

SPECIALE APPLICATION SECURITY

La componente applicativa è attualmente il principale vettore per gli attacchi del cyber crimine. Si tratta di un rischio difficile da contrastare, che interviene a più livelli e per il quale la consapevolezza è ancora troppo bassa. I dati in anteprima dell'osservatorio OAD offrono uno scenario del rischio. **pag. 3**



CYBER ATTACK

SCENDE IL COSTO DEL DATA BREACH

A livello globale calo 10%, meno 26% in Europa, mentre negli Usa è ancora crescita. Le normative incidono sull'impatto delle violazioni. **pag. 10**

SPECIALE

HPE PROTEGGE IL CICLO DI VITA DELLE APPLICAZIONI.

Il vendor punta su un modello di Software Security Assurance per la protezione delle applicazioni che si basa sulla costante ricerca e correzione di vulnerabilità di sicurezza abilitate dalle soluzioni Fortify **pag. 8**

IN QUESTO NUMERO:

SPECIALE

pag. 3-7

- Application Security: proteggere il nuovo perimetro aziendale

pag. 8-9

- HPE Fortify protegge l'intero ciclo di vita delle applicazioni

CYBER ATTACK

pag. 10-13

- Scende il costo del Data Breach secondo il Ponemon

SOLUZIONI

pag. 14

- Barracuda Sentinel protegge dallo spear phishing

pag. 15

- Advanced Malware Detection con i firewall di Forcepoint

pag. 17

- Wi-Fi sicuro con il nuovo Access Point di WatchGuard Watchguard

pag. 18

- Check Point propone la Cybersecurity del futuro

pag. 19

- F-Secure protegge i Mac aziendali con Little Flocker

**Tu con il tuo 5x1000
puoi ridargli la vista!**



Restituisci la vista ai bambini ciechi del Sud del mondo.

*Scrivi sulla tua dichiarazione dei redditi il codice fiscale di **CBM Italia Onlus**.*

97 299 520 151

Restituisci la vista a un bambino che, senza di te, vivrebbe per sempre nel buio della cecità.

cbmitalia.org

cbm
insieme per fare di più

APPLICATION SECURITY: PROTEGGERE IL NUOVO PERIMETRO



Le applicazioni sono il principale vettore di attacco e sempre più difficili da proteggere. I dati di OAD individuano tra i principali driver degli attacchi lo sviluppo di codice poco sicuro, una carente gestione dell'autenticazione e lo sfruttamento delle vulnerabilità delle infrastrutture ICT, del software di base e del middleware utilizzati dalle applicazioni

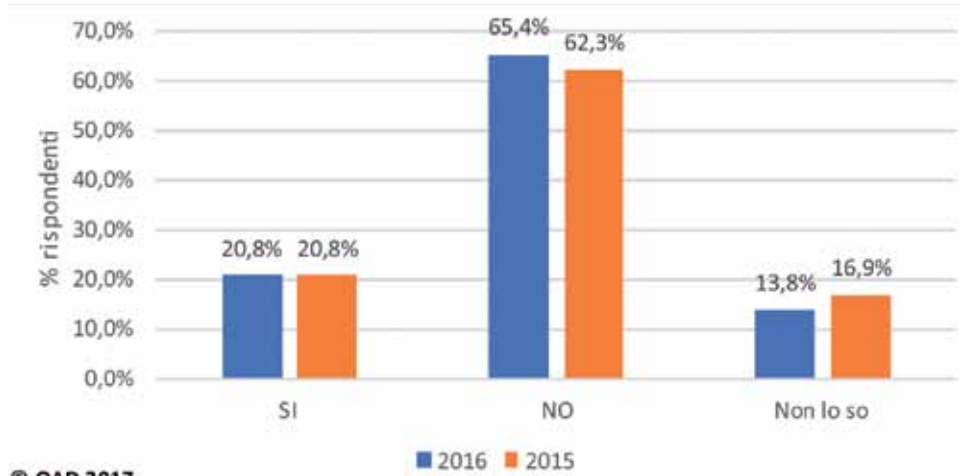
a cura di Riccardo Florio sul rapporto OAD elaborato da Marco Bozzetti

L'apertura delle applicazioni verso fornitori, clienti, utenti remoti e mobili ha dissolto il concetto di perimetro aziendale che concepivamo estendendolo a quello della portata delle applicazioni stesse.

Oggi aumentano le applicazioni che operano direttamente su Internet e il rischio che siano presenti vulnerabilità a livello applicativo è crescente per numerosità e per gravità.

Tutti i software di base e i middleware, anche i più

Attacchi agli applicativi dovuti alle vulnerabilità di tutto il software ed i sistemi sottostanti all'applicazione stessa



diffusi e autorevoli, presentano vulnerabilità, che possono divenire a loro volta vulnerabilità per gli applicativi che usano questi software o costituire punti di ingresso per accedere, in maniera non legale, alle applicazioni.

Inoltre, si deve tener presente che, mentre il sistema operativo, il software di base e il middleware sono realizzati da società di alta specializzazione (che li sottopongono a test profondi e sistematici) ed hanno una vita relativamente lunga, le applicazioni, in particolare quelle Web, possono essere implementate velocemente da tecnici meno competenti in termini di programmazione sicura.

Un rischio difficile da contrastare

Gli attacchi alle applicazioni sono tra i più critici poiché interessano il bene informativo dell'azienda che è sempre più essenziale e strategico.

Uno spaccato sullo stato degli attacchi agli applicativi viene dall'indagine online dell'Osservatorio Attacchi Digitali (OAD, vedi box) che ha interessato 173 rispondenti nel periodo compreso tra fine novembre 2016 e fine marzo 2017 appartenenti prevalentemente al settore merceologico dei servizi ICT e professionali, oltre a quello manifatturiero.

L'obiettivo della ricerca è stato di individuare alcuni specifici trend relativi agli attacchi alle applicazioni riguardanti, soprattutto, l'uso del cloud, le principali modalità di attacco e gli impatti subiti.

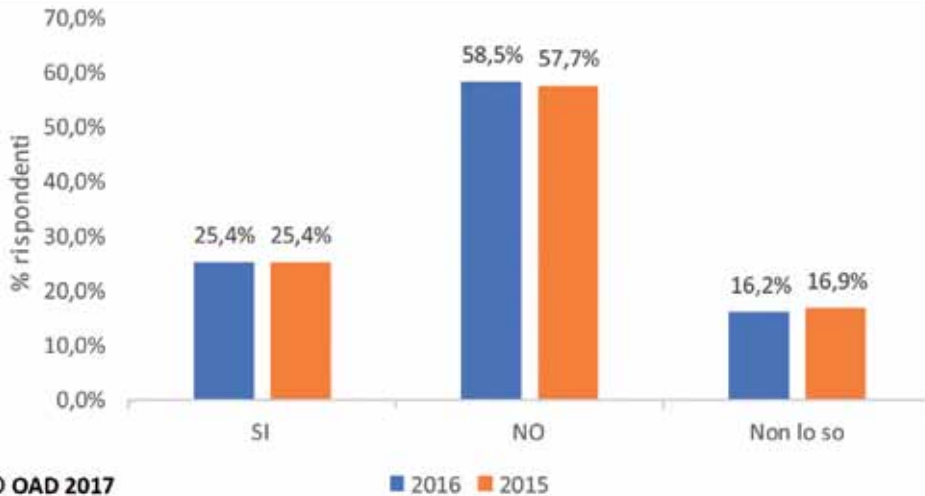
Dall'analisi emerge che, pur su un campione di aziende ed enti in gran parte dotati di buone misure di sicurezza digitale, la difesa degli applicativi è risultata difficile e complessa.

La principale causa degli attacchi agli applicativi è risultata essere legata alle vulnerabilità delle infrastrutture ICT, del software di base e del middleware usati dalle applicazioni (circa il 37%), seguita dalle vulnerabilità intrinseche all'applicativo stesso e, quindi, da quelle dei sistemi di identificazione, autenticazione e controllo degli accessi.

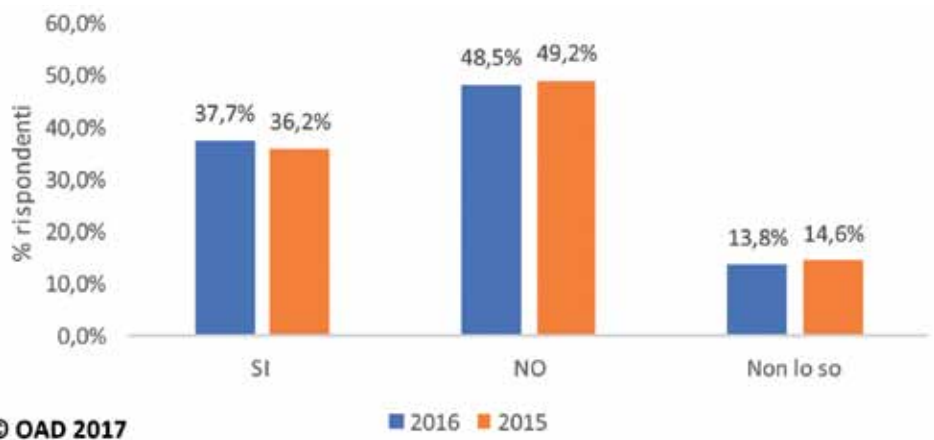
Le principali vulnerabilità applicative

Marco Bozzetti, autore del rapporto OAD, raggruppa le principali vulnerabilità applicative, responsabili della maggior parte dei problemi di sicurezza del software, nei seguenti cinque gruppi:

- programmazione del codice con errori e inadeguati controlli, che a volte sono inseriti di proposito per poter successivamente sfruttarli per effettuare degli attacchi;



Attacchi dovuti a vulnerabilità del codice applicativo



Attacchi agli applicativi dovuti a vulnerabilità dei sistemi di identificazione-autenticazione-controllo accessi

- vulnerabilità delle infrastrutture, del software di base e del middleware che sono usati dalle applicazioni, che rendono vulnerabile l'applicazione stessa;
- errata configurazione dell'applicativo, del middleware e del software di base;
- inadeguati controlli dell'identificazione, autenticazione e controllo degli accessi degli utenti e degli amministratori di sistema che possono essere, a loro volta, causati dal furto di identità digitale e dal suo utilizzo illegale;
- carenze nella crittografia e nella sua gestione.

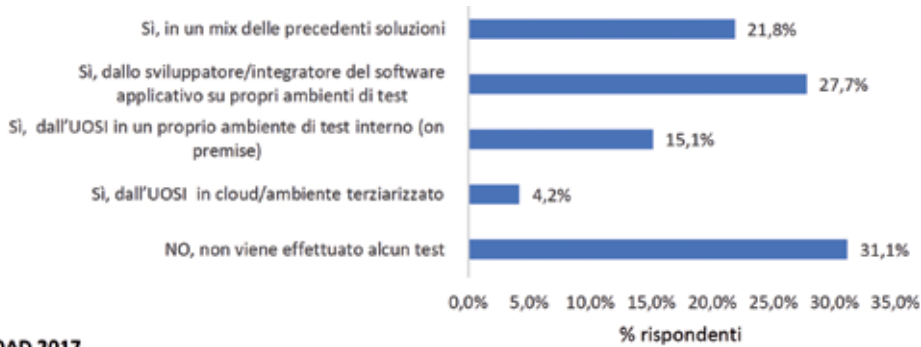
I problemi nello sviluppo del codice

Il rapporto OAD evidenzia come circa un quarto dei

rispondenti abbia subito e rilevato attacchi agli applicativi dovuti a vulnerabilità legate a un codice applicativo intrinsecamente non sicuro, tipicamente dovute a programmazione non accurata, che non tiene ben conto degli aspetti di sicurezza, che presenta banchi e così via.

La progettazione e l'implementazione di codice sicuro parte (o dovrebbe partire) dalla scelta di un linguaggio intrinsecamente sicuro nella sua impostazione. I sistemi di sviluppo integrati (IDE, Integrated Development Environment) sono molto utili per scrivere e documentare software sicuro, ma il loro utilizzo rappresenta solo il primo tassello per la produzione di software a prova di attacco.

Peraltro, nel caso di sistemi sviluppati ad hoc (per



Utilizzo di test tecnici e sulla sicurezza digitale per i programmi applicativi prima di metterli in produzione (risposte multiple)

© OAD 2017



Utilizzo di test funzionali per i programmi applicativi prima di metterli in produzione (risposte multiple)

© OAD 2017

specifiche esigenze, per semplificare il processo di autenticazione e per risparmiare sui costi (non sempre bassi dei prodotti commerciali), banchi e programmazione insicura possono essere più numerosi e più gravi, rispetto a prodotti seri e consolidati di mercato, offrendo così maggiori opportunità di attacco.

Un ulteriore successivo passo deve quindi consistere nell'effettuare test del programma applicativo non solo funzionali ma anche tecnici, per verificare la presenza di banchi nella programmazione, di vulnerabilità tecniche, e così via.

Attacchi legati ai sistemi di autenticazione

L'utente che accede a un applicativo deve essere realmente chi dichiara di essere, altrimenti l'integrità e la consistenza dell'applicativo e dei dati trattati possono essere gravemente a rischio.

Riuscire ad aggirare il sistema di identificazione e autenticazione può essere una delle principali cause

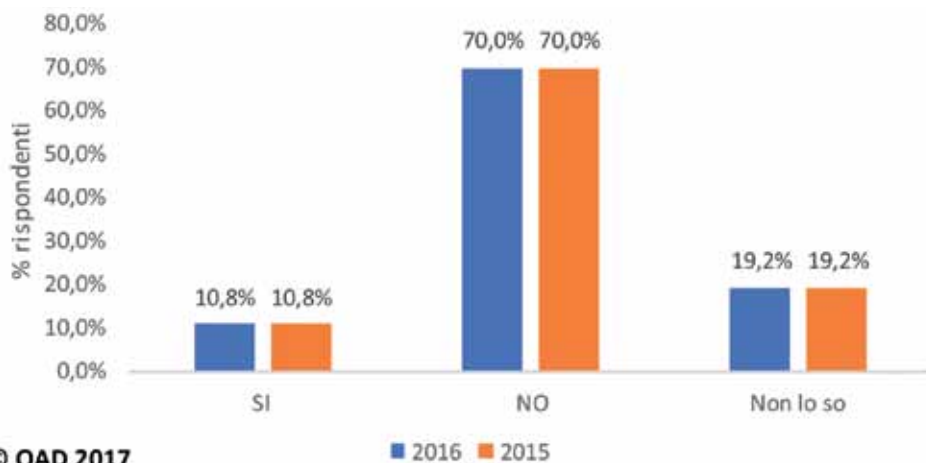
di violazione intenzionale di un applicativo.

Le vulnerabilità dei sistemi di identificazione e autenticazione possono avere diverse cause, tenendo conto che nella maggior parte dei casi sono sistemi sofisticati, complessi e con varie opzioni da scegliere e parametri da configurare.

Come per ogni altro codice software, anche per i sistemi di autenticazione e controllo dell'accesso molte vulnerabilità dipendono da banchi nel programma, da uno sviluppo non sicuro, da una cattiva configurazione nell'installazione o dall'insieme di queste cause.

Una grave e diffusa vulnerabilità è rappresentata dal comportamento degli utenti, sia utenti finali sia amministratori e operatori dei sistemi ICT.

Ulteriori criticità nel controllo degli accessi derivano da una loro inadeguata gestione: tempi lunghi per eliminare account di persone non più in azienda, account generici e non nominativi per fornitori e consulenti, password banali che fanno diretto



Attacchi causati dal furto di dati da dispositivi mobili

riferimento a nomi ed eventi legati all'utente facilmente individuabili navigando sui social network che l'utente frequenta e così via.

I rischi delle applicazioni mobile

Qualsiasi sistema di identificazione, autenticazione e di controllo degli accessi può essere violato, pur senza sfruttare sue eventuali vulnerabilità, se l'identità digitale di un utente autorizzato viene rubata o carpita.

Questa considerazione, traslata sui dispositivi mobili, porta alla considerazione che sul proprio smartphone o tablet non è inusuale tenere l'elenco dei propri account e relative password e, nella maggior parte dei casi, totalmente in chiaro.

Il 10,8% dei rispondenti all'indagine di OAD ha dichiarato di aver subito attacchi ai sistemi di controllo degli accessi a causa di identità digitali sottratte da dispositivi mobili, il 19,2% di non saperlo o di non averne prova.

Si deve poi tenere conto che i dispositivi mobili non includono solo cellulari, smartphone e tablet, ma anche chiavette USB, hard disk removibili e altri supporti rimovibili.

Inoltre i dispositivi mobili sono usati non solo dagli

utenti finali, ma anche dagli operatori e dai responsabili dei sistemi informatici che li gestiscono. Il furto delle identità digitali degli amministratori e degli operatori è ben più grave di quello di un utente finale perchè consente a un cyber criminale che ne entra in possesso di manomettere parte o l'intero sistema informatico.

L'iniziativa OAD

L'iniziativa OAD, Osservatorio Attacchi Digitali in Italia, evoluzione della precedente Iniziativa OAI, Osservatorio Attacchi Informatici in Italia, costituisce l'unica indagine on line via Web in Italia sugli attacchi informatici per tutti i settori merceologici, incluse le Pubbliche Amministrazioni Centrali e Locali, che fornisce una specifica e concreta indicazione del fenomeno degli attacchi intenzionali.

OAD è una iniziativa in collaborazione e sotto l'egida di AIPSI, Associazione Italiana Professionisti Sicurezza Informatica (www.aipsi.org) e, pur garantendo una totale autonomia ed indipendenza, è sponsorizzata da Enti ed Aziende, ed ha il Patrocinio di varie Associazioni del settore ICT.

HPE PROTEGGE L'INTERO CICLO DI VITA DELLE APPLICAZIONI

Le applicazioni sono il nuovo perimetro aziendale e occorre predisporre misure continuative per verificarne la sicurezza. Attraverso la suite Fortify, HPE fornisce una gamma di soluzioni adatte a questo scopo.

di Riccardo Florio

Prevenire significa spostare la protezione lontano dal perimetro e porla il più vicino possibile ai dati stessi. Ciò induce all'uso della crittografia a diversi livelli e a concentrarsi sul principale vettore dei cyber attacchi: le applicazioni. Se un 'insider' non è il responsabile della compromissione della sicurezza della rete, allora è probabile che l'attacco stia avvenendo tramite un'applicazione. Le applicazioni, infatti, sono progettate per essere disponibili e questo le rende intrinsecamente inclini a subire un attacco. Di fatto, le applicazioni hanno dissolto il perimetro tradizionale e introdotto nuovi tipi di rischio per le aziende. Tutti i software presentano vulnerabilità: sia quelli sviluppati ad hoc sia quelli commerciali. Le aziende sono solite effettuare test per verificare le funzionalità del software ma, nella maggior parte dei casi, non provvedono a testare anche gli aspetti tecnici e della sicurezza dell'applicativo. In altre parole, l'azienda utente si fida, in termini funzionali e tecnici di sicurezza, dei prodotti che acquisisce e, probabilmente, non ha né le competenze né il tempo per effettuare test adeguati. Il software è una "commodity" da acquisire e da utilizzare in una logica "plug and play".

Proteggere il ciclo di vita delle applicazioni

Il software è, però, una risorsa nata intrinsecamente per svilupparsi ed evolvere in modo da rispondere nel tempo ai cambiamenti del mercato, delle tecnologie, delle abitudini d'uso degli utenti, dell'integrabilità e delle funzionalità di comunicazione. La sicurezza delle applicazioni va, pertanto, vista in un'ottica di ciclo di vita del software in cui si provveda a:

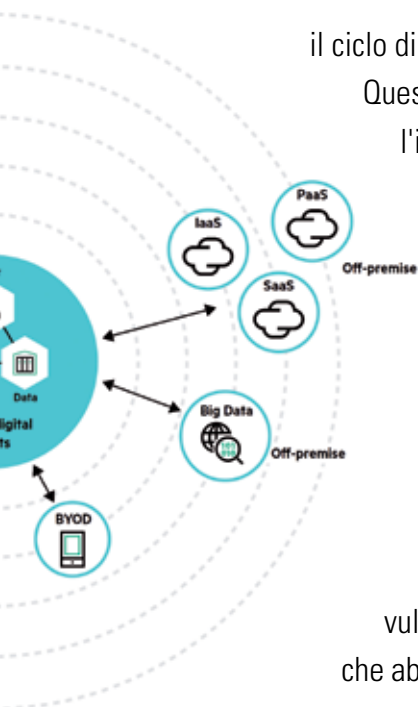
- trovare le vulnerabilità sfruttabili all'interno delle applicazioni mentre sono in esecuzione,
- estendere le operazioni di test anche alle applicazioni Web, mobili e cloud in produzione,
- effettuare una scansione continuativa alla ricerca di vulnerabilità nei sistemi operativi.

Un modello di Software Security Assurance

Per rispondere a queste esigenze HPE Security punta su un modello di Software Security Assurance ovvero su un approccio sistemico e programmatico per la protezione delle applicazioni che si basa sulla ricerca e correzione di vulnerabilità di sicurezza in tutto



L'espansione del perimetro aziendale e la nuova e più estesa superficie di attacco



il ciclo di vita di un'applicazione.

Questo approccio prevede

l'implementazione di

pratiche per la scrittura

di codice sicuro durante lo sviluppo,

l'esecuzione di test di sicurezza sca-

labili e ripetibili e l'utilizzo di monito-

raggio continuo per la scansione di possibili

vulnerabilità. Gli strumenti che abilitano questo processo

sono raggruppati all'interno della famiglia di soluzioni Fortify.

HPE Fortify è una suite completa di soluzioni di sicurezza applicativa per: effettuare test di sicurezza statici e dinamici delle applicazioni sia in modalità on-premise sia on demand; predisporre politiche di software security management; implementare tecnologie di protezione automatica delle applicazioni.

Fortify per lo sviluppo di codice sicuro

All'esigenza di garantire uno sviluppo di codice sicuro sono indirizzate le soluzioni DevInspect, WebInspect, Static Code Analyzer (on Premise) e Fortify on Demand.

DevInspect è uno strumento di codifica sicura che consente l'identificazione e la correzione di vulnerabilità di sicurezza nel codice sorgente operando dall'interno dell'ambiente di sviluppo. Fortify WebInspect è una soluzione per l'effettuazione di test automatizzati e dinamici, che identifica le

vulnerabilità di sicurezza e assegna priorità di intervento nell'esecuzione di applicazioni, imitando le tecniche di hacking e fornendo analisi dinamica di servizi e applicazioni Web.

Fortify Static Code Analyzer è un sistema automatizzato per l'analisi statica, in grado di identificare le vulnerabilità di sicurezza nel codice sorgente, effettuare correlazioni tra codice e vulnerabilità, assegnare le corrette priorità agli interventi e suggerire le best practice da adottare.

Le soluzioni per i test di sicurezza

Il secondo passaggio riguarda i test automatizzati di sicurezza dell'applicazione, sia di tipo statico sia dinamico. Fortify on Demand è lo strumento application security offerto in modalità as-a-service, che consente alle aziende di verificare la sicurezza di una specifica applicazione o di abilitare un programma di protezione completo, senza richiedere investimenti in software e personale.

Attraverso Software Security Center HPE mette a disposizione funzionalità di gestione della sicurezza di livello enterprise da un'unica interfaccia per avere visibilità completa sul programma di test per la sicurezza applicativa, la gestione delle attività di test e la definizione delle priorità di intervento.

Monitoraggio e protezione continui

La terza fase è quella di predisporre una protezione continua e un monitoraggio costante e dinamico dei cambiamenti nel rischio applicativo. A tale obiettivo rispondono Fortify on Demand e Application Defender, un servizio di auto-protezione dell'applicazione fornisce una visibilità immediata sugli attacchi e interviene immediatamente per difendere attivamente le applicazioni in produzione.

SCENDE NEL MONDO IL COSTO DEI DATA BREACH SECONDO IL PONEMON

A livello globale calo 10%, meno 26% in Europa, mentre negli Usa è ancora crescita. Le normative incidono sull'impatto delle violazioni.

di Gaetano Di Blasio

Il costo medio di una violazione alla sicurezza dei dati è, a livello globale di 141 dollari per record. Un dato in controtendenza, perché in calo rispetto ai 158 dollari del 2016.

Il periodico "2017 Cost of Data Breach Study" del Ponemon Institute, commissionato da IBM Security mostra per la prima volta una riduzione dei costi legati alle violazioni informatiche. Secondo gli analisti, le marcate differenze discendono direttamente dalle diverse normative.

Sempre secondo il rapporto, il costo medio di una violazione dei dati è di 3,62 milioni di dollari a livello mondiale, in calo del 10% rispetto ai risultati del 2016.

In Europa si il costo totale di una violazione si è ridotto del 26% e il merito sarebbe dovuto a una maggiore uniformità delle regole. Negli Usa, invece, il contesto normativo vede 48 dei 50 Stati con proprie leggi in materia di violazione dei dati. Rispondere a una moltitudine di requisiti normativi e segnalare il problema potenzialmente a milioni di consumatori può essere un compito estremamente costoso anche in termini di risorse.

In particolare, gli autori del rapporto sostengono che i vizi di conformità alle normative e "la fretta di informare" le vittime senza aver ben compreso la

portata della violazione sono tra i cinque principali motivi per cui il costo della violazione dei dati è aumentato negli Stati Uniti.

Confrontando questi fattori, gli analisti hanno dedotto che le normative negli Stati Uniti potrebbero avere per le imprese un costo per ogni record superiore rispetto a quello sostenuto dalle aziende europee. Per esempio, le mancate conformità costano negli Usa il 48% in più rispetto ai paesi europei e la "fretta di informare" pesa il 50% in più.

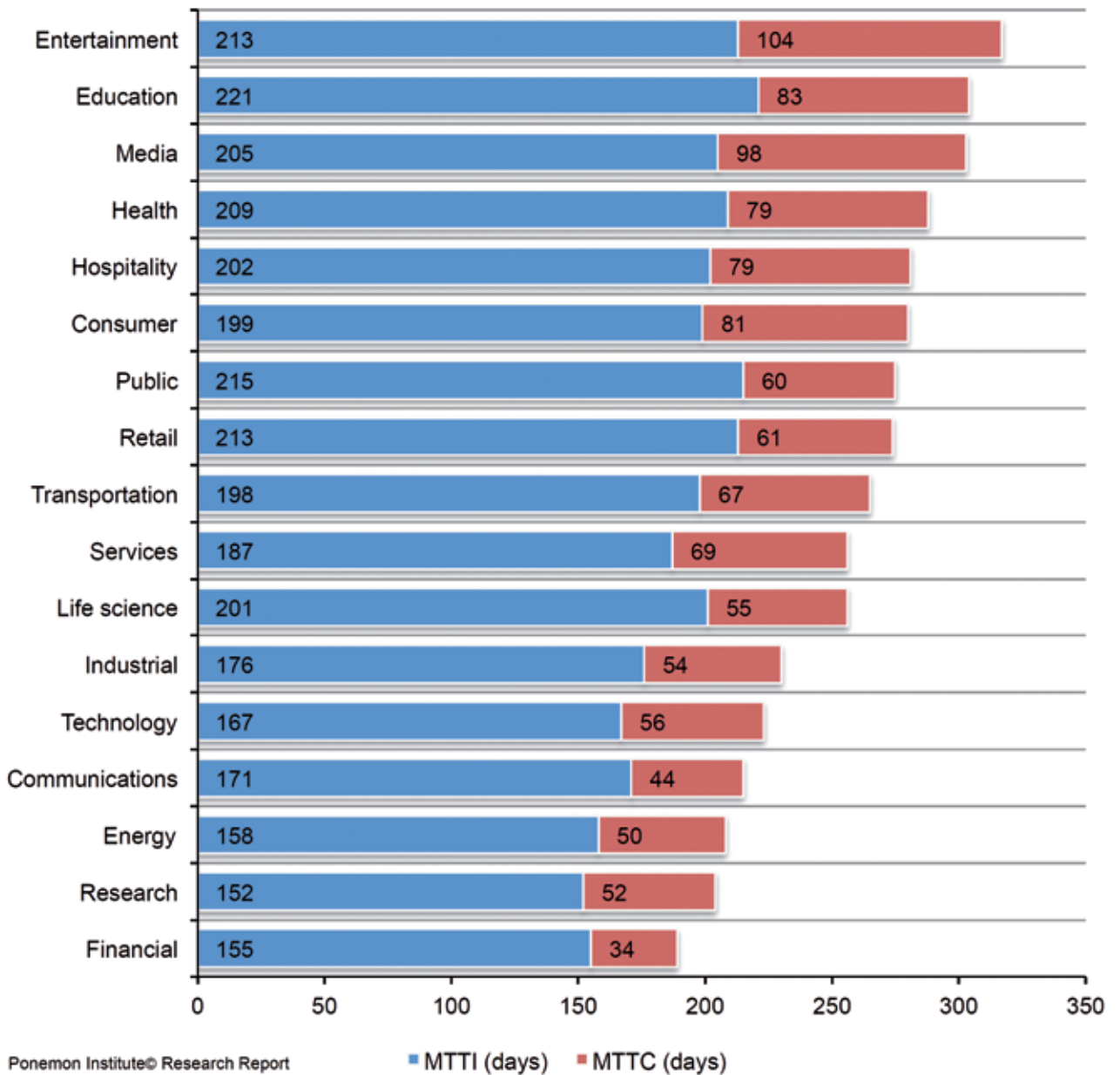
Inoltre, le società statunitensi hanno riferito di aver pagato in media oltre 690mila dollari per le spese di notifica relative a una violazione, che è più del doppio rispetto a qualsiasi altra nazione esaminata nel rapporto. Qui, però, va ricordato che in Europa non vige l'obbligo di notificare gli attacchi, se non per alcuni settori. Un obbligo che verrà introdotto dal maggio 2018, allorquando entrerà in vigore il GDPR (General Data Protection Regulation).

Non a caso Wendi Whitmore, Global Lead, IBM X-Force Incident Response & Intelligence Services (IRIS) ha affermato che «I nuovi requisiti normativi in Europa rappresentano una sfida e un'opportunità per le aziende che cercano di gestire meglio la loro risposta alle violazioni dei dati».

Whitmore ha poi aggiunto: «Oggi più che mai è

Average days to identify and contain a data breach by industry

Consolidated view (n=419)



importante identificare rapidamente ciò che è successo, a cosa l'attaccante ha accesso, e come contenere e rimuovere il loro accesso è più importante che mai. È quindi fondamentale che le organizzazioni abbiano in essere un piano completo per rispondere rapidamente ed efficacemente agli incidenti qualora si verificano».

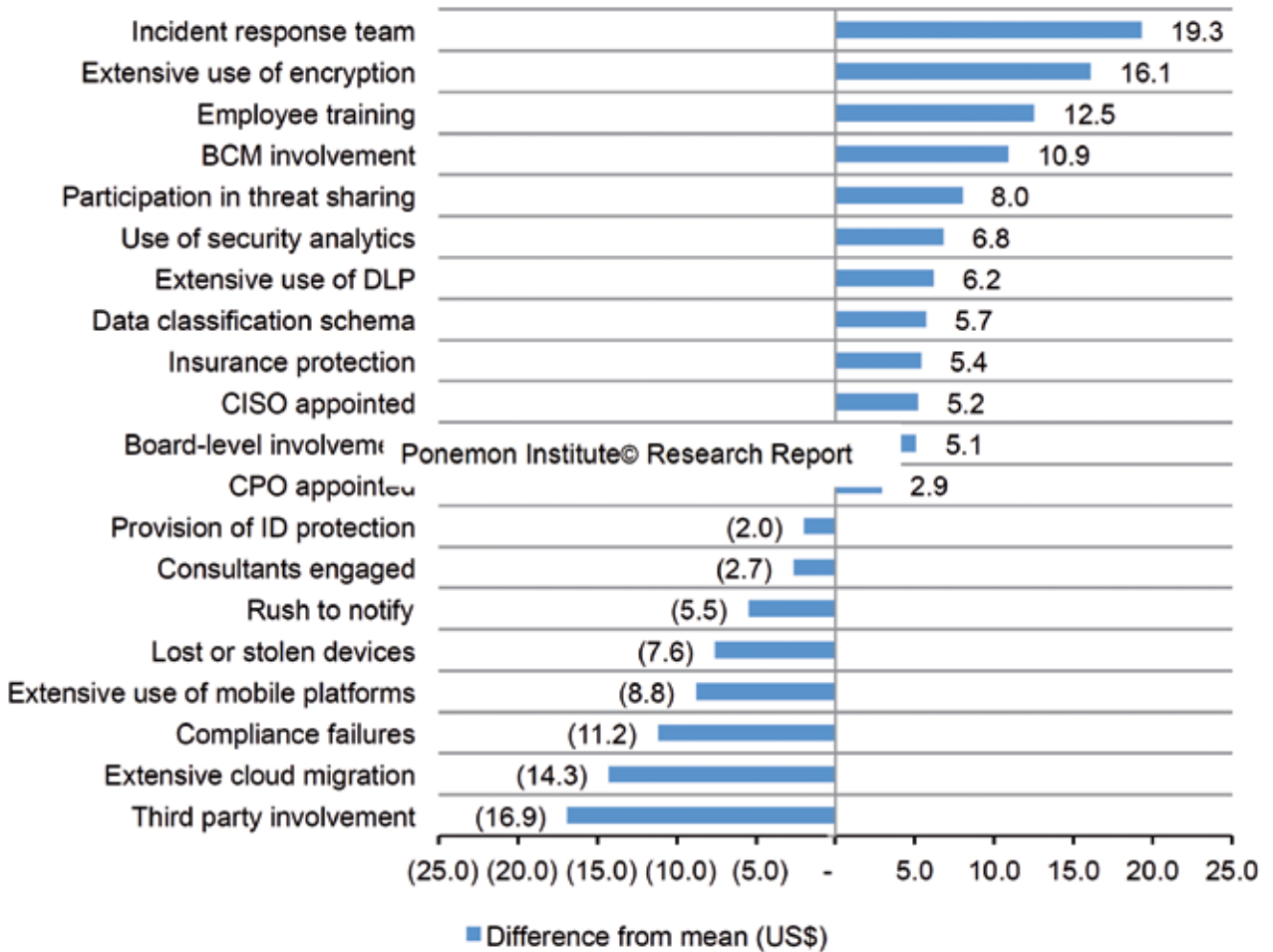
Le differenze nei costi

Nello studio globale del 2017, il costo totale di una violazione dei dati è sceso, rispetto al 2016, a 3,62 milioni di dollari (in calo del 10%) rispetto i 4 milioni di dollari dello scorso anno.

I paesi europei hanno mediamente registrato una riduzione del costo di una violazione di dati rispetto al costo medio dei quattro anni precedenti, come pure

Impact of 20 factors on the per capita cost of data breach

Measured in US\$ consolidated view (n=419)



Australia, Canada e Brasile. In paesi come Medio Oriente, Giappone, Sudafrica e India si è verificato un aumento, con il picco degli Usa in cui il costo di una violazione dei dati è stato calcolato in 7,35 milioni di dollari, in aumento del 5% rispetto al 2016. E anche hanno riportato un aumento rispetto al costo medio dei quattro anni precedenti.

Il tempo è denaro

Per il terzo anno consecutivo, emerge che avere un team di risposta a incidenti di sicurezza (IR) ha ridotto significativamente il costo di una violazione dei dati, permettendo di risparmiare più di 19 dollari

per record perso o rubato. La velocità con cui una violazione può essere identificata e arginata è in gran parte dovuta all'utilizzo di un team IR e a un piano formale di risposta agli incidenti. I team.

Secondo lo studio, la rapidità con cui un incidente di violazione dei dati può essere arginato ha un impatto diretto sulle conseguenze finanziarie. Il costo di una violazione dei dati è stato di circa 1 milione di dollari inferiore alla media per le organizzazioni che hanno potuto contenere una violazione di dati in meno di 30 giorni rispetto a quelli che ne hanno impiegato di più. La velocità di risposta sarà sempre più critica in quanto il GDPR, come ricordato,

richiederà di segnalare le violazioni dei dati entro 72 ore, con il rischio per le imprese di sostenere sanzioni fino al 4% fatturato annuo.

Secondo lo studio, le organizzazioni hanno impiegato, in media, più di sei mesi per identificare una violazione e almeno altri 66 giorni per contenere una violazione una volta scoperta.

Alcuni dati

Dal rapporto emergono alcuni dati che vale la pena evidenziare.

Le violazioni sanitarie sono le più costose: per il settimo anno consecutivo, l'Healthcare si è rivelato come il settore d'industria più costoso rispetto alle violazioni dei dati, costando queste 380 dollari per ogni record violato, più che 2,5 volte la media globale di tutti i settori (141 dollari per ogni record). Fattori principali che incidono sul maggiore costo di una violazione: Il ricorso a terze parti rappresenta il fattore principale che contribuisce ad aumentare il costo di una violazione dei dati. L'incidenza è di 17 dollari per record. Le organizzazioni devono quindi valutare la posizione di sicurezza dei loro fornitori esterni – che siano fornitori di servizi di payroll, di

cloud o di CRM - per garantire la sicurezza dei dati dei propri dipendenti e clienti.

Fattori principali che riducono il costo di una violazione: La risposta agli incidenti di sicurezza, la crittografia e una adeguata formazione del personale sono i fattori che hanno il maggior impatto sulla riduzione del costo di una violazione dei dati. Avere un team di risposta agli incidenti ha portato una riduzione del costo di 19 dollari per ogni record perso o rubato, seguito da un ampio uso della crittografia (riduzione di 16 dollari per ogni record) e la formazione dei dipendenti (riduzione di 12,50 dollari per ogni record).

Impatto positivo anche della resilienza: I programmi di business continuity riducono notevolmente i costi di una violazione dei dati. Secondo lo studio di quest'anno, il costo complessivo medio di violazione dei dati giornalieri è stimato a 5.064 dollari.

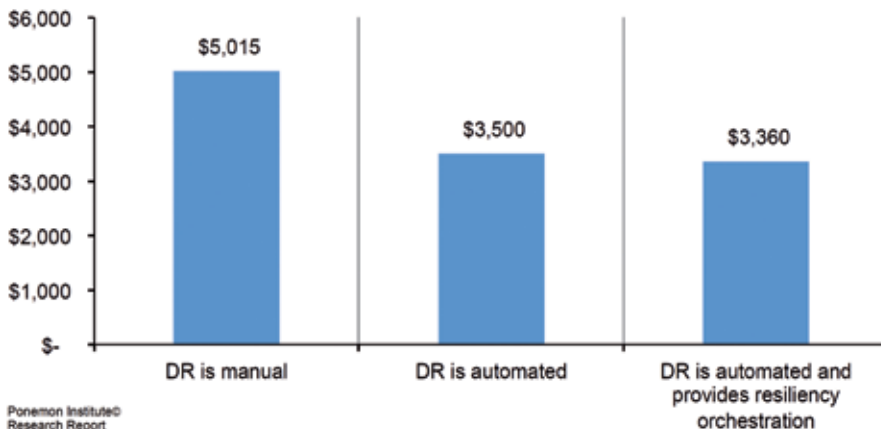
L'automazione e l'orchestrazione delle operazioni di Disaster Recovery riduce in modo significativo l'impatto del costo giornaliero di una data breach

Dal report di Ponemon emerge come le aziende che hanno un processo di disaster recovery gestito manualmente hanno registrato un costo medio stimato

di 6.101 dollari al giorno. Al contrario, le aziende che implementano un processo di disaster recovery automatizzato e che orchestrano la loro resilienza hanno registrato un costo medio molto più basso al giorno, pari a 4.041 dollari con una differenza netta del 39 per cento (o un risparmio sui costi di 1.969 dollari al giorno).

The impact of DR process on cost per day

Consolidated view (BCM Group=226)
Measured in US\$



BARRACUDA SENTINEL PROTEGGE DALLO SPEAR PHISHING

Barracuda ha rilasciato una soluzione di intelligenza artificiale che difende in tempo reale da spear phishing e cyber frodi

di Giuseppe Saccardi

Barracuda Networks, azienda attiva nella sicurezza cloud e nelle soluzioni di protezione dei dati, ha annunciato la disponibilità di Barracuda Sentinel, una soluzione di intelligenza artificiale per la difesa in tempo reale dallo spear phishing e dalle frodi online. Barracuda Sentinel è disponibile come servizio cloud e utilizza l'intelligenza artificiale per proteggere persone, aziende e brand dallo spear phishing, dai tentativi di impersonificazione, dal business email compromise e dalle cybertruffe. Secondo Osterman Research, osserva l'azienda, pur

essendo questo genere di attacchi meno comune del phishing o del ransomware, il 27% delle organizzazioni ne ha subito almeno uno negli ultimi 12 mesi. Secondo l'FBI le aziende hanno già perso 5 miliardi di dollari a causa degli attacchi BEC.

Al di là dell'impatto economico, questi attacchi possono causare danni irreparabili alla reputazione di un'organizzazione e al suo brand. Poiché gli attacchi sono altamente personalizzati – e in genere non contengono allegati o link pericolosi – sfuggono alle soluzioni di sicurezza esistenti.

Barracuda Sentinel è una soluzione fruibile in cloud

Barracuda Sentinel riunisce per contrastarli tre livelli di tecnologia basate sull'intelligenza artificiale, visibilità sulle frodi e formazione antifrode. Si connette



direttamente alla piattaforma di comunicazione, come per esempio Microsoft Office 365, e acquisisce l'accesso immediato ai dati attuali e storici per capire i modelli di comunicazione di un'organizzazione e prevenire i tentativi di impersonificazione. «Osserviamo continuamente nuove combinazioni di tattiche altamente personalizzate – imitazioni del dominio della vittima, fingersi il CEO, imbastire conversazioni convincenti con il personale. In uno scenario dinamico come quello attuale, la miglior difesa deve coinvolgere persone e tecnologia. Sentinel sfrutta l'intelligenza artificiale per offrire ai clienti – persone – un metodo completo per fermare lo spear phishing e le cyberfrodi in tempo reale», ha commentato Asaf Cidon, responsabile content security services di Barracuda.

Alla base del funzionamento di Barracuda Sentinel c'è un motore di AI multi-layer che individua e blocca gli attacchi spear phishing in tempo reale e identifica le persone a maggior rischio di attacco. Esamina le informazioni ricavate da diversi segnali per capire i modelli di comunicazione di ciascuna azienda e analizza il contenuto dei messaggi per riconoscere la presenza di informazioni sensibili. La soluzione di sicurezza è disponibile come servizio cloud senza bisogno di installare e mantenere hardware e software e, ha evidenziato l'azienda, lavora in parallelo con le soluzioni esistenti per la sicurezza delle email quali le funzioni native di Microsoft Office 365, Barracuda Essentials, e altre soluzioni di sicurezza.

ADVANCED MALWARE DETECTION CON I FIREWALL DI FORCEPOINT

Le nuove funzioni sono parte integrante della soluzione Cloud per la protezione di reti, Web, e-mail e applicazioni che collegano le persone ai dati *di Giuseppe Saccardi*

Forcepoint ha annunciato la disponibilità della nuova release software della soluzione Next Generation Firewall (NGFW), che integra il supporto per il nuovo servizio Forcepoint di Advanced Malware Detection basato su cloud.

La combinazione di Forcepoint NGFW con la

capacità di Advanced Malware Detection permette, ha spiegato l'azienda, un accesso aperto e libero a dati critici e proprietà intellettuali da ovunque, e di ridurre anche il rischio di attacchi zero-day e altre minacce emergenti.

"Il servizio di Advanced Malware Detection e il NGFW di Forcepoint lavorano in sinergia per fornire una maggiore visibilità sulle attività delle persone in rete e contemporaneamente impedire l'accesso agli attaccanti. Queste nuove funzionalità verranno attivate anche sulle nostre soluzioni di Web Security, Email Security e sulle soluzioni CASB", ha commentato Antti Reijonen, Vice President & General



*Antti Reijonen,
Vice President
& General
Manager
dell'area di
business
Network Security
di Forcepoint*

Manager dell'area di business Network Security di Forcepoint.

Una volta attivato il nuovo servizio di Advanced MalwareDetection, ha spiegato Forcepoint, migliora la tecnologia di filtraggio dei propri file NGFW in modo da permettere un'analisi più approfondita dei file trasmessi, così da identificare codici malevoli e bloccare più rapidamente eventuali aggressori che puntino a violare una rete e rubare dati critici o proprietà intellettuale.

In questa nuova versione la soluzione di sicurezza dà anche ai team di networking e sicurezza la possibilità di individuare più facilmente le tendenze che segnalano comportamenti e intenti sospetti o rischiosi dei dipendenti, in modo da poter bloccare sul nascere eventuali pratiche di cybersecurity non accettabili.

A livello di funzioni la nuova versione Forcepoint NGFW 6.2 integra il servizio di Advanced Malware Detection e comprende anche:

- Estensione dell'offerta per gli MSP - i partner possono fornire ai loro clienti la protezione delle applicazioni mission-critical tramite Forcepoint Sidewinder Security Proxy, gestito centralmente dal Managed Service Provider.
- Automatizzazione del policy change management - è possibile eliminare i processi manuali e

semplificare la conformità di auditing tramite la funzionalità di approvazione delle modifiche delle policy ora integrata nella console di gestione di Forcepoint NGFW.

- Controllo del traffico criptato - gli amministratori possono controllare in modo granulare il traffico criptato all'interno e all'esterno delle loro reti tramite funzionalità di ispezione ad alte prestazioni delle connessioni HTTPS, il controllo a livello di comando delle applicazioni SSH/SFTP e l'enforcement dinamico di determinati contesti relativi alla privacy degli utenti.
- Scalabilità - i team di operation e sicurezza possono effettuare il provisioning automatico e il controllo di centinaia o di migliaia di firewall virtuali in ambienti VMware NSX tramite il supporto di Open Security Controller (OSC).
- Miglioramenti a livello di workflow - comprendono miglioramenti di carattere generale che permettono agli addetti IT di effettuare in maniera più efficiente il deployment, analizzare e applicare le remediation su Firewall e IPS distribuiti sulla rete aziendale.
- La versione 6.2 del software Forcepoint NGFW insieme al servizio di Advance Malware Detection, ha evidenziato l'azienda, sono già disponibili per la rete globale di partner di canale Forcepoint e per i service provider.

La nuova protezione dai malware sarà inoltre integrata al Forcepoint Cloud Access Security Broker (CASB) e alle soluzioni di protezione Web e sicurezza della posta nel corso terzo trimestre 2017.

WI-FI SICURO CON IL NUOVO ACCESS POINT DI WATCHGUARD AP322

Il nuovo WatchGuard AP322 fornisce una copertura Wi-Fi veloce, sicura e affidabile anche negli ambienti esterni più critici

di Giuseppe Saccardi

WatchGuard Technologies, produttore di soluzioni di sicurezza di rete, ha annunciato il lancio del nuovo AP322, un access point (AP) cloud-ready ad elevate prestazioni per ambienti outdoor. L'apparato è caratterizzato da una robusta custodia con grado di protezione IP67 con supporto MIMO 3x3 e 802.11ac ed estende le funzionalità della soluzione WatchGuard Wi-Fi Cloud agli ambienti esterni. Ambiti di utilizzo, ha evidenziato la società, sono ad esempio stadi, scuole, locali e aree commerciali all'aperto, aree esterne degli hotel come le piscine, e similari.

In pratica, ha evidenziato WatchGuard, indipendentemente dall'ambiente fisico le organizzazioni possono disporre della scalabilità degli access point combinati con una soluzione di sicurezza basata su cloud.

"Wi-Fi Cloud fornisce il set più completo di funzionalità nella sua fascia di prezzo, inclusi una soluzione brevettata di Wireless Intrusion Prevention System (WIPS), strumenti di marketing e funzioni di analitica basate sulla posizione", ha dichiarato Ryan Orsi, Direttore delle soluzioni di Wi-Fi sicuro

in WatchGuard Technologies.

A livello trasmissivo l'AP322 prevede due bande radio simultanee a 5 GHz e 2.4 GHz, con data rate rispettivamente di fino a 1.3 Gbps e 450 Mbps. La connessione ad alta velocità abilita download veloci e prestazioni Internet più responsive.

Come accennato dispone anche di 3 flussi spaziali (MIMO 3x3), adatta per disporre di una maggiore larghezza di banda per grandi gruppi di utenti che accedono contemporaneamente al servizio. Due porte gigabit Ethernet consentono di aggiungere un ulteriore AP per un servizio esteso. Supporta anche alimentazione PoE+. Quando implementata con gli access point WatchGuard, è una soluzione che, ha osservato l'azienda, è in grado di garantire una robusta sicurezza WISP, analitiche approfondite degli accessi ospiti e dello spazio wireless, e fornisce strumenti di marketing.

È anche stata progettata per essere facile da implementare e gestire tramite Wi-Fi Cloud.



WatchGuard ap322

CHECK POINT PROPONE LA CYBERSECURITY DEL FUTURO

Check Point ha presentato Check Point Infinity, un'architettura di cybersecurity ideata per reti, cloud e mobile

di Giuseppe Saccardi

Check Point Software Technologies Ltd. ha annunciato Check Point Infinity, una nuova architettura di cybersecurity pensata per soddisfare le esigenze di sicurezza delle aziende.

È una soluzione di sicurezza consolidata per network, cloud e mobile il cui obiettivo primario è di difendere dal crescente numero di cyberattacchi.

"Check Point Infinity è l'espressione più alta della nostra vision di avere un'architettura di sicurezza che riunisce la miglior sicurezza, la migliore intelligence e la miglior gestione possibile per network, cloud e mobile. Quest'architettura è progettata per fare in modo che le organizzazioni siano pronte a gestire tutte le dinamiche della tecnologia del futuro. Il principio è molto semplice - un'architettura di sicurezza unificata che manterrà le aziende sicure

in ogni momento, con operazioni IT più efficienti ed efficaci", ha commentato Gabi Reish, VP product management di Check Point.

Tre gli elementi chiave:

- **Piattaforma di sicurezza:** permette di utilizzare piattaforme comuni, threat intelligence e infrastruttura aperta per la sicurezza di reti, cloud e mobile.
- **Threat Prevention:** la soluzione si focalizza sulla prevenzione del rischio per bloccare gli attacchi sofisticati sia noti che sconosciuti prima che questi avvengano.
- **Consolidamento:** mette a disposizione una gestione unica, policy modulari e una visibilità integrata delle minacce per gestire in maniera efficiente la sicurezza stando innanzi a un monitor.

In sostanza, ha sintetizzato l'azienda, Check Point Infinity permette di avere il controllo della loro sicurezza e di proteggere e gestire le loro operazioni IT attraverso un'unica architettura logica che mira a semplificar sia le operazioni aziendali che quelle dei clienti.

"Check Point Infinity aprirà la porta ai nostri clienti che vogliono migliorare la sicurezza delle loro aziende grazie a una nuova tecnologia dotata di un'architettura unificata che porterà threat prevention a tutte le piattaforme - reti, cloud e mobile", ha dichiarato Reish



F-SECURE PROTEGGE I MAC AZIENDALI CON LITTLE FLOCKER

Con il nome di F-Secure XFENCE, la tecnologia di Little Flocker migliora la sicurezza aziendale per macOS di F-Secure con il blocco comportamentale del malware

di Giuseppe Saccardi

L'azienda di cyber security F-Secure ha acquisito Little Flocker, una avanzata tecnologia di sicurezza disponibile per Mac. La maggior parte delle soluzioni di sicurezza per Mac, ha commentato l'azienda, si basano interamente su un approccio tradizionale basato su firme contro il malware, ma non possono proteggere gli utenti Mac da attacchi mirati.

Little Flocker protegge i dispositivi Mac usando un'avanzata analisi basata sul comportamento, e monitora le applicazioni che tentano di accedere a file confidenziali e risorse di sistema. Rileva e blocca anche il ransomware per Mac.

F-Secure integrerà il motore di sicurezza di Little Flocker nella sua nuova tecnologia XFENCE e completerà le soluzioni endpoint già esistenti di F-Secure per fornire una protezione Mac avanzata basata sul comportamento, sia per i clienti corporate che consumer.

Il problema, ha evidenziato l'azienda, è che il mito che i Mac non

richiedano protezione contro ransomware, backdoor e altre vulnerabilità del software sta svanendo. Gli attori di minacce persistenti avanzate stanno focalizzandosi sempre più sui Mac a causa della popolarità di Apple tra i dipendenti di livello senior e altri target ad alto valore.

Tramite la tecnologia di Little Flocker e implementandola nel portfolio di soluzioni per la protezione endpoint come XFENCE, F-Secure si propone in sostanza di migliorare ulteriormente le capacità di cyber security dei suoi prodotti per una rilevazione sofisticata degli attacchi zero-day, indipendentemente dalla piattaforma che i clienti scelgono.

"I Mac sono diventati un punto di ingresso invitante per gli attaccanti che cercano di penetrare nelle organizzazioni. Con la tecnologia di Little Flocker miglioreremo le funzionalità di blocco comportamentale nella nostra protezione per endpoint Mac per fermare gli avversari moderni", ha spiegato Mika

Ståhlberg, Chief Technology Officer di F-Secure.

F-Secure progetta anche di arricchire la tecnologia di Little Flocker con la sua sicurezza cloud, e implementarla in Protection Service for Business, una soluzione di sicurezza con una gestione centralizzata della sicurezza di computer, dispositivi mobili e server con gestione integrata delle patch e dei dispositivi mobili.



Mika Ståhlberg, Chief Technology Officer di F-Secure

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