

DIRECTION Reportec 97

SOLUZIONI SERVIZI E TECNOLOGIE ICT

CONTINUA L'INNOVAZIONE NELLO STORAGE

SECURITY
& BUSINESS

SPECIALE

Finance security

Gli attacchi al mercato finanziario in Italia
I principali malware per le frodi bancarie

SOLUZIONI

La security intelligence di FireEye a portata di mid-market
La sicurezza HPE ancora più forte

TECHNOLOGY

Veeam Availability Suite 10
per un'azienda always-on

INTERVIEW

Plantronics: la direzione
è lo smarter working

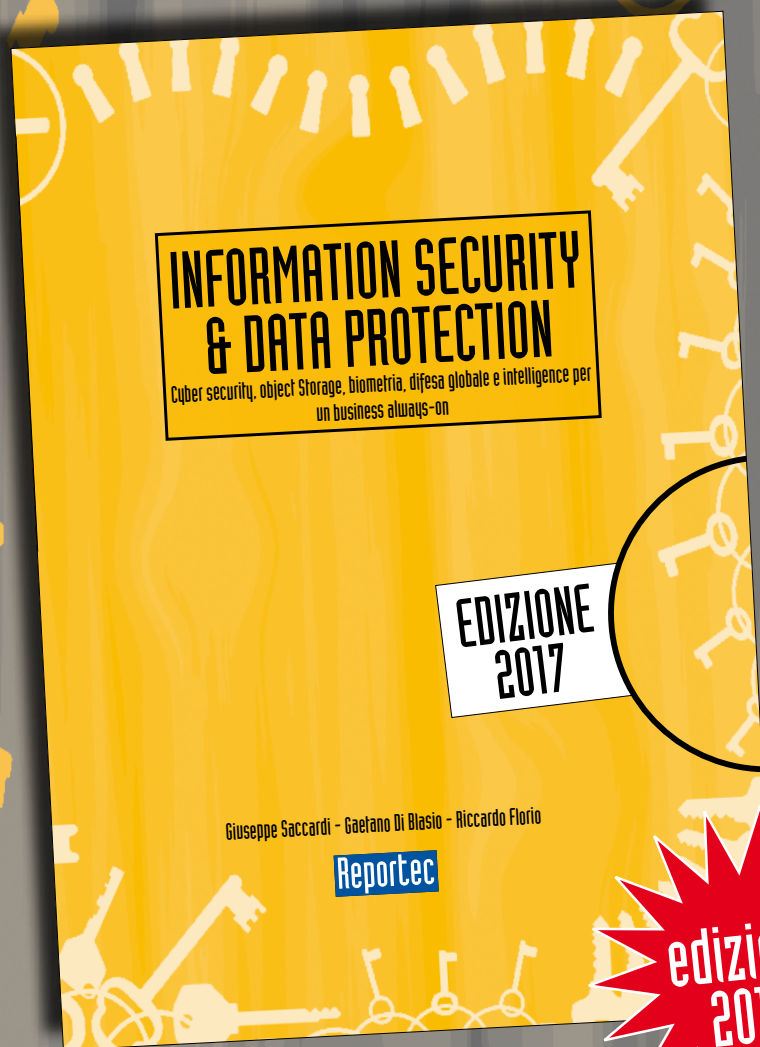
TRENDS & MARKET

Le sfide per
l'industria manifatturiera

CASE HISTORY

Nuova infrastruttura tecnologica
per Reale Mutua

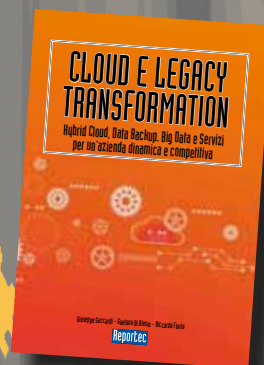
È disponibile il nuovo libro **SICUREZZA E PROTEZIONE DEI DATI**



In oltre 200 pagine il punto sulla situazione della cybersecurity e sulle dinamiche aziendali nella protezione del dato e della continuità del business. Una tematica sempre più vitale per le imprese, le quali devono mettere in conto che saranno attaccate. Ormai esistono sistemi automatici e pressioni da parte dei cybercriminali, tali per cui nessuno può sentirsi al sicuro: chi non è ancora stato attaccato lo sarà e, se non subirà danni gravi, sarà solo perché chi l'ha assalito cercava qualcos'altro.



È disponibili anche
CLOUD E LEGACY TRANSFORMATION



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

Direction Reportec
 anno XV - numero 97
 mensile maggio-giugno 2017

Direttore responsabile: Riccardo Florio

In redazione: Giuseppe Saccardi,
 Gaetano Di Blasio, Paola Saccardi,
 Daniela Schicchi

Ha collaborato: Gian Carlo Lanzetti

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 Marco Aurelio 8,
 20127 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.

FOCUS ON

Continua l'innovazione nello storage	4
DataCore spinge in avanti l'ottimizzazione dello storage	12

TECHNOLOGY

Toshiba punta su client B2B e nuove soluzioni	16
L'adozione che accelera le startup: un nuovo approccio	17
Da CIE un Gateway IoT di classe professionale	19
RAD guida la migrazione da TDM a IP	21
Veeam Availability Suite 10 per un'azienda always-on	24
Centro Computer abilita la Digital Transformation	28
RAD guida la migrazione da TDM a IP	34

TRENDS & MARKET

Le sfide per l'industria manifatturiera	20
--	-----------

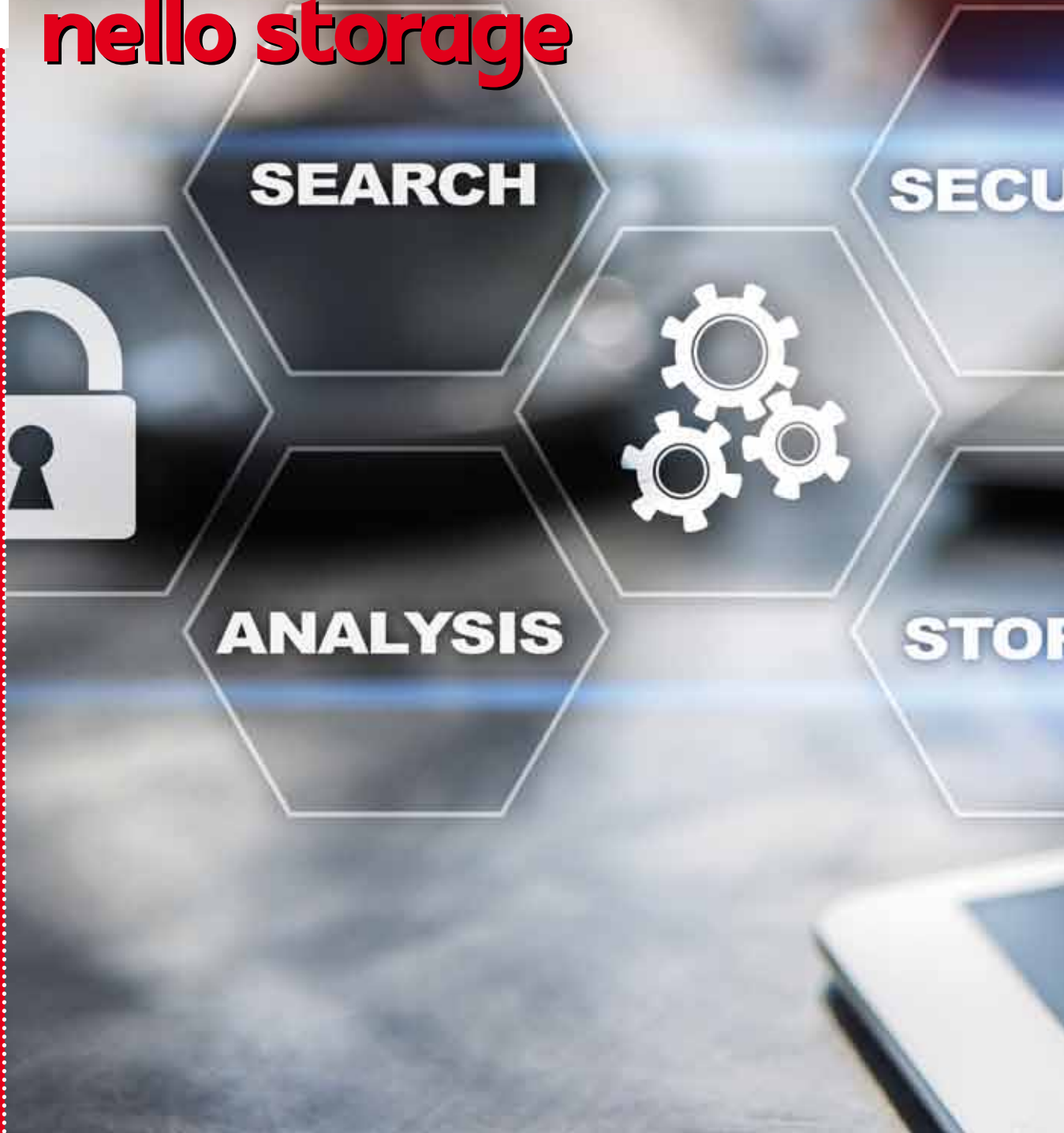
CASE HISTORY

Nuova infrastruttura tecnologica per Reale Mutua	22
---	-----------

INTERVIEW

Plantronics: la direzione è lo smarter working	30
---	-----------

Continua l'innovazione nello storage



Soluzioni sempre più potenti, NAS SAN, Flash e alte prestazioni caratterizzano lo storage a tutti i livelli

BIG DATA

SECURITY

MANAGEMENT

STORAGE

ACQUISITION

Lo storage continua ad essere uno dei settori più attivi per quanto riguarda le novità che appaiono continuamente sul mercato, indipendentemente dalla fascia di azienda o di applicazione specifica a cui si rivolgono o ambiente office o Industry. Lo storage, in sostanza, è una delle componenti chiave di tutti i settori di mercato e applicativi racchiusi in quanto viene collettivamente riferito con il termine di trasformazione digitale.

Dal cloud ai big data, dallo smart working all'IoT, un'affidabile e performante piattaforma storage si sta rivelando un elemento fondamentale per permettere la fruizione di soluzioni sia on-premise classiche sia fruite

as a service, si tratti di una grande azienda che da tempo ha intrapreso il vantaggioso percorso della virtualizzazione di server e storage, che della piccola e media azienda, che su questo percorso non sempre facile ha iniziato a muovere i primi passi.

I paragrafi seguenti illustrano una serie di esempi significativi di questa evoluzione e i benefici che derivano dall'impegno e dagli investimenti profusi dalle aziende produttrici nello sviluppo di nuove generazioni di dispositivi.

NAS sempre più ad alte prestazioni

Quello dei NAS è un campo delle tecnologie storage tra i più soggetti ad evoluzioni e come soluzione adatta dalla PMI alla grande azienda, perlomeno per applicazioni di filiale, è di costante interesse da parte dei produttori.

Un esempio di come si muovono gli operatori di mercato è offerto dagli ultimi annunci di Synology. La società da tempo attiva nel campo dello storage ha rilasciato da poco le nuove soluzioni storage DiskStation DS1517+ e DS1817+, entrambe caratterizzate



La NAS Disk Station DS1817+ di Synology

dalla possibilità di essere equipaggiate con le unità di espansione denominate DX517.

I server NAS rispondono a quelle che sono tipicamente le esigenze installative laddove non si prevede una installazione in armadio. Il loro

fattore di forma è quella a tower e hanno una capacità rispettivamente di 5 e 8-bay, sono entrambe scalabili e sono proposti dalla società per applicazioni molto diffuse a livello di piccole e medie aziende quali quelle di archiviazione in rete e applicazioni dove servono elevate prestazioni, si deve avere una alta affidabilità e parimenti alta versatilità.

Per rispondere adeguatamente a queste esigenze applicative le due disk station NAS equipaggiano un processore Intel Atom quad-core a 2.4GHz, e dispongono di due opzioni di memoria predefinite rispettivamente di 2GB e 8GB, espandibili a 16GB.

Robuste anche le possibilità di networking. Alle quattro porte di rete a 1Gb Ethernet integrate affiancano uno slot PCIe per una scheda di interfaccia di rete da 10GbE opzionale, e porte dual 10GbE per aumentare la banda laddove il problema prestazioni è critico.

Se dotate di memoria dual channel e interfaccia di rete 10GbE opzionale, le prestazioni sequenziali di throughput possono raggiungere secondo dati di targa la velocità di fino a 1.179 MB/s in

lettura e fino a 542 MB/s in scrittura. Tramite un adattatore è poi possibile aggiungere l'SSD SATA dual M.2 come memoria cache laddove serve migliorare le prestazioni.

Come evidenziato, i due NAS supportano la connessione di fino a due unità di espansione DX517, cosa che consente di disporre di fino a 10 slot aggiuntivi e di scalare la capacità di archiviazione. Il volume RAID può essere espanso direttamente senza dover riformattare i dischi rigidi esistenti.

DS1517+ e DS1817+ sono equipaggiate come software da DiskStation Manager (DSM) 6.1, il sistema operativo dei dispositivi NAS di Synology. Sugli apparati sono già disponibili come software anche numerose applicazioni per backup, gestione di rete e produttività.

«DS1517+ e DS1817+ offrono agli appassionati di tecnologie e alle aziende di piccole dimensioni più opzioni di archiviazione in grado di fornire straordinarie prestazioni e flessibilità per attività di archiviazione intensive. DS1517+ e DS1817+ sono i primi due Synology che supportano SSD M.2, concepiti per risolvere il calo di prestazioni in applicazioni con elevato carico di lavoro e per ridurre notevolmente la latenza I/O», ha evidenziato Jason Fan, Product Manager di Synology.

Il NAS
LightningPRO-
SC180 di
Thecus



NAS all-flash in batteria

Novità nel campo NAS sono state annunciate anche da Thecus con la sua nuova serie LightningPRO che comprende modelli compatti con fattore di forma di un'unità rack inseribili in armadi standard, con capacità di 360K IOPS e 10 unità SSD SATA. L'aspetto particolare è il loro uso, destinato ad ambienti di video recorder.

Thecus è un'azienda che negli anni si è specializzata nello sviluppo e commercializzazione a livello mondiale di soluzioni di Network Attached Storage e di Network Video Recorder, con un'offerta ideata per far fronte alle esigenze di home working sino a quelle più tipiche di una grande impresa. Nel corso degli anni ha espanso la sua offerta di prodotti aggiungendovi una piattaforma ideata avendo come punti chiave che risultasse semplice e intuitiva, con prestazioni elevate e una sicurezza di alto livello. Nello specifico, la sua nuova serie denominata LightningPRO comprende due diversi modelli, il SC180 e il SE300. Il primo prodotto ha un fattore di forma ultra compatto di una sola unità rack ed è inseribile in armadi standard. Fornisce una capacità di 360K IOPS in flusso continuo attraverso 10 unità SSD SATA che, per assicurare la continuità operativa e l'affidabilità, sono sostituibili a caldo.

Il modello SE300, invece, è un apparato che si caratterizza per una maggiore potenza elaborativa, pur occupando

anch'esso un solo modulo di un'unità. L'apparato, tramite otto SSD che utilizzano l'interfaccia NVMe, permette di disporre di una velocità di trasferimento dati molto elevata che i dati di targa indicano pari a 700K IOPS per operazioni di scrittura in ordine casuale di 4KB, che contribuiscono ad accelerare l'intero sistema.

Per migliorare le prestazioni i due prodotti utilizzano la

tecnologia FlexiRemap, che riordina le operazioni di scrittura casuali trasformandole in traffico sequenziale. Diversamente dagli algoritmi RAID, ha spiegato l'azienda, FlexiRemap riordina i dati ogni volta che questo rappresenta un vantaggio prima di passarli alla sottostante memoria flash, riducendo così facendo i cicli di programmazione/cancellazione dei chip di memoria, ha osservato Thecus, di fino al 150% rispetto alla tradizionale tecnologia RAID, evitando sovraccarichi non necessari e allungando la vita delle SSD.

Oltre a eliminare i colli di bottiglia è un approccio che permette di ottenere prestazioni inferiori al millisecondo e un miglior ritorno sull'investimento hardware.

Nuove tecnologie per il ripristino dei dati ad alta velocità

Connaturale nello storage dei dati vi è il loro ripristino quando a seguito

di malfunzionamenti o di attacchi cibernetici, ci si trova nella necessità di ripristinarli all'ultimo punto di loro backup.

Per farlo, in particolare in settori in crescita quali quello del broadcasting video e dell'editoria elettronica, Overland-Tandberg ha sviluppato dei sup-

porti RDX ad alta capienza adatti per applicazioni di questo tipo che si caratterizzano tipicamente per l'alto

contenuto di dati.

Nello specifico, la società, controllata da Sphere 3D, ha annunciato che l'utility software RDX per MAC è disponibile ed è possibile effettuarne il download. Nel mondo Windows, ha evidenziato l'azienda, i dispositivi RDX sono lo standard di fatto per lo storage di backup locale nelle piccole e medie imprese.

Va osservato che quella RDX è una tecnologia al suo decimo anno di vita e che continua, ha spiegato Overland-Tandberg, a offrire funzionalità di backup e ripristino estremamente veloci ed economicamente convenienti per l'archiviazione dati a lungo termine. In pratica, mette a fattor comune la portabilità e l'affidabilità del backup basato su nastro alle velocità e semplicità dei dischi fissi e/o delle unità a stato solido.

Robuste le caratteristiche costruttive e meccaniche. Fisicamente le cartucce RDX sono a prova d'urto e in base a dati di targa possono sostenere

Lo storage FAS8020 di NetApp adottato da Contarina



Contarina ha rinnovato lo storage
con le soluzioni NetApp



Contarina rinnova lo storage con dischi a stato solido

La tecnologia a stato solido ha permesso a Contarina di quadruplicare lo spazio storage, aumentare la velocità e porre le basi per una efficiente soluzione di disaster recovery

Contarina è una società con circa 700 dipendenti che opera in provincia di Treviso fornendo servizi di igiene ambientale in modo integrato. Il core business è la gestione dei rifiuti nei 50 Comuni aderenti al Consiglio di Bacino Priula in un territorio di circa 1.300 km quadrati tra centri storici, aree urbane e naturalistiche, un'area che coinvolge 554.000 abitanti e circa 260mila utenti.

Oltre a quello base fornisce anche altri servizi quali la gestione dei servizi informativi territoriali, del verde pubblico integrato e disinfestazioni, nonché servizi cimiteriali e di videosorveglianza nei Comuni consorziati.

Contarina disponeva di uno storage oramai datato al termine del suo ciclo di vita e non più adeguato alla realtà aziendale in espansione, sia dal punto di vista della capacità e delle prestazioni necessarie, che della sicurezza e della durata dell'investimento. Per l'azienda era in sostanza diventato importante disporre di una soluzione che fornisse uno strumento di monitoraggio della SAN, permettendo di verificare se il funzionamento fosse o meno corretto. In pratica fare dell'analisi complessiva in modo autonomo e facilmente gestibile.

Il nuovo storage

Dopo aver indetto una gara e valutato varie soluzioni, e tramite il coinvolgimento del partner tecnologico Imhotech, ha optato per adottare la soluzione NetApp FAS8020. La configurazione ha previsto 24 dischi allo

stato solido da 400 GB ognuno, 3 dischi SSD da 400 GB per l'accelerazione della cache e 56 dischi SAS da 1,2 terabyte. La soluzione permette all'azienda, ha spiegato NetApp, di disporre di circa 45 TB sui dischi SAS e di 8 TB sui dischi allo stato solido, e di una capacità di oltre 66.000 IOPS totali al secondo.

All'adozione del nuovo storage si è abbinata anche la migrazione della rete di connessione, che era di tipo SAN fiber channel, verso un'architettura basata su switch a 10 gigabit con connettività Ethernet sia lato host sia lato storage NetApp.

Il progetto ha fatto sì che ora l'azienda disponga di una soluzione con prestazioni migliorate, un accesso ai dati velocizzato, di strumenti per la gestione dei database e la gestione nonché del monitoraggio dell'intero sistema.

Quasi quadruplicato è poi lo spazio storage disponibile, cosa che, ha evidenziato NetApp, ha permesso l'integrazione con la soluzione di backup Veeam, alla quale l'azienda non voleva rinunciare.

Due le sedi e due i data center che sono stati interessati dal progetto. Alla data è stata fatta l'implementazione su un solo sito, ma con la possibilità di estendere la soluzione storage anche sul secondo. Inoltre, è allo studio per il futuro la possibilità per l'azienda di acquistare un'altra SAN sempre di NetApp per creare un sito di disaster recovery atto a garantire la continuità del servizio.

cadute sul pavimento da un metro di altezza, sono protette dalle scariche elettrostatiche e hanno una vita utile per l'archiviazione che supera i dieci anni.

In particolare, l'utility software RDX per MAC è stata sviluppata dall'azienda per consentire ad ambienti di progettazione grafica, editoria elettronica e di broadcasting video di disporre di una soluzione per lo storage e l'archiviazione in grado di supportare intensivi flussi di lavoro. Si rivela anche utile laddove lo scambio e il trasporto di dati per gli utenti che utilizzano servizi cloud possono essere problematici.

Di tipo "plug and play", si presenta al MAC come un disco fisso tradizionale e che si integra con lo strumento Time-Machine per il backup e anche con altre applicazioni per la gestione e la protezione dei dati che utilizzano dispositivi a disco.

«Siamo felici di poter offrire l'utility RDX per MAC con tutti i nostri prodotti RDX. La sua semplicità d'uso e la sua integrazione continuano la tradizione RDX di offrire soluzioni semplici ma dalle prestazioni elevate a società di ogni dimensione: dalla piccola azienda alla grande impresa», ha commentato il rilascio Hugo Bergmann, Director della RDX Storage Product Line.

La cartuccia dati ad alta affidabilità RDX di Tandberg Data



Object Storage ottimizzato a software

Le novità nello storage non si limitano ai prodotti o ai nuovi settori di interesse. Un esempio di come si muovono a tutto campo i produttori è offerto da NetApp che ha sviluppato un software, una nuova versione di NetApp StorageGRID Webscale, con cui si è posta l'obiettivo di semplificare l'installazione di storage OpenStack e supportare container Docker su server Bare-Metal.

Nello specifico, NetApp ha presentato da poco al mercato e agli operatori l'ultima versione del suo software di nuova generazione per l'object storage, sviluppato per aiutare le imprese ad avere il controllo sui rich content e ad accelerare la propria trasformazione digitale.

I miglioramenti apportati al software StorageGRID Webscale, ha spiegato l'azienda, hanno l'obiettivo di fornire ai team IT e di sviluppo una soluzione storage orientata al software per gestire i dati in scala e facilitano la realizzazione di un data center di prossima generazione. Numerosi gli aspetti salienti della nuova versione. Tra questi:

- Più opzioni di installazione del software, tra cui il supporto a container

L'appliance StorageGRID Webscale SG5600 di NetApp



Docker e la possibilità di installarli su server bare-metal.

- Installazioni semplificate di storage OpenStack con integrazione Keystone, supporto all'elenco di controllo di accesso (access control list - ACL) Swift e distribuzione heat-less.
- Migliore controllo multilivello con la possibilità di monitorare e gestire le quote di capacità degli utenti.
- Certificazione con Veritas Enterprise Vault per centralizzare la gestione della retention di email, file, social media.

«I dati sono la linfa vitale delle imprese di successo di oggi. NetApp è in una posizione unica per aiutare i clienti nel loro cammino verso organizzazioni guidate dai dati. StorageGRID Webscale fornisce un'architettura storage di prossima generazione che aiuta le aziende a creare facilmente data lake scalabili per archivio, analytic e dati

multimediali tra data center distribuiti geograficamente e cloud pubblico» ha commentato il rilascio della nuova versione Clemens Siebler, Manager Solution Architects EMEA di NetApp. La posizione di avanguardia nell'object storage di NetApp è rimarcata anche da IDC.

«Il ritmo sostenuto della digitalizzazione sta creando importanti sfide nella gestione dei dati per le imprese distribuite geograficamente e i service provider. NetApp StorageGRID Webscale è una soluzione di facile installazione e altamente scalabile che aiuterà gli utenti a creare l'infrastruttura necessaria per supportare una crescita massiccia in termini di dati strutturati e non strutturati», è invece l'opinione sostenuta da Amita Potnis, research manager di IDC, e non è difficile essere d'accordo con il ricercatore. ❁



DataCore spinge in avanti l'ottimizzazione dello storage

Il 2016 si chiude con ottimi risultati e il 2017 prepara la strada per nuove funzionalità di software defined storage, un rafforzamento delle infrastrutture storage e nuove partnership

«**D**ataCore si propone di creare un'architettura guidata dal software, duratura e dinamica, in grado di liberare i dati e la sua produttività dalle limitazioni basate su hardware statico».

Così apriva le sue presentazioni nel lontano 1998 George Teixeira, CEO, presidente e cofondatore di DataCore Software, azienda pioniera nella virtualizzazione via software dello storage. A quasi vent'anni di distanza, questa visione si dimostra quanto mai attuale e consente a DataCore di chiudere uno dei migliori anni di sempre, crescendo soprattutto nel settore enterprise.

È lo stesso Teixeira che, durante la sesta edizione dell'evento annuale DataCore Days, illustra le direzioni di sviluppo dell'azienda per il prossimo

futuro: «L'ultimo anno si è chiuso molto positivamente, con risultati che hanno superato le aspettative e confermando il sud Europa come la regione in cui DataCore cresce più rapidamente. Per il 2017 sono previsti nuovi investimenti in personale, marketing e a supporto dell'espansione dell'offerta di prodotti. Abbiamo previsto nuove funzionalità nella roadmap di SANsymphony, stiamo rafforzando l'offerta indirizzata verso le infrastrutture convergenti, ci prepariamo



George Teixeira
CEO, presidente
e cofondatore di
DataCore

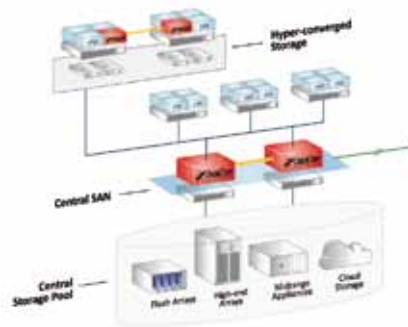
a esplorare nuove opportunità di mercato legate al mondo Microsoft SQL Server e continuiamo ad aggiungere valore alle nostre soluzioni grazie a un ecosistema di aziende partner come Lenovo, HGST e Coservit».

Soluzioni per ottimizzare l'infrastruttura dei dati

Il prodotto di riferimento dell'azienda resta SANsymphony, soluzione di software defined storage giunta alla decima release e utilizzata da oltre 10mila clienti, che consente di raggruppare logicamente risorse storage distribuite ed eterogenee e condividerle all'interno di un set comune di servizi gestiti centralmente. DataCore prevede a breve l'introduzione delle funzionalità di "3 way data resiliency" e "self healing" che si aggiungeranno a quelle esistenti all'insegna della disponibilità (mirroring sincrono, replica asincrona, protezione dei dati continua, snapshot e backup), delle prestazioni (caching, auto tiering, accelerazione random write, QoS) e dell'efficienza (storage pooling, thin provisioning, migrazione dei dati, deduplica/compressione).

La direzione di evoluzione dell'offerta si indirizza anche verso il tema delle infrastrutture convergenti con il software DataCore

DataCore
Hyperconverged
Virtual SAN



I servizi di storage unificati abilitati dalle soluzioni DataCore

Hyper-converged Virtual SAN che viene migliorato per favorire l'interazione con gli hypervisor e abilitare la creazione di un'infrastruttura dati ad alta disponibilità ed elevate prestazioni sfruttando la capacità DAS e lo storage interno disponibili in azienda. Alla base di questa soluzione vi è una tecnologia di I/O parallelo sviluppata dalla stessa DataCore.

«La direzione di sviluppo della ricerca ingegneristica di DataCore - ha proseguito Teixeira - punta a massimizzare la produttività, indirizzandosi sia verso il Parallel I/O per garantire una scalabilità verticale all'interno di uno stesso sistema sia verso il Virtual I/O per abilitare una scalabilità orizzontale attraverso più sistemi».

UNIFIED ENTERPRISE STORAGE SERVICES

AVAILABILITY	PERFORMANCE	EFFICIENCY
<ul style="list-style-type: none"> Synchronous Mirroring Asynchronous Replication CDP Snapshots / Backups 	<ul style="list-style-type: none"> Caching Auto-tiering Random Write Accelerator Quality of Service (QoS) 	<ul style="list-style-type: none"> Storage Pooling Thin Provisioning Data Migration Deduplication/Compression
MANAGEMENT		
<ul style="list-style-type: none"> Centralized Management 	<ul style="list-style-type: none"> Analysis & Reporting 	<ul style="list-style-type: none"> Vvols NAS/SAN (Unified Storage) Cloud Integration

Questo senza che sia necessaria alcuna registrazione, reindicizzazione o reingegnerizzazione delle applicazioni. La nostra intenzione è di rendere questa tecnologia accessibile non solo alle aziende enterprise, ma anche a quelle di dimensione più contenuta».

SDS pronto all'uso con l'appliance di Lenovo "powered by DataCore"

Un'altra novità del 2017 è la disponibilità, da marzo, dell'appliance DX8200D commercializzata da Lenovo e "powered by DataCore", adatta a soddisfare le esigenze di software defined storage correlate alle applicazioni e alla gestione dei dati mission critical. Questo dispositivo coniuga la potenza di elaborazione del server Lenovo x3650 M5 con la soluzione software SANsymphony di DataCore ed è immediatamente pronta all'uso, per rendere disponibili una gamma di funzionalità quali mirroring sincro, data protection con replica asincrona, Continuous Data Protection, snapshot e backup.

Sei le versioni disponibili, suddivise in base a due differenti tipi di esigenze: virtualizzazione dello storage e accelerazione applicativa. Per ognuno di questi carichi di lavoro sono disponibili le tre configurazioni entry level, midrange e high-end che si differenziano per la capacità storage (rispettivamente di 8, 16 e 32 Terabyte usabili) e per la quantità di DRAM. Il prezzo di listino è organizzato in base al numero di nodi.



Il sistema a disco HGST 4U60

Le soluzioni dei partner HGST e Coservit

Le soluzioni DataCore si rafforzano sul mercato anche grazie al contributo dei partner.

Tra questi si segnala Coservit, che ha sviluppato ServiceNav, una piattaforma di monitoraggio "agentless", di facile configurazione e implementazione, che permette di effettuare il monitoraggio delle prestazioni, fornire report sulla disponibilità dei servizi, facilitare la pianificazione della capacità e generare avvisi attraverso l'intero stack di soluzioni DataCore.

Tra le aziende partner di DataCore ricordiamo anche HGST, azienda del gruppo Western Digital, che ha recentemente rilasciato il sistema a disco (JBOD) siglato 4U60: una soluzione ideale per le infrastrutture iperconvergenti e le applicazioni di software defined storage, certificata per DataCore SANsymphony. Questo sistema storage è in grado di consolidare, all'interno di un unico apparato di dimensioni 4U, fino a 60 moduli a disco Ultrastar da 10 Terabyte ciascuno per fornire una capacità complessiva di 600 TB. *

Toshiba punta su client B2B e nuove soluzioni



Vendute le attività consumer, Toshiba Client Solutions diventa una sussidiaria indipendente

Riconquistare la fiducia identificando e correggendo le cause degli errori. Creare una governance più robusta e semplificando la struttura aziendale. Questa la strategia messa in pratica da Toshiba per la divisione pc, oggi diventata una sussidiaria focalizzata sul mercato B2B, dopo essere uscita dal settore consumer per concentrarsi su settori più redditizi e sostenibili. Queste le linee guida che ripoteranno al profitto già quest'anno e poi alla crescita nel 2020, la nuova Toshiba Client Solutions, come spiega Massimo Arioli, Head B2B Sales & Marketing per l'Italia (country parte della region Europea che gestisce anche Africa e Medio oriente).

Quindi più valore e meno volumi, per una Toshiba che guarda con interesse al futuro dei client mobili che va ben oltre i pc per abbracciare la miriade di dispositivi per il mercato dell'Internet delle Cose. Si amplieranno, quindi, le possibilità per i partner di canale, che al momento non cambiano (attualmente i distributori restano Espri-net, Ingram Micro, Computer Gross e Tech Data), ma che potranno beneficiare di una propensione alla customizzazione delle soluzioni e, in prospettiva, di un ingresso nel mondo IoT. Una prospettiva neanche tanto remota, considerando che in Asia ci sono soluzioni già in vendita. In Italia, si ricomincia con le nuove linee Zero Client e i modelli Portégé X20W-D,

Portégé X30 e Tecra X40, di cui abbiamo pubblicato un'anteprima a marzo. Tagliati i rami secchi, imposta una struttura di reporting chiara e coerente, la nuova società (Arioli avverte un'aria da startup, ma "con trent'anni di esperienza", sottolinea) si è dotata di maggiore agilità per prendere decisioni più rapidamente e per focalizzarsi: il 100% della ricerca e sviluppo, del controllo qualità e dell'assistenza ai clienti è dedicato alla nuova proposta di valore. Chiusi gli accordi con le terze parti, la produzione e tutta la supply chain sono interamente gestite da Toshiba, che assicura alti standard qualitativi mantenendo la garanzia "totale", con sostituzione del dispositivo nel primo anno.*

L'adozione che accelera le startup: un nuovo approccio

Dal digital hub Tilt un modello innovativo per supportare la crescita delle nuove imprese

Tilt (Teorema Innovation Lab Trieste), il digital hub creato da Teorema Engineering e Area Science Park in collaborazione con l'Università degli Studi di Trieste e Microsoft, un anno dopo la sua inaugurazione presenta un nuovo modello per supportare l'innovazione e promuovere le proprie startup.

Si tratta di "Adotta una startup": imprese clienti che non solo acquistano prodotti e/o servizi delle startup, ma supportano le stesse, sia facendo da "sponsor" sia aiutandole a superare quello che è lo scoglio principale per una nuova azienda: capire e affrontare il mercato e le sue dinamiche. Tre, fra trenta candidate, le startup "adottate": Emoj, FoodChain e Mysnowmaps. Sei le imprese "adottanti": Fincantieri, Illy

caffè, Gruppo Principe, Specogna, Geoclima e Azienda Agricola Sancin.

Lo sforzo di Michele Balbi, fondatore di Teorema, nasce dalla consapevolezza che, anche se si parla da tempo delle startup come motore d'innovazione per le aziende che vogliono avviare percorsi di trasformazione digitale e per l'intero Paese, non si arriva a nulla di concreto. «Ci sono difficoltà innegabili, come la fuga dei migliori talenti che hanno trovato all'estero in multinazionali solide il terreno fertile per sviluppare un'attività; la mancanza di capitali da investire in R&D che immobilizza molte delle nostre imprese eccellenti; il gap di competenze e know

how. Sono stato al CES di Las Vegas dove non ho trovato startup italiane», ammette Balbi.

Questi però aggiunge: «Ci si preoccupa del denaro, ma i soldi sono una cosa facile da trovare, spiega Balbi: «Molto spesso, quando vengono a presentarmi un'idea, mi accorgo che in tanti sono convinti che questa basti per cominciare a guadagnare subito, quando invece occorre lavorare e lavorare. Abbiamo creato una sinergia

virtuosa tra istituzioni, aziende, università prossime sul territorio per fondare un ecosistema dove la startup può crescere e proliferare per poi entrare in un'azienda strutturata quando è avviata».



Michele Balbi, fondatore di Teorema



Questa volta
siamo noi
a chiedere aiuto
a voi.

Fai un'offerta per una nuova ambulanza.

Servizio emergenza/urgenza 118 - auto medica - trasporto ammalati - trasporto organi - corsi di formazione di primo soccorso per aziende e per la popolazione - stazionamento ad eventi di massa - spettacoli e manifestazioni sportive - 37 sezioni in tutta la Lombardia - 100 anni storia.

Questo è quello che possiamo offrirti, tutti i giorni 365 giorni all'anno. Adesso tocca a te.

DONACI IL TUO 5 x mille: C.F. 03428670156, oppure puoi fare una donazione detraibile
(IBAN It43u0326801603000866949890)

Visita www.crocebianca.org e scoprirai come poterci aiutare.

SPECIALE FINANCE SECURITY

finance security



Nell'anno 2016 sia l'ambito globale sia quello italiano sono stati caratterizzati da un forte incremento delle attività legate al cyber-crime in ambito finanziario e il 2017 presenta trend peggiorativi. Il Rapporto Clusit 2017 delinea caratteristiche trend ed evoluzione delle minacce che interessano gli utenti, le aziende e le organizzazioni correlati ai dati di natura finanziaria.

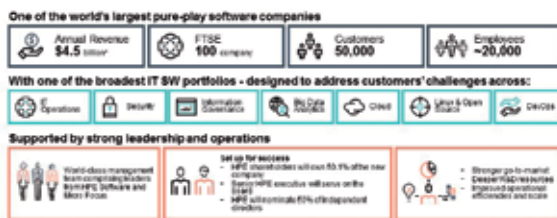
pag. 2

LA SICUREZZA HPE ANCORA PIÙ FORTE

In procinto di integrarsi con Microfocus, Hewlett Packard Enterprise sviluppa e accresce l'offerta software. La futura azienda sarà tra le prime sei software company al mondo, con oltre 50mila clienti e 4,5 miliardi di dollari di fatturato annuo, di cui il 60% costituito da sottoscrizioni ricorrenti. Avrà come Ceo Christopher Hsu, attualmente Executive Vice President, General Manager HPE Software e Chief Operating Officer di Hewlett Packard Enterprise, e come Chief Financial Officer l'attuale CFO di Microfocus, Mike Phillips.

pag. 14

Micro Focus + HPE Software



... and we're just beginning... the new company will have a strong platform for M&A.

*Using 2016 metrics as of April 30, 2017 for HPE & Software segment and the Micro Focus, based on data for the full year

IN QUESTO NUMERO:

SPECIALE

pag. 02-06

- Gli attacchi al mercato finanziario in Italia

pag. 07

- Le regole per proteggersi dalle minacce

pag. 08-09

- I principali malware per le frodi bancarie

pag. 10-11

- Il mercato illegale della compravendita di carte di credito

SOLUZIONI

pag. 12-13

- La security intelligence di FireEye a portata del mid-market

pag. 14-15

- La sicurezza HPE ancora più forte

GLI ATTACCHI AL MERCATO FINANZIARIO IN ITALIA

L'analisi a cura di Gianluigi Sisto di Reply Communication Valley riportata all'interno del Rapporto Clusit 2017, delinea lo scenario per l'anno passato del cyber crime indirizzato alle istituzioni finanziarie del nostro Paese

finance sec

Nell'anno 2016 sia l'ambito globale sia quello Italiano sono stati caratterizzati da un forte incremento delle attività legate al cyber-crime in ambito finanziario.

Reply Communication Valley, tramite il suo Cyber Security Command Center (CSCC), da anni effettua

The background image shows a hand holding a credit card over a laptop keyboard. A large red shield with a white padlock icon is overlaid on the right side of the image. The word "Security" is written in large blue letters on the left side, partially overlapping the keyboard and the shield.

Security

attività di monitoraggio a supporto di alcune delle principali realtà bancarie Italiane.

Questo punto di vista privilegiato ha consentito di analizzare le caratteristiche e l'evoluzione dei principali attacchi in Italia indirizzati all'ambito bancario nel 2016, in uno studio curato da Gianluigi Sisto e

riportato all'interno del Rapporto Clusit 2017.

L'analisi di Reply ha organizzato gli attacchi osservati in tre macro categorie:

- Attacchi di ingegneria sociale (phishing).
- Attacchi tramite malware infostealer.
- Attacchi tramite malware ransomware.

Massima efficacia sfruttando i brand più noti

Nel nostro Paese la tendenza vede ancora i malware classici ingegnerizzati per pc come responsabili per la grandissima maggioranza degli attacchi, ma gli attacchi su dispositivi mobile, in particolar modo in ambiente Android, hanno un trend in continua crescita che li ha portati al 5% degli attacchi globali osservati. Il principale vettore di attacco utilizzato per la diffusione degli attacchi sopracitati è stato, in larghissima maggioranza, lo spam veicolato attraverso posta elettronica.

Le campagne di spam sono a tutti gli effetti attacchi di ingegneria sociale, che diventano sempre più complessi e difficili da contrastare con i normali mezzi a disposizione degli utenti.

Tra le varie campagne di spam osservate in Italia sono da ricordare nel mese di febbraio quella relativa una falsa fattura ENEL da pagare con breve scadenza che portava a scaricare da un sito esterno il file Bolletta ENEL.zip, che conteneva un malware che scaricava il ransomware Cryptolocker. Altra campagna massiva di spam, sempre con l'obiettivo di diffondere malware di tipo ransomware, si è avuta tra i mesi di giugno e luglio avvalendosi del brand Vodafone per spingere gli utenti ad aprire un link contenente un exploit per Microsoft Explorer che abilitava il download e l'esecuzione di Cryptolocker. I altri casi analoghi, i cyber criminali hanno sfruttato altri marchi con messaggi quali: cartella esattoriale Equitalia, pacco DHL in consegna, fattura Telecom.

Degna di particolare attenzione è stata l'imponente

campagna di spam avvenuta su caselle certificate PEC del provider Aruba.

Attacchi di ingegneria sociale (phishing)

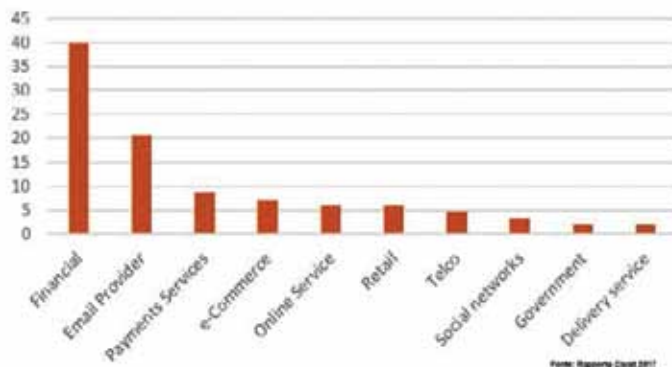
Nell'ultimo anno in Italia il CSCC ha identificato attacchi di ingegneria sociale particolarmente complessi effettuati verso alcuni istituti bancari. Questi attacchi, che ricadono nella categoria del phishing, sono particolarmente efficaci in quanto l'attacco non viene effettuato sul perimetro tecnologico della banca ma sul singolo utente.

Tra le tecniche di attacco utilizzate si segnala lo spear phishing, una forma mirata di truffa via email che prende di mira un gruppo specifico o un'organizzazione a seguito di una lunga fase di studio del target attaccato, basata sullo studio delle comunicazioni aziendali. Gli attacchi di spear phishing hanno uno schema consolidato che prevede sempre l'utilizzo di tre fattori chiave: l'email appare inviata da una persona conosciuta e di fiducia; il layout e il contenuto sono molto accurati; le istruzioni richieste sono logiche e credibili per il destinatario.

Un'altra tecnica, molto utilizzata in Italia e che si è evoluta per attaccare i sistemi bancari dotati di "strong authentication" è l'instant phishing. Il concetto di questo modello di attacco si basa sul fatto che, nell'istante in cui l'utente inserisce le credenziali o più in generale le informazioni all'interno del sito clone, il cyber criminale apre una sessione verso il vero sito della banca e utilizza, quasi contemporaneamente, queste informazioni per effettuare azioni dispositive.

Settori più colpiti dal phishing (dato percentuale)

A partire dal 2016 ha cominciato a diffondersi in Italia anche la tecnica detta del CEO Fraud che prevede attacchi di phishing mirati verso figure aziendali di altissimo profilo, tramite una email il cui testo è solitamente una richiesta di un bonifico urgente verso un determinato IBAN per un determinato motivo. L'email viene scritta come se fosse stata inviata dal CEO, dal CFO o altra figura aziendale con analoghi poteri decisionali, solitamente è molto curata in modo da non contenere elementi sospetti e contiene una motivazione apparentemente valida dell'urgenza del bonifico. È evidente che questo tipo di attacco richiede una lunghissima fase di preparazione e, per avere successo deve contare su una persona con la facoltà di gestire la richiesta, ma che sia poco esperta sui temi della sicurezza, evitando



di porsi il problema di comunicazioni fraudolente simili a quella appena ricevuta.

Attacchi tramite infostealer

L'analisi effettuata dal CSCC ha evidenziato un numero complessivo di attacchi tramite infostealer nel 2016 in linea con il dato dell'anno precedente, mentre si osserva una diminuzione del numero complessivo di attacchi effettuati tramite malware infostealer Zeus.

I principali malware infostealer operanti in Italia sono Dridex e Dyre: due malware di ultima



generazione molto più complessi rispetto alle prime versioni del capostipite Zeus.

In Italia sono state anche individuate diverse campagne di spam con l'obiettivo di diffondere il malware infostealer Gozi che predilige come target i servizi di corporate banking e sono stati identificati diversi malware "informativi" con l'obiettivo di registrare, tramite video ad-hoc, l'intera navigazione effettuata dall'utente.

Nella classifica degli attacchi in base ai target bancari è emerso che il 70% degli attacchi è diretto verso i sistemi di Retail Banking, il 25% verso i siti di gestori carte di credito, il 3% verso i sistemi di Corporate Banking e il 2% nei confronti dei principali fornitori di servizi di social media (Facebook e LinkedIn in particolare) e di servizi freemail (Gmail e Hotmail).

L'analisi dei server Command & Control relativi alle botnet responsabili degli attacchi sulle banche Italiane ha confermato gli Stati Uniti come primo Paese al mondo per hosting di questo tipo di server. Un altro dato interessante relativamente agli infostealer analizzati è che, scelto un campione di 10 dei principali antivirus commerciali, un nuovo sample di malware infostealer viene rilevato mediamente dopo 12 giorni dall'inizio della diffusione e solo due giorni dopo il picco massimo di infezioni.

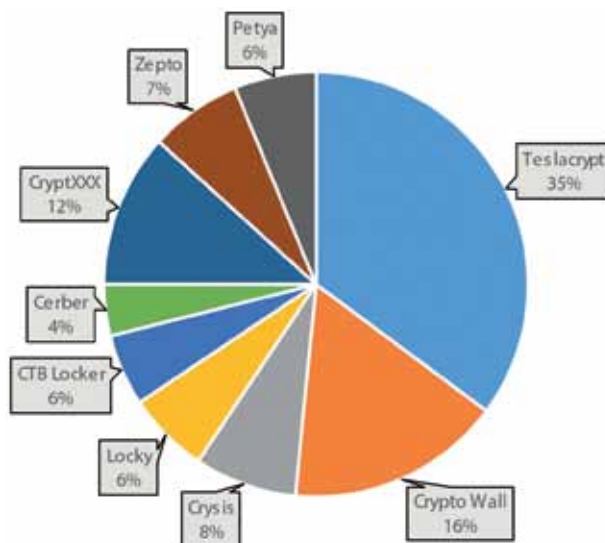
L'arco di tempo nei quali i computer sono mediamente non protetti da malware di ultimissima generazione è quindi di quasi due settimane: un periodo di tempo che risulta più che sufficiente per portare a termine una campagna di attacco da parte dei cyber criminali.

Attacchi tramite ransomware

L'Italia è una triste protagonista dello scenario relativo gli attacchi tramite ransomware, con quasi il 7% degli attacchi globali di questo tipo effettuati, indirizzati verso il nostro Paese.

Analizzando i vari ransomware che hanno attaccato il bacino di utenti Italiani si evidenzia come TeslaCrypt sia stata la minaccia principale, responsabile del 35% degli attacchi; seguono a ruota in seconda e terza posizione i ransomware Crypto Wall (16%) e CryptXXX (12%).

Nel complesso, analizzando l'insieme degli attacchi osservati è emerso che le campagne di spam per la diffusione di ransomware riescono ad aggirare i sistemi antispam con un'efficacia di circa il 20% e che il numero di utenti che effettivamente cade vittima del ransomware è di circa il 3% del totale; in ambito bancario la percentuale scende però a meno dell'1%.



*I ransomware in Italia nel 2016
(Fonte: Rapporto Clusit 2017)*

LE REGOLE PER PROTEGGERSI DALLE MINACCE



Pochi controlli di base per minimizzare il rischio

Con poche regole pratiche è possibile limitare la probabilità di successo di un eventuale malware che dovesse approdare sui nostri sistemi, riducendo se non eliminando l'impatto di potenziali azioni fraudolente. Questa è l'indicazione che proviene da IBM e riportata all'interno del Rapporto Clusit 2017.

L'insieme delle pratiche minime suggerito è di prestare la massima attenzione almeno sui seguenti comportamenti:

- fare backup periodici dei propri dati (con frequenza quotidiana o almeno settimanale) su dispositivi di archiviazione esterni, multipli (almeno 2 diversi), alternati periodicamente e mantenuti in località diverse (ad esempio uno a casa e uno in ufficio);
- diffidare da email non attese, o provenienti da mittenti sconosciuti o non credibili, specie se invitano ad aprire un allegato o cliccare su un link;
- configurare le applicazioni di office automation per aprire sempre in modalità protetta i documenti provenienti da Internet, memorizzati in percorsi potenzialmente non sicuri, o allegati a e-mail;
- avere un antivirus attivo e funzionante su ciascun dispositivo connesso ad Internet;
- attivare sull'antivirus la funzione di navigazione sicura e verifica dei link;
- attivare su tutti i browser le funzioni di navigazione sicura e verifica dei link;
- verificare periodicamente il funzionamento delle

funzioni di navigazione sicura e verifica dei link attraverso i siti di test messi a disposizione dai produttori dei browser;

- attendere sempre che l'antivirus completi la scansione di allegati a email prima di aprirli.

Le realtà enterprise dovrebbero inoltre adottare strategie più articolate per evitare o limitare attacchi aziendali, come:

- sensibilizzare i collaboratori sull'esistenza di attacchi mirati;
- utilizzare servizi di IP address reputation;
- introdurre soluzioni per il calcolo in tempo reale del fattore di rischio di ciascuna transazione;
- bloccare il traffico verso le reti di anonimizzazione;
- adottare soluzioni per la protezione dell'endpoint, con verifica dell'integrità del browser e del sistema;

Le istituzioni finanziarie dovrebbero applicare livelli di protezione ancora più avanzati come, per esempio:

- utilizzare soluzioni specifiche per la fraud-detection e l'account take-over;
- limitare l'accesso ai soli dispositivi che superino un livello considerato minimo di sicurezza;
- autenticazione a fattori multipli, autenticazione out-of-band (per esempio SMS), utilizzo della geo localizzazione del dispositivo mobile come ulteriore fattore di autenticazione;
- fornire ai propri clienti meccanismi di notifica in tempo reale di transazioni elettroniche.

I PRINCIPALI MALWARE PER LE FRODI BANCARIE

Crescono in numero e sofisticazione. La scomparsa di Dyre ha lasciato spazio a Neverquest e Dridex/Bugat

I malware specializzati per frodi bancarie e finanziarie sono certamente tra quelli più critici per pericolosità e sofisticazione. Si tratta per la maggior parte di malware che mirano a impossessarsi delle credenziali di autenticazione usate per accedere ai servizi di Web banking o, in generale ai sistemi di pagamento, per poi riutilizzarle in maniera automatica per effettuare transazioni illegittime a danno della vittima. Le frodi finanziarie hanno un risultato sempre misurabile con attendibilità: il danno è pari alle somme trasferite verso l'esterno con transazioni elettroniche fraudolente e difficilmente recuperabili.

Il 2016 ha visto l'uscita di scena del famigerato malware Dyre a seguito dell'operazione del Novembre 2015, apparentemente a opera delle autorità russe, a cui era attribuibile il 16% di tutte le infezioni individuate nel 2015.

Nel corso del 2014 e 2015 a Dyre erano state imputate frodi per decine di milioni di dollari a carico di utenti di numerose banche del Regno Unito, Stati Uniti, Australia, Spagna e in forma minore anche altre nazioni Europee, oltre a campagne di attacco mirate verso grosse organizzazioni tra cui colossale frode di 4,6 milioni di euro ai danni della compagnia

aerea Irlandese Ryanair del Maggio 2015.

Dati di IBM X-Force e IBM Security Trusteer mostrano che, per l'anno 2016, il fenomeno del malware bancario e malware specializzato in frodi finanziarie, limitatamente al panorama europeo, si è polarizzato attorno a quattro principali famiglie di malware: Neverquest, Dridex/Bugat, Gozi e Gootkit.

Numerosi altri malware sono stati usati nel corso dell'anno (per esempio Goznym, Kronos, tinba, zeus/Zeus_Citadel, corebot, urlzone, kronos, ramnit) ma, cumulativamente, la loro presenza è stata esigua e limitata a campagne di attacco mirate verso organizzazioni e soggetti specifici.

Da un punto di vista generale continua lo spostamento dall'utente individuale verso utenti aziendali e corporate, con il chiaro obiettivo di massimizzare gli importi frodati per ciascuna azione criminale.

Neverquest

Neverquest (conosciuto anche come Vawtrak) ha continuato a dominare la scena, almeno nel primo semestre. Si tratta di un banking trojan individuato per la prima volta nel 2013 e che appare come un'evoluzione della precedente famiglia di malware Gozi/ISFB Trojan, di cui condivide parti di codice e



l'infrastruttura dei server di Command-and-Control (C&C).

Dopo la scomparsa di Dyre, Neverquest si è affermato come il malware per frodi finanziarie più usato in Europa, e così è rimasto durante tutto il 2016. Neverquest è in vendita nei forum dell'undeground sin dalla sua creazione. L'aggiornamento del codice sorgente, l'infrastruttura di botnet che lo veicola e le diverse campagne che si sono susseguite nel corso dell'anno sono a cura di diverse bande di cyber criminali.

Neverquest è un toolkit completo che mette a disposizione strumenti per costruire frodi basate sul furto di credenziali. Tra le funzionalità di base ci sono strumenti di form grabbing con cattura di schermate statiche e di video, file transfer, inserimento di contenuti durante la visualizzazione di una pagina (web injection), controllo remoto della macchina via VNC, furto ed esfiltrazione di certificati.

Neverquest compromette i browser e si interpone tra l'utente e il sito web della banca durante le operazioni di web banking. Basandosi su file di configurazione scaricati dalla rete di Command & Control e costantemente aggiornati, Neverquest è in grado di mostrare contenuti addizionali sullo schermo (web injects) e catturare quanto digitato sulla tastiera per poi inviarlo all'esterno in forma cifrata. Finora le configurazioni di Neverquest hanno avuto come obiettivo principale siti di web banking e altre istituzioni finanziarie di lingua inglese.

Dridex

Dridex (evoluzione del malware Bugat) è stato nel 2016 il malware osservato nel maggior numero di varianti, con una conseguente difficoltà di individuazione da parte dei prodotti antimalware. È un malware specializzato nel furto di credenziali per l'accesso a siti bancari. Di Bugat si ha traccia fin dal 2009. Da allora gli sviluppatori di questo malware hanno gradualmente aggiunto funzionalità, fino alle più recenti tecniche di evasione dagli antivirus. Dal codice principale di Bugat sono state sviluppate varianti di codice con nomi diversi, i più comuni sono Dridex e Cridex. Il vettore d'attacco sono email di spear phishing che inducono la vittima ad aprire documenti Office allegati all'email, oppure raggiunti tramite un link. Questi documenti contengono macro o script oppure, a loro volta, rimandano a siti Web sul quale è ospitato codice che scandisce la macchina della vittima alla ricerca di eventuali vulnerabilità. Successivamente è scaricata la componente principale del malware che sfrutta proprio le vulnerabilità presenti sulla macchina e installa localmente il malware. Il furto delle credenziali avviene attraverso web injects, ovvero contenuti da far comparire nel browser, e keylogger che al momento opportuno tracciano quanto digitato sulla tastiera e lo inviano verso l'esterno.

conoscere l'indirizzo esatto del market che si vuole raggiungere sia avere un accesso privato a esso. Molti black-market specializzati in carding mettono a disposizione dei propri utenti dei servizi di "checker" che eseguono una micro transazione tipicamente verso organizzazioni no-profit, per testare la validità delle carte acquistate sul market. Inserendo i dati delle carte (numero, scadenza, cvv), il checker restituisce il risultato del test effettuato sulla carta, generalmente nella forma "valida" o "non valida". Un black-market tipico può supportare molteplici funzionalità, quali: accesso protetto da password, filtri avanzati di ricerca (Paese, banca, tipo carta, livello, indirizzo, cap e così via), comunicazioni multilingua, per arrivare a fornire anche servizi di customer care (tramite ticketing).

Meno di venti dollari per comprare la vostra carta di credito

I dati delle carte di pagamento sono venduti sui black-market a prezzi variabili in base a diversi fattori che possono essere specifici della carta in vendita come il circuito (per esempio, Visa, MasterCard, JCB, American Express) o la classe di livello (per esempio, Visa Electron, Visa Classic, Visa Gold) oppure relativi alle informazioni disponibili e messe in vendita, come: i dati della carta (numero, scadenza e CVV), il nome dell'intestatario, il suo indirizzo e numero di telefono, il PIN e altri dati aggiuntivi. La completezza dei dati e il plafond disponibile sulla carta (dipendente da circuito e livello) sono i fattori principali che determinano le variazioni dei prezzi delle carte di pagamento vendute. Nella maggior parte dei black-market, una carta viene venduta a un prezzo variabile fra gli 8 e i 15 dollari.

La maggior parte dei black-market presenti in rete ha a disposizione dati prevalentemente statunitensi, poiché negli USA le carte di pagamento non integrano i chip elettronici ma sono dotati solo di banda magnetica. Tuttavia sono presenti numeri significativi anche per quanto riguarda le carte emesse da istituti di paesi europei, fra cui l'Italia.

Il supporto tramite FAQ disponibile sul sito



LA SECURITY INTELLIGENCE DI FIREEYE A PORTATA DEL MID-MARKET

L'azienda specializzata in cyber security rilascia il report M-Trends 2017 che delinea gli scenari a livello globale delle minacce. Nel contempo amplia la propria proposizione commerciale indirizzandosi verso le aziende di dimensione media lanciando la piattaforma integrata Helix

di Riccardo Florio

Acinque anni di distanza dal suo arrivo in Italia, FireEye si conferma un'azienda in crescita e tra le realtà più interessanti all'interno del competitivo mercato della sicurezza ICT.

Focalizzata sul tema della cyber security con un'attenzione agli aspetti di security intelligence e un approccio orientato ai servizi, FireEye si avvale delle tecnologie di intelligence iSight e delle competenze e servizi nell'ambito dell'Incidente response ottenuti con l'acquisizione tre anni fa di Mandiant (azienda presente in quasi tutte le aziende top 500 americane e meno nota in Europa).

La focalizzazione sugli aspetti di resilienza della sicurezza resta la direttrice strategica dell'azienda, che sta ampliando il proprio target, finora concentrato sul "government" e sulle realtà di livello enterprise che dispongono di un Security Operation Center (SOC), anche verso il mid-market. Questo passaggio è legato al recente lancio di Helix, una piattaforma integrata e modulare di sicurezza per la

rilevazione, l'analisi e la risposta alle minacce che, di fatto, mette a disposizione un "SOC in a box" erogato in forma di servizio, appannaggio anche delle realtà più piccole, che non dispongono delle risorse e del know how per realizzare un SOC in casa.

Una svolta che, Marco Riboli, vice president Southern Europe di FireEye, ritiene che contribuirà ad ampliare notevolmente la penetrazione dell'azienda sul mercato italiano.

«Attualmente FireEye vanta in Italia un centinaio di clienti - precisa Riboli - che ricadono tra le società di primaria importanza, che devono confrontarsi con

minacce crescenti in numero e sofisticazione. Trentasei dei nostri clienti li abbiamo acquisiti lo scorso anno, segno che la sensibilità verso il tema della sicurezza sta cambiando. Il mid-market richiede fortemente queste soluzioni e sono convinto che troveremo ampio riscontro. FireEye rappresenta l'eccellenza per quanto riguarda l'Incident response grazie soprattutto alle tecnologie e competenze di Mandiant,



*Marco Riboli, Vice
Presidente per il Sud
Europa di FireEye*

Il Report M-Trends 2017

che è l'azienda che ha dato una svolta metodologica innovativa alla gestione degli incidenti».

FireEye eroga alcuni servizi specifici direttamente ma, prevalentemente, opera attraverso una serie di partner "managed" con cui l'azienda di sicurezza lavora costantemente: Security Reply, Puntotit, R1, Sorint, Innovery, Leonardo, CY4GATE, 7Layers, Lutech, Business E, Var Group. In Italia le soluzioni FireEye sono distribuite da Arrows ed Esclusive Networks che gestiscono un centinaio di partner attivi.

Il report M-Trends 2017 e la situazione italiana

Da diversi anni Mandiant pubblica M-Trends, un report che analizza a livello globale e per aree geografiche lo scenario degli incidenti, per fornire indicazioni su tendenze ed evoluzione dell'attività criminale.

L'Italia in EMEA si colloca al quinto posto come target per gli attacchi e solo il 6% delle aziende interpellate da Mandiant ritiene di non essere a rischio; nonostante ciò un terzo delle aziende soprattutto del settore small e medium investe poco o nulla in sicurezza.

La nuova edizione del report evidenzia che l'attività di cyber crime in Italia è incrementata del 33% rispetto all'anno precedente. Questo anche grazie alla grande facilità con cui le infiltrazioni riescono a

essere efficaci: segno di una carenza culturale in ambiti quali il contrasto al phishing. Gli attacchi hanno generato quasi 9 miliardi di perdite e il target tende ad ampliarsi al di fuori dei settori più tradizionali come quello finanziario.

Tra i "numeri" di rilievo vi è il tempo di permanenza medio di un attaccante all'interno di un ambiente compromesso, che è di 106 giorni nelle organizzazioni EMEA e di 99 giorni su scala globale. Un dato in rapida diminuzione, soprattutto in Europa, anche se si mantiene ancora troppo elevato: a livello globale era di 243 giorni nel 2012 e di 146 nel 2015 mentre in EMEA nel 2015 era di 469 giorni.

Un altro dato interessante è che gli attaccanti con motivazioni finanziarie hanno raggiunto nuovi elevati livelli di sofisticazione spostandosi verso l'uso di backdoor personalizzate con una configurazione unica per ogni sistema compromesso, incrementando il livello di resilienza della loro infrastruttura e migliorando le tecniche anti-forensi utilizzate.

Mandiant segnala anche che nel 2016 gruppi di cyber criminali russi hanno avuto un'ingerenza nelle elezioni presidenziali statunitensi e che ci sono segnali che questi gruppi rivolgeranno le loro prossime attenzioni anche alle elezioni europee.

Tra le indicazioni fornite dal report vi è anche l'invito rivolto alle organizzazioni che risiedono in EMEA a dedicare particolare attenzione ai rischi per il settore energetico e i sistemi di controllo industriali, verso i quali sembra si sta concentrando l'attenzione del cyber crime.

Il report completo M-Trends 2017 è disponibile a questo link: https://www2.fireeye.com/RPT_IT_M-Trends_2017.html

LA SICUREZZA HPE ANCORA PIÙ FORTE

In procinto di integrarsi con Micro Focus, Hewlett Packard Enterprise sviluppa e accresce l'offerta software

di Gaetano Di Blasio

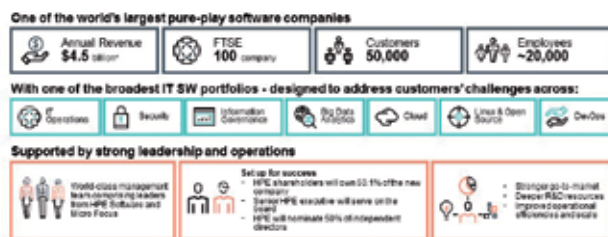
Le risorse combinate di HPE e Micro Focus

Dimitri Crea, channel manager di HPE, intervenuto al Partner Summit di Coretech, ha illustrato l'offerta software che Hewlett Packard Enterprise "porta in dote" nella nuova società che prenderà corpo dopo la fusione tra HPE e Micro Focus: «Noi forniamo un portfolio di livello enterprise completo di soluzioni "best in class" con capacità di analytics integrate. L'operazione prevede lo spin off della divisione software di HPE e la successiva fusione, per un valore complessivo di 8,8 miliardi di dollari, di cui 6,3 miliardi saranno distribuiti come quote della nuova azienda (per un totale di 50,1%, con un valore previsto di 6,3 miliardi di dollari), mentre altri 2,5 miliardi saranno riconosciuti in cash.

La futura azienda avrà come Ceo Christopher Hsu, attualmente Executive Vice President, General Manager HPE Software e Chief Operating Officer di Hewlett Packard Enterprise, e come Chief Financial Officer l'attuale CFO di Micro Focus, Mike Phillips.

Secondo Crea, la futura società sarà tra le prime sei software company al mondo, con oltre 50mila clienti e 4,5 miliardi di dollari di fatturato annuo, di cui il 60% costituito da sottoscrizioni ricorrenti.

Aldilà delle cifre, sono da considerare i software che HPE andrà ad aggiungere al portafoglio di Micro Focus, in ambiti quali i Big data (con Idol, Vertica e HPE



Haven on Demand), le soluzioni di cloud orchestration e data center operation, l'application delivery e management (con ALM e AppPulse), le soluzioni per l'enterprise security (con Fortify, ArchSight, Atalla e Voltage Security, e, per ultime ma non ultime quelle dell'Information management e governance (con VM Explorer, Data Protector e Storage Optimizer).

Proprio queste ultime sono tra quelle che Crea ha evidenziato, ricordando che una delle più importanti soluzioni per fronteggiare i ransomware è un solido sistema di backup e recovery.

HPE VM Explorer, ha spiegato il manager italiano, è la migliore soluzione per il backup di ambienti VmWare e Hyper V, proteggendo e replicando ambienti virtuali per le piccole e medie imprese.

Tra le funzionalità principali: backup completi o incrementali, storage snapshot, disaster recovery basato su replica degli ambienti e test automatici dei backup e recovery delle virtual machine, replica server to server veloce. Cinque i livelli di restore, mentre i backup sono indirizzabili verso supporti quali: NAS, dischi, nastri o cloud.

Altre caratteristiche comprendono un task Scheduler, gestione tramite Command Line Interface, rapporti inviati via mail. Per gli ambienti più esigenti di taglio enterprise, VM Explorer aggiunge: Instant virtual machine recovery (IVMR) per ESX/ESX; cinque livelli di restore dal cloud e test automatici dei backup su cloud; interfaccia Web multiutente; supporto per vMotion su IVMR; supporto VMware vSAN; encryption (256 bit AES) support per snapshot storage EMC ScaleIO.

Massima flessibilità nella destinazione dei backup è garantita sia on premise sia in cloud, dove le imprese possono scegliere tra Amazon S3, OpenStack, Helion & Rackspace, Azure e possono costruire la propria infrastruttura di backup Object Storage, basata su OpenStack.

Tra i clienti, figurano Ricoh, Greenpeace, Hitachi, Swiss Aviation Software, Nokia, Asus, Avaloq, WWF, Swisscom, SAP, Veolia, Siemens, Sungard, Mizou, T System, ThyssenKrupp, Caritas, Infinigate.

Quattro famiglie di soluzioni per una protezione a 360 gradi

La nuova società riceverà in dote il ricco portafoglio di soluzioni software che definiscono l'approccio di Predictive Security sviluppato da HPE.

Quattro attualmente le famiglie di prodotti, per abilitare una protezione a 360 gradi.

La gamma ArcSight raggruppa i componenti della soluzione di Security Information and Event Management (SIEM) di HPE che, da 13 anni di seguito, è inserita da Gartner tra i leader all'interno del suo Magic Quadrant per questo tipo di soluzioni. ArcSight rappresenta una piattaforma integrata per l'individuazione delle minacce e la gestione della compliance che abbina un motore avanzato per la raccolta, l'analisi e la correlazione delle informazioni e dei log di sicurezza, con una piattaforma (ArcSight Data Platform) che sfrutta le più avanzate tecnologie di Machine Learning e la capacità di correlazione in tempo reale di dati provenienti da qualsiasi fonte, per fornire visibilità immediata sulle attività che interessano l'intera infrastruttura enterprise.

Fortify è l'insieme di soluzioni per la sicurezza delle applicazioni che rappresentano, attualmente, il principale vettore di attacco. La gamma di soluzioni Fortify si avvale di tecnologie di autoprotezione RASP (Runtime Application Self Protection) e permette di realizzare un approccio allo sviluppo del codice applicativo di tipo "secure by design", eliminando alla fonte le possibili vulnerabilità e predisponendo ambienti di test di tipo statico, dinamico e in tempo reale adatti a verificare le caratteristiche di sicurezza del codice. Questo livello di protezione viene fornito anche come servizio on-demand per sottoporre a verifica il livello di sicurezza di ogni tipo di applicazione, incluse quelle commerciali.

Voltage è l'insieme di soluzioni per la crittografia dei dati e l'accesso sicuro basato su token adatte per ambienti enterprise, cloud, mobile e Big Data. Realizza un approccio che consente di applicare la sicurezza nel punto di creazione del dato e di seguirlo in ogni condizione: sia a riposo sia in movimento.

La gamma di soluzioni Atalla abilita un approccio alla protezione delle informazioni che sfrutta tecniche innovative di cifratura, proteggendo i dati on-premise e nel cloud e rendendo sicure le transazioni elettroniche.

SICUREZZA COSTANTE, INTELLIGENTE

E PUOI AVERLA SUBITO.

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

I cybercriminali sono sempre più scaltri.

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

Visita www.fortinet.it per maggiori informazioni.

FORTINET®

Sicurezza senza compromessi

Da CIE un Gateway IoT di classe professionale

Il gateway CTS iCPE permette la gestione di sensori e attuatori certificati Z Wave e la connessione di backup su reti 3G/4G

Il mondo dei dispositivi interconnessi sta esplodendo e i produttori di soluzioni di networking sia di back bone che di accesso stanno di conseguenza incrementando il proprio interesse per un settore che si preannuncia molto promettente in termine di mercato e di business.

Nell'arena dei dispositivi IoT è entrata anche CIE Telematica, società di ingegneria italiana che ha introdotto nel proprio portfolio di prodotti per reti di accesso fisse e mobili e di CPE fisici e virtuali, anche il gateway iCPE progettato per l'erogazione di servizi IoT prodotto da CTS, di cui è distributore e system integrator.

L'apparato è ai fini di rete un gateway di layer 2, di classe professionale e gestito, caratterizzato da funzioni

robuste di sicurezza ed è indirizzato a un mercato non consumer. Dispone, ha evidenziato CIE Telematica, di funzionalità di protezione di svariati tipi in modo da assicurare sia elevate prestazioni sia un delivery molto affidabile delle operation. Lo sviluppo di questo prodotto, spiega CIE, ha recepito i desideri e le esigenze specifiche di operatori nel settore delle fibre ottiche, di gestori di real estate, del settore dell'health care e dell'energia, tutti ambienti molto interessati ad applicazioni IoT di tipo professionale.

La fascia professionale del dispositivo è confermata dalle soluzioni di backup che integra per garantire la connessione di rete.

Dispone in proposito di batterie che lo rendono autonomo nel caso l'alimentazione

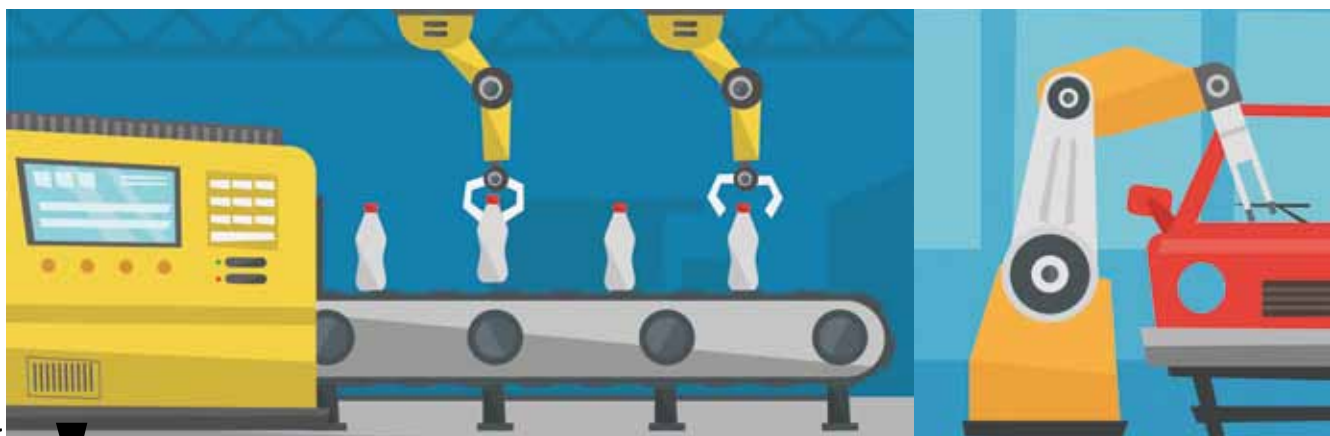
principale dovesse interrompersi per un guasto interno o esterno e di una connessione di back-up su rete mobile 3G/4G nel caso ci dovessero essere problemi sulla connessione di rete fissa.

È anche possibile differenziare l'offerta di servizi basati su QoS mediante strumenti di gestione e di monitoraggio bidirezionali dell'intera piattaforma installata e dei servizi che sono supportati, arrivando sino al controllo dello stato di funzionamento dei sensori e degli attuatori connessi al dispositivo.

Sensori e attuatori sono connessi tramite la tecnologia wireless Z-Wave, che permette di mantenere bassi i consumi energetici e garantire un'elevata sicurezza di funzionamento del dispositivo.

Le sfide per l'industria manifatturiera

Una ricerca Fujitsu evidenzia che 3/4 dei leader dell'industria manifatturiera vedono la tecnologia come la chiave per il futuro successo. I dati per l'Italia



Linnovazione digitale è la più grande sfida del settore manifatturiero secondo quasi 2/3 (62%) dei manager che hanno partecipato ad una recente indagine (“Fit for Digital: Co-creation in the Age of Disruption”) commissionata da Fujitsu, a livello globale. Lo studio conferma che gli effetti della crescente digitalizzazione siano diffusi in molti settori e i principali manager delle aziende di medio/grandi dimensioni concordano su come questo processo stia ridefinendo il modo in cui operare sul mercato.

Il settore manifatturiero è tra i più ottimistici per quanto riguarda l'innovazione digitale, con più di 2/3 (69%) “entusiasti” riguardo la digitalizzazione (percentuale che però scende al 47% per il campione italiano), e ben l'80% che ha dichiarato come questo fenomeno rappresenti una forza positiva per il proprio business e per l'intero settore (il 67% a livello italiano).

Per quanto concerne l'Italia, emerge che il principale impatto derivante dalla digital disruption, fin'ora, per il settore è una maggiore spinta al cambiamento

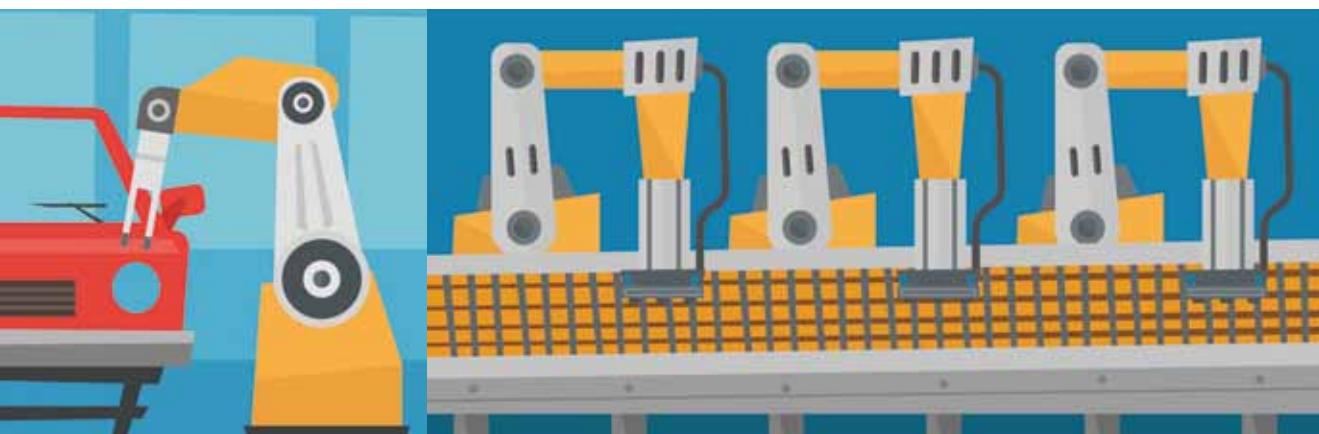
e all'innovazione (50%). Tra i 250 capi di aziende manifatturiere intervistati a livello globale, quasi tutti (il 98%) hanno dichiarato che la propria organizzazione è già stata impattata dai fenomeni di innovazione digitale - cosa vera per il 73% del campione italiano - mentre il 92% della totalità del campione e l'88% del campione nazionale, ha affermato di avere in atto progetti per

affrontare la digital disruption, il 66% del campione indica sia gli investimenti in tecnologia e innovazione sia l'individuazione di specifiche competenze, e il 37% indica invece il cambio di strategia di business e lo sviluppo di nuovi prodotti e servizi.

In termini di approccio, la ricerca ha poi evidenziato come i manager del settore manifatturiero siano molto pragmatici nel non soprav-

lo sviluppo di partnership strategiche.

«I top manager dell'industria manifatturiera credono che la tecnologia e l'innovazione siano la chiave di successo per il loro futuro. Inoltre, lo studio evidenzia come gli intervistati non stiano sovrastimando le proprie capacità, riconoscendo di dover fare di più per sviluppare correttamente le proprie attività digitali e, per questo,



sfruttare al massimo le opportunità che questo processo può offrire.

A livello italiano, i clienti (per il 45% del campione) e i partner e terze parti (per il 26% del campione) hanno avuto un ruolo fondamentale nell'influenzare il cambiamento del settore.

Nel settore manifatturiero nazionale lo studio ha messo in evidenza più aspetti: tra le misure messe in atto per

valutare la propria abilità nell'utilizzare la giusta tecnologia: il 71% ha infatti dichiarato che collaborare con esperti di tecnologia è vitale per il successo futuro. Lo sviluppo di partnership con altre organizzazioni è anch'esso visto come una chiave per poter gestire l'innovazione tecnologica. Il 36% (il 33% a livello locale) ha infatti dichiarato di avere già in programma

stanno stabilendo partnership strategiche per definire i propri piani di sviluppo. Tuttavia questo processo comporta che le aziende dovranno muoversi sempre più velocemente nel futuro per poter tenere il passo con l'intero settore», ha commentato Christof Schleidt, Director Business Development e Trasformazione Digitale di Fujitsu. ❁

Nuova infrastruttura tecnologica per Reale Mutua

TIM e Dimension Data hanno realizzato un progetto che abilita nuovi servizi orientati alla collaborazione e al team working in linea con i requisiti di consolidamento e internazionalizzazione del Gruppo

Fondata a Torino nel 1828, la società Reale Mutua di Assicurazioni è la più importante Compagnia di assicurazioni italiana in forma di mutua. È capofila di Reale Group, un gruppo internazionale nel quale operano più di 3.180 dipendenti per tutelare oltre 3,8 milioni di assicurati. TIM e Dimension Data Italia sono gli artefici della realizzazione di un complesso progetto di rinnovamento dell'intera infrastruttura tecnologica per Reale Group.

In un contesto di apertura all'internazionalizzazione e con l'obiettivo di consolidare in un'unica sede gli altri uffici decentrati sul territorio torinese, la progettazione della nuova sede di Reale Group e il relativo rinnovamento dell'headquarter doveva soddisfare i molteplici requisiti di collaboration tra le diverse realtà, soprattutto a livello internazionale. Da qui la necessità di realizzare un'infrastruttura tecnologica di comunicazione

unica che includesse elementi di connettività e di sicurezza locali e altre componenti remote presso i data centre del Gruppo, oltre a ulteriori requisiti spagnoli. Nel 2015, infatti, nasceva Reale Ites, società creata per l'erogazione di tutti i servizi IT verso i clienti del Gruppo e confluenza delle due direzioni IT italiana e spagnola.

Questo unitamente all'elevata disponibilità e affidabilità di banda per garantire un network che servisse da hub comune a tutti i servizi di building. Imperativa anche la solidità dell'infrastruttura tecnologica per disporre di numerosi contenuti legati al digital signal, streaming e video conferenze per il trasferimento di contenuti video.

Il progetto prevedeva la realizzazione di un "campus metropolitano" in fibra con anello ottico ridonato, la realizzazione di tutta l'infrastruttura LAN e la copertura mobile indoor del nuovo building.

Un'infrastruttura ad alta efficienza

Fondamentale per il progetto è stata tutta la parte di connettività seguita da TIM che ha supportato il Gruppo Reale nella realizzazione degli anelli ottici, tra cui

e wireless, oltre alla realizzazione del campus metropolitano in fibra, al cabling e al posizionamento fisico delle apparecchiature.

Infine, Reale Mutua ha colto l'occasione per riconsiderare e aggiornare anche alcu-

e comunicazione spinta - commenta Giulio Perone, Responsible Network and Communication Systems di Reale Ites -. Un progetto realizzato anche a Madrid grazie a Dimension Data Spagna, che ha permesso di



anche quello metropolitano a 10GB, tra la nuova sede e l'headquarter, nonché la parte di connettività Internet di campus. Inoltre, TIM ha provveduto alla copertura indoor di tutti i locali del nuovo building.

La collaborazione tra Reale Group, TIM e Dimension Data ha consentito di realizzare l'infrastruttura in LAN locale e tutta la parte di infrastruttura wireless del campus nel suo complesso. Inoltre, è stato rivisto completamente il livello di accesso alla rete LAN, sia in modalità wired sia wireless, il livello di core della parte di infrastruttura dati, nonché le relative attività di assessment della copertura dei servizi wired

ne componenti tecnologiche dei servizi del data centre di Reale Group insieme al team TIM - Dimension Data, in qualità di fornitore per la parte della sicurezza, presso Cedacri.

Altro elemento fondamentale del progetto, contestuale e contemporaneo a quanto affidato a TIM e Dimension Data Italia, è stata la realizzazione del nuovo building spagnolo per il quale sono state adottate le stesse tecnologie e modalità operative del palazzo torinese.

«TIM e Dimension Data hanno costruito per noi l'infrastruttura necessaria per l'erogazione dei nostri servizi: multimedialità, video intensivo, collaborazioni

realizzare un'autostrada su cui corrono i medesimi servizi e che ci offre, quindi, le stesse opportunità».

Grazie a questa infrastruttura Reale Group ha abilitato nuovi servizi orientati alla collaborazione e al team working che vengono utilizzati quotidianamente e senza i quali verrebbe a mancare anche quell'identità ormai internazionale del Gruppo. Servizi grazie ai quali Reale Mutua e tutto il Gruppo Reale sono in grado di risparmiare su costi e tempi, di ottimizzare la collaborazione interna e, contemporaneamente, di offrire a tutti i suoi utenti gli stessi servizi e prestazioni, garantendo la medesima user experience. ✨

Veeam Availability Suite 10 per un'azienda always-on

L'azienda specializzata nelle soluzioni enterprise di alta disponibilità annuncia la nuova versione del suo prodotto di punta e nuove funzionalità che estendono ulteriormente il livello di integrazione, supporto e flessibilità della sua piattaforma

A 10 anni dalla sua costituzione, Veeam continua a “costruire” sulla sua piattaforma e sul concetto di Availability per aziende always on, che ne stanno facendo una delle aziende in maggiore crescita del settore, reduce da 34 trimestri di crescita, con un fatturato di 800 milioni di dollari e indicata tra i leader di settore da analisti quali Gartner, IDC e Ovum. A decretare il successo dell'azienda in questi anni ha contribuito non solo l'elevato livello di flessibilità della piattaforma ma, soprattutto, l'elevato indice di gradimento evidenziato dalla propria base di clienti. L'evento annuale VeeamON 2017, in corso in questi giorni, è l'occasione per introdurre una serie di novità che estendono ulteriormente la flessibilità e la portata delle soluzioni di Veeam.

«Da 10 anni Veeam continua a innovare

la propria tecnologia core - ha osservato Peter McKay President e Co-CEO di Veeam -. Siamo il fornitore di backup in cloud numero uno, i primi nella virtualizzazione, abbiamo creato il mercato dell'availability e siamo riconosciuti dagli analisti di mercato come leader di questo segmento. Ora Veeam è la prima azienda a garantire la continuità operativa 365 giorni all'anno, 24 ore su 24, per la vita digitale delle persone».



*Peter McKay,
President e
Co-CEO di
Veeam*

Veeam Availability Suite 10

L'annuncio della versione 10 della soluzione di riferimento di Veeam introduce molteplici novità di carattere tecnologico e funzionale. Il supporto per i server fisici e per il backup e restore su dispositivi NAS (Network Attached Storage)

permette di estendere la protezione agli ambienti del business di un'azienda collegati ai workload che si basano su sistemi che non sono (o non possono essere) virtualizzati. Un'altra novità è l'introduzione delle funzioni di Continuous Data Protection (CDP) con cui Veeam mette a disposizione dei service provider nuove opportunità di fornire servizi a maggior valore e aiutare i propri clienti a preservare i dati delle loro applicazioni business critical in uno scenario di disastro. Sfruttando le funzioni di replica continua su cloud privato o gestito, Veeam promette di riuscire a garantire la disponibilità dei dati con capacità di ripristino dell'ordine dei secondi. CDP può anche essere utilizzato con Veeam Cloud Connect per utilizzare come target primario lo storage in cloud.

L'introduzione in Veeam Availability Suite 10 del supporto nativo per Object storage aggiunge caratteristiche di "agility" nello spostamento dei dati e si propone di ridurre i costi legati alla compliance e alla Data retention sfruttando funzioni di gestione automatizzata basata su policy per liberare backup su storage primario di costo elevato. Veeam prevede il supporto per un'ampia gamma di piattaforme di Object storage su cloud incluse Amazon S3, Amazon Glacier, Microsoft Azure Blob e tutto lo storage compatibile con S3/Swift.

L'introduzione all'interno di Veeam Availability Suite v10 di una nuova Universal Storage API amplia l'ecosistema di partner strategici aggiungendo, all'esistente supporto per i sistemi di Cisco, Dell, NetApp, Nimble,

Exagrid e HPE, anche quello per le soluzioni di IBM, Lenovo e Infinidat.

Con i nuovi annunci Veeam ha posto le basi per quella che definisce: la prima soluzione di settore agentless, nativa per il cloud, per la disponibilità e la data protection delle applicazioni AWS. Le nuove funzionalità per gli ambienti AWS sono pensate per aiutare le aziende di livello enterprise a predisporre in modo affidabile il processo di spostamento e gestione verso un ambiente multi cloud. Le nuove funzionalità consentono il backup e restore per le istanze in cloud AWS EC2, riducendo i rischi nell'accesso alle applicazioni e garantendo la protezione dei dati in caso di cancellazioni accidentali, attività dannose o compromissioni. Veeam ha annunciato anche il lancio di un nuovo agent



per Windows pensato per fornire protezione in tre scenari chiave: semplificazione nella protezione dei sistemi in ambienti public cloud, garanzia di massima disponibilità per sistemi in ambiente Windows che non possono essere virtualizzati, maggiore efficienza per la forza lavoro che opera in mobilità.

I miglioramenti nel Disaster Recovery as a Service (DRaaS)

Veeam ha anche annunciato una serie di miglioramenti legati al tema del Disaster Recovery as a Service.

Il primo di questi è l'integrazione di vCloud Director con Veeam Cloud Connect Replication, che consente ai service provider partner di Veeam di semplificare le configurazioni di tipo "multi tenancy" offrendo la possibilità ai tenant di accedere in modo semplice a repliche delle console delle macchine virtuali in situazioni di disastro, sfruttando le funzionalità native di vCloud Director. Grazie alla nuova offerta di Tape as Service, Veeam abilita il ripristino da nastro fornendo un ulteriore livello di protezione in casi di disastri che comportino la perdita completa di tutto lo storage,

per esempio, nei casi di situazioni compromesse da ransomware o da minacce interne. Questa offerta di servizi si dimostra particolarmente efficace anche per i "tenant" che operano all'interno di settori che richiedono specifici standard di compliance.

Nuove soluzioni dai partner

La piattaforma di availability di Veeam si amplia anche grazie a una serie di nuove soluzioni sviluppate dai partner. Veeam's content pack for VMware vRealize Log Insight è un nuovo strumento di analytics per la Veeam Availability Suite pensato per fornire agli utenti una visibilità aumentata e una capacità di analisi e gestione

dell'infrastruttura Veeam.

Le funzionalità di analytics e ricerca federata offerte da Data Gravity rispondono alle esigenze di conformità agli standard governativi e si indirizzano ai professionisti dell'IT, della sicurezza e della virtualizzazione.

Infine, StarWind VTL per AWS and Veeam fornisce una soluzione per rimpiazzare lo storage su nastro in modo scalabile, spostandolo su soluzioni Object storage Amazon S3 e Amazon Glacier.

Rilasciata anche la versione 1.5 di Veeam Backup for Microsoft Office 365 che estende ulteriormente il livello di disponibilità e di automazione per l'ambiente cloud di produttività personale di Microsoft. ❁



Veeam e Microsoft: una partnership che si rafforza nel cloud

Rilasciata una nuova soluzione per il disaster recovery in ambienti Microsoft Azure e la versione 1.5 di Veeam Backup for Office 365.

Il cloud è già qui secondo Paul Mattes, vice president, global Cloud Group di Veeam, e sta portando un impatto maggiore rispetto a qualsiasi tecnologia comparsa finora con una diffusione nell'adozione che sarà la più veloce di sempre.

In questo scenario di enormi opportunità di business, il cloud si sposa con il focus di Veeam di fornire availability per ogni servizio e attraverso ogni infrastruttura, e una componente importante è legata alla partnership con Microsoft.

Nel corso dell'evento annuale VeeamON 2017, l'azienda ha annunciato un rafforzamento del supporto delle soluzioni Microsoft con una serie di nuove soluzioni e aggiornamenti di prodotti già consolidati.

Al mondo Microsoft Azure si indirizza una soluzione di disaster recovery composta da Direct Restore to Microsoft Azure e dal tool gratuito chiamato Veeam PN (Power Network) for Microsoft Azure. La combinazione di questi due strumenti promette di minimizzare i tempi di downtime semplificando e automatizzando il setup di un processo di disaster recovery on-demand verso le soluzioni Azure.

Il rilascio della versione 8 di Veeam Management Pack, la soluzione per l'integrazione con la Microsoft Operations Management Suite, mette a disposizione all'interno della Suite di Microsoft una serie di cruscotti supportati da Azure per monitorare vSphere, Hyper-V e le soluzioni Veeam di backup e replica.

Annunciata anche la versione 1.5 di Veeam Backup for Office 365, che incrementa il livello di automazione dell'ambiente di produttività personale di Microsoft con funzionalità per automatizzare le API RESTful e PowerShell SDK (Software Development Kit); l'obiettivo è

di minimizzare il carico gestionale, migliorare i tempi di ripristino e ridurre i costi. La nuova versione migliora anche il livello di scalabilità, mettendo a disposizione un'architettura multi-repository e multi-tenant che consente il deployment di grandi ambienti Office 365 tramite una singola installazione. Inoltre, offre ai service provider nuove opportunità di business grazie alla possibilità di fornire servizi di backup di Office 365.

Veeam ha annunciato che nella versione 2 di Veeam Backup for Office 365, il cui rilascio è previsto a breve, sarà introdotto il supporto per Microsoft SharePoint online e per OneDrive.



Centro Computer abilita la Digital Transformation

Centro Computer, società di consulenza specializzata in prodotti, servizi e soluzioni IT per le aziende, ha ampliato la strategia "Vision 2020" con investimenti in strumenti e nuove risorse, per indirizzare al meglio le esigenze di business che le aziende devono affrontare nei prossimi anni.

L'azienda ha chiuso il 2016 positivamente con un fatturato pari a 36 milioni di euro, grazie anche all'incremento delle attività e all'ampliamento dell'offerta, che hanno consentito di allargare il suo raggio d'azione sul territorio con progetti significativi nelle differenti aree di specializzazione. In altri termini è cresciuta del 26% per i servizi gestiti e in particolare per quanto concerne i Managed Service Provider, che permettono alle aziende di beneficiare della formula dei canoni operativi mensili,

Centro Computer cresce e rende operativa "Vision 2020", la strategia che ha sviluppato per guidare le aziende nella trasformazione dell'IT

senza l'onere di dover acquistare postazioni e apparati, con la massima disponibilità di utilizzo, assistenza e manutenzione.

È anche proseguita la sua strategia di acquisizione a portfolio prodotti delle imprese di medie e grandi dimensioni, con nomi del calibro di Decathlon, Acetum, Granarolo e Gi Group, mentre si è leggermente ridotta la sua attenzione verso le aziende più piccole.

Tra le nuove partnership siglate con i leader nel comparto dell'UCC, figurano Enghouse, multinazionale esperta nel comparto della Customer Experience & Interaction Management

con una soluzione per i call center, e Re Mago, che ha apportato una soluzione per le sale riunioni. Entrambe le applicazioni si integrano poi con Microsoft Skype for Business.

«Stiamo operando



con assiduità presso le aziende, portando veri e propri messaggi di evangelizzazione sui temi legati all'IoT, mobility e smart working. Come sempre, l'esperienza è quello che abbiamo e sentiamo dentro di noi. Al primo posto abbiamo messo i nostri valori, l'indipendenza e la qualità dei nostri servizi, senza dimenticare la credibilità che vantiamo presso le aziende, una forza che abbiamo costruito con il lavoro di una vita», ha commentato Roberto Vicenzi, Vice Presidente di Centro Computer. Tra i prossimi obiettivi di Centro Computer, vi è quello di tagliare il traguardo dei 50 milioni di euro entro l'anno fiscale 2020, operando in modo da mantenere elevato il livello di soddisfazione

dei clienti e cercando di raddoppiare anche il margine operativo lordo.

Inoltre, per rispondere con tempestività alle esigenze di mercato ed essere in grado di proporre progetti tecnologicamente avanzati e servizi sempre più performanti, Centro Computer ha attivato un piano di assunzioni per potenziare l'organico, che prevede l'inserimento di almeno 10 nuove risorse specializzate, a supporto delle attività delle proprie divisioni.

È in questo scenario di crescita che si cala Vision 2020, la nuova strategia approntata da Centro Computer che conferma quanto il system integrator sia già entrato in modo pervasivo nella nuova era IT, operando quotidianamente con l'implementazione di progetti legati alla trasformazione

digitale, al mondo multi-cloud, alla mobility, all'IoT e allo Smart Working.

È anche una conferma, ha evidenziato l'azienda, di quanto stia radicalmente cambiando il modello di business delle imprese, che a prescindere dai settori verticali o specialistici, implementano le nuove soluzioni ICT che permettono di ottenere immediati benefici.

I servizi in modalità cloud, ad esempio, soprattutto su piattaforma Microsoft, sono in contrapposizione alla leggera riduzione del numero dei server venduti, anche se cresce sensibilmente il valore medio e il numero delle applicazioni che vengono installate su ogni macchina. ✨



Plantronics: la direzione è lo smarter working

S *smarter working è un termine che viene declinato con molteplici accezioni. Qual è l'interpretazione di Plantronics a riguardo?*

In Plantronics pensiamo allo smarter working come a un modo di esistere, di associarsi, con una connotazione legata al tema dell'uguaglianza che fa parte della nostra cultura aziendale. Smarter working non significa mandare le persone a lavorare da casa ma è più una filosofia articolata su tre capisaldi.

Il primo riguarda la relazione con le persone e, nel mio ruolo di responsabile globale delle risorse umane, passo moltissimo tempo a pensare al modo con cui le persone svolgono la loro attività e agli accor-

InaMarie Johnson, senior vice president & chief human resources di Plantronics delinea la visione dell'azienda produttrice di auricolari per applicazioni professionali e spiega perché un lavoro smarter è un lavoro più conveniente per tutti



di contrattuali, in modo da permettere ai nostri dipendenti di avere una carriera ricca e di impatto all'inter-

no di Plantronics. Il secondo è il posto in cui le persone lavorano, in base all'idea che il lavoro è legato a ciò che si fa e non al posto in cui si va. Lo smarter working offre la

possibilità di lavorare nel posto che ciascuno ritiene più idoneo, dove riesce a essere più produttivo e lavorare meglio. I nostri spazi aziendali sono progettati per incoraggiare la collaborazione, la concentrazione, la comunicazione.

Il terzo caposaldo è la tecnologia che mette a disposizione un'ampia gamma di strumenti e noi utilizziamo tutti quelli disponibili per consentire ai nostri dipendenti di operare al meglio: dai social media alla unified communication.

Quali sono i benefici dello smarter working per i dipendenti e per l'azienda ?

Sposare lo smarter working significa dare rispetto ai dipendenti, fornendo loro la libertà e l'autonomia di lavorare nei modi e luoghi preferiti e di scegliere gli strumenti di produttività. Più si trattano le persone con rispetto e più si alimenta la loro dedizione all'azienda e mettere i dipendenti nelle condizioni di lavorare meglio significa migliorare la loro produttività.

L'azienda deve investire su un modello nuovo per fare le cose in modo differente, creando ambienti confortevoli e attrezzati, cambiando il modo di operare, i modelli di leadership e i sistemi di misura delle prestazioni.

Questo significa anche coinvolgerli nelle scelte, per esempio, dell'ambiente di lavoro?

Esattamente. Nella realizzazione delle nostre sedi utilizziamo strumenti quali survey per chiedere ai nostri dipendenti di manifestare le loro esigenze, al fine di predisporre un design in grado di rispettare questi desideri. Si tratta di un approccio



globale che interessa tutti i nostri uffici e che porta a una personalizzazione di ogni sede in base al motto "Think globally and act locally". Il nuovo Headquarter italiano di Vimercate, alle porte di Milano, è espressione di una precisa volontà di Plantronics di realizzare un ufficio che non sembra tale, con peculiarità che ne rendono evidente il suo carattere italiano: i colori, le trasparenze, i temi e gli arredi hanno elementi caratteristici molto diversi, per esempio, da quelli della nostra sede generale.

In che modo la vostra offerta tecnologica è conforme ai dettami dello smarter working?

Poiché il lavoro va misurato in base ai risultati e si deve

poter operare da qualsiasi posto, servono strumenti e tecnologie idonee. Gli auricolari professionali realizzati da Plantronics prendono in considerazione queste esigenze. Per esempio, dispongono di tecnologie di riduzione del rumore di fondo che permettono di avere un audio perfetto anche quando ci si trova all'interno di un ambiente rumoroso come un aeroporto. Non ci focalizziamo unicamente sui dispositivi ma anche sulle soluzioni software. Abbiamo, per esempio, sviluppato un software specifico per i contact center che ottimizza l'esperienza della conversazione telefonica. Altri aspetti riguardano l'ambiente circostante: per esempio nel nostro Headquarter europeo abbiamo



implementato tecnologie acustiche per migliorare l'intelligibilità di ciò che le persone dicono.

Quale figura professionale deve essere responsabile dello smarter working all'interno dell'azienda?

Lo smarter working deve essere sponsorizzato dall'alto. Sia che si tratti dell'amministratore unico, del proprietario di una piccola azienda o di un manager "C-Level", è questo tipo di figura che deve scegliere di investire in questa direzione. La figura che, invece, dovrebbe averne la responsabilità e gestirlo probabilmente è quella dedicata alla gestione delle risorse umane in collaborazione con il CIO,

così da mettere insieme il responsabile delle persone con quello delle tecnologie. Inoltre, un'altra figura chiave che deve essere coinvolta è il facility manager o chiunque sia responsabile del luogo in cui le persone si trovano.

È possibile un'implementazione per fasi successive?

Si può iniziare con un approccio per fasi, partendo da piccoli cambiamenti dell'ambiente di lavoro per poi espanderli in numero e portata. Si può decidere di partire in molti modi differenti, ma il presupposto di partenza deve essere la fiducia. Si tratta, innanzitutto, di decidere di fidarsi che le persone che lavorano con

te e per te faranno la cosa giusta avendo la possibilità di scegliere. Si deve investire il paradigma che spesso caratterizza le aziende che è quello del controllo. A tal fine può essere utile, nelle nuove assunzioni, cominciare a esplorare questi aspetti e selezionare persone che manifestino una corretta predisposizione mentale rispetto a queste nuove modalità.

Esiste una differente attitudine generazionale allo smarter working?

I cosiddetti Millennials spingono in modo entusiasta queste tendenze, pensano in mobilità e, solitamente, adorano essere coinvolti in decisioni che riguardano, per esempio, l'eco sostenibilità. Altri lavoratori possono avere esigenze diverse: per esempio desiderare di avere postazioni meno mobili e più personalizzate. In questo non c'è niente di sbagliato. Il punto fondamentale è che non si deve obbligare tutti a operare nello stesso modo, ma ci deve essere spazio per accogliere ogni differente stile. È questo, in fondo, che rende il lavoro smart. ✱

DOVE TROVI L'INNOVAZIONE PER LA TUA AZIENDA



A partire dalle specifiche esigenze di innovazione, Smau accompagna le imprese nel **percorso verso la scelta dei giusti partner per il loro business**. Per ciascuna tappa del suo Roadshow Smau propone un programma di momenti formativi gratuiti, presentazioni e incontri dove i protagonisti dell'innovazione del nostro Paese possono stringere la mano ai decisori aziendali delle principali aziende italiane.

IL ROADSHOW 2017

PADOVA, 30-31 MARZO

BOLOGNA, 8-9 GIUGNO

BERLINO, 14-15-16 GIUGNO *internazionale*

MILANO, 24-25-26 OTTOBRE *internazionale*

NAPOLI, 14-15 DICEMBRE

SMAU IN PILLOLE (dati 2016)



RAD guida la migrazione da TDM a IP

Il vendor ha rilasciato una soluzione che permette di erogare servizi TDM su reti IP, aprire al strada a nuovi servizi a valore aggiunto e ottimizzare Capex e Opex

Le reti dati geografiche, sia che si tratti di reti aziendali sia di reti di carrier o di service provider, stanno subendo una profonda trasformazione al cui centro ci sono due paradigmi, l'IP e la virtualizzazione. La oramai universale diffusione dell'IP per quanto concerne le reti aziendali o le reti locali di sedi grandi o piccole sta portando gli operatori a migrare dalle esistenti reti SDH a infrastrutture IP.

Il punto chiave di questa migrazione è che permette di realizzare infrastrutture trasmissive basate sui medesimi protocolli usati dall'utente in casa propria, a basso costo, più piatte nonché più facili

e meno costose da esercire. Quello che deve però essere assicurato è il mantenimento in attività dei servizi in essere, a cui aggiungere nuovi servizi a valore aggiunto nell'ottica delle FNV, ovvero della virtualizzazione delle funzioni di rete.

Soluzioni che permettono di muoversi in questa direzione salvaguardando gli investimenti è quanto sta facendo RAD, società israeliana rappresentata in Italia da CIE Telematica, società di ingegneria specializzata nelle reti di accesso. RAD ha in proposito sviluppato e annunciato una soluzione il cui scopo primario è proprio quello di fornire un percorso

di migrazione da SDH a IP sia ai carrier sia alle aziende che da questi comprano i servizi e la connettività.

In effetti, è una soluzione che si compone di diversi prodotti e che nel suo complesso permette di :

- Mantenere attivi servizi TDM su una nuova rete a commutazione di pacchetto.
 - Permettere ai provider di aggiungere le linee affittate al proprio portfolio di servizi.
 - Supportare un ambiente "first mile" di tipo eterogeneo con CPE che supportino connessioni DSL/SFM, Ethernet e GPON.
 - Abilitare il trasporto con un'unica rete sia di servizi IP/Ethernet che TDM in modo da semplificare le operation e ridurre il TCO.
- Come accennato, la soluzione si compone di diversi dispositivi. L'ETX-2 è un apparato di demarcazione IP e Carrier Ethernet, l'ETX-5 è una piattaforma per l'aggregazione di servizi Ethernet, l'IPmux è un gateway per l'accesso pseudowire TDM. Completa la soluzione di migrazione RAD il software RADview, un sistema di gestione per il management e la orchestrazione dei servizi e dei dispositivi di rete. ❁

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



Restituisci la vista ai bambini ciechi del Sud del mondo.

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

97 299 520 151

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

cbmitalia.org

cbm
insieme per fare di più

ABBONATI TI REGALIAMO LA SICUREZZA E IL CLOUD



DIRECTION

la rivista per i professionisti dell'ICT



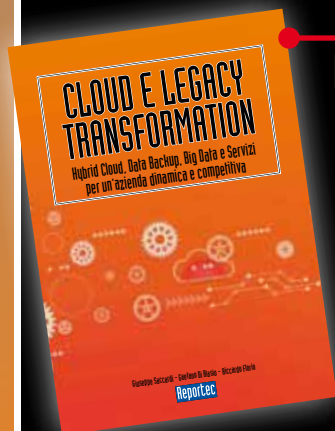
PARTNERS

la rivista per il Canale ICT a valore

**ABBONATI SUBITO A DIRECTION O PARTNERS
A SOLI 61 EURO**

**RICEVERAI I 10 NUMERI DEL 2017 E,
IN OMAGGIO,
2 LIBRI**

**DEDICATI ALLA SICUREZZA IT
E AL CLOUD,
DEL VALORE DI 100 EURO**



vai su

www.reportec.it/abbonamenti
e compila il modulo di abbonamento