Cosa ci aspetta? Previsioni sulla sicurezza per il 2017

Date : 9 novembre 2016

David Gubiani di Check Point parla di quello che ci aspetta nel 2017, in termini di sicurezza informatica

“È difficile fare previsioni, soprattutto sul futuro”, disse il danese Niels Bohr, premio Nobel per la Fisica nel 1922. Dal momento che la fine del 2016 si avvicina, è utile cercare di capire le tendenze sulla sicurezza informatica che ci aspettano e riflettere su quello che è successo quest’anno, per vedere quanto accurate siano state le previsioni fatte per il 2016. L’anno scorso avevamo previsto:

- L’emergere di malware sofisticati e personalizzati progettati per superare le difese delle organizzazioni. I criminali stanno utilizzando varianti su misura di malware esistenti, che sono in grado di aggirare i tradizionali antivirus e strumenti di sandboxing - il nostro Security Report 2016 ha rivelato che ben 971 varianti sconosciute di malware vengono scaricate nelle reti aziendali ogni ora.
- Attacchi mobile - avevamo predetto un aumento di questo tipo di attacchi dal momento che i dispositivi mobili sono diventati sempre più comuni nel mondo del lavoro, offrendo agli hacker un accesso diretto e potenzialmente remunerativo ai dati personali e aziendali. Anche questo è stato confermato - abbiamo visto l’avvento di grandi vulnerabilità come Quadrooter e nuove minacce zero-day, così come un aumento di malware che sfruttano vulnerabilità dei dispositivi mobile.
- Attacchi a infrastrutture critiche - ci aspettavamo che questi aumentassero dal momento che i criminali informatici cercano di sfruttare sia le vulnerabilità insite nei sistemi informatici delle infrastrutture critiche, sia il danno potenzialmente enorme che può essere provocato. Infatti, un attacco che utilizza il malware BlackEnergy ha colpito una società elettrica Ucraina, l’aeroporto Chopin di Varsavia è stato preso di mira da un attacco DDoS e anche i sistemi SCADA della diga Bowman a Rye, New York, sono stati attaccati.
- I criminali informatici che approfittano della crescita dell’Internet of Things e colpiscono sempre più dispositivi smart. Quest’anno abbiamo assistito a uno dei più grandi attacchi DDoS di sempre che ha colpito il sito del blogger specializzato in sicurezza, Brian Krebs. Questo attacco è stato sferrato da milioni di telecamere di sicurezza e altri dispositivi IoT simili.

Purtroppo, le nostre previsioni per il 2016 sono state accurate. Come la maggior parte di chi si occupa di sicurezza informatica, preferirei che non fosse stato così. Mi piacerebbe ancora di più che le aziende non fossero vittima di infezioni da malware, hackeraggi, o violazioni dei dati. Ma prevedendo la prossima ondata di minacce informatiche, speriamo di aiutare le aziende a rimanere un passo avanti gli exploit dei criminali informatici.

Quindi, ecco qui le nostre cinque previsioni sulla sicurezza informatica per il 2017:

Mobile: bersagli in movimento - Dal momento che gli attacchi ai dispositivi mobili continuano a crescere, possiamo aspettarci che gli attacchi informatici alle aziende originati dai dispositivi mobili, diventeranno una delle principali preoccupazioni della sicurezza per le aziende. La recente scoperta di non uno, ma tre vulnerabilità zero-day nell'Apple iOS, a seguito del tentativo di attacco al telefono di un attivista per i diritti umani, mette in luce quanto rapidamente l'industria della sorveglianza e del crimine informatico mobile si stia espandendo - e la necessità, per le aziende, di proteggere i propri dispositivi mobile contro malware, intercettazioni delle comunicazioni e altre vulnerabilità.

Convergenza tra IT e OT - Durante il prossimo anno, ci aspettiamo di vedere un'ulteriore diffusione degli attacchi informatici verso l'IoT industriale. La convergenza tra le tecnologie informatiche (IT) e la tecnologia operativa (OT) sta rendendo entrambi gli ambienti più vulnerabili, in particolare quello della tecnologia operativa degli ambienti SCADA. Questi ambienti spesso eseguono sistemi datati, per i quali le patch non disponibili, o peggio, semplicemente non vengono utilizzate. Molti sistemi di controllo industriali critici sono aperti a Internet - un recente rapporto ha rilevato che oltre 188.000 sistemi in 170 paesi erano accessibili in questo modo. Il 91% è sfruttabile da remoto da parte di hacker, e oltre il 3% ha vulnerabilità sfruttabili. Il manufacturing, come industria, dovrà estendere i controlli dei sistemi e della sicurezza fisica allo spazio logico e implementare soluzioni di prevenzione delle minacce negli ambienti IT e OT.

Infrastrutture critiche - Ancora una volta, indichiamo le infrastrutture critiche nelle nostre previsioni per il prossimo anno - a livello globale, queste rimangono altamente vulnerabili a un attacco informatico. Quasi tutte le infrastrutture, comprese le centrali nucleari, le reti elettriche e quelle per le telecomunicazioni, sono infatti state progettate e costruite prima dell'avvento della minaccia di attacchi informatici. A inizio 2016 è stato segnalato il primo blackout causato intenzionalmente da un attacco informatico. I responsabili della sicurezza delle infrastrutture critiche devono dunque prepararsi alla possibilità che le loro reti e i loro sistemi possano essere attaccati in modo sistematico da diversi attori: altri stati, terroristi e criminalità organizzata.

Prevenzione delle minacce - Parlando di aziende, prevediamo che i ransomware diventeranno diffusi quanto gli attacchi DDoS. Al pari degli attacchi DDoS, le infezioni da ransomware possono bloccare le operazioni quotidiane di un'azienda e la loro mitigazione richiede una strategia di prevenzione multi-strato, che includa tecniche di sandboxing e di estrazione delle minacce avanzate. Le aziende dovranno prendere in considerazione diverse alternative per fronteggiare le persone che lanciano campagne di ransomware. Strategie collaborative come arresti coordinati con colleghi del settore e l'applicazione della legge saranno cruciali. Se è vero che pagare un riscatto non è mai consigliato, perché incoraggia attacchi futuri, a volte è l'unica

opzione per il recupero dei dati e la possibilità di lavorare. Dunque, la disponibilità di riserve finanziarie per velocizzare i pagamenti diventerà sempre più comune.

Prevediamo anche più attacchi mirati a influenzare o far tacere un'organizzazione, con attori “legittimati” che sferrano questi attacchi. L'attuale campagna presidenziale degli Stati Uniti mostra questa possibilità e servirà come precedente per le future campagne.

Diffusione del cloud - Dal momento che le aziende continuano a conservare sempre più dati sul cloud, fornendo una backdoor per gli hacker che vogliono accedere ad altri sistemi aziendali, un attacco mirato a disturbare o spegnere uno dei principali fornitori di servizi cloud avrà ripercussioni sul business di tutti i suoi clienti - come abbiamo visto con il recente attacco DDoS contro il servizio di domain directory DynDNS. Sebbene molto dirompente, un attacco di questo tipo potrebbe essere utilizzato anche solo per colpire un concorrente o un’azienda specifica, che sarebbe uno dei tanti interessati, e quindi renderebbe difficile determinare la fonte.

Infine, ci aspettiamo di vedere un aumento degli attacchi da ransomware diretti verso i data center basati su cloud. Dal momento che sempre più aziende adottano il cloud, sia pubblico che privato, questo tipo di attacchi inizierà a trovare il modo di infiltrarsi in questa nuova infrastruttura, usando sia la diffusione di file crittografati da cloud a cloud, sia utilizzando il cloud come un moltiplicatore di volume.