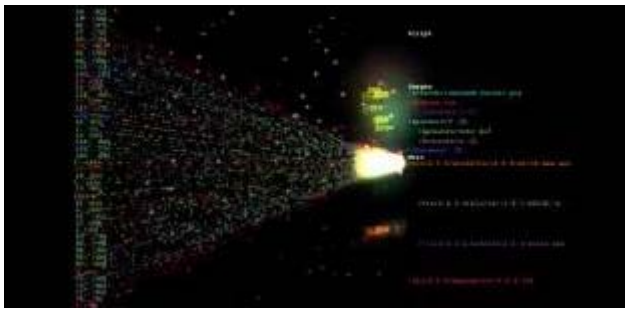
TECH

CLOUD E IOT NEL MIRINO DI HACKER, LE NUOVE TENDENZE DEL 2016

NON PER TERRORISMO MA PER SOLDI: ECCO DA DOVE VENGONO GLI ATTACCHI INFORMATICI

Cyber security e attacchi informatici: due recenti rapporti di società di sicurezza rivelano quali sono stati i principali bersagli del 2015 e le tendenze del 2016. Tra le motivazioni degli attacchi alle aziende più diffusi - i DDoS, che bloccano l'uso di internet - c'è la richiesta di un riscatto



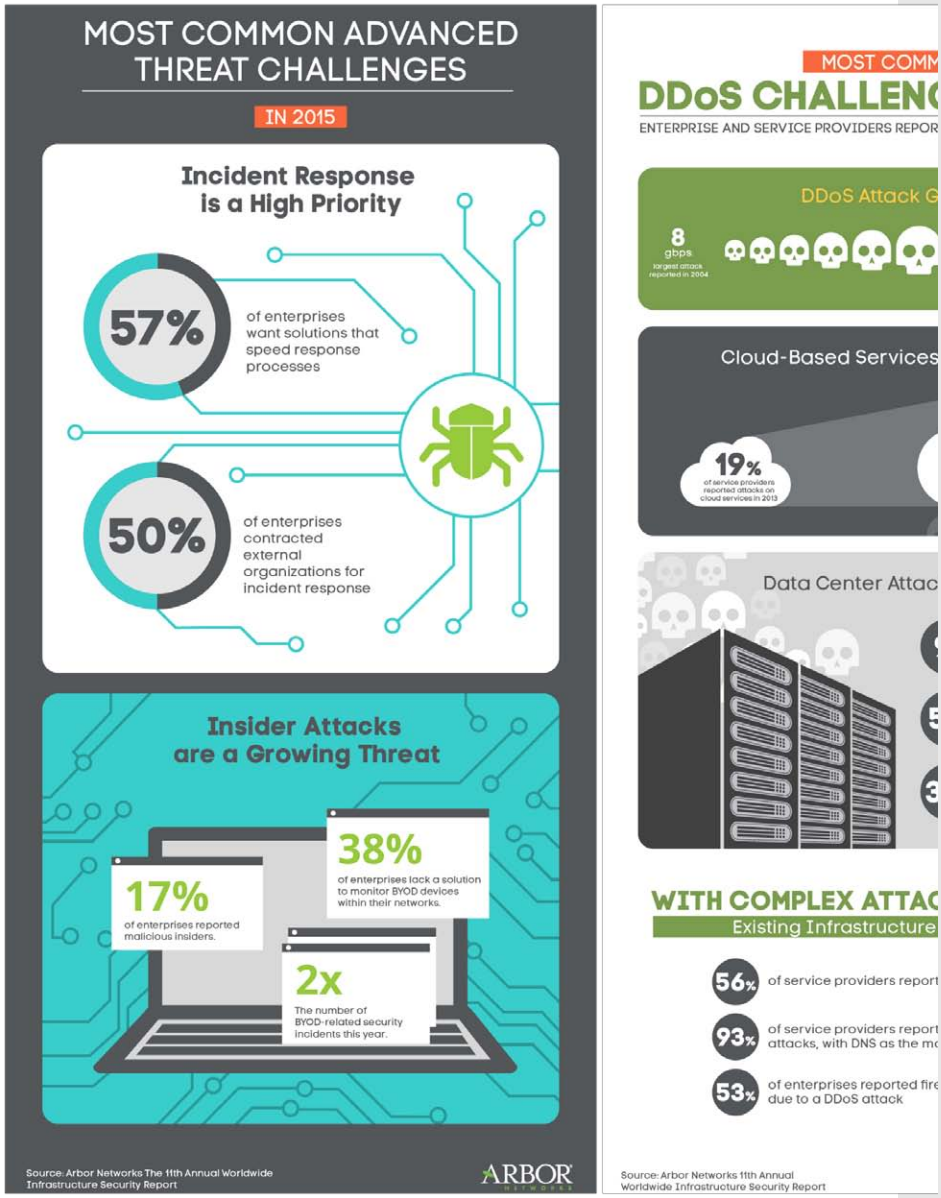
di Celia Guimaraes
Milano
È ormai chiaro che la sicurezza informatica, sempre più importante, lo diventerà ancora nei prossimi anni, grazie anche all'attenzione da parte del grande pubblico.

B Attacchi DDoS, la protesta virtuale
B Terrorismo, Anonymous minaccia l'Isis: "Sappiamo che ci temete, vicini ai vostri padroni"
B Gli alberghi Hilton: "Siamo stati attaccati dagli hacker, controllate i pagamenti"
B Far West 2.0. L'Fbi mette una taglia da 3 milioni di dollari su un hacker

26 gennaio 2016

Tra gli attacchi informatici sono sempre più conosciuti (e diffusi) ci sono i DoS (Denial of Service), azione che "si propone di impedire l'uso di una risorsa di rete, ad esempio un sito web. Quando all'attacco partecipano molti sistemi, spesso dell'ordine di decine di migliaia, si parla di DDoS (Distributed DoS): è facile capire perché sia molto più devastante e difficile da bloccare", recita la spiegazione di Garr News.
Da dove provengono gli attacchi, con quale intensità si verificano, verso quali bersagli sono l'oggetto di ricerche specifiche da parte di società specializzate.

Il recente report di Arbor Networks, ad esempio, identifica alcune tendenze, tra cui l'aumentata dimensione degli attacchi, le sue motivazioni, i servizi cloud presi di mira:



L'influenza dei mass media

E' interessante notare, tra le tendenze rilevate, l'aumento degli attacchi informatici 'a scopo di ricatto', anche se "l'attribuzione degli attacchi informatici a particolari sorgenti o motivazioni è un esercizio particolarmente difficile", sottolinea Marco Gioanola, Senior Consulting Engineer di Arbor Networks e le risposte potrebbero essere state parzialmente influenzate dal risalto dato dai mass media a temi specifici.

E' certo, comunque, che nell'ultimo anno l'hacker indotto da motivazioni politiche è stato un po' meno presente, spiega Gioanola: "Mentre negli anni scorsi i gruppi dei cosiddetti "hacktivisti" come Anonymous utilizzavano ampiamente gli attacchi DDoS come arma di protesta e pressione (e venivano di conseguenza indicati come colpevoli nella maggior parte dei casi), nel 2015 sono state le attività di estorsione di gruppi come DD4BC o Armada Collective a salire agli onori delle cronache, anche grazie all'interesse verso il campo delle cripto-valute come Bitcoin".

Non per terrorismo ma per soldi

"Tali gruppi hanno cercato di monetizzare l'estrema facilità con cui è possibile dotarsi di un'infrastruttura di attacco in grado di generare DDoS di grandi dimensioni, inviando mail ricattatorie a un'ampia base di vittime potenziali: banche, ISP, e-commerce, ecc. Il modus operandi si è ripetuto costantemente: un primo attacco 'dimostrativo' relativamente breve seguito dalla richiesta di soldi dietro minaccia di ulteriori DDoS. Nonostante in alcuni casi il 'pizzo' sia stato effettivamente pagato, va rilevato che gli attacchi, seppur potenti, si sono spesso rivelati relativamente facili da contrastare con l'aiuto degli ISP coinvolti, e recentemente l'Europol ha anche condotto arresti legati a tali attività", aggiunge l'esperto.

Quindi le motivazioni dietro agli attacchi DDoS sono molte e di varia natura, ma "è evidente che questi siano utilizzati sempre più a fini di guadagno illecito, direttamente (come nel caso delle campagne di estorsione) o indirettamente (come strumento di concorrenza sleale o componente accessoria in campagne di intrusione e furto di dati)", è la conclusione di Gioanola.

Il trend proseguirà

Anche per Martin McKeay, Senior Security Advocate di Akamai, crescerà la diffusione dei 'ricatti DDoS': "Nel 2014 abbiamo visto comparire una nuova minaccia, DD4BC. Scomparsa nel 2015, è stata sostituita da Armada Collective. Entrambi i gruppi erano dediti all'invio di email con la richiesta di un pagamento in bitcoin con la minaccia, in caso contrario, di mettere fuori servizio il sito dell'azienda. Il loro successo ha portato Armada Collective a comportamenti sempre più aggressivi e alla nascita di un discreto numero di imitatori. Non c'è dubbio che il trend proseguirà nel 2016 e diventerà sempre più pericoloso poiché sempre più malintenzionati vedranno un potenziale in questo genere di ricatti".

Attacco alle nuvole

Altra tendenza evidenziata dal report di Arbor Networks è la corsa all'attacco al cloud: nel 2013 erano stati osservati dal 19% degli utenti interpellati dalla società di sicurezza informatica. L'anno seguente la proporzione era salita al 29% e nel 2015 ha raggiunto il 33%, una netta indicazione di tendenza. Il 51% degli operatori di data center ha registrato attacchi DDoS che hanno provocato la saturazione della connettività internet disponibile e un deciso incremento (34% contro il 24% dell'anno precedente) nel numero di data center che hanno visto attacchi in uscita lanciati da server ospitati sulle proprie reti.

Gli esempi eclatanti

Il perché di questi attacchi ai servizi cloud-based è così spiegato dall'ingegner Gioanola: "Il termine 'cloud' 'è diventato ormai d'uso comune e ha finito per raccogliere sotto di sé una gamma eterogenea di servizi, dalle dimensioni e caratteristiche profondamente diverse. Il cloud, anche quando tale termine nasconde gli stessi identici servizi che, ad esempio, fino a ieri venivano semplicemente definiti di hosting, è stato adottato in massa dalle aziende e dai privati, convinti che questa fantastica 'nuvola' potesse assorbire qualunque attacco informatico, specialmente quelli legati alla disponibilità del servizio stesso. Svariati esempi ci hanno mostrato che così non è, persino in casi come gli attacchi alla rete delle Playstation del Natale 2014 e 2015. Senza scomodare eventi così eclatanti, più della metà degli operatori di data center che hanno risposto al nostro questionario ha riportato di aver subito attacchi in grado di bloccare l'accesso a tutti i servizi forniti: questo è un dato molto preoccupante, e dovrebbe essere preso attentamente in considerazione da tutte le aziende che intendono appoggiarsi ad architetture cloud per i propri servizi informatici. Basti pensare a quanto sia ormai critica la disponibilità dell'e-mail o dei file conservati in rete per l'operatività quotidiana".

"E' quindi necessario che le aziende indaghino con attenzione i livelli di servizio e di protezione forniti dai fornitori cloud e includano l'analisi degli attacchi informatici nei propri processi di valutazione del rischio. L'altra faccia della medaglia dell'adozione di massa dei servizi cloud-based è che l'accesso a internet rappresenta oggi la risorsa più critica per l'operatività delle aziende, che fanno affidamento sulla disponibilità della connessione in rete per dialogare coi servizi cloud e spesso con le altre aree aziendali. Non basta quindi affidarsi a un servizio cloud che offra garanzie di disponibilità, ma in primo luogo va protetto l'accesso a internet utilizzato per raggiungerlo: pensiamo ad esempio a un'azienda che non riesce a ricevere gli ordini inviati dai clienti sul portale cloud perché i suoi uffici sono isolati dal resto di internet a causa di un attacco DDoS", conclude Gioanola.

L'Internet delle Cose compromesso

L'IoT, Internet of Things o Internet delle Cose rappresenta una vasta classe di tecnologie e prodotti, ma la maggior parte "è stata progettata dedicando nulla più che un veloce pensiero alla sicurezza. Esempi recenti? 'Hello Barbie' e la compromissione del produttore di giochi Vtech", osserva Martin McKeay di Akamai , che sottolinea: "Dobbiamo essere consapevoli che i dispositivi IoT raccolgono più informazioni sui loro proprietari di quanto essi possano immaginare e si tratta di dati molto preziosi. E anche se il dispositivo è perfettamente sicuro, i servizi che stanno dietro a quel dispositivo spesso lasciano molto a desiderare in termini di sicurezza. Ecco perché penso che assisteremo a un crescente numero di attacchi sia ai tool e ai giochi IdC sia alle aziende che raccolgono i nostri dati personali".

Non si impara dagli errori

Nonostante l'aumento dei rischi, la sicurezza non aumenterà in modo significativo secondo Martin McKeay di Akamai: "Questo è un trend sul quale vorrei sbagliarmi ma quasi due decenni trascorsi ad occuparmi di sicurezza mi fanno pensare di aver ragione. Nonostante tutte le dichiarazioni dei fornitori di sicurezza che sostengono di disporre della soluzione a tutti i vostri problemi, un prodotto del genere non esiste. Dobbiamo invece convincerci che assisteremo a una lunga serie di piccoli miglioramenti alla sicurezza e che i progressi si misurano in decenni, non in anni. Le aziende troveranno metodi nuovi e più efficaci per proteggere i loro sistemi e a loro volta i criminali troveranno nuovi e più efficaci metodi

per attaccare gli stessi sistemi. Col tempo e un po' alla volta, capiremo come costruire software e sistemi che siano intrinsecamente sicuri fin dalla nascita. Probabilmente nel 2016 ci sembrerà che la sicurezza peggiori, ma questo sarà un segnale del fatto che le organizzazioni iniziano a riconoscere gli indicatori di una compromissione, più che di un reale peggioramento della sicurezza".

TECH

SAFER INTERNET DAY: FAI LA TUA PARTE, CONVIENE A TUTTI

ANCHE I 'LIKE' SU YOUTUBE VALGONO UN DISCO D'ORO

SAFER INTERNET DAY, RIFLETTORI SUI PERICOLI DELLA RETE

STRAGI DI MAFIA A PALERMO, REATI AMBIENTALI NELLA TERRA DEI FUOCHI: DUE APP PER L'IMPEGNO CIVILE

NOMA, L'APP PER NON DIMENTICARE LE STRAGI DI MAFIA A PALERMO

TAG

DDOS | ATTACCHI INFORMATICI | CLOUD | IOT | HACKER | ANONYMOUS