White paper

Controllo per l'intera durata dell'attacco: prima, durante e dopo

È il momento di passare a un nuovo modello di sicurezza.

L'attuale panorama delle minacce è totalmente diverso rispetto ad appena dieci anni fa. Gli attacchi piuttosto semplici che provocavano danni limitati hanno lasciato il posto alle attività criminali informatiche moderne, che sono sofisticate, ben finanziate e in grado di causare gravi danni alle aziende e all'infrastruttura nazionale. Questi attacchi avanzati, oltre a essere difficili da rilevare, rimangono anche a lungo all'interno della rete, accumulando risorse di rete per poter lanciare attacchi altrove.

Le linee di difesa tradizionali che, per quanto riguarda la protezione, si affidano esclusivamente al rilevamento e al blocco delle minacce non sono più adeguate. È il momento di passare a un nuovo modello di sicurezza in grado di gestire tutte le fasi dell'attacco: prima, durante e dopo.

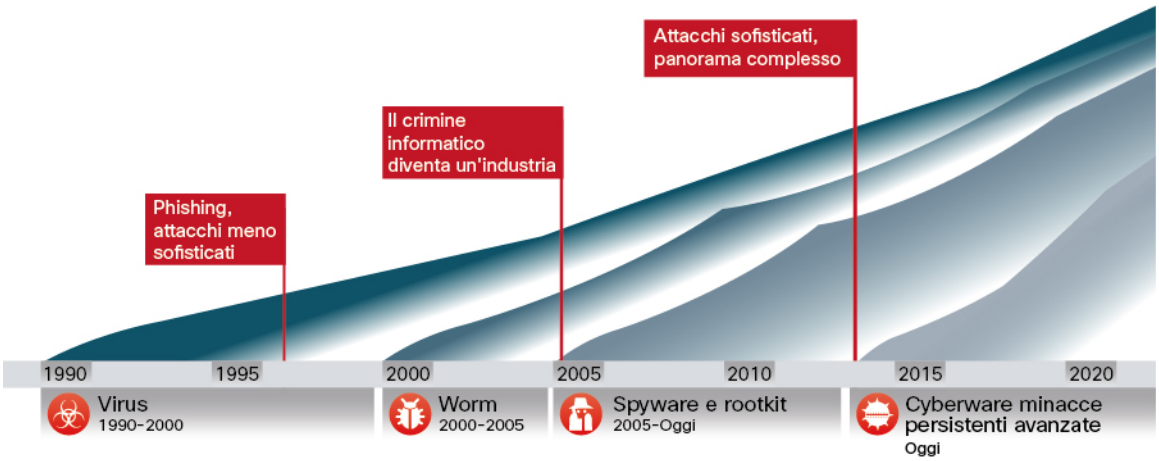
L'industrializzazione degli attacchi

I primi virus per PC risalgono a 25 anni fa. In pochi si resero conto che si trattava solo dell'inizio di un fenomeno che sarebbe sfociato nell'industrializzazione degli attacchi.

Per quasi 10 anni i virus hanno rappresentato il metodo di attacco principale e nel tempo i vari modelli di difesa sono stati sempre più in grado di bloccarli e offrire protezione. Motivati dalla notorietà e dalle conoscenze acquisite grazie alla scoperta e alla pubblicizzazione delle nuove vulnerabilità, gli autori degli attacchi hanno continuato a innovarsi. Ne sono derivati diversi cicli di minaccia che hanno dato luogo a una "corsa agli armamenti", per così dire. All'incirca ogni cinque anni gli autori degli attacchi lanciavano nuovi tipi di minacce, da macrovirus a worm, fino a spyware e Rootkits, e i modelli di difesa dovevano innovarsi rapidamente per proteggere le reti da queste minacce.

Non sorprende quindi che questi cicli possano essere correlati ai grandi cambiamenti tecnologici che si sono caratterizzati per nuovi vettori di attacco (vedere Figura 1). I primi virus prendevano di mira principalmente il sistema operativo e sono stati diffusi con modalità "net sneaker". I macro virus hanno approfittato di utenti che condividevano file. Le minacce di tipo worm che si spostavano da macchina a macchina si sono servite delle reti aziendali e del crescente utilizzo dell'attività Internet. Mentre gli spyware e i Rootkits sono emersi con le nuove applicazioni, i nuovi dispositivi e le nuove comunità online. Oggi dobbiamo affrontare malware avanzati, attacchi mirati e minacce avanzate persistenti (APT). Lo spartiacque tra la nuova era e il passato è costituito dalle motivazioni e dagli strumenti che si collocano alla base degli attacchi e che li rendono particolarmente difficili da rilevare, comprendere e bloccare.

Figura 1. L'industrializzazione degli attacchi



L'industrializzazione degli attacchi sta creando un'economia criminosa più rapida ed efficiente che trae profitto dagli attacchi all'infrastruttura IT. Lo scambio organizzato di exploit è prospero e redditizio, con il mercato aperto che contribuisce ad alimentare il passaggio dallo sfruttamento al furto, all'interruzione fino alla distruzione. Quando i criminali informatici hanno intravisto la possibilità di realizzare grandi guadagni, hanno iniziato a lavorare in un modo più standardizzato, automatizzato e basato su processo. Gli autori degli attacchi conoscono la natura statica delle classiche tecnologie per la sicurezza e le relative implementazioni eterogenee, quindi ne sfruttano le falle e le vulnerabilità. Generalmente i gruppi di hacker seguono persino i processi di sviluppo del software, come il test sulla certificazione di qualità o i test dei prodotti rispetto alle tecnologie di sicurezza prima del rilascio in modo da assicurarsi di poter continuare a eludere le protezioni comuni.

Attualmente vengono offerti notevoli incentivi finanziari per la segretezza e molti gruppi di "hactivist" sono motivati a lanciare attacchi che si traducono in guadagno economico o politico, con poche possibilità di ritorsioni o di azioni penali. Con i nuovi metodi, come hop di porte e protocolli, tunneling crittografato, dropper e minacce e tecniche miste, che utilizzano attacchi di ingegneria sociale e zero-day per gli hacker è più semplice, veloce ed economico accedere, mentre è più difficile rilevarli e bloccarli per i sistemi di difesa. Per complicare ulteriormente l'elusione, gli attacchi stessi possono cambiare rapidamente mentre progrediscono all'interno dell'azienda cercando una posizione salda ed esfiltrando dati importanti.

La sfida Any-to-Any

Le moderne reti estese moderne e i relativi componenti evolvono costantemente e generano nuovi vettori di attacco, ad esempio dispositivi mobili, applicazioni mobili e con interfaccia Web, hypervisor, social media, browser Web e computer integrati nonché una proliferazione di dispositivi e servizi che si riescono appena a immaginare, frutto di Internet of Everything. Le persone si trovano all'interno e all'esterno della rete, su qualsiasi dispositivo, con accesso a qualsiasi applicazione e in vari cloud. Questa ubiquità è la sfida "Any-to-Any" e, pur avendo rafforzato le comunicazioni, queste dinamiche hanno altresì moltiplicato i punti di accesso e i metodi utilizzati dagli hacker per sferrare gli attacchi. Purtroppo le modalità atte a garantire la sicurezza non si sono evolute di pari passo nella maggior parte delle aziende.

In genere le aziende proteggono le reti estese avvalendosi di diverse tecnologie che non funzionano congiuntamente. Potrebbero anche affidarsi ai provider di servizi per la sicurezza nel cloud e su società che forniscono servizi in hosting per proteggere l'infrastruttura Internet. In questa nuova realtà troppo spesso gli amministratori della sicurezza dispongono di poca visibilità e controllo sui dispositivi e sulle applicazioni che accedono alla rete aziendale e hanno una possibilità limitata di tenere il passo con le nuove minacce.

Nuove dinamiche di sicurezza

Di fronte alla combinazione di attacchi avanzati e all'infrastruttura Any-to-Any, i professionisti della sicurezza si pongono tre grandi domande:

1. *Con i nuovi modelli aziendali e i nuovi vettori di attacco, come è possibile mantenere la sicurezza e la conformità dinanzi a un panorama IT in continuo mutamento?* Le aziende in transizione verso la virtualizzazione del cloud o i dispositivi mobili per la produttività, l'agilità e l'efficienza fornite da queste tecnologie, devono adattare la propria infrastruttura di sicurezza.
2. *In un panorama in cui le minacce sono in evoluzione, come è possibile migliorare la capacità di fornire protezione continua contro nuovi vettori di attacco e minacce sempre più sofisticate?* Gli autori degli attacchi non fanno discriminazioni, colpiscono qualsiasi anello debole della catena. Nel portare a compimento i loro attacchi, spesso utilizzano gli strumenti che sono stati sviluppati appositamente per aggirare l'infrastruttura di sicurezza scelta come bersaglio. Mettono in atto tecniche molto sofisticate per sfuggire al rilevamento, utilizzando tecnologie e metodi che si traducono in indicazioni di compromissione quasi impercettibili.
3. *Come è possibile affrontare le prime due problematiche, riducendo al contempo la complessità e la frammentazione delle soluzioni di sicurezza?* Le aziende non possono permettersi di lasciare margini d'azione agli autori di attacchi più sofisticati. Allo stesso tempo, se si aggiunge complessità a causa delle soluzioni di sicurezza non integrate, non è possibile garantire il livello di protezione richiesto contro le minacce avanzate.

> *"Il 100% delle aziende dispone di connessioni ai domini noti come siti malware."*
>
> - Report annuale Cisco sulla sicurezza 2014

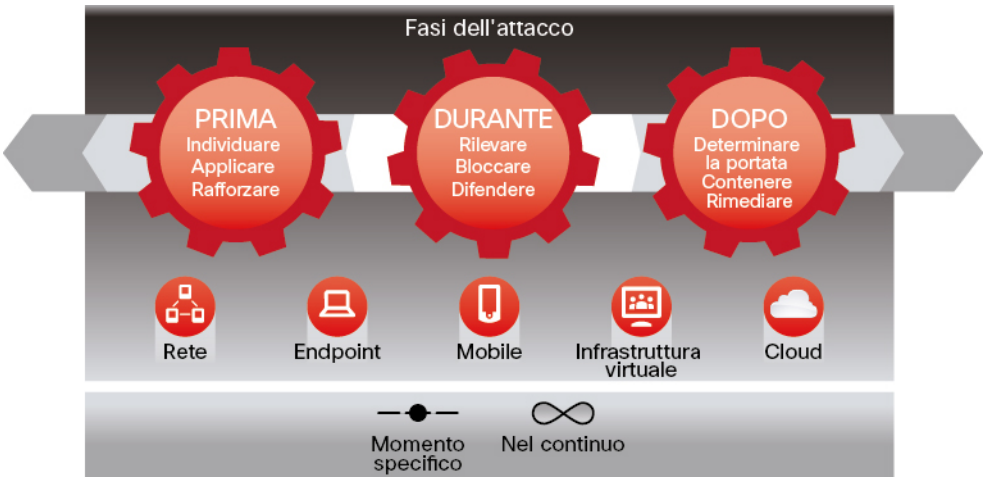
La combinazione di queste dinamiche - modelli aziendali e panorama dalle minacce in evoluzione, oltre a complessità e frammentazione della sicurezza - ha creato delle falle nella sicurezza, interrotto il ciclo di vita della sicurezza, ridotto la visibilità e introdotto problemi di gestione della sicurezza. Per proteggere realmente le aziende di fronte a queste dinamiche, è necessario cambiare l'approccio alla sicurezza. È arrivato il momento di adottare un nuovo modello di sicurezza incentrato sulle minacce.

Controllo per l'intera durata dell'attacco: prima, durante e dopo

La maggior parte degli strumenti di sicurezza attualmente è volto a fornire visibilità nella rete e bloccare il malware al punto di accesso. Questi strumenti eseguono la scansione dei file una volta sola in un momento specifico iniziale per determinare se sono dannosi. Ma gli attacchi avanzati non si verificano in un unico momento specifico, sono attività sistematiche e richiedono un controllo continuo. Ora i malintenzionati adottano tattiche come l'hop di porte, l'incapsulamento, gli attacchi zero-day, l'evasione del rilevamento comando e controllo (C&C), le tecniche di inattività, il movimento laterale, il traffico crittografato, le minacce miste e l'evasione sandbox per eludere il rilevamento iniziale. Se il file non viene rilevato o se si evolve e diventa dannoso dopo essersi inserito nell'ambiente, le tecnologie di rilevamento point-in-time cessano di essere utili nell'identificazione delle successive attività intraprese dall'autore dell'attacco.

I metodi di sicurezza non possono concentrarsi solo sul rilevamento, ma devono anche includere la capacità di mitigare l'impatto una volta che l'autore dell'attacco riesce nel suo scopo. Le aziende devono guardare al proprio modello di sicurezza in modo olistico e ottenere la visibilità e il controllo su tutta la rete estesa e su tutte le fasi dell'attacco: prima che si verifichi, mentre è in corso e anche dopo che sono stati danneggiati sistemi o che sono stati trafugati i dati (vedere Figura 2).

Figura 2. Il nuovo modello di sicurezza



- **Prima:** i modelli di difesa richiedono visibilità e riconoscimento completi di ogni elemento presente nella rete estesa per poter implementare policy e controlli atti a predisporre una difesa.
- **Durante:** la possibilità di rilevare continuamente i malware e bloccarli è di fondamentale importanza.
- **Dopo:** i modelli di difesa richiedono sicurezza retrospettiva per poter ridurre al minimo l'impatto dell'attacco. Devono identificare il punto di accesso, determinare la portata, contenere la minaccia, eliminare il rischio di una nuova infezione e rimediare al danno.

Prima dell'attacco

Per affrontare gli attacchi sensibili al contesto, è necessario disporre di sicurezza sensibile al contesto. Le aziende contrastano gli autori degli attacchi che hanno più informazioni sull'infrastruttura rispetto ai modelli di difesa impiegati per la protezione. Per assicurare protezione prima che si verifichi un attacco, le aziende hanno bisogno di una visibilità totale del proprio ambiente, tra cui, ad esempio, host fisici e virtuali, sistemi operativi, applicazioni, servizi, protocolli, utenti, contenuti e comportamento di rete, nel tentativo di ottenere più informazioni rispetto agli autori degli attacchi. Per i modelli di difesa è necessario comprendere i rischi per l'infrastruttura basandosi sul valore del target, sulla legittimità di un attacco e sulla cronologia. Se non si comprende quali sono gli elementi da difendere, non è possibile essere preparati a configurare le tecnologie per la sicurezza per difendersi. La visibilità deve coprire tutta la rete, dagli endpoint, ai gateway e-mail e Web, ai dispositivi mobili, fino al data center. Partendo dalla visibilità, devono essere generati avvisi proattivi in modo da poter prendere decisioni informate.

Durante l'attacco

Gli attacchi incessanti non si verificano in un unico momento specifico, sono attività sistematiche e richiedono una sicurezza continua. Le tecnologie per la sicurezza tradizionali possono solo rilevare un attacco in un momento specifico sulla base di un punto specifico di dati dell'attacco stesso. Questo approccio non è adeguato per le minacce avanzate. È invece necessaria un'infrastruttura di sicurezza basata sul concetto di riconoscimento che sia in grado di aggregare e correlare i dati attraverso la rete estesa tramite modelli di cronologia e intelligence degli attacchi globale, in modo da fornire contesto e distinguere tra attacchi attivi, esfiltrazione e attacchi di ricognizione e semplice rumore di fondo. In questo modo la sicurezza si evolve passando dall'applicazione in un momento specifico all'analisi e al processo decisionale continui. Ad ogni modo, se un file riuscisse a passare, in quando considerato sicuro, dimostrandosi successivamente dannoso, le aziende hanno ancora margine di azione. Grazie alla sicurezza basata su informazioni in tempo reale, i professionisti della sicurezza possono avvalersi dell'automazione intelligente per applicare le policy di sicurezza senza alcun intervento manuale.

Dopo l'attacco

Per affrontare tutte le fasi dell'attacco, le aziende hanno bisogno di sicurezza retrospettiva. La sicurezza retrospettiva è una sfida di Big Data ed è una capacità che solo pochi sono in grado di offrire. Grazie a un'infrastruttura in grado di raccogliere e analizzare continuamente i dati per creare informazioni sulla sicurezza, i team di sicurezza possono, attraverso l'automazione, individuare indicazioni di compromissione, rilevare il malware abbastanza sofisticato da modificare il proprio comportamento per evitare il rilevamento e quindi porre rimedio al problema. Le compromissioni che passano inosservate per settimane o mesi possono essere identificate e ne può essere determinata la portata, possono venire contenute e si può porre rimedio all'eventuale danno.

Questo modello di sicurezza incentrato sulle minacce consente alle aziende di affrontare tutte le fasi dell'attacco, su tutti i vettori di attacco e rispondere sempre in qualsiasi momento e in tempo reale.

Il nuovo modello di sicurezza

Per favorire l'utilizzo di un nuovo modello di sicurezza, Cisco ritiene che le moderne tecnologie per la sicurezza debbano concentrarsi su tre priorità strategiche: devono basarsi sulla visibilità e sulla piattaforma ed essere incentrate sulle minacce.

Visibilità: gli amministratori della sicurezza devono essere in grado di visualizzare con precisione ogni evento in corso. Questa capacità richiede una combinazione di ampiezza e profondità (vedere Figura 3). Con ampiezza si intende la capacità di vedere e raccogliere dati da tutti i potenziali vettori di attacco attraverso il fabric di rete, gli endpoint, i gateway e-mail e Web, i dispositivi mobili, il cloud e i sistemi virtuali per reperire informazioni sugli ambienti e sulle minacce. La profondità offre la capacità di associare queste informazioni e applicarle per comprendere il contesto, prendere decisioni migliori e agire sia manualmente sia automaticamente.

Figura 3. Ampiezza e profondità

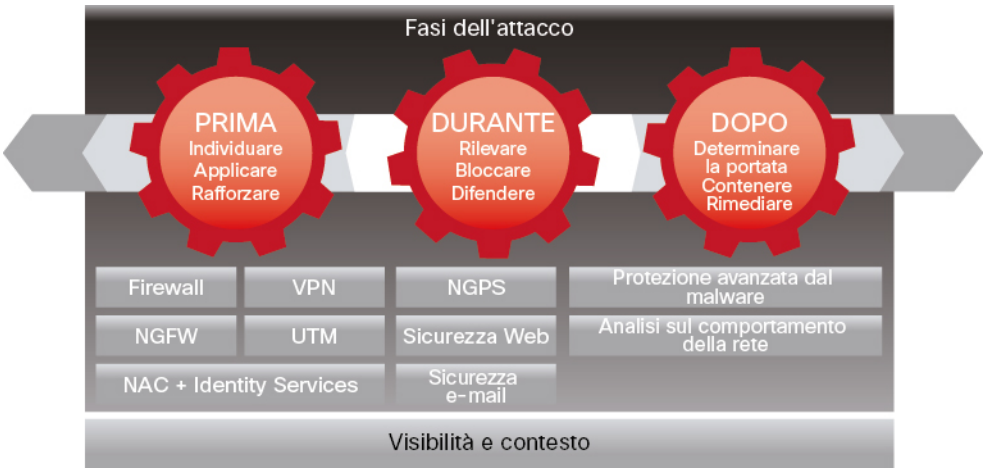
Focus sulle minacce: le reti attuali si estendono a qualsiasi punto in cui si trovano i dipendenti, i dati e ai relativi punti di accesso. Benché ci si impegni al massimo, tenere il passo con vettori di attacco in costante evoluzione rappresenta una sfida per i professionisti della sicurezza e un'opportunità per gli autori degli attacchi. Le policy e i controlli sono fondamentali per ridurre l'area vulnerabile agli attacchi, ma le minacce possono comunque eluderli. Di conseguenza le tecnologie devono incentrarsi anche sul rilevamento, la comprensione e il blocco delle minacce. Focalizzandosi sulle minacce, viene preso in considerazione l'approccio del fautore dell'attacco, si applicano la visibilità e il contesto per identificare i cambiamenti e adattarsi al nuovo ambiente e successivamente si sviluppano le protezioni per attivarsi e fermare le minacce. A causa dei malware avanzati e degli attacchi zero-day, questo è un processo costante che richiede informazioni sulla sicurezza in tempo reale e analisi continue fornite dal cloud e condivise in tutti i prodotti per conseguire una maggiore efficacia.

Importanza della piattaforma: al momento la sicurezza rappresenta più di un semplice problema relativo alla rete, richiede un sistema integrato di piattaforme agili e aperte che comprende rete, dispositivi e cloud. Queste piattaforme devono essere estensibili, progettate per la scalabilità e gestite centralmente per assicurare policy unificate e controlli coerenti. In definitiva, devono essere pervasive quanto gli attacchi. A tal fine è necessario passare dall'implementazione di singole appliance di sicurezza all'adozione di una piattaforma con servizi e applicazioni realmente scalabili e facili da implementare. Un approccio basato sulla piattaforma, oltre ad aumentare l'efficacia della protezione, eliminando barriere e falle della sicurezza, accelera altresì i tempi di rilevamento e semplifica l'esecuzione.

Controllo per l'intera durata dell'attacco

Per superare le attuali sfide di sicurezza e ottenere una migliore protezione, le aziende hanno bisogno di soluzioni che coprono tutte le fasi dell'attacco, che siano progettate in base agli assunti su visibilità e importanza della piattaforma e focus sulle minacce. Cisco offre una gamma completa di soluzioni di sicurezza informatica incentrate sulle minacce in grado di coprire tutte le fasi dell'attacco.

Figura 4. Controllo per l'intera durata dell'attacco



Queste soluzioni specifiche basate sulla piattaforma offrono la più vasta gamma del settore di opzioni di applicazione e correzione ai vettori di attacco in cui si manifestano le minacce. Funzionano congiuntamente per garantire protezione in tutte le fasi dell'attacco e si integrano in soluzioni complementari per realizzare un sistema di sicurezza globale.

- Prima dell'attacco le soluzioni che ad esempio includono firewall, firewall di prossima generazione, Network Access Control e Identity Services offrono ai professionisti della sicurezza gli strumenti per identificare le minacce e applicare nonché rafforzare le policy.
- Durante l'attacco le soluzioni Next-Generation Intrusion Prevention System e le soluzioni di sicurezza e-mail e Web permettono di rilevare, bloccare gli attacchi che sono penetrati nella rete e sono attualmente in corso, predisponendo una difesa idonea.
- Dopo l'attacco le aziende possono avvalersi di Cisco Advanced Malware Protection e dell'analisi del comportamento della rete per riuscire in modo rapido ed efficace a determinare la portata dell'attacco, contenerlo e porvi rimedio riducendo al minimo i danni.

Grazie a una scalabilità che si adatta anche alle imprese globali di grandi dimensioni, queste soluzioni sono disponibili a seconda delle esigenze dell'azienda in termini di tempi e modalità, sotto forma di appliance fisiche o servizi basati su cloud. Sono anche integrate per fornire visibilità e controllo costante sulla rete estesa e su tutti i vettori di attacco.

Conclusioni

L'industrializzazione degli attacchi unitamente alla sfida Any-to-Any stanno provocando un drastico cambiamento nelle modalità di protezione dei sistemi, dando luogo a un nuovo approccio alla sicurezza informatica. Con le strategie di sicurezza che si concentrano sulle linee di difesa perimetrali e sulle tecniche preventive, gli autori degli attacchi possono agire indisturbati una volta che riescono ad accedere all'interno della rete.

L'evoluzione dei modelli aziendali e del panorama delle minacce, oltre alle complessità e alla frammentazione della sicurezza hanno creato delle falle nella sicurezza, interrotto il ciclo di vita della sicurezza, ridotto la visibilità e introdotto problemi di gestione della sicurezza. È arrivato il momento di passare a un nuovo modello di sicurezza incentrato sulle minacce, che sia in grado di offrire la visibilità e il controllo richiesti dalle aziende sulla rete estesa e per tutte le fasi dell'attacco.

Cisco offre una capacità esclusiva di realizzare questo tipo di approccio alla sicurezza, riducendo la complessità, ma con la garanzia di una visibilità superiore, un controllo continuo e la protezione dalle minacce avanzate in tutte le fasi dell'attacco. Con questo nuovo modello di sicurezza le aziende possono agire in modo più intelligente e rapido prima, durante e dopo l'attacco.

Sede centrale Americhe
Cisco Systems Inc.
San Jose, CA (USA)

Sede centrale Asia e Pacifico
Cisco Systems (USA) Pte. Ltd.
Singapore

Sede centrale Europa
Cisco Systems International BV Amsterdam,
Paesi Bassi

Le sedi Cisco nel mondo sono oltre 200. Gli indirizzi, i numeri di telefono e di fax sono disponibili sul sito web Cisco all'indirizzo **www.cisco.com/go/offices**.

Stampato negli Stati Uniti C11-731741-01 06/14