SOPHOS
Security made simple.

Progetto Galileo

Le soluzioni di protezione Next-generation per reti, server ed enduser operano congiuntamente per offrire un livello di sicurezza efficace a tutte le aziende

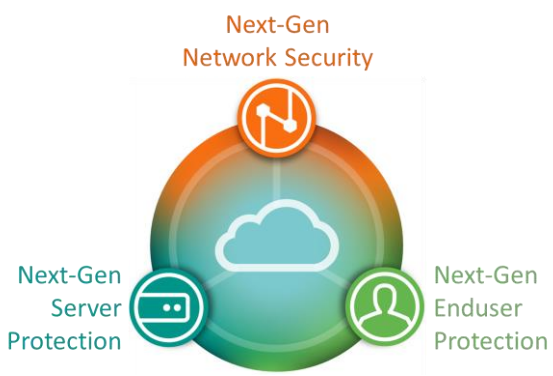
Informazioni di background

La maggior parte delle soluzioni di protezione disponibili sul mercato non sono al passo coi tempi. Gli IT Manager si vedono costretti a scegliere ed utilizzare soluzioni spesso incomplete, molto complesse e poco efficaci; Questo si traduce in un netto aumento di incidenti legati alla sicurezza informatica, quali sistemi compromessi e perdita di dati. Il *Verizon 2014 Data Breach Investigations Report* indica che nel corso del 2013 sono stati *registrati* 63.497 incidenti legati alla sicurezza informatica, 1.367 dei quali corrispondono a casi confermati di perdita di dati. Questi incidenti hanno coinvolto tutti i settori, dal finanziario a quello dell'hospitality, da enti per l'educazione ad istituzioni governative, oltre che numerose attività commerciali. Le grandi organizzazioni e le principali agenzie governative non sono state gli unici bersagli; ben un terzo degli incidenti registrati riguardanti il settore privato ha colpito aziende di piccole dimensioni.

La strategia Sophos

Sophos si pone sul mercato con una strategia completamente diversa che ha l'obiettivo di costruire un'infrastruttura di protezione efficace per tutte le aziende, che si basa su tre principi fondamentali:

1. **La sicurezza deve essere completa.** Le nostre soluzioni dispongono di tutte le funzionalità di sicurezza necessarie per rispondere in modo efficace alle esigenze dei nostri clienti.
2. **La sicurezza può essere semplificata.** Tutte le funzionalità incluse nelle nostre soluzioni sono estremamente semplici da utilizzare: dalle operazioni di delivery e gestione, alle opzioni di licenza e supporto, oltre che l'intera esperienza utente.
3. **La sicurezza è più efficace se viene considerata come un sistema.** L'idea di mettere in comunicazione e far cooperare in modo efficiente tutti i componenti tecnologici apre nuovissime opportunità rispetto ad ambienti in cui le diverse tecnologie implementate operano singolarmente.



L’obiettivo è quello di trasformare la vision in realtà ed integrare tecnologie di protezione all'avanguardia in tutti i prodotti per la sicurezza di reti, server ed enduser offerti. Ma questo non è tutto. Grazie al nuovo **Progetto Galileo**, inoltre, sarà possibile creare un reale collegamento tra le soluzioni per la protezione di reti, server ed enduser e tra questi e Sophos Cloud, creando una piattaforma di protezione unificata. Potremo così offrire una soluzione di sicurezza completa e facile da gestire, che opera a tutti gli effetti come un sistema e garantisce protezione ancora più efficace contro malware e minacce avanzate.

Integrazione efficace dei prodotti di sicurezza

Sono innegabili i vantaggi legati all'integrazione di più prodotti in un'unica console di gestione: riduzione dei costi, attuazione omogenea delle policy e gestione semplificata. Ma questo non è tutto: una soluzione integrata può garantire **protezione ancora più efficace**.

Le più tradizionali soluzioni di protezione possono essere paragonate alla sede di un'azienda protetta da due security guard, una collocata al di fuori dell'edificio e l'altra all'interno. Certamente disporre di due security guard ha i suoi vantaggi; se la guardia all'esterno non vede eventuali intrusi, è molto probabile che quella all'interno li individui. Se però le due guardie non comunicano fra loro, l'intruso dovrà semplicemente evitare la security per riuscire a mettere a segno il colpo.

Se le guardie invece sono munite di ricetrasmittenti che consentano loro di comunicare, e sono state addestrate al lavoro di squadra, nel caso in cui la guardia all'esterno senta rumori sospetti, potrà informare in tempo reale il collega all'interno. Mentre se la guardia all'interno vedrà un intruso che scappa, potrà immediatamente allertare il collega all'esterno che prontamente bloccherà gli accessi all'edificio. È quindi evidente che aumentando il livello di collaborazione fra le guardie, la sicurezza dell'intero edificio migliorerà notevolmente.

Con l'ascesa di minacce sempre più sofisticate, in grado di sfruttare tecnologie diversificate, è quasi impossibile per i prodotti che offrono un solo livello di protezione garantire sicurezza efficace. È quindi necessario sviluppare una nuova generazione di soluzioni di sicurezza capaci di collaborare fra loro e di condividere informazioni, oltre che di offrire protezione al passo coi tempi e senza la complessità dei prodotti attualmente sul mercato.

La realizzazione del Progetto Galileo

Progetto Galileo non è un prodotto, ma è la nuova vision di Sophos che ha come obiettivo l'integrazione e la collaborazione fra le soluzioni esistenti. Abbiamo programmato il rilascio dei primi componenti del Progetto Galileo per metà 2015, quando effettueremo l'integrazione di “heartbeat” (il “cuore” del sistema) fra la nostra soluzione Endpoint Protection e le appliance Sophos UTM. La prima versione di "heartbeat" dovrà consentire alle appliance UTM di rilevare gli endpoint compromessi, allertarli, in modo tale da consentire l'attuazione di tutte le misure di protezione necessarie, avvisare gli amministratori IT ed isolare gli endpoint colpiti da ogni utilizzo di Internet. Nel frattempo gli endpoint potranno identificare e terminare l'applicazione malevola e quindi comunicare all'appliance UTM e all'amministratore IT i dettagli della procedura eseguita. In questo modo una minaccia avanzata, che sarebbe altrimenti passata inosservata, viene invece automaticamente rilevata e bloccata, senza richiedere lunghe e dispendiose investigazioni e analisi da parte del dipartimento IT aziendale.

In programma abbiamo inoltre una roadmap ambiziosa e ricca di innovazioni, che consentirà nei prossimi mesi di realizzare al meglio tutti gli obiettivi del Progetto Galileo. Stiamo, per esempio, progettando la realizzazione di un “compromise center,” incluso in Sophos Cloud, in cui verranno raccolti gli eventi sospetti rilevati all’interno degli endpoint, dei server e dei dispositivi di rete. Come eventi si considerano ad esempio: tentativi falliti da parte del software di aumentare all’utente i privilegi a lui associati (per es. diventare amministratore), tentativi di esecuzione di applicazioni non incluse nelle whitelist dei server, oppure tentativi di stabilire connessioni di rete verso server di comando e controllo sospettati di essere gestiti da cybercriminali.

Sfruttando tutte le potenzialità delle analisi condotte da "big data" e dell'esperienza e competenza degli specialisti dei SophosLabs, il "compromise center" sarà in grado di stabilire collegamenti logici fra gli eventi raccolti e di identificare i sistemi infetti o le reti sotto attacco. Dal momento che Sophos Cloud consente di amministrare centralmente più prodotti, l'intera gamma di operazioni di controllo disponibili nei nostri prodotti (per es. cifratura file, rimozione malware, isolamento della rete ecc.) potrà entrare in gioco per garantire protezione dei dati efficace, limitando al minimo i danni. Le azioni di **prevenzione, rilevamento e rimozione** di malware e minacce avanzate garantiranno risultati eccellenti, mantenendo la parte gestionale in-the-cloud.