

DIRECTION Reportec **78**

SOLUZIONI SERVIZI E TECNOLOGIE ICT

LA PAROLA ALL'ESPERTO

Gastone Nencini, country manager Trend Micro
Proteggersi dagli attacchi mirati

REPORT

ICT SECURITY

Con approfondimenti dedicati a:

**TREND MICRO • RETELIT • ARUBA • HP SECURITY • BT
F-SECURE • FUJITSU • SOCOMEC • VEEAM • OVERLAND**



Smau ti accompagna
nello sviluppo e nella crescita del tuo business
in qualità di partner di innovazione.



Nell'anno di **Expo 2015** Smau varca i confini nazionali per creare nuove occasioni di networking a livello internazionale supportando la crescita e lo sviluppo dell'ecosistema dell'innovazione Italiano. Attraverso il suo Roadshow Smau rappresenta il partner di riferimento a supporto della **"digital transformation" delle imprese e delle pubbliche amministrazioni** facilitando l'incontro diretto con 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 svolgono un ruolo fondamentale **per rilanciare l'economia italiana e l'innovazione made in Italy.**

Le tappe 2015:

BERLINO
12-13 marzo

PADOVA
1-2 aprile

TORINO
29-30 aprile

BOLOGNA
4-5 giugno

FIRENZE
8-9 luglio

MILANO
21-22-23 ottobre

NAPOLI
10-11 dicembre

ICT SECURITY E PROTEZIONE DEI DATI

Il difficile equilibrio tra rischio accettabile e investimento	5
Minacce in evoluzione e nuovi modelli di attacco	6
La centralità della sicurezza nella mobility aziendale	8
Sicurezza e business continuity nell'era del SDDC	12
Biometria: la protezione siamo noi	14
La sicurezza di Trend Micro per ambienti fisici, virtualizzati e cloud	16
I servizi end-to-end Retelit per un IT sicuro ed efficiente	18
Business continuity e Disaster Recovery centrali nelle soluzioni Aruba	22
La sicurezza quadrimensionale di HP Enterprise Security	24
I servizi BT per ripensare la protezione	26
La security intelligence di F-Secure	30
Fujitsu protegge data center e device	32
Più disponibilità nei data center con gli UPS di Socomec	34
Data center always-on e ripristino rapido nella mission di Veeam	37
Le soluzioni Overland Storage per backup e conservazione sicura	38

la parola all'esperto

Cambiare approccio per proteggersi dagli attacchi mirati	42
--	----

l'innocenza

Direction Reportec - anno XIII - numero 78 mensile maggio 2015 Direttore responsabile: Riccardo Florio
 In redazione: Giuseppe Saccardi, Gaetano Di Blasio, Paola Saccardi.
 Grafica: Aimone Bolliger Immagini da: Dreamstime.com Redazione: via Marco Aurelio, 8 - 20127 Milano
 Tel 0236580441 - fax 0236580444 www.reportec.it - redazione@reportec.it
 Stampa: A.G. Printing Srl, via Milano 3/5 - 20068 Peschiera Borromeo (MI) Editore: Reportec Srl, via Gian Galeazzo 2, 20136
 Milano Presidente del C.d.A.: Giuseppe Saccardi Iscrizione al tribunale di Milano n° 212 del 31 marzo 2003 Diffusione (cartaceo
 ed elettronico) 12.000 copie Tutti i diritti sono riservati; Tutti i marchi sono registrati e di proprietà delle relative società.

**COGLI L'OPPORTUNITÀ
DI RICEVERE DIRECTION
COMODAMENTE NELLA TUA
CASELLA DI POSTA
SE SCEGLI DI RICEVERE LA
TUA RIVISTA VIA E-MAIL
SCRIVI SUBITO A
servizi@reportec.it**



**Mai più copie "rubate" dal collega, ma possibilità di
rapida condivisione dei nostri esclusivi contenuti.
Sfrutta il formato elettronico per una più veloce
consultazione e creati il tuo archivio personale.
Rispetta l'ambiente e aiutaci a usare meno carta**

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

SICUREZZA E PROTEZIONE DEI DATI

Cyber security, object Storage, biometria, difesa globale e intelligence
per un business always-on

Giuseppe Saccardi - Gaetano Di Blasio - Riccardo Florio

Reportec

**edizione
2015**

In oltre 250 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.

Sono disponibili anche
CLOUD COMPUTING E IT AS A SERVICE
STORAGE



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

ICT SECURITY E PROTEZIONE DEI DATI

Per competere nel nuovo mondo digital le imprese devono investire nella sicurezza delle informazioni e nella protezione dei dati, primari asset aziendali in un'Era in cui non si vendono prodotti ma esperienze, sapendo che il cyber crimine dispone di più tempo e più risorse ed è oramai strutturato secondo i medesimi crismi di un'impresa legale. Cambiano le tipologie di attacco e il dato non viene più "rubato" in modo plateale, ma copiato restando nascosti. Pertanto, a essere compromessa è soprattutto la sua riservatezza e buona parte del danno economico per un'azienda dipende dall'utilizzo che il cybercriminale può farne. Ovviamente ridurre l'esposizione al rischio richiede dei costi e ciascuna impresa ha il compito di valutare qual sia il livello d'investimento più adeguato alle proprie esigenze e commisurarli alle quelle di protezione del proprio business.

A ostacolare questo processo contribuisce in massima parte l'incapacità da parte della classe dirigente di comprendere il costo che deriva dalla perdita di un dato o dall'interruzione di un servizio.

Il difficile equilibrio tra rischio accettabile e investimento

La totale sicurezza informatica non è un obiettivo raggiungibile, ma le aziende devono preoccuparsi di definire il valore dei loro asset per poter pianificare un'efficace gestione del rischio

L'estensione in rete dell'azienda, il successo di Internet, intranet ed extranet hanno favorito lo sviluppo di soluzioni e strumenti informatici, sia hardware sia software, che rispondono a esigenze di protezione differenti dal passato. Un mondo quindi completamente nuovo che coglie impreparate molte aziende, ma per il quale ci si può e si deve organizzare, anche perché le minacce hanno cambiato forma e obiettivi: il mondo virtuale della Rete sta diventando sempre più simile a quello reale, solo un po' più "cattivo", perché più distaccato.

Va ricordato innanzitutto che la totale sicurezza informatica non è un obiettivo raggiungibile. Innanzitutto perché anche il più sofisticato, articolato e integrato sistema di protezione deve rispondere alla teoria dei sistemi, ben nota in ingegneria, per cui il livello di sicurezza è pari a quello del suo elemento più debole. In tutte le aziende questo è rappresentato dal fattore umano.

Esistono soluzioni di più o meno recente generazione che introducono diversi automatismi con l'obiettivo di arginare il più possibile l'impatto di un errore umano, ma il più possibile non è il 100%.

Ogni nuova ricerca che indaga le cause primarie degli incidenti alla sicurezza aziendale indica l'errore umano al primo posto. Può essere un errore dovuto all'ingenuità del suo comportamento, come l'aver cliccato su una mail palesemente falsa, l'attaccare un post-it con la password

sul monitor, oppure un errore dovuto a una casualità, come l'aver spedito un file confidenziale alla persona sbagliata o, ancora, l'aver perso un dispositivo mobile su cui risiedevano dati importanti.

La stragrande maggioranza (tra l'85% e il 95%, in base alle ricerche pubblicate più di recente) dei più clamorosi incidenti verificatisi negli ultimi due anni sono dovuti a errori di questo tipo.

Peraltro, può anche trattarsi di un comportamento volutamente doloso, come nel famoso caso avvenuto in Formula 1 alcuni anni orsono, quando un dipendente della Ferrari consegnò dei progetti ai tecnici del concorrente McLaren. Per la verità, sempre secondo le molteplici analisi sui dati degli attacchi, i casi di sabotaggio o di spionaggio "cyber" sono in crescita.

Condividere le informazioni per ridurre il rischio

Un approccio concreto, dunque, mette in conto l'incidente, ma prevede anche di mitigare l'impatto dello stesso. Come detto si può ed è anzi fondamentale ridurre il più possibile l'esposizione all'attacco, renderlo cioè più difficile e, in secondo luogo, si possono attivare sistemi di protezione dinamici che contrastano l'attacco in corso per bloccarlo. Infine, è opportuno impostare sistemi di analisi forense, per comprendere fino in fondo l'accaduto ed evitare che si ripeta. A tal proposito è fondamentale intraprendere un percorso di condivisio-

ne delle informazioni relative agli incidenti di sicurezza informatica, come strettamente consigliato sia dal CERT italiano, che a fine 2013 ha annunciato il "Piano per la protezione cibernetica e la sicurezza informatica", sia dall'Enisa (European Network and Information Security Agency, l'Agenzia europea per la sicurezza delle reti e dell'informazione) e come previsto dalla Piattaforma europea su Network e Information Security (NIS).

Peraltro tutti i rapporti evidenziano che sta aumentando il divario tra le competenze tecnologiche dei cyber criminali e di chi ha il compito di proteggere la sicurezza aziendale. Un divario che appare incolmabile considerate le forze economiche in gioco: basti pensare che, secondo alcune stime del Clusit, il ROI (Return on Investment) del crimine informatico è immediato in termini di tempo e con tassi di guadagno pari al 750% settimanale!

Ormai esistono aziende che vendono malware: con le stesse logiche di una qualsiasi società che sviluppa software, tali società investono una parte dei proventi in ricerca e sviluppo, forniscono assistenza e supporto tecnico tramite call center e danno garanzie soddisfatti o rimborsati, riuscendo a essere estremamente efficienti. Anche se, per fortuna, non è così facile raggiungerle, praticamente chiunque potrebbe realizzare attacchi "semplici" ma molto remunerativi, come per esempio quelli basati sui Ransomware, cioè

software maligni che bloccano il computer della vittima (l'ultima generazione di questi malware utilizza la crittografia) costretta a pagare un "riscatto" (ransom in inglese) per vederselo sbloccare.

Assodato che la sicurezza assoluta non esiste, una corretta strategia per l'enterprise security prevede un processo ciclico che alterna: vulnerability assessment, analisi del rischio, definizione di un piano di contenimento del rischio, realizzazione di tale piano. Le tecnologie che andranno implementate sono, di volta in volta, dipendenti dalle condizioni al contorno, oltre che dalle esigenze delle specifiche imprese.

Il problema è tipicamente fare i conti con il budget a disposizione, che troppo spesso risulta insufficiente a realizzare il sistema di sicurezza idealmente definito dal piano.

Definire il livello di rischio accettabile

Il valore di un sistema di sicurezza

deve essere correlato al livello di rischio accettabile per un'impresa. Dove per rischio s'intende il danno economico che si avrebbe in caso di un attacco andato a buon fine, di un disservizio totale o parziale e così via. Il primo passo da compiere per il calcolo del ROI coincide con quello che è necessario per definire quale sistema di sicurezza implementare: effettuare un'analisi delle vulnerabilità cui è esposta l'azienda e del livello di rischio relativo.

Non si tratta di un'operazione banale, tanto che è codificata in precisi standard ISO, meglio noti con la sigla BS7799. Per effettuare tale operazione è bene affidarsi a una società indipendente, ovviamente dotata delle opportune certificazioni, poiché non di rado in questa fase si fanno vere e proprie scoperte: per esempio, applicazioni o servizi ritenuti poco importanti, se confrontati con l'impatto reale sul business, possono risultare molto più critici di quanto pensato

fino a quel momento.

Condotta con tutti i crismi, tale analisi produce una documentazione oggettiva che, ricordando che questa fase deve essere ciclicamente ripercorsa, sarà molto utile per valutazioni successive.

Per valutare il rischio correttamente, quindi correlando alle dinamiche le logiche di business, è anche necessario coinvolgere il management aziendale a vari livelli. Infatti, costretti a riflettere sulle ripercussioni di un attacco informatico, i manager svilupperanno quella sensibilità verso i temi della sicurezza che per anni è stata il cruccio degli addetti ai lavori. All'atto pratico, una soluzione di sicurezza deve raggiungere almeno uno dei seguenti obiettivi per poter dimostrare di avere un ritorno sull'investimento sostenibile: ridurre i costi correnti, ridurre i costi futuri, ridurre il rischio finanziario, aumentare la produttività, aumentare il fatturato. *



Minacce in evoluzione e nuovi modelli di attacco

Gli attacchi e le vulnerabilità non solo crescono in numero ma diventano più sofisticati, sfuggenti, diversificati e quindi efficaci, riuscendo a sfruttare in modo integrato ogni tipo di debolezza umana o tecnologica

Il Web è diventato il terreno di incontro tra tutti gli abitanti del pianeta che hanno la possibilità di collegarsi in Rete attraverso un computer o altri dispositivi che lo permettono. Nel Web è possibile informarsi (Wiki), socializzare (social networking), scambiare file (P2P networking), creare pagine di opinioni personali (blog) e così via. Il Web è diventato un mondo senza confini e aperto a chiunque voglia parteciparvi per portare il proprio contributo.

Purtroppo proprio questa apertura totale lo rende un'attrattiva interessante per chi ha ben altri scopi, non del tutto leciti, come i cybercriminali intenzionati a compiere frodi a danno degli utenti, spesso inconsapevoli dei pericoli che corrono.

Uno dei rischi maggiori consiste nel diventare il mezzo di trasmissione di un malware, condividendo un contenuto o un link diretto che porta a scaricare un codice maligno.

I social network tra i principali vettori di attacco

Uno tra i più labili confini per le aziende è rappresentato dai social network. Sono utilizzati da moltissime imprese, soprattutto quelle che si rivolgono al consumatore finale e, soprattutto, sono "visuti" da molti dipendenti. Peccato i social network siano anche tra i più semplici e quindi più utilizzati vettori di attacco per la diffusione di malware e per le frodi basate sul social engineering, come sottolineano gli esperti del Clusit.

In particolare, i siti che sono già stati utilizzati per scopi malevoli, e sempre più lo saranno, sono i più diffusi: Facebook, LinkedIn e Twitter. Lo saranno, in particolare, attraverso i dispositivi mobili, utilizzati con eccessiva confidenza e "fiducia" per accedere quotidianamente ai social media e, grazie al fenomeno del Bring Your Own Device, per collegarsi alla rete aziendale. Cliccare su un link condiviso da qualcuno che probabilmente si conosce è facile, ma nell'accesso a tale link sarà sempre più facile incontrare un malware che si installerà sul proprio dispositivo. Proprio gli attualmente in voga ransomware si stanno propagando anche attraverso questa strada. Elenchiamo le prime 5 minacce sui social network secondo gli esperti:

1 - Mobile ransomware

I malware di tipo "cryptolocker" hanno subito un duro colpo con la chiusura del botnet Zeus, ma le strade del "profondo blu" sono infinite e nuovi ransomware stanno trovando altre vie. Conviene ignorare tutti i messaggi che vi accusano di crimini osceni contro animali o bambini. Purtroppo, talvolta, non sono così espliciti.

2 - Trojan e video raccapriccianti

Sfruttando il gusto del macabro, piuttosto diffuso a giudicare dal successo di alcune serie televisive, i cybercriminali legano i malware, trojan in particolare sembrerebbe, a video su delitti efferati, come decapitazioni o peggio.

3 - Attacchi scam da account LinkedIn

Meno truculenti, ma anche più pe-

ricolosi sono gli attacchi scam, condotti tipicamente, attraverso messaggi e-mail. Sono in crescita quelli mandati da falsi indirizzi LinkedIn, che promettono guadagni facili con un comodo lavoro da casa, poco impegnativo e molto remunerativo. Una volta abboccato tutti i vostri dati personali saranno con ogni probabilità utilizzati per frodi dirette a voi e/o altri.

4 - Scam o spam legati alle ricerche popolari

Come già in tante occasioni (tra le ultime, tuttora in voga, Ebola), i cybercriminali sfruttano l'attenzione a specifici temi e, con la tecnica detta di search o SEO poisoning, fanno in modo che siti Web creati ad hoc risultino tra i primi risultati nelle parole più popolari sui motori di ricerca. Non è un caso se la classifica delle ricerche su Google ha una corrispondenza quasi uno a uno con le campagne di spam. In particolare, i cybercriminali non mancano mai di sfruttare la morte di una qualche celebrità.

5 - Pubblicità malevola sui social network

La pubblicità maligna, cioè che reindirizza a pagine Web contenenti malware, è utilizzata da tempo, per esempio per il ransomware collegato a siti porno o peer-to-peer. Sono direttamente le reti pubblicitarie che distribuiscono minacce integrate in Web advertising, ovviamente non consapevolmente, ma, quantomeno, perché non si pongono il problema e non controllano i file dei banner che l'inserzionista manda loro. Tali network

evidentemente non hanno sistemi di sicurezza adeguati e, indirettamente, tradiscono la fiducia del sito che gli ha affidato la vendita di spazi pubblicitari. Risultato, per esempio, è che anche la piattaforma advertising di Facebook, dotato di ottima reputazione, ospita adware.

L'avvento del Ransomware

Cryptolocker è stato probabilmente uno dei principali protagonisti del 2014, gettando il panico tra molti utilizzatori di dispositivi mobili. Appartiene alla categoria emergente del cosiddetto ransomware: l'ultima "moda" tra i cybercriminali perché consente loro di guadagnare tanto in poco tempo e poco sforzo.

Ransom in inglese significa riscatto. Il dispositivo infettato viene bloccato e il codice maligno chiede di pagare un riscatto al proprietario per "liberarlo". Non è una novità assoluta, perché è nato diversi anni fa, ma era poco diffuso all'inizio in quanto meno efficace di oggi. Infatti,

all'inizio i ransomware venivano annidati soprattutto nella pubblicità sui siti pornografici, bloccando il computer su una videata alquanto esplicita e, per taluni, imbarazzante. Il successo è stato però notevole e nel 2014 si è passati a un uso più massiccio con una nuova generazione di malware. I primi, infatti, solo apparentemente bloccavano il computer, ma in realtà fermavano la videata che era relativamente semplice da eliminare. Con la nuova generazione di ransomware, il computer viene effettivamente bloccato, perché i dati vengono crittografati. Inoltre, nel 2014 sono comparsi i primi codici di questo tipo indirizzati ai dispositivi mobili come smartphone e tablet: è facile immaginare il panico di chi si vede bloccata quella che per tanti è diventata un'estensione vitale del proprio io. La crescita è costante dall'introduzione della prima variante che ha preso di mira i dispositivi iOS, alla prima variante per Android che

crittografa i dati del dispositivo. Sono quattro i mobile ransomware più dannosi scoperti nel 2014: Simplocker, Cryptolocker, iCloud "Oleg Pliss" e FakeDefend.

Simplocker è stato identificato giugno 2014. Si presenta come applicazione trojan, per esempio in file Flash Player. Si tratta del primo "vero" ransomware per Android, nel senso che crittografa realmente i file (con estensione jpeg, jpg, png, bmp, gif, pdf, doc, docx, txt, avi, mkv, 3gp e mp4) sul telefono.

Un avviso sullo schermo che indica che il telefono è bloccato e che per sbloccarlo è necessario effettuare un pagamento. Anche dopo la disinstallazione dell'applicazione in modalità provvisoria, i file devono essere decrittografati.

Cryptolocker, scoperto a maggio 2014, viene camuffato come un'applicazione BaDoink per scaricare video. Anche se il malware non causa danni ai dati del telefono, visualizza una schermata di blocco ad



opera della polizia locale, personalizzato in base alla geolocalizzazione dell'utente finale. Il blocco dello schermo viene lanciato ogni 5 secondi rendendo difficoltoso il funzionamento del dispositivo senza la disinstallazione del malware.

Il terzo è iCloud "Oleg Pliss", scoperto anch'esso a maggio 2014 ed è il primo caso segnalato di ransomware per dispositivi Apple. In effetti non si tratta di un malware vero e proprio, perché gli attacchi avvengono tramite account iCloud compromessi in combinazione con alcune tecniche di social engineering.

Gli esperti ipotizzano che gli autori degli attacchi sfruttino la funzionalità "Trova il mio" iPhone, iPad o Mac di Apple, unitamente a password riciclate ottenute tramite violazioni delle password.

L'attacco, tuttavia, non funziona se il dispositivo ha già un codice di accesso impostato (blocco del telefono). Il malware potenzialmente può violare informazioni relative a calendario e contatti e consentire all'autore dell'attacco di eliminare informazioni dal telefono.

Infine, FakeDefend è il più vecchio, scoperto a luglio 2013, e prende di mira i dispositivi Android. Si presenta come un'applicazione antivirus contraffatta che invita l'utente finale a pagare una sottoscrizione completa dopo avere eseguito una falsa scansione e avere mostrato un elenco di "infezioni" hard-coded individuate sul telefono.

Se l'utente decide di pagare la somma, i dettagli della carta di cre-

dito forniti vengono trasmessi al server dell'autore dell'attacco in forma di testo normale. I dettagli rubati della carta di credito possono essere usati successivamente per transazioni illecite.

Il ritorno d'investimento per i cybercriminali è alto, vista la diffusione dei dispositivi mobili, per questo si ipotizza che i ransomware saranno sempre più indirizzati verso gli smartphone. C'è un ulteriore vantaggio, rappresentato dalla minore consapevolezza dei rischi che hanno gli utenti di dispositivi mobili, rispetto ai "vecchi lupi di mare della navigazione da pc".

Gli attacchi mirati e persistenti

Tutti i rapporti divulgati dalle principali società impegnate nella sicurezza concordano su un dato: aumentano il numero degli attacchi "mirati", cioè condotti con un preciso fine, e di quelli "silenti", cioè orientati a un obiettivo evitando di "far rumore". Sono quelli che vengono raccolti nella categoria Advanced Persistent Threat.

Gli APT sono lo strumento principale per perseguire tali obiettivi illeciti e sono utilizzati in tutti gli ambiti: nello spionaggio industriale o governativo, nelle azioni di sabotaggio, nelle frodi, nei furti di proprietà intellettuale, nella sottrazione di dati e così via.

Gli aggettivi "advanced" e "persistent" indicano le caratteristiche principali di questi attacchi: l'uso di tecniche sofisticate, la combi-



nazione delle stesse in una strategia basata su più fasi e la tenacia con cui questa viene applicata con continuità fino all'ottenimento dell'obiettivo e oltre. Oltre, perché in casi come lo spionaggio, il malware è progettato per annidarsi e continuare a spiare anche per anni, finché non viene scoperto.

Recentemente, per esempio, sono stati trovati malware che "spiavano" enti governativi e aziende statunitensi, probabilmente di origine russa (un sospetto dovuto alla presenza di caratteri cirillici in alcune stringhe di testo incluse nel codice).

Le fasi di un attacco APT sono diverse: secondo alcune classificazioni 5, per altri 6 o 7. Di fatto, non c'è una reale uniformità, perché alcune di queste fasi possono mancare o, più spesso, essere accorpate in un'unica azione a seconda dei casi. La caratteristica principale è l'utilizzo di più tecniche organizzate secondo una sequenza abbastanza standard, perlopiù rappresentata in una serie di fasi ognuna propedeutica alla successiva, che partono dalla ricognizione, alla



compromissione di un primo sistema, all'espansione all'interno della rete aziendale e alla paziente e costante osservazione dell'attività svolta al suo interno (predisponendo un centro di Command e Control) fino alla fase centrale di sottrazione delle informazioni.

L'Internet of Things e le nuove botnet

Dopo il Web 2.0, si è cominciato a parlare di Web 3.0, una definizione che è stata presto abbandonata a vantaggio di due altre diciture: Machine to Machine (M2M) o Internet of Things (IoT). Di fatto, il Web è sempre stato concepito come l'interazione tra un individuo e una macchina (server), poi si è passati al 2.0, che prevede l'interazione tra gli individui, comunque mediata da una macchina. Il terzo passo è l'interazione diretta tra macchine. Di fatto, sarà presto maggioritario il numero di dispositivi posti in rete per svolgere compiti diversi da quelli di mettere in comunicazione individui o fornire informazioni a questi stessi. Si tratta,

per esempio, di sistemi di controllo di impianti industriali collegati a sensori che rilevano determinati parametri. Quando questi ultimi superano una soglia potrebbe partire un allarme e il sistema di controllo genera un'azione corrispondente. La possibilità di utilizzare la rete IP e Internet in particolare per attuare una soluzione del genere è già stata presa in considerazione. Ancora una volta, sono le problematiche di sicurezza che faranno la differenza. Quali saranno le sfide del futuro per le aziende che si occupano di sicurezza, una cosa è certa: non possono continuare a giocare a nascondino con i "ragazzi cattivi". Una rincorsa senza sosta da una minaccia a un nuovo rimedio non ha senso. È necessario modificare le regole del gioco: cambiare approccio e anticipare le mosse dell'avversario, scendendo sul suo stesso terreno e partendo dagli obiettivi che si pone.

Le minacce rivolte all'IoT che, oggi, sono ipotizzabili, riguardano in primo luogo la disponibilità del servizio: un DDoS mette in seria difficoltà la trasmissione delle informazioni cui le macchine in rete sono preposte.

Ovviamente, gli attacchi a infrastrutture critiche rivolte a sistemi SCADA rappresentano un fronte di "guerra" e scenari da vera e propria Cyber War sono certamente realistici. In questi contesti è ipotizzabile che enti governativi possano stanziare i fondi necessari per sviluppare kit di attacco mirati, al fine di colpire un singolo obiettivo.

Già il costo per un sabotaggio è poco probabile sia sostenibile per colpire un concorrente, ma se si tratta di un "nemico" lo scenario cambia.

Il cybercrime, invece, si sta attrezzando per abbandonare le botnet così come oggi le conosciamo, cioè composte da pc e server, e sta sfruttando la maggiore superficie di attacco, grazie al fatto che un numero consistente di dispositivi M2M in Rete utilizzano sistemi noti come Linux.

Botnet complesse, composte da dispositivi di differente natura, sono già una realtà: è stato, infatti, registrato il primo caso di frigorifero utilizzato in una sorta di botnet per mandare spam. Il grosso rischio, in questo contesto, è che in molti di questi dispositivi vengano utilizzati vecchi pezzi di codice o, comunque, software open source che difficilmente saranno aggiornati: chi si occuperà dell'upgrade del firmware del forno a microonde o della lavatrice? La probabilità che buona parte delle macchine in rete resti indifesa rende l'IoT una miniera d'oro per chi cerca una macchina da usare gratuitamente.

È, infine, ipotizzabile un futuro in cui avverrà il passaggio dalla minaccia informatica a quella fisica: già oggi alcuni modelli di automobile dispongono di componenti elettronici e computer di bordo raggiungibili da remoto via wireless, che potrebbero essere manomessi provocando un incidente.

A quel punto la sensibilizzazione verso l'importanza della cyber security sarà compiuta. *

La centralità della sicurezza nella mobility aziendale

La mobilità, nell'odierno contesto lavorativo, non rappresenta una scelta ma un'esigenza, che porta con sé molti benefici ma anche nuovi rischi

I nuovi modelli di lavoro in mobilità rappresentano la fase finale di quel processo di allargamento del perimetro aziendale cominciato con l'avvento di Internet di cui la mobilità ha rimosso gli ultimi limiti in termini di spazio e tempo, non solo per l'azienda ma anche per i suoi clienti e fornitori. Dispositivi come gli smartphone e i tablet ci hanno abituato a trovare online tutti i contatti e gli strumenti che servono per organizzare la nostra vita sociale e professionale, contribuendo in maniera sostanziosa al processo di "business transformation", che ridefinisce completamente i processi aziendali, aumentando la produttività, cambiando le relazioni di lavoro e sviluppando attività completamente nuove.

Il primo aspetto da considerare è l'abitudine all'utilizzo: come ormai da qualche anno ha insegnato la consumerization o quella che oggi è preferibile chiamare digital transformation, gli utilizzatori sono avvezzi a utilizzare strumenti semplici e si aspettano la stessa "user experience" in azienda. Come raccontato da un CISO (Chief Information Security Officer) di una nota casa del lusso, se prima arrivavano all'IT richieste del tipo "ho bisogno di fare questa cosa", oggi il business manager chiede: "mi serve una app per fare questa cosa".

Il cambiamento è epocale e non c'è possibilità che si torni indietro. Questo implica ripensare i processi in chiave mobile e immaginare i

futuri servizi sempre in quest'ottica. Alla base di questa rivisitazione deve esserci un'attenzione costante per la sicurezza, da porre al centro e la via più logica per rispondere a queste esigenze è di integrare la sicurezza direttamente nell'applicazione mobile.

I temi della mobile security

Le tematiche di sicurezza legate alla mobilità sono riconducibili a quelle che oggi le aziende si trovano a gestire nel loro complesso. Il primo problema è che la quasi totalità dei dispositivi mobili sono progettati e costruiti per il mondo consumer. Le prime generazioni di smartphone e tablet non consentivano di installare un antivirus, per esempio. Oggi che i device mobili intelligenti, cioè dotati di capacità computazionale, sono più diffusi di quelli "fissi", l'attenzione dei cybercriminali si è spostata e le minacce direttamente rivolte a tali dispositivi sono aumentate. Questo, se aumenta il rischio generale, dall'altro lato ha portato le aziende produttrici a progettare con più attenzione i dispositivi e sta favorendo lo sviluppo di soluzioni specifiche per la sicurezza dei device mobili.

Ciò premesso, va sottolineato che le tecniche con cui nei dispositivi mobili si insidiano malware ed eventi di exploiting presentano la medesima complessità di quelli che attaccano i comuni pc e ne condividono i medesimi deleteri effetti. In alcuni casi possono causare un imme-

diato danno economico, per esempio connettendo il dispositivo a servizi a pagamento, effettuando telefonate o spedendo SMS verso numeri Premium che applicano tariffazioni a consumo, o danni indiretti, magari esportando fraudolentemente dati.

Le criticità del BYOD

Un terzo fondamentale aspetto riguarda le modalità di utilizzo dei dispositivi mobili. È ormai entrata nel linguaggio comune la sigla BYOD (Bring You Own Device), che rappresenta una conseguenza del fenomeno più ampio della digital transformation o consumerizzazione, portando con sé i rischi legati a un uso promiscuo, personale e aziendale, di dispositivi informatici.

Una soluzione parziale al problema è stata fornita dai principali produttori di software con soluzioni o appliance per la protezione degli endpoint, che si preoccupano di verificare che un dispositivo mobile che si vuole connettere alla rete aziendale soddisfi i requisiti di sicurezza e conformità necessari: per esempio che abbia installato l'ultima patch del sistema operativo o che non abbia disattivato funzioni di protezione.

Queste soluzioni forniscono una protezione efficace per evitare di portare all'interno della rete aziendale malware contratti all'esterno, ma non c'è tecnologia che tenga per proteggersi dalla superficialità e dalla noncuranza manifestata troppo spesso dagli utenti.

La possibilità di lasciare incusto-

dito il proprio dispositivo mobile o di connettersi a una rete domestica che non dispone dei sistemi di protezione di quella aziendale, lascia aperta la possibilità di smarrire o di diffondere informazioni aziendali importanti e riservate, incluse password di accesso alla rete aziendale, dati sensibili o business critical. Tuttora ogni persona dispone di più di un device personale, anche se è ipotizzabile un certo consolidamento nel tempo. Già oggi sono molti i sistemi "convertibili" che, per esempio, possono essere utilizzati come un pc portatile o come un tablet. D'altro canto, si stanno anche diffondendo i phablet, cioè smartphone dotati di un display maggiore di 5 pollici che consentono di navigare su Internet con maggiore facilità rispetto agli smartphone e di telefonare anche senza un auricolare e certamente più agevol-

mente che con un tablet.

Quale che sia il dispositivo scelto, la tendenza è comunque di usarne uno solo sia per le attività personali sia per quelle attinenti alla sfera lavorativa. Da qui nasce il problema generato dall'ospitare su un'unico dispositivo mobile dati fondamentali per l'azienda: per esempio password di accesso alla rete che, di fatto, lasciano una porta aperta per entrare nell'intero network aziendale.

I rischi delle App

Altro ambito delicato è quello delle App. È facile che l'abitudine a utilizzare app e servizi per i propri dati personali venga "trasferita" anche ai dati aziendali. Per esempio, usando servizi come Dropbox per tutto o sincronizzando tutti i dati dell'iPhone su iCloud di Apple, senza preoccuparsi che i dati aziendali

possano essere copiati, come è accaduto per le immagini private di alcune celebrità. Spesso manca la consapevolezza dei rischi.

L'utilizzo indiscriminato delle app porta altre implicazioni pericolose per le imprese. Per avere un'idea della portata del rischio si pensi che il numero di App potenzialmente nocive presenti sull'App store Android è stato stimato abbia superato i due milioni: un numero che, per quanto sembri grande, alcuni vendor stimano in raddoppio entro sei mesi. Si tratta di un fenomeno che ricorda quello che ha caratterizzato altri sistemi operativi di grandissima diffusione, come Windows, con la differenza che lo sviluppo tecnologico sta rendendo tutto più rapido portando il numero di minacce a crescere costantemente sia in numero sia in pericolosità. *



Sicurezza e business continuity nell'era del SDDC

L'evoluzione verso modelli di data center software defined data porta a ripensare le modalità per garantire l'operatività aziendale e la gestione dei dati

L'aspetto fondamentale di una strategia di business volta a salvaguardare i dati, le informazioni e i processi aziendali prevede un primo passaggio obbligatorio: la salvaguardia della continuità operativa del business. Quello tra business continuity e sicurezza rappresenta un binomio non solo indispensabile, ma che può sorprendentemente portare a importanti risparmi economici.

Certe volte la continuità del business è, però, un concetto aleatorio di cui se ne scopre l'importanza quando è troppo tardi e ci si trova a un passo da eventi disastrosi o, peggio, il limite è stato superato. Cionondimeno, le interruzioni dell'operatività aziendale possono essere improvvise, drammatiche e terribilmente estese e le stesse cause possono andare dai fenomeni naturali agli errori umani, dai guasti meccanici sino a eventi con carattere doloso. A fronte di una crescente dipendenza delle applicazioni e dell'operatività quotidiana dai dati e dall'e-business, si delinea sempre più chiaramente l'importanza di elaborare, attuare e mantenere piani efficaci e aggiornati di business continuity e disaster recovery, anche sotto forma di semplici provvedimenti cautelativi.

Verso il Software Defined Data Center

Il punto centrale e iniziale di una strategia volta ad assicurare la sicurezza e la disponibilità dei dati aziendali e del funzionamento delle

applicazioni business o di produzione è, in sostanza, il data center. Il data center come lo conoscevamo è negli ultimi anni profondamente mutato. I trend che l'hanno interessato e lo stanno tutt'ora interessando sono numerosi.

La virtualizzazione, il cloud, la ri-centralizzazione delle funzioni prima demandate ai server in un'architettura client-server che ha dominato le scene sino a ora, la virtualizzazione dei desktop, il BYOD e cosa ciò implica per la sicurezza dei dati e la gestione delle immagini e dei dati attinenti i dispositivi remoti, il cloud nelle sue diverse incarnazioni (public, private o hybrid) e, ultimo in ordine di tempo ma con un effetto dirompente, il Software Defined Data Center (SDDC). Con quest'ultimo termine, in sostanza, si intende la capacità di organizzare un data center in modo che sia facilmente gestibile via software, con un disaccoppiamento tra hardware e la sua immagine virtuale così come viene proposta alle applicazioni e con la implicita possibilità di gestire in modo trasparente le diverse tipologie di risorse, che si tratti dei server, dello storage o della rete. È immediato capire come una tale evoluzione sia congruente con le esigenze di chi desidera adottare un cloud di tipo sia ibrido sia public.

La complicazione ovviamente non si ferma al contorno, perché se software defined deve essere un data center, software defined devono necessariamente essere tutte le sue

componenti, come per esempio lo storage e il substrato di rete.

Quella dell'SDDC è un'evoluzione che era nell'aria e sembra essere la conseguenza diretta della virtualizzazione, oramai fortemente attuata dalle aziende, e dalla crescente diffusione del cloud, soprattutto di tipo ibrido, che appare sempre più essere la strada che imboccheranno le aziende nel passaggio a un nuovo modo di concepire e fruire di un'infrastruttura ICT il più possibile basato sul concetto di dinamicità nell'uso delle risorse e del loro pagamento.

In sostanza, quello che ci si aspetta abiliti concettualmente un SDDC è di disaccoppiare del tutto le applicazioni dalla componente fisica sottostante e, tramite un strato software e un insieme di API (che permettano alle diverse componenti di interagire in modo standardizzato), far sì che a un'applicazione vengano automaticamente assegnate le risorse che le servono in funzione di parametri prestabiliti, come: la potenza elaborativa necessaria; il volume di dati da trattare; il grado di sicurezza; il livello RAID; la dispersione geografica dei dati da accedere e così via.

Ciò vuol dire poter orchestrare automaticamente l'assegnazione delle risorse alle singole applicazioni e farlo non solo in modo fisso, ma anche in base alle esigenze del momento.

Ripensare la gestione dei dati per garantirne la protezione

Un'infrastruttura basata sulla virtualizzazione e l'orchestrazione

delle risorse virtualizzate in chiave software defined, porta a rivedere le infrastrutture di backup, restore e disaster recovery basate sulla copia dei dati, il vaulting fisico e tutte le procedure correlate che, soprattutto, non sempre vengono condotte pienamente. In particolare, troppo frequentemente viene saltata la fase di test con il rischio che, al momento del bisogno, non si riesca a effettuare il ripristino così come lo si era ipotizzato e, quindi, impedendo un ritorno allo stato precedente all'evento disastroso. Peraltro, proprio la complessità di questi sistemi rende difficile abbandonarli in tempi rapidi, senza contare i vincoli legacy e quelli legali, che impongono di poter accedere a determinati contenuti e di rispettare alcune normative anche di settore.

Il risultato è che presso le aziende si è in una fase di transizione, indirizzandosi verso nuove architetture incentrate sulla gestione dei dati con nuove garanzie di availability, in cui intere risorse e applicazioni possono essere memorizza-

te sostanzialmente in un file, con i dati duplicati nel cloud e l'immagine del proprio sistema informatico che possono essere ripristinati in tempi rapidi, da qualsiasi parte del globo.

L'aspetto impiantistico

Garantire ai propri utenti una continuità del servizio e una disponibilità dello stesso richiede non solo un'attenzione ai sistemi prettamente IT ma anche preoccuparsi che le altre componenti infrastrutturali siano dotate di opportune caratteristiche costruttive e operative. Nel far funzionare correttamente gli apparati di un data center un ruolo sempre più importante fondamentale lo gioca l'ambiente e l'infrastruttura di supporto e, in sostanza, quanto attinente al condizionamento ambientale e all'alimentazione energetica. La loro qualità è l'elemento indispensabile perché il sistema nel suo insieme funzioni correttamente e risulti sicuro.

Va osservato che minori consumi energetici espongono anche a minori rischi per quanto concerne la mancanza di energia necessaria al funziona-

mento, implicano l'uso di macchine meno esigenti dal punto di vista dimensionale e in sostanza quello che ne deriva sono strutture che risultano meno critiche e più sicure. In genere, ridurre i consumi significa anche ridurre la produzione di calore e questo ha un impatto positivo sulla durata delle macchine e quindi sulla sicurezza di poter continuare a godere delle applicazioni IT.

Per assicurare un livello di funzionamento continuo del 99,9999% è auspicabile che sottosistemi storage, server, network e infrastruttura, compresi gli impianti di alimentazione e raffreddamento, adottino il medesimo approccio implementativo, scalabile, modulare, ridondato e con componenti sostituibili a caldo in caso di guasto.

La necessità di soluzioni a basso consumo ed ecocompatibili deriva anche da esigenze di compliance alle normative, che interessano e coinvolgono nel processo di rinnovamento tecnologico anche quelle società che, per vari motivi, sono potenzialmente meno attente a questo trend evolutivo. *



Biometria: la protezione siamo noi

Si diffonde l'utilizzo di sistemi di sicurezza basati su dati direttamente e univocamente collegati all'individuo per esigenze di controllo dell'accesso ad asset fisici e digitali

L'uso di dispositivi e tecnologie per la raccolta e il trattamento di dati biometrici è in costante incremento per rispondere a esigenze sempre più stringenti di controllo e verifica dell'identità. Sistemi basati sull'analisi di parametri biometrici possono essere adottati per il controllo fisico ed elettronico degli accessi, per abilitare l'accesso fisico a locali e aree specifiche, l'attivazione di macchinari oppure per un controllo degli accessi di tipo logico (autenticazione informatica). Un caso a parte è quello dei sistemi di firma grafometrica, in cui vengono incorporate all'interno del documento informatico una serie di informazioni strettamente connesse al soggetto firmatario senza che necessariamente sia effettuato un riconoscimento biometrico.

Metodi di confronto

Il metodo alla base della sicurezza biometrica è quello di impiegare delle caratteristiche personali quali le impronte digitali, i lineamenti del volto, l'immagine della retina, l'iride, il timbro vocale, la calligrafia, la struttura venosa delle dita, la geometria della mano per autenticare un individuo tramite comparazione. La comparazione può essere condotta in due modi, che implicano tipicamente diversi utilizzi del sistema biometrico: la verifica o l'identificazione.

Il processo implica due fasi. La prima consiste nella registrazione del tratto biometrico, che viene

catturato, estrapolato e convertito in un codice binario per generare un modello biometrico che sarà memorizzato in modo persistente e invariabile nel tempo all'interno di un database. Questo modello costituirà la base per una comparazione basata su metodi statistici e metriche tipici del sistema biometrico prescelto. Per rendere più veloce il sistema o per applicazioni particolari, il modello originale può essere memorizzato anche direttamente su una smart card, ovviamente con tecniche cosiddette di "tampering", che ne impediscono la manomissione. Per esempio, questo può essere utile per applicazioni di servizio pubblico: l'utente porta con sé un certificato digitale che contiene il template biometrico che può impiegare per autenticarsi presso determinati sportelli o enti senza doversi collegare a un server remoto. La seconda fase è quella di "matching". Quando l'utente richiede l'accesso (per esempio, quando si presenta alla porta d'ingresso di un laboratorio riservato, oppure quando semplicemente dal proprio pc vuole accedere a dati riservati) è chiamato a sottomettere il tratto caratteristico precedentemente registrato all'apposito lettore biometrico, in modo che venga rilevato e comparato con il modello presente nel database. Nelle applicazioni di verifica biometrica l'immagine acquisita viene sovrapposta al modello per verificare l'identità dichiarata della persona (è il caso utilizzato per le tecniche di autenticazione). Il

metodo della verifica, impiegato in un sistema di autenticazione, può essere poi abbinato ad altri elementi di identificazione, come user ID, password, token, smart card e così via, per incrementare ulteriormente il livello complessivo di sicurezza. Nel processo di identificazione biometrica, invece, il sistema confronta il modello rilevato con tutti i modelli biometrici disponibili all'interno di una banca dati per individuare l'identità del soggetto (confronto uno a molti). Si tratta della modalità tipica da investigazioni utilizzata dalla Polizia.

I rischi della biometria

L'elevato grado di unicità nella popolazione di molte caratteristiche biometriche espone al rischio che soggetti privati e istituzioni possano acquisire informazioni sui singoli individui per finalità differenti da quelle per cui tali dati biometrici sono stati in origine raccolti, incrociando e collegando dati provenienti da più banche dati. Peraltro, alcune caratteristiche biometriche possono essere acquisite senza la consapevolezza o la partecipazione di un individuo.

Un altro elemento di rischio specifico è la possibilità di furto di identità biometrica che può causare effetti lesivi rilevanti e duraturi poiché, diversamente dai sistemi di autenticazione tradizionali, diventa impossibile fornire alla vittima del furto una nuova identità biometrica che utilizzi la stessa tipologia di dato biometrico.

Inoltre, va ricordato che il riconoscimento biometrico avviene generalmente su base statistica e non deterministica e, pertanto, non è esente da possibili errori. In particolare, un sistema di autenticazione biometrica può commettere due tipi di errore: può portare erroneamente ad accettare il confronto con una persona che è in realtà un impostore (falso positivo) oppure negare l'accesso a un utente autorizzato (falso negativo). In generale, i sistemi in commercio dichiarano il tasso di errore dei due tipi e sarà l'impresa utilizzatrice a dover scegliere quale dei due rischi è il meno grave. Nel primo caso, si può prevedere di inserire, come accennato, ulteriori meccanismi di controllo, migliorando l'accuratezza originale del sistema. Non va neppure esclusa, in teoria, la possibilità di falsificazione biometrica. È stato, per esempio, dimostrato nel caso delle impronte digitali che è possibile ricostruire un campione biometrico corrispondente a un modello biometrico di partenza. Si pensi, per esempio, alla possibilità di realizzare una sorta di "dito artificiale" che riproduca le

sembianze anatomiche del polpastrello, magari utilizzando tecniche di stampa tridimensionale a basso costo. La diffusione di sistemi mobili e di modelli BYOD, da una parte difonde l'utilizzo di sistemi di autenticazione biometrica (predisposti magari dall'azienda sul tablet di un dipendente con il suo consenso) e dall'altro espone a rischi maggiori rispetto allo svolgersi del trattamento all'interno del perimetro di sicurezza aziendale. Infatti, l'uso promiscuo dei dispositivi solitamente mal si concilia con la sicurezza dei dati e sull'adozione puntuale e continua di meccanismi di controllo degli accessi anche di tipo basilare e di modalità di connessione sicura con protocolli avanzati per proteggere i dati in mobilità.

Tipologie di sistemi biometrici

Le tecniche biometriche possono essere classificate in diversi modi. Possono essere interattive ovvero richiedere la consapevole partecipazione dell'interessato durante l'acquisizione del dato biometrico (per esempio scansione della retina o firma autografa) oppure passive come

quando si effettua la registrazione dell'immagine di un volto o una voce senza che l'interessato ne sia reso partecipe. Possono essere basate su caratteristiche biologiche, fisiche o comportamentali (per esempio nel caso di apposizione della firma). In ogni caso devono possedere caratteristiche di univocità per ogni persona e di presenza in ogni individuo. I parametri biometrici sono differenti anche in merito alla stabilità temporale e alla tipologia di decadimento per cause naturali o accidentali e questo può avere un effetto sul confronto con il modello di riferimento. Le principali tipologie di parametri biometrici comprendono il trattamento delle impronte digitali, le modalità di apposizione della firma autografa, il riconoscimento vocale, il controllo delle caratteristiche della rete venosa delle dita e della mano di un individuo, il rilevamento della struttura vascolare della retina, la lettura della forma dell'iride, la rilevazione delle proprietà geometriche della mano acquisite in modalità bidimensionale o tridimensionale, il riconoscimento del volto. *



La sicurezza di Trend Micro per ambienti fisici, virtualizzati e cloud

L'approccio integrato e user centrico dell'azienda giapponese permette di contrastare in modo proattivo e in tempo reale l'evoluzione delle minacce in ambienti fisici, virtuali e cloud avvalendosi di un livello di intelligenza distribuita

Garantire la sicurezza aziendale è un processo che non si interrompe mai e che richiede continue revisioni dell'approccio metodologico di difesa. Sulla base di questo presupposto, Trend Micro propone un modello di sicurezza che evolve dinamicamente, basato su un framework unificato e un'intelligenza distribuita, per la gestione e la protezione di dati, infrastrutture, applicazioni e dispositivi mobili in ambienti fisici, virtuali e cloud. Trend Micro propone anche un differente approccio alla lettura dei log di sicurezza che, fino a oggi, è sempre stata incentrata sul dispositivo che era deputato a segnalare il malware. Con gli attuali sistemi di mobilità e le odierne infrastrutture IT, soprattutto in contesti di attacchi mirati, il veicolo principale dell'attacco ovvero l'anello più debole della catena di protezione è la persona, che può utilizzare moltissimi dispositivi all'interno dell'azienda. Per questo motivo Trend Micro affronta l'analisi dei log con un approccio user centrico che consente, in caso di attacco, di controllare l'attività di uno specifico utente sia su tutti i dispositivi personali sia sui sistemi utilizzati.

La Smart Protection Network

Smart Protection Network è l'infrastruttura per la protezione automatizzata e proattiva degli ambienti fisici, mobili, virtuali e cloud che sta alla base di tutti i prodotti e le strategie di sicurezza di Trend Micro.

La Smart Protection Network sfrutta un approccio di difesa intelligente basato sulle conoscenze collettive ottenute dell'ampio bacino dei clienti Trend Micro e da oltre 150 milioni di sensori distribuiti a livello globale. Mettendo in correlazione in tempo reale i dati provenienti da decine di miliardi di query giornaliere attraverso i propri centri di controllo globale, la Smart Protection Network permette di assegnare, tramite una serie di criteri oggettivi, un livello di reputazione a URL, e-mail, file, di convalidare gli indirizzi IP o di attivare azioni

preventive di protezione in base a queste indicazioni per inibire eventuali vulnerabilità. L'infrastruttura di Trend Micro fornisce agli utenti anche un meccanismo per valutare dinamicamente la reputazione delle App, impedendo di scaricare quelle dannose e identificando quelle che potrebbero abusare della privacy o dell'uso del dispositivo.

La tecnologia di reputazione di Trend Micro si basa su database integrati e correlati tra loro in modo che ogni nuova minaccia, identificata tramite una verifica di routine della reputazione di un singolo cliente, aggiorni automaticamente tutti i database delle minacce di Trend Micro e blocchi ogni successiva interazione del cliente e di tutti i clienti Trend Micro con una specifica minaccia. La Smart Protection Network mette anche a disposizione white list "in-the-cloud" per un'identificazione rapida e accurata degli eventi sicuri al fine di minimizzare i falsi positivi.

L'azienda giapponese, a partire dal 2015, ha reso anche disponibile come servizio la possibilità di correlare le informazioni reputazionali fornite dalle Smart Protection Network (feed e query) con quelle di altri database e anche la sua integrazione con prodotti di terze parti, per esempio sistemi SIEM, allo scopo di migliorare la comprensione degli eventi di sicurezza e contrastare in modo più efficace le nuove tipologie di minacce.



Trend Micro Smart Protection Network

La strategia delle tre C

Trend Micro ha sintetizzato la sua proposizione strategica all'insegna di tre "C".

La prima è la **Custom defense** ovvero la possibilità di predisporre un livello di protezione personalizzato per ogni specifico ambiente aziendale per rafforzare la protezione dai nuovi rischi come quelli associati agli attacchi APT. Per contrastare gli APT Trend Micro ha sviluppato la soluzione **Deep Discovery** che consente di controllare più di 80 protocolli alla ricerca di anomalie. Per le aziende di dimensioni più piccole è disponibile anche una versione del prodotto che controlla il solo flusso SMTP ed entro la fine del 2015 è previsto il rilascio

Il retro scanning per analisi sempre più precise

Una delle ultime innovazioni tecnologiche per la data protection che caratterizza i prodotti di Trend Micro è la possibilità di effettuare un'azione di "retro scanning". Per esempio, in risposta a un allarme fornito dalla Smart Protection Network su un file, le soluzioni Trend Micro possono verificare se il file è entrato in contatto con un indirizzo IP, controllare se altri file della stessa azienda hanno interagito con lo stesso IP, analizzare lo stato dell'IP e verificarne l'attività per capire se da quell'indirizzo sono stati lanciati attacchi per sfruttare specifiche vulnerabilità. Sulla base di questa analisi, la soluzione di Trend Micro può controllare se l'infrastruttura risulta protetta per queste vulnerabilità e, in caso contrario, intervenire in modo automatizzato applicando patch virtuali e bloccando eventuali minacce.

di una soluzione per il controllo del solo flusso Web (http). La Custom defense di Trend Micro affianca a un livello di protezione di tipo "generalizzato", un ambiente smart sandbox personalizzato per l'azienda utente che rispecchia in modo fedele il loro scenario in termini di dispositivi e ambienti operativi utilizzati.

La seconda C sta per **Complete user protection** e significa fornire risposte alle sfide della consumerization ovvero controllare tutto ciò che attiene all'utilizzo personale. A queste esigenze si indirizza, per esempio, la soluzione **Safe Mobile WorkForce**, che permette un accesso sicuro da mobile ai dati corporate, attraverso il delivery da un sistema operativo in remoto. Il telefono è virtualizzato e rimane su un data center, mentre l'utente ha la stessa user experience, senza che i dati risiedano sul dispositivo fisico. Un altro esempio è **Safe Sync**, che offre funzionalità di memorizzazione analoghe a Dropbox, ma fornite come servizio on-premises su cloud ibrido, con un elevato livello di controllo e protezione.

La terza C è quella di **Cloud & data center security** con cui Trend Micro conferma la centralità della focalizzazione sul mercato enterprise e sulla protezione di data center fisici, virtuali, ibridi e cloud.

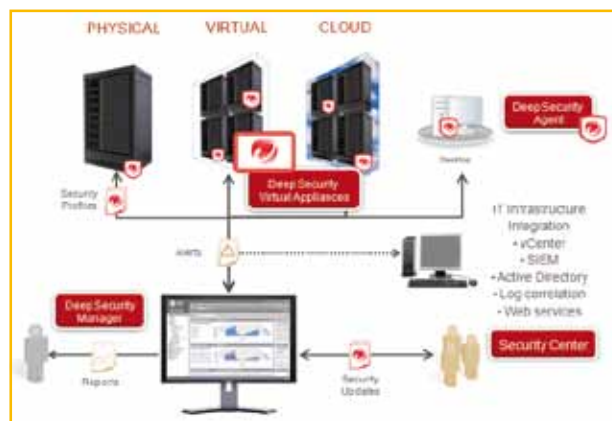
L'azienda prevede il continuo supporto e ampliamento dell'offerta per le piattaforme di virtualizzazione. Il focus primario riguarda le piattaforme di VMware (incluse quelle di rete virtualizzata VMware NSX) e Microsoft. Ma l'azienda si sta orientando anche verso le piattaforme di virtualizzazione Linux based e, prossimamente, anche Open Stack.

Trend Micro Deep Security

Trend Micro ha sviluppato una serie di tecnologie di sicurezza capaci di integrarsi con gli hypervisor delle macchine virtuali. Una di queste soluzioni è **Deep Security**, sviluppata in stretta collaborazione con VMware per ottimizzare la protezione dei sistemi virtualizzati, che include un ventaglio di differenti tecnologie di sicurezza e anti malware specializzate.

Questa soluzione si integra con VMware e le sue API vShield Endpoint e VMsafe, fornendo protezione anti-malware per le Virtual Machine in modalità sia agentless sia basata su agent.

L'architettura della piattaforma prevede i seguenti componenti:



Trend Micro Deep Security

Trend Micro Deep Discovery è la soluzione per la protezione contro gli attacchi mirati

- Deep Security Virtual Appliance, che applica in modo trasparente i criteri di protezione sulle macchine virtuali VMware;
- Deep Security Agent, un componente software installato su server fisico o su macchine virtuali non VMware, che garantisce il rispetto dei criteri di protezione del data center;
- Deep Security Manager per la gestione centralizzata, con possibilità di creare profili di sicurezza e di applicarli ai server, di monitorare gli avvisi e le azioni preventive eseguite in risposta alle minacce, di distribuire gli

aggiornamenti della protezione ai server e di generare rapporti su tutto il data center, sia esso fisico oppure virtuale.

La protezione offerta da Deep Security si estende all'ambiente cloud sino a comprendere i Cloud Client in modo da estendere il perimetro della protezione e correlando in tempo reale il grado di reputazione dei siti Web, dei file scambiati e delle entità sorgenti delle email.

Il livello di sicurezza fornito da Deep Security prevede molteplici funzionalità di protezione che includono: Intrusion Detection e Prevention (IDS/IPS), Virtual Patching, Firewall, Protezione delle applicazioni Web, Protezione antivirus, Integrity Monitoring, Controllo applicativo, Analisi del registro e dei Log e Virtualization Compliance.

Trend Micro Deep Discovery

Trend Micro Deep Discovery è il fulcro della soluzione di difesa personalizzata del vendor contro gli attacchi mirati (detti anche APT). Deep Discovery prevede il monitoraggio a livello di rete con tecnologia smart sandbox personalizzata e in tempo reale, per rilevare precocemente eventuali attacchi.

L'approccio di Deep Discovery punta a individuare contenuti, comunicazioni e comportamenti dannosi su tutte le fasi della sequenza di attacco. La soluzione è costituita da due componenti.

- Deep Discovery Inspector che effettua l'ispezione del traffico di rete, il rilevamento delle mi-

nacce e l'analisi e la segnalazione in tempo reale.

- Deep Discovery Advisor, opzionale, che abilita un'analisi personalizzata aperta e scalabile della sandbox, la visibilità sugli eventi di sicurezza a livello di rete e le esportazioni di aggiornamento della sicurezza.

Consentendo di adattare i meccanismi di protezione per reagire agli attacchi, Deep Discovery offre protezione anche contro malware "zero-day", exploit e download inconsapevoli, Bot, trojan, worm, keylogger, phishing/spear-phishing e attività di sottrazione dei dati.

Trend Micro SecureCloud

Trend Micro fornisce sicurezza "dal cloud" con l'infrastruttura Trend Micro Smart Protection Network e sicurezza "per il cloud" con server e tecnologie crittografiche. Per la protezione multilivello per i dati che risiedono all'interno dei cloud pubblici o privati Trend Micro ha sviluppato SecureCloud, una soluzione che protegge i dati di livello enterprise all'interno degli ambienti cloud mediante l'uso di crittografia e di tecniche di key management basate su policy. Questa tecnologia permette di tutelare i dati del cloud e di favorire la flessibilità necessaria per rivolgersi a cloud provider differenti, senza essere vincolati al sistema crittografico di un unico vendor.

SecureCloud consente di esercitare il controllo sulle modalità e sui punti di accesso alle informazioni

Deep Security as a Service

In linea con il paradigma Cloud, Trend Micro ha reso disponibile Deep Security anche in modalità as a service. L'obiettivo è di proteggere le istanze degli utilizzatori attivate sui server. È un servizio compatibile con i tool di Cloud deployment più utilizzati (Chef, Puppet, Rightscale, OpsWorks e così via) che fornisce una Instant-On Security riconoscendo automaticamente le nuove istanze quando vengono lanciate e che permette di personalizzare specifiche policy in modo che vengano applicate immediatamente e automaticamente ai server dell'ambiente cloud.

Il servizio, mediante la console di controllo centrale, permette di attivare le diverse funzioni in modo da aggiungere in modo elastico la sicurezza a una specifica istanza di un server virtuale.

Amazon ha certificato Deep Security come scanner pre-autorizzato per le Web App su Amazon Web Services, eliminando la necessità di passaggi manuali per l'abilitazione di uno scanner di vulnerabilità.



per mezzo di funzioni che permettono di autenticare l'identità e l'integrità dei server che richiedono di accedere a volumi storage sicuri. Questa soluzione abilita il rilascio automatico delle chiavi di cifratura. Gli utenti possono gestire le loro chiavi crittografiche per ambienti Amazon EC2, Eucalyptus e VMware vCloud direttamente tramite il servizio hosted Trend Micro SecureCloud o da un key server SecureCloud installato all'interno dei loro data center fisici. Trend Micro SecureCloud è disponibile mediante abbonamento mensile o annuale, oppure tramite licenze software tradizionali.

Trend Micro OfficeScan

È una soluzione di sicurezza degli endpoint per le medie e grandi aziende che combina tecnologie di sicurezza in sede e in-the-cloud per salvaguardare file server, desktop, laptop e desktop virtualizzati. Grazie alla sua architettura modulare mette a disposizione un livello di protezione ampliabile che comprende funzioni di:

- Data Loss Prevention (DLP) attraverso un modulo implementato come plug-in).
- Protezione per ambienti Mac con un modulo implementato come plug-in)

- Infrastruttura desktop virtuale (implementata come plug-in).
- Endpoint Encryption.
- Endpoint Application Control.
- Vulnerability Protection.
- Control Manager per una gestione centralizzata).

OfficeScan è in grado di identificare gli endpoint virtualizzati e di ottimizzare l'efficienza della protezione risorse attraverso la serializzazione delle operazioni di scansione e degli aggiornamenti di sicurezza, evitando pertanto i tipici problemi di rallentamento che coincidono con gli update degli antivirus o il riavvio delle macchine. OfficeScan lavora anche in abbinamento con le tecnologie di sicurezza protettive come il controllo delle applicazioni, la protezione della vulnerabilità, la sicurezza mobile e la crittografia degli endpoint per potenziare ulteriormente la protezione contro le minacce. Consente anche di estendere la protezione degli endpoint a smartphone e tablet mediante l'implementazione di Trend Micro Mobile Security.

Trend Micro Mobile Security

A supporto delle esigenze di protezione alimentate dal BYOD Trend

Micro mette a disposizione Trend Micro Mobile Security, una soluzione di sicurezza rivolta alle aziende enterprise e di media dimensione per la protezione di un'ampia gamma di dispositivi mobili quali iPhone, iPad, sistemi in ambiente Android, Blackberry OS e Apple iOS.

Questa soluzione integra gestione dei dispositivi e delle applicazioni dei dispositivi mobili e protezione multilivello dei dati (dalla crittografia, alla DLP, alla cancellazione da remoto) attraverso una singola console di gestione centralizzata. Consente al business di avere visibilità e controllo ma, nel contempo, lascia la libertà ai dipendenti di condividere i dati in modo sicuro attraverso ambienti fisici, virtuali e cloud.

Trend Micro Mobile Security verifica quali App possono essere installate, consente il blocco per i dispositivi mobili e offre la possibilità di definire policy che consentano di autorizzare o negare la connessione alle risorse aziendali, di disabilitare la fotocamera del dispositivo mobile, la connessione Bluetooth e il lettore di schede SD. La soluzione prevede anche l'integrazione con, il servizio di reputazione delle App mobile di Trend Micro. *

I servizi end-to-end Retelit per un IT sicuro ed efficiente

Una rete multiservizio ad alte prestazioni, che permette di disporre di una sicurezza orchestrata su più livelli, a partire da quello fisico garantito dalle connessioni ottiche

Retelit è una società italiana quotata alla borsa di Milano dal 2000 che si posiziona tra i principali fornitori nazionali di servizi di connettività di rete a larghissima banda, di trasporto dati, nonché per la fornitura di infrastrutture per il settore delle telecomunicazioni, delle aziende e della PA. La sua mission è quella di rappresentare un riferimento nazionale per le aziende che necessitano di connettività sicura di alta capacità e di alto livello.

Contrariamente ad altri operatori, che adottano infrastrutture di terzi, i servizi di connettività e dati che fornisce si basano su un'infrastruttura di rete in fibra ottica completamente di sua proprietà. Dal punto di vista dell'infrastruttura, ha evidenziato Federico Protto, amministratore delegato e direttore generale di Retelit, i suoi servizi (dalla connettività al cloud), vengono erogati su base end-to-end con il controllo e monitoraggio diretto dell'intera filiera tecnologica del servizio, dal firewall che abilita e controlla l'accesso a Internet, all'intera infrastruttura fisica della rete ottica compresi gli apparati di rete che connettono le sedi dell'azienda e, se desiderato, il controllo si estende sino a comprendere il firewall presso l'utente. Tramite la rete in fibra ottica e 18 data center, Retelit fornisce sia

servizi di connettività che servizi cloud di tipo infrastrutturale alle aziende che scelgono di demandare a un operatore qualificato la gestione della componente fisica del proprio IT.

Rete a 100 Gb

Elemento chiave nell'offerta Retelit di servizi di connettività di rete e Internet in un quadro di massima sicurezza è la recente evoluzione della sua rete ottica dalla tecnologia SDH a quella Carrier Ethernet con dorsali che raggiungono i 100Gbps, che per la sua qualità ha ottenuto la certificazione del Metro Ethernet Forum 2.0 (MEF 2.0). La MEF 2.0 garantisce il corretto funzionamento e l'interoperabilità quando una connessione end-to-end, mediante interconnessioni NNI, transita su più operatori.

La tecnologia alla base della rete ottica di Retelit le permette anche di realizzare reti OTN (Optical Transport Network) con protocollo ROADM (Reconfigurable Optical Add-Drop multiplexer), uno standard che permette on-demand di modificare rapidamente la capacità di banda per sostenere picchi di traffico in base alle specifiche esigenze

del cliente. In pratica, evidenzia Protto, è possibile a livello ottico incrementare in pochissimo tempo la velocità di un canale da 10 a 20 a 30 a 40 Giga in modo da rispondere all'esigenza specifica semplicemente riconfigurando gli switch ottici.

Quella del MEF non è l'unica certificazione che conferma la qualità e le prestazioni della rete Retelit. A questa si aggiungono anche le certificazioni UNI CEI ISO/IEC 9001, UNI CEI ISO/IEC 27001, UNI CEI ISO/IEC 14001 e la certificazione NATO ALL/NALLA per erogare servizi in ambito militare.

Una sicurezza a più livelli

La configurazione e le caratteristiche della rete ottica permettono di disporre di una sicurezza orchestrata su più livelli, a partire da quello fisico garantito dalle connessioni ottiche. A livello di trasporto è possibile disporre di VPN ottiche, che garantiscono allo stesso tempo un elevato livello di sicurezza delle connessioni oltre che una parimenti elevata velocità

e una bassissima latenza. Le connessioni possono inoltre essere protette mediante il protocollo di encryption AES-256, implementabile in modalità on-demand. A livello ancora superiore Retelit fornisce in ambito IP il servizio di DDoS



Federico Protto,
amministratore delegato e direttore generale di Retelit

mitigation. Il servizio è erogato tramite un suo apposito SOC che oltre a rilevare gli attacchi permette anche di intervenire rapidamente per bloccarli. Sempre a livello centralizzato è possibile fruire da parte dei clienti che hanno la necessità di uscire con il loro traffico su Internet, di un servizio di firewall virtualizzato e dedicato con la possibilità da parte del cliente di selezionare e configurare direttamente le funzioni che gli sono necessarie. A livello 3 vi è anche la possibilità di implementare connessioni private virtuali (VPN) IPsec ed SSL.

Data Backup e storage sicuro con Cloud Storage

Numerosi i servizi dati per le aziende disponibili tramite la rete Retelit. Il Cloud Storage, ad esempio, è un servizio che permette alle aziende di richiedere e attivare risorse di Data Backup & Storage erogate in modalità Public o Private Cloud. Il servizio Cloud Storage permette di estendere in rete, utilizzando una connessione Ethernet privata o tramite Internet, ambienti storage esistenti in modo da realizzare cloud ibridi. Tramite il servizio è possibile poi implementare e gestire le proprie infrastrutture virtuali e soluzioni di Disaster Recovery e Business Continuity. Tra i punti salienti del servizio vi sono:

- Spazio Disco su infrastruttura Storage distribuita su più Data Center: prevede tre diversi livelli, rispettivamente di 2, 7 e

10 TB e una connettività fino a 10Gbps. L'accesso può avvenire anche via Internet tramite connessioni sicure VPN.

- Connettività in fibra ottica tramite l'infrastruttura proprietaria e mediante protocolli CIFS ed NFS.
- Opzioni di sicurezza tramite l'infrastruttura di Managed Firewall di Retelit.
- Piattaforma che assicura elevati livelli di continuità e performance tramite un'architettura ridondata senza "single point of failure".

Consistenti le caratteristiche, che comprendono, tra l'altro, il supporto nativo per client Microsoft Windows e Linux tramite i protocolli standard CIFS/NFS, l'upgrade/downgrade dello spazio disco in modalità on-demand, deduplica dei dati, tier storage multipli e accesso protetto di tipo privato o tramite firewall. Retelit ha posto particolare attenzione anche alle esigenze di continuità operativa, assicurata grazie a un servizio di virtualizzazione che garantisce la resilienza dell'infrastruttura IT e un funzionamento "always on".

Fisicamente la piattaforma per la Cloud Virtualization, certificata 27001, è costituita da un cluster di server disposto all'interno di due POP (Milano e Bologna) situati presso i data center riferiti come primario e secondario anch'essi entrambi certificati ISO 27001, che oltre alle garanzie fisiche di sicurezza assicurano anche la distan-

za minima necessaria richiesta ad un servizio di Business Continuity. Non ultimo, la connettività verso la piattaforma virtuale viene garantita da link dedicati e protetti e tramite accesso Internet.

Disaster Recovery per dati e applicazioni sicure

Le soluzioni Retelit di disaster recovery fanno parte di una suite di servizi basati sulla sua rete ad alta capacità e sui propri data center: servizi che permettono alle aziende private e alle PA di far fronte ad eventi critici per i propri sistemi informativi e garantire la sicurezza e la continuità operativa delle applicazioni. La soluzione è modulabile in funzione delle esigenze specifiche e permette di ripristinare l'operatività in tempi brevissimi e di garantire la continuità dei servizi. Due le tipologie di soluzioni disponibili: disaster recovery semplice e disaster recovery bilanciato.

La prima soluzione è erogata tramite un'architettura di tipo attivo-passivo, basata su due ambienti identici costituiti dalla stessa tipologia di apparati situati in due siti diversi, uno di produzione e uno di recovery, la seconda, si basa invece su un'architettura di tipo attivo-attivo.

Oltre a godere di tutte le funzionalità e dell'architettura della soluzione precedente ognuno dei due data center può operare come primario per una parte dei servizi gestiti e secondario per la parte restante. *

Business continuity e Disaster Recovery centrali nelle soluzioni Aruba

Dall'hosting al cloud, un percorso d'innovazione che alle imprese fornisce opzioni personalizzate e flessibili per garantire la salvaguardia e l'accesso ai dati sempre e comunque

Il brand Aruba nasce nel 2000, quale fornitore di servizi di hosting, registrazione domini e posta elettronica. Oggi Aruba, che nel 2014 si è anche aggiudicata il registro ufficiale a livello mondiale del dominio .cloud, conta in Europa su un network di sei data center: uno a Ktiš, in Repubblica Ceca, a Londra, Parigi e Francoforte e due ad Arezzo con un'offerta alle imprese che, tra le altre, comprende soluzioni di Business Continuity, Disaster Recovery, Data Center Extension, Private Cloud e Public Cloud, Disaster Recovery as a Service e soluzioni di co-location.

La Business Continuity e il disaster recovery che occorre

«Grazie ai due data center vicini, collegati in fibra ottica su percorsi stradali differenti, possiamo realizzare soluzioni di business continuity particolarmente efficaci ed efficienti: implementando l'infrastruttura primaria in un data center e quella secondaria nell'altro, infatti, possiamo replicare i dati in modalità sincrona», spiega Stefano Sordi, direttore marketing di Aruba. Questo permette di dare continui-

tà in tempo reale alle risorse di data storage e di fruibilità delle applicazioni. Inoltre, così si realizza un "mini" disaster recovery, cioè un sistema di protezione da ciò che rappresenta la quasi totalità dei "disastri" che colpiscono le imprese e i loro sistemi informatici. Ovviamente, potrebbe non essere sufficiente nel caso cadesse un meteorite, ma l'errore umano, l'incendio, il blackout smettono di essere un problema: «Il 95% e più dei disastri sono interni all'infrastruttura stessa», sottolinea Stefano Sordi, direttore marketing di Aruba, continuando: «A parte i disastri ambientali più gravi, che sono molto rari, il fatto di avere due edifici separati ai due estremi di una città permette di avere una copertura dei rischi ampia, efficace ed efficiente».

Va da sé che, qualora, si volesse proteggere l'infrastruttura anche dal "meteorite" è possibile appoggiare la soluzione di disaster recovery ai data center Aruba del Centro o Nord Europa.

In pratica, è possibile realizzare un sistema di protezione adeguato ai rischi che ciascuna azienda corre, in base al contesto di mercato in cui opera e al proprio modello di business, senza appesantire i costi delle infrastrutture o limitarne le capacità. Anzi, può altresì avve-

nire il contrario, aggiungendo innovazione grazie alla flessibilità delle soluzioni cloud di Aruba.

La flessibilità del cloud Aruba

La consistenza delle soluzioni per la business continuity e il disaster recovery è garantita da un altro punto di forza di Aruba: la flessibilità della propria offerta di soluzioni Data Center. Il provider italiano è infatti in grado di fornire ai suoi potenziali clienti una qualsiasi combinazione delle soluzioni che a oggi si possono pensare, evidenzia ancora Sordi, rimarcando un approccio aperto praticamente su misura.

In particolare, i clienti possono scegliere molteplici soluzioni fra tre tipologie di architetture:

- un'infrastruttura fisica di proprietà dell'azienda che la installa nel data center di Aruba in co-location;
- un'infrastruttura, sempre fisica e dedicata al cliente, ma basata su hardware fornito da Aruba;
- un'infrastruttura virtuale in cloud, che potrà essere pubblico o privato.

Sono quindi possibili diverse strutturazioni adottando configurazioni miste tra proprietario e non e tra fisico e virtuale. Proprio queste soluzioni ibride sono quelle che meglio permettono di soddisfare le varie esigenze, integrando ambienti legacy con piattaforme "agili" di nuova generazione e sfruttando le possibilità messe a disposizio-

ne dai tanti servizi in cloud che stanno caratterizzando la cosiddetta “digital transformation”.

Questa flessibilità è riproposta nella realizzazione di un’infrastruttura replicata per finalità di business continuity e disaster recovery, per le quali è anche possibile decidere di adottare un mix di risorse, tra pubblico e privato o tra fisico e virtuale differente per il sito secondario.

In buona sostanza, l’approccio generale di Aruba alla definizione di un adeguato sistema di disaster recovery sfocia tipicamente in tre scenari principali:

1. aziende che hanno la propria infrastruttura fisica e vogliono un disaster recovery basato ancora su un’infrastruttura fisica;
2. aziende che hanno la propria infrastruttura fisica e vogliono un disaster recovery basato su cloud;
3. aziende che non possiedono un’infrastruttura e optano per un’infrastruttura totalmente in cloud, quindi un’infrastruttura virtuale al 100% per la produzione e per la business continuity.

«Molti cloud provider forniscono soluzioni di disaster recovery chiavi in mano, ma prestabilite, mentre noi ci mettiamo attorno al tavolo con il cliente, potendo configurare qualsiasi tipo di infrastruttura per soddisfare pienamente le sue esigenze e richieste, grazie all’elevato livello di flessibilità e alla notevole diversificazione delle nostre infrastrutture», evidenzia Sordi.

Partendo dunque dalla consapevolezza, maturata in anni di esperienza, che non esiste una soluzione standard di disaster recovery applicabile a tutte le realtà di business, gli ingegneri di Aruba approcciano ogni attività come “soluzione a progetto” e, insieme al team costituito in seno al cliente, partono con una fase di pre-analisi per identificare i possibili rischi e le probabilità relative. Successi-



Stefano Sordi, direttore marketing di Aruba

vamente vengono definiti gli obiettivi del sistema e il conseguente livello di servizio da assicurare in termini di RTO (Recovery Time Objective) e RPO (Recovery Point Objective). Ciascuno dei tre scenari prima evidenziati porta vantaggi a chi li ha scelti a ragion veduta. Per esempio nel primo caso, viene attivata un’infrastruttura fisica presso il data center di Aruba, in grado di replicare ed erogare tutti o parte dei servizi del cliente. Si tratta di definire e configurare il giusto dimensionamento sulla base dell’infrastruttura “as-is” del

cliente e secondo le priorità di ripristino dei servizi. Il vantaggio, in questo caso deriva dalle risorse fisiche dedicate completamente al cliente, che potrà valutare maggiori capacità computazionali.

Nel secondo scenario, il sito di disaster recovery potrà essere realizzato in cloud con infrastruttura privata, quindi dedicata esclusivamente al cliente, o pubblica, dove le risorse sono garantite ma condivise. Il vantaggio è soprattutto determinato dalla virtualizzazione che ottimizza l’architettura in termini di hardware necessario per il disaster recovery e semplifica le operazioni di ripristino, sia in caso di effettivo disastro sia di test delle procedure. È possibile automatizzare e semplificare il failover delle macchine virtuali a livello applicativo e di storage, accelerando il processo di Disaster Recovery.

Nel terzo caso c’è la massima flessibilità e si potrà valutare, a seconda delle specificità, se realizzare un cloud privato o pubblico. I vantaggi sono massimi nel caso si scelga una piattaforma pubblica, che permette di modificare il dimensionamento dell’infrastruttura sulla base di esigenze anche momentanee e di contenere i costi. Se poi si realizzerà un cloud privato, un vantaggio si rifletterà nelle prestazioni garantite dall’ambiente dedicato. *

La sicurezza quadrimensionale di HP Enterprise Security

Un modello di sicurezza enterprise a quattro dimensioni, pensato per rispondere anche alle richieste di protezione dei nuovi ambienti virtualizzati e cloud

Per comprendere e combattere adeguatamente il cyber crime occorre pensare come l'avversario. Quali sono le nuove frontiere del crimine cibernetico organizzato? Come contrastarlo? La sicurezza va ripensata in un'ottica quadridimensionale: identificare le nuove minacce, riconoscere le diverse fasi di un attacco, rendere sicure le applicazioni ed integrare la sicurezza a livello del dato realizzando un efficace Adversary Management System. Attraverso un'offerta di soluzioni hardware e software ampia e diversificata, la divisione Enterprise Security Products (ESP) di HP, guidata in Italia da Pierpaolo Ali, mette a disposizione della aziende enterprise un insieme di componenti e strumenti adatto a rispondere alle esigenze di rilevamento delle minacce esterne e interne e a predisporre azioni di risposta che intervengono per proteggere dati, rete e applicazioni.

Grazie a una serie di centri di ricerca e l'offerta di servizi distribuiti a livello globale HP mette a disposizione delle aziende una "intelligence" di sicurezza globale e aggiornata in tempo reale che contribuisce ad accelerare la risposta a minacce e predisporre azioni proattive nei confronti di nuove minacce come le APT. Queste risorse includono laboratori, strutture di ri-

cerca (HP Security Research), competenze, piattaforme collaborative di security intelligence (HP Threat Central), risorse distribuite e una serie di soluzioni e servizi che, tutte insieme, operano in modo sinergico per analizzare costantemente a livello globale le nuove minacce, stabilire la reputazione e il livello di rischio e abilitare interventi proattivi.

HP TippingPoint Next Generation Firewall e IPS

I sistemi firewall di nuova generazione (NGFW) della gamma HP TippingPoint forniscono il livello di visibilità necessario a riconoscere quali applicazioni stanno girando sulla rete aziendale e chi sta accedendo a tali applicazioni per poi consentire di predisporre le policy richieste per bloccare e controllare le applicazioni non richieste, per contrastare il malware avanzato e le minacce APT. Per fronteggiare i rischi legati alla mobilità gli NGFW/NGIPS di HP abilitano il blocco automatico del codice nascosto o dannoso che può introdursi in rete, ricorrendo a capacità di blocco delle vie d'uscita in modo da evitare la

fuoriuscita di dati sensibili verso destinazioni "Command-and-Control". Per rispondere ai rischi introdotti dal BYOD gli utenti delle soluzioni HP TippingPoint hanno a disposizione controlli sulle policy delle applicazioni a livello granulare, che consentono anche di gestire l'interazione con le più diffuse piattaforme social. Tra i punti distintivi di queste soluzioni vi sono la capacità di analizzare enormi volumi di dati grazie a un throughput Firewall scalabile da 500 Mbps a 10 Gbps, i ridottissimi tempi di latenza e anche la semplicità d'uso le rende adatte anche alle organizzazioni prive di personale specializzato. L'affidabilità è un altro aspetto su cui HP intende rimarcare il valore dei propri dispositivi mentre, per quanto riguarda l'efficacia della propria tecnologia di protezione nel bloccare possibili minacce, HP mette sul piatto l'attività del team di ricerca di sicurezza DV Labs che ha pubblicato migliaia di filtri (vaccini digitali) per la protezione contro ogni tipo di vulnerabilità (non solo gli exploit noti) applicando tecniche di decodificazione e analisi all'avanguardia.

I sistemi per la prevenzione delle intrusioni di nuova generazione HP TippingPoint NGIPS offrono funzionalità avanzate di rilevamento delle minacce, compresa la rilevazione delle anomalie di comportamento, la reputazione IP e analisi di tipo euristico. Questi metodi di rilevamento sono necessari se si vuole sperare di scon-



HP Next Generation Firewall TippingPoint S8010F

figgere exploit su misura, attacchi zero-day e polimorfici. Inoltre, deve essere in grado di identificare ed effettuare controlli sia a livello di applicazioni sia di utenti finale. Le soluzioni appliance e virtual machine HP TippingPoint Security Management System (SMS) forniscono funzioni di gestione della sicurezza di livello enterprise a tutti i prodotti di sicurezza HP TippingPoint.

HP TippingPoint Advanced Threat Appliance (ATA)

HP TippingPoint ATA sfrutta i Next-Generation Firewall, gestiti attraverso la HP TippingPoint Security Management System (SMS), per bloccare immediatamente le minacce evitandone la propagazione attraverso la rete, spuntando una delle armi che caratterizzano l'attacco strutturato in più fasi che contraddistingue gli attacchi mirati e persistenti (i cosiddetti APT).

Questa soluzione utilizza un insieme diversificato di tecniche di rilevamento di tipo statico, dinamico e comportamentale affiancando tecniche di blocco automatizzato con sistemi di rilevazione delle minacce. L'obiettivo è quello di fornire una difesa efficace in corrispondenza o immediatamente dopo il punto iniziale di infezione (paziente zero), bloccando rapidamente ulteriori infiltrazioni e la possibile diffusione laterale e, nel contempo, predisponendo in modo automatizzato le condizioni per inibire attacchi futuri dello stesso tipo.

HP Application Defender: l'autoprotezione in cloud

HP ha introdotto nella sua offerta già da qualche tempo tecnologie di "Runtime Application Self Protection" (RASP) che consentono di analizzare il codice in tempo reale direttamente nell'ambiente di produzione e di attuare contromisure sulla base dei risultati. Tecniche RASP sono utilizzate, per esempio, nelle soluzioni HP WebInspect, HP ArcSight Application View e, in particolare, all'interno di HP Application Defender un managed service per l'autoprotezione delle applicazioni in cloud che consente alle aziende di identificare automaticamente le vulnerabilità del software e di proteggersi in tempo reale.

Le soluzioni HP Fortify per un codice sicuro

Con la gamma di soluzioni Fortify, HP ESP fornisce una risposta efficace alle esigenze di sviluppare codice sicuro, di eliminare alla fonte le possibili vulnerabilità e di predisporre ambienti di test di tipo statico, dinamico e in tempo reale

adatti a verificare le caratteristiche di sicurezza del codice.

HP Fortify predispone un approccio proattivo di Software Security Assurance per affrontare in modo sistematico il rischio di vulnerabilità nel software sulla base del principio che è più efficace e conveniente proteggere le applicazioni mentre sono in fase di sviluppo che farlo dopo che sono state rilasciate.

HP Fortify definisce quattro livelli di priorità per classificare la gravità delle vulnerabilità: critico, alto, medio e basso. I risultati delle valutazioni sono consegnati in un insieme di semplici grafici basati su un sistema coerente di valutazione, che fornisce informazioni sulla probabilità che la vulnerabilità venga identificata e sfruttata da un outsider e sull'impatto in termini di danno potenziale che un malintenzionato potrebbe arrecare al patrimonio aziendale, sotto forma di perdita finanziaria, violazione della conformità, perdita di reputazione del marchio, pubblicità negativa o altro. HP Fortify è disponibile anche come servizio on demand.



La dashboard di HP Fortify on Demand

La gamma Atalla

La gamma di soluzioni Atalla abilita un approccio alla protezione dei dati che sfrutta tecniche innovative di cifratura, proteggendo i dati on premises e nel cloud e rendendo sicure le transazioni elettroniche. **HP Atalla Cloud Encryption** è la soluzione che combina cifratura allo stato dell'arte implementata su appliance (fisica o virtuale) con una tecnologia brevettata di gestione delle chiavi progettata per proteggere i dati critici in ambienti cloud di tipo pubblico, ibrido e privato. Questa soluzione permette di crittografare l'intero layer dei dati, inclusi i principali database (Oracle, MySQL, Microsoft SQL Server e IBM DB2), i file e lo storage distribuito all'interno di un Cloud pubblico, ibrido e privato con chiavi che non risultano mai esposte in modo vulnerabile.

HP Atalla Information Protection and Control (IPC) mette a disposizione una serie di soluzioni per la classificazione e la protezione delle informazioni all'interno dell'organizzazione aziendale. L'offerta HP Atalla IPC include software di gestione, reporting e analytics, moduli per la protezione di file e cartelle, protezione dei dati delle applicazioni, protezione della posta e dei dati non strutturati multi-formato. HP Atalla fornisce anche una gamma di soluzioni di sicurezza per pagamenti e transazioni elettroniche basata su due componenti che operano congiuntamente: il modulo di crittografia hardware

HP Atalla Network Security Processor (NSP) e il sistema sicuro di gestione delle chiavi HP Enterprise Secure Key Manager (ESKM).

Le soluzioni HP ArcSight

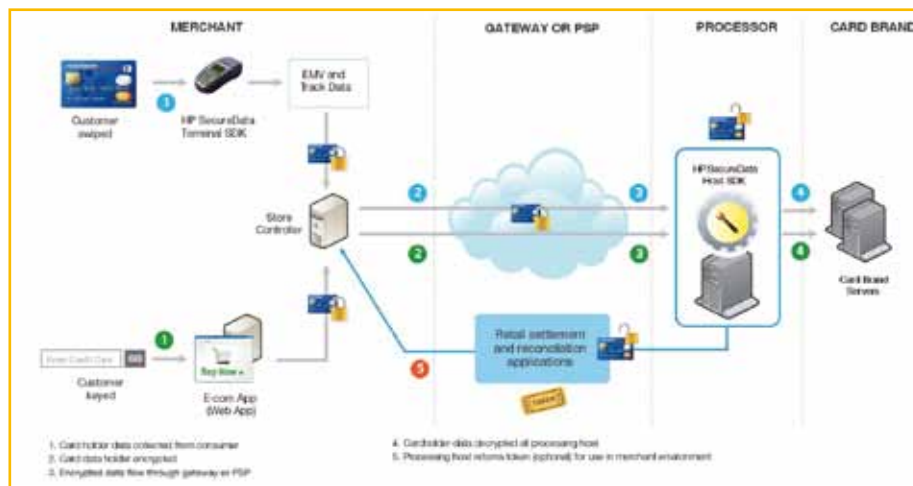
HP ha raggruppato all'interno della famiglia ArcSight le soluzioni software indirizzate a proteggere i dati attraverso il monitoraggio, l'analisi e la correlazione di eventi di sicurezza provenienti da differenti tipologie di sorgenti. Nel suo complesso ArcSight rappresenta una piattaforma integrata di Security Intelligence e Risk Management in grado di abbinare le funzionalità di un Sistema di gestione delle informazioni e degli eventi di sicurezza (SIEM) con un approccio preventivo basato su un modello di analisi intelligente delle minacce, effettuato su scala globale attraverso una serie di servizi predisposti da HP. La piattaforma HP ArcSight Security Intelligence fornisce visibilità sulle attività che interessano l'intera infrastruttura enterprise correlando log, ruoli dell'utente e flussi di rete per individuare eventi legati alla sicurezza in base ai quali definire priorità e predisporre risposte efficaci e preventive a minacce di vario tipo. Attraverso una console di sicurezza unificata e centralizzata (HP ArcSight Management Center) è possibile configurare, distribuire e gestire l'analisi dei Log su deployment a larga scala e fornire funzioni unificate di gestione delle modifiche. L'elemento centrale e abilitante di questa fa-

miglia di soluzioni è il motore di analisi per la gestione di minacce e rischi **HP ArcSight ESM**, una soluzione SIEM per la raccolta, l'analisi e la correlazione delle informazioni di sicurezza e degli eventi di rischio, la protezione delle applicazioni e la difesa della rete e per il Governance, Risk management and Compliance (GRC). All'interno di questa famiglia va segnalata anche **HP ArcSight Application View**, una soluzione per la visibilità sugli eventi di sicurezza delle applicazioni che combina le funzionalità di HP Fortify e di ArcSight ESM. HP ArcSight Application View controlla automaticamente le applicazioni per fornire un'analisi intelligente sulle minacce combinando i log degli eventi di sicurezza generati dalle diverse applicazioni, incluse quelle legacy o personalizzate che, in molti casi, non sono state progettate per fornire capacità di registrazione dei log.

HP Security Voltage

La più recente aggiunta al portafoglio di sicurezza HP è la gamma di soluzioni HP Security Voltage, risultato dell'acquisizione avvenuta nel 2015 di Voltage Security. HP Security Voltage mette a disposizione una gamma di soluzioni per la crittografia dei dati e la gestione di token di sicurezza per proteggere i dati associati alle carte di credito e di debito, le informazioni personali e per garantire la conformità allo standard PCI (Payment Card Industry).

Schema generalizzato del flusso di pagamento con cifratura dei dati del titolare della carta di credito e gestione dei token



Alla base di queste soluzioni vi sono due tecnologie brevettate. La prima è HP Format-Preserving Encryption (FPE) una soluzione di crittografia che si differenzia da altri metodi per il fatto di non alterare il formato originale dei dati. Questo permette alle applicazioni, ai processi di analytics e ai database di utilizzare i dati protetti senza alterazioni, anche attraverso sistemi, piattaforme e strumenti distribuiti. HP FPE preserva l'integrità referenziale, il che significa che i dati protetti possono ancora essere referenziati e uniti in

modo consistente attraverso tabelle e data set: un requisito importan-

te per operazioni che interessano insiemi di dati inseriti in Hadoop e particolarmente critico quando vengono utilizzati identificatori comuni come il codice fiscale o la carta di identità come riferimenti comuni tra insiemi di dati diversi. Voltage Secure Stateless Tokenization (SST) è una tecnologia di gestione dei token di sicurezza per la protezione dei dati delle carte di pagamento. La tecnologia SST elimina il database del token; infatti le tabelle dei token sono pre-generate e possono risiedere in molteplici data center e operano nella memoria di sistema. In questo modo si elimina la necessità di memorizzare i dati del titolare della carta o altri dati sensibili e si migliora velocità, scalabilità, sicurezza e gestibilità del processo di gestione dei token. Le due tecnologie FPE e SST proteggono i dati in modo trasparente, abilitando un deployment rapido con cambiamenti nulli o minimi delle applicazioni esistenti. *

Le soluzioni HP Voltage

L'offerta HP Voltage comprende una serie di soluzioni pensate per sfruttare in modo ottimizzato le tecnologie di crittografia e gestione dei token tecnologie HP FPE e HP SST.

L'offerta comprende:

- **HP SecureMail:** una soluzione end-to-end di crittografia per la posta elettronica per soluzioni desktop, cloud e mobile pensata per mantenere sicure e riservate le informazioni personali e private.
- **HP SecureData Enterprise:** una soluzione end-to-end pensata per proteggere i dati aziendali nel loro ciclo di vita durante la loro cattura, elaborazione e memorizzazione attraverso una varietà di dispositivi, di sistemi operativi, di database e di applicazioni. Utilizza le tecnologie FPE e SST e prevede una gestione trasparente delle chiavi di crittografia.
- **HP SecureData Payments:** una soluzione per la protezione dei dati dei titolari di carta di credito a partire dal momento della loro acquisizione fino al sistema di elaborazione del pagamento. Fornisce una protezione persistente dei dati che non si limita alle fase dei flussi autorizzativi, ma che si estende anche alle applicazioni di back office e ai processi che interessano il titolare della carta di credito.
- **HP SecureData Web:** una soluzione per la sicurezza dei pagamenti e la riservatezza dei dati personali nelle transazioni basate su browser. Sfrutta la tecnologia Page-Integrated Encryption (PIE), che codifica i dati nel browser al momento della cattura e li mantiene protetti durante tutto il percorso attraverso il Web, il livello applicativo, l'infrastruttura cloud, i sistemi e le reti a monte, fino all'host di destinazione dove possono essere decifrati in modo sicuri.
- **HP SecureFile:** utilizza tecnologia di crittografia persistente per proteggere file e documenti sensibili archiviati, in uso o in transito. HP SecureFile può essere implementata come applicazione desktop, come processo di crittografia in modalità batch o essere integrata con i portali di collaboration.

I servizi BT per ripensare la protezione

L'offerta BT Assure abilita una difesa globale e proattiva della rete, dei dispositivi e delle applicazioni per ridurre al minimo i rischi cibernetici

Realizzare e mantenere un'infrastruttura dedicata alla sicurezza che sia continuamente e tempestivamente aggiornata contro i rischi conosciuti e quelli che continuamente appaiono è un compito sempre più difficile e oneroso.

È quello che si è proposta di fare BT con BT Assure, un servizio alle aziende che si basa sull'analisi continua di un ampio insieme di dati, che permette di identificare i nuovi attacchi e i pattern ed evidenziare le anomalie in modo proattivo al fine di intervenire tempestivamente.

I servizi compresi in BT Assure esaminano, controllano e correlano una vastissima categoria di eventi, integrando le informazioni provenienti da diverse sorgenti. Gli elementi principali di BT Assure realizzano:

- L'integrazione delle informazioni provenienti da più sorgenti.
- L'analisi basata su un mix di in-

telligenza artificiale e umana con visualizzazione in tempo reale e interattiva dei risultati.

- L'identificazione dei pattern e dei link interessati da un attacco.
- La notifica automatica di malfunzionamenti, anomalie riscontrate nel comportamento delle applicazioni, threat potenziali e attacchi in atto.

I paragrafi seguenti illustrano alcuni dei servizi compresi nel portfolio BT Assure.

BT Assure Managed Cloud per proteggere il traffico Web

BT Assure Managed Cloud è un servizio che supporta e rende sicure le differenti modalità di lavoro dei dipendenti e le diverse esigenze di connettività. Permette ai dipendenti, indipendentemente da dove si trovano e dal tipo di tecnologia utilizzata, di accedere in modo sicuro alle risorse aziendali.

Il servizio è basato sul cloud e garantisce una protezione consistente e in linea con le policy aziendali per le diverse tipologie di utenti ed applicazioni, sia all'interno che all'esterno della rete aziendale, inclusi utenti e dispositivi mobili. Tra le più salienti funzionalità che lo caratterizzano vi sono:

- Difesa contro malware Web-based.
- Protezione di informazioni confidenziali evitando che possano uscire dalla rete aziendale.
- Utilizzo di applicazioni Web, come Facebook, senza dover bloccare l'intero sito.
- Possibilità di prevenire l'uso di applicazioni che aumentano il rischio o riducono la produttività.
- Possibilità di attivare rapidamente nuovi utenti o nuove funzionalità.

BT Assure Denial of Service Mitigation

BT Assure Denial of Service Mitigation è un servizio che BT ha ideato per proteggere da attacchi cibernetici che inondano di tentativi di accesso

o di operazioni il sito target o l'applicazione Web al fine di renderli non operativi. In una tale evenienza il servizio BT Assure blocca l'attacco elimi-



I servizi disponibili con BT Assure

nando il traffico non convenzionale. La funzione di protezione si attiva e interviene automaticamente non appena viene rivelato un volume o un tipo di traffico anomalo. Immediatamente ha inizio il processo che separa il traffico DDoS dalle normali transazioni. Qualsiasi tipo di richiesta considerata non sicura viene reindirizzata al sistema di Threat Management mentre le richieste sicure sono inoltrate in modo trasparente a destinazione. L'identificazione dell'attacco è istantaneo e richiede solo pochi millisecondi e, evidenzia BT, l'indirizzo IP sotto attacco non sperimenta nessun tipo di fuori servizio percepibile, indipendentemente dalla dimensione o dalla frequenza con cui l'attacco è portato. Non ultimo, il servizio ha una struttura modulare che permette di aggiungere e pagare i differenti livelli di protezione disponibili in base alle effettive esigenze.

BT Assure Threat Defence

Le soluzioni di protezione standard, come i firewall (tradizionali e di nuova generazione), i sistemi di intrusion prevention, gli anti-virus e i gateway Web sicuri si occupano della ricerca degli attacchi inbound, che sono solo la prima mossa di un attacco. Questi sistemi, per identificare e bloccare le minacce, si affidano essenzialmente alle cosiddette "signature" ed ai pattern di aggressione già noti. Questo è causa di gravi debolezze nelle difese della rete, che re-

stano vulnerabili agli attacchi di tipo "zero-day" e targeted APT (Advanced Persistent Threat).

Un monitoraggio efficace della sicurezza di rete, osserva BT, deve basarsi innanzitutto sull'individuazione dei problemi quando sono ancora di dimensioni ridotte, prima che questi si aggravino e arrivino ad impattare negativamente il business. Per una protezione in tempo reale, il servizio di BT di monitoraggio real-time e di correlazione provvede a monitorare tutti i device che si trovano sulla rete e, sempre in tempo reale, fornire gli alert. Questo significa che gli attacchi possono essere bloccati prima che siano in grado di causare danni gravi.

BT Assure Threat Defence identifica automaticamente le diverse fasi di una minaccia avanzata attraverso il monitoraggio del traffico di rete. Con l'attività di behavioural analysis è possibile ad esempio identificare le fasi di obfuscated exploitation, di payload download e di command and control exfiltration che compongono l'attacco, insieme alle minacce nascoste e all'attività criminale che coinvolge la rete. BT Assure Threat Defence è specificamente progettato per ricercare gli attacchi mirati ("targeted") avanzati, con lo scopo di prevenire e proteggere dalle minacce che eludono i sistemi di sicurezza perimetrale esistenti, e che potenzialmente mettono gli endpoint infetti sotto il controllo di chi ha posto in essere gli attacchi.

BT Assure Threat Monitoring

BT Assure Threat Monitoring è un servizio sviluppato da BT per le aziende che hanno l'esigenza di sapere cosa avviene nella propria rete 24 ore al giorno in modo da non mettere a rischio il proprio sistema informativo e gli utenti. Il servizio provvede a monitorare il comportamento dei dispositivi di rete quali i sistemi di rivelazione delle intrusioni, di prevenzione delle intrusioni, firewall, router, server, mainframe o pc. Il monitoraggio fa uso di un data base che comprende i threat conosciuti e del supporto di un team globale worldwide di analisti esperti specializzati nel suggerire come proteggere le infrastrutture aziendali. Il servizio prevede anche la possibilità di gestire in completo outsourcing tutti gli aspetti connessi al management di un ambiente IT. L'obiettivo del servizio sviluppato da BT è quello di garantire la rivelazione di attacchi interni od esterni apportati alla rete prima che questi arrechino danni, in modo da eliminare i costi connessi al ripristino delle loro conseguenze. Tra gli obiettivi principali del servizio vi è anche quello di eliminare i falsi positivi che impegnano risorse aziendali, in modo che queste possano dedicarsi e intervenire esclusivamente in caso di reale necessità. Non ultimo, permette di essere "compliant" con le normative e pronti con i dati necessari alle attività di auditing. *

La security intelligence di F-Secure

Una protezione a 360 gradi con il supporto del cloud e con le soluzioni di Analytics sui dati della sicurezza, senza trascurare la mobility

La crescita della mobility aziendale come strumento atto a favorire il business porta a un costante incremento sia del volume e della qualità dei dati residenti sui dispositivi mobili sia, complice in questo le nuove reti a larghissima banda, di quelli scambiati tramite connessioni di rete e sul cloud.

La conseguenza più evidente, osserva F-Secure, è che l'utilizzo che un dipendente fa del proprio dispositivo mobile e come ne protegge i dati e le comunicazioni sta ponendo serie sfide ai manager IT. È una sfida che interessa sia quanto concerne la gestione dei dispositivi sia quanto relativo alle policy per l'accesso alle applicazioni interne alla rete aziendale.

Il problema però è ancora più complesso, perché al rischio di perdere dati sensibili si aggiunge quello di essere "compliant" alle severe normative nazionali in termine di conservazione, protezione o di inalterabilità dei dati sensibili, normative che includono anche la responsabilità diretta del manager che gestisce i dispositivi e si estende sino all'alta direzione.

È da questa considerazione e in base ai dati emersi da una sua recente ricerca che deriva la strategia posta in atto da F-Secure, una socie-

tà di valenza internazionale il cui core business è focalizzato sulle soluzioni di cyber security, per una mobilità aziendale sicura e a prova di hacker.

I dati in proposito parlano chiaro, osserva F-Secure. Si è in presenza di un forte incremento nel numero di malware. Nel solo secondo semestre del 2014 sono state identificate 259 su un totale di 574 varianti conosciute della famiglia SmsSend, che risulta il mobile malware in più rapida crescita. SmsSend infetta dispositivi Android con un trojan che invia messaggi SMS a numeri Premium-Rate. Il Ransomware ha poi continuato a colpire gli utenti mobili, con le famiglie Koler e Slocker identificate come le più diffuse minacce per i dispositivi Android. I danni economici derivanti alle flotte aziendali infettate possono essere molto consistenti. Ma non è solo questione di spese di comunicazione. Il Ransomware usa la crittografia o altri meccanismi per bloccare l'uso dei dispositivi stessi da parte degli utenti e questo può portare a impossibilità di comunicare e a creare seri problemi nella gestione del work flow e nelle relazioni di business. Il problema di come proteggere efficacemente dispositivi e dati è poi aggravato dal fatto che i dipendenti, soprattutto quelli delle generazioni più recenti e i più creativi, vogliono poter usare per

il business il dispositivo mobile a loro più familiare in linea con il paradigma BYOD. L'adozione del BYOD può però implicare una più che sensibile riduzione del grado di sicurezza dell'infrastruttura IT.

La risposta di F-Secure ai problemi esposti si è concretizzata in Freedom for Business, un suo nuovo servizio dedicato specificatamente alle aziende.

Freedome for Business (F4B) per una mobility sicura e flessibile

Freedome for Business (F4B) è un servizio che F-Secure ha ideato per rispondere contemporaneamente sia alle crescenti esigenze di sicurezza espresse dalle aziende che alle richieste di flessibilità da parte dei dipendenti. Nella sua articolazione generale, rappresenta la versione per le aziende dell'app consumer Freedom, arricchita con funzionalità definite appositamente per rispondere alle necessità dell'attuale modo di condurre il business.

Di Freedom la soluzione conserva l'interfaccia per attivare i criteri di sicurezza con un solo bottone della versione consumer, ma a questa aggiunge un set molto ampio, e studiato per le aziende, di funzionalità che sono di ausilio nell'assicurare la sicurezza delle reti e dei dati aziendali.

Il software F4B integra in un solo servizio di sicurezza basato su cloud tre differenti tipi di protezione che sono essenziali per le aziende:

Con Freedom for Business la sicurezza di dati e applicazioni viaggia con il dispositivo. Basta premere un bottone per attivare le funzioni di comunicazione sicura

- comunicazioni crittografate;
- sicurezza del Web e delle applicazioni;
- gestione dei dispositivi mobili aziendali.



Dal punto di vista del dipendente mobile è sufficiente,

come evidenziato, premere un bottone per attivare il software di sicurezza e poter iniziare il proprio lavoro in modo sicuro, a prova di attacchi e su connessioni protette.

I paragrafi seguenti esaminano in dettaglio gli aspetti chiave di F4B e i benefici che dal suo utilizzo derivano per il business, la sicurezza e la flessibilità aziendale.

Una policy per gestire i dispositivi basata su cloud

Rendere più sicura la mobility è semplice, osserva F-Secure. Le aziende possono implementare Freedom for Business partendo dalla suite F-Secure Protection Service for Business (PSB) basata sul cloud che Freedom for Business estende alla protezione dei dispositivi mobili che si connettono alla rete aziendale.

Una volta attivate le funzionalità premendo un bottone, F4B provvede a crittografare le comunicazioni dei dipendenti e a proteggere le loro applicazioni e la navigazione in Internet. Per garantire che il dispositivo usato nell'ambito della pro-

pria funzione di lavoro sia sicuro e protetto il servizio fornisce anche la capacità di implementare funzioni aggiuntive di sicurezza.

Gli IT Manager hanno inoltre la possibilità di rilevare lo stato di sicurezza dei dispositivi e se viene notato un numero eccessivo di visite a siti potenzialmente pericolosi sono in grado di intervenire e affrontare il problema prima di incorrere in un possibile incidente o importare infezioni nella rete aziendale.

F4B è, ai fini pratici, una soluzione di gestione della flotta in modo globale che si fa carico della gestione della sicurezza di tutti i dispositivi di utente sia fissi che mobili, sia basati su sistema operativo Android che iOS.

In particolare, la funzionalità "antifurto" permette agli IT Manager e ai responsabili della security di effettuare operazioni quali il blocco immediato dei dispositivi o cancellare da remoto i dati residenti nel dispositivo quando viene acceso e si connette alla rete.

La funzione ricopre un ruolo chiave nel garantire la protezione di dati

sensibili perché protegge le aziende contro le possibili violazioni di dati causate dal furto o dal semplice smarrimento dei dispositivi.

Le aree di intervento del servizio F4B

Le aree principali di intervento del servizio di gestione e di sicurezza per dispositivi mobili Freedom for Business sono quattro e interessano i seguenti temi:

- **Gestione della flotta:** F4B fornisce un'estesa visibilità sullo stato della sicurezza dei singoli dispositivi mobili e integra gli strumenti per gestire e proteggere sia i dati che i dispositivi.
- **Sicurezza per le comunicazioni su reti Wi-Fi:** F4B permette di proteggere le connessioni e i dati dei dispositivi mobili tramite anti-malware di ultimissima generazione, VPN personali e crittografia.
- **Anti-Malware di ultimissima generazione:** F4B prevede robusti criteri di protezione contro le applicazioni dannose senza causare, evidenzia F-Secure, percepibili rallentamenti nei dispositivi o nel consumo della batteria.
- **Rimozione dei dati sensibili e gestione centralizzata di passcode:** F4B protegge con password l'accesso ai dati e permette la cancellazione remota dei dati residenti nel dispositivo. Inoltre, permette di applicare passcode in tutta la flotta. *

Fujitsu protegge data center e device

Protezione diffusa, tecnologie biometriche, robuste modalità di cifratura ed evolute tecniche RAID proteggono i dati e l'accesso alle applicazioni business

Nell'ambito di quello che rappresenta il mercato della sicurezza inteso in termini generali, Fujitsu ha sviluppato un'estesa offerta di soluzioni per la protezione e la sicurezza del dato.

A quelle che sono proprie tecnologie aggiunge poi, in progetti di ampio respiro, anche prodotti hardware, software o appliance di terze parti qualificate quali dispositivi specifici come firewall, antivirus o anti malware. Posizionata tra i produttori leader nella ideazione e fornitura di soluzioni, prodotti e servizi in ambito IT, è una società particolarmente attenta agli aspetti di sicurezza, aspetti insiti in tutti i suoi prodotti per garantire l'accesso sicuro al dato e contemporaneamente anche la sua disponibilità e la certezza che chi vi sta accedendo sia abilitato a farlo. La sicurezza, come evidenziato, è in ogni caso un termine ampio che comprende sicurezza fisica e logica e Fujitsu vi è impegnata sotto svariati punti di vista. Ad esempio, pur non essendo come evidenziato concentrata sulla Sicurezza in senso stretto, ha brevettato e portato sul mercato numerose tecnologie che inserisce nei suoi dispositivi e soluzioni o è fruibile stand-alone per il controllo degli accessi fisici. Ad esempio, il Palm-Secure che provvede alla mappatura e al riconoscimento biometrico

del reticolo venoso del palmo della mano e viene usata per diversi scopi: dal controllo dell'accesso fisico ad edifici e data center alla identificazione della persona ed è già utilizzato in diversi progetti come in Turchia nell'ambito della sanità, in Brasile in ambito bancario, e nell'ambito di progetti di fraud prevention e identificazione della persona.

«Per specifici ambiti tecnologici ci avvaliamo di partnership e di collaborazioni con terze parti, come Brocade, Cisco per tutta la parte networking o Symantec e CommVault per il software di backup e archiviazione, oppure altri produttori che sono specifici per certi ambiti di soluzione inerenti la sicurezza», ha evidenziato Roberto Cherubini, IT Architect Consultant di Fujitsu Italia.

Roberto Cherubini,
IT Architect Consultant, Fujitsu Italia



La sicurezza del dato inizia dalla sua disponibilità

Parlare di sicurezza di un dato, evidenzia Fujitsu, implica necessariamente la sua disponibilità. In sostanza, nell'ambito di una fornitura di prodotti e soluzioni che consentono la fruizione di applicazioni coesistono necessariamente diversi aspetti. Facendo riferimento a una infrastruttura generica, chi utilizza dispositivi di client computing, come notebook, tablet, pc o smartphone riceve servizi ed informazioni forniti da applicazioni e, in generale, da un data center.

Questo implica che bisogna assicurare, da un lato la parte di identificazione e autenticazione dell'utente per poter garantire l'accesso ai dati solamente a chi è effettivamente abilitato, e dall'altra parte, per le componenti costituenti il data center, bisogna assicurare la protezione del dato sia per quanto concerne l'accesso sia per quanto riguarda la sua disponibilità.

«Va considerato che, al giorno d'oggi, uno dei principali elementi costitutivi del data center è, per vari motivi, lo storage. Questo perché sicuramente c'è una crescita enorme dei dati, ma anche perché la virtualizzazione dei data center è oramai estremamente diffusa e le macchine virtuali sostanzialmente sono dei file che risiedono nello storage. In buona misura, lo storage diventa il punto focale per quello che riguarda la disponibi-

lità del dato, e quindi da questo punto di vista le nostre soluzioni di storage si sono dotate ed arricchite nel tempo di tutte quelle tecnologie che ne garantiscono la disponibilità. Per esempio è un fatto scontato che ci sia una protezione RAID ma il nostro storage è forse tra quelli che ne garantisce il maggior numero come tipologia», osserva Cherubini.

Al di là di tutto questo entrano poi in gioco le soluzioni e i software che garantiscono la ridondanza del dato nonché la possibilità di costruire l'architettura IT in un'ottica di Business Continuity e di Disaster Recovery, il tutto con l'obiettivo di garantire diversi livelli di servizio a fronte di eventuali fault sia del dispositivo che del data center.

Ma nello storage Fujitsu sono insiti anche altri tipi di garanzie e di protezione del dato. Per esempio, Fujitsu ha reso disponibile nei suoi dispositivi la funzione software di "Data Block Guard" che aggiunge un codice di controllo di 8 byte ad ogni scrittura di un blocco di 512 byte di dati sullo storage (rimuovendolo in fase di lettura), aggiungendo, a quelli esistenti, un livello di controllo superiore per la protezione e la consistenza del dato.

Non è l'unico meccanismo adottato da Fujitsu. Quello denominato Drive Patrol provvede a controllare periodicamente, in background, lo stato dei dischi per verificarne la piena funzionalità, in modo da pre-

venire failure e assumere decisioni prima che si guasti ed entri in gioco la ricostruzione RAID.

Se è vero, peraltro, che esiste la protezione offerta dalla tecnologia RAID è parimenti vero, evidenzia Fujitsu, che con l'aumento della capacità dei dischi (si è arrivati ai 6TB) la ricostruzione di un disco mediante RAID può comportare tempi molto lunghi, ad esempio una settimana o anche più. Questo perché il sistema comunque continua ad essere acceduto dalle applicazioni di business.

«Lo studio di questo problema ci ha fatto realizzare un meccanismo detto Fast Recovery, che è proprio di Fujitsu, e che consente di abbattere fortemente il tempo richiesto per la ricostruzione del dato in caso di fault in modo tale che l'impatto di un evento sfavorevole risulti il minore possibile», ha evidenziato Cherubini.

Quello alla base di Fast Recovery è un meccanismo proprio di Fujitsu legato al RAID6. Fondamentalmente consiste nel disporre all'interno di ogni disco del gruppo RAID di un'area riservata destinata a essere scritta in parallelo nel momento in cui si deve ricostruire il disco. L'effetto pratico è quello di ridurre drasticamente i tempi di ripristino (da 1/6 alla metà del normale tempo). Ad esempio nel caso di un disco da 1TB si passa dalle 9 ore a 90 minuti. Poiché le applicazioni accedono allo storage continuamente, in quanto è impensabile sospendere l'operatività, abbattere

i tempi della ricostruzione dei dischi è fondamentale per l'efficienza del sistema IT e la produttività aziendale.

Un'altra possibilità disponibile nelle piattaforme Fujitsu è quella di encryption per la singola LUN. È una funzione disponibile in modo nativo nello storage che l'azienda fornisce e che permette di cifrare in modo selettivo le singole LUN, lasciando la libertà all'utilizzatore di decidere quale LUN criptare o meno.

Una ulteriore possibilità consiste nell'uso di dischi self-encrypting (SED), ma in questo caso viene criptato l'intero contenuto del disco e non si ha la possibilità di decidere quale LUN criptare.

Nel portfolio Fujitsu sono compresi anche item di sicurezza per il controllo dell'accesso al dispositivo di storage, come ad esempio i meccanismi di RBAC (Role Based Access Control), per cui si consente agli utenti di fruire esclusivamente delle operazioni abilitate dal loro profilo. L'interazione può avvenire mediante GUI (mediante protocollo HTTPS) o mediante CLI (protocollo SSH).

Nel loro complesso, quelli illustrati, sono tutti meccanismi connessi alla sicurezza e volti a far sì che l'apparato di storage, intrinsecamente tramite i suoi dispositivi di recovery per la protezione del contenuto da eventuali fault, ma anche di sicurezza dell'accesso, goda di una protezione degna del fatto che al suo interno risiedono dati



Notebook protetto tramite PalmSecure

aziendali, dati personali e delle applicazioni. Dati che poi verranno forniti alle applicazioni di business perché gli utenti che dispongono di dispositivi client computing possano fruire in modo certo e sicuro del servizio che richiedono.

Big Data Analytics nel futuro della sicurezza

Continua in casa Fujitsu l'impegno nel far fronte anche a quella che è la vita quotidiana di un'azienda, con la fornitura di soluzioni sempre più efficaci e intelligenti in

modo tale da prevenire la "disruption" di informazione e dei dati, e la conseguente riduzione di efficienza e business.

Questo si traduce nella ricerca e sviluppo di soluzioni di data backup e di data recovery che siano sempre più efficienti ed efficaci, facendo leva e supportando tecnologie che prevedono la deduplica del dato in maniera tale che le finestre temporali per realizzare backup ed eventuali recovery risultino estremamente ridotte. «In un'ottica generale il trend nell'ambito della

sicurezza e disponibilità del dato verso cui stiamo muovendo, anche con la collaborazione di diverse aziende, visto che il tema è sempre più ampio e globale, è quello del Big Data Analytics, che è volto a permettere di attuare una reazione molto veloce non appena si percepisce che ci sono attacchi massicci in atto oppure a individuare quali tipi di attacchi possono essere prevedibilmente portati per mettere fuori uso client o istituzione di qualsiasi genere esse siano», ha dichiarato Cherubini. *

Più disponibilità nei data center con gli UPS di Socomec

Il produttore propone una gamma di UPS modulari, ad alta efficienza e sostituibili a caldo, che aumentano l'affidabilità e riducono i tempi di ripristino

Sono quasi 100 anni che Socomec è attiva sul mercato. Oggi la multinazionale si presenta con un fatturato globale di circa 500 milioni di Euro, un'offerta a catalogo di quasi 18mila prodotti e un'organizzazione strutturata nelle quattro divisioni: Critical Power, Solar Power, Power Control & Safety, Energy Efficiency. Distribuita a livello globale, Socomec in Italia è presente con sedi a Firenze, Roma, Milano, Padova e Vicenza.

All'interno della divisione Critical Power si inserisce l'offerta di soluzioni UPS dedicate ai data center. L'esperienza di Socomec in questo settore parte da lontano: è del 1968, infatti, la produzione del suo primo UPS. L'offerta ora si concentra, come spiega Giancarlo Battini, Southern Europe Regional Managing Director, nel conseguire più compattezza e massima efficienza a prezzi competitivi.

Socomec evidenzia come, a livello tecnologico, due siano le direttrici principali verso cui tradizionalmente si indirizza l'evoluzione degli UPS.

La prima è quella del miglioramento delle prestazioni elettriche attraverso l'incremento di potenza attiva e di rendimento: con rendimenti ormai al 96%, le possibili evoluzioni in questa direzione sono limitate. Il secondo è quello della modularità che, spiega Valente, lascia più spazio al processo di innovazione. Un tema che è correlato direttamente alla disponibilità in base alla relazione che vede la disponibili-

tà percentuale di un UPS crescere all'aumentare del tempo medio tra due guasti successivi, parametro solitamente indicato con la sigla MTBF (Mean Time Between Failures) e diminuire alla riduzione del tempo medio di ripristino MTTR (acronimo di Mean Time To Restore).

L'approccio modulare di Socomec consente una scalabilità non solo in termini di potenza ma anche di autonomia: aspetto quest'ultimo fondamentale, dato che le statistiche indicano che l'80% dei problemi legati agli UPS è solitamente correlato alle batterie. «L'adozione di un sistema parallelo modulare - spiega Valente - evita di collegare l'intero carico a un unico dispositivo UPS, consentendo di distribuirlo su più sistemi collegati tra loro. In questo modo la soluzione è in grado di supportare anche il failure di uno dei moduli senza che questo comprometta il supporto al carico».

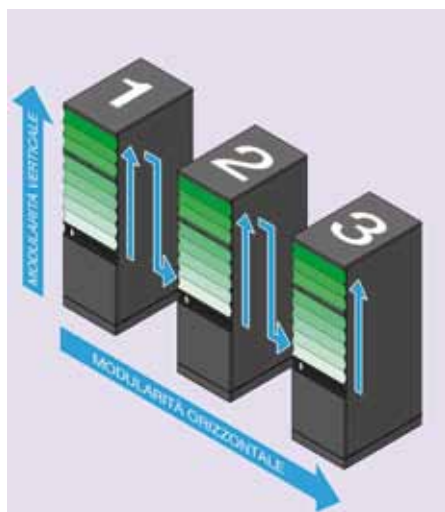
Socomec propone un ulteriore perfe-

zionamento di questo modello utilizzando non solo moduli di potenza ad alto rendimento ma anche sostituibili a caldo: un'operazione, quest'ultima, che richiede 5 minuti e che può essere effettuata anche dall'utente senza la presenza di personale tecnico specializzato.

Grazie all'approccio modulare parallelo, unito alla funzionalità hot swap, Socomec sostiene di aver ridotto il MTTR da 48 ore a 3 ore, con un conseguente incremento del livello di disponibilità.

La modularità delle soluzioni UPS di Socomec è di tipo sia orizzontale sia verticale. La gamma Modulys GP permette un'elevata scalabilità in potenza per estensioni non programmate. La potenza installata per singolo sistema può raggiungere i 200 kW aggiungendo moduli di potenza a step di 25 kW, favorendo le politiche di costo e il rendimento. Con la configurazione in modularità orizzontale è possibile ottenere la massima flessibilità collegando fino a 3 sistemi in parallelo, ottenendo una potenza complessiva di 600 kW.

L'ultima novità riguarda la gamma Delphys Xtend GP, un sistema scalabile fino a 1200 kW tramite unità di potenza da 200 kW che si avvale della tecnologia ad alta efficienza Green Power 2.0 e che prevede un sistema di cablaggio in ingresso e uscita molto semplice che favorisce l'espansione. *



Gli UPS Socomec abilitano una modularità sia verticale sia orizzontale

Data center always-on e ripristino rapido nella mission di Veeam

Attraverso le proprie soluzioni software l'azienda mette a disposizione funzioni per garantire la continuità operativa, elevando lo standard della sicurezza

Fondata negli USA nel 2006 e con sede attuale in Svizzera, Veeam Software nella sua mission ha fatto proprie le sfide che le aziende si trovano oggi ad affrontare per garantire una operatività di business di tipo Always-On.

Con lo sviluppo della soluzione Veeam Availability Suite, si propone di fornire un ripristino dei dati ad alta velocità, l'eliminazione della possibilità della perdita dei dati, la protezione certa delle informazioni, l'ottimizzazione dei dati e un'approfondita visibilità dello stato del sistema.

Veeam Availability Suite comprende anche Veeam Backup & Replication, un software che sfrutta la virtualizzazione, lo storage, e le tecnologie cloud che consentono a un moderno data center di permettere alle organizzazioni di risparmiare tempo, diminuire i rischi e ridurre sensibilmente sia le spese in conto capitale che quelle operative.

Il problema che si deve affrontare per rispondere alla sfida dell'always-on e dell'efficienza, è che

buona parte delle soluzioni tradizionali ancora in uso sono state progettate per lavorare sulla base di silos tecnologici e non in base al concetto di virtualizzazione e cloud e sono pertanto complesse da implementare e da gestire e tali da richiedere tempi anche lunghi e procedure complesse per il backup, il recovery e i processi di business continuity.

È a tutto questo che si propone di porre rimedio la piattaforma Veeam, che ha una architettura nativa adatta per i nuovi ambienti virtuali e software defined, in modo da consentire la flessibilità che oggi viene richiesta al reparto IT dalle altre Line Of Business, che hanno la necessità di disporre di un IT che permetta un utilizzo dinamico dell'hardware e una disponibilità continua dei dati di business.

La Veeam Availability Suite

Veeam Availability Suite è un prodotto software che combina le capacità di backup, ripristino e replica del software Veeam Backup & Replication con le funzionalità di monitoraggio, reportistica e capacity planning di Veeam ONE.

La Suite comprende, evidenzia Veeam, le funzionalità che servono per proteggere e gestire in modo affidabile ambienti VMware vSphere e Microsoft Hyper-V.

Tra le funzionalità più salienti di Veeam Backup & Replication volte a garantire la protezione e la disponibilità del dato vi sono quelle per il:

- **Backup degli Snapshots (HP e NetApp):** permette di creare backup veloci dagli snapshot storage.
- **Integrazione con EMC Data Domain Boost:** aumenta sino al 50% la velocità dei backup e di sino a un ordine di grandezza la creazione e trasformazione di backup full sintetici.
- **Cloud Connect:** permette di creare una replica dei dati nel cloud senza dover investire in un secondo sito di Disaster Recovery.
- **Crittografia end-to-end:** protegge i dati sia nel corso del backup che nei periodi di attività e inattività.
- **Replica efficiente:** accelera i processi di replica e ripristino tramite Wan Accelerator.
- **Built-in WAN Acceleration:** aumenta di sono a 50 volte la velocità di trasferimento dati nella fase di backup su WAN.
- **Backup su nastro:** supporta in modo nativo il backup su nastro con scrittura sia di interi backup delle VM oppure di singoli file su nastro, ripristinandoli dal nastro quando necessario.

La modalità che permette di effettuare rapidi ripristini, ha spiegato Albert Zammar, Country Manager Italia di Veeam Software, deriva dal fatto che il tipo di funzionalità di Veeam Availability Suite è tale per cui il ripristino è indipenden-

Albert Zammar,
Country Manager Italia di Veeam Software



te dal dominio di dati o dal volume della massa di dati da ripristinare, perché la soluzione è progettata per effettuare una “fotografia” del contenitore dei dati.

In sostanza, il ripristino non viene effettuato in maniera classica, ma rendendo immediatamente disponibile la “fotografia” dell’intera infrastruttura e del dato da ripristinare. Si è così subito operativi, con gli utenti che possono lavorare sui dati in oggetto, mentre il software continua ad occuparsi in background di effettuare e completare il ripristino in maniera classica.

Se il restore deve poi avvenire tramite rete geografica interviene la funzione di WAN Accelerator che permette di eliminare le criticità trasmissive tipiche di una rete geografica.

Veeam Availability Suite effettua inoltre test continuativi sul corretto funzionamento delle operazioni di ripristino, per cui se c’è una condizione di potenziale disastro la criticità viene subito individuata.

Backup veloci e a basso costo con Veeam Cloud Connect

Come accennato, una componente di rilievo della Veeam Availability Suite è la suite Veeam Cloud Connect, un software che permette di usare il cloud per il backup/restore e in sostanza di evitare di acquistare ulteriori componenti hardware o di dover investire in un secondo sito per i backup. L’unica cosa mandatoria è individuare un provider di

servizi che usi Veeam Cloud Connect per l’hosting dei propri backup e pagare solo ciò che viene utilizzato. Numerose le funzioni disponibili. Tra queste:

- **Backup offsite in hosting:** permette di eseguire i backup offsite verso un cloud repository in hosting tramite una connessione SSL sicura e un cloud gateway.
- **Controllo e visibilità:** permette l’accesso e il recupero dei dati nei repository di backup in hosting direttamente dalla console del software, il controllo dell’utilizzo del cloud repository e provvede all’invio automatico di avvisi relativi al rinnovo dello spazio storage utilizzato in hosting.
- **Architettura di backup:** permette di sfruttare la tecnologia di

backup di Veeam, inclusa la backup copy, l’accelerazione WAN integrata, i backup incrementali, retention policy in modalità GFS (grandfather-father-son), per applicare la regola 3-2-1 della data protection mediante un unico prodotto.

La corrispondenza della soluzione Veeam in termini funzionali alle esigenze delle aziende ha trovato una chiara conferma nei dati di mercato, che ha visto crescere nel bilancio 2014 i suoi ricavi del 40% rispetto all’anno precedente.

«Il nostro è stato recepito come standard di fatto per la protezione e la gestio-

ne degli ambienti virtuali grazie, oltre all’always on business, anche all’analisi continua delle risorse e alla possibilità di realizzare operazioni di analisi planning. Inoltre, Veeam Availability Suite permette di dotarsi a costi tutto sommato contenuti rispetto a quelli usuali, di una soluzione di business continuity per cui garantiamo tempi di ripristino inferiori ai 15 minuti per applicazioni e dati», ha affermato Albert Zammar. *

Le soluzioni Overland Storage per backup e conservazione sicura

Una gamma di tecnologie e servizi che permettono di virtualizzare lo storage e di proteggere i dati anche nel cloud

Backup e conservazione sicura del dato sia a breve sia a lungo termine sono al centro degli sviluppi di Overland Storage, azienda presente in Italia tramite la sua partecipata Tandberg Data.

I prodotti a portfolio, sono soluzioni volte nel complesso ad abilitare la gestione unificata e la protezione dei dati nel loro intero ciclo di vita e, in particolare, i sistemi disco sono dotati di tecnologie RAID molto evolute atte a garantire la disponibilità, il recupero e la ricostruzione di un disco in caso di failure di sistema anche particolarmente pesanti.

Più in generale, Overland Storage progetta, produce e fornisce una gamma integrata di tecnologie e servizi sia per lo storage primario e nearline che offline e per l'archiviazione dati sul lungo periodo.

La mission di Overland, congiuntamente a Tandberg Data, una sua consociata interamente controllata, è dichiaratamente quella di semplificare ed ottimizzare sotto il piano dei costi la gestione e l'archiviazione di dati e informazioni, siano esse conservate e trattate localmente che distribuite su scala geografica.

La presenza sul mercato di Overland Storage si è poi ulteriormente espansa

tramite la fusione con Sphere 3D. Obiettivo primario di questa operazione è stato quello di accelerare lo sviluppo e l'integrazione di tecnologie di nuova e prossima generazione nell'ambito della virtualizzazione e del cloud, abbinandole ad una proposizione di soluzioni di storage scalabile.

In Italia le soluzioni storage, per il backup, l'archiviazione e la conservazione nel lungo periodo sono disponibili attraverso il canale distributivo Sphere3D, Overland Storage e Tandberg Data e anche tramite una rete di rivenditori a valore aggiunto e system integrator.

SnapServer XSD

Alle esigenze enterprise di protezione dei dati Overland Storage dedica SnapServer XSD 40, una soluzione storage in formato desktop che prevede robuste funzionalità di

protezione dati quali SnapShot ad alte prestazioni, backup diretto su RDX, BitTorrent Sync e opzionalmente la replica remota. Questa soluzione supporta accessi sia a livello file sia a blocchi ed è compatibile con sistemi Windows, Linux, UNIX e Macintosh.

Il suo campo di utilizzo, suggerisce Overland Storage, spazia dagli ambienti con server virtualizzati e Microsoft Exchange, fino a architetture di backup e consolidamento dello storage.

Per quanto concerne la fruizione dei dati in ambienti distribuiti è integrato con il prodotto software di condivisione file BitTorrent Sync. Tramite il software i dati salvati sullo SnapServer XSD 40 possono essere consultati da qualsiasi luogo, cosa che rende possibile realizzare la collaborazione tra uffici distribuiti o remoti.

Il sistema operativo GuardianOS 7.6, sviluppato da Overland Storage, si fa anche carico di fornire robusti criteri di protezione e salvaguardia dei dati, in modo da rendere sicura

la disponibilità delle informazioni business. Secondo dati di targa, permette di disporre di illimitati volumi protetti mediante il DynamicRAID.

Poiché SnapServer è una soluzione virtualizzata è possibile aggiungere drive (anche di dimensioni differenti) a un array DynamicRAID esistente e avere operativo il tutto automaticamente in tempi molto contenuti.



SnapServer XSD 40



Un backup ottimizzato con SnapServer e RDX

Abbinando SnapServer XSD 40 con i prodotti della famiglia RDX (che comprende dispositivi storage equipaggiati con dischi rimovibili) è possibile realizzare soluzioni per le esigenze di backup e di salvaguardia dell'integrità dei dati in ambienti SMB e SME. In pratica, collegando un apparato RDX QuikStor allo SnapServer attraverso la porta USB integrata, il sistema di archiviazione RDX viene automaticamente rilevato come una periferica di backup. La soluzione combinata di RDX e SnapServer consente agli amministratori di copiare selettivamente i dati dai dischi del NAS al dispositivo storage RDX e memorizzare i dati di backup off-site come parte di un piano di disaster recovery. Essendo integrati nel software GuardianOS 7.6, gli amministratori possono formattare direttamente i media RDX connessi con file system XFS o NTFS.

Protezione dei dati in ambienti enterprise e cloud

Le soluzioni di storage della serie SnapScale usufruiscono del sistema operativo di classe enterprise RAINcloud OS.

RAINcloud OS comprende servizi per la realizzazione di una infrastruttura storage definita dal software

SnapScale, la soluzione di classe enterprise per cloud privati

in grado di eseguire automaticamente e in modo intelligente operazioni di gestione e protezione dei dati senza la necessità di intervento manuale. Tra i servizi che Overland Storage evidenzia come particolarmente interessanti ai fini della sicurezza e dell'operatività si annoverano:

- **Windows-only Tree:** migliora la funzionalità di Permission Handling and Authentication, permettendo agli utenti Windows e UNIX/Mac di condividere i documenti in ambienti misti.
- **Lightweight Directory Access Protocol (LDAP):** consente agli amministratori di impostare i permessi e definire gli accessi alle cartelle utilizzando il "name lookup" da e verso gli Unique User Identifier (UID).
- **Monitoraggio storico delle prestazioni:** consente agli amministratori di ottenere report riferiti a specifici periodi per ottimizzare il trasferimento dati e minimizzare i colli di bottiglia della rete.
- **Creazione di cloud privati e protezione dei dati:** consente di creare un cloud privato senza doversi preoccupare di problemi di sicurezza e spese legati a servizi cloud di terze parti.

Non ultimo, gli strumenti per gestire i dati in mobilità

compresi in RAINcloud OS consentono di implementare cloud privati per condividere e sincronizzare i dati e permetterne l'accesso anche quando si è fuori ufficio.

Una sicurezza che passa per la virtualizzazione

Un altro elemento importante per incrementare la sicurezza è la virtualizzazione, che permette di gestire centralmente dati e dispositivi. La proposta Sphere3d, società proprietaria dei brand Overland Storage e Tandberg Data, in questo campo si basa sulle piattaforme VDI di V3, società controllata, che permettono di realizzare una infrastruttura distribuita di virtual desktop come parte di una architettura iperconvergente. Le appliance sono disponibili in 3 modelli: V50, V100 e V200, in grado rispettivamente di supportare sino a 50, 100 e 200 user concorrenti ma con una scalabilità di sino a 10.000 desktop. Le appliance sono già pronte per essere inserite in un ambiente VMware.

I pool di appliance V3 sono gestiti centralmente tramite il Desktop Cloud Orchestrator, un software di management user friendly che permette di creare, eliminare, abilitare, disabilitare e realizzare il provisioning dei desktop virtuali.*

Appliance V3 per rack per la virtualizzazione dei desktop in ambiente VMware





Gastone Nencini
country manager
Trend Micro Italia

GUARDA IL VIDEO ►►►



Cambiare approccio per proteggersi dagli attacchi mirati

Nell'attuale scenario della sicurezza informatica, gli attacchi mirati rappresentano una minaccia emergente e in costante diffusione.

Si tratta di una tipologia di attacco tra le più difficili da contrastare poiché utilizza tecniche sofisticate e diversificate, combinate in una strategia basata su più fasi e applicate con tenacia e continuità fino al conseguimento dell'obiettivo.

Gli attacchi mirati sono rivolti ad aziende di ogni tipo e sono utilizzati in tutti gli ambiti: nello spionaggio industriale o governativo, nelle azioni di sabotaggio, nelle frodi, nei furti di proprietà intellettuale, nella sottrazione di dati e così via.

Il punto di partenze di un attacco mirato è la raccolta di informazioni sulla singola organizzazione target e sui soggetti indirettamente collegati a essa; tra questi ultimi possono esserci aziende partner, collaboratori o clienti dell'organizzazione sotto attacco, spesso aggirati con l'uso di tecniche di social engineering al fine di ottenere informazioni che, separatamente, possono sembrare poco rilevanti ma che, se correlate tra loro, possono fornire chiavi per la compromissione della sicurezza.

Una volta identificato l'elemento debole della catena (il computer di un dipendente, un dispositivo mobile aziendale, un server ...), l'attaccante ne sfrutta le vulnerabilità riuscendo spesso a eludere gli strumenti di protezione

generali predisposti dall'azienda e a installare un malware. Questo primo sistema compromesso rappresenta il grimaldello su cui costruire le azioni successive, cominciando dalla predisposizione di un centro di comando e controllo per stabilire una comunicazione costante con l'host compromesso.

A questo punto l'attaccante rimane per lungo tempo ad agire inosservato spostandosi all'interno della rete alla ricerca di sistemi che ospitano informazioni sensibili o in grado di fornire un accesso di livello superiore alle altre risorse di rete, analizzando le vulnerabilità ed espandendo la propria presenza e controllo.

L'ultima fase è quella dell'attacco vero e proprio verso il target prefissato, che può proseguire indisturbata anche per mesi, durante i quali vengono sottratte informazioni chiave attraverso una backdoor, svuotando l'azienda di tutti i suoi asset.

Questa tipologia di attacco definita "tailor made" necessita di un sistema di difesa che sia anch'esso costruito su misura, capace di tenere conto delle vulnerabilità associate a ognuna delle fasi di attacco e che sia in grado di intercettarlo, bloccarlo e renderlo inattivo all'interno della rete.

Servono meccanismi di difesa basati su analisi e correlazione degli eventi, in grado di operare in modo efficace e sinergico.

Trend Micro affronta questa sfida con prodotti quali la suite Deep Discovery e il suo modello di Custom Defense, in grado di adattarsi allo specifico ambiente IT di ogni azienda.

È disponibile il libro sul **CLOUD COMPUTING**

In oltre 280 pagine analizza gli economics e le strategie alla base dell'adozione del Cloud come strumento per rendere l'IT più efficace, razionale e meno costoso, nonché gli aspetti connessi ai nuovi paradigmi dell'IT e del cloud. Tra questi l'Hybrid Cloud, i Big data e il Software Defined Data Center. Completa l'opera l'esame della strategia e della proposizione di primarie aziende dell'IT internazionale che hanno fatto del Cloud uno degli elementi portanti del proprio portfolio di soluzioni e servizi.

CLOUD E LEGACY TRANSFORMATION

Hybrid Cloud, Data Backup, Big Data e Servizi
per un'azienda dinamica e competitiva

Giuseppe Saccardi - Gaetano Di Blasio - Riccardo Florio

Reportec

**edizione
2015**



Sono anche disponibili i libri

- **STORAGE**
- **SICUREZZA E PROTEZIONE DEI DATI**

Il libro è acquistabile al prezzo di 50 euro (più IVA) richiedendolo a
info@reportec.it - tel 02 36580441 - fax 02 36580444



DE gustare

alla scoperta dei sapori d'Italia



NOTIZIE
ROAD TO DUBAI, LE ECCELLENZE ITALIANE SI PRESENTANO

**giornalisti,
enologi,
chef,
nutrizionisti,
esperti alimentari
vi promettono
un'esperienza
nuova**



01 GIUGNO 2015
La Toscana di Biella

Agricoltura biodinamica

Asparago in cucina



DE gustare
alla scoperta dei sapori d'Italia



Alla corte del RE

www.de-gustare.it