

## IBM E RED HAT ACCELERANO LO SVILUPPO A TUTTO CLOUD

Un nuovo portfolio cloud native con oltre 100 nuovi software e 5 soluzioni Cloud Paks, all'insegna di Red Hat OpenShift, per abbattere tempi e costi.



Red Hat

a pag. 11

## L'INNOVAZIONE PER TUTTI CON LA SMARTER TECHNOLOGY DI LENOVO

Emanuele Baldi, Amministratore Delegato di Lenovo per l'Italia, spiega che la Smarter Technology rappresenta la nuova vision di Lenovo incentrata sul valore delle persone, che trovano nei nuovi dispositivi il supporto necessario per lavorare meglio, ma non solo: «Lenovo Smarter Technology for All significa dare attraverso i nostri prodotti massimo valore alle persone e aiutarle a migliorare la propria vita, sia privata sia professionale». L'AD Italiano rivela anche che la posizione di Lenovo si è ulteriormente consolidata.



a pag. 03

## Partecipa all'indagine nazionale sugli attacchi digitali intenzionali in Italia (OAD)

E' in pieno corso l'iniziativa OAD, Osservatorio Attacchi Digitali in Italia, giunta all'undicesimo anno consecutivo di indagine on line sugli attacchi intenzionali ai sistemi informatici di aziende ed enti, di qualsiasi dimensione.

a pag. 05



## SOMMARIO

L'IoT di Teltonika distribuito da Arrow Electronics in EMEA

pag.09

Il finto help desk, la truffa su Twitter

pag.09

Cambium Networks acquisisce le soluzioni Wi-Fi Xirrus da Riverbed Technology

pag.10

I dati e il cloud dei servizi di Intesa Sanpaolo al sicuro con Pure Storage

pag.10

Partners Flip  
anno VIII - numero 244 - quindicinale  
Direttore responsabile: Gaetano Di Blasio  
In redazione: Giuseppe Saccardi, Paola Saccardi, Edmondo Espa.  
Redazione: via Marco Aurelio, 8 - 20127 Milano  
Tel 0236580448 fax 0236580444 www.partnersflip.it  
Proprietà: Reportec srl, via Gian Galeazzo 2, 20136 Milano  
Iscrizione al tribunale di Milano n°514 del 13/10/ 2011  
Tutti i diritti sono riservati; Tutti i marchi sono registrati e di proprietà delle relative società.



# L'innovazione per tutti con la Smarter Technology di Lenovo

*Dispositivi consumer e "commercial" per aumentare il potenziale di ogni tipologia d'utente e trasformare il modo di lavorare. Dalla realtà aumentata all'artificial Intelligence, dall'IoT allo svago*

di Gaetano Di Blasio

**Emanuele Baldi**, Amministratore Delegato di Lenovo per l'Italia, spiega che la Smarter Technology rappresenta la nuova vision di Lenovo incentrata sul valore delle persone, che trovano nei nuovi dispositivi il supporto necessario per lavorare meglio, ma non solo: «Lenovo Smarter Technology for All significa dare attraverso i nostri prodotti massimo valore alle persone e aiutarle a migliorare la propria vita, sia privata sia professionale».

L'AD Italiano rivela anche che la posizione di Lenovo si è ulteriormente consolidata. Più precisamente, Baldi afferma: «Oggi un pc su quattro venduti è Lenovo; è una grande soddisfazione e al contempo una grande responsabilità, che ci spinge a innovare in tutti i campi della tecnologia, dalla Realtà

Virtuale e Aumentata, con significative applicazioni anche in campo scientifico, professionale e industriale, all'Intelligenza Artificiale, con importanti applicazioni nella Smart Home e nello Smart Working, fino all'IoT, con innovative ricadute nella logistica e nell'organizzazione aziendale».

Negli ottimi risultati evidenziati, Baldi specifica che non è conteggiata la fusione di Fujitsu.

Molte le novità, ma ci soffermiamo solo sull'ambito professionale e sulle soluzioni più innovative, senza considerare la divisione Data Center di Lenovo.

Tocca a **Federico Carozzi**, Head Product Marketing di Lenovo illustrare alcuni dei dispositivi e delle soluzioni più recenti, non prima di aver lanciato un video dedicato al prossimo pc "pieghevole".



Emanuele Baldi - Amministratore Delegato di Lenovo



Federico Carozzi - Head Product Marketing di Lenovo



smette di guardare lo schermo del laptop, i sensori AI dello Yoga S940 se ne accorgono e bloccano il display per proteggere i dati da sguardi indiscreti. Possono pure rilevare e segnalare uno sguardo indiscreto alle spalle dell'utente.

Lenovo Yoga S940

### Un ThinkBook ultra sottile

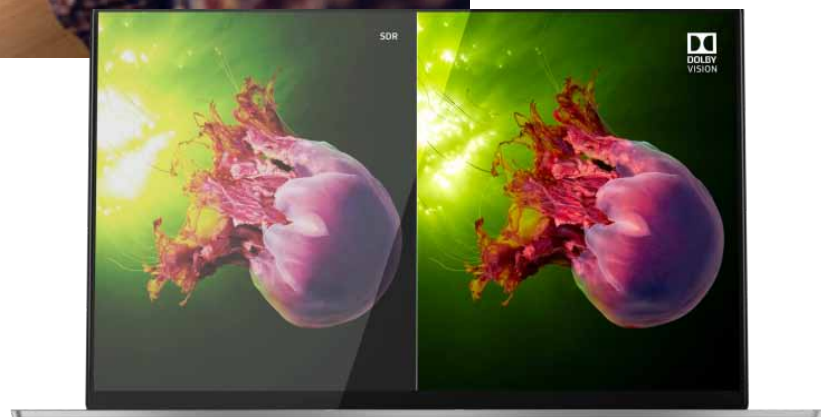
In attesa del foldable il nuovo ThinkBook da 13 pollici ultra sottile stupisce per il design in un pc pensato per il mondo professional, che richiede un sistema costantemente connesso, leggero, che possa soddisfare le generazioni Millennial e Gen Z, affinché possano esprimere la loro capacità nell'aumentare la produttività.

Questo in base a ricerche che, spiegano presso Lenovo, evidenziano il nuovo marchio ThinkBook quale dispositivo "specificamente progettato per le piccole e medie imprese che normalmente acquistano laptop consumer in virtù dei vantaggi per-

cepiti di prezzo e di design, ma sono costretti a rinunciare a servizi e garanzie estese di tipo professionale". Carozzi, in particolare, mostra lo stile moderno e gli elementi di design tipici dei dispositivi consumer, ad esempio gli chassis in alluminio, abbinati alle funzioni di sicurezza che si trovano nei pc della famiglia Think.

### Uno Yoga più intelligente a prova di spioni

Altra novità riguarda il laptop Yoga S940 ultra sottile con Windows 10, che fornisce sicurezza e privacy senza compromettere la produttività e



la praticità d'uso, come evidenziano in Lenovo. Più precisamente, la nuova gamma si distingue per l'artificial intelligence abbinata a tecnologie audio e video avanzate, grazie a una suite di funzioni Lenovo Smart-Assistant, che, per esempio, consentono di eliminare automaticamente il rumore di fondo e sfocare le immagini in secondo piano nel corso delle videochiamate. Inoltre, se l'utente

Altra funzione, pensata per una maggiore produttività, permette di spostare contenuto delle finestre aperte ma non in uso su un monitor esterno connesso al computer in automatico. Carozzi segnala inoltre: «Yoga S940 è il primo laptop al mondo a presentare un vetro curvo Contour Glass che si avvolge attorno alla cornice del display, riducendone ancora di più lo spessore».

# Partecipa all'indagine nazionale sugli attacchi digitali intenzionali in Italia (OAD)



È in pieno corso l'iniziativa OAD, Osservatorio Attacchi Digitali in Italia, giunta all'undicesimo anno consecutivo di indagine online sugli attacchi intenzionali ai sistemi informatici di aziende ed enti, di qualsiasi dimensione (come numero di dipendenti) ed operanti in Italia: dalle aziende manifatturiere a quelle di servizi, dagli studi professionali agli esercizi commerciali ed alberghieri, dalle scuole e università alle ASL e agli ospedali, dai Comuni alle Province, dalle Regioni ai Ministeri.

## L'iniziativa OAD

OAD è una iniziativa di MALABO Srl ([www.malabo-advisoring.it](http://www.malabo-advisoring.it)), la società di consulenza direzionale sull'ICT dell'autore Marco R. A. Bozzetti che realizza l'indagine online, elabora i dati raccolti e stende il rapporto finale, in collaborazione con AIPSI, Associazione Italiana Professionisti

Sicurezza Digitale, capitolo italiano di ISSA ([www.aipsi.org](http://www.aipsi.org), [www.issa.org](http://www.issa.org)), con l'editore Reportec Srl ([www.reportec.it](http://www.reportec.it)), e con la Polizia Postale e delle Telecomunicazioni (<http://www.commissariatodips.it/>), che fornisce dati essenziali sugli attacchi alle infrastrutture critiche e a quelle finanziarie, incluso il numero di denunce e di arresti.

L'OAD, Osservatorio Attacchi Digitali in Italia, è l'unica iniziativa in Italia per l'analisi sugli attacchi intenzionali ai sistemi informativi delle Aziende e degli Enti Pubblici italiani, **realizzata tramite una indagine anonima indirizzata a tutte le aziende e alle Pubbliche Amministrazioni** di ogni settore merceologico e dimensio-

**Il Questionario 2019 OAD è online e accessibile alla seguente pagina web:**

<https://www.oadweb.it/limesurvey/index.php/799974?lang=it>



Fig.1

ne, **tramite un questionario compilabile online con un browser**. Il questionario è rivolto principalmente ai Responsabili dei Sistemi Informativi e della Sicurezza Informatica. Sulla base delle risposte

anonime al questionario, opportunamente elaborate e sintetizzate, viene preparato un Rapporto finale gratuitamente scaricabile dal sito web <https://www.oadweb.it/>, che costituisce l'archivio storico di

tutti i rapporti pubblicati, e di tutte le presentazioni ed articoli che su di essi sono stati realizzati.

La fig. 1 mostra le copertine degli otto rapporti finora pubblicati (non sono dieci perché alcuni rapporti includono due anni consecutivi).

Obiettivo principale di OAD è fornire reali e concrete indicazioni sugli attacchi ai sistemi informatici che possano essere di riferi-

mento nazionale, autorevole e indipendente, per la sicurezza ICT in Italia e per l'analisi dei rischi ICT, necessaria anche per essere conformi alle normative sulla privacy

Le/i potenziali rispondenti sono i decisori ed il personale tecnico che hanno a che fare con il Sistema Informatico dell'azienda/ente nella quale operano o cui fanno riferimento (ad esempio quali "terze parti"

gestori dell'intero sistema e/o della sua sicurezza digitale): per le aziende di medie e grandi dimensioni tipicamente il CIO, Chief Information Officer, o il CISO, Chief Information Security Officer, o loro collaboratori interni od esterni dalla loro struttura. Per le piccole e piccolissime imprese e strutture, risponde normalmente il responsabile dell'azienda o dello studio, in quanto è lui che decide

sul sistema informatico, o la terza parte che lo gestisce. Tutte queste persone sono (o dovrebbero essere) informate tramite i social network, le associazioni cui appartengo (che sono spesso patrocinatori dell'iniziativa OAD), gli articoli, come questo, che promuovono l'indagine, ed anche direttamente contattati via e-mail e/o chiamate telefoniche, soprattutto per i responsabili delle aziende

Che cosa è attaccato	Come (tecniche attacco)						
	Attacco fisico	Raccolta informazioni (es. social engineering, phishing, pharming, hoax, scanning, indagini su Internet, ecc.)	Script e programmi maligni (ransomware, spyware, adware, ..)	Agenti autonomi: programmi maligni che si replicano e diffondono autonomamente, come virus e worm	Toolkit: programmi in grado di scoprire e sfruttare vulnerabilità (rootkit, metaexploit, ..)	Strumenti distribuiti controllati centralmente (Command Control) quali bootnet	utilizzo di due o più delle precedenti tecniche (APT, Advanced Persistent Threat)
S1d2 - Distruzione fisica di dispositivi ICT o di loro parti							
S1d3 - Furto di dispositivi ICT mobili							
S1d4 - Furto di dispositivi ICT fissi o di loro parti							
S1d5 - Furto informazioni da sistemi fissi (PC, server, storage system, ...)							
S1d6 - Furto informazioni da sistemi mobili (palmari, smartphone, tablet, etc.)							
S1d7 - Attacchi all'identificazione, autenticazione e autorizzazioni degli utenti finali e di quelli privilegiati (operatori-amministratori di sistemi)							
S1d8 - Attacchi alle reti locali e geografiche, fisse e wireless, alle loro unità, alle connessioni e ai DNS							
S1d9 - Attacchi ed uso non autorizzato risorse IT							
S1d10 - Attacchi e modifiche non autorizzate ai programmi applicativi e alle loro configurazioni (non terziarizzate)							
S1d11 - Modifiche non autorizzate alle informazioni trattate dai sistemi ICT							
S1d12 - Saturazione risorse digitali (DoS, DDoS)							
S1d13 - Attacchi ai propri sistemi in cloud o in housing/hosting presso Fornitori							
S1d14 - Attacchi a dispositivi IoT (Internet of Things) in uso							
S1d15 - Attacchi ai propri sistemi di OT, Operational Technology, che includono sistemi di automazione (DCS, PLC, ..) e di robotica							
S1d16 - Attacchi a sistemi e/o servizi basati su blockchain							

Fig.2

ed enti di maggiori dimensioni.

Il passa parola è sempre lo strumento più efficace per promuovere l'indagine OAD, che in taluni casi "spaventa" la/il potenziale rispondente sia per certe domande un poco tecniche, sia, soprattutto, perché non si fida (ma questa volta a torto) del reale anonimato: e di conseguenza non ritiene opportuno far sapere che il suo sistema informatico, piccolo o grande che sia, è stato attaccato.

**Si invitano pertanto tutti i lettori di questo articolo da un lato di compilare il questionario, dall'altro di invitare i loro interlocutori di altre aziende/enti a compilarlo e a loro volta "passare parola".**

OAD garantisce totalmente l'anonimato della/del rispondente, e data la relativa generalità delle domande, non è possibile, in alcun modo, risalire all'azienda/ente cui si fa riferimento.

## Il questionario 2019 OAD

Dal 2018 l'indagine OAD individua 15 tipologie di attacchi digitali basate su che cosa viene attaccato, separandole il più chiaramente possibile dalle tecniche usate

per portare l'attacco, come schematizzato nella **fig.2**.

Il questionario 2019 di OAD si articola in 7 Sezioni, come mostrato in **fig. 3**:

- Le prime due sono relative agli attacchi rilevati per le 14 tipologie considerate, e con alcune delle loro più significative caratteristiche: frequenza nell'anno, tecniche di attacco usate, impatti subiti, tempi di ripristino nei casi più gravi. Qualora non fossero stati rilevati attacchi, o alcune tipologie di attacco, tutte le domande relative vengono saltate automaticamente dall'applicazione web: nel primo caso sono saltate tutte le domande sugli attacchi, ossia sia S1 che S2, nel se-

condo caso sono saltate le domande sulle caratteristiche del tipo di attacco, e si passa automaticamente al tipo di attacco successivo. Questi automatismi facilitano e velocizzano fortemente i tempi per completare l'intero questionario;

- La Sezione 3 rileva i futuri tipi d'attacco digitale più temuti, e con quali tecniche;
- Le sezioni 4 e 5 pongono domande sulle misure di sicurezza organizzative e tecniche in essere, o a piano in breve termine
- La Sezione 6 pone domande non di dettaglio per garantire l'anonimità sulle principali caratteristiche dell'Azienda/Ente (settore merceolo-

gico, dimensioni, area di copertura, etc.) e della/del rispondente (suo ruolo nella struttura)

- La sezione 7 rileva, sempre in termini generali, le caratteristiche del Sistema Informatico considerato: dalle sue dimensioni (es. numero di server, numero di dispositivi d'utente fissi e mobili) ai sistemi operativi usati, dal tipo di architettura ICT complessiva all'outsourcing.

Il tempo richiesto per la compilazione del questionario dipende dal numero di diversi attacchi subiti, e dalle dimensioni e complessità del Sistema Informatico dell'azienda/ente della/del rispondente: tipicamente varia tra i **15 ed i 30 minuti complessivi**.

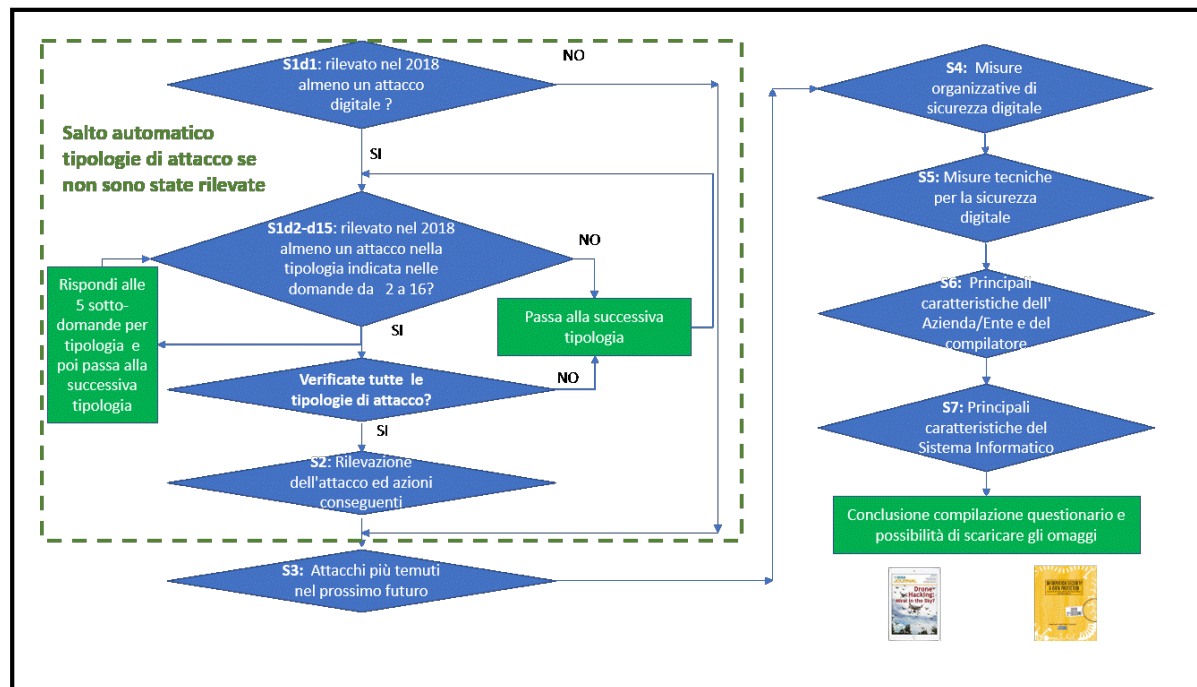


Fig.3

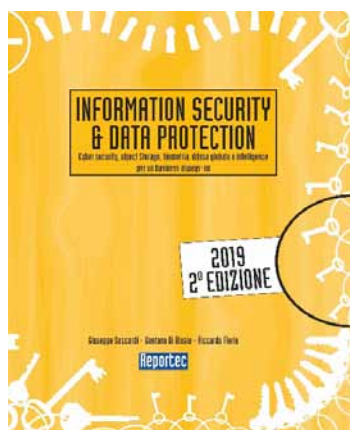
## Un significativo omaggio a chi completa il Questionario 2019

La motivazione principale alla **corretta e veritiera compilazione** del questionario è il contribuire all'indagine che, unica in Italia, fornisce una **fotografia realistica del fenomeno degli attacchi digitali in Italia**, soprattutto per le piccole e piccolissime organizzazioni che costituiscono l'ossatura dell'economia italiana.

Per ulteriormente spronare la/il potenziale rispondente a completare il questionario, OAD offre come piccolo **ringraziamento per il contributo** fornito ed i minuti spesi:

- Il numero di luglio 2019 della rivista mensile ISSA Journal, focalizzata sugli attacchi e sulle protezioni per i sistemi IoT, inclusi i droni dell'articolo di copertina;
- La recentissima ultima edizione del volume di 184 pagine, edito da

Reportec, sulla sicurezza delle informazioni e la protezione dei dati.



### Il piano di lavoro per OAD 2019

Come evidenziato nel Gantt per OAD 2019 in **fig.**

**4**, si stima la pubblicazione del rapporto finale verso la fine di ottobre-primi di novembre 2019. Il Rapporto 2019 avrà una struttura simile a quella del 2018 (Il Rapporto 2018 OAD è scaricabile gratuitamente da <https://www.oadweb.it/it/rapporti-e-relativi-convegni/2018.html> dopo aver effettuate il log in come utente registrato. Per registrarsi, gratuitamente, cliccare sulla seguente pagina ed inserire i pochi dati richiesti).

**Il Questionario 2019 rimarrà on line fino alla fine di settembre 2019,**

per poter elaborare nei tempi previsti i dati raccolti e stendere il rapporto finale.

Non rimane quindi molto tempo per la compilazione e per il passa parola!!

### Sponsor e Patrocinatori

OAD è una iniziativa senza scopi di lucro, e le sponsorizzazioni servono solo a coprire una parte dei costi complessivi dell'intera iniziativa. E' ancora

possibile l'adesione di nuovi Sponsorizzatori e di nuovi Enti patrocinatori: i primi per coprire, almeno parzialmente, i costi dell'intera iniziativa OAD 2019, i secondi per allargare quanto più possibile sia ora il bacino di rispondenti, sia poi i lettori del rapporto finale.

Le Aziende e gli Enti che fossero interessati a considerare una sponsorizzazione di OAD 2019 possono direttamente contattare l'ideatore/realizzatore dell'indagine, inviando una e-mail a [m.bozzetti@aipsi.org](mailto:m.bozzetti@aipsi.org).

La proposta di sponsorizzazione è scaricabile dall'allegato in fondo alla pagina web: <https://www.oadweb.it/it/oad2019/oad-2019.html>.

Analogamente, le Associazioni, anche di categoria, che fossero interessate a patrocinare OAD 2019 sono pregate di inviare quanto prima una e-mail di richiesta a [m.bozzetti@aipsi.org](mailto:m.bozzetti@aipsi.org).

ATTIVITA'	apr-19	mag-19	giu-19	lug-19	ago-19	set-19	ott-19	nov-19	dic-19	1° trim. 2020
Lancio ed inizio OAD 2019										
Acquisizione Sponsor e Patrocinatori										
Creazione Questionario OAD 2019 via web										
Ampliamento e aggiornamento mailing list potenziali rispondenti										
Invio invito a compilare il Questionario 2019 OAD via web										
Raccolta risposte al Questionario 2019 OAD via web e loro elaborazione										
Stesura Rapporto 2019 OAD										
Pubblicazione Rapporto 2019 OAD e comunicato stampa, creazione pagina web per il download del Rapporto 2019 OAD										
raccolta dei nominativi di chi lo scarica										
Convegni e workshop per la presentazione generale o settoriale dei risultati raccolti										
Primo elenco di chi ha scaricato il Rapporto 2019 OAD										
Ulteriori elenchi di chi ha scaricato il Rapporto 2019 OAD										
Eventuali iniziative ad hoc per Sponsor Gold e Platinum										

# L'IoT di Teltonika distribuito da Arrow Electronics in EMEA

Il distributore di tecnologia Arrow Electronics ha siglato un nuovo accordo di distribuzione con Teltonika, fornitore di soluzioni IoT con sede in Lituania, con esperienza ventennale nella fornitura delle regioni di Europa, Middle Est e Africa (EMEA). I prodotti di Teltonika rispondono alle sfide delle comunicazioni industriali, indirizzano il tracking di asset e personale e le comunicazioni machine-to-machine in ambito mobile.

«Siamo entusiasti di lavorare con Arrow, leader nel portare la tecnologia sul mercato - ha commentato **Antanas Segzda**, CEO di Teltonika - e sono certo che

questa collaborazione ispirerà molte soluzioni IoT nel prossimo futuro. Questo aiuterà entrambe le aziende, non solo a rafforzare la reciproca leadership di mercato, ma, ancora più importante, permetterà un cambiamento nell'approccio di mercato alla tecnologia e accelererà l'adozione globale dell'IoT»

Teltonika offre una gamma di soluzioni collegate all'IoT e dispone di oltre 100 prodotti, avendo venduto ad oggi più di 8,6 milioni di dispositivi in tutto il mondo. Il portfolio dell'azienda copre il tracking del dispositivo gestendo sia l'hardware sia il software su reti 2G, 3G, LTE, Bluetooth, GNSS,

GPRS, NB-IoT e ogni altra tipologia di connettività. I prodotti assicurano una serie di funzionalità, tra cui la modalità 'geofencing', gli aggiornamenti del firmware via connessioni wireless, il rilevamento dell'accensione, l'immobilizzatore, le chiamate vocali. Il vendor offre anche soluzioni di networking, includendo router, gateway, modem e antenne per la rete aziendale, così come strumenti per l'utilizzo industriale M2M/IoT. Inoltre, sono disponibili tracker portatili per il monitoraggio del carico di rete e di altri dispositivi mobili.

«Teltonika offre ai clienti un facile accesso al mondo dell'IoT - ha dichiarato

**Paul Karrer**, Direttore del Business IoT di Arrow ECS in EMEA - . Parliamo di un provider ben consolidato ed attrezzato che sta fornendo imprese e organizzazioni di tutto il mondo, con una moltitudine di prodotti che assicurano comunicazioni intelligenti e connettività in molte aree industriali. Teltonika offre una grande varietà di soluzioni, unitamente ai prodotti di networking specifici per il mondo IoT, che consentono ai nostri clienti del canale di poter scegliere tra un'ampia gamma di offerta per soddisfare le esigenze su ogni singolo dispositivo IoT o applicazione dei propri end user».

## IL FINTO HELP DESK, LA TRUFFA SU TWITTER

Il vendor di sicurezza Trend Micro ha rilasciato un **nuovo studio** che rivela come i cybercriminali sfruttino Twitter per compiere truffe, eseguire operazioni command-and-control (C&C) ed esfiltrare dati. I social network ormai rappresentano un'immensa fonte di dati e per questo sono diventati bersaglio della criminalità informatica, sempre alla ricerca di informazioni da poter sfruttare in maniera illegittima.

Una truffa ricorrente che è stata rilevata consiste nell'utilizzare finti account Twitter che falsificano quelli legittimi dei vendor per architettare truffe attraverso il supporto tecnico. Sono sempre più numerose le aziende che utilizzano i canali social per sviluppare le relazioni e il supporto alla clientela e i

criminali ne sono consapevoli. Gli utenti chiamano il numero telefonico fornito da questi account falsi pensando di parlare con l'help desk dell'azienda, ma in realtà attraverso la chiamata i cyber criminali richiedono e si impossessano di dati sensibili, come per esempio quelli della carta di credito, oppure riescono a installare contenuti maligni sui pc.

Trend Micro raccomanda agli utenti di assicurarsi della validità degli account Twitter che consultano, controllando direttamente i siti delle aziende. È anche importante, lato team di security, accertarsi di analizzare dati di twitter validi nel corso delle investigazioni.



# Cambium Networks acquisisce le soluzioni Wi-Fi Xirrus da Riverbed Technology

Cambium Networks, società di soluzioni di rete wireless con sede a Chicago, ha annunciato l'acquisizione dei prodotti e servizi cloud Xirrus Wi-Fi da Riverbed Technology. Cambium Networks fa sapere che il portafoglio Xirrus di access point Wi-Fi enterprise ad alte prestazioni e i servizi in abbonamento, tra cui XMS Cloud Management, EasyPass Access, Application Control, Xirrus Positioning System (XPS) e MSP Com-

mand Center, migliora e facilita l'implementazione e le funzionalità dei Network Service Application (NSA) esistenti della società americana, mettendo a disposizione dei clienti un ampio set di nuovi servizi.

In pratica, le soluzioni Xirrus ampliano e rafforzano l'attuale offerta Wi-Fi di Cambium Networks, per offrire ai clienti dell'area enterprise, istruzione, enti governativi, hospitality e ai managed service provider

(MSP), una più ampia scelta di tecnologie e soluzioni per la connettività wireless. Le soluzioni Xirrus saranno ancora acquistabili presso i rivenditori Xirrus esistenti e saranno rese disponibili tramite i ConnectedPartner esistenti di Cambium Networks nelle prossime settimane.

**Atul Bhatnagar**, Presidente e CEO di Cambium Networks ha affermato: «Siamo orgogliosi di poterci unire al talentuoso team di Xirrus, che porta

con sé una storia di innovazione e una profonda esperienza nello sviluppo di soluzioni Wi-Fi ad alte prestazioni, servizi cloud scalabili, implementazioni ad alta densità, analisi di rete avanzate e servizi in abbonamento cloud. Siamo inoltre felici di dare il benvenuto ai clienti di Xirrus in tutto il mondo e ai partner di canale nella comunità Cambium Networks e non vediamo l'ora di costruire insieme un proficuo rapporto».

# I dati e il cloud dei servizi di Intesa Sanpaolo al sicuro con Pure Storage

Pure Storage, società attiva nello sviluppo di soluzioni storage all-flash a supporto della digital transformation centrata sui dati, è stata scelta da Intesa Sanpaolo, per disporre di maggiore efficienza, resilienza e velocità nel sistema informatico.

Un fattore chiave nella scelta della soluzione e del partner tecnologico era la necessità di avere un time-to-market veloce per

portare i nuovi prodotti sul mercato.

Nel corso della realizzazione sono stati migrati sulla piattaforma Pure Storage dati, applicazioni e funzionalità mission-critical, come parte del CRM e dei sistemi che abilitano funzioni di pagamento per i clienti della banca. Un altro aspetto saliente sono state le funzionalità di Intelligenza Artificiale e analisi predittiva della soluzione

adottata.

Il punto chiave, evidenzia Pure Storage, è stata la semplicità della tecnologia che ha consentito di migliorare l'automazione dei processi di provisioning legati all'infrastruttura storage, con un impatto diretto sul time-to-market infrastrutturale. Il tutto, ha permesso anche di comprimere i tempi di esecuzione delle analisi, abilitando performance superiori a costi minori.

«La soluzione ha un design eccellente, le performance elevatissime e la facilità di utilizzo non facilitano solo le attività del day-by-day, ma anche quelle relative all'analisi preliminare dei requisiti applicativi in quanto l'ambiente è già progettato per rispondere alle richieste di tutte le applicazioni» ha osservato **Nicola Carotti**, Responsabile ufficio servizi cloud e collaboration della banca.

# IBM e Red Hat accelerano lo sviluppo a tutto cloud

*Un nuovo portfolio cloud native con oltre 100 nuovi software e 5 soluzioni Cloud Paks, all'insegna di Red Hat OpenShift, per abbattere tempi e costi*

di Gaetano Di Blasio

IBM accelera nello sviluppo di prodotti e soluzioni che beneficiano dello stretto rapporto con Red Hat.

In particolare, grazie all'integrazione sempre più profonda sul fronte Red Hat OpenShift, sono stati annunciati numerosi software e gli "IBM Cloud Paks", che, a detta degli esperti di IBM, portano, tra gli altri, benefici quali fino all'84% delle spese operative e una riduzione dei tempi di sviluppo che si abbatte del 75%.

Inoltre, vengono annunciati Red Hat OpenShift su IBM Cloud, Red Hat OpenShift su IBM Z e LinuxONE. A questo si aggiungono consulenza e servizi tecnologici per Red Hat.

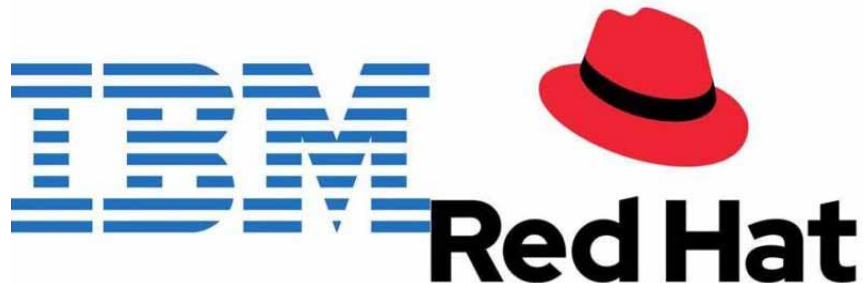
Il vantaggio principale, però, consiste nella possibilità, per le aziende, di sviluppare un'applicazione critica di business una sola volta, potendo poi eseguirla pressoché su qualsiasi cloud anche

pubblico, incluse Amazon Web Services, Microsoft Azure, Google Cloud Platform, Alibaba e IBM Cloud.

Qui entrano in gioco i cloudPak, che abilitano le nuove funzionalità. Al momento sono 5 e comprendono, di cui una è Cloud Pak for Data, progettata per gli insight, che accelera grazie a un'architettura di virtualizzazione dei dati per l'AI con una velocità aumentata del 500% in prove di laboratorio.

Cloud Pak for Applications, invece serve per integrare app, dati, servizi cloud e API, il tutto abbattendo i tempi di sviluppo dell'84% secondo un'indagine realizzata da Ovum. e riducendo i costi di integrazione del 33% in base a una misurazione di Forrester Research.

Il quarto "pacchetto" è Cloud Pak for Automation,



che è stato pensato per diminuire i processi decisionali dell'80%, stando a ulteriori analisi di Forrester. Infine Cloud Pak for Multi-cloud Management è stato progettato per fornire visibilità, limitando governance e automazione per le spese operative di supporto e spese operative di supporto, come ricavato da Ovum.

## I prossimi passi di IBM e Red Hat

In funzione di questo annuncio, segnalano da IBM e Red Hat, vengono forniti modelli operativi e un insieme di servizi, tra cui la gestione delle identità, la sicurezza, il monitoraggio e la registrazione.

Un unico operativo IBM Red Hat fornisce elevata

una visibilità e capacità di controllo.

Come accennato, una conseguenza dell'annuncio IBM Red Hat è che IBM porterà Red Hat OpenShift sui sistemi IBM Z e LinuxONE che, insieme, alimentano più di 30 miliardi di transazioni applicative al giorno a livello globale. OpenShift è già sui Power Systems e Storage di IBM. Inoltre, va segnalato che i nuovi servizi IBM Red Hat saranno forniti da un team molto ampio di consulenti certificati Red Hat, che dispone di una grande community storica e da oltre 80.000 professionisti dei servizi applicativi cloud per aiutare i clienti a spostare, costruire e gestire i carichi di lavoro in ambienti cloud.



PER RESTARE SEMPRE AGGIORNATO  
SULLE NOVITA' DEL **CANALE ICT**

SEGUICI SUL SITO  
[WWW.REPORTEC.IT](http://WWW.REPORTEC.IT)

E SULLE NOSTRE PUBBLICAZIONI

**abbonati a PARTNERS!**

scrivi a [info@reportec.it](mailto:info@reportec.it)