

Dai sistemi di intrusion detection all'analisi comportamentale per rilevare le tecniche di evasione, continua la rincorsa alle minacce di ultima generazione mentre si aprono scenari apocalittici con lo sviluppo dell'IoT e gli attacchi DDoS di massa.

L'attenzione alla sicurezza dell'identità digitale e l'avvento delle tecniche basate su analytics e machine learning **pag. 10**

malware

**SPECIALE
THREAT PREVENTION**

UNA RUBRICA SULLA SICUREZZA DIGITALE CURATA DA AIPSI

Da questo numero di Security&Business inizia la pubblicazione della rubrica mensile di AIPSI, Associazione Italiana Professionisti Sicurezza Informatica, che tratterà temi e strumenti sulla sicurezza digitale. Si rafforza la partnership con Reportec, con attività online. **pag. 3**



CYBER ATTACK

LA SECURITY FABRIC DI FORTINET ORCHESTRA I FIREWALL

Una ricerca di Check Point rivela le preoccupazioni sulla sicurezza che rendono critiche le scelte nel cloud. Un'indagine di F5, invece affronta il tema dell'application security e della delicata questione delle identità digitali. **pag. 8**

IN QUESTO NUMERO:

AIPSI

pag. 3-5

- Una rubrica sulla sicurezza digitale curata da AIPSI

CYBER ATTACK

pag. 6-7

- La sicurezza resta la prima preoccupazione del cloud

pag. 8-9

- F5 mette l'Application Security al centro della protezione

SPECIALE

pag. 10-13

- Threat Prevention, intelligence e resilienza

pag. 14-15

- La protezione dal ransomware e oltre con Kaspersky Lab

SOLUZIONI

pag. 16-17

- HPE Security Arcsight: intelligence di sicurezza a massima velocità

pag. 18-19

- Proteggere i sistemi SCADA per non fermare la produzione

SICUREZZA COSTANTE, INTELLIGENTE

E PUOI AVERLA SUBITO.

Le tue aree di vulnerabilità aumentano. I contenuti si moltiplicano.

I cybercriminali sono sempre più scaltri.

Fortinet offre una singola infrastruttura di sicurezza intelligente che protegge la tua rete dalle minacce attuali e future.

Visita www.fortinet.it per maggiori informazioni.

FORTINET®

Sicurezza senza compromessi

UNA RUBRICA SULLA SICUREZZA DIGITALE CURATA DA AIPSI

Da questo numero di Security&Business inizia la pubblicazione della rubrica mensile di AIPSI, Associazione Italiana Professionisti Sicurezza Informatica, che tratterà temi e strumenti sulla sicurezza digitale.

di Marco Bozzetti

AIPSI (www.aipsi.org) è il capitolo italiano di AISSA (www.issa.org), l'associazione internazionale no-profit di professionisti ed esperti praticanti, focalizzata nel mantenere la sua posizione di "Global voice of Information Security". Più precisamente, si tratta, grazie all'attiva partecipazione dei singoli soci e dei relativi capitoli in tutto il mondo, della più grande associazione non-profit di professionisti della sicurezza (vanta oltre diecimila associati a livello mondiale).

L'organizzazione di forum e di seminari di approfondimento e di trasferimento di conoscenze, la redazione di documenti e pubblicazioni, la formazione per le certificazioni europee eCF per la sicurezza informatica (normato in Italia come UNI 11506), oltre all'interazione fra i vari professionisti della sicurezza, contribuiscono concretamente a incrementare le competenze e la crescita professionale dei soci, oltre che promuovere più in generale la cultura della sicurezza ICT e della sua gestione in Italia. L'appartenenza al contesto internazionale ISSA, permette ai soci AIPSI di interagire con gli altri capitoli

europei, americani e del resto del mondo.

Numerosi i benefici per i Soci AIPSI, sintetizzati nel Box 1.

La strategia AIPSI 2017-18

AIPSI è una associazione di singole persone, non anche di aziende ed Enti, che professionalmente si interessano e/o operano nell'ambito della sicurezza digitale. Quindi un'associazione di liberi professionisti e dipendenti lato domanda e lato offerta ICT, specialisti tecnici e manager della sicurezza digitale, professionisti e manager di altri settori che si occupano anche saltuariamente di sicurezza digitale. Tipici esempi di questa ultima tipologia di soci includono svariati settori e ordini professionali, dalla sanità alla finanza, dall'industria ai servizi, dagli avvocati ai commercialisti, dai consulenti manageriali ai fornitori di servizi ICT, dai progettisti agli sviluppatori di software, dai gestori di risorse umane ai responsabili degli acquisti.

Come per ogni libera associazione, l'obiettivo primario è la continua crescita dei Soci. Per questo

occorre far conoscere AIPSI e le sue qualificate attività al più ampio bacino possibile di potenziali soci, oltre che realizzare per essi servizi reali e utili nell'ottica primaria della loro crescita professionale. Per ottenere tali risultati AIPSI in particolare, per il biennio 2017-8:

- ha recentemente rifatto il proprio sito web quale portale dei servizi digitali per i propri Soci e come punto di informazione e promozione delle proprie attività per tutti i potenziali interessati alla sicurezza digitale;
- collabora e promuove OAD, Osservatorio Attacchi Digitali in Italia, e la sua diffusione, oltre ad altre indagini relative alla sicurezza digitale in Italia;
- supporta i Soci nelle qualificazioni e certificazioni professionali, in primis l'europea eCF;
- fornisce lo scambio di informazioni su opportunità professionali e di business tra i Soci;
- favorisce e contribuisce all'aggiornamento continuo delle competenze sulla sicurezza digitale con convegni, workshop, seminari e nel prossimo futuro con corsi di formazione e sensibilizzazione in aula e a distanza (elearning), anche grazie alle numerose iniziative di ISSA e all'ISSA Journal;
- presidia vari tavoli istituzionali fornendo un proprio autorevole contributo.

Iniziative AIPSI 2017

Per il 2017 AIPSI ha in cantiere varie iniziative, alcune delle quali in collaborazione con Reportec, che è il suo primo Media Partner.



Un'iniziativa attualmente in corso è l'indagine sugli attacchi agli applicativi informatici, il cui questionario, completamente anonimo, è online all'indirizzo <http://vm2538.cloud.seeweb.it/lime/index.php/survey/index/sid/258122/newtest/Y/lang/it>.

Si invitano tutti i lettori di Security&Business a compilarlo quanto prima possibile, dato che l'indagine è in fase di chiusura: bastano pochi minuti, sono solo 14 domande con le risposte tra cui scegliere preimpostate.

Come riconoscimento dell'aiuto fornito con la compilazione del questionario online, alla fine i rispondenti potranno scaricare un numero della rivista mensile ISSA Journal, che rappresenta uno dei principali benefici per i soci in termini di aggiornamento e di reale trasferimento di know-how.

Il Rapporto 2016 OAD è scaricabile gratuitamente da http://www.malaboadvisoring.it/index.php?option=com_sfg&formid=43, inserendo i pochi dati richiesti e il codice coupon AIPSI: ABmi5VmTIH (attenzione a non inserire caratteri blank prima o dopo il codice!).

L'elenco dei Convegni e workshop a calendario è riportato nella pagina <http://www.aipsi.org/eventi/calendario-eventi-2017.html>.

L'elenco è "corrente", man mano si aggiorna. Alcune manifestazioni sono effettuate in collaborazione con altri Enti e associazioni, e per talune deve ancora essere fissata la data precisa. Alle iniziative italiane si affiancano quelle internazionali di

ISSA, che sono di elevata qualità e di forte interesse, specialmente i webinar riservati ai soci, il cui calendario sarà quanto prima pubblicato online.

Dal 2015 è stato costituito in ISSA un gruppo di lavoro dei referenti dei capitoli europei, per cooperare su possibili comuni iniziative e migliorare lo scambio di informazioni inerenti l'ambito europeo.

I principali benefici nell'essere socio AIPSI

- Ricevimento di ISSA Journal, la rivista mensile di ISSA.
- Accesso/ricevimento newsletter di ISSA e newsletter italiana di AIPSI.
- Partecipazione ai webinar ISSA.
- Trasferimento di conoscenza e formazione continua sulla sicurezza per l'aggiornamento e la crescita professionale dei soci.
- Corsi per le certificazioni professionali per le competenze sulla sicurezza, in particolare per eCF.
- Networking con altri professionisti del settore.
- Possibilità di costituire gruppi di lavoro per ricerche e condivisione informazioni su tematiche d'interesse comune.
- Accesso e sconti a seminari, conferenze, training a carattere nazionale e internazionale.
- Pubblicazione di articoli e contenuti nel sito web AIPSI.
- Possibilità di redigere articoli per conto di AIPSI/ISSA.
- Pubblicazione e ricerca di curricula vitae per agevolare la domanda/offerta di competenze e di professionalità.
- Accesso al materiale riservato ai soci sul sito web ISSA.
- Visibilità nazionale e internazionale grazie al riconoscimento di ISSA nel mondo.
- Possibilità di partecipare a seminari e conferenze come operatore per conto di AIPSI/ISSA.
- Nel prossimo futuro la rappresentanza dei soci professionisti dell'Information Security, nell'ambito delle recenti normative italiane stabilite dal D.Lgs. 4/2013 sulle professioni non regolamentate.

LA SICUREZZA RESTA LA PRIMA PREOCCUPAZIONE DEL CLOUD

Una ricerca di Check Point evidenzia i timori e gli accorgimenti dei professionisti IT legati ai processi di migrazione dei dati nel cloud di Riccardo Florio

Il tema della sicurezza è da sempre una variabile centrale in tutti i progetti cloud.

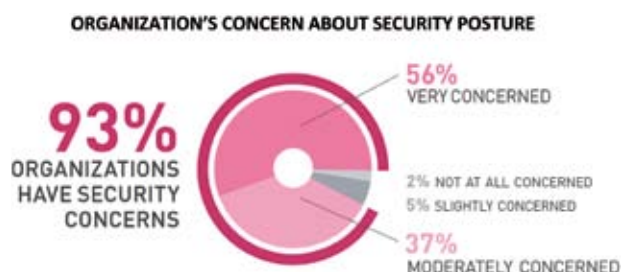
Le aziende, nel corso degli anni, hanno dovuto imparare a superare la barriera psicologica di aprire la propria infrastruttura all'esterno verso clienti e partner. Il cloud, però, richiede un passo in più perché la natura stessa con cui i dati vengono memorizzati e "backuppati" rende più difficile (e qualche volta impossibile) sapere sempre dove questi si trovano fisicamente e riduce, pertanto, la percezione di controllo da parte dell'azienda.

Mettere i dati critici sul cloud significa affidare a un'organizzazione esterna e alle sue procedure interne operative, di gestione e di sicurezza il futuro della propria azienda.

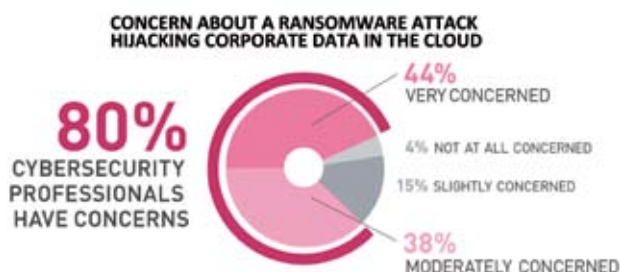
Per queste ragioni, nonostante gli investimenti nel

cloud continuano ad aumentare guidati dalla ricerca di modi per ridurre i costi, aumentare l'agilità e migliorare il supporto al business, la sicurezza di dati, applicazioni e sistemi critici all'interno del cloud resta una barriera importante che rallenta la diffusione dei servizi cloud. La percezione di una sicurezza insufficiente rappresenta il principale singolo contributore al rallentamento nell'adozione del cloud computing.

A questo tema Check Point ha dedicato un survey condotto a novembre 2016, coinvolgendo oltre 200 professionisti dell'IT e della sicurezza per evidenziare le preoccupazioni e i fattori di rischio correlati alla migrazione nel cloud e per individuare i controlli di sicurezza e le best practice adottate dagli esperti in cyber security nel passaggio al cloud.



Livello di preoccupazione per la sicurezza



Livello di preoccupazione riguardo agli attacchi ransomware

*Dall'alto:
Le minacce maggiori agli ambienti cloud.
Capacità di sicurezza per incrementare la
fiducia in ambienti cloud.
I 5 metodi più efficaci per proteggere
i dati nel cloud.*

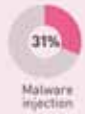
Il primo dato evidente che è emerso è l'elevato grado di preoccupazione per la sicurezza mano a mano che sempre più dati vengono spostati nel cloud. Il 93% è mediamente o molto preoccupato di questo aspetto. Un altro elemento di preoccupazione è rappresentato dalle principali minacce che possono colpire i dati nel cloud. Tra queste innanzitutto il ransomware che preoccupa l'80% dei professionisti della cyber security, a cui si aggiungono, nell'ordine, l'accesso non autorizzato (67%), il data leakage (65%) e gli attacchi del tipo Denial-of-Service (52%).

Le funzionalità di sicurezza su cui si fa affidamento per ridurre i rischi legati al cloud sono innanzitutto legate alla possibilità di ottenere visibilità, report e controllo costante sugli eventi di sicurezza esteso attraverso tutte le piattaforme cloud (74%), di riuscire a mappare i controlli di sicurezza delle applicazioni installate localmente nei confronti dell'infrastruttura cloud (51%) e l'utilizzo di policy efficaci e consistenti (48%).

La tecnologia di sicurezza e controllo considerata più efficiente per proteggere i dati nel cloud è la cifratura dei dati e del traffico, seguita dalle soluzioni di controllo dell'accesso (56%), monitoraggio a livello di rete (53%) e l'uso di sistemi di Intrusion prevention (44%).

Alle specifiche esigenze di sicurezza nel cloud Check Point indirizza vSEC, una soluzione di protezione dalle minacce caratterizzata da scalabilità dinamica, "intelligent provisioning" e controllo dell'accesso esteso attraverso reti fisiche e virtuali.

THE BIGGEST CYBER THREATS TO CLOUD ENVIRONMENTS



Share memory attacks 21% | Lateral movement of threats (east-west traffic) 17% | Other 6%

SECURITY CAPABILITIES TO INCREASE THE CONFIDENCE IN ADOPTING CLOUD ENVIRONMENTS



74%

VISIBILITY, REPORTING, AUDITING AND ALERTING ON SECURITY EVENTS ACROSS ALL CLOUD PLATFORMS



51%

EFFECTIVE MAPPING OF SECURITY CONTROLS FOR INTERNALLY-HOSTED APPLICATIONS TO THE CLOUD INFRASTRUCTURE



48%

CONSISTENT SECURITY POLICIES AND ENFORCEMENT ACROSS CLOUD PLATFORMS



Other 5%

TOP 5 MOST EFFECTIVE METHODS TO PROTECT DATA IN THE CLOUD



- Data leakage prevention 41%
- Firewalls / NAC 36%
- Endpoint security control 38%
- Patch management 38%
- Security information and event management (SIEM) 34%
- Anti-virus / anti-malware 28%
- Sandboxing 25%
- Content filtering 20%
- Other 7%

F5 METTE L'APPLICATION SECURITY AL CENTRO DELLA PROTEZIONE

Il 72% degli attacchi mira all'identità digitale degli utenti e alle applicazioni, ma il 90% degli investimenti in sicurezza è focalizzato sulla protezione di un perimetro che non esiste più

di Gaetano Di Blasio

La sicurezza informatica è tradizionalmente basata sulla protezione del perimetro aziendale, ma quest'ultimo non esiste più o, più precisamente, non è più definibile come un confine tra un esterno insicuro e un interno dove sistemi e dati sono al sicuro. Maurizio Desiderio, country manager di F5 Networks, lo spiega chiaramente tracciando le attività quotidiane di un information worker, che accede alla propria mail e a una serie di applicazioni, come, cita per esempio il dirigente, Office e SharePoint, Dropbox, Concur, ServiceNow, Workday, Webex. Solo alcune delle quali appartenenti alla categoria del cosiddetto "shadow IT", cioè non controllate dall'IT aziendale.

«Tutte attività che non richiedono alcun accesso al perimetro di rete aziendale», continua Desiderio, che poi aggiunge: «Viviamo in un mondo application centric», mostrando i risultati tratti da una recente ricerca svolta negli Usa, secondo la quale oltre il 54% delle aziende utilizza in media più di 201 applicativi. Il 31% conferma di adoperare anche un numero superiore alle 500 applicazioni.



Maurizio Desiderio, country manager di F5 Networks

I dati sono relativi a 406 rispondenti, estrapolati da un campione di 3000 interviste in tutto il mondo. Aldilà della rappresentatività statistica, il dato qualitativo è poco confutabile e appare coerente con altre analisi che certificano il massiccio utilizzo di strumenti "esterni" all'azienda, come i device mobili spesso usati con pratiche BYOD (Bring Your Own Device) o il cloud.

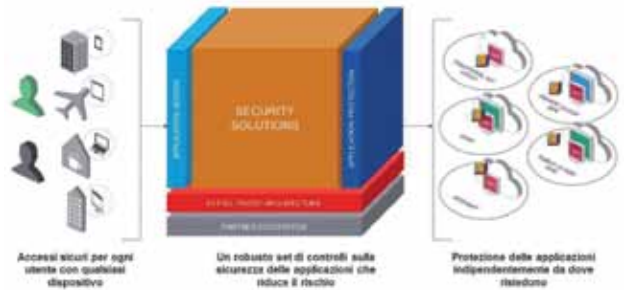
«Tutte le aziende, a prescindere dal settore merceologico, erogano servizi tramite applicativi. Le applicazioni sono il cuore dell'azienda e la rappresentano in termini di brand e reputazione sul mercato», evidenzia il manager e il pensiero non può che andare alle app protagoniste della cosiddetta digital

transformation. I processi aziendali, compresi quelli rivolti verso l'esterno, per esempio nelle relazioni con la clientela, si basano sulle applicazioni, che, quindi, «devono essere sempre disponibili, veloci e sicuri», afferma ancora il country manager di F5.

I cyber criminali, hanno da tempo compreso che non è necessario bucare un firewall o eludere un IPS (Intrusion Prevention System), ma può



Proteggere le applicazioni ovunque risiedono



Application Security integrata

essere più facile ottenere le credenziali di accesso o sfruttare vulnerabilità degli applicativi.

Secondo dati in possesso di F5 solo il 25% degli attacchi informatici è rivolto verso il tradizionale perimetro della rete aziendale, mentre ben il 72% delle minacce mirano alle identità digitali e alle applicazioni per guadagnare un "comodo" accesso. Ciononostante, il 90% degli investimenti per la sicurezza informatica è dedicato alla protezione del perimetro.

Uno squilibrio che va corretto con un cambio d'approccio, spiega Desiderio dopo aver così introdotto l'azienda: «F5 Networks è stata fondata nel 1996. Nel 2015 ha registrato un fatturato di 1,92 miliardi di dollari e annovera tra i suoi clienti aziende di fama mondiale, comprese le prime 10 telco e le prime dieci case automobilistiche».

Di fatto una specialista "storica" di Internet che oggi propone un set completo di soluzioni per la protezione, integrate in un sistema di controllo unico, ideato per fornire l'accesso sicuro di ogni utente, con ogni dispositivo, a qualsiasi applicazione, ovunque essa risieda, spiega il country manager.

Questo comprende soluzioni realizzate grazie alla collaborazione con Microsoft per Azure, come, per esempio, il servizio F5 SharePoint Online, che rende sicuro l'uso di SharePoint da mobile, poiché la directory rimane in azienda e tutto il resto è gestito nel data center di F5.

Come detto, la sicurezza proposta da F5 si concentra sulla protezione dell'identità e delle applicazioni. Per la prima è necessario poter effettuare controlli incrociati, per esempio sulla posizione dell'utente e sul tipo di dispositivo che sta utilizzando. C'è ovviamente differenza se quest'ultimo dispone o meno di un sistema biometrico o di altre funzioni per una strong authentication. Anche la "salute", cioè lo stato d'aggiornamento del dispositivo, richiede considerazioni adeguate.

Le principali funzionalità comprendono identity e access control, e SSL inspection.

Sul fronte applicativo, F5 dispone di un'ampia gamma di funzionalità, perché non è sufficiente proteggersi solo dalle vulnerabilità. Per questo il portfolio F5 comprende firewall, Web Application Firewall, sicurezza del DNS (spesso preso d'assalto con gli attacchi DDoS), Web Fraud protection.

Come s'intuisce, concentrarsi su accesso e applicazioni sembrerebbe portare a trascurare i controlli tradizionalmente legati al perimetro, come l'anti-malware, ma permette di arrivare a controllare il livello 7 della "vecchia" pila OSI. Significa anche realizzare le protezioni nel data center aziendale e anche nel cloud, quando si ha a che fare con l'hybrid cloud, ormai la condizione predominante presso le imprese.

THREAT PREVENTION, INTELLIGENCE E RESILIENZA

Dai sistemi di intrusion detection all'analisi comportamentale per rilevare le tecniche di evasione. Continua la rincorsa alle minacce con analytics e machine learning

di Gaetano Di Blasio

Agli albori di Internet, le principali minacce erano rappresentate dalle vulnerabilità che consentivano a malintenzionati di penetrare nei sistemi informatici attraverso la rete. Ben presto i firewall dimostrarono la loro inadeguatezza e nacquero i sistemi di intrusion detection, prima, e intrusion prevention dopo. La differenza tra rilevamento e prevenzione stava (e sta) tutta nel tempo di risposta, cioè nella capacità di correlare i diversi dati relativi alla sicurezza per bloccare un attacco prima che andasse a buon fine.



Oggi questo approccio è ancora utilizzato anche se i sistemi preposti al rilevamento non possono più limitarsi all'analisi del traffico, perché devono considerare più tecniche di penetrazione e non solo quelle basate su exploit in grado di sfruttare vulnerabilità. Si sono, infatti, diffuse anche tecniche di mascheramento, che consentono di bypassare buona parte dei controlli tradizionali e di annidare dei codici maligni, il cui scopo è studiare il sistema, il più "silenziosamente" possibile per preparare successivi attacchi.

È ormai frequente, inoltre, che l'attacco abbia inizio con un errore umano, dovuto alla scarsa preparazione "culturale": è il caso, per esempio, dell'ingenuo click su un link in una mail di spear phishing. Questo tipo di mail sono ormai sempre più sofisticate e scritte in un ottimo italiano ed è facile essere tratti in inganno.

Per accelerare il tempo di risposta, considerando anche che le minacce riescono a fare il giro del mondo in pochi minuti, se non secondi, sono stati sviluppati nuovi meccanismi per mantenere aggiornati i sistemi di protezione. Tali meccanismi si basano sul cloud e sulla condivisione delle cosiddette informazioni di "intelligence", che, in buona parte alimentate da soluzioni di sandboxing. Queste ultime consistono in software di analisi che verificano in una zona protetta (la scatola di sabbia) il funzionamento di un codice sconosciuto, prima di inoltrarlo all'interno del sistema informativo.

Data la rapidità con cui le tecniche e le modalità di attacco si susseguono, si è storicamente assistito

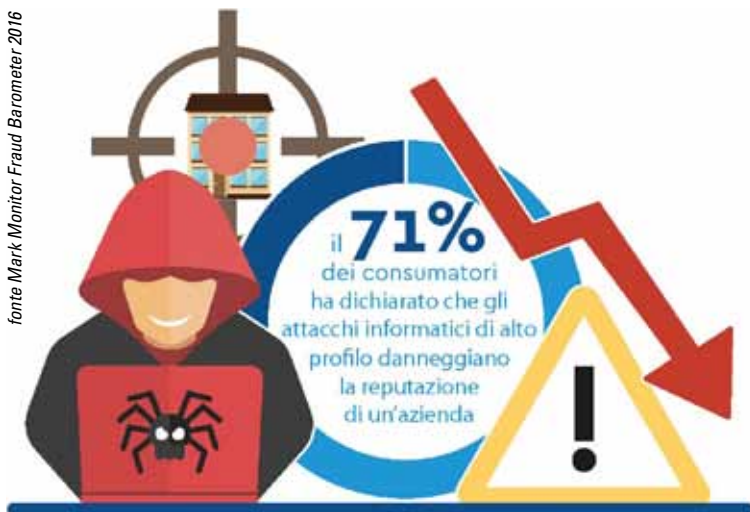
a un continuo rincorrersi tra minaccia e rimedio. L'ultima tendenza è quella di integrare le soluzioni di protezione in un unico sistema, che si potrebbe denominare Universal Threat Management o UTM 2.0, prendendo spunto dalle appliance nate una decina d'anni fa che semplicemente racchiudevano in una scatola soluzioni diverse, senza, però, condividere l'intelligenza dei vari controlli.

I sistemi integrati, oggi, devono consentire l'integrazione di tutte le soluzioni preposte a controllare traffici, codici e anomalie, in modo da avere la maggiore visibilità possibile su ciò che sta accadendo sulla rete.

Condivisione, analytics e machine learning

Per accelerare ulteriormente i controlli, in modo da reagire in tempo reale si stanno impiegando tecnologie nate in altri contesti, come la business intelligence, al fine di riuscire ad analizzare il più rapidamente possibile i miliardi di dati provenienti dai sistemi di sicurezza, anche quelli installati dall'altra parte del globo.

Attenzione: stiamo parlando di una prevenzione ancora una volta basata sulla velocità di reazione. Considerando che i mezzi economici dei cyber criminali sono superiori a quelli dei "buoni" o quandanche



si confidasse di sostenere il confronto, sarebbe comunque una sfida a chi arriva prima.

La vera sfida è ottenere una vera prevenzione, cioè essere in grado di vedere prima cosa sta per accadere. Per questo alle soluzioni di security analytics si stanno abbinando sistemi di machine learning, che possano riconoscere i prodomi di un attacco e bloccarlo prima che sia pronto.

Resilienza, governance e incident response

Finora si è illustrato il punto di vista del "soldato" che sul fronte protegge la patria, ma è tempo di capire che le minacce informatiche non costituiscono un problema tecnico, bensì un rischio economico che deve essere gestito nell'ambito della governance aziendale. Un passaggio epocale reso maturo dal ransomware.

Da Cryptoloker in poi, gli imprenditori hanno violentemente compreso che la violazione del sistema informatico ha un impatto economico diretto sull'azienda. Come ci ha recentemente evidenziato Rik Ferguson, vice President Security Research di Trend Micro, il ransomware ha avuto e avrà ancora per molto successo perché mette in relazione il cyber criminale e la vittima senza intermediari,

rendendo semplice al criminale la monetizzazione, al contrario, per esempio, di una frode economica che richiede una forma di riciclaggio del denaro.

Come si è accennato, è facile essere tratti in inganno da una mail o un altro tipo di messaggio, ancor di più se questo

ci raggiunge attraverso uno smartphone, sul quale è più "facile" cliccare su: "se non visualizzi correttamente clicca qui". Questo fatidico clic può innescare un processo drammatico. Il link apparentemente non funziona e l'utente viene rassicurato da un messaggio "riprova più tardi", ma in realtà viene scaricato un malware, che troverà la strada per passare dallo smartphone al sistema informatico (magari insieme ai file delle foto via USB o tramite un servizio cloud gratuito). Arrivato nel punto giusto, il malware comincerà a crittografare i backup, per poi passare agli storage di produzione e, infine, presenterà una



richiesta di riscatto: "paga o non recupererai più i tuoi dati".

Praticamente tutti pagano, ma solo pochi riottiranno i dati. Ecco perché, anche strutturando sistemi di threat prevention è opportuno partire dal presupposto che, prima

o poi, si sarà colpiti. Le strutture e le strategie di incident response, anche se talvolta non riescono a fare piena luce sulle origini dell'attacco, consentono di ridurre il costo della violazione ai dati, come dimostra il rapporto sui costi dei data breach pubblicato ogni anno dal Ponemon Institute.

Queste strategie, infatti, riducono drasticamente i tempi di ripristino. È il concetto di resilienza, cioè della capacità tipica in natura di molte specie di ritornare alla posizione di riposo o di stabilità. In questo caso, in quello di stabilità.

Con questo spirito e avendo compreso che la



sicurezza informatica è un fattore di business, le imprese ne stanno rivedendo i processi guidandone l'evoluzione che «si esprime in termini di: governance, per la tutela degli asset-chiave delle organizzazioni (sempre più immateriali); controllo, come monitoring del corretto disegno e dell'efficacia ed efficienza del sistema IT; Trasformazione, ovvero delle capacità di continuo aggiustamento correttivo ed evolutivo del sistema di controllo; prevenzione degli attacchi e degli incidenti, intesa come capacità di monitorare trend e comportamenti interni ed esterni alle organizzazioni allo scopo di prevenire la costituzione degli attacchi; gestione degli incidenti, come capacità tecnologiche di rilevare tempestivamente l'evento- incidente, filtrarlo rispetto a logiche di analisi in grado di scartare gli eventuali falsi positivi, innescare i processi di comunicazione, escalation e reazione, predisporre i relativi piani di rientro». Come scrivono nel focus "Dalla Sicurezza Informatica alla Protezione aziendale: nuovi modelli di prevenzione e di gestione degli incidenti" contenuto nel Rapporto Clusit 2016, Federico Santi e Danilo Benedetti, rispettivamente Security Principal e Security Solutions Architect di Hewlett Packard Enterprise.



LA PROTEZIONE DAL RAMSONWARE E OLTRE CON KASPERSKY LAB

La nuova versione di Kaspersky Small Office Security prelude allo sviluppo dell'offerta per la protezione delle Pmi e delle aziende enterprise con soluzioni avanzate

di Gaetano Di Blasio



La principale minaccia per ogni impresa, ma in particolare per quelle più piccole, è rappresentata dal ransomware, le cui campagne s'intensificano vieppiù. Una recente ricerca condotta da Kaspersky Lab ha rilevato come il 42% delle microimprese sia preoccupata dal fenomeno dei crypto-malware. Ne hanno ben donde, considerando che secondo il Kaspersky Security Network (KSN) le piccole imprese hanno subito un numero di attacchi ransomware otto volte superiore nel terzo trimestre del 2016 rispetto a quello del 2015. Più precisamente, Kaspersky Small Office Security ha individuato e fermato 27.471 tentativi di blocco all'accesso ai dati aziendali, rispetto a 3.224 attacchi simili nel medesimo periodo dell'anno precedente.

Il ransomware blocca tutte le operazioni o cripta i dati importanti per le aziende finché non viene pagato un riscatto. La perdita economica può essere significativa, anche considerando la totale mancanza di scrupoli dei cyber criminali, che non sono più i programmatori, magari un po' nerd che producono il software maligno, ma veri e propri delinquenti che affittano il malware e intendono massimizzare i guadagni.

Nell'indagine di Kaspersky Lab Corporate Security Risks 2016, oltre metà (55%) degli intervistati di piccole imprese ha dichiarato che, in seguito a un attacco, ci sono voluti diversi giorni per ripristinare l'accesso ai dati crittografati.

Il problema è che non sempre ci si riesce, anche perché il pagamento del riscatto non garantisce il recupero della chiave per decriptare i dati, come evidenzia Morten Lehn, General Manager Italy di Kaspersky Lab, che aggiunge: «Per assicurare la protezione contro ransomware e altri tipi di attacco, le imprese devono implementare soluzioni di sicurezza up-to-date affidabili come misura preventiva». I requisiti minimi di sicurezza dovrebbero includere la formazione dei dipendenti su come resistere ai tentativi di social engineering e di phishing, la creazione di backup dei dati critici e copie degli stessi, l'aggiornamento costante dei software e, infine, l'implementazione di soluzioni per la sicurezza delle piccole imprese.

Per questo Kaspersky Lab ha preparato una nuova versione del proprio software Kaspersky Small Office Security, che comprende una funzionalità anti-ransomware potenziata, una migliore protezione delle

transazioni finanziarie online e un monitoraggio dedicato dello status della sicurezza. Inoltre la funzionalità anti-ransomware inclusa nella componente System Watcher, oltre a bloccare i tentativi nocivi di cifratura, avvia anche il backup e il ripristino automatico.

Safe Money e monitoring

Tra le novità della nuova versione troviamo l'aggiornamento della funzionalità Safe Money, che protegge l'accesso all'home banking e la sua operatività. Di fatto, spiega Kaspersky, le transazioni sono protette anche dagli screenshot o dall'utilizzo della funzione appunti, su cui normalmente si basano i cyber criminali per rubare informazioni aziendali e asset finanziari. Kaspersky Small Office Security fornisce anche una semplice modalità per monitorare lo stato della sicurezza. Mediante una console di monitoraggio dedicata, basata su cloud, le aziende ottengono una visione completa del livello di protezione relativo a ciascun dispositivo interno al proprio network: server, pc notebook e qualsiasi device. Il portale online permette di accedere a queste informazioni ovunque e in qualsiasi momento, modificare le impostazioni di protezione.

Kaspersky Small Office Security è progettato per aziende con un numero di computer tra 5 e 25, ma in termini di funzionalità, afferma ancora il responsabile della filiale italiana, è una soluzione completa che consente di affrontare le problematiche cui deve rispondere anche la grande impresa. «Abbiamo investito in una nuova piattaforma per potenziare la formazione, non solo verso le aziende del canale, ma anche verso gli utenti finale», racconta Lehn,

Morten Lehn, General Manager Italy di Kaspersky Lab



precisando: «La piattaforma ci consente di creare scenari realistici e simulare gli attacchi. Sono convinto che insegnare a capire che un link è malevolo, sensibilizzare gli utenti sui rischi, risolva più dell'80% dei problemi». La piattaforma sarà anche a disposizione dei rivenditori.

Nel 2017 Kaspersky Lab festeggia vent'anni tutti dedicati alla sicurezza e con l'occasione porterà sul mercato un'importante serie di novità, spiega il general manager: «Eugene (in dizione inglese il fondatore Evginij Kaspersky) intende rimanere alla guida dell'azienda che ha fondato ancora a lungo ed è alle sue intuizioni che si devono gli sforzi in ricerca e sviluppo degli ultimi tre anni». Sforzi che hanno portato ad allargare il portfolio di soluzioni e servizi. La rinnovata soluzione per gli ambienti SCADA e, più in generale, per il mondo industrial è un esempio, cui vanno aggiunti il nuovo sistema operativo, le soluzioni per gli ambienti virtualizzati, i servizi gestiti.

Questi sono stati immessi sul mercato nell'autunno scorso e comprendono attualmente Kaspersky Endpoint Security Cloud, Kaspersky Endpoint Security for Business Basic e Kaspersky Security for virtualization. Importanti gli sforzi effettuati sulla componente d'intelligence che fornisce una protezione estesa a

un'ampia varietà di sistemi IT con novità importanti quali l'Anti Targeted Attack Platform (per gli attacchi mirati). A questo si aggiungono due soluzioni: una per la protezione da attacchi DDoS, e l'altra per la sicurezza del data center (con un motore di scansione che interagisce direttamente con i NAS) Da citare, inoltre, la rinnovata soluzione per ambienti virtuali, la prevenzione dalle frodi e la citata sicurezza per gli ambienti industriali.

HPE SECURITY ARCSIGHT: INTELLIGENCE DI SICUREZZA A MASSIMA VELOCITÀ

La famiglia di soluzioni di HPE permette di fronteggiare le esigenze di analisi dei Big Data della sicurezza e di rispondere agli APT. In arrivo ArcSight Investigate per effettuare analisi ancora più velocemente.

di Riccardo Florio

Il numero enorme di potenziali minacce e rischi ha alimentato la proliferazione delle tecnologie di protezione dando origine veri e propri Big Data correlati agli eventi di sicurezza. L'approccio basato sull'uso di applicazioni di business intelligence per estrarre informazioni utili dalla grande quantità di dati grezzi manifesta, sempre più, le proprie difficoltà nel riuscire a essere nel contempo efficace e rapido.

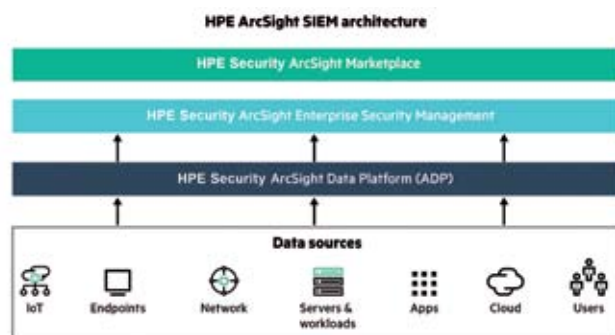
A queste esigenze si indirizza HPE Security ArcSight, una famiglia di soluzioni avanzate di System Information and Event Management (SIEM) per effettuare in tempo reale, attraverso l'intera infrastruttura enterprise, il monitoraggio, l'analisi e la correlazione di eventi di sicurezza provenienti da scansioni di vulnerabilità, analisi intelligenti delle minacce, firewall, IDS/IPS, applicazioni legacy e altre applicazioni di sicurezza. Il componente centrale e abilitante della soluzione SIEM di HPE è il motore per la gestione di minacce e rischi HPE Security ArcSight Enterprise Security Management (ESM), le cui capacità di correlazione consentono di identificare, all'interno del complesso scenario fatto da miliardi di eventi di sicurezza, le reali minacce e di definire in modo accurato e automatizzato le priorità di intervento.

Il secondo componente fondamentale è HPE Security

ArcSight Data Platform (ADP), una piattaforma che raccoglie dati di sicurezza provenienti da qualsiasi fonte (inclusi log, sensori, flussi di rete, apparati di sicurezza, Web server, applicazioni custom, social media e servizi cloud), li memorizza, effettua ricerche e produce report con prestazioni compatibili con le esigenze di gestione dei Big Data: è in grado di ricevere fino a un milione di eventi per secondo e di comprimere e archiviare fino a 480 TB di dati di log.

Difesa efficace contro gli APT

L'approccio offerto da HPE Security ArcSight si dimostra particolarmente efficace per contrastare gli attacchi APT (Advanced Persistent Threat) che sono caratterizzati da una serie di fasi di attacco in successione. Grazie all'uso di tecnologie di "stateful security



L'architettura della soluzione SIEM sviluppata da HPE

HPE Security ArcSight riconosciuta come migliore soluzione SIEM

La soluzione di HPE Security ArcSight da 13 anni di seguito viene inserita da Gartner tra i Leader all'interno del Magic Quadrant per le soluzioni SIEM e di recente ha ottenuto il premio SC Awards 2017 come migliore soluzione SIEM, da un gruppo di selezionati professionisti del settore della sicurezza, scelti dal team editoriale di SC Media. Il prestigioso riconoscimento è stato attribuito ad HPE nel corso della RSA Conference di San Francisco.

«La categoria 'Trust Award' è una delle più attese della premiazione agli SC Award - ha detto Illena Armstrong, vice presidente di SC Media - perché rappresenta la voce delle persone che stanno veramente utilizzando i prodotti e i servizi. HPE Security ArcSight ha vinto come migliore soluzione SIEM per la sua capacità di soddisfare le esigenze e di superare le aspettative dei propri clienti».

context", la soluzione di HPE è in grado di capitalizzare sulle attività di correlazione svolte in precedenza utilizzandole come input da associare ai nuovi log di eventi. Questo permette di ridurre notevolmente il carico elaborativo del motore di correlazione che non deve preoccuparsi, a ogni sospetto di attacco, di analizzare l'intero storico dei log di sicurezza, con il risultato di fornire risultati più affidabili in minor tempo. HPE Security ArcSight User Behavior Analytics, attraverso la combinazione di tecniche di machine learning e sofisticati algoritmi di rilevamento delle anomalie, fornisce un'aggiunta naturale che migliora la capacità della soluzione SIEM di HPE di individuare minacce potenzialmente sconosciute all'interno dei

registri di eventi, senza presupporre alcuna conoscenza preliminare dei dati. Altri punti di forza della soluzione proposta da HPE nella difesa contro le nuove minacce sono la possibilità di aggiungere in tempo reale dei metadati ai log di sicurezza, per migliorare l'attività di analisi e distinguere eventi provenienti da ambienti in cui l'indirizzo IP viene assegnato dinamicamente (DHCP) e in cui il medesimo IP può risultare, nel tempo, associato a differenti "host name".

HPE Security ArcSight Investigate

HPE Security ArcSight Investigate è un nuovo prodotto di indagine che andrà ad aggiungersi al portafoglio ArcSight a partire dal secondo trimestre del 2017. Questo prodotto mette a disposizione degli utenti funzioni di analisi di sicurezza di nuova generazione e costituisce un passaggio importante nel processo evolutivo della "vision" di HPE per le Intelligent Security Operations. In particolare, HPE Security ArcSight Investigate garantisce funzioni di ricerca più veloce utilizzando HPE Vertica come database incorporato in grado di elaborare enormi volumi di dati a grande velocità. HPE Security ArcSight Investigate è completamente integrato con gli altri prodotti della famiglia ArcSight e consente un'esperienza di ricerca particolarmente intuitiva grazie all'utilizzo di cruscotti personalizzabili. Prevede, inoltre, un algoritmo contestuale di sicurezza in grado di comprendere le parole chiave e suggerire query in modo dinamico, in modo tale che l'utente ha la possibilità di effettuare interrogazioni in linguaggio naturale anziché dover utilizzare un linguaggio tecnico e complesso. L'integrazione diretta con Hadoop come archivio di dati a lungo termine, consente l'accesso a una gamma completa di dati storici, per cercare e analizzare i dati di qualsiasi periodo di tempo da una singola interfaccia utente.

PROTEGGERE I SISTEMI SCADA PER NON FERMARE LA PRODUZIONE

Cloud e IoT migliorano la produzione ma espongono a dei rischi che rendono necessario investire in sicurezza. Il perchè lo spiega Paolo Emiliani di Positive Technologies

di Giuseppe Saccardi

La diffusione dell'IoT e i problemi di sicurezza recentemente segnalati mettono in guardia contro i rischi che si corrono sia per i dati inerenti le tipiche attività IT sia contro i rischi che si possono correre a livello industriale. In quest'ultimo campo un potenziale elemento critico sono i sistemi SCADA. Il termine è l'acronimo dall'inglese di "Supervisory Control And Data Acquisition" (traducibile in controllo di supervisione e acquisizione dati), e si riferisce ad un sistema informatico, dall'architettura tipicamente distribuita e con gestione centralizzata, utilizzato per il monitoraggio e controllo elettronico dei sistemi industriali.

I sistemi da un lato monitorano i sistemi fisici, inviando segnali per controllare e gestire da remoto i macchinari e tutti i processi industriali, dall'altro acquisiscono dati per tenere sotto controllo il funzionamento dei macchinari ed inviare segnali nel caso di problemi.

La svolta per quanto concerne questi sistemi di controllo industriale si è registrata con l'avvento delle applicazioni cloud prima e dell'Internet



*Paolo Emiliani -
Industrial Security
Lead Expert di Positive
Technologies*

of Things più di recente, che li stanno rendendo di più facile fruizione. Ma come in tutte le medaglie il rovescio è costituito dall'aumento dei rischi.

L'interconnessione dei sistemi SCADA, mette in guardia Paolo Emiliani, Industrial Security Lead Expert di Positive Technologies, costituisce da un lato un beneficio per tante applicazioni industriali, consentendo accessibilità maggiore, dall'altro espone le debolezze e le vulnerabilità dei sistemi, che in passato rimanevano confinate all'interno di un sicuro perimetro, a rischi molto più elevati.

«Per questo motivo è necessario affidarsi a produttori qualificati in grado di effettuare un'analisi globale della postura di sicurezza dell'intero sistema ora evoluto in eco-sistema, non limitandosi ad analizzarlo ma verificando ogni interconnessione o componente e identificandone le rispettive vulnerabilità ed il relativo impatto che queste possono avere sui processi produttivi. In gergo definito come Comprehensive threat modelling», mette in guardia Emiliani.



orario 9:00 - 20:00

Security Summit Milano - IX edizione 14-15-16 marzo 2017

ATAHOTEL EXPO FIERA - via G. Keplero, 12 - Pero (MI)

Quanto l'innovazione tecnologica può incidere sulla cultura e quanto quest'ultima può influire sull'innovazione tecnologica e ispirare anche dei principi base della sicurezza informatica?

Lo scopriremo insieme nel nuovo programma serale “parallelo” del Security Summit!

Tre serate, a partire dalle 18.00, con ospiti e iniziative per riflettere sulla connessione tra cultura, innovazione tecnologica e sicurezza informatica.
#seratesummit #CulturaAISummit

L'agenda di Security Summit Milano 2017 prevede **7 tavole rotonde**, **18 sessioni formative**, **7 seminari** e **28 atelier tecnologici**, che si svolgeranno con il contributo di **oltre 100 relatori**.

**LA PARTECIPAZIONE È GRATUITA, PREVIA REGISTRAZIONE
SUL SITO WWW.SECURITYSUMMIT.IT**

Organizzato da

