CYBER SECURITY: TRA ERRORE UMANO E SOCIAL ENGINEERING

A CURA DELLA REDAZIONE

FURTI, FRODI E ATTACCHI: LA CYBER SECURITY STA DIVENTANDO UN ELEMENTO IMPRESCINDIBILE DEL BUSINESS. ECCO QUALI SONO I RISCHI MAGGIORI E COME CI SI PROTEGGE

L'investimento delle aziende italiane in cyber security è in crescita (+6,1% nel 2016 rispetto al 2015 secondo i dati Assinform). Nonostante siano stati fatti passi avanti, la maggior parte delle organizzazioni dimostra ancora un approccio inefficace. Perché? Bruce Schneier ha detto "Le persone spesso rappresentano l'anello più debole della catena della sicurezza e sono cronicamente responsabili per il fallimento dei sistemi di security". In cosa sbagliano? Lo abbiamo chiesto ai principali player di mercato.

Quali sono gli errori più gravi che mettono a repentaglio la sicurezza delle aziende?

Sono in molti a concordare con le parole di Bruce Schneier, a cominciare da Vittorio Bitteleri, Head of Sales Enterprise Security Italia di Symantec. "La sicurezza dipende da persone, processi e tecnologie. Gli errori più comuni sono collegati alle password: se ne utilizzano di troppo semplici, oppure se ne sceglie una sola per diversi servizi, in alcuni casi condividendola con altri, questi sono tutti comportamenti a rischio. Un'altra problematica è legata alla mancanza di attenzione: quando si ricevono email da un mittente sconosciuto o se il messaggio sembra fuori contesto, è importante evitare di aprirlo. Infine, durante le nostre attività di formazione dei clienti, abbiamo rilevato una generale mancanza di formazione specifica: ricordiamo sempre che quando un software richiede un aggiornamento ci sono motivi più che validi per accettarlo. In tutti questi casi, training per i dipendenti possono essere di grande aiuto per le aziende".
Gli investimenti in tecnologie di sicurezza spesso vengono vanificati dal comportamento di un singolo utente, come sottolinea Mirko Gatto, Direttore Divisione Cyber Var Group. "Gran parte degli attacchi vengono compiuti utilizzando tecniche di ingegneria sociale, volte a sfruttare la mancanza di formazione e di consapevolezza dell'utente, unite molto spesso a distrazione. Errori ricorrenti come il mancato riconoscimento di un allegato malevolo a una email o il click su un link ingannevole sono in grado di mettere a rischio la struttura di sicurezza progettata dall'azienda. Non bisogna inoltre sottovalutare il valore delle informazioni che riveliamo all'esterno. Quella che sembra una cosa di poco conto, può invece essere un'informazione preziosa per un malintenzionato che vuole condurre un attacco verso l'azienda stessa".
"Lo diciamo da anni, è proprio l'essere umano che, oltre a rappresentare il bersaglio, è anche il vettore inconsapevole degli attacchi informatici" conferma Ferdinando Torazzi, regional director Italy & Greece, Intel Security. "I cyber criminali adottano metodi sempre più complessi per bypassare il firewall umano con l'obiettivo di convincere un individuo a eseguire un'azione che provoca un'infezione o la divulgazione di informazioni preziose. Il tema più ricorrente che vediamo quando si studiano le violazioni dei dati di oggi è l'uso dell'ingegneria sociale per costringere l'utente a un'azione che faciliti e favorisca le infezioni di malware".
Fabrizio Croce, Area Director South Europe, WatchGuard Technologies, individua due tipologie di errori, quelli involontari dovuti dall'imperizia, imprudenza o negligenza e quelli indotti dall'esterno con l'inganno. "Nella prima tipologia possiamo includere la scelta di password, facilmente identificabili, usate per più scopi anche esterni all'azienda; condivisioni di rete lasciate aperte, Wi-Fi non protette o con chiavi deboli; mancanza d'uso di salvaschermi con password. Nella seconda invece rientrano i casi nei quali l'utente viene portato a compiere una particolare azione, che erroneamente ritiene non pericolosa, utile o addirittura obbligatoria. In questa categoria ricadono tutti gli attacchi basati sul social engineering, il phising, che consentono ad esempio di carpire le credenziali dell'utente o dell'amministratore IT".
Secondo Fabrizio Cassoni, Sales Engineer, F-Secure Corporation, "gli attacchi basati sul social engineering esisteranno sempre, perché sfruttano le nostre debolezze e possono essere mitigati solo in parte dalle soluzioni tecnologiche. L'esperienza e l'informazione aiutano a contenere questi rischi: sarebbe importante insegnare la cultura della sicurezza informatica, dovrebbe fare parte del curriculum di studi. Sul fronte aziendale, uno dei grandi problemi irrisolti è tuttora quello dell'aggiornamento dei propri asset. Sono molto frequenti gli attacchi basati su exploit di falle note e risolte da tempo, ma che hanno successo perché l'amministratore non ha tempo o risorse per gestire le patch".
Loris Angeloni, Sales Manager Italy di SolarWinds, conclude: "Il problema principale è la non consapevolezza dei rischi che si corrono utilizzando un dispositivo collegato alla rete. Manca la percezione dell'importanza dei dati, considerati un'entità astratta e non tangibile. Le policies aziendali in materia di sicurezza IT vengono spesso percepite come restrizioni e questo sfortunatamente si traduce in continui tentativi di aggirare le barriere messe in atto dai responsabili IT per poter essere autonomi e più flessibili. O almeno, questo è quello che crede l'utente".

Quali sono i pericoli maggiori? Quali le tipologie di attacco più diffuse?

Il 2016 è stato l'anno delle estorsioni online. "Il nuovo demone della rete è senza ombra di dubbio il ransomware, un malware i cui effetti sono devastanti, perché prende in ostaggio, cifrandoli, i file dell'utente con la promessa della loro restituzione a seguito del pagamento di un riscatto. Proprio gli attacchi che sfruttano vulnerabilità legate al fattore umano, come

il phishing e i trojan, sono attualmente i più diffusi ed efficaci e possono provocare danni ingenti ai sistemi di sicurezza aziendali, perdita di dati sensibili e informazioni strategiche, danno alla reputazione. Per andare a buon fine hanno bisogno dell'intervento, il più delle volte inconsapevole, di una persona interna all'azienda. Un'altra tipologia molto frequente è il cosiddetto attacco man-in-the-mail, che si verifica a seguito di violazione della casella di posta elettronica di un utente e intercettazione delle comunicazioni che hanno come oggetto trattative e pagamenti" ha detto Mirko Gatto di Var Group.
Carla Targa, Marketing and Communication Manager Trend Micro, fornisce i numeri relativi al Q3 2016, che confermano come l'Italia sia stata colpita soprattutto da ransomware e app maligne. "Il trend di queste ultime si è dimostrato in continua crescita per tutto il 2016, erano 392.715 nel Q1, 655.553 nel Q2, nel terzo trimestre sono salite ancora a 805.490. I malware bloccati in Italia nel Q3 sono stati 5.527.089. Mezzo milione in più rispetto al Q2, quando ne erano stati rilevati 4.936.148. I ransomware sono invece 1.793.055. Il nostro Paese ha raggiunto così il totale di 5.460.439 ransomware solo nei primi nove mesi dell'anno, che rappresenta il 3% di quelli rilevati in tutto il mondo. Con questi numeri l'Italia è stato il Paese europeo più colpito da questo fenomeno nel periodo Q1-Q3".
Anche Fabrizio Cassoni di F-Secure individua il ransomware tra i pericoli più diffusi, ma cita anche casi di cyber-spionaggio su obiettivi di alto profilo condotti mediante malware: "Di certo esiste una casistica di cui non siamo a conoscenza, dato che non esiste obbligo di denunciare alle autorità gli attacchi subiti e le vittime non sono portate a rendere pubblica la cosa. Gli attacchi DDoS sono già in forte aumento rispetto agli anni passati e le Botnet legate all'IoT stanno facendo sentire la propria influenza, anche con assalti multi-vettore che rendono la difesa ancora più difficile". Morten Lehn, General Manager Italy di Kaspersky Lab, conferma: "Il panorama delle cyber minacce è soggetto a rapide e profonde evoluzioni. Sono diventati ormai all'ordine del giorno gli attacchi mirati di alto profilo e quelli dell'Internet of Things, così come i ransomware. Secondo un'indagine di Kaspersky Lab, un solo incidente di cyber-security costa 861.000 dollari alle grandi aziende e 86.500 dollari alle piccole e medie imprese, questo dimostra come la sicurezza IT debba essere uno degli argomenti al tavolo di discussione del top management".
Secondo PierPaolo Alì, Director South Europe HPE Security, "il panorama è così complesso che l'unicità di un pericolo o di una tipologia di vulnerabilità non esiste più, ogni azienda ha il proprio spettro in base alla categoria di informazioni che tratta, al modello di business, alla reputazione e alle norme a cui deve sottostare. L'imminente applicazione del nuovo regolamento europeo porterà una nuova categoria di criticità e aggiungerà una riga alla lista delle cose da fare nell'agenda di ogni security manager. L'attacco più pericoloso è sempre quello ancora sconosciuto. In questo campo, diventa difficile spesso anche realizzare con certezza di aver subito un attacco. Le tecnologie che possono aiutare sono quelle di analytics, che devono essere in grado di evidenziare comportamenti, pattern, anomalie che non sono conformi alla normale attività aziendale".
Stefano Volpi, Cisco Security Practice Leader per l'Italia, sottolinea come attualmente gli hacker possano agire quasi senza limiti temporali. "Spesso agiscono senza essere rilevati per giorni, mesi o anche più a lungo. D'altro canto, i responsabili della sicurezza spesso non hanno la visibilità necessaria sulle minacce note ed emergenti e non riescono a ridurre i tempi di rilevamento (Ttd). Sebbene stiano facendo grandi progressi, è ancora tanta la strada da fare per riuscire effettivamente a sventare le azioni degli hacker mirate a preparare il terreno per gli attacchi di grande portata".

La sicurezza è diventata parte integrante delle strategie delle aziende italiane?

In realtà, dipende dalle diverse realtà e il panorama in Italia sembra essere variegato. "Dipende. La maggioranza delle aziende italiane ha adottato dei sistemi di protezione ma la loro qualità è molto diversa. Le Pmi con poca propensione alla spesa spesso sono malamente protette con tecnologie e prodotti di basso costo, talvolta open source" commenta Fabrizio Croce di WatchGuard Technologies.
Anche per Morten Lehn di Kaspersky Lab le grandi aziende sono le più protette, per una maggiore disponibilità sia di budget sia di competenze tecniche interne. Le piccole e medie imprese sono consapevoli dei rischi, ma spesso non hanno messo in atto una strategia di sicurezza che permette di prevenire eventuali attacchi proprio per la ridotta disponibilità di budget e la mancanza di professionisti all'interno dell'azienda.
Paolo Ciotti, Marketing Manager di HP Italy, fornisce alcuni dati: "Secondo i risultati di una recente ricerca realizzata per noi da Redshift Research sulla sicurezza dell'utilizzo di dispositivi aziendali in mobilità, che ha coinvolto più di mille IT decision maker in sette paesi europei tra cui l'Italia, il 20% delle aziende che ha implementato un'iniziativa basata sul Byod ha subito almeno una violazione della sicurezza nell'anno in esame (2015). Un dato rimarcato anche dalla preoccupazione espressa dal 36% degli intervistati

Carla Targa
TREND MICRO

Fabrizio Cassoni
F-SECURE

Francesco Teodonno
IBM

Fabrizio Croce
WATCHGUARD TECHNOLOGIES

Loris Angeloni
SOLARWINDS

Morten Lehn
KASPERSKY LAB

su possibili virus. Le aziende del nostro Paese stanno iniziando a comprendere sempre di più l'importanza di proteggere le proprie reti, a partire dai dispositivi mobili ad esse connessi, per soddisfare le esigenze di mobilità dei dipendenti. Sembra che avere device e stampanti sicure rimanga una delle principali preoccupazioni per oltre il 90% degli IT decision maker europei e italiani".
Ferdinando Torazzi di Intel Security racconta come una loro ricerca mostri che, in media, le aziende non sono in grado di analizzare sufficientemente il 25% degli avvisi di sicurezza il 93% non sa reagire prontamente a tutte le potenziali minacce.
Insomma, abbiamo visto alcuni miglioramenti, ma c'è ancora molto da fare, specialmente in vista dell'attuazione della General Data Privacy Regulation europea, come sottolinea Vittorio Bitteleri di Symantec. "Le aziende italiane dovranno muoversi a tutta velocità per rispettarne i parametri, dal momento che una mancanza provata nella protezione dei dati potrà portare a multe che corrisponderanno anche al 4% del loro giro d'affari oppure a 20 milioni di euro, a seconda di quale sia il valore maggiore. Come Symantec, purtroppo non vediamo ancora nelle aziende una piena consapevolezza di cosa questo significhi nell'ambito degli investimenti in tecnologia, personale specializzato nell'IT e processi, ma siamo qui per accompagnarle nel loro cammino".

Come ci si protegge?

Per prima cosa, come dice Loris Angeloni di SolarWinds, "è fondamentale sfatare il mito della soluzione singola da adottare: la sicurezza informatica è un processo, non un prodotto. Il concetto di multilayered security è la chiave per avvicinare il proprio rischio di data breach allo zero. Molteplici tecnologie, ognuna per aspetti e criticità diverse, orchestrate da policies che rendano la gestione lineare e scalabile. Quindi non solo un antivirus, ma protezione della posta elettronica, gestione dell'asse, monitoring della rete, protezione dell'endpoint, sicurezza perimetrale e della navigazione e un solido sistema di disaster recovery".
Secondo Francesco Teodonno, IBM Security Leader di IBM Italia, è necessario identificare i rischi e inserire i controlli di sicurezza opportuni all'interno del servizio in fase di disegno della soluzione, non dopo che si è ricevuto un attacco. Una sicurezza che sia dunque preventiva e concepita by design. Inoltre, con l'abbattimento delle barriere geografiche e dei confini tra ciò che è digitale e ciò che è fisico, la security non può prescindere da nuovi modelli di protezione integrati ed evoluti. "La sicurezza

Pierpaolo Alì
HPE

Stefano Volpi
CISCO

Vittorio Bitteleri
SYMANTEC

Ferdinando Torazzi
INTEL SECURITY (MCAFEE)

Paolo Ciotti
HP

Mirko Gatto
VAR GROUP

intesa come difesa perimetrale è ormai un concetto obsoleto. Occorre mettere in campo una strategia con la security intelligence al centro, che permetta di acquisire, normalizzare e analizzare, in tempo reale, i dati strutturati generati da utenti, applicazioni e infrastrutture. Fondamentali sono i sistemi avanzati di analytics che, grazie alla capacità di analizzare enormi volumi di informazioni, sono in grado di rilevare eventuali compromissioni in tempi rapidi, ma anche di ridurre i falsi positivi, risparmiando così tempo e risorse" dice Teodonno.

La strategia è importante anche per Paolo Ciotti di HP Italy: "I Cio devono implementare politiche IT ottimali per la propria organizzazione e preservare le identità, i dispositivi e i dati, con prodotti che rispondano alle esigenze degli utenti per invogliarli ad attuare quelle best practice che garantiscano la massima protezione. A mio avviso le aziende oggi devono pensare a strategie di sicurezza che consentano di salvaguardare i dati sensibili per il business senza gravare eccessivamente sulle risorse IT, proprio per questo abbiamo recentemente sviluppato servizi pensati per semplificare processi critici per il business, portando a una riduzione di costi e carichi di lavoro IT e aumentando la produttività dei dipendenti. Abbiamo inoltre tecnologie e soluzioni nell'ambito della protezione degli end-point, come ad esempio HP Sure View, che protegge la privacy rendendo le informazioni visibili unicamente a chi utilizza un laptop e non a chi gli è vicino, oppure HP SureStart, che consente di ripristinare il bios di un computer infetto già entro 30 secondi da un attacco o dalla sua compromissione".

Ferdinando Torazzi di Intel Security suggerisce, tra le contromisure, la condivisione dell'intelligence delle minacce tra imprese e fornitori di sicurezza. "Per stare al passo con gli avversari, anticiparli e bloccarli, dobbiamo unire lo scambio di informazioni di intelligence, la potenza del cloud computing, l'agilità delle piattaforme e le risorse umane che i criminali informatici sfruttano regolarmente. Per vincere le battaglie contro le minacce future, le aziende devono avere una visione più approfondita e dettagliata e di più lungo periodo. Non è più possibile affidarsi a soluzioni di sicurezza isolate e non integrate. I sistemi devono comunicare per affrontare in modo efficace il ciclo della protezione dalle minacce, che Intel Security identifica nel framework Protect, Detect, Correct e che indirizza con un portafoglio ampliato di prodotti strettamente integrati e soluzioni specializzate che aiutano i clienti a porre rimedio a un numero maggiore di minacce, più velocemente e con meno risorse".

Stefano Volpi di Cisco continua: "Oggi le tecnologie focalizzate sulla sola prevenzione rimangono un pilastro della sicurezza degli endpoint ma queste sono insufficienti a difendersi contro gli attacchi più sofisticati che sono perfettamente in grado di eluderli. Occorre lavorare insieme e condividere le informazioni attraverso un'architettura di sicurezza

più estesa, che consenta di ridurre il tempo necessario per il rilevamento delle minacce. Gli attacchi sono sempre più efficaci e almeno nel 25% dei casi questi avvengono indipendentemente dal numero di tecnologie che si hanno a disposizione. Ci sono imprese che hanno fino a 70-80 prodotti diversi di sicurezza che spesso non dialogano neppure tra loro".
Insomma, bisogna adottare una strategia che abbia un approccio totale e che non punti solo a risolvere una criticità contingente. Per questo Trend Micro costruisce soluzioni su misura per ogni tipo di azienda e organizzazione, fornendo strumenti che tengano conto della tipologia dell'infrastruttura, del settore e di tutti i parametri necessari. "Ultimamente abbiamo presentato, XGen Security, che fa compiere un ulteriore passo avanti alla protezione endpoint, integrandola con il machine learning" spiega Carla Targa. "È un insieme intergenerazionale di tecniche di difesa dalle minacce che applicano in maniera intelligente la giusta tecnologia nel momento corretto. Il risultato è una protezione più efficace ed efficiente contro le minacce. L'approccio unico di Trend Micro utilizza metodi comprovati per identificare velocemente i dati benigni e le minacce conosciute, mentre attiva le sue tecniche avanzate come il controllo delle applicazioni, la prevenzione degli exploit, le analisi comportamentali e il machine learning, per identificare più velocemente e in maniera accurata le minacce sconosciute. Trend Micro è la prima a includere il machine learning ad alta fedeltà nel suo approccio, analizzando i file sia prima della loro esecuzione che durante e utilizzando funzioni di controllo e whitelisting per ridurre i falsi positivi".

Lo spostamento delle infrastrutture aziendali verso il cloud aumenta o diminuisce i rischi?

Come spiega PierPaolo Allì di HPE Security, "lo spostamento delle infrastrutture non diminuisce né aumentai rischi, li sposta sul provider del servizio verso il quale le aziende potranno poi rivalersi. Il problema non è quindi risolto, anche se apparentemente la responsabilità sembra ridotta, ma attenzione: da un punto di vista di visibilità o di aderenza alle normative, i responsabili dei dati nel cloud continuano a essere le aziende che originariamente li trattavano. Siamo quindi in un ambito dove forse è meglio fornire i dati con una sicurezza intrinseca ancor prima che essi vengano trasferiti esternamente nel cloud, in modo che ovunque essi siano, l'azienda detentrice avrà la garanzia che non possano essere utilizzati da terze parti in modo fraudolento. HPE Security, con la suite Voltage, presenta delle soluzioni in grado di proteggere il dato ovunque esso sia, spostando la sicurezza dal luogo al dato stesso. Per realizzare un compito così innovativo efficacemente è stata resa necessaria la creazione di alcune tecnologie che sono state poi brevettate, come la Format Preserving Encryption, la Secure Stateless Tokenization e l'Identity Based Encryption. Queste rendono possibile svincolare la sicurezza del dato dalla fisicità del luogo dove si trova e concorrono a realizzare un'infrastruttura di dialogo tra il "dato sicuro" e le applicazioni snella e flessibile in modo da poter essere sempre conforme anche alle normative più strette e contemporaneamente pronta all'abilitazione di nuovi servizi di business senza la preoccupazione ed il rischio di aperture di nuove falle nel sistema informativo".
Anche Francesco Teodonno di IBM Italia sottolinea come il cloud sia un modello di erogazione e di consumo dei servizi IT, con aspetti intrinseci che vanno presi in considerazione. "L'approccio da avere è quello di identificare i controlli di sicurezza e assicurarsi che siano validi sia sul cloud che on premise. Discorso a parte è la sicurezza relativa all'Internet of Things. Negli ultimi mesi del 2016 si sono registrati attacchi a dispositivi intelligenti che a loro volta sono stati usati per attaccare istituzione importanti e server funzionali alla stessa Internet. Nel portafoglio di offerta di IBM Security vi sono soluzioni che permettono la implementazione di tutti i controlli di sicurezza a prescindere dal modello di delivery utilizzato".
Fabrizio Cassoni di F-Secure conclude: "Il Cloud comporta dei rischi differenti, che vanno governati. I provider per primi devono necessariamente assicurarsi della correttezza delle loro implementazioni e analizzare continuamente il proprio modello di sicurezza, senza tralasciare il fattore umano. Al momento, sembra che il tradeoff sia positivo: le aziende hanno individuato una convenienza economica in questo modello e gli stessi operatori della security utilizzano pesantemente il Cloud per rendere più efficienti i propri prodotti. I bad boys fanno lo stesso, però, quindi non bisogna mai abbassare la guardia". ■