

SPECIALE

LA SICUREZZA DELLA POSTA ELETTRONICA

Attacchi mirati con tecniche di spear phishing dimostrano le vulnerabilità rappresentate dalla posta elettronica e generate spesso da comportamenti erronei o avventati

pag.6-15



CYBER ATTACK

FORCEPOINT

La febbre di Star Wars ha colpito anche gli esperti informatici di Forcepoint, che hanno battezzato una nuova botnet "Jaku" (o Jakku), come il desolato pianeta di frontiera della famosa saga fantascientifica, centro di traffici illeciti.

pag.5

PROTAGONISTI

GASTONE NENCINI, TREND MICRO: LA MINACCIA RANSOMWARE

È una tipologia di malware in rapida diffusione, soprattutto per l'elevato ritorno economico che offre al cyber crimine. La prevenzione resta la prima linea di difesa da affiancare a soluzioni di sicurezza specifiche come quelle proposte da Trend Micro.



pag. 18-19

IN QUESTO NUMERO:

CYBER ATTACK

pag.3

- Che la forza sia con noi contro gli attacchi informatici

pag.4

- La protezione tradizionale non basta più

SPECIALE

pag.6

- La sicurezza della posta elettronica

pag.9

- HPE Secure Mail: protezione end-to-end per posta e allegati

pag.12

- Check Point: protezione Zero-Day per le e-mail cloud-based

pag.14

- Barracuda, maggiore protezione contro gli attacchi e-mail mirati

SOLUZIONI

pag.16

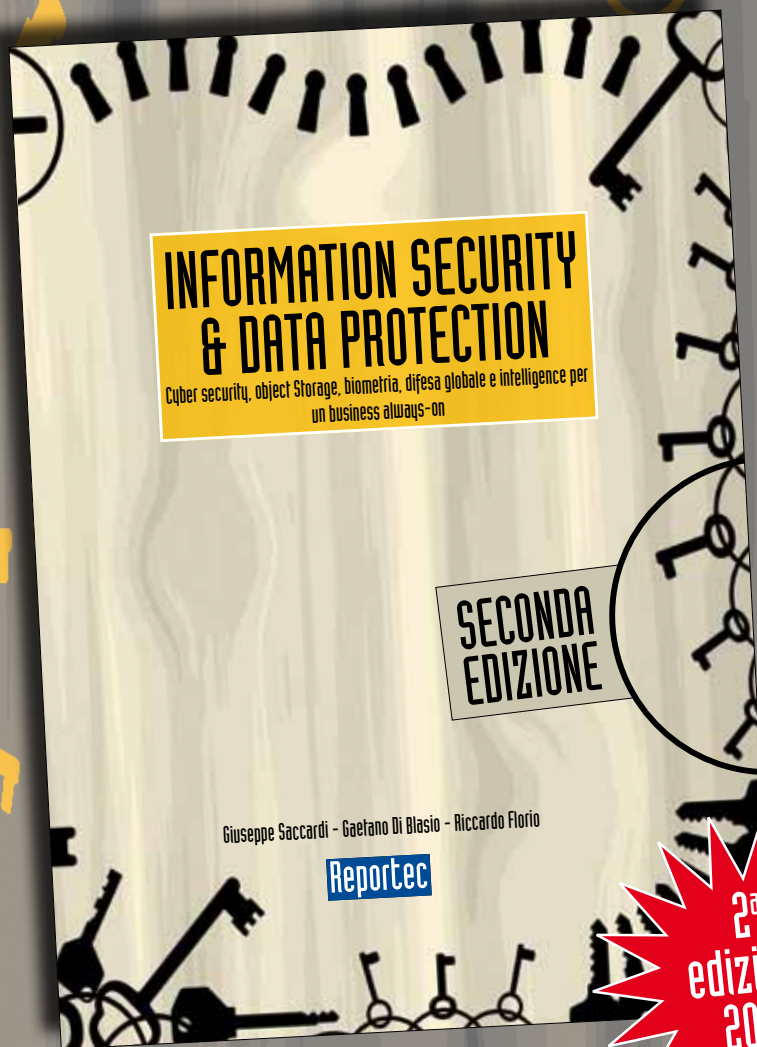
- Servizio F-Secure: rileva gli attacchi entro 30 minuti

PROTAGONISTI

pag.18

- Gastone Nencini, Trend Micro: la minaccia ransomware

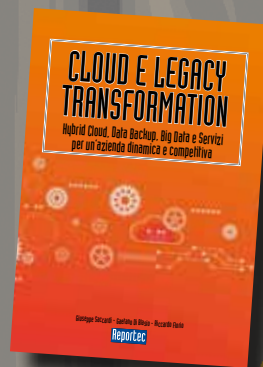
È disponibile il nuovo libro **SICUREZZA E PROTEZIONE DEI DATI**



In oltre 200 pagine il punto sulla situazione della cybersecurity e sulle dinamiche aziendali nella protezione del dato e della continuità del business. Una tematica sempre più vitale per le imprese, le quali devono mettere in conto che saranno attaccate. Ormai esistono sistemi automatici e pressioni da parte dei cybercriminali, tali per cui nessuno può sentirsi al sicuro: chi non è ancora stato attaccato lo sarà e, se non subirà danni gravi, sarà solo perché chi l'ha assalito cercava qualcos'altro.



È disponibili anche
CLOUD E LEGACY TRANSFORMATION



Il libro è acquistabile al prezzo di 48 euro (più IVA 22%) richiedendolo a
info@reportec.it - tel 02 36580441 - fax 02 36580444

CHE LA FORZA SIA CON NOI CONTRO GLI ATTACCHI INFORMATICI

Dalla botnet Jaku assalto all'Asia. Minacce interne e nuovi ransomware nel Threat Report di Forcepoint

di Gaetano Di Blasio



La "febbre di Star Wars ha colpito anche gli esperti informatici di Forcepoint, che hanno battezzato una nuova botnet "Jaku" (o Jakku), come il desolato pianeta di frontiera della famosa saga fantascientifica, centro di traffici illeciti. È una delle rivelazioni del Forcepoint Global Threat Report 2016.

Jaku è stata scoperta a seguito di un'indagine durata 6 mesi dalla squadra Forcepoint Special Investigations, che ha identificato l'Asia come bersaglio della rete.

Il report mette in evidenza alcune delle più recenti minacce in evoluzione, con dati raccolti da oltre tre miliardi di data point al giorno in 155 paesi in tutto il mondo. Oltre a Jaku, tra i principali risultati si trova:

- il rilevamento di una nuova ondata di ransomware opportunistici;
- l'incremento delle violazioni ai causate da insider sia malevoli sia "accidentali";
- il gap tra i controlli per la sicurezza dei cloud provider e quelli delle aziende loro clienti;
- la convergenza continua di vettori di attacco via e-mail e via Web in pratica il 90% dei messaggi indesiderati contengono una o più URL malevole e inoltre milioni di macro dannose sono inviate.

Secondo il rapporto, nel 2015, le campagne di contenuti dannosi via email sono aumentate del 250% rispetto al 2014, guidate in gran parte da malware e ransomware. Gli obiettivi di questi ultimi, in particolare, si stanno affinando e vengono identificati come target paesi, economie e settori in cui c'è maggiore probabilità che possa essere pagato un alto riscatto. Sono, peraltro, gli Stati Uniti a ospitare il maggior numero di siti Web di phishing rispetto a tutti gli altri paesi messi insieme.

Eppure, spiega Luca Livrieri, responsabile prevenzione per Italia e Spagna di Forcepoint, la minaccia maggiore continua a essere rappresentata dagli insider. I dipendenti stessi delle aziende che, spesso commettono stupidi errori di comportamento cliccando su link pericolosi senza criterio. Preoccupano, anche, tecniche di evasione avanzate, che stanno guadagnando popolarità e sono la combinazione di più metodi di evasione, come per esempio la frammentazione IP e la segmentazione TCP, per creare nuovi modi che consentono di aggirare i controlli di accesso mediante mascheramento del traffico e strategie di watering holes. (infezione di server affidabili comunemente utilizzati dalla vittima).

LA PROTEZIONE TRADIZIONALE NON BASTA PIÙ

FireEye propone una piattaforma per la protezione, in tempo reale, dalle minacce avanzate. L'intervista a Marco Riboli, senior vice president Southern Europe.

di Riccardo Florio



I cambiamenti finanziari, geopolitici ed economici hanno fatto del 2015 un anno molto impegnativo per l'Europa, il Medio Oriente e l'Africa (EMEA), che si riflette anche nelle minacce e negli attacchi informatici. Dal report M-Trends 2016, realizzato da Mandiant, azienda posseduta da FireEye, emerge uno scenario sempre più complesso fatto di attacchi altamente specializzati in grado spesso di aggirare le difese tradizionali basate sulle firme digitali (come firewall, IPS, antivirus, gateway), in cui cresce il numero di breccie nella sicurezza che diventano di dominio pubblico mentre diventano sempre più diversificate le origini e le motivazioni degli attacchi, a livello globale.

FireEye è approdata in Italia da qualche anno forte di oltre 4700 clienti in 67 Paesi, tra cui oltre 730 delle aziende Forbes Global 2000 e per fronteggiare le nuove generazioni di cyber attacchi ha progettato e realizzato una piattaforma di sicurezza basata su una macchina virtuale che fornisce protezione in tempo reale dalle minacce per aziende e pubbliche amministrazioni di tutto il mondo.

Marco Riboli, senior vice president Southern Europe

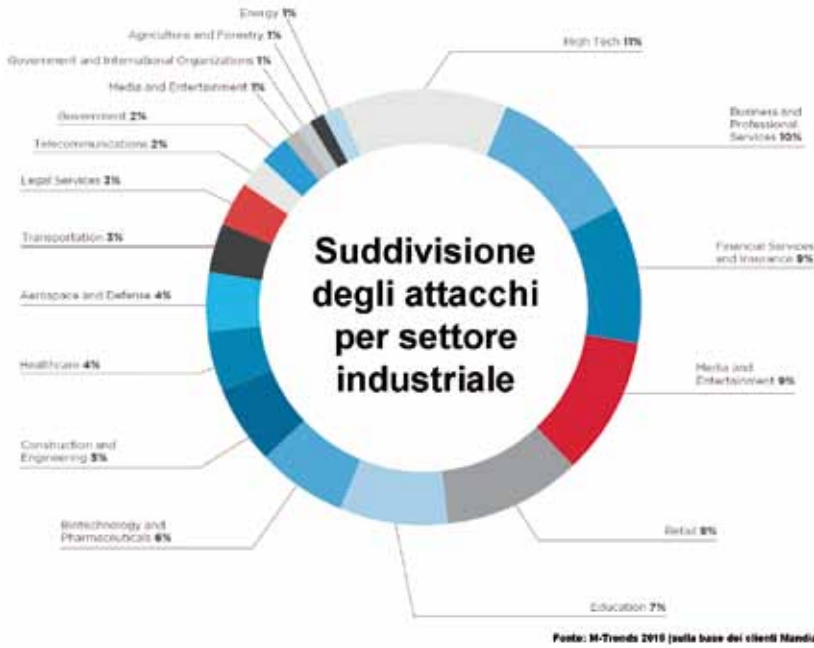
di FireEye delinea il quadro delle nuove minacce e i punti di forza di FireEye.

Direction: FireEye ha realizzato il report M-Trends 2016 che analizza lo scenario dei cyber attacchi. In base alle vostre ricerche quali sono i principali elementi di cambiamento in atto nello scenario della sicurezza aziendale?

Marco Riboli: Nei cyber attacchi analizzati abbiamo registrato un'impennata di casi dove l'attaccante è riuscito a compromettere sistemi critici per il business, bloccando o mettendo in seria difficoltà le operazioni aziendali. Infatti, sono diversi i casi nei quali l'attaccante è riuscito a colpire nel cuore l'azienda, riuscendo ad esempio a mettere offline i sistemi di broadcasting o a cifrare tutti i dati delle cartelle cliniche dei pazienti.

D: Quali sono le principali minacce, da dove arrivano, quali metodi utilizzano?

MR: Le minacce sono sempre più legate alla motivazione degli attaccanti: Il cyber-crime continua a creare nuove strategie per massimizzare i ritorni



finanziari delle loro campagne e il ransomware è diventato il loro principale strumento. Il cyber-espionage continua a puntare a vantaggi competitivi a discapito delle aziende o delle nazioni colpite, mentre gli hacktivist o i cyber-terroristi sono spinti da motivazioni politiche. Anche le App infette stanno diventando un veicolo di attacco sempre più frequente. Dato che ogni gruppo ha obiettivi e motivazioni diverse, è sempre più importante riuscire subito a dare un'attribuzione chiara all'attacco in corso per permettere la corretta gestione dell'incidente ed evitare conseguenze più gravi.

D: Cosa serve alle aziende per difendersi in modo efficace ed eventualmente come deve essere ripensata l'infrastruttura di sicurezza?

MR: Oggi, più che mai, le compromissioni informatiche sono inevitabili e richiedono di ripensare alla sicurezza aziendale in termini totalmente diversi rispetto al passato, spostando l'attenzione sulla mitigazione o eliminazione delle conseguenze per il business di un incidente informatico. La domanda da porsi è: sono preparato a rispondere a un attacco?

D: L'Italia rispetto ad altri Paesi ha delle specificità che richiedono un approccio particolare ?

MR: Una volta connessi a Internet non esiste più un reale limite geografico o regionale in quanto si diventa parte di una rete globale dove gli attaccanti sono sempre in agguato. Un sistema debole connesso a Internet diventa subito terreno fertile per un attaccante. Pertanto, se si è sottovalutato per molto tempo il reale rischio informatico, oggi la sfida per l'Italia potrebbe proprio essere il rimettersi in pari velocemente con una protezione adeguata.

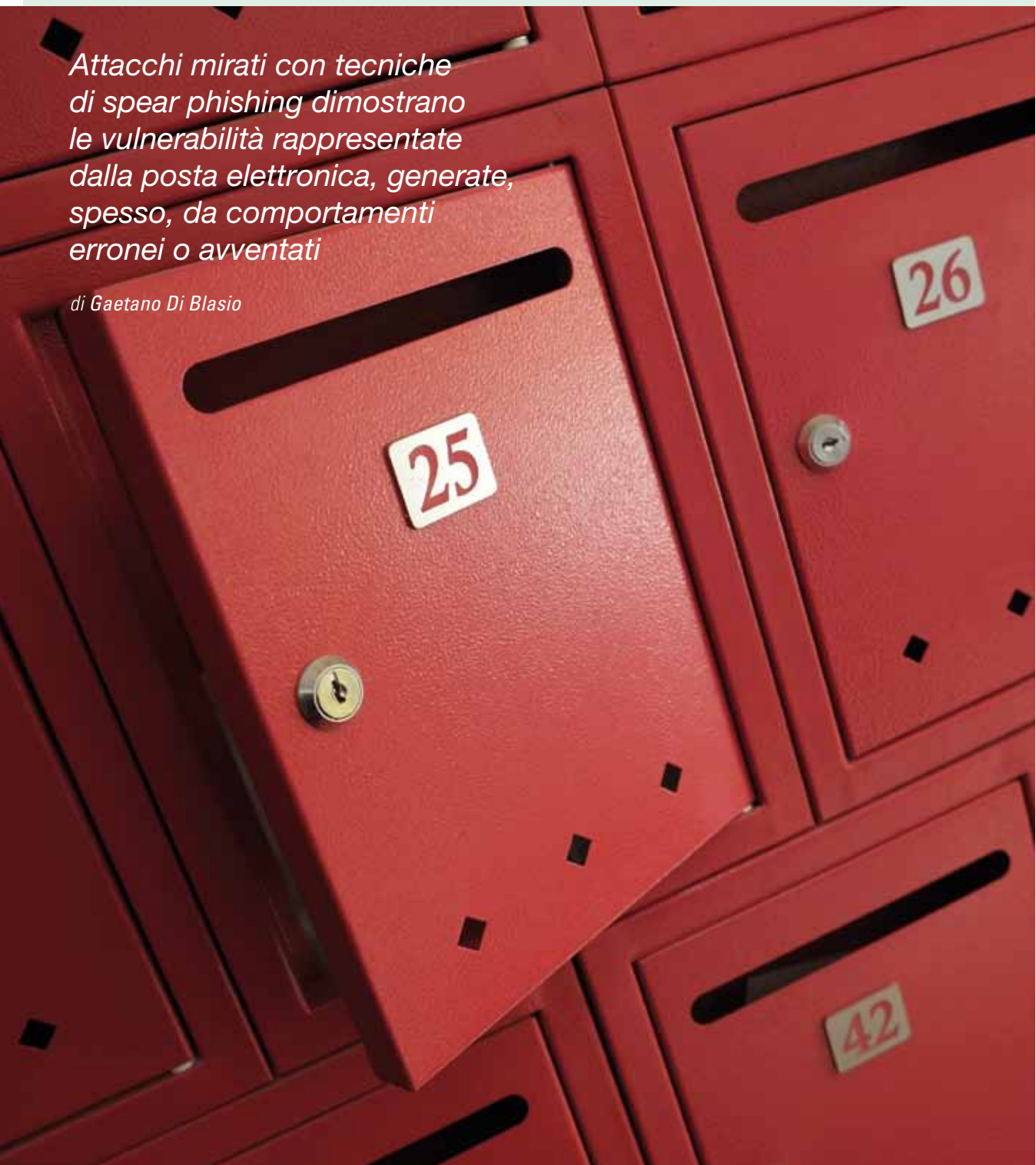
D: In che modo FireEye si propone di rispondere a queste nuove sfide ?

MR: Con tre elementi strettamente collegati tra loro: tecnologia capace di identificare attacchi sconosciuti; esperti che ogni giorno lavorano nell'analisi e risoluzione dei più importanti attacchi informatici; intelligence raccolte tramite l'infiltrazione di "spie" nei gruppi degli attaccanti.

LA SICUREZZA DELLA POSTA ELETTRONICA

Attacchi mirati con tecniche di spear phishing dimostrano le vulnerabilità rappresentate dalla posta elettronica, generate, spesso, da comportamenti erronei o avventati

di Gaetano Di Blasio



L'Instant messaging sta crescendo anche in ambito business, trainato dal massiccio utilizzo cui gli utenti sono avvezzi nel loro privato. Nonostante il successo di queste nuove forme di comunicazione, la posta elettronica è attualmente un elemento critico nei processi aziendali, sia essa parte integrante strutturata di quest'ultima o un elemento d'uso comune che ha sostituito strumenti tradizionali, come le vecchie circolari.

Ormai è normale utilizzare l'email per una fattura, anzi, la PA, con la PEC e la fattura elettronica ha definitivamente rotto un tabù, che, prima o poi sarà una regola per ogni impresa e procedura.

Ma la criticità risiede anche in utilizzi meno raccomandabili: è, per esempio, una consuetudine comune è quella di utilizzare la casella di posta elettronica come repository non solo delle corrispondenze importanti con colleghi, collaboratori, clienti e fornitori, ma anche di file e documenti che possono essere così recuperabili in qualsiasi momento, anche attraverso un dispositivo mobile. Inoltre, lo sviluppo della Unified Communication e Collaboration non fa altro che confermarne l'utilità. Questo, però, insieme allo sviluppo della mobility fornisce continui grattacapi ai responsabili dei sistemi informativi e della sicurezza in particolare.

La protezione dei dati sta diventando sempre più importante e oramai una priorità per i dipartimenti IT in alcuni settori economici come sanità e finanza, in particolare per quanto riguarda i dati privati dei clienti o assistiti. Non si tratta solo di regolamenti

cui adeguarsi, perché piuttosto che le sanzioni per una mancata uniformità, i rischi maggiori in caso d'incidente sono i danni derivanti dalla perdita di fiducia da parte della clientela. Chi manterrebbe il conto in una banca dopo che questa non è riuscita a impedire che il vostro conto corrente venisse prosciugato?

L'email è una delle principali forme di comunicazione verso l'esterno, cioè oltre il firewall. Se non adeguatamente protetta, si trasforma, anche, nella principale via per immettere nel sistema aziendale del malware o, più in generale, dei kit software preposti a sferrare attacchi all'infrastruttura. Ma non basta entrare, bisogna anche uscire con i dati copiati ed è sempre l'email a rappresentare una delle vie d'uscita più vulnerabili e, come tale, utilizzata per portare le informazioni all'esterno dell'azienda.

La posta come mezzo per il malware e via per la fuoriuscita delle informazioni

Se guardiamo solo l'ultimo decennio, possiamo osservare come la posta elettronica sia stata utilizzata per realizzare varie tipologie di truffe o attacchi informatici. Vanno ricordati, per esempio, i "worm", cioè un particolare tipo di codice malware il cui scopo era di penetrare nel computer della vittima lasciando traccia del suo passaggio con un virus, praticamente impedendone l'uso. Per entrare utilizzava un messaggio email contenente un allegato infetto e, per diffondersi si "autoinviava" a tutti i contatti della vittima stessa. Il più famoso è "I Love

You", il cui scopo era compiere il "giro del mondo" nel più breve tempo possibile.

Ancora oggi evoluzioni di I Love You o semplicemente pezzi di codice che lo componevano sono utilizzate in alcune fasi degli attacchi mirati o di quelli persistenti (Advanced Persistent Threats).

Per il dipartimento che si occupa della sicurezza informatica la sfida consiste nel riuscire a implementare un sistema per la protezione della posta elettronica che sia facile da integrare nel sistema informativo e non penalizzi i processi di business per i quali l'email è, ormai, vitale, ma al tempo stesso che sia conforme alle leggi nazionali e internazionali e ai regolamenti industriali.

Una soluzione che appare "definitiva" è la crittografia che renderebbe illeggibile i dati e le informazioni contenute nelle mail, soprattutto se a essere cifrati fossero tanto i messaggi quanto i file allegati. Ma non è così semplice. Gli approcci tradizionali non riescono a garantire la sicurezza che ci si aspetta quando il messaggio è codificato. I sistemi legacy, come S/MIME e PGP PKI, sono complessi, spesso troppo per l'IT aziendale. Inoltre non sono compatibili con piattaforme molto diffuse, quali Gmail, Yahoo e Android. Dall'altro lato, chiavi simmetriche utilizzate da sistemi proprietari, potrebbero generare un falso senso di sicurezza, perché, al costo di una complessa gestione delle chiavi, che dovranno essere memorizzate in un database a sua volta sicuro, potrebbero portare a un grave danno in dati "persi",

allorquando una chiave venisse compromessa. Anche implementare sistemi di posta proprietari personalizzati rischia di aggiungere complessità, senza aumentare affidabilità e sicurezza.

Per ridurre il rischio, la risposta non può essere rinunciare alla posta elettronica, né restringerne l'utilizzo. Eppure, anche a causa di queste problematiche molte imprese continuano a basare molti processi critici su una documentazione cartacea, che non solo rallenta il go to market e le decisioni interne, ma impone costi di gestione elevati e ostacola l'efficientamento.

In realtà c'è un rischio anche maggiore, considerando l'attuale tendenza alla digitalizzazione di molti processi. Oggi il consumatore medio è abituato a gestire la propria vita personale e familiare con strumenti quali i dispositivi mobili, dove la posta elettronica è ancora molto impiegata, ma sempre più soppiantata da altre forme di comunicazione. Per un'impresa rimanere ancorata al cartaceo può significare "l'estinzione". Si pensi a quanti portali offrono servizi come la prenotazione di visite specialistiche, viaggi, soggiorni oppure preventivi per assicurazioni e prestiti bancari, senza dimenticare l'e-commerce e immaginando quanti servizi ancora da inventare sorgeranno a breve. Si potrà restare scettici sulla dematerializzazione nella Pubblica Amministrazione, ma non si può restare fuori dalla corsa alla digitalizzazione. Neanche se le proprie attività sono "limitate" a rapporti con altre imprese.

HPE SECURE MAIL: PROTEZIONE END-TO-END PER POSTA E ALLEGATI

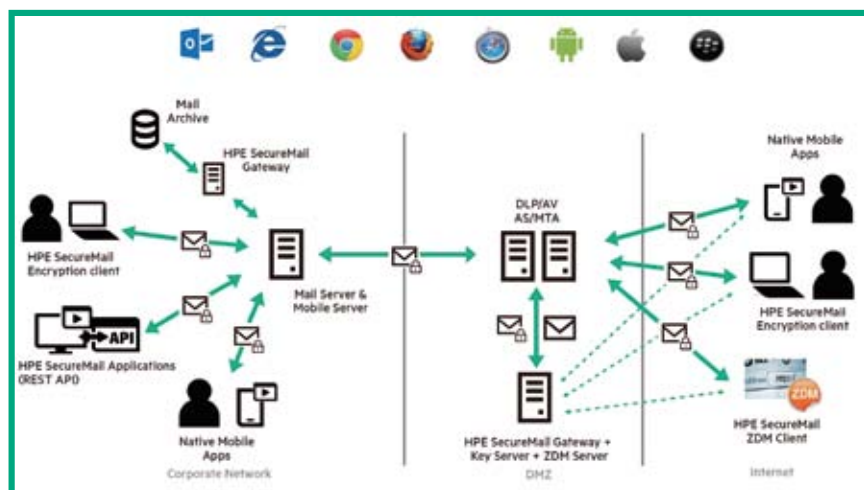
Una soluzione di crittografia che affronta gli aspetti della protezione della posta elettronica non dimenticando di affrontare temi quali la sicurezza in ambito mobile e cloud.

di Gaetano Di Blasio

HPE Security, la divisione dedicata alla sicurezza informatica all'interno della neo costituita HP Enterprise, dopo la riorganizzazione del colosso statunitense, ha sviluppato un'interessante soluzione modulare denominata HP SecureMail per la protezione tramite crittografia della posta elettronica. Una delle caratteristiche più importanti di HPE SecureMail è l'unicità della soluzione. In pratica la stessa sia per i computer desktop sia per i dispositivi sia per gli ambienti cloud. La decifratura può essere fatta dal pc, via Web o dal device mobile, tanto da un utente interno quanto da quello esterno e comprende scansione e filtraggio della posta in ingresso e in uscita. La soluzione può essere installata sia on premise sia su cloud pubblici o privati, come

pure in ambienti ibridi, come nel caso di un servizio come Office 365 di Microsoft. In particolare, sono supportati sistemi quali Outlook, Exchange, Blackberry Enterprise Server (BES) e altri sistemi di mobile device management (MDM). Questo è possibile anche perché HPE SecureMail mantiene una completa separazione tra la crittografia e il metodo di autenticazione, lasciando libertà di scelta per quest'ultimo, compresi Active Directory, LDAP o sistemi proprietari con propri portali. Altresì rilevante è la centralità del dato nella

Schema di funzionamento di HPE SecureMail



protezione sia del messaggio sia degli attachment, che sono memorizzati su storage interni e non di terze parti. In altre parole tutto viene cifrato e protetto, in modo che quandanche la posta venisse intercettata, il contenuto criptato non sarebbe di alcun valore.

Fondamentale è il sistema per la gestione delle chiavi per le prestazioni e la qualità del servizio. Basato sullo standard sviluppato da HPE, l'HPE Identify-Based Encryption (IBE), il sistema di cifratura non richiede che sia memorizzata o gestita alcuna chiave di cifratura.

È un aspetto cruciale, perché impedisce al malintenzionato di acquisire tali chiavi e riduce drasticamente gli oneri di un amministratore.

Inoltre, questo permette che i messaggi possano essere inviati a qualsiasi destinatario senza che questi debba preventivamente effettuare alcun tipo di configurazione. È anche grazie a ciò che la soluzione presenta un'elevata scalabilità. Le grandi imprese possono, dunque, contare su ampi margini, ma non solo. La soluzione è anche integrabile nelle infrastrutture per la sicurezza della posta già in essere in azienda, quali i sistemi anti-virus, anti-spam o di content filtering, nonché quelli preposti all'archiviazione dei messaggi.

A proposito di quest'ultima operazione, va segnalato che HPE SecureMail fornisce più opzioni per un'archiviazione delle mail basata su policy con un controllo supervisionato. I messaggi vengono memorizzati come normali mail, ma, grazie alle

HPE SecureMail Mobile Edition

HPE SecureMail Mobile Edition consente di leggere e inviare email codificate; funziona su dispositivi iOS, Android e BlackBerry, che è possibile controllare attraverso policy di utilizzo e sicurezza.

La soluzione, in questo modo estende la protezione centrata sui dati di HPE Security e rende conforme alle normative per la privacy e la security la gestione dei messaggi email e loro allegati, residenti o in transito sui dispositivi. Tutto questo, spiegano in HPE, senza modificare l'utilizzabilità del dispositivo da parte dell'utente finale. Più precisamente, è stata progettata una user experience nativa che integra la sicurezza con le capacità delle app e permette di applicare le policy di sicurezza in maniera non invasiva.

La soluzione estende la compliance ai dispositivi mobile, con una protezione end-to-end di messaggi email e attachment, mitigando il rischio di violazioni alla confidenzialità dei dati.

L'utilizzo di una tecnologia completamente "push", elimina il rischio di falle nelle procedure di sicurezza, mentre un sistema di Mobile Device Management (MDM) completa e migliora la sicurezza e la compliance, senza entrare in conflitto con le policy.

capacità di indicizzazione, ricerca, visualizzazione, e identificazione dei dati interni alle mail stesse, HPE SecureMail semplifica le richieste durante eventuali audit, contenziosi e indagini.

Sempre grazie alle caratteristiche di HPE IBE, non occorrono le descrizioni aggiuntive delle chiavi, tipicamente richieste dai sistemi PKI e Open PGP.

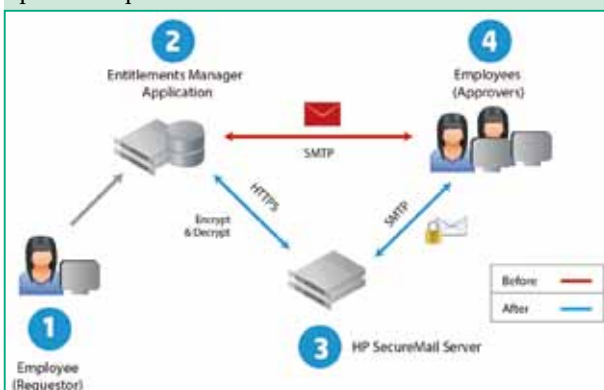
HPE SecureMail Application Edition

La protezione centralizzata dei dati fornita di HPE SecureMail può essere estesa ai dati strutturati e destrutturati presenti nei messaggi e gli attachment che vengono inviati, ricevuti e gestiti direttamente da applicazioni di business, portali o siti Web destinati a raccogliere o contenere informazioni riservate.

Questa estensione è attuata grazie ad HPE SecureMail Application Edition, che abilita una maggiore penetrazione in azienda dei processi di business automatizzati, proteggendo i dati che vengono gestiti direttamente dalle applicazioni, rendendo sicura la posta elettronica end to end interna e proveniente dal cloud.

HPE SecureMail Application Edition protegge i dati contenuti nel messaggio non appena questo viene spedito dall'applicazione, prima che passi dal backbone di posta, e per tutto il percorso fino alla destinazione. Un'architettura che assicura la compatibilità con tutte le normative su ricordate.

La soluzione è compatibile con qualunque client, sia esso desktop, mobile o Web, e con tutti gli attuali browser disponibili per pc o dispositivo mobile.



Un flusso di lavoro con un processo di approvazione basato su email che utilizza HPE SecureMail Application Edition

HPE SecureMail Cloud

Cifrare messaggi di posta dal computer in ufficio o da uno smartphone, distribuendoli attraverso portali, drive USB o altri sistemi di storage diventa facile con HPE SecureMail Cloud, che non richiede sforzi aggiuntivi da parte del destinatario.

Tutto questo è possibile grazie a una soluzione cloud erogata in modalità Software as a Service (SaaS) che consente di proteggere email, file e documenti senza investire in infrastrutture on premise.

Con la tecnologia di HPE SecureMail, che è accessibile via cloud, i mittenti devono semplicemente "premere" il bottone invio sicuro sul sistema di posta, da pc o device mobile, mentre il destinatario non vede modificata la propria experience e non deve far altro che aprire il messaggio.

I documenti crittografati sono, a quel punto, sicuri e distribuibili senza timore tramite portali, chiavette USB e vari storage di rete, senza bisogno di capire la crittografia. Un modulo software che è disponibile per il download permette l'accesso da un pc Windows per la crittografia dei documenti di Office.

La soluzione è utilizzabile anche via smartphone, senza bisogno di definire un nuovo account di posta né di definire un'apposita cartella di posta per i messaggi crittografati.

HPE SecureMail Cloud è disponibile in una versione Standard e in una Enterprise che dispone di alcune caratteristiche esclusive che consentono di aggiungere le funzionalità previste nella versione per l'on premise.

CHECK POINT: PROTEZIONE ZERO-DAY PER LE E-MAIL CLOUD-BASED

Il nuovo SandBlast Cloud protegge le e-mail dei clienti Microsoft Office 365 da malware conosciuti e sconosciuti

di Giuseppe Saccardi



Nathan Shuchami, head of advanced threat prevention di Check Point

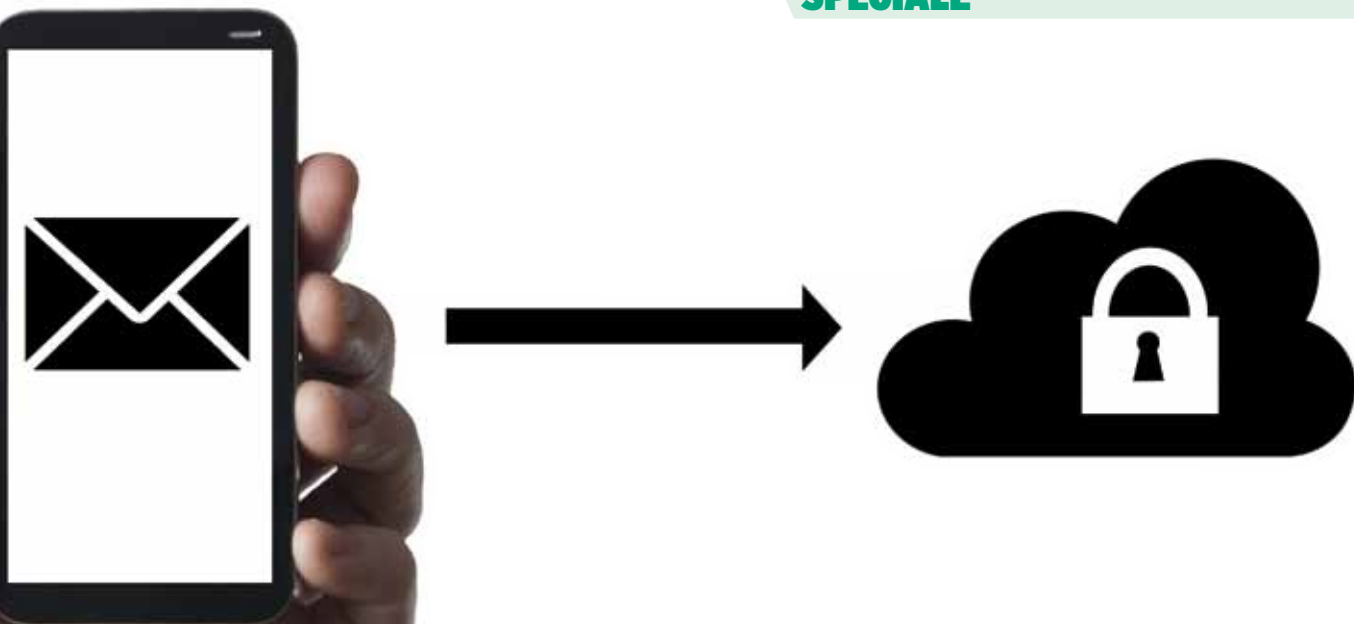
Continua la rincorsa tra attaccanti e difensori. Dal momento che le aziende stanno rapidamente migrando le proprie e-mail verso le infrastrutture cloud e gli hacker si sono attrezzati, Check Point Software Technologies ha studiato la contromossa. La società ha annunciato la disponibilità di SandBlast Cloud, una soluzione ideata per difendere le aziende dalle principali e più attuali minacce dei cyber criminali, che sfruttano le e-mail come ingresso principale per i propri attacchi.

SandBlast Cloud, l'ultimo arrivato della linea di mercato di soluzioni SandBlast, è stato progettato al fine di salvaguardare la sicurezza delle aziende con un'e-mail Microsoft Office 365 dalle minacce sofisticate quali ransomware e APT.

L'obiettivo di base è di consentire alle organizzazioni di migrare verso le infrastrutture cloud in tutta sicurezza. SandBlast Cloud è dotato del rilevamento a livello della CPU di Check Point e delle funzionalità di Threat extraction che prevengono, in modo proattivo, gli attacchi prima che colpiscano gli utenti.

Se, da un lato, l'e-mail ha permesso di trasmettere in modo più efficace che mai comunicazioni e informazioni, dall'altro, riconosce la società, rappresenta anche un vettore privilegiato per trasmettere malware, anche di tipo ransomware. In proposito, secondo il Data breach investigations report 2016 di Verizon, gli allegati delle e-mail sono il mezzo più comune per recapitare contenuti malevoli e i dati mostrano, inoltre, che gli utenti hanno aperto e cliccato sul 12% circa degli allegati infetti ricevuti. Considerando il fatto che l'intervallo trascorso tra la ricezione del contenuto e il primo click è stato solo di 3 minuti e 45 secondi è evidente che prevenire che questi file malevoli vengano recapitati agli utenti è essenziale al fine di evitare il propagarsi delle infezioni.

«I metodi degli hacker sono in continua evoluzione e



le aziende rischiano sempre più di cadere vittime di attacchi via e-mail personalizzati, quindi devono armarsi di misure di sicurezza proattive e sofisticate, per mantenersi un passo avanti alle minacce più evolute. SandBlast Cloud offre uno dei livelli di protezione più elevati sul mercato ai clienti con un'e-mail Office 365, attraverso una soluzione cloud pura, che fornisce contenuti sicuri velocemente, con una visibilità completa, e gestibili attraverso il relativo portale cloud-based», ha dichiarato Nathan Shuchami, head of advanced threat prevention di Check Point.

Nella lotta infinita, che ogni giorno viene portata avanti, per difendersi dalle email infette che possono causare violazioni dei dati, perdite finanziarie e diminuzione della produttività, le aziende devono, in sostanza, poter contare su una evoluta soluzione di sicurezza cloud per le proprie email, in grado non solo di prevenire gli attacchi dei malware esistenti, ma anche riuscire a individuare, in modo proattivo e quindi bloccare, le eventuali minacce non ancora conosciute, appena vengono individuate.

SandBlast Cloud fornisce in tal senso agli utenti di Office 365 una difesa stratificata, per essere al sicuro contro le minacce conosciute e sconosciute. Questo compito è assolto dalla protezione antivirus e dalla URL reputation, che protegge gli utenti dalle minacce conosciute, mentre le funzionalità avanzate, tra cui Threat extraction e Threat emulation, evitano che malware sconosciuti e minacce zero-day siano recapitate all'utente finale.

Tra le principali caratteristiche che possiamo riconoscere a SandBlast Cloud vi sono:

- Integrazione con Microsoft Office 365, gestita come una soluzione cloud.
- Alto tasso di rilevamento malware attraverso mediante tecnologia brevettata di analisi a livello della CPU.
- La trasmissione di versioni sicure e ricostruite dei formati di documento più diffusi, nel giro di secondi, e l'accesso completo al file originale, nell'arco di minuti, una volta che è stata ultimata l'analisi completa.

Come prodotto SandBlast Cloud sarà disponibile, sul mercato, a partire dall'estate 2016.

BARRACUDA, MAGGIORE PROTEZIONE CONTRO GLI ATTACCHI E-MAIL MIRATI

Disponibili nuove funzionalità per la protezione contro le minacce avanzate per le soluzioni in cloud Essentials for Office 365 ed Email Security Service

di Ricardo Florio

Barracuda Networks ha reso disponibili nuove funzionalità anti-phishing e di difesa contro gli attacchi mirati per le proprie soluzioni cloud per la sicurezza email Barracuda Essentials for Office 365 e Barracuda Email Security Service.

Barracuda Essentials for Office 365 è una soluzione per la protezione di e-mail, dati e infrastruttura cloud che mette a disposizione funzioni di sicurezza multi-layer, di archiviazione e di backup che favoriscono un uso più rapido, sicuro ed efficiente di Microsoft Office 365.

Barracuda Email Security Service è una soluzione SaaS pensata per bloccare le minacce provenienti dalle e-mail prima che queste possano avere accesso alla rete aziendale. È un servizio che si propone come possibile alternativa alle soluzioni basate su software e hardware per garantire sicurezza delle e-mail sfruttando i vantaggi di flessibilità e scalabilità del cloud. Barracuda Email Security Service



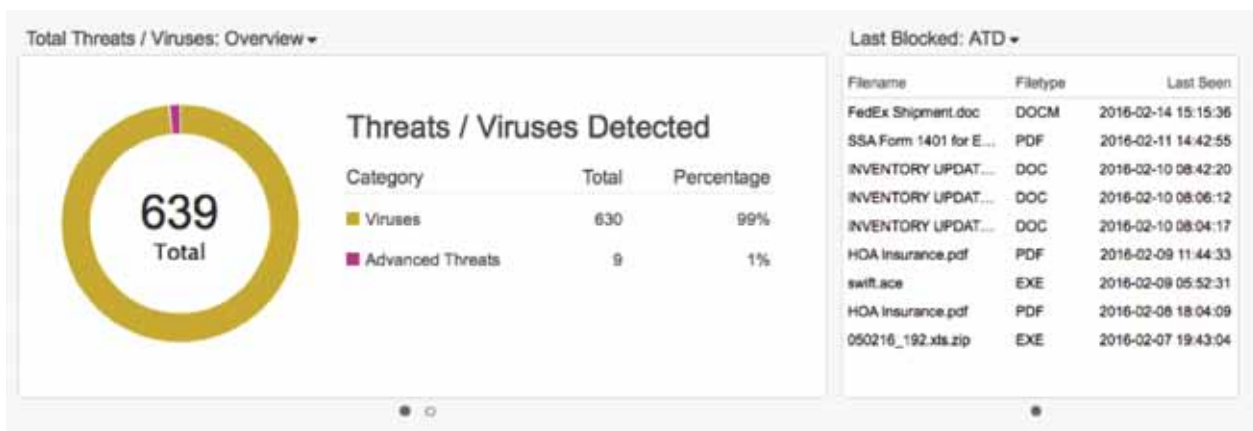
gestisce il traffico delle e-mail in entrata e in uscita per fornire protezione contro le perdite di dati e possibili attacchi e permette di crittografare i messaggi e di eseguire lo "spool" delle e-mail qualora i server di posta non siano disponibili.

Le nuove funzionalità: Advanced threat protection e Link protection

Le nuove funzionalità introdotte da Barracuda sono indirizzate ad aziende di ogni dimensione, in ambienti sia cloud sia on premise, per la protezione contro attacchi mirati diffusi tramite allegati di posta elettronica, per inibire l'accesso a URL pericolosi e contrastare le pratiche di phishing. Sfruttano un patrimonio di conoscenze aggregate, raccolte anche grazie a 150mila clienti distribuiti in tutto il mondo, per trasformarle in informazioni utili a fornire funzionalità avanzate di protezione.

La componente di Advanced Threat Protection coniuga tecnologie comportamentali, euristiche e di sandboxing per proteggere gli utenti dal malware, dagli attacchi mirati e "zero day" diffusi tramite gli allegati e-mail. Il framework di analisi di Barracuda

I risultati del blocco delle minacce di un'istanza di Email Security Service utilizzando la funzione Advanced threat protection



unisce la conoscenza delle minacce veicolate da molteplici vettori, quali e-mail, reti, applicazioni, Web, mobile e utenti.

La funzione di Link Protection di Barracuda è pensata per proteggere gli utenti che cliccano su link dannosi o fraudolenti aprendo questi link all'interno di una sandbox protetta. Si tratta di una tecnologia particolarmente utile per gli utenti remoti che accedono alle e-mail da dispositivi mobili e che potrebbero accidentalmente cliccare su URL compromessi. Link Protection identifica le anomalie negli URL, blocca l'accesso e avvisa l'utente della possibile minaccia. «Gli attacchi mirati stanno diventando un fenomeno comune - ha osservato BJ Jenkins, presidente e CEO di Barracuda -. Il phishing è il punto di lancio più diffuso per gli attacchi multilayer: è chiaro che il possesso di una tecnologia anti-phishing e la formazione degli utenti sono passaggi critici nella protezione dell'azienda. Barracuda si trova nella posizione ideale per individuare e aggregare le minacce attraverso tutti i vettori, il che ci permette di avere una visione olistica dello scenario delle minacce. Siamo in grado di utilizzare queste conoscenze e

aggiornare le nostre soluzioni di sicurezza in tempo reale, offrendo alle aziende clienti di ogni dimensione una protezione completa contro questi attacchi mirati a un costo vantaggioso, un beneficio in genere riservato a quelle organizzazioni che dispongono di budget e risorse molto elevati».

Barracuda ha previsto una nuova versione di Essentials for Office 365 denominata Email Security Edition che include, in un unico bundle, le funzioni di sicurezza e-mail Link protection e Advanced threat protection e che sarà disponibile a partire da 1,80 Euro al mese per utente. I clienti Barracuda Email Security Service possono usufruire della funzionalità anti-phishing Link protection senza costi aggiuntivi mentre la componente Advanced threat protection può essere aggiunta all'abbonamento esistente con un costo aggiuntivo a partire da 1,40 Euro al mese per utente.

SERVIZIO F-SECURE: RILEVA GLI ATTACCHI ENTRO 30 MINUTI

F-Secure Rapid Detection Service combina sensori, intelligence e monitoraggio h24 effettuato da un team di esperti allo scopo di combattere gli attacchi informatici

di Giuseppe Saccardi

Se non stai rilevando incidenti alla tua sicurezza, probabilmente è perché ti stai perdendo qualcosa. Questo è il messaggio che F-Secure ha lanciato in occasione della presentazione di un suo nuovo servizio di rilevazione delle intrusioni e di risposta agli incidenti per scoprire le minacce presenti sulla rete aziendale.

Il servizio gestito Rapid Detection, ha evidenziato l'azienda, si è proposto di combinare il meglio dell'uomo con l'intelligenza delle macchine per informare le aziende in soli 30 minuti dalla rilevazione di una minaccia.

Il fatto è che, in media, le violazioni di dati possono durare settimane, mesi o persino anni prima di essere rilevate. Secondo Gartner, la più grande area di bisogni insoddisfatti è, quindi, rappresentata da un'efficace rilevazione di attacchi mirati e di violazioni. Le organizzazioni, in pratica, non riescono a effettuare diagnosi precoci di una violazione e, secondo l'analista, ben il 92% di violazioni restano nascoste all'organizzazione che è stata colpita. Molte aziende si basano solamente sulla difesa



Pekka Usva, vice president of Advanced Threat Protection in F-Secure

perimetrale per proteggersi che è, sì importante, ma solo come parte di una strategia di sicurezza informatica globale.

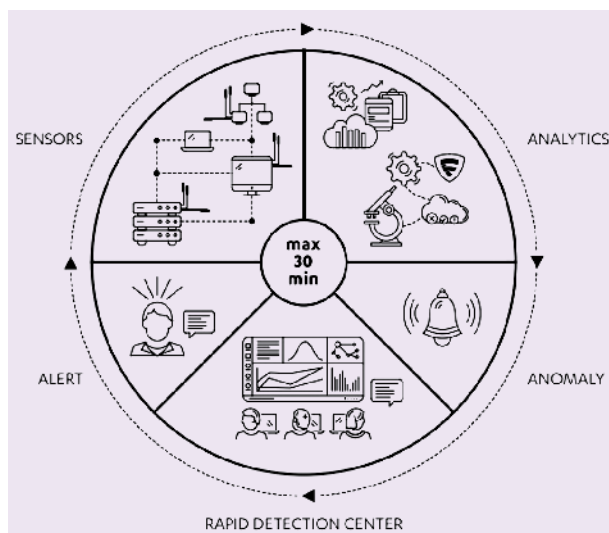
Con attori di minacce avanzate che colpiscono le organizzazioni con attacchi altamente mirati, un tentativo di attacco finirà, inevitabilmente, col superare i controlli di sicurezza e penetrare nella rete. La capacità nel riuscire a rilevare velocemente le intrusioni e a rispondere in modo immediato è, pertanto, fondamentale, ma non è semplice da mettere in atto.

«Le aziende si stanno rendendo conto che da sole fanno realmente fatica a rilevare intrusioni e a rispondere agli incidenti ha osservato Pekka Usva, VP of Advanced Threat Protection in F-Secure -. Creare al proprio interno un sistema appropriato di questo tipo è estremamente difficile e costoso e richiede anni per poterlo fare. Ecco perché ha senso affidarsi a un servizio gestito, che fornisca un immediato e tangibile ritorno sull'investimento».

Il meglio dell'uomo e della macchina

Il servizio Rapid Detection di F-Secure si basa,

L'architettura del servizio di rilevamento rapido degli attacchi



come abbiamo accennato, sulla forza dell'intelligenza umana unita a quella della macchina in modo da fornire un servizio all-in-one di rilevazione delle intrusioni e di risposta pronto a entrare in azione immediatamente.

Il servizio consiste di tre componenti principali: sensori di rete e degli endpoint che raccolgono dati sugli eventi e le attività; l'analisi comportamentale e l'intelligence delle minacce di F-Secure che analizzano i dati e identificano le anomalie; il Rapid Detection Center presidiato da un team di esperti di sicurezza informatica 24 ore al giorno, sette giorni su sette, in grado di identificare e gestire gli incidenti di sicurezza.

Quando viene rilevata una violazione un esperto contatta il cliente entro 30 minuti con una risposta per l'incidente e per fornire servizi opzionali di investigazione on-site se necessario.

«La componente umana è un fattore decisivo - ha commentato Erka Koivunen, cyber security advisor di F-Secure -. Gli attaccanti del resto sono umani, quindi per scoprirli non ci si può basare solo sulle

macchine. Il fattore umano elimina anche i falsi positivi, che rappresentano, senza ombra di dubbio, un ampio spreco di risorse».

Nel momento in cui una violazione viene rilevata, il servizio Rapid Detection è in grado di fornire, anche, delle informazioni che possono suggerire azioni per la fase di risposta. Il team preposto alla sicurezza del cliente riceverà informazioni su come la violazione è avvenuta, su come isolarla e otterrà consigli su come porre rimedio.

Con una rilevazione veloce, una diagnosi accurata e i consigli di un esperto su come rimediare alla situazione, le aziende possono limitare i danni e tornare al loro business prima possibile. F-Secure può, in aggiunta, fornire altri servizi on-site opzionali per la gestione degli incidenti e le investigazioni di tipo forense.

Rapid Detection, precisa F-Secure, è un servizio che si integra con i diversi ecosistemi esistenti e fornisce un ulteriore livello di sicurezza per rafforzare la strategia di sicurezza informatica dell'azienda.

LA MINACCIA RANSOMWARE



Gastone Nencini,
country
manager di
Trend Micro
Italia



È uno dei malware più insidiosi e in rapida crescita. Sfrutta spesso la posta elettronica per installare un programma che inibisce l'utilizzo di sistemi e file facendo leva sulla scarsa consapevolezza dei rischi da parte dei dipendenti

È decisamente un astro nascente nel panorama del cyber crime. Si tratta del ransomware, un tipo di malware che impedisce o limita l'accesso degli utenti al loro sistema, bloccandone lo schermo oppure impedendo l'accesso ai file. Le più moderne famiglie di ransomware, collettivamente classificate come cripto-ransomware, sono invece in grado di cifrare determinati tipi di file presenti sui sistemi infetti, rendendoli inaccessibili.

Alle vittime malcapitate viene offerta la possibilità di riprendere il controllo di sistemi e file dietro pagamento di una somma in denaro. Il nome di questo malware deriva proprio dalla parola inglese ransom, che significa riscatto.

Pagare o non pagare ?

Le vittime sono spesso tentate di risolvere subito il problema cedendo al ricatto. Tuttavia, l'esperienza dimostra che non vi è alcuna garanzia che pagando il riscatto si riesca a ottenere la chiave di decrittografia o lo strumento di sblocco necessario per riottenere l'accesso ai sistemi infetti o ai file presi in ostaggio: i documenti e file spesso sono persi. D'altronde non è saggio pensare a impostare un rapporto di fiducia con qualcuno che vi sta ricattando.

I prezzi del riscatto possono variare in base alla variante di ransomware o anche ai tassi di cambio in corso delle valute digitali. Infatti, grazie all'anonimato offerto dalle valute digitali, chi sfrutta i ransomware spesso richiede il pagamento del riscatto in Bitcoin. Esistono tuttavia molteplici varianti e alcune ransomware prevedono anche opzioni alternative di pagamento come carte regalo iTunes e Amazon.

Il comportamento dei ransomware

È possibile incorrere in questa minaccia attraverso una varietà di mezzi. Un ransomware può essere scaricato sul sistema quando un ignaro utente si trova a visitare siti Web compromessi. Oppure può essere diffuso come "payload" che viene rilasciato da "exploit" su sistemi vulnerabili oppure scaricato da parte di altri malware. Molti ransomware sono noti per essere distribuiti come allegati di e-mail spam.

Una volta eseguito nel sistema, un ransomware può bloccare lo schermo del computer o, nel caso di cripto-ransomware, crittografare file predeterminati. Nel primo scenario, viene visualizzata un'immagine a tutto schermo che impedisce alle vittime di usare il loro sistema. L'immagine solitamente notifica l'infezione in atto e mostra le istruzioni su come gli utenti possono

pagare per il riscatto. Il secondo tipo di ransomware impedisce l'accesso a file potenzialmente critici o importanti, come documenti e fogli di calcolo.

Per esempio, i laboratori Trend Micro sono stati i primi a intercettare un'ondata di attacchi crypto-ransomware che ha flagellato l'Europa nel corso delle festività natalizie, facendo leva sulle attitudini all'online shopping e inviando migliaia di mail in cui si cercava di persuadere le vittime ad aprire allegati o cliccare link correlati a spedizioni di pacchetti o altre merci acquistate. Il link conduceva a un sito controllato dai cyber criminali, dove all'utente veniva chiesto di inserire un codice "captcha"; questo innescava il download di un file che crittografava tutti i documenti del computer.

Come proteggersi

La migliore protezione contro i ransomware è impedire che possano raggiungere il sistema. Per non farsi sorprendere da attacchi di questo genere è, dunque, meglio adottare sin da subito misure preventive mantenendo costantemente nel tempo pratiche efficienti di protezione e seguendo alcune semplici regole.

La diffusione della sicurezza all'interno dell'azienda e la consapevolezza rappresenta sempre e comunque una pratica da perseguire poiché i dipendenti sono molto spesso l'anello debole della catena di protezione.

La posta elettronica è uno dei principali veicoli per i ransomware e, di conseguenza, imparare a diffidare di allegati provenienti da mittenti poco affidabili, contenenti un eseguibile, un file compresso o altrimenti sospetto deve far nascere il sospetto e farci essere più attenti. È importante che gli utenti adottino comportamenti responsabili e verifichino attentamente le e-mail ricevute prima di aprire allegati o cliccare su link che potrebbero sembrare sospetti. Una delle caratteristiche tipiche del phishing o delle tecniche di social engineering, che

alimentano la diffusione di ransomware, è l'urgenza sempre associata alla comunicazione, in modo da spingere l'utente a ridurre la cautela per la percezione di dover agire in fretta. Anche questo è un segnale da valutare per riconoscere e-mail o attività sospette.

È necessario installare le ultime versioni e applicare configurazioni delle soluzioni di sicurezza conformi alle best practice come quelle fornite da Trend Micro, per impostare una sicurezza multi-livello.

Va predisposta l'impostazione di policy mail per bloccare le potenziali minacce contenute negli allegati, così come installare soluzioni anti-spam o di email scanning. È importante anche che le soluzioni di sicurezza siano mantenute aggiornate e che vengano applicati i più recenti aggiornamenti critici e patch per il sistema operativo e per gli altri software chiave (per esempio il browser). Infatti, così come i produttori di sicurezza sono costantemente al lavoro per aggiornare i propri strumenti, anche gli scrittori di ransomware costantemente modificano i loro metodi e tattiche, per cercare di rendere inefficaci gli strumenti di protezione.

Da ultimo, ma non meno importante, è bene conservare sempre una copia in backup non in linea o in cloud dei propri dati critici e più importanti.

Trend Micro, grazie alla sua infrastruttura Smart Protection Network, mette a disposizione un'infrastruttura per la protezione automatizzata degli ambienti fisici, mobili, virtuali e cloud che sfrutta una tecnologia di assegnazione del livello di reputazione di URL, e-mail, file e App per abilitare una difesa efficace e in tempo reale contro ogni tipo di minaccia, incluse quelle cosiddette "zero day".

A questa tecnologia Trend Micro abbina una gamma di soluzioni di sicurezza che abitano una protezione multi-livello e persino un tool gratuito (Ransomware File Decryptor) per provare a decifrare i file cifrati da certe famiglie di ransomware.

#VUOILMIONUMERO?

**VUOI
IL MIO
NUMERO?**

dejavu.it



95051730109

**"LA TUA FIRMA È LA NOSTRA FORZA."
IVAN, GIOVANE PAPÀ CON UNA FORMA GRAVE DI SCLEROSI MULTIPLA.**

PRENDI NOTA, DAI IL TUO 5X1000 A FISM.

Scegli di donare il 5x1000 alla Fondazione Italiana Sclerosi Multipla, firmando nel riquadro "finanziamento della ricerca scientifica e della università" e inserendo il codice fiscale 95051730109.

CODICE FISCALE FISM: 95051730109 | NUMERO VERDE: 800.094.464 | www.sostienici.aism.it

**SCLE
ROSI
MULT
IPLA**
ONLUS
fondazione
italiana

un mondo
libero dalla SM