PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 18 - numero 3690 di martedì 05 gennaio 2016

Cyberthreat Defense Report ? il punto sugli attacchi informatici

È finalmente disponibile un rapporto annuale sulle minacce informatiche, che rappresenta una lettura pressoché obbligatoria per qualunque responsabile della protezione dei sistemi informativi. Di Adalberto Biasiotti.

E' con una certa amarezza che si constata che oggi le difese disponibili ed attuate contro forme tradizionali di attacchi criminosi, come ad esempio le rapine ed i furti, sono assai più efficienti di quelle disponibili ed adottate per la protezione da attacchi informatici.
Il furto di dati, di cui è rimasto vittima all'ufficio del personale federale americano, ne è una drammatica prova: in questo caso, oltre 40 milioni di dati personali, anche sensibili, di dipendenti federali sono stati sottratti dai malviventi.
Senza andare al di là dell'Atlantico, ma rimanendo a casa nostra, l'attacco subito dalla azienda Hacking Team, che forniva software di spionaggio discreto ad enti pubblici e privati di tutto il mondo, ha sollevato un gran polverone. Lo stesso capo della polizia, Pansa, ha dichiarato che l'attacco subito da questa azienda, che ha compromesso l'utilizzabilità dei suoi software, ha compromesso numerose indagini in corso, che venivano sviluppate grazie alla possibilità di sottrarre dati personali presenti a bordo di telefoni cellulari e computer, in possesso di persone indagate.

Il rapporto, che è stato messo appunto dalla ormai famosa CyberEdge Group, offre un quadro accurato e preoccupante di come i professionisti della sicurezza informatica percepiscono la minaccia di crimine informatico e mettono a punto i piani di difesa.
Questo studio è stato condotto intervistando più di 800 responsabili della sicurezza informatica, è stato ultimato nel dicembre 2014 ed è stato pubblicato nel giugno 2015. I risultati dell'indagine sono oltremodo preoccupanti e permettono di inquadrare quali sia l'atteggiamento di molti responsabili della sicurezza e dell'alta direzione, nei confronti di questi rischi.
Offriamo di seguito una sintesi delle principali risultanze dello studio.

- Con un certo senso di realismo, più della metà dei soggetti intervistati è convinta che entro il 2015 le loro aziende saranno vittime di un attacco informatico, con una crescita rispetto al 39% del 2013.
- Le applicazioni che girano sul Web sono oggi sotto attacco, tanto è vero che i responsabili informatici sono convinti che quest'area sia la più pericolosa e debba essere tenuta sotto più stretto controllo.
- Le preoccupazioni che riguardano gli strumenti informatici mobili sono in crescita esponenziale. Quando è stato chiesto ai responsabili informatici di valutare il livello di protezione delle proprie aziende contro attacchi diretti a smartphone, laptop e altri strumenti informatici in dotazione ai dipendenti, la risposta complessiva si è situata ad un livello assai basso.Gli strumenti di difesa situati sui terminali non sembrano così efficienti come si sperava; più dei due terzi dei soggetti intervistati stanno cercando di individuare e installare strumenti più efficienti e più efficaci.
- Soft ware-defined networking (SDN), vale a dire le reti protette, sembrano rappresentare un nuovo e più sicuro strumento di protezione da attacchi informatici

Come accennato in precedenza, i software che girano sul Web sono quelli che maggiormente preoccupano, anche perché oggi sono sempre più diffusi all'interno di qualsiasi organizzazione, che utilizzi un sistema informativo.

Il fatto che questi applicativi possano spesso portare ad un diretto contatto con dati sensibili aumenta la vulnerabilità dei dati stessi. Non sorprende pertanto il fatto che questi applicativi sono quelli che destano la maggiore preoccupazione.

Cosa ci riserva il futuro

Appare evidente che le squadre incaricate di proteggere i sistemi informativi devono vivacizzare il loro impegno, per mantenersi aggiornate e garantire protezione a un ambiente informatico in continua evoluzione, così come sono in evoluzione gli attacchi relativi.

Per fortuna, molti soggetti intervistati hanno confermato che il loro budget per la sicurezza informatica verrà aumentato nel 2015.

Gli investimenti si concentreranno soprattutto su:

- difese di nuova generazione, attive sia a livello di terminali sia a livello di dispositivi mobili;
- servizi di intelligence sulla evoluzione delle minacce informatiche;
- soluzioni di sicurezza incorporate nel software.

Per ottenere una copia di questo documento, i lettori possono collegarsi a www.bit.do/2015-cdr

Adalberto Biasiotti