IBM Threat Protection System e Critical Data Protection Services per promuovere la lotta contro le minacce informatiche

Con l'aumento del costo delle violazioni dei dati e degli Advanced Persistent Threat, IBM aiuta i clienti a rilevare, prevenire e reagire agli attacchi

Milano - 08 mag 2014: IBM ha presentato nuovi software e servizi per la sicurezza in grado di aiutare le organizzazioni a proteggere i loro dati critici in un contesto come quello attuale in cui minacce di tipo Advanced Persistent Threats, attacchi di tipo "zero day", violazioni dei dati e relativo impatto economico sono in continuo aumento. Grazie ai sempre più diffusi strumenti di analytics – che permettono di prevedere le conseguenze di comportamenti umani – e all'esperienza dei propri ricercatori, IBM aiuta le organizzazioni a impedire agli hacker di sfruttare queste vulnerabilità. Secondo due studi del Ponemon Institute, commissionati da IBM, il costo medio aziendale delle violazioni di dati è aumentato del 15% a livello globale, raggiungendo una media di 3,5 milioni di dollari. La maggior parte delle aziende intervistate afferma che gli attacchi mirati costituiscono la minaccia più grande, con un costo medio di 9,4 milioni di dollari solo in termini di valore del brand.
L'annuncio dell'IBM Threat Protection System e del Critical Data Protection Program è il frutto di due anni di investimenti significativi nello sviluppo dell'offerta e nell'acquisizione di società, tra cui *Q1 Labs, Trusteer, Guardium, Ounce Labs, Watchfire e Fiberlink/MaaS360*. Dall'annuncio della divisione dedicata alla sicurezza avvenuto a fine 2011, IBM è diventata uno degli attori più importanti nel mercato della sicurezza aziendale, conseguendo una crescita a due cifre per sei trimestri consecutivi. Secondo il Software Tracker di IDC, la crescita di IBM ha superato in misura significativa quella del mercato del software di sicurezza, salendo nel 2013 dal 4° al 3° posto tra i fornitori di soluzioni per la sicurezza.

IBM Threat Protection System aiuta a prevenire gli attacchi – prima che si verifichi il danno
Il nuovo Threat Protection System di IBM è basato sulla Security Intelligence e sull'Analytics e permette di andare al di là delle difese tradizionali di controllo accessi e firewall tradizionali, permettendo di interrompere gli attacchi sull'intera catena – dall'intrusione (*break-in*) alla sottrazione dei dati (*exfiltrate*).

IBM Threat Protection System si basa su un'architettura end-to-end, costituita da software di analitica e indagine, per aiutare le organizzazioni a prevenire, rilevare e reagire ai cyber-attacchi continui e sofisticati e, in alcuni casi, a eliminare la minaccia prima che si verifichi il danno. Tra i punti salienti:

- La **prevenzione**, IBM annuncia una nuova soluzione Trusteer Apex per il blocco del malware negli endpoint, e significativi potenziamenti dell'appliance IBM Network Protection tra cui la funzionalità di quarantena e relative integrazioni con le sandbox fornite dai principali partner.

- Il **rilevamento**, IBM potenzia la sua piattaforma di Security Intelligence QRadar con nuove funzionalità, consentendo alle organizzazioni di rilevare gli attacchi attualmente presenti su nuova scala e di bloccare gli exploit rilevati con un semplice clic.

- La **risposta**, IBM presenta IBM Security QRadar Incident Forensics ed inoltre continua ad espandere i suoi Emergency Response Services presenti a livello globale.

I clienti che stanno testando IBM Threat Protection System hanno riscontrato risultati immediati. Ad esempio, un'azienda sanitaria con migliaia di endpoint ha rilevato immediatamente la presenza di decine di istanze di malware, nonostante l'uso di svariati tool di sicurezza tradizionali. Questo codice malevolo avrebbe potuto

essere sfruttato per controllare gli endpoint in remoto o sottrarre i dati, ma è stato invece disabilitato all'istante. Analogamente, una grande banca europea ha sperimentato di recente le funzionalità messe a disposizione dalla soluzione ed è riuscita a individuare e disabilitare malware non rilevato e presente in tutta l'azienda.

IBM Threat Protection System è supportato in tutto il mondo dai Security Operations Center (SOC) di IBM, che possono monitorare i sistemi di produzione dei clienti in servizio. I consulenti IBM possono inoltre disegnare e realizzare progetti di integrazione dei SOC IBM con i SOC dei clienti.

"Gli Advanced Persistent Threat hanno cambiato radicalmente il modo in cui le organizzazioni devono affrontare la sicurezza dei dati", spiega Brendan Hannigan, General Manager, IBM Security Systems. "Oggi per difendersi dai cyber-attacchi non basta più un approccio 'signature-based' o perimetrale. Approfondite funzionalità analitiche e indagini accurate sono essenziali e devono comprendere prevenzione degli endpoint, protezione perimetrale e capacità di difendersi dagli attacchi prima che possano causare danni".

IBM Security Services per la salvaguardia del valore di un'azienda e la protezione del marchio
Il nuovo Critical Data Protection Program aiuta a proteggere i dati critici, ovvero il valore di un'azienda. La fortuna di un'organizzazione è spesso generata da meno del 2% dei suoi dati aziendali, ma che hanno un impatto sostanziale su vantaggio competitivo, reputazione del marchio, valore di mercato e crescita di business.

"I timori riguardo alla capacità di proteggere i dati critici dai cyber-attacchi sono ormai all'attenzione dei vertici aziendali", spiega Kris Lovejoy, General Manager, IBM Security Services. "Gli attacchi informatici e la perdita di dati hanno la capacità di influire sulla reputazione del marchio, di ridurre il valore per gli azionisti e di esporre un'organizzazione a controversie legali. Il nuovo software e i nuovi servizi di IBM sono progettati per fornire alle aziende una soluzione esclusiva, che consenta ai vertici aziendali di focalizzarsi sul business e sui propri clienti".

Le organizzazioni si rivolgono sempre più a IBM per definire un approccio alla sicurezza che sia realmente completo e finalizzato a individuare e prevenire rapidamente le minacce prima che possano fare danni. I nuovi servizi di consulenza per la sicurezza si basano sull'esclusivo Data Centric Security Model di IBM, basato su soluzioni come Guardium e StoredIQ e su IBM Research per aiutare a proteggere le informazioni aziendali critiche.

Si stima che i dati critici aziendali, che possono comprendere risorse di altissimo valore come piani di acquisizione e dismissione, delibere del consiglio direttivo e proprietà intellettuale, rappresentino il 70% del valore di una società quotata in borsa. Di conseguenza, questo tipo di dati è ad alto rischio di attacco, sia da parte di soggetti interni all'azienda sia di hacker sofisticati.

Nonostante l'importanza e il valore dei dati aziendali critici, molte organizzazioni addirittura non sanno quali siano le informazioni più preziose, dove risiedano, chi vi abbia accesso o come siano protette, rendendo quindi difficile il loro monitoraggio e la loro protezione. In effetti, in più del 95% dei casi possono essere necessari diversi giorni per scoprire una perdita di dati e, in oltre il 90% dei casi, più settimane per arginarla. Questi tempi possono avere un impatto catastrofico su un'azienda.

Il nuovo Critical Data Protection Program di IBM offre un approccio multifase iterativo, che passa attraverso le fasi di definizione (Define), rilevazione (Discover), Baseline, protezione (Secure) e monitoraggio (Monitor) per l'intero ciclo di vita della sicurezza dei dati, con l'obiettivo di salvaguardare redditività, vantaggio competitivo e

reputazione.

IBM Security

Il portafoglio IBM per la sicurezza fornisce la Security Intelligence necessaria per aiutare le organizzazioni a proteggere in modo completo dipendenti, dati, applicazioni e infrastruttura. IBM offre soluzioni per la gestione delle identità e degli accessi, la gestione delle informazioni e degli eventi di sicurezza, la sicurezza del database, la sviluppo applicativo, la gestione del rischio, la gestione degli endpoint, la protezione dalle intrusioni più de molto altro ancora. IBM gestisce una delle più vaste organizzazioni al mondo per la ricerca e sviluppo e per il delivery di servizi in materia di sicurezza. IBM monitora 15 miliardi di eventi di sicurezza al giorno, in più di 130 paesi, e detiene più di 3.000 brevetti in materia. Per ulteriori informazioni, visitate il sito www.ibm.com/security, seguite @IBMSecurity su Twitter, oppure visitate il blog di IBM Security Intelligence.
