

SECURITY

& BUSINESS

n.30

COMPLIANCE

PRIVACY, LE REGOLE DELL'UNIONE EUROPEA

Ci sono voluti tre anni e ancora il percorso burocratico non è terminato, ma il testo della legge sulla protezione dei dati personali emanato dall'Unione Europea è stato rilasciato e sancisce il diritto alla privacy dei cittadini, creando qualche problema alle imprese, che dovranno più o meno rapidamente adeguarsi alle nuove regole. Lo spirito della riforma è ben sintetizzato in un tweet di Viviane Reding, membro del Parlamento Europeo, relatrice del TiSA (Trade in Service) e promotrice del GDPR:



«Bel giorno per i cittadini europei, le nuove regole stabiliscono che i dati personali appartengono agli individui e non alle imprese».

pag.14-15

CYBER ATTACK

NEL 2016 CRIMINALI INFORMATICI SEMPRE PIÙ CATTIVI

Estorsioni, danni fisici, 20 milioni di app maligne: questi gli elementi di spicco nelle previsioni sulle minacce nel 2016 secondo gli esperti dei Trend Labs. **pag.08**



SPECIALE

SICUREZZA E PROTEZIONE DEI DATI



Dati e informazioni sono un asset sempre più importante per il business aziendale. Una violazione alla loro sicurezza, provoca danni economici potenzialmente devastanti. Le soluzioni disponibili per proteggerli.

pag.15

IN QUESTO NUMERO:

EDITORIALE pag.3

• Il risveglio della sicurezza

NEWS pag.4-6

• Active Solutions punta sul TCO ed entra nel mercato della sicurezza
• Maurizio Desiderio alla guida di F5 Networks in Italia e Malta
• Rigby Private Equity investe in Zycko

CYBER ATTACK pag.08-10

• Nel 2016 criminali informatici sempre più cattivi

CYBER LAW pag.12-13

• Dati, dati, dati

COMPLIANCE pag.14

• Privacy, le regole dell'Unione Europea

SPECIALE SICUREZZA E PROTEZIONE DEI DATI

pag. 16 F-Secure

pag. 19 Fujitsu

pag. 22 Oracle

pag. 25 Trend Micro

pag. 28 Veeam

SOLUZIONI

pag.31

• Sicurezza gestita e nel cloud con iNebula

pag.32

• Cisco rafforza la security everywhere

Reportec

Le violazioni della sicurezza? Non sulla stampante.

Proteggi la tua rete con le stampanti più sicure al mondo.

Le nuove stampanti enterprise HP LaserJet con tecnologia JetIntelligence offrono la sicurezza di stampa più robusta del settore,¹ grazie a funzionalità integrate quali HP Sure Start con BIOS di auto-riparazione, la tecnologia di whitelisting e il rilevamento intrusioni durante l'operatività.

hp.com/go/printersthatprotect

A large HP printer is shown from a high angle. The printer's control panel features a large touchscreen display. The screen displays a statistic in white and green text: 'IL 53% dei manager IT è consapevole della vulnerabilità delle stampanti ai crimini informatici.'² The background of the screen shows a man in a yellow shirt standing in a server room. The printer is surrounded by various data visualization elements like charts and graphs.

IL 53%
dei manager IT
è consapevole della
vulnerabilità delle
stampanti ai crimini
informatici.²

¹ Le stampanti più sicure al mondo e il massimo livello di sicurezza: sulla base di verifiche HP pubblicate nel 2015 sulle funzionalità di sicurezza integrate nelle stampanti della stessa categoria dei produttori concorrenti. Solo HP offre una combinazione di funzionalità di sicurezza per la verifica dell'integrità fino alle capacità di auto-riparazione del BIOS. Potrebbe essere necessario un aggiornamento dei service pack FutureSmart per attivare le funzionalità di sicurezza sui modelli HP LaserJet M527, M506, M577. Alcune funzionalità saranno disponibili come aggiornamento dei service pack HP FutureSmart su modelli di stampanti enterprise esistenti selezionati. Per un elenco dei prodotti compatibili visita: <http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA6-1178ENW>. Per maggiori informazioni, visita: hp.com/go/ljsecurityclaims.

² Ponemon Institute, "Annual Global IT Security Benchmark Tracking Study", marzo 2015.
© Copyright 2015 HP Development Company, L.P.

Il risveglio della sicurezza



di Gaetano Di Blasio

Qualsiasi amministratore si preoccupa che il portone della propria azienda sia ben chiuso durante la notte, ma non accetta di spendere per la sicurezza informatica. L'eco mediatica sempre più frequente di attacchi a opera di cyber criminali sta significativamente contribuendo ad aumentare la consapevolezza sul pericolo, ma ancora manca una reale percezione dei rischi.

Di fatto, nelle aziende in cui vengono tipicamente prese decisioni in funzione di un ROI (Return On Investment), è difficile poter valutare il ritorno di un investimento in sicurezza, se non è possibile mettere sull'altro piatto della bilancia la quantificazione del rischio che si corre. Peraltro, è comunque difficile valutare quale sia l'investimento necessario e sufficiente per ridurre il rischio in questione. Ammesso che si sappia calcolare quale sia il livello di rischio accettabile.

In altre parole, le variabili sono spesso troppe per consentire di risolvere l'equazione e l'investimento in sicurezza viene limitato al minimo, sperando che a essere attaccato sia il vicino.

La situazione sta cambiando: da un lato il nuovo regolamento europeo (si veda pag.17) aumenterà un po' il minimo sforzo che deve essere realizzato per legge; dall'altro lato, la digitalizzazione sta comportando lo sviluppo di soluzioni che prevedono necessariamente una componente di sicurezza. In questi casi, diventa facile calcolare il ROI, perché il ritorno atteso non è una impalpabile riduzione del rischio, ma il ricavo derivante dal nuovo servizio digitale, mentre la sicurezza è semplicemente conteggiata come una delle voci di costo.

Questa sicurezza "embedded" potrà garantire elevati livelli di protezione nelle aziende digitali del futuro, ma patto che sia sicura by design e supportata da adeguati sistemi di sicurezza centralizzata concentrati sul dato e sull'identità digitale. Con ancora tanta tanta cultura e formazione presso i dipendenti.

Numero 30
Tutti i marchi sono registrati
e di proprietà delle relative
società

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

Editore: Reportec srl

Direttore responsabile:
Gaetano Di Blasio

In redazione: Riccardo Florio,
Giuseppe Saccardi, Paola
Saccardi

Immagini: dreamstime.com -
www.securityebusiness.it

Reportec

SECURITY
& BUSINESS

Active Solutions punta sul TCO ed entra nel mercato della sicurezza

di Gaetano Di Blasio

Al Partner Day del Vad milanese soluzioni all'avanguardia che rappresentano un elemento differenziante nella progettazione di soluzioni avanzate

Poter mettere a disposizione tecnologie innovative in grado di distinguersi sul mercato è un valore aggiunto tra i più importanti che un Value Added Distributor può fornire ai propri clienti.

È quello che si propone di realizzare Active Solutions stringendo partnership con vendor in grado di distinguersi per i contenuti innovativi e una strategia focalizzata nello sviluppo di prodotti adatti alle esigenze del mercato italiano.

All'Active Solutions Partner Day si è avuto un assaggio importante di soluzioni che possono determinare una differenza. In particolare, erano presenti rappresentanti di brand affermati e marchi meno noti ma dall'elevato contenuto innovativo, quali Samsung, Supermicro, Sphere 3D, Qsan, Spectra Logic, CloudFuze, Hillstone Networks. Un tratto comune che vale la pena sottolineare subito è il rapporto costo prestazioni: le soluzioni presentate sono state progettate per ridurre ogni componente di costo che incide sul TCO (Total Cost of Ownership) e, al tempo stesso, per ottimizzare il rendimento, che si tratti di minimizzare il costo per GB nelle applicazioni di archiviazione o di ingegnerizzare i server per abbattere i con-

sumi dei data center, o, ancora, di aumentare la densità e le prestazioni dello storage.

Tra le aziende presenti, Hillstone Networks rappresenta una novità per il mercato italiano e, soprattutto, per Active Solutions, che grazie alla collaborazione avvia-

ta con questa azienda presente in Cina e negli Usa, entra nel mercato della sicurezza. Una svolta favorita dall'ingresso in Active di Davide Carlesi in qualità di Sales & Business Development Manager.

L'aumento delle minacce e degli attacchi informatici rende estremamente critica la protezione del dato e avvicina sempre più il mondo server e storage, mercato di elezione per il VAD di San Donato Milanese, e la sicurezza. «Grazie alle compe-

tenze di Davide in questo mercato abbiamo deciso di compiere questo passo, convinti di poter fornire un valore aggiunto ai nostri clienti anche qui», afferma Guido D'Alonzo, managing director di Active Solutions.

Hillstone, inserita nel 2014 da Gartner nel magic quadrant dell'Unified Threat Management ha ricevuto diversi riconoscimenti per l'architettura innovativa dei propri firewall, disegnati per contrastare le moderne minacce



Zhong Wang - Hillstone Networks

APT, grazie all'integrazione di intelligence e soluzioni avanzate, come l'analisi del network behaviour. Ma si fa presto a dire behavior, come spiega Zhong Wang, vice president responsabile del Product Management, «perché occorre "imparare" il modello di comportamento per ciascun server».

«Abbiamo messo alla prova le capacità di questi firewall, facendoli testare a diversi esperti di security verificando la loro potenza», racconta Carlesi, che aggiunge: «La linea entry level di HillStone è perfetta per il mercato delle medie imprese, fornendo un livello di sicurezza molto avanzato a un costo assolutamente giusto».

Sphere 3D è in realtà la nuova veste di Tadberg Data e Overland, che si sono fuse con la software house Sphere 3D per sfruttarne i vantaggi, come spiega il channel sales manager italiano Paolo Rossi.

Simone Ceccano, sales manager di QSan, ha invece presentato le ultime novità in termini di network storage, tra cui spicca una soluzione ottimizzata per la memorizzazione della videosorveglianza.

Un salto nel futuro delle memorie SSD, sempre più dentro il data center, e nello stato dell'arte delle tecnologie NAND e Nvme o Open Express, quello che propone Massimo Germanò, B2B Senior Sales Manager SSD/



Forse meno appariscenti, ma analogamente all'avanguardia i server ottimizzati di Supermicro, che, come ricorda il sales manager Luca Arduini, è il primo produttore di server al mondo con fabbriche in Usa, Cina e Taiwan.

Memory di Samsung. Il Partner Day, che si è concluso con una memorabile visita al museo Alfa Romeo di Arese, ha anche permesso di valutare le soluzioni per l'archiviazione con le tecnologie a nastro e disco innovative di Spectra Logic.

Maurizio Desiderio alla guida di F5 Networks in Italia e Malta

F5 Networks, specializzata nell'application delivery networking, ha nominato Maurizio Desiderio Country Manager per l'Italia e Malta



Maurizio Desiderio - F5 Networks

con il ruolo di definire la strategia nella Region per espandere ulteriormente il business dell'azienda, in particolare nelle aree della security, dell'application delivery e del deployment delle applicazioni cloud. Il manager ha alle spalle 25 anni di esperienza nel mercato IT, con ruoli di crescente responsabilità nelle vendite e nel business.

Prima di approdare in F5 Networks, dal 2010 è stato Sales Director Italia, Turchia e Medio Oriente per Infoblox, occupandosi di guidare lo sviluppo, incrementare le vendite e la competitività. Precedentemente, ha ricoperto il ruolo di Direttore Commerciale Southern Europe and Middle East per Imprivata e Sales Director Italia e Grecia per Novell. Ha maturato inoltre esperienze significative nel regno Unito dal 1989, occupandosi di vendite e consulenza di business in aziende come Silvestream, Staffware e Bancotec. «Siamo molto contenti di avere con noi Maurizio, un manager con una grande esperienza nello sviluppo del business, nelle vendite e nella gestione del canale. Grazie alle sue capacità, continueremo a far crescere il business di F5 Networks e a rafforzarne la posizione nel mercato della sicurezza e dell'application delivery, per rispondere sempre in maniera efficace alle esigenze dei clienti» ha commentato Diego Arrabal, VP Southern Europe and Middle East di F5 Networks.

Rigby Private Equity investe in Zycko

La società Rigby Private Equity (RPE), il braccio di Rigby Group Investments dedicato al private equity, ha annunciato la sigla di un accordo con il quale ha effettuato importanti investimenti nel distributore specializzato in servizi e soluzioni IT, Zycko. Con questo accordo il distributore avrà la possibilità di espandere ulteriormente la propria presenza nell'area EMEA. RPE è stata costituita all'inizio di quest'anno proprio per identificare e investire in quelle società che hanno un'ampia proposta a valore e piani in forte crescita.

Zycko rappresenta la seconda acquisizione per Rigby Private Equity, che ha deciso di investire nel business della distribuzione ad alto valore e



specializzata a livello EMEA. Lo scorso luglio la società ha effettuato un investimento nel VAD specializzato in sicurezza Wick Hill. David Galton-Fenzi, CEO di Zycko, ha dichiarato: «Il supporto e il sostegno di RPE significa che ora siamo in grado di accelerare i nostri piani di crescita ambiziosi. È una grande opportunità per Zycko poter continuare la propria crescita e trasformazione in un'organizzazione più grande, ma che sia sempre focalizzata sulla fornitura di prima classe, il supporto professionale ai venditori che cercano servizi dedicati, la distribuzione a livello EMEA»

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

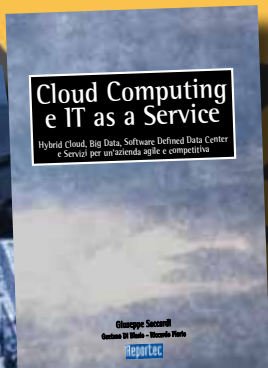
In oltre 250 pagine il punto sulla situazione della cybersecurity e sulle dinamiche aziendali nella protezione del dato e della continuità del business.

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.

**edizione
2015**

Giuseppe Saccardi - Gaetano Di Blasio - Riccardo Florio

Reportec



Sono disponibili anche
CLOUD COMPUTING E IT AS A SERVICE
STORAGE

Il libro è acquistabile al prezzo di 50 euro (più IVA 21%) richiedendolo a
info@reportec.it - tel 02 36580441 - fax 02 36580444

NEL 2016 CRIMINALI INFORMATICI SEMPRE PIÙ CATTIVI

Estorsioni, danni fisici, 20 milioni di app maligne: questi gli elementi di spicco nelle previsioni sulle minacce nel 2016 secondo gli esperti dei Trend Labs

di Gaetano Di Blasio

Gli esperti di Trend Micro hanno realizzato il report "Previsioni sulla sicurezza per il 2016". Si tratta di macro tendenze che caratterizzeranno le problematiche sulla protezione dei dati nel nuovo anno e che sono state spunto per una serie di interessanti riflessioni durante il Trend Micro Security Barcamp svoltosi a Milano alla presenza della stampa.

Gastone Nencini, Country Manager di Trend Micro Italia, è stato affiancato da esperti di mercato ed esponenti di aziende di primo piano: Donato Ceccomancini, Sales Operation and Sales Consultant Director di Fujitsu Italia, Francesco Traficante, Data Protection Officer & Privacy Consultant, Founder e CEO di Microell, Vincenzo De Lisi, CIO di Sirti, Davide Maria Rossi, Partner di Spike Reply e Rodolfo Rotondo, Business Solution Strategist di VMware, con la moderazione di Enrico Pagliarini, giornalista di Radio 24.

A dare il via ai lavori, Carla Targa, Marketing & Communication Manager di Trend Micro Italia: «I Trend Labs, oltre alla ricerca e sviluppo, elaborano anche studi, che hanno anche lo scopo di diffondere la cultura sulla sicurezza. Una necessità, come ha sottolineato recentemente anche Tim Cook (Ceo di Apple), in un'epoca in cui sempre più condividiamo dati sui social, navighiamo con device mobili, esponendo a pericoli la nostra privacy».

Se, da un lato, l'aumento di consapevolezza sui rischi on-



line renderà più efficaci le politiche di protezione dei dati, dall'altro, per la paura di perdere i dati gli utenti finali diventeranno più vulnerabili ai ricatti online.

Gastone Nencini, infatti, commentando le previsioni degli esperti Trend Micro per il 2016, sottolinea l'efficacia già ottenuta con i cryptoware e i ramsonware in generale: «Nel 2016 si registrerà una crescita delle estorsioni online, anche su mobile. Già è avvenuto "adescando" le vittime con pubblicità falsa di noti retailer italiani».

Le minacce in tal senso diventeranno sempre più sofisticate, ma questa volta non dal punto di vista tecnologico, bensì psicologico: «I cybercriminali hanno creato gruppi di ricerca con psicologi che li aiutano a comprendere le dinamiche per sfruttare i punti deboli degli utenti».

Le previsioni per il 2016

→ Il 2016 sarà l'anno delle estorsioni online. Più che i tecnicismi, i gruppi di cyber criminali, con la collaborazione di psicologi professionisti, sfrutteranno la paura come componente chiave del loro piano criminale, già dimostratasi un'arma efficace con il ransomware, i police trojan e i cryptoransomware.

→ Con la crescita (67% all'anno fino al 2019, secondo Gartner) dei dispositivi smart connessi a Internet (dall'elettronica a bordo delle auto ai baby monitor, dalle smart Tv ai sistemi per la domotica) cresce la probabilità che un guasto di tali device di fascia consumer causi un danno fisico. Potrà dipendere dall'inaffidabilità del dispositivo o della connessione, potrebbe essere un malfunzionamento, dovuto ad hacking o a un uso scorretto dei dispositivi

→ Minacce nel mobile: la Cina porterà la crescita delle minacce informatiche mobili a 20 milioni entro la fine del 2016. A livello mondiale, verranno presi di mira i metodi di pagamento mobili. Secondo alcune relazioni, in Cina 3 app su 4 sono malware. Google, invece, ha pubblicato un rapporto che riferisce che meno dell'1% delle app che si trovano su Google Play Store sono potenzialmente dannose. I dati di Trend Micro confermano sostanzialmente questi rapporti: 13% delle app presenti nei mercati cinesi è dannosa, 0,16% di app su Google Play dannose. Le minacce informatiche mobili in Cina si prevede raggiungano i 20 milioni entro la fine del 2016.

Nel resto del mondo l'attenzione dei cybercriminali si concentrerà soprattutto sui sistemi di pagamento mobile di ultima generazione, come carte di credito EMV, carte di credito contactless RFID e portafogli mobili quali Apple Pay e Google Wallet.

→ Gli hacktivistri utilizzeranno violazioni dei dati per danneggiare i loro obiettivi. Sulla scia degli attacchi che hanno visto protagoniste organizzazioni come Sony, Ashley Madison e persino Hacking Team, gli hacktivistri, invece che defacing e DDoS, esporranno informazioni compromettenti quali pratiche aziendali discutibili, messaggi riservati e transazioni sospette.

Gli esperti di Trend Micro ipotizzano anche infezioni secondarie che si affidano alla presenza Web di un obiettivo e la rivoltano contro i consumatori, come nel caso degli attacchi Watering Hole visti in passato.

→ Anche a seguito della nuova direttiva Ue sulla protezione dei dati, la prevista figura del Responsabile della protezione dei dati/Responsabile della sicurezza informatica sarà essenziale per garantire l'integrità dei dati e la conformità alle regole e alle normative dei

paesi in cui questi sono archiviati. Ciononostante, meno del 50% delle aziende disporrà di queste figure entro la fine del 2016. In un sondaggio, il 22,8% degli intervistati ha ammesso di non conoscere affatto la legge e il 50% ha affermato che non era in programma alcuna revisione dei criteri in linea con la nuova normativa.

Tuttavia, l'attenzione imposta sulla protezione dei dati aprirà la strada a un significativo salto di qualità nella mentalità e nella strategia aziendale contro gli attacchi informatici.

→ Riduzione della pubblicità cattiva. I fornitori di servizi ridurranno la pubblicità sui propri siti, modificando il modello di business pubblicitario a causa della crescente avversione degli utenti online per le inserzioni indesiderate e degli attacchi attuati con il "malvertising".

Nei primi sei mesi dell'anno, i tecnici di Trend micro hanno constatato come i kit di exploit siano stati usati nei piani di malvertising. Nel febbraio 2015, hanno individuato un exploit zero-day in Adobe Flash che veniva utilizzato negli attacchi di malvertisement.

Questo spiega il senso di consapevolezza apparentemente più intenso tra i consumatori che vogliono bloccare la pubblicità. Gli utenti non sono più semplicemente "seccati" dalle pubblicità indesiderate, ma sono pienamente consapevoli del tipo di rischi che esse rappresentano.

→ La legislazione sul crimine informatico compirà notevoli passi in avanti e diventerà un movimento realmente globale.

Le organizzazioni che combattono il crimine informatico stanno riscuotendo successi crescenti e l'orientamento mostrato dalle amministrazioni pubbliche fa ritenere che sarà possibile essere più reattivi agli attacchi informatici.

Anche la cooperazione e le partnership prospereranno, come dimostrano le operazioni coordinate di Trend Micro, INTERPOL, Cyber Defense Institute e di altre aziende di sicurezza che hanno portato allo smantellamento del botnet SIMDA in aprile. Le cooperazioni internazionali faciliteranno la rimozione o la messa in luce dei forum sommersi.

Secondo le previsioni di Trend Micro, il 2016 vedrà un significativo cambiamento nella mentalità delle pubbliche amministrazioni e dei legislatori, i quali punteranno verso un ruolo ancora più attivo nella protezione di Internet e nella tutela dei suoi utenti. Verrà avviato il dibattito sulle norme relative alla criminalità informatica e verranno rese obbligatorie modifiche agli standard di sicurezza informatica obsoleti per promuovere una posizione più efficace sulla sicurezza.

Da sinistra a destra:
Gastone Nencini, Rodolfo Rotondo,
Vincenzo De Lisi, Davide Maria Rossi



Lisi, che racconta quanto alta sia l'attenzione alla sicurezza in Sirti che da qualche anno spinge sull'acceleratore per la mobility nei processi sul campo, ma sottolinea la necessità rispondere al business, che non tollera aggravii procedurali, per esempio nella gestione delle password.

De Lisi, in particolare, sottolinea l'importanza di andare oltre la sicurezza fisica, che invece resta ancora la priorità per molte aziende.

Internet of Things

Viene da pensare che la sicurezza informatica incontri quella fisica su un piano criminale "antico". Di fatto Ci sono stati casi di suicidio istigato dall'estorsione online, ma il proliferare di dispositivi "smart", cioè collegati a Internet e quindi hackerabili, apre scenari ancora più vasti: «C'è chi ha montato una pistola su un drone progettato per il mondo consumer», spiega ancora Nencini, accennando ai potenziali danni fisici, anche alle persone, che può comportare la manipolazione informatica di sistemi industriali, dalla metropolitana senza autista agli SCADA, alle diverse declinazioni dell'industry 4.0.

È il più ampio tema dell'Internet of Things, che preoccupa molti, nel quale stanno confluendo tante tecnologie. Qui la sicurezza deve essere preventiva in un framework che permetta anche di correggere e risolvere le vulnerabilità e le imperfezioni di progettazione, come evidenzia Davide Maria Rossi.

Su questo fronte, una testimonianza arriva anche da De

Identità digitale

In altre parole, il controllo degli accessi è spesso fermo ai tornelli d'ingresso, mentre l'identity management digitale è trascurata. È un aspetto fondamentale, soprattutto perché proprio l'ID digitale è il principale obiettivo dei cybercriminali, che possono utilizzarla per gli scopi più vari, come acquistare un POS senza essere rintracciati e usarlo per scansionare carte di credito contactless nei luoghi affollati.

Un contributo alla sensibilizzazione potrebbe arrivare dalle nuove normative. Lo stesso Rossi ci assicura che il lavoro sullo Spid (Sistema Pubblico Identità Digitale) sta proseguendo, forse non abbastanza velocemente, ma più rapidamente di quanto si possa pensare.

Traficante, da parte sua, fa un rapido punto sulle normative prossime al varo da parte del Parlamento Europeo, in cui un elemento centrale è l'istituzione del Data Protection Officer.



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**



4 ORE AGO
NOTIZIE
**OLIO, FIRMATO
PROTOCOLLO PER
VALORIZZARLO**



NOTIZIE
**SARCHIO,
SFOGLIETTE BIO PER
TUTTI I GUSTI**

4 DEL AGO
NOTIZIE
**DIETA
MEDITERRANEA
PREMIO
GRUPPO**



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

DATI, DATI, DATI

di Riccardo Abeti

Usare i Big Data per ricavare informazioni utili dalla loro analisi, anche non generando profitto economico, può comportare ricadute di natura legale



Riccardo Abeti ama definirsi "tecono-avvocato" in quanto esperto di leggi relative all'ICT. Socio di EXPLegal, da oltre 15 anni si confronta con tecnici e top manager per risolvere problemi legati al rispetto delle leggi e alla sicurezza IT

Ogni giorno persone, imprese, enti governativi, si districano tra crescenti moli di dati.

Tutti hanno bisogno dei dati di tutti, spesso a priori, "perché qualcosa ci si può sempre fare".

In questo panorama, esistono però soggetti con chiare strategie di data raising, concepite per avere un preciso termometro dei fenomeni e del sentire di alcune moltitudini, siano esse di consumatori, elettori, assistiti e quant'altro.

I dati e le analisi condotte su di essi sono ormai intesi come elemento primario per generare "business" e a essi viene ricondotto un notevole valore economico e sociale.

Oggi questo fenomeno, comunemente noto come big data, è ormai diventato strumento per un crescente numero di soggetti che, in forza di enormi quantità di dati, possono perseguire una qualche finalità con conseguenti e più o meno prevedibili, ricadute di natura legale.

All'atto pratico, la tutela di cui stiamo parlando è perseguibile in molti modi, alcuni apparenti, altri sostanziali ma è pur vero che chi persegue uno scopo dovrà minimizzare gli impatti "regolamentari" e "normativi" a favore della massimizzazione degli effetti del trattamento sulla propria attività (attenzione, non parliamo solamente di profitto).

Proprio dall'uso massivo dei dati e dalle analisi sempre più

sofisticate degli stessi, emerge una delle più "decise" minacce ai diritti riconosciuti all'individuo dall'articolo 8 della Carta dei diritti fondamentali dell'Unione Europea, cui corrisponde un fenomeno che possiamo definire di overcharging burocratico, che viene affrontato con formulette standard, financo con software e applicazioni che automatizzano ragionamenti tutt'altro che banali, e conducono a risultati di dubbia legittimità.

Come per ogni tema che abbia un qualche impatto legale, per capire la portata e l'impatto del fenomeno e poterlo affrontare nel modo migliore, occorre partire da una valutazione che analizzi: la legittimità dell'acquisizione delle informazioni, la coerenza tra le finalità per le quali sono state acquisite e le finalità per le quali verranno trattate, le misure di sicurezza applicate alle informazioni.

Occorre inoltre resistere alla tentazione di partire dalla fine ovvero dall'anonimizzazione dei dati.

A norma di diversi position papers l'anonimizzazione, come peraltro è logico che sia, è considerata un "trattamento ulteriore", ciò significa che in presenza dei big data, procedere all'anonimizzazione è solo un passaggio di un processo molto più complesso.

L'attività di analisi deve consentire di valutare quali conseguenze può avere la "ricongiunzione" di database pro-

venienti da fonti differenti. Si tenga infatti presente che nell'epoca del "riuso", la possibilità di ottenere enormi quantità di informazioni, provenienti da molteplici sorgenti, è cresciuta esponenzialmente, a ciò si aggiunga che, spesso, i soggetti, magari pubbliche amministrazioni, che rilasciano "open-data" non hanno la possibilità o le competenze per preconizzare il possibile sfruttamento dei dati stessi in ottica di business.

Non dimentichiamo, infine, che il prodotto delle attività condotte sui big data può, a sua volta, generare servizi innovativi e meritevoli di essere protetti.

Dunque, quello dei big data è un fenomeno ingestibile?

No, come tutti i fenomeni i big data possono essere gestiti, forse il quadro normativo in cui sono maturati, non è metodologicamente pronto per tutelare le persone senza "compromettere gli usi e le applicazioni dei big data", tuttavia si può contemperare l'ipertrofia burocratica con un approccio che tenga conto della necessaria efficacia dei processi coinvolti.

L'evidenza dell'esperienza ci dice che, a oggi, si è ricorso a un approccio in qualche modo "presuntivo" ossia si è cercato di dimostrare la sicurezza e la legittimità dei trattamenti operati, facendo sentire gli utenti "al sicuro", al di là dell'effettività di questa sicurezza, prova ne è che, allorquando i meccanismi di tutela della riservatezza dei dati si sono "inceppati" oppure in sede ispettiva a opera del Garante per la protezione dei dati personali, ci si è accorti che la "sicurezza" era largamente compromessa e

le valutazioni di rischio, fuori fuoco, né emerso un quadro desolante di trascuratezza dei più elementari principi di data protection.

Viceversa, con un approccio razionale, orientato da quella privacy by design che è tanto ostentata negli ultimi tempi e seguendo alcune preziose indicazioni fornite in merito dalle best practices, si può ottenere l'abbattimento del rischio, in particolare, una volta appurata la legittima acquisizione delle informazioni e del relativo consenso e della coerenza con il principio di finalità, ci si dovrà porre l'interrogativo su come abbattere il rischio di riconoscimento dei singoli. In questo senso un'analisi del contesto iniziale ripetuta sia con cadenza regolare sia in relazione con eventi e mutamenti che la possano influenzare, può consentire di prevenire fenomeni di controllo abusivo così come la reidentificazione degli interessati, per esempio introducendo livelli crescenti di incertezza per cui un certo record possa essere attribuito a più persone, almeno 3 secondo i principi della deontologia statistica, oppure eliminando i requisiti che rendono atomistici i gruppi con caratteristiche comuni, o ancora affogando il profilo del singolo in un elevato numero di altri per i quali le caratteristiche dell'analisi non consentono di isolare un soggetto preciso. Quest'ultima attività può essere condotta lasciando integri i requisiti che fanno riferimento a una molteplicità di persone.

Sulla scorta di quanto sostenuto, si tenga, infine, presente che queste e altre misure possono consentire la convivenza dei big data con il vigente quadro di tutela della riservatezza ma l'approccio metodico è di gran lunga più efficace di molteplici misure adottate in modo disorganico.

PRIVACY, LE REGOLE DELL'UNIONE EUROPEA

di Gaetano Di Blasio

Pronto il testo del GDPR, General Data Protection Regulation, che protegge la privacy dei cittadini e impone nuove regole alle imprese sull'uso dei dati e la loro sicurezza



Ci sono voluti tre anni e ancora il percorso burocratico non è terminato, ma il testo della legge sulla protezione dei dati personali emanato dall'Unione Europea è stato rilasciato e sancisce il diritto alla privacy dei cittadini, creando qualche problema alle imprese, che dovranno più o meno rapidamente adeguarsi alle nuove regole.

Lo spirito della riforma è ben sintetizzato in un tweet di Viviane Reding, membro del Parlamento Europeo, relatrice del TISA (Trade in Service) e promotrice del GDPR: «Bel giorno per i cittadini europei, le nuove regole stabiliscono che i dati personali appartengono agli individui e non alle imprese».

Il framework rappresentato dal GDPR andrà a sostituire i regolamenti dei singoli paesi e per molti sarà più restrittivo. Potrebbe non essere il caso dell'Italia, che è piuttosto all'avanguardia sul fronte delle norme (un po' meno su quello dell'approvazione delle stesse). Questo è l'aspetto più importante, perché l'uniformazione delle leggi è alla base del Mercato Digitale Unico voluto dalla Commissione Europea. Come detto, però, in alcuni casi saranno necessari importanti adeguamenti. Stewart Room, socio di PwC (Price Waterhouse Coopers) a capo della funzione legale per la data privacy and protection, avverte: «Il business non è pronto ai complessi cambiamenti legali che il nuovo regolamento impone, con le ripercussioni in termini di compliance, auditing e rischio di un aumento di cause/ricorsi. D'altro canto, Jan Philipp Albrecht, parlamentare europeo

tra i relatori della "futura" legge (tecnicamente al momento in cui scriviamo manca il voto di ratifica, ma non si prevedono sorprese), sottolinea i passaggi finali che hanno vinto le proteste di alcune imprese grazie a un aumento del 4% nelle vendite previste a seguito delle nuove norme. Sono miliardi di euro che dovrebbero entrare nelle tasche dei colossi globali dell'online.

Per contro, come già anticipato, le imprese che gestiscono un numero significativo di dati sensibili (la quantità precisa inserita nel testo finale ci è ancora ignota, ma si parlava di oltre 5mila) saranno tenute a nominare un data protection officer. Lo stesso se monitorizzano il comportamento di numerosi consumatori. Sembrerebbe, quindi, una sorta di compensazione a beneficio della sicurezza. Di fatto, si impone un'attenzione maggiore alla sicurezza e si sancisce che i dati appartengono all'individuo, ma si permette anche l'utilizzo dei dati, purché l'individuo dia esplicito consenso. Una limitazione per molti paesi, ma non per l'Italia che già ha adottato questa politica da tempo. Come poi accade nella pratica, i fornitori di servizi "estorcono" facilmente tale consenso subordinandolo all'erogazione del servizio stesso. Occorrerà maggiore rigidità nel pretendere che siano dati specifiche autorizzazioni per ogni tipologia di utilizzo.

Attenzione ai minori: il consenso deve essere fornito dai genitori sotto un limite di età che ciascuno stato membro potrà fissare tra un minimo di 13 e un massimo di 16 anni.

Sicurezza e protezione dei dati

Dati e informazioni sono un asset sempre più importante per il business aziendale. Una violazione alla loro sicurezza, in termini di riservatezza, integrità e disponibilità, provoca danni economici potenzialmente devastanti. L'evoluzione delle minacce, la disposizione di tecnologie innovative, l'offerta di servizi ad hoc, nonché la trasformazione dell'IT aziendale verso un concetto più allargato di "digital technology", sono tutti elementi da considerare per definire una strategia aziendale per la protezione dei dati e dell'impresa stessa.

Se, del resto, implementare misure per la protezione del dato è previsto dalle normative italiane e internazionali, risulta altresì un elemento imprescindibile in uno scenario globale dove la rincorsa di una maggiore competitività, include la capacità di sfruttare le opportunità di Internet e delle nuove tecnologie, dalla mobility al cloud, dai big data al machine to machine. Ancor di più oggi, nel nuovo mondo "digital" dove non si vendono più prodotti ma esperienze.

MOBILITÀ SICURA CON F-SECURE FREEDOME FOR BUSINESS

La crescita della mobility aziendale come strumento fatto a favorire il business porta ad un costante incremento sia del volume e della qualità dei dati residenti sui dispositivi mobili che, 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 nel proprio dispositivo mobile e come ne protegge dati e comunicazioni sta ponendo serie sfide ai manager IT. E' una sfida che interessa sia quanto concerne la gestione dei dispositivi che 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.

E' 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 società 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 mal-

ware. 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.



Antonio Pusceddu - F-Secure

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

Con F4B una mobility sicura e flessibile

Freedom 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:

- 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 propria 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.

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

Disporre della visibilità in tempo reale e a 360 gradi della intera flotta di dispositivi mobili rappresenta la condizione sine qua non per una sua efficace protezione e

per garantire rapidità di intervento nel caso si incorra in incidenti di sicurezza. Freedom for Business affronta il problema dando una estesa visibilità sullo stato della sicurezza dei singoli dispositivi mobili e integra gli strumenti per gestire e proteggere sia i dati che i dispositivi. Particolarmente nutrite e ricche sono le funzioni di gestione della flotta. Tra queste:

- Blocco delle funzioni Web e in-app che tracciano profili ed eseguono operazioni di tracciamento degli utenti.
- Protezione della navigazione su Web impedendo l'accesso a link e siti dannosi.
- Neutralizzazione di furti tramite la funzione di cancellazione remota.
- Visibilità sullo stato generale della flotta, con la possibilità di verificare la versione del sistema operativo, i dispositivi con routing o il numero di telefono.
- Monitoraggio e tracciamento della frequenza e del volume dei siti Web bloccati, delle applicazioni, dei tentativi di tracciamento e dei dati protetti.
- Identificazione dei problemi al fine di identificare rapidamente una soluzione.

Sicurezza per le comunicazioni su reti Wi-Fi

F4B permette di proteggere le comunicazioni dei dispositivi mobili tramite anti-malware di ultimissima generazione all'interno di reti Wi-Fi aperte e di non mettere a rischio i dati aziendali sensibili. La protezione delle connessioni e dei dati che vi transitano è garantita tramite la realizzazione di una connessione VPN personale e tramite la crittografia dei dati.

Anti-Malware di ultimissima generazione

F4B risolve e mitiga gli incidenti derivanti da malware

che colpiscono i dispositivi mobili. In particolare la soluzione 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

Per la sua stessa natura e la modalità d'uso che lo caratterizza, un dispositivo mobile, evidenzia F-Secure, finisce con il conservare numerosissimi dati ed informazioni di business sensibili. Il suo furto può implicare danni diretti per l'azienda se si tratta di documenti commerciali o di progetti o a danni derivanti da azioni legali nel caso contenga dati riservati di terze parti, come nel caso di dati finanziario o sanitari. F4B gestisce il problema sia proteggendo con password l'accesso ai dati che permettendo dal centro, in caso di furto o semplice smarrimento la cancellazione remota dei dati residenti nel dispositivo. Inoltre, permette di applicare passcode in tutta la flotta con la possibilità di impostare lunghezza, livello, ora e frequenza di rinnovo delle password in accordo alle politiche aziendali.

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

FUJITSU PROTEGGE DATA CENTER E DEVICE CON BIOMETRIA E SOFTWARE EVOLUTO

Nell'ambito di quello che rappresenta il mercato della sicurezza inteso in termini generali, Fujitsu ha sviluppato una 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 PalmSecure 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 cen-

ter 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 Architecture Consultant di 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 ad una infrastruttura generica, chi utilizza dispositivi di client computing, quindi dispositivi come notebook, tablet, Pc o Smartphone riceve servizi ed informazioni forniti da applicazioni ed, in generale, da un Data Center.



Roberto Cherubini - Fujitsu

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 che per quanto riguarda la sua disponibilità.

«Va considerato che, al giorno d'oggi, uno dei principali elementi costitutivi del datacenter 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 disponibilità 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. Ad 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 ed 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. Ad 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 prevenire 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. E' 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 aziendali, dati personali, e dati 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 anche l'impegno nel far fronte a quella che è la vita quotidiana di un'azienda, dove è impegnata nella fornitura di soluzione sempre più efficaci ed 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 con 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 o volto 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.

CON ORACLE DATI PROTETTI E CONTROLLO IDENTITÀ INTEGRATO IN CLOUD E ON PREMISE

Le decisioni in azienda vengono prese tipicamente in funzione di un ROI (Return On Investment). Con questo approccio, la sicurezza ICT “soffre” la difficoltà di applicare un calcolo matematico a un processo il cui scopo è provvedere “che non accada nulla”. Di fatto, nella maggior parte dei casi, la sicurezza viene assimilata a un costo senza ritorno da ridurre il più possibile.

Di recente, le imprese stanno adottando nuovi modelli di business e/o di go to market che sfruttano le tecnologie mobile, social, big data, cloud. È la Digital Transformation che sta cambiando la tradizionale impostazione dei sistemi informativi, chiamati a supportare più direttamente il business nello sviluppo di nuovi servizi e approcci alla vendita.

In molti di questi casi, la sicurezza diventa parte integrante del progetto: per esempio, per una banca è inammissibile fornire una Payment App che non sia sicura. In questi casi, diventa semplice calcolare il ROI collegato alla sicurezza, perché il costo di quest'ultima è solo una voce che contribuisce a determinare l'investimento complessivo.

Oracle, attraverso la propria Oracle Security Community, contribuisce significativamente al gruppo di lavoro sul ROSI (Return on Security Investment) in seno al Clusit, ponendo sempre tale questione nell'approccio con la

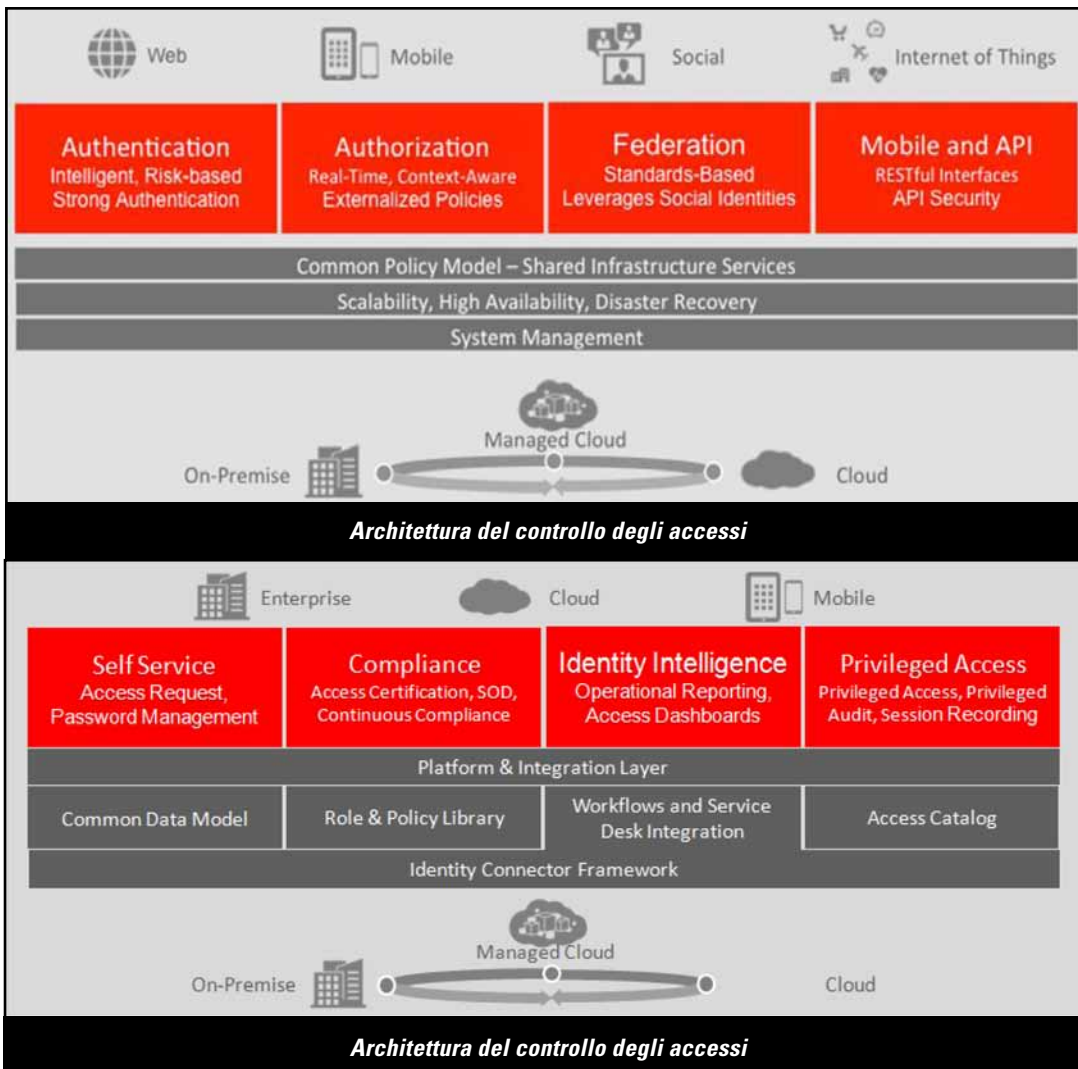
propria clientela. Il problema è che i sistemi attualmente in uso presso la maggiore parte delle imprese sono molto insicuri, essendo stati creati in un periodo in cui l'innovazione tecnologica era rapida e convulsa, mentre il pericolo del cybercrime non era ancora percepito nella sua realtà.

Oggi, evidenziano in Oracle, presso le imprese si registra una sensibilità crescente per la sicurezza e la protezione del dato. A ciò concorre l'eco mediatica raggiunta dai crimini informatici, la Compliance a numerose normative con nuove regole più severe sulla Privacy (che presentano anche risvolti penali per il responsabile del trattamento dati), e alcuni temi tecnologici, come il Bring Your Own Device, che pone l'accento sulla necessità di proteggere un perimetro sempre più allargato e di difficile definizione.

Sicurezza in cloud e on premise

Per rispondere a queste criticità e alla sfide tecnologiche poste dalle nuove tecniche di attacco altamente sofisticate, in Oracle è stato adottato un modello “cloud”, basato su un principio semplice: proteggere il dato con la stessa tecnologia sia sul cloud sia on premise.

L'impegno verso la data protection si affianca a quello per l'Identity and Authentication Management. Una stra-



dato. Nel caso del database Oracle, inoltre, tutte le funzionalità evolvono con il prodotto e sono poi rapidamente aggiornate per tutte le piattaforme terze.

Tra le soluzioni principali:

- Oracle Advanced Security, che, tra l'altro, fornisce funzioni di crittografia Transparent Data Encryption (TDE), prevenendo l'accesso diretto ai dati dal sistema operativo e codifica il contenuto dell'intero

tegia di protezione che si concentra sugli obiettivi finali del cybercrime, appunto interessato ai dati e alle identità digitali, piuttosto che disperdere sforzi e risorse nel presidiare un perimetro sempre più indefinibile.

La protezione del dato

Oracle deve il proprio successo al Database ed è quindi assolutamente logico che abbia sviluppato una serie di tecnologie e soluzioni che ruotano attorno a esso, sfruttando le caratteristiche intrinseche del database e, soprattutto, la conoscenza delle dinamiche a esso pertinenti. In particolare, questo significa che non solo per i database Oracle, ma anche per quelli di terze parti sono disponibili e attivabili una serie di soluzioni per la sicurezza dei dati sensibili ai fini della privacy, per la protezione dalle minacce e dagli attacchi e per facilitare la conformità alle normative in termini di sicurezza del

database nonché dei dati di backup.

- Oracle Data Masking, che fornisce funzioni di mascheramento avanzato, particolarmente utili per i test di sviluppo, permettendo di mascherarli per poterli usare prima di portare il nuovo servizio, per esempio, in produzione. I dati. Il mascheramento si può effettuare anche su un sottoinsieme di dati.
- Oracle Key Vault, che consente di centralizzare le chiavi in una piattaforma di Key management, la quale registra, per eventuali auditing successivi, qualsiasi accesso e azione riguardanti le chiavi.
- Oracle Database Vault, il quale consente di rafforzare il controllo sulle operation, prevenendo l'abuso dei privilegi nell'accesso al database sia dalla rete aziendale sia da remoto e proteggendo dati sensibili.

Il controllo dell'accesso e delle identità

Ciò che distingue la soluzione per la gestione delle identità di Oracle è l'approccio integrato, che non significa semplicemente disporre di tante funzionalità in grado di cooperare ed essere gestite da un'unica console, che pure non è poco, ma anche di avere unificate nella stessa piattaforma le capacità di gestione dell'identità on premise e nel cloud, con le stesse funzionalità e, ancora lo stesso, sul mobile.

In altre parole, è una soluzione completa che gestisce l'identità nell'accesso alle risorse aziendali con regole basate su ruoli, privilegi e altro indipendentemente dal luogo o dal dispositivo con cui si effettua l'accesso.

Come evidenziano in Oracle, questo comporta che, quando una persona lascia l'azienda o cambia ruolo, si deve intervenire in un unico punto per disattivare o modificare un account e automaticamente la persona potrà operare con i suoi nuovi privilegi o non potrà più accedere alla rete né potrà farlo qualcun altro tentando di sfruttarne l'identità. Si ottiene così di poter gestire efficacemente il ciclo di vita end to end delle identità utente su tutto il fronte delle risorse aziendali, sia all'interno o all'esterno del firewall e nel Cloud.

La piattaforma è stata progettata per fornire ampia scalabilità per i servizi di identity governance, gestione degli accessi e per i servizi di directory.

Anche solo per le caratteristiche architetturali, l'IDM

di Oracle si presenta idoneo ad aiutare le imprese a rafforzare la sicurezza nel suo complesso, semplificare i processi per la compliance alle normative, rendere sicure le applicazioni critiche e proteggere i dati sensibili dell'impresa. Il tutto indipendentemente se tali applicazioni o dati siano residenti in Cloud oppure in azienda.

Senza entrare nel dettaglio, osserviamo che la piattaforma Oracle Identity Management è composta da diverse soluzioni, a loro volta composta da moduli integrati fra loro e fra le soluzioni.

Recentemente, in particolare, è stata rilasciata la versione 11gR2 Patchset 3 di Oracle Identity Management, che integra soprattutto nuovi elementi per la sicurezza del mobile e risponde alle pressanti necessità di fornire un accesso protetto e senza soluzione di continuità a un'ampia varietà di applicazioni, da un numero crescente di dispositivi.

La nuova versione integra le funzioni di Enterprise Mobility Management nello stack Oracle Identity Management. La soluzione presenta funzionalità avanzate, per esempio meccanismi SSO avanzati e autenticazione sensibile al contesto, oltre ad alcune novità sostanziali, come il rinnovamento dell'interfaccia utente, che semplifica l'interazione con il sistema migliorando i processi di identificazione e accesso e riducendo la necessità di interazione con l'help desk.

LA SICUREZZA PERSONALIZZATA E USER CENTRICA DI TREND MICRO CONTRO LE NUOVE MINACCE

Da oltre 25 anni Trend Micro si dedica esclusivamente al tema della Content Security, con un'offerta che ha anticipato sui tempi molti temi legati alle nuove sfide tecnologiche e ai nuovi modelli di archiviazione, accesso e distribuzione delle informazioni. Il modello di sicurezza proposto dall'azienda giapponese integra la protezione dei dati estesa attraverso l'intera organizzazione con la sicurezza dalle minacce e dagli attacchi mirati, sfruttando a livello locale le analisi e le correlazioni effettuate su scala globale mediante un'intelligenza distribuita. Il risultato è una protezione in grado di affrontare il tema della riservatezza e della protezione dei dati in ambienti fisici, virtuali e in-the-cloud.

L'azienda in Italia è guidata da Gastone Nencini, che ricopre il ruolo di country manager. «Oggi mantenere la sicurezza all'interno di un'azienda è un processo continuo che non si interrompe mai - spiega Nencini -. I sistemi tradizionali di difesa non sono adeguati alle nuove tipologie di minacce come, per esempio, ransomware, minacce mobile o APT. Serve un approccio differente ed è per questo che le soluzioni Trend Micro evolvono costantemente seguendo i cambiamenti dei malware. La Smart Protection Network è il sistema di intelligenza alla base di tutti i nostri prodotti e strategie di sicurezza, che offre la possibilità di effettuare analisi di intelligence e di controllare a priori le sorgenti di informazioni, consentendoci di essere proattivi sulle minacce e di bloccare in tempi molto più rapidi i possibili attacchi e le infezioni».

La Smart Protection Network

Trend Micro Smart Protection Network è l'infrastruttura per la protezione automatizzata degli ambienti fisici, mobili, virtuali e cloud che sfrutta un approccio di difesa intelligente basato sulle conoscenze collettive ottenute dall'ampio bacino dei clienti Trend Micro e oltre 150 milioni di sensori distribuiti a livello globale. Mettendo in correlazione in tempo reale i dati provenienti da decine di miliardi di query sulle minacce 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, evidenziare eventuali vulnerabilità e di attivare azioni preventive di protezione in base a queste indicazioni. 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. Ogni nuova minaccia, identificata tramite una verifica di routine della reputazione di un singolo cliente, aggiorna automaticamente tutti i database delle minacce di Trend Micro e blocca 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 degli eventi sicuri, al fine di minimizzare i falsi positivi. «Abbiamo sviluppato una tecnologia di reputazione che si basa



Gastone Nencini - Trend Micro

su database integrati e correlati tra loro in modo che un eventuale avviso di sicurezza a uno dei database può fare alzare il livello di allarme sugli altri - precisa Nencini -.

Si tratta di un approccio che non tutti i vendor di sicurezza hanno intrapreso o, perlomeno, non su una scala così ampia come ha fatto Trend Micro. Alcuni nostri competitor hanno database per classificare indirizzi IP o siti Web pericolosi, ma non tutti, per esempio, dispongono come noi anche di un database delle vulnerabilità o delle applicazioni mobile potenzialmente nocive». La Smart Protection Network è integrata nei prodotti e nei servizi Trend Micro. L'azienda giapponese offre anche come servizio la possibilità di correlare le informazioni reputazionali fornite dalla 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 ha sintetizzato la sua proposizione strategica all'insegna di tre "C".

Custom Defense

La prima C è la Custom defense per rafforzare la protezione dai nuovi rischi come quelli associati agli attacchi APT. Il vendor, infatti, offre ai propri clienti la possibilità di predisporre un livello di protezione personalizzato per il loro specifico ambiente. In altre parole, accanto a un livello di protezione di tipo "generalizzato" la Custom defense mette a disposizione un ambiente smart sandbox personalizzato che rispecchia in modo fedele lo scenario aziendale in termini di dispositivi e ambienti operativi utilizzati.

La piattaforma Deep Discovery è il centro nevralgico del-

la Trend Micro Custom Defense e il fulcro della soluzione di difesa personalizzata contro gli attacchi APT. Trend Micro Deep Discovery prevede il monitoraggio a livel-

lo di rete con tecnologia smart sandbox personalizzata e in tempo reale ed è in grado di controllare oltre 80 protocolli alla ricerca di anomalie per rilevare precocemente eventuali attacchi. 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 Deep Discovery è risultato, dai test effettuati dai laboratori indipendenti NSS Labs (NSS Labs, Breach Detection Systems Test Report, luglio 2015), il sistema di rilevamento delle minacce più efficace e più raccomandabile. Il report riporta che, nei test effettuati, "Trend Micro Deep Discovery Inspector ha individuate il 100% del malware HTTP, il 100% del malware email e il 100% del malware SMB". Deep Discovery Inspector ha anche superato tutti i test di stabilità e affidabilità.

Complete user protection

La seconda C della strategia Trend Micro 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 Sync, che offre funzionalità di memorizzazione dei dati fornite come servizio on-premises su cloud ibrido, con un elevato livello di controllo e protezione. Tramite Trend Micro OfficeScan è poi possibile proteggere file server, desktop fisici e virtuali e laptop, oltre

a endpoint POS (point-of-sale) e bancomat. Tutti questi endpoint, sia fisici sia virtuali, vengono protetti sfruttando le informazioni sulle minacce condivise in Cloud. In questo modo si ottiene una protezione di tipo immediato, che è in grado di rilevare e bloccare le attività di crittografia del ransomware, di arrestare i botnet e d'identificare le comunicazioni Command&Control utilizzate negli attacchi mirati e persistenti.

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 prestigiosa società di analisi internazionale Gartner Group ha inserito Trend Micro all'interno del quadrante dei Leader nel "Magic Quadrant for Endpoint Protection Platforms" (Dicembre 2014) per completezza di visione e capacità esecutiva.

Cloud & data center security

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 più diffu-

se. 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 Open Stack.

Trend Micro ha sviluppato una serie di tecnologie di sicurezza capaci di integrarsi con gli hypervisor delle macchine virtuali. Una di queste soluzioni è Trend Micro Deep Security, una piattaforma software di sicurezza integrata, che permette di proteggere i data center dinamici, i server (fisici, virtuali e in-the-cloud) e i desktop virtuali utilizzando funzioni anti-malware di tipo agent-based e agent-less. Trend Micro Deep Security è stata sviluppata in stretta collaborazione con VMware e include un ventaglio di differenti tecnologie di sicurezza e anti malware specializzate come rilevamento e prevenzione delle intrusioni (IDS/IPS), protezione delle applicazioni Web basata sul livello di reputazione, firewall, monitoraggio dell'integrità e ispezione dei log di registro.

Un approccio strutturato alla protezione aziendale

La gamma di soluzioni software che traduce in realtà il modello di protezione di Trend Micro comprende molte altre soluzioni tra cui ricordiamo: Mobile Security for Enterprise per la protezione e gestione dei dispositivi mobile; Scan-Mail per la protezione dei server di posta Exchange e Domino; Endpoint Encryption per la cifratura e la riservatezza dei dati; InterScan Messaging Security per la protezione del gateway di posta; Server Protect per la difesa di file server, Web server e sistemi di archiviazione.

A queste si affiancano le soluzioni IPS di prossima generazione provenienti dalla recente acquisizione della gamma di prodotti TippingPoint e i moduli di Data Loss Prevention integrati con gestione centralizzata delle policy.

DATA CENTER ALWAYS-ON E RIPRISTINO IN 15 MINUTI CON IL SOFTWARE VEEAM

Veeam Software (<http://www.veeam.com/it>) è una società privata fondata negli USA nel 2006 con sede attuale in Svizzera e che si caratterizza con una presenza e aziende clienti worldwide. 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.

La risposta a questa sfida in termini di soluzioni l'ha data con lo sviluppo di prodotti che si posizionano nel nuovo mercato della "Availability for the Modern Data Center", un suo marchio registrato, con l'obiettivo di supportare le organizzazioni dalle piccole alle grandi dimensioni nell'ottenere degli RTO (recovery time and point objectives), ovvero i tempi di ripristino entro cui poter tornare operativi a seguito di un guasto, inferiori a 15 minuti per tutte le applicazioni e i dati.

L'obiettivo è stato perseguito con lo sviluppo di un nuovo tipo di soluzione riferita come Veeam Availability Suite, che abilita, evidenzia Albert Zammar, suo responsabile per l'Italia, 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 una 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 ad 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. Quelle dell'always-on e dell'efficienza sono di fatto, riconosce Veeam Software, le nuove regole del business imposte dal mercato alle aziende, ormai conscie del dover garantire la continuità operativa, e con l'esigenza di far fronte alle nuove sfide dei mercati globali che esigono la disponibilità continua e non ammettono fermi macchina e del servizio per il recupero di dati che risultino funzionali al business.

È una sfida e un campo d'azione in cui Veeam Software si è posta l'obiettivo di essere di fondamentale aiuto alle aziende, e di farlo tramite un portfolio di soluzioni che si calano funzionalmente e architetture nel nuovo scenario di mercato, in cui il cloud, la elevata mobility e il forte incremento in volume e qualità delle minacce impongono l'adozione di nuovi criteri e architetture hardware e software (ad esempio virtualizzazione, Software Defined Storage, Software Defined Data Center e Cloud) nella gestione delle informazioni e nella organizzazione dei data center. «Oggi la nuova sfida risiede nella dotazione di



Albert Zammar - Veeam

infrastrutture che siano sempre operative, con recupero dei dati in tempi rapidissimi. Già da quest'anno il concetto dell'always-on business si prevede venga adottato da tutte le aziende in tutto il mondo, puntando all'alta disponibilità dei data center attraverso soluzioni che abbiano tempi di recupero molto veloci. Ed è proprio questo l'ambito di azione di Veeam Software, che offre una soluzione per le moderne infrastrutture IT che consenta loro di garantire continuità di servizi erogati dai data center nell'ottica dell'always-on business», osserva Albert Zammar, responsabile della filiale italiana di Veeam Software.

La proposta Veeam volta ad assicurare l'always-on alle applicazioni business rendendo prontamente disponibili i dati tramite processi di backup e restore molto efficienti, si cala quindi, sotto il profilo tecnologico e architetturale, nello scenario costituito dalle nuove architetture di data center ad elevata virtualizzazione e software defined, a cui si richiede di essere non solo efficienti, ma anche flessibili, dinamici e ottimizzati sul piano dei costi.

Il problema che si deve affrontare 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.

E' 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, deriva dal fatto

che il tipo di funzionalità di Veeam Availability Suite è tale per cui il ripristino è indipendente 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.

Uno standard di fatto

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 gestione 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.

SICUREZZA GESTITA E NEL CLOUD CON INEBULA

La società specializzata nel cloud del Gruppo Itway lancia i servizi di Managed Security per migliorare il controllo nella gestione della sicurezza

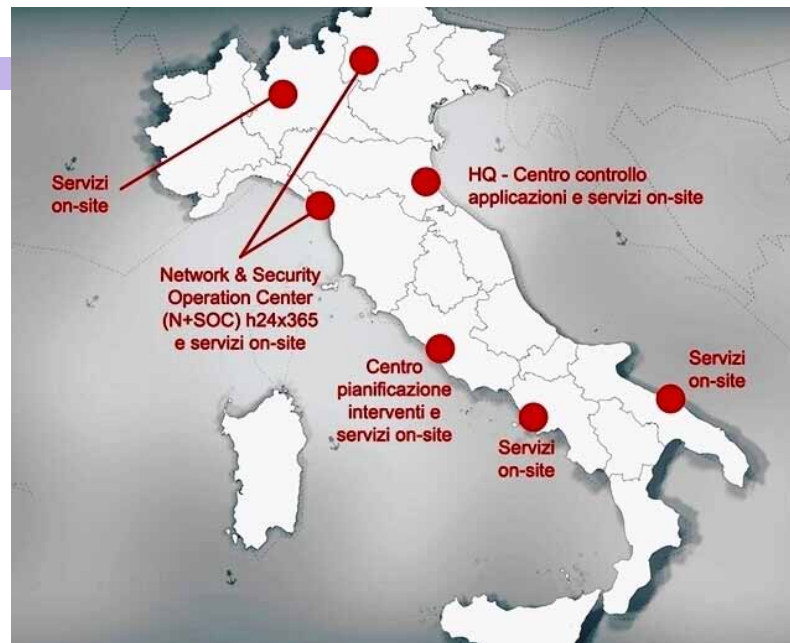
di Giuseppe Saccardi

In Nebula, società del Gruppo Itway e specializzata nelle soluzioni cloud, ha annunciato la disponibilità sul mercato italiano degli iNebula Managed Security Services, servizi di sicurezza integrata disponibili in lingua italiana che hanno l'obiettivo di consentire alle aziende di gestire la propria sicurezza a 360° e in cloud.

La famiglia iNebula Managed Security Services, ha evidenziato la società, è stata ideata e sviluppata per essere fruita in modalità cloud nativa e tramite il Network Operation Center (NOC) e il Security Operation Center (SOC). L'integrazione dei due centri di servizio, ha spiegato iNebula, consente di gestire la sicurezza delle reti e dell'operatività aziendale da diversi punti di controllo dislocati in Italia con un monitoraggio che è attivo in modalità h24.

Inoltre, grazie agli help desk e al monitoraggio sempre operativo, i clienti del servizio usufruiscono del controllo per la gestione della sicurezza, della manutenzione e assistenza tecnica, del supporto sistemistico e della gestione proattiva della rete.

In particolare, iNebula Managed Security fornisce agli utenti il monitoraggio attivo e in tempo reale di ambienti complessi al fine di implementare una sicurezza che consente di mettere in relazione gli eventi a livello di rete, applicazioni, transazioni e comunicazione fra



sistemi, a prescindere dal dispositivo e dal sistema coinvolti.

Il funzionamento si basa sulla raccolta di dati dalle fonti accreditate di Worldwide intelligence in modo da consentire di verificare in anticipo i potenziali problemi, utilizzando attivamente le informazioni raccolte per definire le strategie di difesa e reazione ad eventuali violazioni. Si ha inoltre la possibilità di impostare livelli di sicurezza predefiniti, in modo da valutare preventivamente i costi e gestirli al meglio.

«Con gli iNebula Managed Security Services i nostri clienti hanno a disposizione una soluzione di grande valore aggiunto, che consente loro di gestire efficacemente la sicurezza delle loro aziende direttamente dall'Italia e in lingua italiana. Possono inoltre fare affidamento su una rete di oltre 200 specialisti di IT security con più di 500 certificazioni tecnologiche e di processo, e della competenza di una delle poche aziende italiane ad avere una certificazione NATO; non a caso Gartner posiziona questi servizi nel Magic Quadrant Managed Security Services», ha commentato Stefano Della Valle, vicepresidente di iNebula.

CISCO RAFFORZA LA SECURITY EVERYWHERE

Più visibilità, controllo e protezione per Shadow IT, Endpoint e Cloud è quanto Cisco ha messo a disposizione delle aziende per proteggere le reti aziendali

di Giuseppe Saccardi

Cisco ha annunciato importanti sviluppi nella propria strategia di Security Everywhere indirizzati a cloud, rete ed endpoint, tra cui la disponibilità di nuovi prodotti e funzionalità di sicurezza, oltre a un servizio di consapevolezza delle minacce che intendono supportare la trasformazione digitale delle aziende.

Gli sviluppi derivano dalla considerazione della società che oggi le aziende stanno puntando su iniziative digitali per identificare nuovi percorsi di crescita e ridurre la complessità operativa. Mentre i dati diventano sempre più pervasivi, anche gli attacchi si fanno però più aggressivi e spesso le imprese non sono in grado di proteggere i loro asset. I responsabili della sicurezza si trovano in pratica ad affrontare una complessa serie di soluzioni differenti, spesso non interoperabili, e che offrono una visibilità limitata sulle potenziali minacce e violazioni delle reti aziendali.

Il valore dell'architettura di Cisco, ha evidenziato l'azienda, sta proprio nell'approccio che vede la sicurezza integrata nella rete – e nelle sue componenti come router, switch e data center – e che è in grado di colmare le lacune di visibilità durante il continuum di un attacco e ridurre significativamente i tempi di rilevamento e bonifica.

In particolare, Cisco ha introdotto Cisco Cloud Access Security (CAS), che fornisce visibilità e sicurezza dei dati per le applicazioni basate su cloud; ampliamenti a Identity Services Engine (ISE), che estendono la visibilità e il controllo



per reti e endpoint con nuovi controlli di accesso geolocalizzati; e Threat Awareness Service che dà alle aziende una elevata visibilità sulle minacce nelle loro reti.

«Persone e oggetti sono sempre più esposti a problematiche di sicurezza. Un rischio confermato dal 68% di aziende che dichiara che i dipendenti utilizzano dispositivi mobili mettendo a rischio le loro reti, dal 93% delle reti che accedono a siti web che ospitano malware e dal 90% di organizzazioni che non sono pienamente consapevoli dei dispositivi connessi alla propria rete. Inoltre, nelle imprese vengono utilizzati un numero di 5-10 volte maggiore di servizi cloud all'insaputa del dipartimento IT, il cosiddetto fenomeno dello 'shadow IT'», ha evidenziato Stefano Volpi, Area Sales Manager, Global Security Sales Organization (GSSO) di Cisco. In particolare, dallo studio dei dati sull'utilizzo di Servizi Cloud di Cisco si evidenzia come il numero di applicazioni cloud non autorizzate utilizzate dai dipendenti nelle aziende sia da 15 a 20 volte superiore rispetto a quanto previsto dai CIO: il cosiddetto fenomeno dello Shadow IT. La nuova soluzione Cisco Cloud Access Security (CAS) si propone di consentire alle aziende di affrontare questa complessità, oltre che aumentare la visibilità e il controllo sui dati nelle applicazioni cloud. Inoltre, CAS si integra con Cisco Cloud Web Security in modo da fornire agli uffici dislocati un accesso diretto a Internet sicuro con il router della serie Cisco Integrated Services Router 4K.

IDC BANKING FORUM 2016

La banca dall'e-business al d-business



16 febbraio, Milano – Palazzo Clerici



Scenario

La banca dall'e-business al d-business

Tutte le banche mirano a diventare protagoniste nel mondo digitale perché è proprio lì che stanno andando i loro clienti. Ma avere successo nel digital banking non significa fornire un servizio online, comporta una profonda trasformazione della tecnologia, dei processi e della cultura interna per offrire una customer experience univoca e superiore in ottica omni-channel, mantenendo inalterati i valori di fiducia e sicurezza alla base del rapporto con i clienti. Per una banca che nasce digitale e che può fornire servizi end-to-end su piattaforme digitali, agilità e semplicità sono caratteristiche intrinseche. Per una banca consolidata, affrontare la digital transformation implica invece orchestrare tecnologie e processi diversi, integrare canali fisici e virtuali, adattare i modelli operativi a nuove opportunità di business non dimenticando i fronti di redditività tradizionali. In una parola, operare a due velocità.

Key Words

Digital transformation, Mobile banking, Real-time banking, Customer-centricity, Mobile and P2P payments, Bitcoin, Crowdfunding, Modernization and core transformation, Big data analytics, Social.

PER INFORMAZIONI

Nicoletta Puglisi, Senior Conference Manager, IDC Italia
npuglisi@idc.com · 02 28457317

http://www.idcitalia.com/ita_banking16

 #IDCBanking16

