

**SPECIALE**

## LA NETWORK SECURITY OLTRE IL PERIMETRO

C'era una volta il firewall a guardia del perimetro aziendale. Oggi c'è il "next generation firewall", ma, purtroppo, c'è ancora, in molte realtà, lo stesso firewall di un tempo, magari gestito da remoto e quindi completamente dimenticato, a dare l'illusione di una protezione della rete aziendale.

**pag. 9-15**

### CYBER ATTACK

#### I CYBER CRIMINALI SFRUTTANO LA NATURA UMANA

Anche per questo 2016 è stato presentato, da Verizon, il consueto report con il quale, l'azienda, fa il punto sulla delicata questione degli attacchi informatici.

Secondo i dati riportati dal report, si evidenzia, con sempre maggiore incisività, quanto il comportamento umano del singolo utente sia una discriminante fondamentale nel rendersi più o meno vulnerabili ai cyber criminali.

**pag. 4**

### SOLUZIONI

#### DA INTESI E THALES FIRMA DIGITALE EIDAS COMPLIANT

Proteggere i dati non è più una semplice precauzione o il modo per evitare eventuali problemi legali. Per le aziende sta diventando un fattore sempre più strategico, perché la non disponibilità delle informazioni, il loro trafugamento o la loro alterazione, può portare a decisioni di business sbagliate o mettere in pericolo la sopravvivenza stessa dell'azienda.

**pag. 18**

## IN QUESTO NUMERO:

### OPINIONE

*pag. 3*

- Una sicurezza impreditoriale

### CYBER ATTACK

*pag. 4*

- I cyber criminali sfruttano la natura umana

*pag. 7*

- Malware: l'Italia è il paese più colpito d'Europa

### SPECIALE

*pag. 9*

- La network security oltre il perimetro

*pag. 13*

- Quando la rete è wireless la sicurezza è un imperativo.

### SOLUZIONI

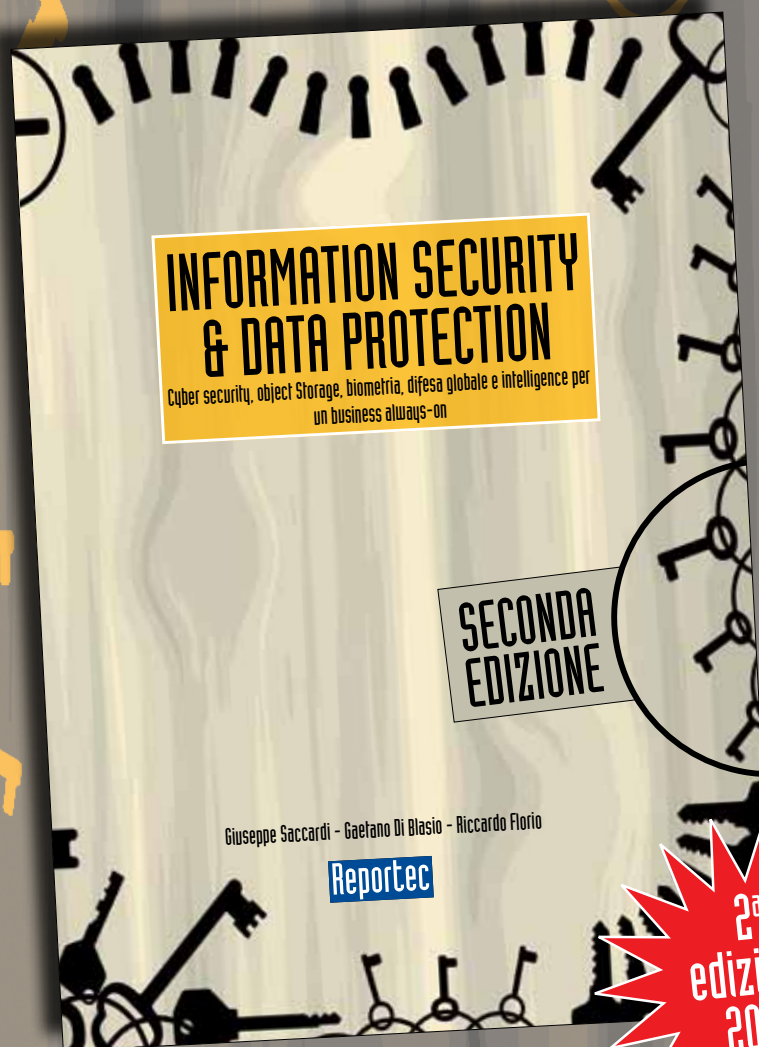
*pag. 16*

- HPE rafforza la "security analytics"

*pag. 18*

- Da Intesi e Thales firma digitale eIDAS compliant

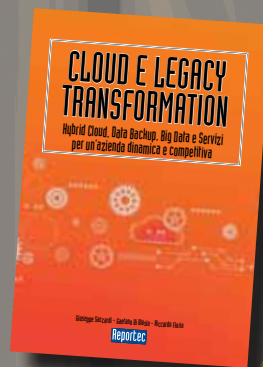
# È disponibile il nuovo libro **SICUREZZA E PROTEZIONE DEI DATI**



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**

*Il cybercrime si va trasformando in un vero e proprio settore economico. L'ultima conferma arriva dalle anticipazioni del rapporto Clusit, che a ottobre aggiunge un'analisi degli attacchi avvenuti nel primo semestre 2016.*

*Non solo è passato di moda il goliardismo degli hacker, ma questi ultimi stanno sempre più industrializzando i loro sforzi. Gli attacchi stessi sono sempre più condotti da criminali "comuni" con poche competenze tecniche che acquistano kit di attacco "chiavi in mano".*

*Il ransomware è uno degli elementi che meglio di altri rappresenta la situazione attuale della sicurezza: è semplice da inviare e ha un "ottimo" tasso di successo, poiché statisticamente è facile che qualcuno cui viene inviato un link in una mail finisca per cliccarci sopra, avviando il download del software maligno e compromettendo tutto il sistema aziendale.*

*Ricordiamo che gli esperti del Clusit prendono in esame solo gli attacchi più gravi e di dominio pubblico, cioè un sottoinsieme che rappresenta solo la punta dell'iceberg. I dati mostrano una crescita degli attacchi che passano da una media di 84 al mese nel 2015 a una di 86,3 nei primi 6 mesi del 2016. A preoccupare è soprattutto il 26% di attacchi per i quali non è stato possibile risalire alla causa della violazione. Gli attacchi riferibili al cybercrime sono saliti al 71% dal 68% del semestre precedente. Questa trasformazione, insieme al profilo degli attaccanti, cambia anche gli scenari d'attacco. È emblematico l'episodio raccontato da Andrea Zapparoli Manzoni, membro del consiglio direttivo del Clusit, il quale ha letto il dibattito su un forum underground tra i "vecchi" hacker che criticavano gli attacchi rivolti agli ospedali e i "nuovi" cybercriminali, che attaccano con il ransomware chiunque sia più facilmente disposto a pagare.*

*Per quanto riguarda le vittime degli attacchi, gli esperti del Clusit hanno osservato un calo degli attacchi rivolti verso il settore dell'hospitality: alberghi e ristoranti, presi di mira principalmente per sfruttarne il WiFi e arrivare a credenziali e carte di credito degli ospiti. Sono, invece, quasi raddoppiati gli assalti rivolti al mondo finance: con un incremento del 93,94% tra il secondo semestre 2015 e il primo semestre 2016. Stupisce gli analisti il più 9% dello spionaggio industriale, anche in considerazione del campione preso in esame. Sono stati considerati, infatti, solo gli attacchi di dominio pubblico più gravi, quindi una porzione molto bassa degli attacchi complessivi. In altre parole, è probabile che lo spionaggio stia crescendo considerevolmente.*

### **Security & Business 38 settembre 2016**

Direttore responsabile:  
Gaetano Di Blasio

In redazione:  
Riccardo Florio, Giuseppe  
Saccardi, Paola Saccardi,  
Daniela Schicchi

Grafica: Aimone Bolliger  
Immagini: dreamstime.com  
www.securitybusiness.it

Editore: Reportec srl  
Via Marco Aurelio 8  
20127 Milano  
tel. 02.36580441  
Fax 02.36580444  
www.reportec.it

Registrazione al tribunale  
n.585 del 5/11/2010

Tutti i marchi sono registrati  
e di proprietà delle relative  
società

## I CYBER CRIMINALI SFRUTTANO LA NATURA UMANA

*Presentato il Data Breach Investigations Report 2016 di Verizon, secondo il quale il comportamento degli utenti è la discriminante nella prevenzione degli attacchi informatici*

*di Daniela Schicchi*

**A**nche per questo 2016 è stato presentato, da Verizon, il consueto report con il quale, l'azienda, fa il punto sulla delicata questione degli attacchi informatici.

Secondo i dati riportati dal report, si evidenzia, con sempre maggiore incisività, quanto il comportamento umano del singolo utente sia una discriminante fondamentale nel rendersi più o meno vulnerabili ai cyber criminali.

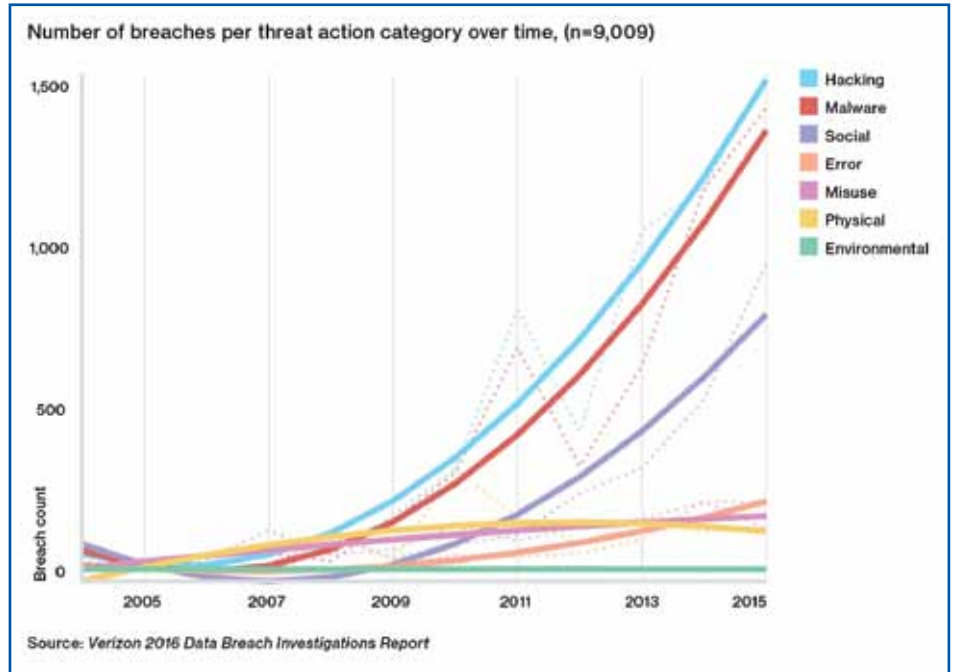
Alcuni dati sottolineano questa rilevanza in modo importante. Prima di tutto emerge il fatto che l'89% di tutti gli attacchi implica motivazioni finanziarie o di spionaggio. A seguire viene sottolineato, come la maggior parte degli attacchi sfrutti vulnerabilità conosciute, ma irrisolte. Questo nonostante le patch siano disponibili da mesi, se non addirittura anni. Infatti, le dieci vulnerabilità più conosciute riguardano l'85% degli exploit di successo. Il 63% delle violazioni di dati rilevate, inoltre, ha interessato l'utilizzo di password deboli, predefinite o sottratte. Il 95% delle violazioni e l'86% degli incidenti di sicurezza segnalati, rientrerebbe in sole nove tipologie individuate; gli attacchi ransomware sono in crescita del 16% rispetto ai dati riportati nel report del 2015 e,

infine, le difese di base sono, ancora oggi, gravemente assenti in diverse organizzazioni.

Come afferma Chris Formant, president Verizon Enterprise Solution: «Cresce l'importanza del Data Breach Investigations Report per le imprese, le forze dell'ordine e le agenzie governative, attestazione di un forte desiderio di essere sempre un passo avanti rispetto al crimine informatico», che ha aggiunto: «Oggi più che mai, la collaborazione e il contributo evidenziato nel DBIR da parte delle organizzazioni di tutto il mondo è fondamentale per comprendere appieno il panorama delle minacce. La conoscenza è il primo passo quando si affronta questo tipo di minacce».

### **Il phishing regna sovrano**

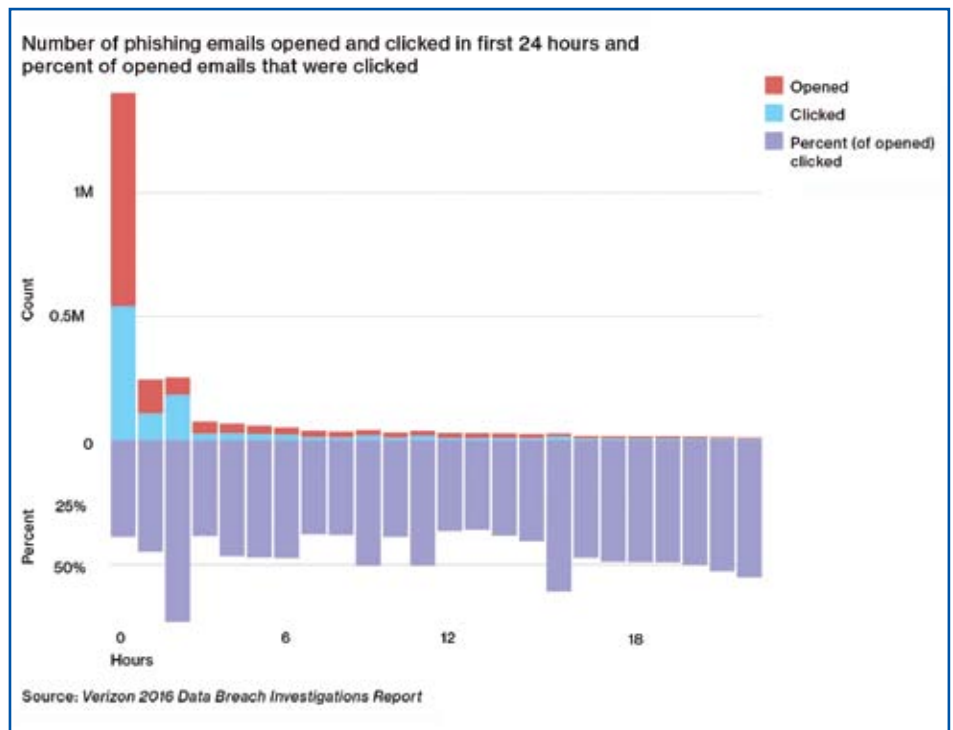
Sembra quasi impossibile, vista la grande diffusione e sensibilizzazione che le aziende che si occupano di cyber security fanno, ma il phishing resta ancora la principale forma utilizzata dai criminali informatici. È allarmante notare come nel 30% dei casi questi messaggi di phishing vengano aperti – un dato in crescita rispetto a quello registrato nel DBIR 2015 (23%) – e come il 13% di questi utenti abbia cliccato



sull'allegato malevolo o sul link dannoso, permettendo l'infiltrazione di un malware e l'accesso dei cyber-criminali.

Se negli anni precedenti, il phishing è stato un modello di attacco utilizzato esclusivamente per il cyber-spionaggio, oggi, il report, mostra come sia estremamente efficace e offra agli attaccanti una serie di vantaggi, come tempi molto stretti di compromissione del sistema e la possibilità di concentrarsi su individui e organizzazioni specifiche. La rapidità con cui viene commessa un'azione di cybercrime, infatti, rappresenta una tra le crescenti preoccupazioni dei ricercatori di Verizon. Un dato tra

tutti offre la misura delle tempistiche. Nel 93% dei casi, gli attaccanti impiegano un minuto o meno per compromettere un sistema, mentre il furto di dati si verifica in pochi minuti nel 28% dei casi.

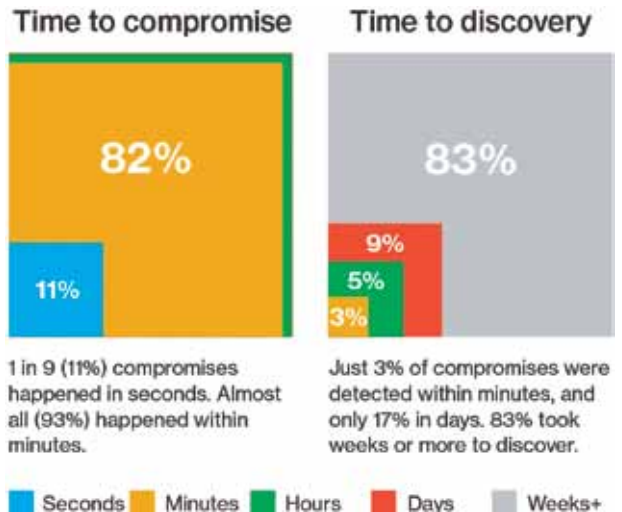


## Attacchi e mobile

Per quanto si continui a evidenziare un timore crescente per attacchi a dispositivi mobile e tablet, nel report 2015 è emerso come la compromissione di dispositivi mobili o dell'Internet of Things non rappresenti ancora un fattore significativo. Tuttavia, l'edizione 2016 del DBIR evidenzia come esistano già una serie di prototipi di exploit e che si tratta perciò solo di una questione di tempo prima che si verifichi una violazione su più larga scala che coinvolga dispositivi mobili e IoT. Ciò significa che le organizzazioni non possono abbassare la guardia e devono proteggere i propri smartphone e i vari oggetti connessi.

## In crescita l'attacco a tre fasi

Contrariamente alla stabilità degli attacchi mobile, il report 2016 ha portato alla luce come si sia diffusa, con grande regolarità, la modalità di attacco a tre fasi che comprende: l'invio di una mail di phishing che include un link a un sito web dannoso o, principalmente, un allegato malevolo; il download del malware sul PC dell'utente, punto d'accesso iniziale, mentre malware aggiuntivi possono essere utilizzati per individuare documenti segreti, sottrarre informazioni interne (spionaggio) o crittografare file a scopo di estorsione. Nella maggior parte dei casi, il malware ruba le credenziali di numerose applicazioni attraverso un key-logging e, infine, l'uso di credenziali per futuri attacchi, come l'accesso, ad esempio, a siti web di terze parti come banche o siti di e-commerce.



## Prevenire è sempre meglio che curare

Come sempre, una buona prevenzione è l'arma migliore per evitare di dover correre ai ripari successivamente. Una buona protezione, dunque, comprende alcune regole da seguire e comportamenti da tenere, che dovrebbero diventare parte integrante dell'attività di ogni utente

- 1) riconoscere quali sono i modelli di attacco più comuni nel proprio settore di appartenenza;
- 2) utilizzare l'autenticazione a due fattori per i propri sistemi. Incoraggiare gli utenti ad utilizzare l'accesso a due fasi per le applicazioni di social networking;
- 3) applicare rapidamente le patch;
- 4) monitorare tutti gli accessi: esaminare i log-in per identificare più facilmente le attività dannose;
- 5) crittografare i dati: se i dispositivi rubati sono criptati, è molto più difficile, per gli attaccanti, accedere ai dati;
- 6) formare il personale: sviluppare la consapevolezza della sicurezza all'interno della propria organizzazione è fondamentale, dato soprattutto l'incremento nel numero di attacchi di phishing;
- 7) conoscere i dati e proteggerli di conseguenza, limitando anche l'accesso.

## MALWARE: L'ITALIA È IL PAESE PIÙ COLPITO D'EUROPA

*Il Threat Index di Check Point Software Technologies mostra un calo del malware tradizionale a luglio 2016 e un aumento degli attacchi da varianti per i dispositivi mobile*

*di Gaetano Di Blasio*

L'ultimo aggiornamento del Threat Index, l'indice sulle minacce alla sicurezza informatica di Check Point Software Technologies, rileva che anche in luglio l'Italia è il paese più "infettato" d'Europa (35esimo a livello mondiale). A rendere ancora più vergognosa tale realtà è il fatto che a colpire più spesso le macchine italiane sono minacce ormai conosciute, come Conficker e Hummingbad, seguite dal "vecchio" Zeus, trojan Windows di importazione USA, che colpisce attraverso attività di phishing ed è utilizzato principalmente per rubare informazioni bancarie. Il futuro si prospetta nero, considerato che lo stesso rapporto segnala che le varianti di software malevolo attive sono diminuite del 5%, ma, rispetto a giugno, c'è una crescita pari al 50% delle varianti per dispositivi mobile, così tanto diffusi nel nostro Paese. In particolare, a luglio il numero di malware per i dispositivi mobili è arrivato a rappresentare il 9% di quelli attivi. Ben 18 le nuove variante entrate nel gruppo delle prime 200.

Conficker si conferma il codice malevolo più comunemente utilizzato, mentre, per il quarto mese consecutivo, quello più utilizzato per attaccare i dispositivi mobili è HummingBad. Più in dettaglio, a Conficker è

stato addebitato il 13% degli attacchi a livello mondiale; al secondo posto troviamo, invece, JBossjmx, imputabile del 12%, al terzo c'è Sality, che è stato usato per attaccare l'8% delle vittime. Le 10 varianti più diffuse sono la causa del 60% di tutti gli attacchi rilevati.

Piccola nota positiva: per la prima volta negli ultimi quattro mesi, gli esperti di Check Point hanno osservato un calo nel numero di famiglie di malware unici. Però il totale di software malevoli a luglio è stato il secondo più alto dall'inizio del 2016.

Mette in guardia Nathan Shuchami, Head of Threat Prevention at Check Point: «Le imprese non devono cullarsi in un falso senso di sicurezza per questo lieve calo tra le famiglie di malware attivi in luglio. Il numero delle stesse resta ancora a livelli record, mettendo in evidenza la portata delle sfide che le aziende devono affrontare per mettere in sicurezza le proprie reti contro i cyber-criminali».

Preoccupa il crescente numero di varianti che vengono prodotte dei vari malware attivi, che aumenta la gamma di minacce che le imprese devono affrontare e team di sicurezza gestire, per prevenire un attacco alle informazioni critiche di business.

## Le principali minacce

Ecco la classifica delle prime tre minacce protagoniste nel mese di luglio 2016, evidenziate da Check Point.:

- Conficker - Worm che consente operazioni da remoto, download di malware e furto di credenziali disattivando i sistemi di sicurezza di Windows Microsoft. Le macchine infettate vengono controllate da una botnet, che contatta il server Command&Control, pronta a ricevere istruzioni.
- JBossjmx - Worm che prende di mira i sistemi con una versione vulnerabile di JBoss Application Server. Il malware crea una pagina JSP malevola sui sistemi vulnerabili che esegue comandi arbitrari. Inoltre, crea un'altra Backdoor che accetta comandi da un server IRC remoto.
- Salaty - Virus che colpisce le piattaforme Windows e permette di eseguire operazioni da remoto e download di altri malware nei sistemi infetti..

## Varianti di malware per i dispositivi mobili:

- HummingBad - Malware Android che installa un rookit persistente sul dispositivo, oltre a applicazioni fraudolente e innesca altre attività malevole, come l'installazione di key logger, il furto di credenziali,

e scavalcare i sistemi di crittografia delle email utilizzati dalle aziende. Questo malware finora è riuscito a infettare 85 milioni di dispositivi mobili.

- Ztorg - Trojan che utilizza i privilegi di root per scaricare e installare applicazioni sul telefono cellulare all'insaputa dell'utente.
- XcodeGhost - A Una versione compromessa della piattaforma di sviluppo iOS Xcode. Questa versione non ufficiale di XCode è stata alterata, e inietta codice malevolo in tutte le app che sono state sviluppate e assemblate basandosi su questo servizio. Il codice iniettato invia le informazioni sull'app a un server C&C, consentendo all'app infetta di leggere la clipboard del dispositivo.

## Il Threat Index di Check Point

Il threat index di Check Point si basa sulla threat intelligence della ThreatCloud World Cyber Threat Map, che monitora come e dove si stanno svolgendo i cyber-rattacchi nel mondo in tempo reale. La Threat Map si avvale dell'intelligence ThreatCloudTM di Check Point, la più grande rete che collabora contro i cyber-criminali e fornisce dati sulle minacce e sull'andamento degli attacchi, attraverso una rete globale di sensori delle minacce. Il database di ThreatCloud contiene più di 250 milioni di indirizzi, che vengono analizzati per scoprire bot, più di 11 milioni di firme di malware e più di 5 milioni e cinquecentomila siti Web infetti, e ogni giorno individua milioni di varianti di malware.



## LA NETWORK SECURITY OLTRE IL PERIMETRO

*Un approccio alla sicurezza sempre più integrato cambia i paradigmi del best of breed e del risk management* di Gaetano Di Blasio

C'era una volta il firewall a guardia del perimetro aziendale. Oggi c'è il "next generation firewall", ma, purtroppo, c'è ancora, in molte realtà, lo stesso firewall di un tempo, magari gestito da remoto e quindi completamente dimenticato, a dare l'illusione di una protezione della rete aziendale.

I dati di mercato mostrano la massiccia presenza di firewall a protezione delle aziende italiane, ma i conti non tornano con lo stato della sicurezza nelle stesse aziende, visto che gli investimenti languono. Statisticamente questo potrebbe dipendere dal tessuto economico italiano, fatto di 3700 aziende con oltre 250 dipendenti e circa 6 milioni di partite IVA, cioè imprese che non superano i 10 dipendenti. Un buon numero di piccolissime imprese dispone di un servizio di firewalling fornito dal provider di connettività, ma nella pratica è perlopiù un dispositivo infilato in un rack o messo su uno scaffale a prendere polvere. Anche se sono pesci, probabilmente troppo piccoli, per essere bersaglio di un attacco, c'è sempre la possibilità che la loro sia violata e utilizzata come "porta di servizio" per entrare in una realtà più grande (il caso Target docet). Neanche vanno trascurati i rischi per la compliance (considerando il regolamento europeo che entro il 2018 vuole tutti conformi al GDPR). Non è detto che tutti dovranno riformare il proprio sistema di sicurezza, ma certamente le imprese medie e grandi hanno bisogno di mantenerlo aggiornato e in grado di supportare l'evoluzione del business aziendale.

Questo potrebbe non bastare, perché oggi è necessario un approccio nuovo, reso necessario dallo scenario delle minacce, ma anche dai cambiamenti che stanno rivoluzionando le architetture dei sistemi informatici nelle imprese.

### **Il crollo della torre di Babele in una civiltà che cambia**

L'evoluzione delle soluzioni e tecnologie per la sicurezza ha sempre avuto un fattore chiave costituito dalla necessità di trovare una soluzione a una nuova minaccia: sono arrivati i virus e si è creato l'antivirus, con lo spam ecco l'antispam e così via. Un meccanismo naturale, ma evidentemente inefficace, essendo sempre e comunque una rincorsa (tra l'altro ad armi impari).

La logica del best of breed, cioè dell'aggiunta continua della nuova migliore soluzione per ogni minaccia, che questo approccio ha promosso ha portato alla creazione di sistemi "mastodontici" di complessità troppo elevata e onerosi da gestire, soprattutto laddove è necessario che essi si "parlino".

I vendor della sicurezza, da qualche tempo, hanno compreso la situazione d'impasse che si è venuta a creare e hanno cercato nuovi approcci, non sempre con successo.

Una delle strade percorse è quella del Security Information Event Manager (SIEM) intelligente. In estrema sintesi, una soluzione alla Babele di dispositivi, linguaggi, protocolli e console proprietarie, sotto forma di sistema di gestione integrato, almeno a livello di policy management.

### **I next generation firewall**

Cloud, mobility, social, BYOD sono tutti esempi di come il perimetro aziendale sia ormai impalpabile, con la conseguenza che le forme tradizionali per la protezione della rete siano da superare. Più precisamente è difficile, oggi, parlare di network security immaginandola separata dal resto delle soluzioni per la protezione dei dati e del sistema informatico aziendale.

I firewall così come erano stati creati e concepiti non sono in grado di garantire la protezione oggi necessaria. Le tipologie di traffico sono aumentate e gli espedienti per evitare i controlli, le cosiddette "tecniche di evasione", richiedono capacità aggiuntive. Non basta neanche che i firewall siano abbinati ai sistemi di intrusion prevention (IPS).

È così nata una nuova classe di dispositivi, sempre più sofisticata, che integra funzionalità di controllo innovative, basate sull'analisi del comportamento/simulazione del funzionamento.

Si tratta dei next generation firewall, definiti per la prima volta dai ricercatori del Gartner nel 2009, che hanno attribuito loro le seguenti funzionalità integrate: Deep Packet Inspection, Intrusion Detection, application recognition, controllo granulare.

Le modalità con cui vengono effettuati questi controlli variano, come pure cambia, da soluzione a soluzione, la profondità d'integrazione. Nel tempo si sono aggiunte capacità di sandboxing avanzate, scalando al livello 7 della pila Osi, alla ricerca di anomalie comportamentali. Oggi si stanno applicando metodi euristici per creare sonde IPS in grado di "prevedere" un attacco.

Altri approcci puntano sul "think out of the box", rompendo gli schemi costituiti e cercando punti di vista differenti. È, per esempio, il caso della data protection, che si concentra sul dato, ritenuto l'obiettivo finale: se questo fosse sotto gli occhi di tutti, ma inutilizzabile e incomprensibile, esso perderebbe di interesse per il criminale informatico. La crittografia è certamente una valida soluzione, ma non è detto sia un ostacolo insormontabile per chi possiede capacità di calcolo a sufficienza. In ogni caso, il dato non sempre è l'unico obiettivo.

C'è chi, invece, punta il dito sull'accesso, mettendo al centro l'Identity e Access Management. Tutto utile e necessario, ma, nella sostanza, si ritorna alla logica da cui ci si voleva allontanare, aggiungendo complessità invece che eliminandole.

Il nocciolo della questione è che le diverse funzionalità sono tutte utili e a tendere tutte necessarie, considerando l'articolazione delle minacce che si fanno sempre più intelligenti. Ci sono exploit, infatti, che si adattano alle forme di difesa, cambiando tipologia d'attacco se vengono bloccati, magari attivando un altro malware in corso d'opera.

Il prossimo passo dovrà per forza essere un sistema altrettanto intelligente che non si deve limitare a riconoscere le diverse minacce e ad attivare la

protezione relativa, ma deve prevenire le violazioni, intercettando, per esempio, comportamenti anomali. Anche questa è una frontiera già aperta, che, più recentemente, ha esteso l'analisi del comportamento a tutti e 7 i livelli del protocollo OSI, ivi compreso quello applicativo, dove si cerca d'intercettare anomalie del software: cioè quel comportamento non previsto che, con ogni probabilità, significa un uso improprio dell'applicazione stessa al fine di sfruttare una qualche vulnerabilità.

I motori intelligenti, d'altro canto, potranno correlare le anomalie anche con tutti gli altri controlli previsti dall'architettura a cominciare dai dati di accesso e user identity, per capire se siano stati violati i privilegi di un utente o carpite le sue credenziali. Solo orchestrando un sistema di sicurezza perfettamente integrato e armonizzato è possibile ristrutturare la torre di Babele, creando una nuova "civiltà" di soluzioni per la sicurezza.

### **Il perimetro cancellato**

Per quanto bene orchestrato, un sistema di sicurezza deve potersi estendere al di fuori dell'infrastruttura informatica dell'azienda, non solo per le ragioni tecnologiche su esposte, ma per via del processo di cambiamento delle imprese verso la digital



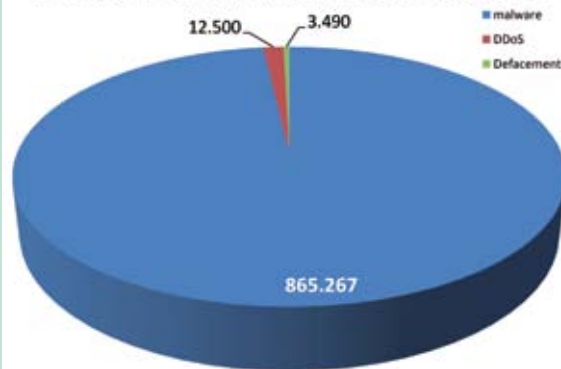
transformation e del relativo utilizzo di soluzioni in cloud che non sono sotto il controllo dell'IT aziendale. In un numero sempre più grande di imprese si sottoscrivono servizi in cloud per supportare i processi aziendali. Talvolta ciò avviene senza che ne sia informato il dipartimento ICT: sono i casi che gli analisti chiamano di "shadow IT", ma anche quando le scelte sono effettuate coinvolgendo gli IT manager, sussistono problemi di gestione e soprattutto criticità che riguardano la sicurezza.

I social sono considerati una delle "fonti d'infezione" più potenti. È sempre così: quando uno strumento diventa molto diffuso, i cyber criminali ne approfittano. Il punto è, che è facile cliccare su un link che viene proposto su una piattaforma social che si è abituati a utilizzare. Vietare l'accesso ai social network è inutile, oltre che impossibile per chi li utilizza per lavoro.

In pratica, occorre essere pronti a fronteggiare le minacce all'interno della rete, perché qualsiasi sistema potrebbe essere compromesso in ogni momento. È questo lo scopo dei sistemi integrati cui abbiamo accennato prima e che, pur in una fase in molti casi embrionale, già esistono.

La rete non costituisce più le mura che tengono all'esterno gli assalitori, ma sono, anzi sono sempre state, le strade che interconnettono le i centri vitali dell'impresa, supportandone i processi. Sono strade che vanno controllate costantemente, perché sarà sempre più facile che ci si possa trovare qualche "forestiero malintenzionato" e bisognerà essere pronti a individuarlo e bloccarlo.

Tipologia di attacchi misurati da Fastweb nel 2015



### Gli attacchi DDoS da Anonymous alla cyber war, sfruttando l'IoT

Gli attacchi Distributed Denial of Service (DDoS) sono un'importante criticità per le reti, perché, di fatto, le rendono inutili, saturando la banda.

Questo tipo di attacco è diventato famoso con le "dimostrazioni" degli hacktivisti che attaccavano i siti delle organizzazioni osteggiate. Con la crescita del cyber crime, gli obiettivi sono cambiati e gli attacchi si sono moltiplicati, allargando gli ambiti di impiego. Crescono, per esempio, gli attacchi mirati di sabotaggio. Sabotaggi che riguardano soprattutto il mondo aziendale, con episodi di concorrenza sleale, per esempio nell'ambito del gaming online e del commercio elettronico.

È anche aumentata di molto la capacità degli attacchi, fino al record registrato nel primo semestre del 2016, realizzato con un attacco DDoS che ha saputo sfruttare sistemi di videosorveglianza collegati in rete per "bombardare" il blog di un esperto di security con un traffico da 1 Tbps!

# QUANDO LA RETE È WIRELESS LA SICUREZZA È UN IMPERATIVO

*Soluzioni di ultima generazione permettono di ottenere livelli di protezione uguali a quelli delle reti cablate, andando oltre il controllo degli accessi*

*di Gaetano Di Blasio*

L'accesso WiFi è sempre più richiesto dai dipendenti aziendali, soprattutto per quelli tra loro che lavorano in mobilità e sono abituati a utilizzare dispositivi mobili collegandoli a una rete wireless. Non a caso, secondo lo studio Network Purchase Intention realizzato da ZK Research nel 2015, circa il 70% delle imprese interpellate hanno dichiarato di aver già implementato (15%) un'infrastruttura di rete "completamente" wireless o hanno espresso l'intenzione di implementarla entro il 2018. In questa indagine per completamente s'intendeva una rete wireless cui si collega più del 90% dei dispositivi client.

Esistono diversi contesti in cui il wireless è certamente una necessità, ma in tante altre situazioni è certamente una comodità. A tal proposito val la pena di ricordare che in molte aziende si pratica il cosiddetto BYOD (Bring Your Own Device) e per gli utenti che utilizzano il proprio dispositivo ovviamente mobile, il WiFi risulta essenziale.

Secondo l'indagine "Mobile Business Mobility" effettuata nel 2016 da ZK Research l'82% delle aziende supporta l'utilizzo sul posto di lavoro di dispositivi consumer (anche da 3 a 5 dispositivi per utente). Questo anche in molte realtà verticali in cui

vige una stretta regolamentazione, come il settore sanitario e i servizi finanziari. In più, è emerso che la maggior parte di tali dispositivi può essere connessa solo via wireless.

C'è poi un'ulteriore tendenza in atto che pone il wireless sotto i riflettori: si tratta dell'IoT (Internet of Things). Siamo solo agli inizi di quella che si prospetta come una vera rivoluzione. Ci sono molte imprese che stanno sviluppando progetti e applicazioni IoT. La maggior parte sono grandi imprese che hanno fatto da apripista, ma nelle medie sta crescendo e, presto, arriverà l'ondata delle piccole, cui gli operatori telco, in primis, forniranno soluzioni chiavi in mano, anche gestite.

Alle reti aziendali, dunque, saranno connessi anche numerosi dispositivi che nulla hanno a che vedere con pc, stampanti e altri dispositivi tipicamente informatici, appartenendo alla variegata categoria della operational technology. Sensori connessi alle catene di montaggio, dispositivi per il monitoraggio sanitario, sonde tra le più disparate, telecamere di videosorveglianza (migliaia di queste sono state usate per un DDoS da record) rappresentano e sempre più rappresenteranno un mondo interconnesso per la maggior parte attraverso reti wireless.



## Requisiti di sicurezza per il wireless

Ci sono, però, delle criticità da valutare, soprattutto in termini di sicurezza. È, infatti, inaccettabile che la WLAN si trasformi in un punto debole dell'infrastruttura, anche considerando che al WiFi è usuale che si colleghino anche ospiti esterni all'impresa. Sono due i requisiti basilari di un'infrastruttura wireless per reti enterprise che siano affidabili: la gestibilità e la sicurezza end to end, parte integrante dell'infrastruttura aziendale.

Bisogna riconoscere, però, che la sicurezza delle reti WLAN è sempre stata concentrata sull'accesso. Gli attuali standard di crittografia e autenticazione wireless (WPA2, 802.1X e così via) sono in buona parte riconosciuti come robusti meccanismi per il controllo degli accessi WiFi. Occorre, però, un livello di sicurezza superiore, perché l'accesso fraudolento ai sistemi è molto più sofisticato che in passato e i cyber criminali adottano tecniche che superano l'accesso diretto utilizzando come ponti email e siti Web.

Le imprese sono consapevoli dell'importanza di un'architettura sicura, come dimostra un sondaggio condotto dalla società di ricerca Lightspeed, secondo il quale nell'ultimo anno, è stato implementato un mix più equilibrato di metodi per la sicurezza: più precisamente, i sistemi per la protezione dalle intrusioni sono aumentati del 45% e del 60% sono cresciuti quelli per il riconoscimento delle applicazioni.

## I requisiti per un Cloud WiFi sicuro


Nell'era dell'IT as a Service, appena iniziata, non possono mancare soluzioni che forniscono reti

WiFi senza controller e gestite da remoto. Stanno riscontrando un interesse crescente da parte di molte aziende, perché permettono di non installare i costosi e onerosi, in termini di gestione, controller. In ambienti ad alta densità, con centinaia o migliaia di access point installati i controller sono probabilmente necessari, ma le imprese che hanno pochi punti di accesso wireless nonché quelle molto distribuite, che pure hanno pochi access point per sede, devono valutare i vantaggi offerti dalle soluzioni WiFi gestite nel cloud, che consentono ai clienti di acquistare solo gli access point, potendo fare a meno di controller o server di gestione.

I vantaggi non si fermano qui, anche considerando che queste soluzioni sono più recenti, quindi nate nell'epoca della user experience, con tutto ciò che ne consegue in termini di interfacce semplificate e maggiore gestibilità.

Un altro beneficio consiste nella flessibilità, tipica del cloud, che in questo caso, per un'azienda significa poter iniziare con un solo access point per poi crescere in base alle sopravvenute esigenze.

Tuttavia, la maggior parte delle soluzioni Cloud WiFi, deludono in termini di contenuti e sicurezza delle applicazioni. Esse, infatti, non spostano i paradigmi delle reti wireless basate su controller: semplicemente spostano questi ultimi fisicamente dall'azienda al data center del provider. Il che introduce anche problematiche, a cominciare da un potenziale point



of failure dell'infrastruttura wireless, qualora la connessione con il cloud dovesse cadere. Inoltre, anche la sicurezza è fornita nel cloud, ma i punti di accesso restano ovviamente on premise, aprendo il fronte a nuove vulnerabilità.

Affinché una soluzione Cloud WiFi possa rispondere alle esigenze di un'impresa è necessario che risponda a una serie di attributi, soprattutto se si vuole realizzare una infrastruttura completamente wireless. Il primo requisito è quello della gestibilità, certamente soddisfatto da quelle soluzioni che forniscono un sistema di management completo per il provisioning di aggiornamenti e configurazioni degli access point.

Ma i controller, che siano on premise o in cloud devono fare i conti con le minacce di ultima generazione, che impongono l'esigenza di superare le forme di controllo basilari, a beneficio di una console unica per la gestione scalabile di sicurezza e infrastruttura sull'intera rete.

Il secondo requisito riguarda il provisioning, che, essendo in cloud, non deve prevedere interventi manuali. In pratica, a beneficio delle imprese molto distribuite, deve essere possibile distribuire nuovi access point da remoto, ovunque nel mondo, senza dover ricorrere al supporto tecnico locale.

Terzo punto fondamentale è la visibilità granulare delle applicazioni. È fondamentale riconoscere il traffico che attraversa la rete e distinguere tra quello

che è sensibile ai tempi di latenza o richiede larga banda. La molteplicità di servizi che oggi usano la rete rende ancora più necessario poter gestire al meglio la QoS (Quality of Service) sulle reti wireless. Inoltre, è utile poter analizzare lo stato e l'utilizzo delle applicazioni layer 7, in modo da consentire l'impostazione di un modello gestionale predittivo. È opportuno monitorare utilizzo e consumo di banda delle applicazioni e da parte di chi. Informazioni che servono per la sicurezza e per attività di manutenzione preventiva e programmazione.

Questo vale anche per svolgere gli adeguati e sempre più sofisticati controlli di sicurezza e, a tal riguardo, è fondamentale che le configurazioni eseguite nel cloud scarichino le relative policy negli access point in tempo reale.

L'autenticazione degli utenti su specifici SSID è un altro requisito da soddisfare, affinché il personale IT possa creare profili di accesso separati per diversi gruppi all'interno dell'azienda: per esempio per definire policy diverse tra studenti, insegnanti e personale ATA in una scuola.

Un gruppo che viene tipicamente trattato a parte è quello dei "guest", per i quali occorre sia previsto un captive portal apposito. La rete WiFi dovrebbe consentire la configurazione di SSID senza limiti quantitativi.

Infine, una rete wireless non può fermarsi all'autenticazione, come avviene per la maggioranza delle Cloud WiFi, ma deve comprendere intrusion prevention e tutte le soluzioni che occorrono per mitigare la crescente ondata di minacce cyber.

## HPE RAFFORZA LA "SECURITY ANALYTICS"

*Il rilascio della versione 2.0 di HPE ArcSight Data Platform rafforza la gamma di strumenti per una sicurezza intelligente, adatta a identificare in tempo reale le minacce, evitare falsi positivi e introdurre criteri sofisticati per gestire modalità di risposta più rapide ed efficaci*

*di Riccardo Florio*

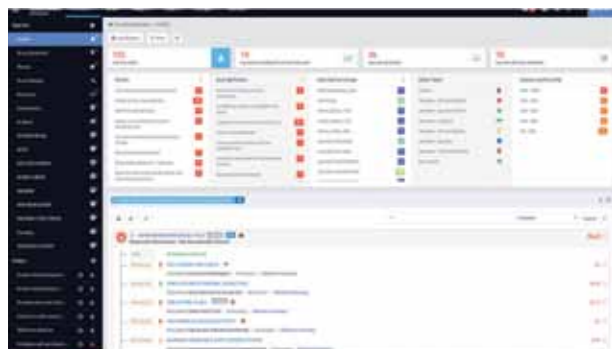
Hewlett Packard Enterprise (HPE) sta costantemente rafforzando il suo approccio verso modelli di sicurezza intelligente, per la protezione dei dati e per lo sviluppo software in base alla metodologia DevOps introducendo una serie di novità che interessano l'ambito della "security analytics". A questo tema, HPE, indirizza ArcSight, una piattaforma modulare per l'individuazione delle minacce, la gestione delle modalità di risposta e la "compliance" pensata per supportare gli analisti della sicurezza e i team che operano all'interno dei Security Operations Center (SOC) e aiutarli a rispondere nel modo più veloce possibili agli indicatori di compromissione. Grazie a sofisticate funzionalità di sicurezza intelligente basate su tecnologie di analytics, ArcSight è in grado di identificare in modo automatico possibili minacce, assegnando la corretta priorità di intervento. La tecnologia alla base di questa soluzione consente, secondo HPE, di escludere completamente i falsi positivi favorendo una risposta efficace alle minacce di nuove tipo come le Advanced Persistent Threat (APT). Inoltre, ArcSight offre il vantaggio di non richiede alcuno script o sviluppo personalizzato, né la presenza di hardware aggiuntivo

### **HPE ArcSight Data Platform 2.0**

L'ultimo annuncio di HPE all'interno della gamma di soluzioni è ArcSight Data Platform 2.0 (ADP 2.0), che si indirizza - in modo particolare - ai team che operano all'interno dei SOC per fornire loro nuovi strumenti in grado di rispondere alle sfide poste dall'enorme volume di dati generati da dispositivi di ogni tipo e che rischiano di sovraccaricare le risorse e bloccare la capacità di risposta: un'esigenza che trova conferma nello studio HPE State of Security Operations Report 2016, che evidenzia come ben l'85% dei SOC attualmente non riesca a rispettare i propri obiettivi di business.

HPE ADP 2.0, rispetto alla versione precedente, non solo incrementa del 50% la velocità di ricerca, ma mette anche a disposizione un "event broker"

### *HPE ArcSight User Behavior Analytics*



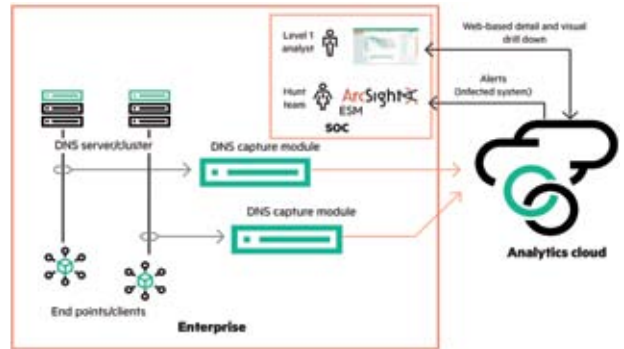
### L'architettura di HPE ArcSight DNS Malware Analytics

centralizzato in grado di ricevere 1 milione di eventi al secondo. La nuova versione della soluzione sfrutta le più avanzate tecnologie di machine learning e capacità di correlazione in tempo reale, per fornire analisi molto rapide. Inoltre, grazie alla sua architettura aperta, è in grado di connettersi in maniera trasparente alle applicazioni di terze parti, lasciando così alle aziende la flessibilità di scegliere il modo con cui memorizzare, ricercare e analizzare i propri dati di sicurezza.

### Analisi del comportamento e dell'entità con HPE UBA

Un altro tassello importante della security analytics di HPE è ArcSight User Behavior Analytics (UBA), soluzione pensata per rilevare minacce sconosciute e per aiutare le aziende a identificare la sottrazione dei dati, l'abuso di privilegi e di account e le APT. Grazie all'accoppiamento di tecniche di machine-learning e algoritmi di rilevamento delle anomalie, HPE ArcSight UBA riesce a identificare minacce sconosciute senza doversi basare unicamente su metodi di confronto con firme di minacce note o di controllo delle violazioni delle policy aziendali. Tramite il confronto tra utenti e entità, HPE ArcSight UBA può identificare le attività che si discostano da un modello di comportamento "normale", anche nel caso in cui si tratti di eventi unici o siano utilizzate credenziali legittime.

ArcSight UBA, quando viene utilizzato in combinazione con un'installazione di ArcSight SIEM, può sfruttare lo stesso personale, feed di dati e processi



di risposta agli incidenti già in atto, incrementando il livello generale di efficacia.

### HPE Security ArcSight DNS Malware Analytics (DMA)

Tramite ArcSight DNS Malware Analytics (DMA) HPE fornisce una soluzione per l'identificazione di host ed endpoint infetti (server, pc, dispositivi mobile e così via) che sfrutta una tecnologia brevettata di data analytics che interviene a livello di host e di protocollo IP per analizzare il traffico DNS e separare in tempo reale il traffico dannoso da quello legittimo.

Si tratta di una soluzione erogata in modalità "as a service" che opera con il modulo di cattura DNS che viene installato all'interno della rete e che provvede a filtrare i pacchetti DNS e inviare le segnalazioni di problemi al servizio cloud. DNS Malware Analytics permette, dunque, di disporre di un sistema automatizzato per rilevare rapidamente possibili brecche nella sicurezza e rispondere a minacce sconosciute senza sovraccaricare i sistemi SIEM con un numero eccessivo di log DNS.

ArcSight DMA si integra in modo trasparente con ArcSight ESM a cui invia segnalazioni in formato CEF; ArcSight ESM, a sua volta, consente la correlazione anche con altre fonti di dati per estendere ulteriormente l'infrastruttura di protezione.

## DA INTESI E THALES FIRMA DIGITALE EIDAS COMPLIANT

*Le due aziende hanno integrato le rispettive tecnologie e consentono ad aziende e PA di realizzare i processi digitali transfrontalieri resi possibili da eIDAS*

*di Giuseppe Saccardi*



*Fernando Catullo,  
CEO di Intesi Group*

**P**roteggere i dati non è più una semplice precauzione o il modo per evitare eventuali problemi legali. Per le aziende sta diventando un fattore sempre più strategico perché la non disponibilità delle informazioni, il loro trafugamento o la loro alterazione, può portare a decisioni di business sbagliate o mettere in pericolo la sopravvivenza stessa dell'azienda.

Quello della protezione, ha evidenziato Intesi Group, è un tema che deve considerare anche la crescente mobilità del personale aziendale che, in quanto tale, deve essere messo in condizione di intervenire in modo sicuro nei processi di business, sia che si trovi in azienda, sia che si trovi in missione in qualsiasi parte del mondo.

Il tema della protezione del dato e dei processi di business, porta quasi automaticamente al concetto di accesso sicuro o apposizione sicura di firme su documenti aziendali o di terzi.

Per risolvere i problemi che in tal senso si incontrano e anche per adeguarsi alla normativa europea eIDAS sulla firma digitale remota, Intesi e Thales hanno stretto una partnership il cui obiettivo dichiarato è di offrire, inizialmente sul mercato italiano ma stante l'esclusività del prodotto con piani di

espansione in tutta Europa, una soluzione di Firma Digitale Remota eIDAS compliant che, ha illustrato il CEO di Intesi Group Fernando Catullo, combina le tecnologie delle due società.

La soluzione è stata ideata per pubbliche amministrazioni e aziende di settori quali quello bancario, assicurativo e sanitario. In sostanza, consente di cogliere le opportunità introdotte dal Regolamento eIDAS UE 910/2014 relativamente all'attuazione di processi paperless e di digital business transfrontaliero.

### **È operativo il regolamento europeo**

Dallo scorso 1° luglio, osserva Catullo, l'entrata in vigore del Regolamento eIDAS garantisce l'interoperabilità e la certezza giuridica ai servizi fiduciari: la firma elettronica gioca in questo un ruolo importante nell'offerta di trust service e abilita la libera circolazione di documenti elettronici con valore legale in tutta la UE.

Dal punto di vista ingegneristico e funzionale le due aziende hanno integrato le loro tecnologie: PkBox di Intesi Group e gli nShield Hardware Security Modules (HSMs) di Thales.



*Peter Carlise,  
VP sales EMEA di  
Thales e-Security*

«PkBox è uno dei server di sicurezza più potenti e flessibili disponibili sul mercato per la gestione delle operazioni di firma digitale massiva, conformemente alla normativa italiana, e supporta le applicazioni che si occupano della sicurezza logica dei dati. È utilizzato per implementazioni in-house, presso i clienti, ma è anche alla base di Time4Mind, l'offerta di servizi cloud di firma remota di Intesi Group», ha illustrato Catullo.

### **Crittografia semplice e sicura**

Peraltro, per sfruttare le opportunità di mercato ed accelerare il processo di certificazione, lo scorso maggio l'ente di certificazione austriaco A-SIT ha attribuito alla più recente versione di PkBox, la 3.1, la certificazione di conformità Secure Signature Creation Device (SSCD), che ne attesta il pieno supporto di tutti i nuovi requisiti sia normativi che tecnici. La certificazione austriaca ha automaticamente validità di utilizzo estesa a tutti i Paesi membri UE.

A sua volta, sempre lo scorso maggio, gli HSM Thales nShield hanno conseguito il certificato di conformità Common Criteria per il livello di garanzia EAL4+ dall'Organismo di Certificazione della Sicurezza Informatica (OCSI).

La certificazione riconosce gli HSM Thales nShield come SSCD nonché come Qualified Signature Creation Devices (QSCDs), anche nel rispetto del Regolamento eIDAS.

«Siglare una partnership con una realtà di valore e dimensioni internazionali quale Thales conferma

come, in tema di Firma Digitale, la nostra azienda sia ormai percepita quale punto di riferimento in un Paese, l'Italia, che a sua volta riveste un ruolo guida in ambito europeo», ha commentato l'accordo Fernando Catullo, CEO di Intesi Group, «PkBox 3.1 si integra con gli HSM leader di mercato Thales nShield per proteggere e gestire le chiavi crittografiche usate per supportare l'intero processo di firma dei documenti. Il risultato è una soluzione completamente certificata e ad alte prestazioni che consente di gestire volumi molto elevati di utenze e di transazioni (quali firma digitale massiva, verifica delle firme ricevute, autenticazione o crittografia) con la massima flessibilità, affidabilità e scalabilità e con la possibilità di trasferire agli utenti un'esperienza d'uso semplice e accessibile via web e mobile».

In sostanza, gli HSM Thales nShield funzionano come root of trust per i sistemi di protezione dei dati basati su crittografia, fornendo un ambiente a prova di manomissione per generare e gestire chiavi crittografiche e di firma.

«Thales lavora insieme ai suoi clienti per aiutarli a portare avanti la trasformazione digitale in un'ampia gamma di settori. Nel momento in cui l'Italia e il resto d'Europa attraversano il processo di trasformazione digitale, Thales è lieta di collaborare con Intesi Group per offrire una soluzione di firma digitale completamente conforme a eIDAS sia a enti pubblici che ad aziende, per i quali una firma elettronica deve avere almeno la stessa validità giuridica di una firma autografa», ha spiegato Peter Carlisle, VP Sales EMEA di Thales e-Security.

## I NUOVI PROTAGONISTI DELL'INNOVAZIONE AL SERVIZIO DI IMPRESE E PROFESSIONISTI

Al centro del nuovo progetto Smau sempre più occasioni di incontro e matching con un nuovo ecosistema di attori italiani a disposizione nel soddisfare le esigenze di innovazione di imprese, professionisti e pubbliche amministrazioni locali.



### SMAU 2016 CONFERMA IL SUO RUOLO DI "MATCHING PLATFORM" PER L'INNOVAZIONE E L'AGGIORNAMENTO PROFESSIONALE

Smau è oggi la piattaforma indipendente e dinamica scelta ogni anno da oltre 50.000 imprenditori, manager di aziende e di pubbliche amministrazioni (dati Smau 2015) per crescere e aggiornarsi su temi quali **innovazione**, **tecnologia** e **digital**.

Grazie ai tanti progetti ed eventi, primo fra tutti il Roadshow, Smau è anche il partner che raccoglie gli operatori dell'ecosistema digitale e ICT, il meglio delle startup italiane, importanti Università e Business School, le Associazioni dell'Industria e del Commercio e tutte quelle realtà che stanno lavorando con passione ed energia per **rilanciare l'economia italiana** e l'**innovazione made in Italy**.

## SMAU 2016 È:



### BUSINESS MATCHING

Incontra il giusto partner e confrontati con potenziali fornitori per far decollare i tuoi progetti.



### ORIENTAMENTO ALL'INNOVAZIONE

Scopri l'innovazione di startup, incubatori e centri di ricerca e innova con loro la tua impresa.



### VALORIZZAZIONE DELLE ECCELLENZE

Conosci da vicino le imprese e le PA che hanno innovato e impara dai loro casi di successo.



### FORMAZIONE E AGGIORNAMENTO

Aggiornati con i qualificati formatori e i numerosi workshop disponibili in ogni tappa.

## LE TAPPE 2016

PADOVA  
10-11 marzo

FIRENZE  
7-8 aprile

BOLOGNA  
26-27 maggio

BERLINO  
16-17 giugno

TORINO  
30 giugno-1 luglio

MILANO  
25-26-27 ottobre

NAPOLI  
15-16 dicembre