, e riduce i tempi di risposta a pochissimi secondi, invece di diverse ore.

Una volta isolati tutti i dispositivi interessati, in modo da renderli inutilizzabili per le botnet, la nostra protezione endpoint rimuove automaticamente il malware della botnet.

Dopo che i sistemi sono stati ripristinati al loro stato iniziale e integro, l'amministratore IT può quindi reimpostare nuovamente lo stato di integrità dell'endpoint come VERDE. Queste informazioni vengono immediatamente condivise con il resto del sistema di sicurezza per mezzo del Security Heartbeat. L'XG Firewall autorizza nuovamente l'accesso alla rete per il dispositivo, e vengono restituite le chiavi di cifratura. La rete è ora libera dalle botnet.

Ransomware

Il ransomware è un business molto lucrativo. Rappresenta fino al 35% di tutte le minacce informatiche presenti nel mondo, e gli autori di attacchi più abili possono ricavare fino a 400.000 $ al mese.

Di solito il ransomware viene inviato per e-mail. Non appena l'ignaro utente apre il messaggio e attiva il ransomware, la tecnologia antiransomware di Sophos Intercept X blocca l'attacco su desktop, laptop e server, mentre Sophos Mobile Security difende i dispositivi mobili.

La Sicurezza Sincronizzata attiva su Sophos Central uno stato di integrità ROSSO per i dispositivi a rischio. Il cambio di stato, insieme alle relative informazioni sulle minacce, viene inviato, tramite Security Heartbeat, al Sophos XG Firewall, che procede isolando automaticamente il dispositivo infettato tramite la rimozione del suo diritto di accesso alla rete. In questo modo si impedisce che il ransomware comunichi con un server di comando e controllo, eliminando quindi il propagarsi dell'infezione.

Security Heartbeat agisce simultaneamente, contattando Sophos Encryption, che a sua volta revoca le chiavi di cifratura del dispositivo interessato fino a quando non viene risolto il problema. Analogamente a quanto accade per le botnet, la durata totale del processo, da rilevamento a isolamento e rimozione della chiave, è brevissima e riduce i tempi di risposta da diverse ore a pochissimi secondi.

Una volta eliminate tutte le minacce, l'amministratore IT può nuovamente reimpostare lo stato di integrità dell'endpoint come VERDE, e l'informazione viene condivisa con il resto del sistema tramite Security Heartbeat. L'XG Firewall autorizza nuovamente l'accesso alla rete per il dispositivo, e vengono restituite le chiavi di cifratura. L'utente ritorna quindi a essere operativo.

Tutto ciò avviene in maniera automatica, e all'istante. Non occorrerà muovere nemmeno un dito.

Riepilogo

La sicurezza della maggior parte delle aziende non riesce a tenere il passo con lo sviluppo di attacchi sempre più complessi e coordinati. Il personale IT, già oberato di lavoro, non è in grado di rispondere abbastanza rapidamente alle minacce che si infiltrano nelle infrastrutture informatiche in costante espansione.

Continuare a gestire prodotti di sicurezza diversi aumenta il rischio a cui sono esposte le aziende. A meno che non si verifichi un cambiamento drastico nell'approccio ai sistemi di sicurezza, la situazione non può altro che peggiorare.

La Sicurezza Sincronizzata offre un sistema di protezione di primissima categoria, nel quale prodotti integrati condividono in maniera dinamica informazioni relative a minacce, stato di integrità dei dispositivi e sicurezza. Tutto ciò contribuisce a garantire difese più rapide e di migliore qualità contro le minacce avanzate. Il risultato è una protezione e una facilità d'uso di livelli inediti, che semplifica notevolmente la vita ai moderni professionisti dell'IT.

Per saperne di più e per provare in prima persona la sicurezza sincronizzata, visitare: sophos.it/heartbeat.

[1] Global Web Index, 18 febbraio 2016

[2] UK Business Insider, agosto 2015

[3] CNBC, febbraio 2016

[4] Briefing di ESG, Cybersecurity Skills Shortage: A State of Emergency, febbraio 2016

Sicurezza Sincronizzata

Per ulteriori informazioni, visitare:
sophos.it/heartbeat

Vendite per Italia:
Tel: (+39) 02 94 75 98 00
E-mail: sales@sophos.it

17-02-15 WPIT (DD-2560)

SOPHOS