PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 16 - numero 3438 di mercoledì 26 novembre 2014

La rivoluzione nella protezione

La protezione dei sistemi informatici: come evolvere l'approccio alla sicurezza informatica affinché sia realmente efficace.

La Rivoluzione industriale ha cambiato per sempre il mondo, creando settori dell'economia più agili e più efficienti. Basandosi su questo importante periodo storico, molto è stato scritto sull'Industrializzazione dell'Hacking, un settore particolarmente dinamico che ha l'obiettivo di trarre profitto dagli attacchi informatici alle nostre infrastrutture IT. Alimentati dalla convergenza di metodi meccanici e guidati dai processi, incentivi politici e sociali, punti deboli nella sicurezza e nuove vulnerabilità nei modelli di business in continua evoluzione, gli hacker sferrano attacchi sempre più sofisticati e dannosi. Questa era sta cambiando profondamente le modalità di protezione dei nostri sistemi, portandoci a riflettere su come evolvere il nostro approccio alla sicurezza informatica.

Come professionisti della sicurezza, dobbiamo seguire una traiettoria simile a quella degli hacker e applicare quanto imparato dalla Rivoluzione Industriale per diventare più veloci, più efficienti e più efficaci nel nostro settore: una sorta di "Rivoluzione nella Protezione". Le tecnologie e le funzionalità a disposizione degli hacker sono notevolmente migliorate e ciò deve accadere anche per quelle a disposizione di chi si deve difendere. Tutto ciò ci da un'occasione unica per muoverci verso sistemi di sicurezza basati su un'ampia visibilità, un'approfondita raccolta dei dati, sulla capacità di apprendere attraverso la correlazione e il contesto e, di conseguenza, l'applicazione dinamica dei controlli.

Nel corso degli anni, l'hacking (o pirateria informatica) si è evoluto e la protezione deve progredire a sua volta. E' necessario considerare il controllo statico, quello che necessita dell'intervento umano, quello semi-automatico, quello dinamico e quello intuitivo:

Controllo statico ? un ambiente in cui i controlli critici esistono ma non la visibilità e l'intelligenza per aggiornarli. Molte tecnologie di sicurezza point-in-time tradizionali lavorano in questo modo, il sistema che fornisce protezione necessità dell'intervento del vendor per essere aggiornato. Questo approccio ha funzionato abbastanza bene quando il principale metodo di attacco è stato il virus su PC. Ma oggi, di per sé, non fornisce tutto ciò di cui ha bisogno un sistema preposto alla protezione, per valutare correttamente il suo stato di sicurezza e per apportare modifiche in tempo reale. Tuttavia, in alcune implementazioni, questi controlli sono destinati ad essere statici per essere conformi alle normative. E sebbene forniscano una protezione base, non hanno ancora l'agilità per proteggersi e adattarsi in ambienti in continuo cambiamento.

Controlli che richiedono l'intervento umano ? Visibilità e intelligenza sono disponibili, ma i controlli devono comunque essere modificati manualmente. Un intervento manuale intensivo non è sostenibile dato il ritmo e la complessità degli attacchi, nonché la carenza di competenze nell'ambito della sicurezza informatica. Sebbene i controlli statici siano la realtà nella maggior parte delle organizzazioni di oggi, sono stati creati numerosi Security Operations Centers (SOC) per compensare la mancanza di flessibilità e agilità di tali controlli e la mancanza di personale qualificato interno. Ricorrere a un intervento umano per effettuare le necessarie modifiche alla sicurezza non può funzionare con le moderne minacce che utilizzano nuovi metodi che rendono ancora più semplice e meno costoso sferrare attacchi, penetrare nella rete e cambiare rapidamente mentre progrediscono all'interno dell'azienda.

Controlli semi-automatici ? vi è visibilità e intelligenza e, in alcuni casi, è concesso ai sistemi di applicare automaticamente alcuni controlli. Tuttavia, per i dati più sensibili ? considerando che la protezione dei dati non avviene in modo uguale ? questo tipo di ambienti permetteranno ai sistemi di automatizzare e generare suggerimenti ma richiederanno comunque un intervento

umano per la revisione e la pressione del giusto tasto. Ma questi dati altamente sensibili sono proprio il bersaglio preferito degli hacker. E tornando all'intervento umano, si da un'opportunità in più all'hacker. Negli ambienti semi-automatici la protezione sta evolvendo, ma non è sufficientemente standardizzata, meccanizzata e guidata dai processi come dovrebbe essere per essere efficace.

Controlli dinamici ? Chi si deve difendere utilizza visibilità e intelligenza per adattarsi rapidamente e in tempo reale alle policy di sicurezza e alla loro applicazione basandosi su ciò che si è imparato per ridurre la superficie di attacco . I controlli dinamici offrono già un elevato livello di automazione, dove i sistemi di sicurezza rispondono automaticamente alle minacce. L'automazione è stata alla base della Rivoluzione Industriale ed è il cuore della Rivoluzione nella Protezione. Rappresenta l'unico modo per combattere i moderni attacchi che aggirano la protezione utilizzando metodi quali ad esempio l'hopping della porta/del protocollo, il tunneling cifrato, i dropper, le minacce combinate e le tecniche che integrano il social engineering e gli attacchi zero-day. Questi attacchi cambiano rapidamente poiché progrediscono all'interno dell'azienda alla ricerca di un punto d'appoggio permanente e sottrarre i dati critici. Grazie a controlli dinamici, i professionisti della sicurezza aumentano il livello di automazione basato sulla "fiducia adattiva" o sulla maggiore fiducia nei dispositivi, negli utenti e nelle applicazioni. E possono implementare le tecnologie appropriate, se necessario, per la massima flessibilità. I controlli dinamici esistono già e sono necessari per rispondere alle nuove pressioni sulla sicurezza dettate dalla mobility, dal cloud, dall'Internet of Things (IoT) e dall'Internet of Everything (IoE).

Intuitivi ? Un ambiente intuitivo non significa necessariamente che sia in grado di prevedere un attacco prima che si verifichi, ma piuttosto di sfruttare l'apprendimento automatico e l'analisi avanzata per apprendere e migliorare costantemente l'intelligenza, per arrivare alla definizione delle priorità nel controllo, nella protezione e nella remediation. Le basi per sviluppare tecnologie intuitive ci sono ma sono ancora in una fase iniziale. Nel tempo, continueremo a evolvere e migliorare in questo senso, liberando tutta la potenza di una nuova era nella protezione.

L'avanzamento dei controlli alla sicurezza di certo non avverrà dall'oggi al domani. Ma siamo sulla buona strada con tecnologie e funzionalità che stanno già andando in questa direzione, implementando controlli dinamici per avere maggiore visibilità, apprendere di più e adattarsi rapidamente ai cambiamenti. Il modo e la velocità con cui ci muoviamo, nonché dove giungeremo dipenderanno dai nostri modelli e dalle infrastrutture esistenti, dai requisiti del settore, dalle risorse disponibili e dalle esperienze. Una cosa è certa: la nuova era ci permetterà di rivoluzionare il modo in cui ci proteggiamo dagli attacchi informatici.

Stefano Volpi

---

www.puntosicuro.it