

PARTNERS

INFORMAZIONE E FORMAZIONE PER IL CANALE ICT A VALORE

GEN-FEB N°42

**Logistica,
competenze
digitali e nuovi
modelli per
ottimizzare
i processi**



SCENARIO RETAIL

INCHIESTA SICUREZZA

IL RITARDO DELL'ITALIA
SULLA SICUREZZA
pag. 32-58

SPECIALE

DATA CENTER
pag. 59-62





Atahotel Expo Fiera

Via Giovanni Keplero 12

20016 Pero (Mi) –

13-14-15 marzo



Security Summit è la manifestazione dedicata alla sicurezza delle informazioni, delle reti e dei sistemi informatici che, da anni, appassiona i partecipanti con contenuti e approfondimenti sull'evoluzione tecnologica del mercato.

Giunto alla X edizione il Security Summit si è imposto, ed è riconosciuto dal mercato, come l'Evento di eccellenza nel panorama italiano grazie all'alta qualità dei relatori e alla numerosa partecipazione di pubblico sempre più qualificato.

Anche nel 2018 si confermano questi valori: una struttura articolata in sessioni plenarie, percorsi formativi, atelier tecnologici, tavole rotonde e seminari tecnici.

Certificata dalla folta schiera di relatori (più di 500 sono intervenuti nelle scorse edizioni) provenienti dal mondo della ricerca, dell'Università, delle Associazioni, della consulenza, delle Istituzioni e delle imprese, la manifestazione è stata frequentata da oltre 15.000 partecipanti, e sono stati rilasciati circa 10.000 attestati validi per l'attribuzione di oltre 16.000 crediti formativi (CPE).

La manifestazione vede impegnati in prima persona gli esperti del Clusit per la parte dei contenuti e Astrea sul fronte organizzativo per le quattro tappe annuali: quest'anno si parte dalla tre giorni di **Milano**, in programma presso l'Atahotel Expo Fiera il 13, 14 e 15 marzo con un'agenda articolata in sessioni plenarie, percorsi formativi, atelier tecnologici, tavole rotonde e seminari tecnici, a partire dalla presentazione del **Rapporto Clusit 2018 sulla sicurezza ICT in Italia e nel mondo**.

La partecipazione a Security Summit è gratuita, previa registrazione al sito securitysummit.it, dove sarà a breve disponibile il programma della tre giorni milanese.

Security Summit ha il patrocinio della Commissione Europea e di ENISA, l'Agenzia dell'Unione Europea per la sicurezza delle informazione e della rete.

Organizzato da



www.securitysummit.it

PARTNERS

Anno VII - numero 42

gennaio-febbraio 2018

Direttore responsabile: Gaetano Di Blasio

In redazione: Giuseppe Saccardi,
Paola Saccardi

Grafica: Aimone Bolliger

Hanno collaborato: Gian Carlo Lanzetti

Redazione, amministrazione, pubblicità:
REPORTEC srl

via Marco Aurelio, 8 - 20127 Milano

Tel 0236580441 - Fax 0236580444

www.partnersflip.it

partners@reportec.it

pubblicità: edmondo.espa@reportec.it

Diffusione: 35.000 copie

Iscrizione al tribunale di Milano n° 515 del 13 ottobre 2011.

Stampa: Media Print Srl, Via Brenta 7

37057 S.Giovanni Lupatoto (VR)

Immagini: Dreamstime.com

Proprietà: Reportec Srl, via Gian Galeazzo 2, 20136 Milano

Tutti i diritti sono riservati

Tutti i marchi sono registrati e di proprietà
delle relative società

TRA VIRGOLETTE

L'importanza delle partnership in un
mercato sempre più liquido 6

PANORAMI

Trend opposti nel percorso
verso la digitalizzazione 7

Le trasformazioni in atto
nelle aziende italiane 8

I nuovi ecosistemi digitali 11

Urgono competenze 4.0,
soft skill e soprattutto
consapevolezza 12

PRIMO PIANO

LOGISTICA E COMPETENZE DIGITALI
PER GUIDARE IL RETAIL 14

La customer experience al centro della strategia
dei retailer innovativi 18

Dalla centrale al negozio, l'operatività integrata
con Brother 20

Sap aiuta il retail con l'ERP di nuova generazione 23



Le diverse facce del
consumatore digitale 24

L'Unified Retail Planning
di Relx Solutions 28

Bricocenter rinnova la
gestione delle risorse
umane con Talentia 30

OAD: Osservatorio Attacchi Digitali in Italia

L'OAD, Osservatorio Attacchi Digitali, è l'unica iniziativa in Italia per l'analisi sugli attacchi intenzionali ai sistemi informatici delle aziende e degli enti pubblici in Italia, basata sui dati raccolti attraverso un questionario compilabile anonimamente on line.

Obiettivo principale di OAD è fornire reali e concrete indicazioni sugli attacchi ai sistemi informatici che possano essere di riferimento nazionale, autorevole e indipendente, per la sicurezza ICT in Italia e per l'analisi dei rischi ICT. La disponibilità di un'indagine sugli attacchi digitali indipendente, autorevole e sistematicamente aggiornata (su base annuale) costituisce una indispensabile base per contestualizzare l'analisi dei rischi digitali, richiesta ora da numerose certificazioni e normative, ultima delle quali il nuovo regolamento europeo sulla privacy, GDPR.

La pubblicazione dei rapporti OAD aiutano in maniera concreta all'azione di sensibilizzazione sulla sicurezza digitale del personale a tutti i livelli, dai decisori di vertice agli utenti.

OAD è la continuazione del precedente OAI, Osservatorio Attacchi Informatici in Italia, che ha iniziato le indagini sugli attacchi digitali dal 2008. In occasione del decennale OAD, in termini di anni considerati nelle indagini sono state introdotte numerose innovazioni per l'iniziativa, che includono:

- sito ad hoc come punto di riferimento per OAD e come repository, anno per anno, di tutta la documentazione pubblicata sull'iniziativa OAD-OAI: <https://www.oadweb.it>
- visibilità di OAD nei principali social network: pagina facebook @OADweb, in LinkedIn il Gruppo OAD <https://www.linkedin.com/groups/3862308>
- realizzazione di webinar gratuiti sugli attacchi agli applicativi: il primo, sugli attacchi agli applicativi, è in <https://aipsi.thinkific.com/courses/attacchi-applicativi-italia>
- questionario OAD 2018 con chiara separazione tra che cosa si attacca rispetto alle tecniche di attacco, con nuove domande su attacchi a IoT, a sistemi di automazione industriale e a sistemi basati sulla block chain
- omaggio del numero di gennaio 2018 della rivista ISSA Journal e di un libro di Reportec sulla sicurezza digitale ai rispondenti al questionario OAD 2018
- ampliamento del bacino dei potenziali rispondenti al questionario con accordi di patrocinio con Associazioni ed Ordini di categoria, quali ad esempio il Consiglio Nazionale Forense con i vari Ordini degli Avvocati territoriali
- Reportec come nuovo Publisher e Media Partner
- collaborazione con Polizia Postale ed AgID (in attesa di conferma).





INCHIESTA

SIAMO IN RITARDO PER IL GDPR E INVESTIAMO TROPPO POCO IN SICUREZZA	32
End-point al sicuro nell'era della mobility del cloud	38
Il machine learning di CyberArk protegge gli utenti privilegiati	39
End-point sicuri con il cloud e l'analisi comportamentale	40
Vecchie e nuove minacce mettono a rischio aziende e governi	43
L'automazione della network security	45
La sicurezza per l'IoT e le infrastrutture critiche	49
La protezione fisica di ambienti Smart	53

SPECIALE DATA CENTER

Il data center cambia e va nel cloud	59
Come garantire la sicurezza dei Container	61



L'IMPORTANZA DELLE PARTNERSHIP IN UN MERCATO SEMPRE PIÙ LIQUIDO

Con questo numero di **Partners** si inaugura una nuova linea editoriale, suggerita dall'evoluzione dei rapporti, lungo la catena del valore, tra i protagonisti che la compongono.

Il cloud e la digital transformation stanno cambiando per sempre il mercato dell'Information e Communication Technology, finora caratterizzato dalla vendita di hardware, software e servizi necessari per creare e mantenere un'infrastruttura informatica a supporto delle attività aziendali tipiche del settore economico di riferimento.

Il dipartimento IT era "isolato" in quello che si chiamava CED (Centro Elaborazioni Dati) e spesso soprannominato "quelli dei computer".

Costoro, impegnati per la maggior parte del tempo sulla manutenzione ordinaria, erano praticamente all'oscuro delle strategie di business e totalmente ignari dei processi produttivi.

Pietosamente non solleviamo il velo sui processi per

Le imprese ICT devono smettere di vendere tecnologia alle aziende utenti finali, che hanno bisogno di soluzioni e servizi gestiti

l'acquisto della tecnologia. Ancora oggi le organizzazioni aziendali delegano la responsabilità dell'ICT alle funzioni aziendali più disparate. Ma tutto ciò sta cambiando. All'interno delle aziende si è andato affermando l'acquisto di servizi in cloud da parte di manager di vario livello, che non hanno neanche pensato di dover coinvolgere l'IT interno.

Oggi il cosiddetto fenomeno dello "shadow IT", che vede l'Italia al primo posto, si sta "strutturando". Le imprese del canale ICT non possono più proporre progetti monolitici dai costi esorbitanti e devono, invece, arrivare a parlare direttamente con l'imprenditore per aiutarlo ad aumentare la competitività, migliorare i prodotti, rinnovare i modelli di business e a crescere, magari all'estero. System integrator e Var devono stringere una vera e propria partnership strategi-

ca con quelli che finora consideravano semplicemente dei clienti. Devono loro stessi integrarsi con il reparto IT, se non assumersene in toto la responsabilità in outsourcing. È un rapporto di fiducia come mai prima, che richiede competenze profonde sul business del "nuovo partner", più di quante ne possedevano gli addetti interni del "vecchio cliente".

Il modello è quello dei servizi gestiti, ma assumendo il rischio di non poter replicare il servizio per più clienti/partner, perché si deve garantire il vantaggio competitivo. Per supportare questo cambiamento Partners proporrà inchieste per orientare le scelte in uno scenario di continua evoluzione, contenuti di approfondimento, per la formazione interna ed esterna.

Buona lettura

di *Gaetano Di Blasio*



Trend opposti nel percorso verso la digitalizzazione

L'economia digitale divide in due il mercato, tra le aziende che si rinnovano e quelle più tradizionaliste, come confermano le analisi di IDC

di Paola Saccardi

La disponibilità di nuove tecnologie in grado di sostenere la digital transformation da un lato sta consentendo la modernizzazione delle aziende, ma dall'altro crea un divario profondo con quelle che resistono e hanno mantenuto un approccio più tradizionale.

D'altronde le innovazioni rese possibili dalle nuove tecnologie stanno aiutando molte aziende a rimanere competitive sul mercato, così come a inserirsi con successo nell'ecosistema digitale, sviluppando nuovi modelli di business.

La spesa mondiale in tecnologia

Secondo le ultime previsioni formulate da IDC, la spesa mondiale in tecnologie per la trasformazione digitale arriverà a sfiorare i 1.300 miliardi di dollari nel 2018, con una crescita del 16,8% sul 2017, e i 1.700 miliardi nel 2019, crescendo del 42% sempre rispetto al 2017. La parte più consistente, 1.300 miliardi di dollari, sarà spesa negli Acceleratori dell'Innovazione, quelle tecnologie che poggiano sulla Terza Piattaforma e che animeranno un processo di discontinuità in tutti i settori industriali.

IDC identifica queste tecnologie nell'IoT, nella robotica, nel cognitive/IA, nella realtà aumentata e virtuale, nel 3D Printing, nella blockchain, per citare le principali.

L'analisi di IDC ha anche preso in considerazione la spesa ICT nel periodo 2016-2021. A livello mondiale le previsioni di crescita (CAGR - tasso di crescita annuale composto) riportano un + 5,6%.



Un risultato proveniente da due tendenze opposte: nel 2021 gli investimenti nella Seconda Piattaforma caleranno del 3,3%, mentre quelli nella Terza Piattaforma aumenteranno del 4,7% e negli Acceleratori dell'Innovazione del 18,4%. In tutto, la spesa in tecnologie per la digital transformation crescerà con un CAGR 2016-2021 del 17,9%.

In particolare IDC si aspetta che dei 1.700 miliardi previsti nel 2019, 400 saranno investiti nelle quattro tecnologie della Terza Piattaforma: cloud, mobility, big data & analytics e social.

La tendenza in Italia

Anche in Italia l'andamento della spesa ICT è oggi il risultato di due trend opposti. Mentre da un lato sono in aumento gli investimenti nella Terza Piattaforma e negli Acceleratori dell'Innovazione, dall'altro risulta in contrazione la spesa ICT tradizionale che si focalizza sul mantenimento dell'infrastruttura esistente senza importanti progetti evolutivi. Nel 2017, il mercato ICT italiano è cresciuto dell'1,9%, per un valore totale di 30 miliardi di euro, evidenzia IDC. Terza Piattaforma e Acceleratori dell'Innovazione sono tuttavia cresciuti a un ritmo molto più elevato: per esempio, il cloud del 27,8% e la realtà aumentata/virtuale del 335,6%. L'impatto che le tecnologie della Terza Piattaforma e gli Acceleratori dell'Innovazione avranno sulle aziende sono temi che sono stati approfonditi nel corso dell'IDC Digital Transformation Conference 2018 che si sono tenute di recente a Milano e Roma. ❖

Le trasformazioni in atto nelle aziende italiane

Secondo i dati contenuti nell'Assintel Report 2018, elaborato da IDC, emergono parecchi elementi di novità che disegnano per l'IT nazionale un possibile cambiamento di passo rispetto al passato

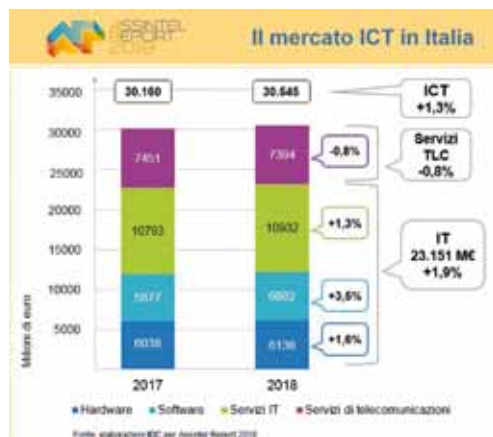
di Gian Carlo Lanzetti

L'Assintel Report 2018 realizzato da IDC ha messo in evidenza alcune tendenze in corso nelle aziende italiane. Di seguito abbiamo individuato alcune trasformazioni, che in alcuni casi sono già abbastanza radicate, in altri soltanto abbozzate.

Finalmente aperti all'innovazione

L'Italia ha sempre avuto una curva dell'innovazione tecnologica più lenta di altri paesi, a cominciare da Germania, Francia e Inghilterra. Tuttavia con i fenomeni legati alla Terza Piattaforma il nostro Paese ha saputo dimostrare di avere compreso fin da subito l'importanza strategica che soluzioni come cloud computing, big data /analytics, mobility e social business possono dare nel raggiungimento dei principali obiettivi IT e di business: contenimento dei costi, miglioramento dell'agilità infrastrutturale, time-to-market più spinto e customer experience più efficace e in grado di attrarre nuovi clienti e di fidelizzare quelli esistenti. Compresa l'importanza strategica che le nuove tecnologie e i nuovi modelli di delivery sono in grado di generare, molte aziende italiane hanno intrapreso il percorso di trasformazione digitale, consapevoli che "Questa volta un ritardo avrebbe creato un gap evolutivo molto più difficile da colmare". Lungimiranza, quindi, ma anche maggiore consapevolezza stanno inducendo le aziende nostrane ad allargare l'orizzonte anche verso innovazioni che vanno oltre quelle della Terza Piattaforma. E segnatamente verso i mercati del cognitive computing, della realtà virtuale e aumentata, della robotica, della stampa 3D oltre naturalmente dell'Internet of Things. Quell'insieme di innovazioni contrassegnato da IDC come il mercato delle tecnologie emergenti. Un business che nel 2017 ha raggiunto i 14176 milioni di euro, di

Il mercato ICT in Italia
fonte: IDC



cui la quasi totalità rappresentato da prodotti e servizi che ruotano attorno all'Iot (connettività compresa). Per la sola attività IoT lo sviluppo è stato nel 2017 del 16,4%, destinato a essere sostanzialmente ripetuto nel 2018.

Il cognitive computing vale 14 milioni che diventeranno 17 nel 2018. Realtà aumentata e realtà virtuale esprimono valori di 25 e 47 milioni di euro rispettivamente per i due anni. Di una decina di milioni di euro è valutato il mercato del wearable, con una prospettiva di raddoppio nei prossimi 12 mesi.

In linea nel cloud pubblico e nei big data

La stessa considerazione vale per il cloud pubblico e il mercato dei big data/analytics. Anche in questo caso l'Italia non sembra sfigurare rispetto al lavoro fatto all'estero. Nel 2017 questo settore è cresciuto del 28%, raggiungendo i 1.182 milioni di euro e anche per il prossimo anno il tasso dovrebbe restare indicativamente questo. Delle tre voci che lo compongono la quota dei servizi SaaS è quantificata in 742 milioni di euro (+23 l'andamento anno su anno). Ma i tassi di espansione maggiori spettano alle componenti IaaS e PaaS: +36-38%.

Facilità di utilizzo, possibilità di accedere a soluzioni emergenti con un metodo di pagamento basato sul principio del pay-as-you-go e una maggiore consapevolezza dei livelli di sicurezza sono i driver degli investimenti delle aziende verso il cloud pubblico.

Per quanto riguarda il segmento dei big data & analytics la curva di crescita è tutta in salita anche nel nostro paese: +21% nel 2017 e +26% nel 2018, con valori assoluti rispettivamente pari a 276 e 348 milioni di euro.

Come sottolineato anche da altre ricerche, a sostenere la domanda vi è in questo caso la necessità delle aziende di estrarre valore da una quantità e da una varietà di dati in continuo forte aumento, al fine di prendere decisioni

informate e anche di configurare nuove tipologie di modelli di business. L'ottica perseguita è soprattutto quella predittiva.

Priorità al cliente

Nelle nuove tecnologie IT le aziende non investono più unicamente per la riduzione dei costi (28%) o per il miglioramento della produttività (27% delle risposte multiple). Si spende principalmente per il miglioramento del grado di soddisfazione e la fidelizzazione dei clienti: per ben il 61% delle aziende questa rappresenta la priorità per il 2018. Si tratta di una indicazione relativamente nuova. Si legge nel report: la focalizzazione sul cliente rappresenta, secondo questa fonte, la strategia di business emergente delle aziende che sono riuscite e uscire dalle paludi della crisi e che stanno cercando ora di impostare una strategia di sviluppo definita basandosi sul principale vantaggio competitivo di cui dispongono e su cui ritengono esercitare un certo grado di controllo: la relazione con il cliente. Priorità minori rispetto alle tre citate sono il miglioramento della marginalità su prodotti e servizi (23% delle preferenze sempre in una scala di risposte multiple), lo sviluppo di nuovi prodotti e servizi (18%), la conformità alle normative (13%) e l'ingresso in nuovi segmenti di mercato (11%).

Un cenno alla riduzione dei costi aziendali: questo obiettivo resta invece prioritario soprattutto per le imprese che stanno faticosamente cercando di stare ancorate alla propria tradizionale posizione di mercato, senza investire più di tanto in innovazione.

DX: il focus sul ripensamento dei processi

Si parla tanto di trasformazione digitale: ma cosa significa esattamente e come si stanno preparando le imprese italiane? Il documento di Assintel-IDC fornisce delle prime risposte. "Per il 39% di esse la DX (digital transformation) si configura con la capacità di ripensare il modello di business dell'organizzazione, una missione strategica che si alimenta attraverso la capacità di avere una visione chiara del futuro e la confidenza di appartenere a un ecosistema che si muove in modo sinergico". Pur nella complessità di questo tema, una seconda angolazione mette in risalto l'orientamento all'informazione come cardine per la costruzione di un vantaggio competitivo. Il 38% delle aziende punta a una delle variabili destinata a caratterizzare in modo ancora più determinante le regole dell'economia cosiddetta "driven data". Stando sempre alle rilevazioni di detta fonte, il 22% delle imprese attribuisce al percorso DX una valenza prettamente cliente-centrica, da tradurre nella capacità di implementare metodi e strumenti per orchestrare i canali di interazione digitale. Il ridisegno dei processi che si estendono e si ramificano a valle e a monte comincia a fare capolino anche nel tessuto italiano, sebbene non assuma ancora un carattere sistemico (6% di citazioni).

La disponibilità di capital di rischio e la disponibilità del management a rischiare rappresentano il carburante per la trasformazione digitale. Sono quindi dei freni all'avanzata della DX, unitamente alla mancanza di una cultura al cambiamento continuo e, ma più indietro, allo sviluppo di competenze.

Servono competenze

Quali sono gli approcci per orientarsi e valorizzare le nuove tecnologie digitali? A livello globale una delle sfide più grandi è lo sviluppo di competenze e attitudini in grado di orientare e far crescere le organizzazioni nella nuova economia digitale. L'Ita-

lia non fa eccezioni. In questo senso va letto con interesse, come evidenzia il report, l'approccio delle imprese nostrane orientato soprattutto a percorsi di formazione delle risorse esistenti (79%). Una scelta imposta anche dalle difficoltà a reperire sul mercato profili adatti alla sfida, nonostante la disponibilità di assumere nelle imprese anche figure al di fuori del nostro paese. Nella formazione comunque, stando ai numeri riportati, si fa ancora poco. Il 36% delle imprese italiane nell'ultimo anno ha erogato meno di 4 ore di formazione per addetto; il 30% ne ha erogato da 4 a 8; il 7% da 8 a 16.

A cosa serve l'IT?

Da ultimo un accenno alla direzioni dell'IT. Ovvero della funzione IT o non di quella business come visto in precedenza. Per il prossimo anno la principale priorità sarà ancora il controllo dei costi, indicata dal 45% delle aziende. In ogni caso, è sottolineato, il controllo dei costi può essere visto anche come una razionalizzazione e una revisione della spesa, con un spostamento di risorse verso tecnologie che abilitano una trasformazione dei processi aziendali e uno snellimento della struttura dei costi di tipo tradizionale. Dopo la riduzione dei costi le altre voci di priorità accertate nel documento aiutano a comprendere quali sviluppi tecnologici le imprese abbiano in programma per il breve-medio termine. Il 21% avrà come obiettivo l'automazione e l'ottimizzazione dei processi IT. Un passo ritenuto fondamentale nel percorso di trasformazione digitale del business aziendale, in particolare per poter liberare risorse dalla gestione dei processi a favore dell'innovazione. In questo contesto, viene fatto notare, razionalizzare e migliorare infrastrutture organizzazione del reparto IT significa affidare a partner esterni la gestione della complessità tecnologica: l'outsourcing dei servizi IT sarà infatti una priorità per il 17% delle imprese. ❖

I nuovi ecosistemi digitali

Entro il 2020 più di un terzo della spesa IT mondiale per software e infrastrutture si indirizzerà verso il cloud

di **Gian Carlo Lanzetti**



Nei prossimi due-tre anni un terzo delle imprese del Global Ranking 2000 di Forbes crescerà su prodotti e servizi digitali a un tasso almeno doppio rispetto agli equivalenti tradizionali. Entro il 2019, prevede IDC, il 40% dei progetti IT avrà come obiettivo quello di monetizzare dati e informazioni creando nuovi prodotti e servizi digitali. Uno dei paradigmi di Industry 4.0 è anche questo. Si stima ancora che entro il 2020 la metà delle imprese del Ranking prima citato avrà creato prodotti, servizi ed esperienze del tutto nuovi basati esclusivamente su architetture digitali. Sono alcune previsioni riguardanti la DX Economy, o della digital transformation. La trasformazione digitale sta infatti tracciando un solco profondo nei mercati internazionali tra le imprese che riescono ad espandersi nell'ecosistema digitale e quelle che restano ancorate a modelli tradizionali. Secondo IDC lo spending globale veicolato dalle tecnologie della Terza Piattaforma si espanderà oltre duemila miliardi di dollari, con un trend di crescita a doppia cifra rispetto al tradizionale spending Ict, che andrà ad attestarsi su tassi di crescita simili a quelli del Pil in un orizzonte quinquennale.

Cloud, tecnologie cognitive e AI

L'integrazione nei nuovi ecosistemi digitali passa attraverso il rinnovamento delle infrastrutture aziendali, dove il cloud rappresenta il connotato di una rivoluzione che sta attraversando il mondo intero: entro il 2020 più di un terzo della spesa IT mondiale per software e infrastrutture si indirizzerà verso il cloud. Negli ultimi anni, puntualizzano gli studi di IDC, non soltanto è cambiata in modo radicale la proposta tecnologica degli operatori ma stanno cambiando progressivamente le relazioni nella filiera industriale. Sempre entro il 2020 il 70% della attività dei cloud software provider sarà mediato da nuovi operatori di canale, che sapranno muoversi come broker e advisor tra ecosistemi diversi. Come più altre volte ricordato un ulteriore fattore tecnologico

Le offerte di lavoro relative alle nuove professioni digitali emergenti sono cresciute da febbraio 2013 ad aprile 2017 a ritmi del +280%. Tra i profili oggi più ricercati ci sono: data scientist, cloud computing, cybersecurity expert, business intelligence analyst, big data analyst, social media marketing. Ma anche nelle professioni non strettamente tecnologiche sale la componente di competenze legate al digitale soprattutto nelle aree HR, contabilità e marketing. Anche le soft skill sono sempre più ricercate insieme ai profili digitali e su questo punto il divario è ancora maggiore.

È quanto emerge da un convegno organizzato presso l'Università Bicocca di Milano in cui le principali associazioni ICT - AICA, Anitec-Assinform, Assintel e Assinter Italia – insieme al MIUR e ad AgID – hanno preso spunto dagli aggiornamenti dell'Osservatorio delle Competenze Digitali per lanciare alcuni messaggi al mondo pubblico e imprenditoriale. Le loro proposte confluiranno in un nuovo documento, il quarto della serie, che sarà presentato nei prossimi mesi.

Questi dati confermano, se c'era bisogno, che la Trasformazione Digitale sta velocemente cambiando la fisionomia delle competenze necessarie ad aziende, pubbliche amministrazioni e cittadini per restare al passo con la globalizzazione. In più c'è la mancanza di consapevolezza su questo tema che rischia di lasciare sul campo molte Pmi. Manca un mercato del lavoro "modernizzato" per questo, manca un sistema della formazione capace di stare al passo con le professionalità richieste, manca infine una consapevolezza soprattutto dei piccoli imprenditori sulle trasformazioni in atto e l'urgenza di coglierne tutte le opportunità anziché farsi travolgere dalle stesse.

Verso competenze trasversali

Le trasformazioni in atto, che il mondo politico sta cominciando a cogliere con provvedimenti come Impresa 4.0 e le iniziative del

Miur e della Funzione Pubblica, stanno sempre più delineando la necessità di uscire dagli schemi tradizionali di valutazione e selezione delle figure professionali "digitali" per cogliere il mondo liquido delle competenze trasversali, in cui primeggia la capacità di cogliere e gestire il cambiamento continuo: non ha più senso seguire la moda di una ricerca "genetica" di nuove professioni, occorre cogliere attitudini, versatilità e capacità di collaborazione coniugate con capacità uniche di "vivere" le nuove tecnologie, oltre che ad utilizzarle.

Per Giancarlo Capitani, Presidente di NetConsulting cube, nel 2018 i paradigmi che guideranno il cambiamento nelle imprese, in crescita rispetto agli anni precedenti, saranno il mobile (67%), le attività di intelligence e analytics sui big data (61%), la cybersecurity (61%), l'Internet of Things (52%) e trasversale, a tutti i precedenti, il paradigma del cloud computing che si conferma pertanto oggi come il driver principale dell'Economia 4.0.

A questi vanno aggiunte le soft skills, intese come capacità di gestire aspetti relazionali, problemi complessi e scenari in rapido cambiamento.

Occorre quindi attivare nuovi percorsi di orientamento, partendo dal basso. Per esempio, secondo Fabio Fulvio, Responsabile Settore Politiche per lo Sviluppo di Confcommercio, su 800mila negozi aderenti all'Associazione dei commercianti soltanto il 54% ha un sito e di questo appena il 12% lo usa in qualche misura in modo attivo. Meno ancora (37%) sono i negozi che si avvalgono di strumenti social, con appena l'11% di questi che ne fanno un utilizzo moderatamente dinamico.

Bisognerà, infine, pensare anche a individuare un responsabile della Formazione, visti i cambiamenti in atto e il bisogno di riqualificazione delle persone all'interno delle aziende. Basti pensare che il 40% delle imprese meccaniche non ha laureati al suo interno e la meccanica è un settore portante del nostro tessuto produttivo. ❖

LOGISTICA E COMPETENZE DIGITALI PER GUIDARE IL RETAIL

Ottimizzare i processi,
proporre modelli di
vendita innovativi e
accrescere il rapporto
con la clientela.

Le aziende del
settore esplorano
le strade per
aumentare i
profitti e ridurre
i costi

di *Gian Carlo Lanzetti*





Il mondo del retail si interroga sulla ricerca di nuovi modelli e di una panacea che non esiste. Tante sono le tendenze in atto esplorate per ottimizzare le operation e massimizzare i risultati di vendita.

Si parla e discute soprattutto della 'predictive distribution' come quella del modello Amazon, ma anche della logistica a supporto dell'eCommerce. Come pure temi caldi sono l'automazione dei magazzini, il ruolo della logistica collaborativa o l'Internet of Things all'interno dei nuovi schemi di supply chain con, in particolare, una forte attenzione ai possibili utilizzi della blockchain.

Un elemento centrale sono sempre i dati: secondo Giuseppe Grandinetti di Vibram (azienda di calzature) i dati sono il nuovo petrolio e il digital dovrebbe essere un aggregante, un settore orizzontale per far interagire tutte le divisioni aziendali. Questi i principali temi emersi all'ultimo Forum Retail, che ha fatto il punto sul commercio in Italia.

Secondo Altroconsumo e QVC il canale più utilizzato per lo shopping è ancora il retail fisico con una quota dell'80,9%

Magazzini 4.0

Dell'automatizzazione nei magazzini si parlò soprattutto come premessa o «corollario» per una applicazione efficace del concetto di Industria 4.0.

«Per una industria di questo tipo – sostiene Antonio Rizzi, Professore Ordinario di Logistica e Supply Chain dell'Università degli

Studi su Parma – ci vuole una logistica 4.0. Uno degli obiettivi da porsi è la identificabilità degli oggetti dato che ognuno di essi è per sua natura univoco».

Di progetti concreti hanno parlato Theo Ricoveri, Responsabile Sviluppo Logistico di Coop Italia, e Giuseppe Cigarini, Corporate Logistics Manager di Nestlé Italia. Il primo si è soffermato sui lavori di efficientamento degli spazi presso l'hub di Prato dove si è passati dal picking tradizionale al Miniload per i 4680 colli mediamente lavorati ogni giorno e ora ci si accinge a implementare Shuttle 2018. Con ulteriore miglioramento in termini di flessibilità e produttività e un payback articolato su quattro anni.

Cigarini ha invece portato come testimonianza l'investimento in corso presso il sito di Benevento che produce pizze che da quest'anno saranno distribuite non solo in Italia ma anche in Europa (in precedenza le pizze di questa azienda erano «made in Germany»). Nello spirito della digital transformation, il magazzino da 3600 posti pallet è stato ridisegnato in simultanea con quello della fabbrica, con impiego di tecnologie multi-Shuttle e più avanti forse anche di blockchain. Il payback in questo caso si aggira intorno ai tre anni, tenuto conto dei benefici economici della normativa sull'Industry 4.0.

L'ottimizzazione non si ferma in magazzino, ma continua in negozio, con processi che devono sempre più integrarsi ed espandersi in una strategia che contempi tutti i passaggi chiave dell'attività commerciale al dettaglio: il merchandising, la supply chain e le operazioni nei punti vendita.

Ci spiegano in particolare i responsabili di Relex Solutions, che è possibile migliorare la propria competitività attraverso assortimenti localizzati, l'uso redditizio dello spazio commerciale, la previsione accurata della domanda e il riassortimento, la pianificazione ottimale della forza lavoro. Grazie a specifiche soluzioni software tutto ciò può essere ottimizzato.



La digital transformation riporta le pizze dalla Germania a Benevento

Altroconsumo e QVC: prevale ancora lo shopping fisico

Dalle ricerche di Altroconsumo e Osservatorio QVC, realizzate e presentate in esclusiva per Forum Retail, emerge che il canale più utilizzato per lo shopping è ancora il retail fisico con una quota dell'80,9%; il web è utilizzato dal 55,2% del campione e nella maggioranza dei casi si sovrappone agli altri canali; la Tv rappresenta il 5,5%.

La tecnologia utilizzata a favore della customer experience digitale viene utilizzata nel 32% dei casi ed è maggiormente apprezzata se presente un ausilio di assistenza: casse self check out (72%), totem (59%) e APP (32%) sono le tecnologie maggiormente presenti nei negozi odierni.

Durante i due giorni, nel Future Lab sono emersi alcuni spunti per vincere la sfida dell'innovazione partendo da una «Road to Technology» fino alla definizione un Action Plan ed Ecosistemi, grazie al contributo di Speaker del calibro di Ernesto Ciorra (Enel), Lucia Chierchia (Electrolux) e Daniele Pes (Altromercato).

Forum Retail: più di 900 partecipanti

Più di 900 partecipanti, di cui oltre 150 relatori e 25 amministratori delegati del mondo retailer, si sono incontrati nelle due giornate d'evento e si sono confrontati su come connettere il consumatore digitale nel settore Retail.

«Le aziende si devono adoperare per fornire un servizio rapido ed efficiente nell'e-commerce e un'esperienza unica nel PdV (punto vendita) soprattutto devono essere in grado di mettere subito in pratica l'idea, migliorandola successivamente e prendendo qualche rischio», afferma Francesca Cattoglio, socio unico di IKN Italy.

Le molte testimonianze hanno permesso d'indagare dei beni nel mercato, le logiche dell'eCommerce e dei sistemi di vendita e la gestione dei comportamenti del consumatore nel punto vendita tradizionale.

La logistica braccio operativo dell'eCommerce

Nell'era digitale le aziende ricorrono alla logistica per diverse ragioni. Una è quella di aumentare il fatturato. Le testimonianze raccolte sono chiare al riguardo ed è questa la ragione per cui si è proceduto e si procede a una riconfigurazione della logistica per meglio asservirla al cliente digitale. «Dobbiamo essere più efficaci ed efficienti di prima», sostiene Filippo Bandini, Chief Operating Officer di È qui, un network di 103 parafarmacie con un fatturato di 52 milioni di euro, che aggiunge: «All'eCommerce provvediamo al momento con uno stock di prodotti dedicato ma all'interno dello stesso magazzino che serve i negozi. L'aggiornamento è giornaliero e la consegna avviene il giorno successivo a quello dell'ordine se fatto entro le 13. Ci siamo attivati per raggiungere anche zone geografiche non altrimenti presidabili».

I risultati realizzati sono confortanti: l'eCommerce genera attualmente il 12% dei ricavi, tra un paio di anni si prevede di arrivare al 20%. La personalizzazione della fascia oraria di consegna è forse il connotato principale della esperienza di Digital (Easy Coop), attiva nel settore alimentare. Dice Marco Di Falco, Co-Founder & Chief Operating Officer: «Al cliente inviamo anche un sms che mostra la foto del corriere. Il nostro assortimento è forte di circa 3mila prodotti a diversa temperatura controllata. Realizziamo il 98% delle consegne in orario, nel restante 2% dei casi il ritardo è inferiore ai dieci minuti».

Il food consegnato a casa anche grazie al digitale

Un settore in crescita è quello dei pasti a domicilio. Quello in cui opera Just Eat, marketplace che vanta più di 7mila ristoranti affiliati sparsi in circa seicento città italiane. «La nostra piattaforma - precisa il Delivery Director Francesco Valvano, - si preoccupa di gestire l'incontro tra domanda e offerta e di fornire consulenza ai ristoranti, avvalendosi anche dell'uso di tecnologie big data. Per i ristoranti si tratta di una opportunità per registrare un business incrementale, grazie a un servizio di consegne preciso e accurato, oltre che di notevole potenzialità».

Il tasso di penetrazione è per il momento basso: meno del 5% del mercato raggiungibile. Non mancano peraltro i competitor.

Just Eat è una idea nata in Danimarca ma sviluppatasi nel Regno Unito, basata sui concetti della community e della omnicanalità. Poiché la supply chain tradizionale non è più sostenibile essa va riconfigurata in un'ottica cliente-centrica sposandola a modelli di logistica sempre più flessibili.

Un ruolo importante nello sviluppo di nuovi business e modalità di vendita lo gioca la digitalizzazione, che significa in primis app seguite da chatbot, ma supportate da soluzioni progettate per ottimizzare i processi. Le prossime evoluzioni sfrutteranno anche altre tecnologie come intelligenza artificiale e blockchain

In particolare, le criticità da affrontare sono almeno 5: allocazione intelligente delle risorse a disposizione; sviluppo della tracciabilità; esecuzione puntuale e flessibile; possibilità di accesso ai dati in mobilità (da ogni dispositivo e da ovunque); automazione avanzata bilanciata con le altre funzioni aziendali.



I big data guidano le consegne di Just Eat

La customer experience al centro della strategia dei retailer innovativi

Una ricerca di JDA e RSR condotta su un campione di retailer innovativi e tradizionali ha analizzato il diverso approccio verso l'utilizzo della tecnologia

di Paola Saccardi

L'innovazione tecnologica sta portando vantaggi a molti settori tra cui quello della vendita al dettaglio e i retailer stanno capendo che investire in questo senso è una strategia vincente. Tuttavia al centro dell'evoluzione del settore c'è sempre il cliente, attorno al quale ruotano esigenze, abitudini di acquisto, preferenze e così via.

Entrare in relazione stretta col cliente, prevederne i bisogni e soddisfarli sarà essenziale per il successo del settore. In questo la tecnologia rappresenta uno strumento fondamentale per offrire una customer experience di valore.

Risultati interessanti per capire l'evoluzione in atto sono stati presentati da JDA Software Group nell'indagine '2018 Retail Disruptors Survey', elaborata da Retail Systems Research (RSR), che ha coinvolto oltre 100 retailer innovativi e non in tutto il mondo, rivelando dati interessanti.

«I risultati dell'indagine sono chiari: gli innovatori sono più disposti a sacrificare una crescita più rapida per riuscire ad offrire l'esperienza cliente che gli acquirenti si aspettano. I retailer innovativi inoltre sono consapevoli che

la tecnologia rappresenti un fattore strategico e non solo un costo da gestire. Questa consapevolezza sarà fondamentale per il loro

successo nella fase di continua evoluzione del settore» ha dichiarato JoAnn Martin, vice president industry strategy, JDA.

Dai risultati dell'indagine è emerso che il 66% degli innovatori si dichiara profittevole, mentre il 18% ha indicato una previsione di crescita nei prossimi 18 mesi. Il 49% dei retailer innovativi cresce a un tasso annuale superiore all'11%, mentre solo il 30% dei retailer tradizionali registra la stessa percentuale in positivo. Gli innovatori affermano che la chiave del loro successo risiede nella velocità fornita dalla tecnologia, nel bilanciare i profitti e nel mantenere le promesse al cliente. L'affidabilità, in particolare l'attenzione alla coerenza di esecuzione (62%) e alla profittabilità (60%), è la qualità che gli innovatori ritengono più importante, mentre si rifiutano di sacrificare la redditività per una crescita più rapida.

Quello che sembra caratterizzare i retailer innovativi rispetto a quelli più tradizionalisti è in pratica l'utilizzo della tecnologia per migliorare l'esperienza cliente. Il 25% degli innovatori, infatti, offre un'esperienza di shopping continua attraverso tutti i canali, rispetto al solo 13% dei tradizionali.

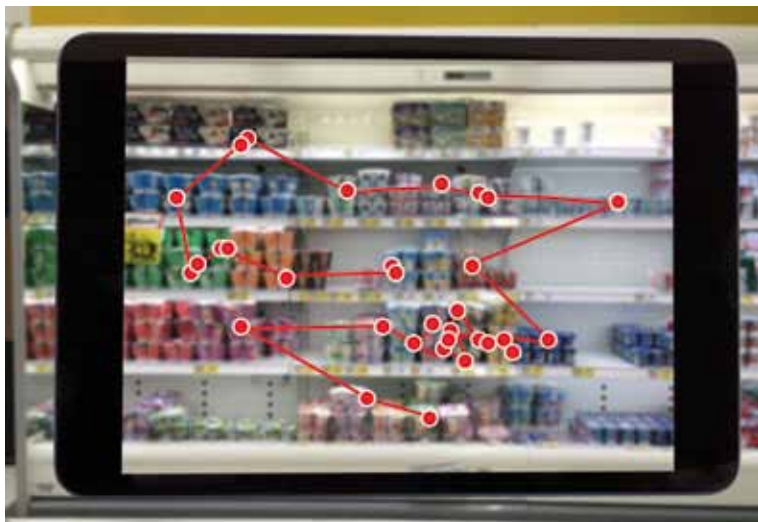
I retailer innovativi privilegiano investimenti in funzionalità digitali incentrate sul cliente. Il 25% degli intervistati ha implementato tecnologie digitali, rispetto al 19% dei non innovatori. Dato ancor più interessante, il 35% dei



retailer tradizionali non ha in programma di implementare tecnologie digitali, rispetto al 25% degli innovatori. Il divario maggiore si riscontra tra le capacità digitali già implementate e la pianificazione di un cambiamento, prova che gli innovatori del retail hanno un approccio 'fail fast and move on' verso le tecnologie che non soddisfano le loro esigenze. Quindi questi ultimi sono più propensi a implementare nuove tecnologie per migliorare l'esperienza del cliente, ma sono anche veloci nel cambiare direzione quando non vedono i benefici previsti.

Per quanto riguarda, invece, l'evoluzione futura dei negozi, dall'indagine emerge che anche secondo i retailer innovatori l'importanza dei negozi fisici non scomparirà in quanto riconoscono che l'esperienza diretta del cliente è vitale. Infatti l'87% degli innovatori e il 79% dei non innovatori hanno negozi fisici e continueranno ad aprirne altri in futuro.

Gli innovatori del retail progettano anche di investire nelle aree prioritarie per l'acquisizione dei clienti che si focalizzano sulla creazione della vendita esperienziale. Il 58% degli innovatori si concentra su contenuti lifestyle coinvolgenti mentre sul lato non innovatori la percentuale scende al 45%. Inoltre, il 57% degli innovatori afferma di investire in eventi e attività orientati al cliente, mentre solo il 34% dei non innovatori lo sta facendo. Tuttavia, tutti i retailer concordano sul fatto che investire nella customer experience è fondamentale per attirare clienti presso i propri negozi e farli ritornare (55% degli innovatori vs. il 54%



dei non innovatori).

La chiave del successo dei punti vendita dipenderà proprio dalla capacità di creare esperienze accattivanti e nell'utilizzarli anche come centri di distribuzione per evadere gli ordini effettuati tramite altri canali. Il 71% degli innovatori intervistati ha dichiarato che la soddisfazione cross-channel porterà traffico nei negozi, un chiaro segno che le opzioni volte alla soddisfazione del cliente come acquistare online, ritirare in negozio (BOPIS) e acquistare online e fare il reso in negozio (BORIS) saranno sempre più diffuse. Anche la tecnologia interattiva (62%) e i programmi di fidelizzazione (60%) sono consideranti rilevanti per favorire l'incremento delle visite ai negozi.

Secondo JoAnn Martin, la direzione che i retailer dovranno prendere, soprattutto per andare nella direzione dell'innovazione, sarà quella di: «trovare il giusto equilibrio tra intuizioni umane e basate sui dati. Implementare nuove tecnologie rapidamente, e cambiare direzione se non funzionano. Sarà importante anche mantenere la massima priorità di velocità e agilità per poter rimanere sempre in prima linea nel mutevole settore della vendita al dettaglio».

Dalla centrale al negozio, l'operatività integrata con Brother

di **Gaetano Di Blasio**

Soluzioni e servizi all'avanguardia per rendere più efficienti i processi e i flussi di lavoro nel retail, grazie all'etichettatura mobile, l'integrazione con i sistemi centrali e la gestione documentale

La reingegnerizzazione in chiave digitale del retail deve principalmente puntare a due obiettivi: massimizzare l'esperienza dei clienti e migliorare l'efficienza lungo tutta la filiera, con una concentrazione particolare sul punto vendita e sull'ottimizzazione dei processi.

Il tutto in un contesto ipercompetitivo e in continuo cambiamento.

Brother fornisce soluzioni e servizi progettati per aiutare il retail a vincere queste sfide, superando le aspettative dei clienti attraverso efficienza e velocità, come spiegano in Brother.

Più precisamente, questo è possibile grazie a servizi gestiti del parco tecnologico, a soluzioni di stampa mobile per l'operatività in magazzino e in negozio, a scanner e software per la gestione documentale elettronica.

Non esistono soluzioni adatte a tutto, affermano in Brother, evidenziando quanto sia dispendioso e inefficace adottare infrastrutture tecnologiche che non si integrano né connettono all'ambiente preesistente.

Per questo, grazie alle capacità di personalizzazione delle proprie soluzioni e attraverso l'esperienza dei propri partner, Brother fornisce strumenti progettati per essere facili da

utilizzare, in grado di accelerare i flussi di lavoro e portare efficienza nei processi cardine del retail: magazzino, scaffale, back office.

In negozio e sullo scaffale

Il punto di contatto col cliente è chiaramente il più importante e a questo Brother dedica le soluzioni di stampa P-touch, che consentono di creare e personalizzare etichette, in diversi formati, con font, immagini, bordi e codici a barre per veicolare qualsiasi informazione ai clienti del punto vendita. Le gamme QL e TD, spiegano in Brother sono l'ideale per stampare informazioni importanti che devono durare nel tempo, come nel caso dei badge o, soprattutto, per etichette di medicinali e prodotti sanitari, alimenti con date di scadenze e così via.

In negozio l'etichettatura in particolare è uno strumento fondamentale: si pensi anche semplicemente ai capi di abbigliamento che sono provati e maneggiati dalla clientela o, meglio ancora, ai processi di repricing che possono essere effettuati direttamente a scaffale, in tempo reale e senza errori, ottimizzando in questo modo i flussi di lavoro interni al punto vendita.

Effettuare in negozio questa operazione apparentemente banale, richiede uno strumento adeguato ed efficiente, come le stampanti RJ di Brother.

Si tratta di una gamma mobile a elevata qualità, che consente di stampare e trasferire etichette o ricevute nel formato

Back office avanzato per fornire la digitalizzazione ai clienti del retailer



Il repricing in negozio con l'etichetta che arriva dalla centrale

Per massimizzare i risultati delle promozioni (sia in occasioni speciali, come il Black Friday sia per azioni estemporanee) le operazioni di etichettatura devono essere svolte in negozio rapidamente, ma devono essere a prova di errore, anche se spesso avvengono in momenti convulsi.

Per questo Brother mette a disposizione strumenti portatili e indossabili per la stampa in piccoli formati, che, grazie a un team di esperti in grado di personalizzare o creare soluzioni dedicate su specifiche richieste del cliente, ottimizzano i flussi di lavoro, integrando il back office. In particolare, le stampanti RJ possono essere collegate al sistema gestionale centrale.

In questo modo l'etichettatura in negozio avviene senza rischio di errore, perché l'operatore non deve fare nulla: il dispositivo Brother legge il codice a barre e riceve dal gestionale il nuovo prezzo corretto e autorizzato che viene automaticamente stampato.

Inoltre, sono disponibili etichette nere e rosse, altamente visibili, che gli esperti di Brother propongono come soluzioni ideali per evidenziare informazioni importanti a scaffale.

po" rapidamente, all'occorrenza. La flessibilità di stampa permette di stampare etichette pretagliate o continue, lunghe fino a un metro e tagliate con una taglierina automatica.

In magazzino

I flussi di lavoro vanno resi efficienti il più possibile e assicurarsi spedizioni certe e veloci prevede anche fornire indicazioni chiare ed evidenti, come quelle che si ottengono utilizzando etichette in due colori, oppure etichette e barcode personalizzabili. Anche in questo caso, dunque, si possono sfruttare le caratteristiche della famiglia RJ, sottolineano i responsabili di Brother, aggiungendo un dettaglio relativo a questa gamma di dispositivi: la robustezza. In sostanza sono resistenti agli urti, il che non guasta, sia per l'uso in negozio, sia per quello in magazzino, qualora dovessero cadere.

La gamma QL, inoltre, permette di stampare su supporti in plastica, che consentono di personalizzare i badge dei dipendenti, dando un nome al personale, soprattutto quello a contatto con il pubblico, con un impatto non trascurabile sulla customer experience.

I servizi per i clienti partono dal back office

Presso la centrale di un retailer, quanto nei suoi punti vendita, è fondamentale l'affidabilità degli strumenti con cui quotidianamente si producono documenti critici per il business e la relazione con il cliente: quali contratti, offerte, fatture, documenti di trasporto, opuscoli informativi e altro.



da 2, 3 e 4 pollici, spiegano i responsabili di Brother.

La stampa delle etichette è possibile anche tramite laptop, tablet o smartphone, in modalità wireless, grazie alla app gratuita Brother iPrint&Label, in modo da "intervenire sul cam-

Le stampanti RJ migliorano la fase di etichettatura in negozio essendo connesse alla centrale

La gestione documentale e gli info point

I servizi di scansione e archiviazione forniti da Brother permettono di migliorare l'accesso e la condivisione delle informazioni, passando a flussi di lavoro digitali.

Le soluzioni scanner di Brother consentono di acquisire, indicizzare, recuperare e proteggere i documenti. Soluzioni disponibili anche come servizio, che comprende sia i processi front-end sia quelli di back-end, gestendo una vasta gamma di supporti, compresi documenti di diverso spessore e schede di plastica. Sono servizi pensati tanto per le infrastrutture centralizzate quanto per i singoli punti vendita.

Questi ultimi, in particolare, possono organizzare i tipici "info point" in modo da accrescere l'esperienza del cliente. I sistemi L6000, L9000 o la Inkjet A3, in unico passaggio, consentono di stampare e digitalizzare fatture, contratti, piani finanziamento o documenti d'identità dei clienti proteggendone i dati con sistemi di sicurezza avanzati.

Opuscoli o altre informative possono essere personalizzate direttamente con A3 a colori.

Un'efficiente operatività si traduce in un miglior servizio al cliente, cui, per esempio, vengono fornite informazioni aggiornate in tempi rapidi, oppure sono offerti servizi quali la fornitura della documentazione in formato elettronico.

Brother mette a disposizione soluzioni di stampa e scanner di ultima generazione, valutando le esigenze del singolo cliente attraverso un servizio di assessment, in modo da consigliare i dispositivi più idonei.

Guardando oltre la scelta degli strumenti giusti, il punto di forza dell'offerta Brother è il servizio di stampa gestita Pagine+, che elimina le inefficienze in azienda. Sono, infatti, i partner di Brother a preoccuparsi della continuità operativa dei dispositivi, attraverso una manutenzione preventiva, per migliorare i flussi di lavoro, garantire la sicurezza dell'ambiente informatico e minimizzare i costi.

Più precisamente, viene effettuata una consulenza strategica determinata ad abbattere i costi, identificando le criticità dei processi di stampa. Il piano personalizzato prevede un costo copia certo, con report dettagliato di stampa sempre aggiornato. Un tool Web

consente di monitorare in modo completo e dettagliato le stampe effettuate.

La garanzia Premium assicura il corretto funzionamento della macchina (con eventuali ripristino per tutta la durata del contratto, manodopera e sostituzione componenti incluse) e la consegna automatica dei toner originali in sede. Un'operatività facilitata dalle capacità di autodiagnostica dei dispositivi Brother. I tempi d'intervento vengono abbattuti e, come accennato, la business continuity salvaguardata. Sono benefici importanti, che è difficile comprendere se non si misura la produttività e l'efficienza operativa.

Oltre che ai flussi di lavoro nel back office, le soluzioni Brother portano benefici diretti ai clienti, anche grazie alla possibilità di personalizzare le funzionalità dei dispositivi e utilizzando la tecnologia NFC. ❖

Brother L6000

La gamma Brother L6000, nel 2017, ha vinto il "Line of the Year award" di BLL, che misura l'affidabilità: ogni dispositivo ha mantenuto costantemente alte performance durante tutti i test, posizionandosi al di sopra dei valori medi di mercato.

Le caratteristiche riportate dal costruttore evidenziano il supporto di un volume medio mensile fino a 10mila, pagine, con caratteristiche quali tempo di uscita della prima stampa di 7,5 secondi e velocità fino a 50 pagine al minuto, capacità toner per fino a 20mila pagine, tecnologia NFC (Near Field Communication), integrata per un'autenticazione degli utenti semplice e sicura e stampa da mobile. A ciò si aggiunge un'interfaccia di utilizzo più intuitiva rispetto ai modelli precedenti, con display touch screen fino a 12,3 cm e una migliore connessione ai servizi cloud più diffusi.

Scanner

I nuovi modelli di scanner Brother permettono a più utenti di acquisire, memorizzare, recuperare, modificare e condividere documenti in più formati di file, senza bisogno di un pc. Le scansioni possono essere avviate dal touch screen o dai tasti funzione programmabili. Un sistema anti-inceppamento permette di scandire diverse tipologie di carta (27-413 g/m²). Tra le altre caratteristiche: rilevamento automatico del colore, allineamento automatico, salto pagine vuote, formattazione grassetto, gestione schede di plastica, scansione verso USB, funzione Secure Function Lock, Autenticazione Active directory, supporto FC.

Sap aiuta il retail con l'ERP di nuova generazione

La business suite SAP S/4HANA completamente ridisegnata su SAP HANA sfrutta la potenza di gestione di grandi volumi di dati, strutturati e non, per supportare la gestione 'live' del business

di **Paola Saccardi**

Il retail oggi è un settore che sta cambiando rapidamente con tempi decisionali sempre più serrati, aspettative dei consumatori in costante evoluzione e un'inarrestabile generazione di dati. Processi tradizionali come merchandising, supply chain e le operazioni in store sono attivati autonomamente da fonti nuove facilitate dall'intelligenza artificiale, dal machine learning e dai sensori voce e IoT. Le regole del gioco per continuare a essere un'azienda di successo sono in continua trasformazione e rappresentano una grande sfida per i retailer. E SAP segue questo settore e i principali trend che lo caratterizzano da oltre 40 anni. Oggi l'80% dei clienti retail secondo la classifica Forbes 2000 sono clienti SAP. In questo contesto, l'azienda di software tedesca ha creato un framework articolato per digitalizzare l'intera catena del valore, compreso il core, che funge sia da piattaforma per l'innovazione (ad esempio dei sistemi

di ingaggio con i clienti) che per l'ottimizzazione dei processi aziendali.

Su queste basi, SAP ha introdotto una nuova generazione di ERP intelligente e in tempo reale: SAP S/4HANA, una business suite completamente ridisegnata su SAP HANA che sfrutta la potenza di gestione di grandi volumi di dati strutturati e non. SAP S/4HANA è stata progettata per supportare una gestione "live" del business attraverso le tecnologie più avanzate: IoT, Mobile, Big Data, Cloud.

Molti i grandi retailer globali che sfruttano le soluzioni SAP, tra questi Lidl che con SAP for Retail basato su SAP HANA analizza i dati di inventario in tempo reale e risparmia tempo attraverso processi semplici e ottimizzati, o Zalando che per gestire la mole di tutte le transazioni finanziarie ha posto SAP HANA al centro della sua strategia di smart data e ora gestisce fino a 10 volte il volume delle transazioni. In Italia, Sibeg, imbottigliatore ufficiale per la Coca Cola, ha realizzato una "frigovertrina intelligente" basata su SAP Leonardo, con una smart box che monitora i prodotti all'interno, comunica posizionamento, temperatura, consumo delle bibite e lo stato degli asset; DPV, gruppo che opera nel mondo retail e GDO, sfrutta invece le potenzialità di SAP Business ByDesign, ERP in Cloud basato su SAP HANA, per gestire i picchi di attività e dei volumi di prodotto dei propri clienti, accedendo ai dati da qualsiasi luogo e dispositivo. ❖



Le diverse facce del consumatore digitale

Il processo di acquisto di oggi è diventato più complesso di una volta perché sono cresciuti i punti di acquisto e quelli dove acquisire informazioni. Il consumatore è quindi profondamente cambiato. Com'è oggi? Che percorso di acquisto intraprende? Come utilizza gli strumenti online e offline messi a disposizione dalle aziende?

di **Giancarlo Lanzetti**

“Il consumatore digitale allo specchio” è il titolo della ricerca condotta da Net-comm, il Consorzio del Commercio Elettronico Italiano, in collaborazione con Diennea MagNews, azienda socia del Consorzio e specializzata da oltre 15 anni nel digital direct marketing (MagNews si considera la prima piattaforma italiana per la comunicazione digitale multimediale). L'obiettivo dello studio era individuare il profilo del nuovo consumatore digitale e tracciare il suo customer journey in ottica omnicanale, attraverso un'analisi incrociata di caratteristiche socio-demografiche, comportamenti di acquisto e livello di interazione con i diversi strumenti di relazione tra l'azienda e l'acquirente, provenienti sia dal contesto digitale che da quello fisico.

La survey è stata condotta su un campione rappresentativo di 29,8 milioni di internauti italiani (uomini e donne di almeno 18 anni di età che risiedono su tutto il territorio nazionale) composto da circa 2.000 individui che hanno acquistato online o offline nei sei mesi precedenti al periodo di somministrazione della ricerca (praticamente nella seconda metà del 2017) almeno una delle cinque categorie di prodotto oggetto dell'analisi: abbigliamento, scarpe e accessori; elettronica di consumo; bellezza e cosmesi, salute e benessere, arredamento e home living. Ma le indicazioni emerse, hanno sottolineato gli esten-



sori della ricerca, hanno valenza universale. Il 70% degli intervistati sono risultati essere e-shopper, mentre il restante 30% acquirenti "analogici".

Gli internauti italiani sono stati segmentati attraverso tre dimensioni relative al percorso di orientamento di acquisto: i touchpoint che hanno composto l'esperienza di shopping, gli eventi ('trigger') che hanno portato alla finalizzazione dell'acquisto, il canale in cui è stato effettuato l'acquisto (online e offline). Ogni consumatore, approcciando in maniera diversa

queste tre variabili chiave, crea la sua personale esperienza di acquisto, dove il contesto online e offline si intrecciano sempre più.



Le tipologie di consumatore

Attraverso la ricerca, sono stati individuati 8 tipologie di consumatori, caratterizzate da specifici comportamenti di shopping e di relazione con il brand. La segmentazione, come detto, è stata sviluppata sulla base di tre dimensioni: il canale utilizzato (online o offline), i touchpoint attivati e considerati rilevanti nella decisione e gli eventi (o trigger) che hanno convinto il consumatore ad acquistare un determinato prodotto in un preciso momento.

- 1. Il Tradizionalista informato:** over 65, alto spendente, acquista offline ma si informa online, perché riconosce le fonti digitali come strumenti utili per reperire informazioni. Utilizza quindi con disinvoltura i touchpoint digitali per orientarsi nei suoi acquisti offline. Rappresenta il cluster con la spesa media più elevata (+130% rispetto alla media).
- 2. Il Conservatore irremovibile:** è la categoria che ha meno confidenza con il digitale e si caratterizza per avere la spesa media più bassa (-72% rispetto alla media). Acquista solo in negozio, mai online. L'acquisto non è quasi mai preceduto da un processo di orientamento e informazione ed è immune agli stimoli "push"; considera rilevante solo il parere dei commessi in negozio.
- 3. L'Influenzabile:** è un cluster variegato, con maggiore concentrazione di donne, sotto i 25 o sopra i 65 anni. Poco digital confident, ma con grande familiarità nell'uso del mobile. Meno fidelizzato a un brand o a un prodotto, compra prevalentemente offline, ma è "digitalizzabile". La spesa media è bassa (-47%).
- 4. L'Informivoro:** i più evoluti digitalmente, sono maggiormente uomini, under 30. Comprano online e spesso attraverso le App. Sono alto spendenti (+85% rispetto alla media) ma scarsamente fidelizzati ai brand e molto sensibili alle offerte e ai trigger di ogni genere. Hanno un percorso di acquisto molto lungo.
- 5. Il Fast shopper:** sono soprattutto donne, con un'età media compresa tra i 35 e 54

anni. Comprano online: per loro l'acquisto è la risposta a un bisogno e per questo sono poco influenzate dai trigger. Sono razionali e hanno un ricambio di prodotti elevato. Usano la tecnologia, ma non in modo avanzato. La spesa media è bassa (-44%). È il cluster di maggior peso: raggruppa quasi il 32% dei consumatori (quello di peso minore, 5,7%, è il precedente).

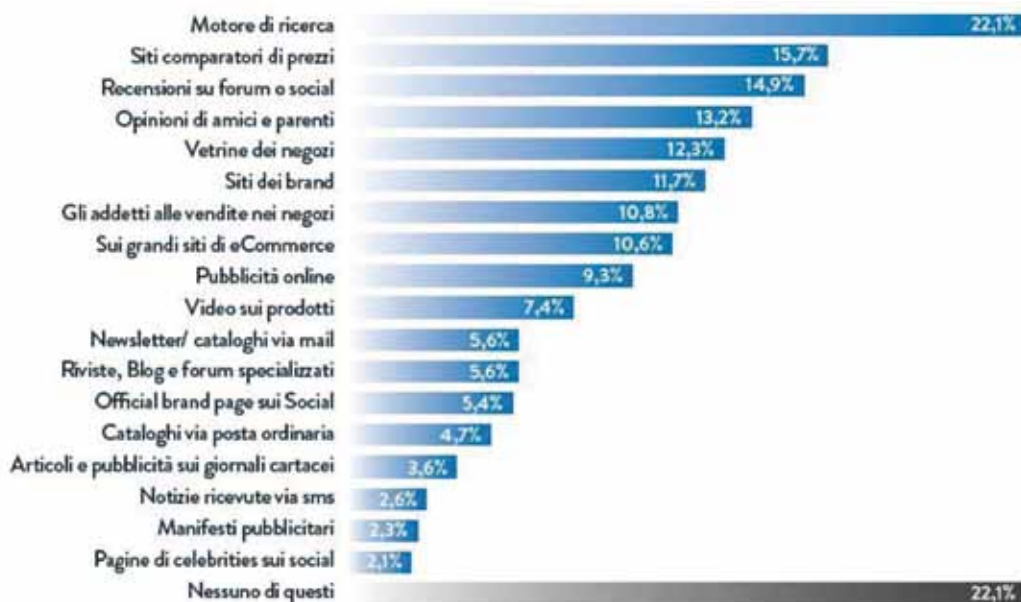
6. Lo "Sherlock" digitale: uomini, under 30, molto digital e social confident. Comprano online e via App. La loro categoria di prodotto preferita è l'Elettronica di consumo e difficilmente riacquistano lo stesso prodotto. Sono molto influenzati dai comparatori e dalle recensioni. La spesa è elevata (+25% rispetto alla media). Come per gli Informatori, il loro customer journey è molto articolato. Il loro peso è dell'11,7%, grosso modo come quello del Consumatore Irremovibile.

7. Il Look maniac: donne, under 24. Sono molto attente a quello che dicono i social e gli influencer, danno importanza ai con-

sigli di amici e conoscenti, non trascurano le vetrine dei negozi: cercano ispirazione e sicurezza, vogliono acquistare i prodotti più cool secondo i trend del momento. Comprano online, principalmente abbigliamento e arredamento. Sono abbastanza fedeli ai brand e la loro spesa è leggermente inferiore alla media (-20%).

8. Il Friend follower: decidono cosa acquistare basandosi sui consigli di amici e conoscenti. Se vanno in negozio prestano molta attenzione alle opinioni degli addetti alle vendite. Sono principalmente uomini, tra i 55 e i 64 anni. Comprano online, non hanno un brand preferito e sono poco fedeli. La spesa è superiore alla media (+33%).

I touchpoint informativi utilizzati dai consumatori



Valore spesa (euro) e tasso di penetrazione (peso) degli 8 cluster



Considerazioni e osservazioni

Dall'analisi dei dati e delle metodologie impiegate si possono cogliere i seguenti rilievi:

- La materia è molto complessa e la complessità si coglie a ogni livello. Più il consumatore è digitale maggiore è il grado di complessità.
- Conseguentemente la definizione e gli ambiti di ciascuno degli otto cluster si devono intendere come molto flessibili.
- Di fatto ogni consumatore ha una sua customer journey, con in comune la omnicanalità;
- Anzi la omnicanalità si può considerare il driver principale di ogni strategia riguardante il processo di acquisto.
- I costi sono anche in relazione alla complessità: più questa è elevata maggiori sono perché più elevati sono i punti di contatto da presidiare.

- I consumatori digitali utilizzano più punti di contatto di quelli offline: per l'Informivoro mediamente sono circa 5 i touchpoint usati a fronte di un indicatore medio per l'online di 1,6.
- Il primo strumento di informazione è il motore di ricerca (lo usano il 22,1% di tutti i consumatori), seguito dai siti comparatori di prezzi (15,1%) e dalle recensioni su forum o social (14,9%).
- In ogni caso il 70% degli acquisti online e offline analizzato in questa survey viene innescato da un trigger, cioè un evento specifico che scatena la decisione di acquisto;
- La ricezione di un messaggio è il trigger più efficace per gli acquisti online (29%) mentre la visita in negozio è il primo per lo shopping offline.
- I pagamenti digitali sono un importante elemento di differenziazione oltre che una opportunità per la multicanalità. L'orientamento anche in Italia è verso i micro pagamenti. ❖

L'Unified Retail Planning di Relex Solutions

Un software promette una riduzione del 30% dei livelli delle giacenze, del 40% dei deperimenti, mantenendo una disponibilità a scaffale superiore al 99%

di **Giancarlo Lanzetti**

Fra le tante soluzioni a supporto dell'attività relativa al retail c'è quella, del tutto nuova, proposta dalla finlandese Relex Solutions, l'Unified Retail Planning è un approccio nuovo, come ci spiega Elisa Bonaldi, Administration and Marketing Coordinator Italy: «I nostri competitor non sono in grado di offrire quello che per noi è invece possibile integrando le nostre soluzioni "storiche" per l'ottimizzazione della supply chain e dalla forza lavoro con i nuovi moduli per l'ottimizzazione degli spazi e dei planogrammi».

Relex Solutions è un'azienda nata nel 2005 come fornitore di soluzioni per la gestione della supply chain ed è andata incontro a una rapida espansione. Nel 2016 ha acquisito l'azienda britannica Galleria RTS, fornitore di un software per l'ottimizzazione degli spazi e dei planogrammi, e a giugno 2017 ha assunto una partecipazione nell'azienda finlandese Zenopt, che si occupa di ottimizzazione e gestione della forza lavoro.

In seguito a queste acquisizioni, Relex è ora in grado di offrire ai clienti un approccio unificato alla pianificazione, che permetta l'ottimizzazione trasversale dei principali processi dell'attività commerciale: il merchandising, la supply chain e le operazioni dei punti vendita.

Ottimizzando queste operazioni in maniera unificata si ottengono benefici ulteriori rispetto all'ottimizzazione di ogni operazione singolarmente.

«Per esempio il nostro modulo per la gestione della supply chain è in grado di calcolare proposte di ordine per il riassortimento dei punti vendita, sulla base di previsioni accurate della domanda. Tipicamente, i nostri clienti ottengono una riduzione del 30% dei livelli delle giacenze, del 40% dei deperimenti, mantenendo una disponibilità a scaffale superiore al 99%» afferma Bonaldi, che aggiunge: «Al tempo stesso il nostro modulo per la gestione degli spazi e degli assortimenti (ex Galleria) consente di personalizzare l'assortimento in base al profilo dei consumatori dei vari punti vendita, aumentando le vendite e diminuendo gli sprechi. Questi sono i benefici che le nostre soluzioni possono portare se utilizzate singolarmente».

La manager ci spiega inoltre: «Un esempio di pianificazione unificata è calcolare i riassortimenti non solo in base alle previsioni della domanda, ma anche in base alla disposizione dei prodotti all'interno del punto vendita e all'ampiezza dello scaffale, in modo da evitare, in fase di rifornimento degli scaffali, di fare avanti e indietro per il negozio e di riporre la merce in eccesso in magazzino. In questo modo, i riordini saranno probabilmente più frequenti (e quindi meno ottimizzati), ma

Le opportunità in Italia

Abbiamo intervistato Jarno Martikainen, Country Director di Relex Italy.

Parners: Come valuta il grado di maturità del mercato italiano verso soluzioni come le vostre?

Jarno Martikainen: A differenza di altri mercati in cui operiamo, quello italiano è piuttosto vario e frammentato, con una moltitudine di player di dimensione medio-grande, media e piccola. Un altro aspetto che abbiamo notato è la scarsa standardizzazione dei punti vendita all'interno della stessa catena, che rende più difficile l'introduzione di soluzioni per l'ottimizzazione della supply chain e dei planogrammi specifici per punto vendita. In questo senso, per Relex Solutions ci sono buone opportunità di portare vantaggi concreti con una gestione centralizzata e guidata dai dati, visto che siamo considerati la soluzione più flessibile e configurabile.

Detto questo, la pianificazione unificata dei processi nel retail deve essere vista come l'esito di un processo da intraprendere con il cliente. I vantaggi maggiori si ottengono quando il retailer sta già utilizzando la soluzione di riassortimento automatizzato dei punti vendita, quella per la pianificazione degli spazi, o entrambe. A questo punto, collaborando con il cliente, possiamo arrivare a integrare l'ottimizzazione della supply chain con quella dei planogrammi, o viceversa. L'ultima soluzione che stiamo integrando nella logica della pianificazione unificata è quella per la gestione dei turni di lavoro del personale all'interno del punto vendita.

P: In quali ambiti vedete le migliori opportunità?

J.M: Le opportunità migliori per noi sono nella GDO, in particolare del settore Food, grazie la presenza dei tanti prodotti, anche deperibili, con circolazione veloce e volumi alti.



Il secondo settore più adatto a Relex è del retail non-food continuativo, come per esempio DIY, elettronica di consumo, cura delle persone e casa.

Siamo fortunati che il valore concreto che possiamo portare al cliente è tipicamente e facilmente misurabile in termini di denaro; con prodotti ad alta rotazione si vede l'impatto positivo sull'abbassamento degli sprechi, sulla disponibilità a scaffale e sul valore totale dell'inventario già in un paio di settimane di produzione. I miglioramenti della pianificazione nell'ambito operativo

sono complementari specialmente per i retailer che riescono ad automatizzare i processi di pianificazione con il nostro aiuto.

P: State già trattando qualche implementazione: quali le modalità di pagamento?

J.M: Sì, nel mercato italiano abbiamo quattro progetti implementati e in fase di implementazione. Con tre siamo già in produzione. A livello globale Relex ha circa 180 implementazioni in produzione.

Per quanto riguarda la modalità di pagamento, Relex fattura un fee mensile per un servizio Software-as-a-Servive (SaaS). Non dovendo pagare una licenza, gli investimenti iniziali per i nostri clienti sono molto limitati. Curiamo personalmente sia la configurazione che l'implementazione del nostro software e i nostri progetti sono tipicamente molto snelli e veloci. Per quanto riguarda l'impegno del cliente nei nostri confronti, abbiamo scelto una strategia di obbligarci a fornire un servizio che porta valore al cliente. Offriamo condizioni di recesso dal servizio molto flessibili e spesso la fatturazione viene anche legata ai KPI conseguiti dal cliente, così che abbiamo un target comune di assicurare che il sistema faccia un bellissimo lavoro.

si potrà risparmiare nel rifornimento degli scaffali, che è una delle operazioni in assoluto più costose. In base a uno studio condotto da un nostro collaboratore su un retailer di generi alimentari, con questo approccio è possibile ridurre il costo del rifornimento a scaffale del 20%».

Tradizionalmente la pianificazione della forza lavoro viene fatta sulla base dei budget di vendita o delle previsioni di vendita. Un grosso retailer di fast moving goods utilizza

invece i dati provenienti dalla supply chain, e in particolare la previsione della domanda (tradotta in previsione dell'afflusso di clientela) e il programma di consegna delle merci, ottenendo un risparmio stimato nel 12% sul costo del lavoro e un servizio migliore, perché tarato sui reali bisogni della clientela. ❖

Bricocenter rinnova la gestione delle risorse umane con Talentia

Implementato un nuovo sistema di valutazione e gestione delle performance e dell'esperienza lavorativa, più dinamico e valorizzante per il collaboratore

di Paola Saccardi

In un mercato in continua evoluzione le competenze rappresentano uno strumento importante per supportare al meglio i clienti. È questa convinzione che ha spinto Bricocenter verso la necessità di rinnovare la gestione delle proprie risorse umane in modo da poterle analizzare e monitorare per favorire una collaborazione più efficace.

Il colosso del "fai da te" ha scelto Talentia Software per dotarsi di un nuovo sistema di valutazione e gestione delle performance e dell'esperienza lavorativa.

La società necessitava di un sistema agile e flessibile per adattarsi in modo veloce alla trasformazione all'interno dell'azienda e alle continue evoluzioni delle missioni. Dopo un'attenta analisi delle soluzioni presenti sul

mercato, Bricocenter ha scelto Talentia Software che è stata in grado di capirne i bisogni e di supportare il continuo progresso dei processi legati alle risorse umane.

Bricocenter è una realtà che fa parte di Adeo, una comunità di imprese aperte e interconnesse nel settore del miglioramento dell'habitat, e in Italia è presente con 53 negozi e oltre 1.500 dipendenti (che Bricocenter chiama 'collaboratori') che operano sul territorio.

«Bricocenter è parte di un colosso internazionale e nella strategia messa in campo nel mercato di prossimità le risorse diventano una componente ancora più importante per raggiungere gli obiettivi prefissati - ha spiegato Marco Bossi, Managing Director di Talentia Software -. Abbiamo analizzato le loro esigenze e sviluppato insieme una soluzione su misura che potesse rispondere immediatamente ai loro primari bisogni e continueremo a supportarli al massimo anche in futuro».

I vantaggi della nuova gestione HR

Una delle principali necessità espresse da Bricocenter è stata quella di "rendere dinamici i processi HR e di lavorare con sistemi di valutazione delle performance più semplici, snelli e intuitivi. In questo modo avremmo potuto beneficiare di una visione più ampia delle



Marco Bossi,
Managing Director
di Talentia
Software



ze espresse dai nostri collaboratori, che ha iniziato a scardinare i perimetri geografici e quelli fra le diverse funzioni aziendali, e abbiamo migliorato il livello di autonomia dei collaboratori che ora possono inserire nella propria missione delle aree di competenza o dei progetti individuali che prima non venivano tenuti in considerazione».

Nella nuova applicazione sono disponibili anche tutti i documenti e strumenti di accompagnamento alla formazione, sia per i collaboratori sia per i manager, così da garantire l'aggiornamento continuo e la fruizione dei contenuti tramite mobile.

Marco Bossi ha evidenziato come: «Le aziende che si sono affidate a Talentia Software stanno diventando realmente più "digitali", attraverso una vera evoluzione di strumenti, approcci e soluzioni, con l'obiettivo di migliorare i processi interni, incrementare l'operatività e la collaborazione, al fine di permettere una condivisione agile e veloce dei processi e dei dati. Queste realtà sono solitamente distribuite sull'intero territorio italiano, hanno un numero elevato di dipendenti e, di conseguenza, di competenze e ruoli professionali da gestire e monitorare. Introdurre strumenti tecnologici efficienti permette di snellire le attività, procedere in modo più flessibile e rapido, ottimizzare i tempi e concentrarsi così sulle attività di core business».



competenze, dei bisogni e delle ambizioni dei nostri collaboratori "a ogni livello" come ha evidenziato Laura Arioli, Responsabile Risorse Umane Servizi Interni di Bricocenter Italia. Un primo passo verso il cambiamento è stato quello di dotare di uno smartphone tutti i collaboratori, così da garantire la possibilità a questi di utilizzare tecnologie e applicazioni per sostenere la relazione con i clienti e semplificare le attività, ma anche di liberare tempo da dedicare a quelle prioritarie. Bricocenter ha deciso di installare su tutti gli smartphone aziendali un'app su misura sviluppata con Talentia per compilare e inviare la propria valutazione e i feedback verso altri colleghi in modo facile.

A un anno di distanza dall'inizio dell'utilizzo della soluzione di Talentia, Bricocenter ha potuto notare i vantaggi ottenuti a livello di esperienza collaboratore e di evoluzione dei processi in termini di accompagnamento.

Un altro aspetto importante per la società era quello di fornire ai collaboratori la possibilità di esprimere le proprie ambizioni e motivazioni così da favorire l'espressione dei talenti e delle potenzialità personali per intraprendere un percorso di carriera che tenga conto non soltanto delle competenze possedute ma anche delle aspirazioni personali.

«Abbiamo implementato questo nuovo metodo di valutazione e gestione da solo un anno, ma i benefici sono già molto positivi - ha spiegato Laura Arioli -. Abbiamo finalmente una visione globale delle competen-



di **Gaetano Di Blasio**

SIAMO IN RITARDO PER IL GDPR E INVESTIAMO TROPPO POCO IN SICUREZZA

Il 79% delle aziende italiane non è pronto per il GDPR e il 76% investe in sicurezza meno del minimo necessario. È il triste scenario emerso da un'inchiesta della nostra redazione

Guardando il lato positivo, possiamo osservare una crescita di attenzione nei confronti della sicurezza. Attacchi devastanti come WannaCry dello scorso anno e altri episodi legati alle estorsioni con il ransomware hanno portato in televisione e sui tanti canali d'informazione il problema della sicurezza informatica. Sembra tuttavia prevalere la vecchia logica del "tanto a me non capita", visto i livelli bassi d'investimento in sicurezza.

Un'inchiesta della nostra redazione ha sondato il tema della conformità al regolamento europeo e quello della spesa per la struttura dedicata alla sicurezza informatica.

I risultati sono deludenti: il 76% delle imprese che hanno risposto al nostro sondaggio o che abbiamo intervistato direttamente, spendono meno del 10% in sicurezza informatica, cioè meno dello stretto necessario, stando alle valutazioni effettuate dagli esperti di Gartner. Questi ultimi, infatti, ritengono che la suddetta quota occorra solo per la gestione ordinaria della sicurezza, come ci riporta Davide Del Vecchio, Global Head of Enterprise Security di Yoox Net-a-porter Group,

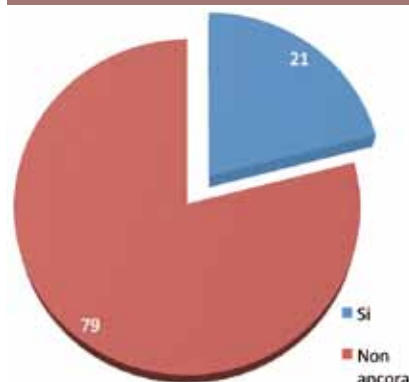
nonché membro del consiglio direttivo del Clusit. In altre parole potrebbe bastare a chi ha già messo in piedi una strategia per la security. Nella realtà, però, le imprese italiane sono ancora molto indietro, come sostengono molti analisti e come viene confermato dal nostro sondaggio.

Sono ben il 79% le imprese italiane che ammettono di non essere pronte per il GDPR (General Data Protection Regulation). Una normativa che è stata varata dall'Unione Europea nell'aprile del 2016 ed è entrata in vigore il 25 maggio dello stesso anno, fissando al 25 maggio del 2018 la data in cui avrà efficacia. In altre parole sono stati concessi due anni di tempo per mettersi in regola con la normativa.

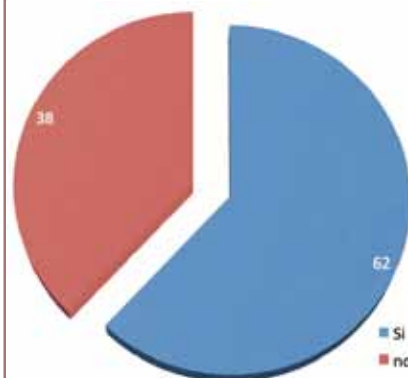
Sono rimasti poco più di quattro mesi, ma le imprese italiane non sono ancora pronte, almeno stando a una nostra inchiesta, realizzata sulla base di alcune interviste dirette e, soprattutto, un sondaggio cui hanno partecipato oltre 200 addetti ai lavori.

Sondaggio che, ci teniamo a precisare, non ha alcun presupposto statistico, non trattandosi di un campione

La tua azienda è già compliant con il GDPR?



Ritieni che il GDPR aumenterà la protezione delle imprese?



Il costo preferito alle prestazioni nella scelta del cloud provider

significativo, né in termini numerici né quale rappresentanza dell'universo di specialisti ICT, security manager e business manager (le tre tipologie di intervistati da noi contattati).

Peraltro, i risultati ottenuti, costituiscono una base di riflessione che ci permette d'integrare le opinioni espresse da numerosi esperti, sia in seno a società di ricerca qualificate, sia presso vendor del settore ICT, specializzati in sicurezza.

Sempre all'ultimo momento

In sostanza, dunque, sono poco più del 20% le imprese che si sentono a posto con la nuova normativa ed è probabile che si tratti perlopiù delle più grandi o, in particolare, delle banche e

delle società di telecomunicazioni, già soggette a regole stringenti imposte sia dall'attuale normativa italiana sulla privacy sia da normative internazionali. Aziende che avevano poco o nulla da aggiungere per essere conformi al GDPR.

Sappiamo bene che in Italia siamo abituati a ridurci all'ultimo momento, ma non sempre poi ci riescono le ciambelle col buco, come può testimoniare l'attuale sindaco di Milano, Giuseppe Sala, chiamato all'ultimo momento per far partire l'Expo 2015 e ora accusato di aver usato qualche scorciatoia. Meno male che è stato un successo, perché Gian Piero Ventura, ex commissario tecnico della nazionale di calcio, non può nemmeno

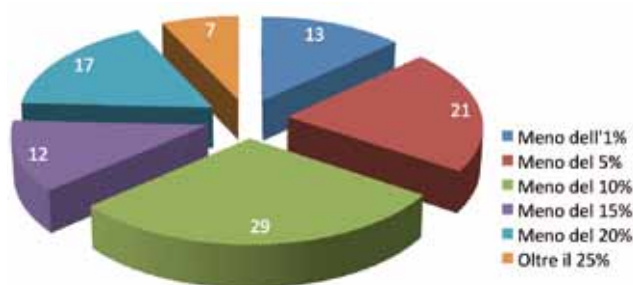
consolarsi dell'esito finale. Ad andarci di mezzo è stato anche il suo "capo" Carlo Tavecchio, costretto alle dimissioni dalla presidenza della Federazione Italiana Giuoco Calcio.

Rischi che corrono anche dirigenti delle imprese che non saranno conformi al GDPR in tempo.

Purtroppo in molti hanno ritenuto il 25 maggio prossimo, come la data in cui cominciare a realizzare il piano per la sicurezza e adeguarsi alle nuove norme. Di fatto, invece, è il giorno in cui potrebbero arrivare le prime ispezioni. Molti degli esperti con cui abbiamo parlato sono convinti che la corsa alla compliance partirà veramente solo dopo che fioccheranno le prime multe.



Quale percentuale del budget ICT dedichi alla cyber security?



Ricordiamo, infatti, che mentre banche e telco da tempo erano tenute a informare di eventuali violazioni, dal 25 maggio toccherà farlo a tutti e sono in tanti a non accorgersi di un attacco andato a buon fine se non dopo settimane o mesi

Un aspetto importante è la possibilità di “scaricare” parte della responsabilità a una società esterna. Un vantaggio per chi già utilizza servizi di terze parti per la sicurezza, cioè il 38% dei rispondenti al nostro sondaggio, che hanno dichiarato di esternalizzare almeno in parte la gestione della sicurezza.

Questo dato mostra un’opportunità importante per tutti: sia per le imprese del settore, che possono ampliare i propri servizi aumentando l’offerta di managed security service (o MSS) sia per le aziende della domanda, che possono concentrarsi sul proprio core business, delegando agli esperti le onerose e delicate operazioni di protezione dei dati. È evidente che il tutto dovrà reggersi grazie a un rapporto di fiducia, una vera e propria partnership tra chi finora ha “semplicemente” venduto soluzioni, come

firewall e antivirus e chi fino a ieri si limitava a installare del software e dei dispositivi.

Sul fronte della fiducia, la nostra inchiesta mostra un buon grado di maturità, rappresentato, a nostro avviso, dal punteggio più alto ottenuto dalla sicurezza nella scelta di un cloud provider, laddove il costo è l’ultima delle preoccupazioni.

Il cloud cambia le regole del gioco e spinge l’innovazione

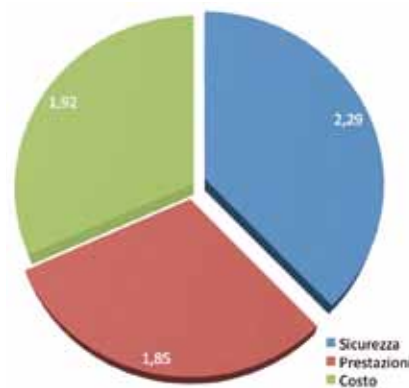
Il passaggio appena descritto potrebbe non riguardare solo la sicurezza e invece estendersi ad altri servizi informatici, secondo la logica “dell’as a service” introdotta dal cloud. Le imprese del canale ICT possono trovare crescenti benefici per il loro business dalla trasformazione in managed service provider, di cui la sicurezza è solo la punta dell’iceberg.

Alla fine, per un imprenditore si tratta di trovare il partner giusto che sappia fare il proprio mestiere, per concentrarsi sulle attività principali. Ciò non impedisce di conservare un reparto interno dedicato all’informatica e alla sua sicurezza, ma deve sussistere

La gestione della cyber security nella tua azienda è tutta interna o in parte in outsourcing?



Nella scelta del cloud provider in quale ordine hai considerato la sicurezza, le prestazioni e il costo (mettiti in ordine da 1 a 3 dove 1 è quello considerato il più importante).



una motivazione forte, quale potrebbe essere lo sviluppo innovativo. Sempre più la digitalizzazione sta portando “intelligenza” nelle operazioni industriali. È il fenomeno dell’Internet of Things. Le imprese devono e possono sfruttare le nuove tecnologie e le capacità di connessione e integrazione per ottimizzare i processi a tutti i livelli. In sintesi, il “vecchio” reparto IT” mai prima d’ora può guadagnare un ruolo di primo piano in azienda,

facendo diventare il CED il motore dell'innovazione aziendale.

L'adozione del cloud è in crescita, rallentata solo dalla necessità di salvaguardare investimenti pregressi e dalla vecchia abitudine italiana di aspettare che l'esperienza dei primi consolidi i processi a garanzia del successo.

Secondo quanto emerge dalla nostra inchiesta, la maggior parte di chi usa il cloud lo fa con attenzione: il punteggio più alto per le priorità viene infatti

assegnato alla sicurezza, con un 2,9 rispetto a massimo di 3, o, quantomeno alla sensazione di sicurezza che il cloud provider scelto è riuscito a trasmettere. Al secondo posto, ma quasi a pari merito c'è il costo, che arriva a 1,92, appena sopra all'1,85 assegnato alle prestazioni.

Non abbiamo approfondito le ragioni di questo voto, anche se la sensazione è che il cloud oggi viva principalmente di servizi storage ed è ovvia la preoccupazione per la sicurezza dei

dati, mentre le prestazioni vengono faticosamente accettate in funzione della banda a disposizione.

Sul prossimo numero di Partners l'inchiesta dedicata allo storage potrebbe fornire un tassello in più.

Non esitate a scrivere alla redazione (redazione@reportec.it) per suggerire temi per i prossimi sondaggi e per iscrivervi alle nostre survey. ❖



End-point al sicuro nell'era della mobility del cloud

di **Giuseppe Saccardi**

L'affermazione della mobilità come strumento atto a spingere la produttività e a favorire il contatto con il cliente e tra partecipanti di un gruppo di lavoro, nonché a facilitare gli sviluppi nello smart working, ha aperto la strada al mercato della sicurezza dell'end-point, un mercato che è in continua crescita e apre la strada agli operatori di canale per perseguire nuovi obiettivi di business, ma allo stesso tempo dare risposte concrete ai propri clienti, che chiedono sia apparati sia servizi di supporto e di gestione.

Che poi questo avvenga sotto forma di classica assistenza o che prenda la forma di un servizio di gestione via cloud dipende dal contesto e dalla propensione del cliente a esternalizzare la propria infrastruttura IT e di comunicazione, che sia realizzata tramite smartphone o dispositivi mobili di altra natura.

Il settore è molto interessante e con buone prospettive per vari motivi. Uno è che non sempre è percepita l'insicurezza di un end-point come la si percepisce per il desktop, questo perché molto spesso in un'ottica BYOD si tende a trascurarlo quando si tratta di un dispositivo personale e non aziendale in senso stretto. Il secondo è che nel novero dei dispositivi riferiti come end-point stanno

Servizi di gestione e protezione dei dispositivi mobili rispondono alle esigenze di alta disponibilità, attraverso soluzioni sempre più sofisticate, anche grazie al machine learning



entrando sempre più massicciamente dispositivi intelligenti generalmente annoverati sotto il nome di IoT.

Non ultimo, c'è quanto attinente a dispositivi che sino a ora hanno vissuto di vita propria ma che le attuali tecnologie stanno mettendo in rete, come avviene per esempio per ambienti industriali SCADA nel quadro dell'evoluzione riferita come Industry 4.0.

Questi fattori e altri stanno portando a una forte crescita del mercato volto a garantire la sicurezza dell'end-point in generale, un mercato che richiede risposte anche puntuali in funzione del settore e delle caratteristiche di utilizzo, e quindi non solo prodotti ma anche capacità e competenze

progettuali e di integrazione.

Naturalmente un mercato esigente fa sì che sia di interesse per le aziende del settore e le risposte non hanno tardato ad apparire, sia come soluzioni ex-novo, come per esempio nel settore dell'IoT, che come evoluzione di un già consolidato portfolio di offerta, o come sviluppo nell'ambito di una roadmap volta a fornire soluzioni che siano praticabili sia on-premise che tramite cloud, e quindi aperte alla fornitura da parte del canale di servizi a forte valore aggiunto. ❖

Il machine learning di CyberArk protegge gli utenti privilegiati

di **Giuseppe Saccardi**

Con il diffondersi della mobilità e con aziende che sono sempre più virtuali, si è andato enfatizzando il problema degli utenti privilegiati e come garantirne la sicurezza. Si tratta di

utenti, della fascia dei manager, che richiedono una protezione ad alto livello a causa dei dati riservati di cui sono sovente in possesso, sia quando operano dal loro ufficio sia quando si trovano all'esterno e accedono alle applicazioni e ai dati mediante dispositivi mobili.

Una risposta che si è focalizzata proprio sulla protezione degli utenti privilegiati e delle loro credenziali l'ha resa disponibile CyberArk tramite la soluzione CyberArk Privileged Account Security Solution V10 (CyberArk V10), una piattaforma di sicurezza scalabile come funzionalità che protegge da exploit critici gli account privilegiati ovunque si trovino, sia quando utilizzano infrastrutture ICT on-premise che quando accedono ad applicazioni e dati tramite ambienti cloud ibrido o attraverso workflow DevOps.

Due i punti su cui CyberArk si è concentrata. Il primo è volto a prevenire l'attacco ad account privilegiati sugli End-point, visto che costituiscono uno dei punti maggiormente critici

Analitiche basate su cloud disponibili su AWS, Azure e Google, risk analysis e machine learning proteggono gli end-point e le credenziali dei privileged account



Udi Mokady, Co-Founder,
Chairman & CEO di CyberArk

per la sicurezza. Per eliminare il rischio connesso alla perdita di dati o credenziali, CyberArk ha sviluppato CyberArk Endpoint Privilege Manager, una soluzione che ha il compito di bloccare e contenere

attacchi dannosi proteggendo l'end-point da exploit che mirano a carpire le credenziali privilegiate.

In pratica, tramite le funzionalità contenute di Risk Analysis si ha la possibilità, mediante funzioni di machine learning e analitiche basate su cloud, di aiutare a bloccare gli attaccanti e impedire, rilevando le applicazioni potenzialmente dannose e in grado di accedere a dati e informazioni sensibili, che questi possano posizionarsi in un end-point.

Il secondo è mirato a migliorare la sicurezza nel cloud. Per farlo la V10 ha esteso il supporto per Amazon Web Services (AWS), e automatizzato il

caricamento delle credenziali tramite l'integrazione con CloudWatch e Auto Scaling. In pratica, ne è risultato ridotto significativamente il rischio di credenziali non gestite in ambienti di elastic computing e il team dedicato alla sicurezza ha la possibilità di ridurre sensibilmente il tempo che vi deve dedicare in modo da potersi meglio focalizzare sulla mitigazione dei potenziali rischi.

Peraltro, CyberArk garantisce anche la sicurezza delle credenziali attraverso piattaforme cloud pubbliche quali AWS, Microsoft Azure e Google Cloud Platform (GCP) ed ha validato la sua capacità di attivare la sicurezza per account privilegiati su AWS in un massimo di 15 minuti.

La risposta data alle esigenze del mercato Enterprise sono alla base della forte crescita di CyberArk che, ha evidenziato Udi Mokady, suo Co-Founder, Chairman & CEO, ha a portfolio oltre 3650 clienti, compresi tra questi quasi il 30% dei Global 2000, a cui fa fronte con 1015 dipendenti, oltre ai partner commerciali e di canale.



End-point sicuri con il cloud e l'analisi comportamentale

di **Giuseppe Saccardi**

Sempre più necessarie le tecnologie di prevenzione che sfruttano informazioni collettive e si appoggiano al cloud per aggiungere intelligenza



Un approccio alla sicurezza dell'end-point come evoluzione di una soluzione di sicurezza già consolidata è per esempio quella che è stata messa a punto da F-Secure, che di recente ha annunciato il potenziamento della sua suite Protection Service for Business basata su cloud. La nuova versione è stata sviluppata per migliorare la propria tecnologia di protezione degli end-point aggiungendovi capacità di blocco comportamentale per Windows e Mac in modo da proteggere contro le minacce usate dagli attaccanti.

È una soluzione che ingloba la tecnologia XFENCE, che l'azienda ha annunciato lo scorso Aprile, e che ora ha integrato in Computer Protection for Macs. In pratica, e ai fini dell'interesse degli utenti finali, F-Secure XFENCE evita che processi e applicazioni abbiano accesso ai file, ai dati, a microfoni, tastiere e webcam senza il permesso dell'utente. Funzionalmente

si comporta come un firewall per file evitando, per esempio, che il ransomware crittografi file sui dispositivi infettati, un rischio sempre pendente e forte nel caso di end-point mobili che utilizzano per accedere a dati o la rete web o reti di terze che possono essere poco controllate, o perlomeno non esserlo quanto quelle aziendali. Nel portfolio F-Secure la soluzione cloud-based citata si affianca peraltro a Business Suite, che fornisce una sicurezza on-premise anch'essa erogante capacità di protezione basate sul comportamento.

A Protection Service for Business, per esempio, è stato poi aggiunto DataGuard, una funzione che fornisce un livello ulteriore di protezione contro minacce come il già citato ransomware; una nuova funzione di protezione delle password che rende semplice usare password forti e univoche per le organizzazioni; e un'architettura software migliorata che permette di sviluppare e implementare nuove funzionalità.

L'approccio alla cyber security adottato da F-Secure è paradigmatico di un'altra evoluzione nel settore della sicurezza, quella centrata sull'analisi

GDPR e risk management

Le recenti sfide informatiche e le normative alle porte hanno reso improcrastinabile un radicale cambiamento di paradigma per le politiche di sicurezza IT. La sicurezza, intesa come best practice e tutela integrata degli asset aziendali, va considerata quale parte integrante del risk management e quindi deve permeare i processi produttivi di qualsiasi organizzazione. Ciò non solo per adeguarsi al GDPR ma soprattutto per proteggersi efficacemente contro le perdite economiche conseguenti a un incidente informatico, contro l'impatto economico delle sanzioni previste e l'impatto reputazionale in presenza di un furto di dati. Quello della sicurezza è però un impegno a largo spettro. Una risposta olistica che la vede come un processo e non un mero prodotto è stata ideata da G Data con lo sviluppo di soluzioni che consentono di implementare una buona strategia di sicurezza, con la garanzia di avvalersi di strumenti conformi ai dettami del nuovo regolamento e in grado di proteggere in modo proattivo l'infrastruttura IT dalle eventuali minacce.

Per aiutare le aziende a valutare le vulnerabilità delle infrastrutture, G Data ha nello specifico sviluppato il servizio G Data Advanced Analytics, che sarà disponibile progressivamente a partire dal secondo trimestre 2018.

Ma c'è un altro problema che va affrontato: quello del rischio. Con l'introduzione del GDPR le aziende devono preoccuparsi più che in precedenza del rischio di furto di dati sensibili e della vulnerabilità dell'infrastruttura di operatori a cui hanno commissionato servizi che richiedono la condivisione dei propri dati riservati. Ai rischi legati alla propria sicurezza concorre anche l'intrinseca debolezza dei processi legati al trattamento dei dati rispetto alle esigenze normative.

Dalla collaborazione tra G Data, Reale Mutua e il broker Margas, è così derivata la soluzione Insurtech, denominata Privacy & Cyber Risk, che integra le tecnologie di sicurezza G Data con una polizza assicurativa per la Responsabilità Civile dedicata alle PMI, in modo che queste possano intraprendere più tranquillamente il percorso verso la compliance normativa.

La polizza non sostituisce una corretta Data Governance, avvisa G Data, ma sostiene finanziariamente i fruitori delle proprie soluzioni in caso di leakage, trasmissione di ransomware e pubblicazione di informazioni lesive della reputazione e della privacy di terzi, come conseguenza di un incidente informatico.

comportamentale e sull'intelligenza artificiale, cosa che le è valsa da Gartner il posizionamento tra i Visionary nel Magic Quadrant 2018 per le Piattaforme di Protezione End-point.

La sicurezza e la criticità del cloud e degli ambienti ibridi

Uno degli aspetti critici nella sicurezza degli end-point è il fattore tempo e cioè l'intervallo temporale intercorrente tra il rilevamento di un nuovo tipo di attacco e il momento in cui le patch sono disponibili.

È un problema che risulta enfatizzato quando l'end-point opera tramite reti terze o quando si collega raramente alla rete aziendale perché in questo lasso di tempo può risultare non protetto.

In pratica, la combinazione di ambienti IT caratterizzati da una forte presenza di dispositivi mobili che si collegano alle applicazioni business tramite infrastrutture cloud ibride e multi-cloud apre la strada a problematiche connesse allo stato di aggiornamento

delle infrastrutture di terzi che si interpongono tra il dispositivo end user e il data center o i data center dove risiedono dati e applicazioni.

In sostanza, può avvenire che per mettersi al passo con la sofisticatezza degli attacchi e delle capacità elaborative e di analisi richieste si renda necessario da parte dei provider l'apportare modifiche significative alla infrastruttura che data la scala di intervento richiesta possono finire con il ritardare l'entrata in funzione delle contromisure di sicurezza.

Anche in questo caso un aiuto, come ha fatto Forcepoint, può venire dall'analisi comportamentale estesa a livello di end-point.

In particolare, la vision strategica che l'ha guidata negli sviluppi è consistita



nel rendere disponibili funzionalità basate sull'analisi del comportamento e sull'analisi predittiva, volte a rafforzare le policy di sicurezza per quanto concerne lo scambio dei dati tra ambiente informatico legacy da e verso il cloud esterno, come per esempio nel caso delle banche i cui dipendenti utilizzano Microsoft Office 365, la sicurezza su Web e quella della posta elettronica.

L'assunto di base di Forcepoint è stato in sostanza che approcciare la security attraverso un filtro human-centric aiuta le organizzazioni a comprendere meglio gli indicatori del normale comportamento informatico e a identificare rapidamente attività e operazioni, quali la shadow IT, che rappresentano i maggiori rischi. ❖



Vecchie e nuove minacce mettono a rischio aziende e governi

di **Gaetano Di Blasio**

Il 2018 appena iniziato vedrà crescere ancora la pressione del cybercrime, con vecchie e nuove minacce, oltre quelle "reingegnerizzate". Gli oltre duemila ricercatori di Trend Micro hanno stilato le previsioni sulla sicurezza, che vede sempre più strumenti automatici sofisticati utilizzare tecnologie all'avanguardia, come il machine learning e la blockchain, per eludere i controlli e sfruttare ogni vulnerabilità. Queste ultime sono i "buchi" del software che andrebbero "rattoppati" con le operazioni dette di patch management, sulle quali punta il dito Gastone Nencini, country manager di Trend Micro Italia: «Molti attacchi, che sono stati devastanti nel 2017, hanno sfruttato vulnerabilità conosciute e le loro conseguenze si sarebbero potute evitare se i sistemi fossero stati aggiornati preventivamente. Per questo patch management e formazione dei dipendenti devono diventare una priorità».

Per questo ma non solo, aggiunge il manager, spiegando: «Abilità e risorse sono i due elementi che costituiscono l'arsenale di un aggressore che, tuttavia, non è in grado di violare

la sicurezza o addirittura eseguire attacchi sofisticati senza aver prima individuato i punti deboli di un sistema. Attacchi malware massivi, furti tramite email, dispositivi compromessi e servizi interrotti richiedono tutti una vulnerabilità nella rete, sotto forma di tecnologia o persona, per poter essere attivati.

Il GDPR (General Data Protection Regulation) sarà certamente un'occasione per spingere le imprese a investire nella sicurezza, ma per assurdo, teme Nencini, rappresenta un'opportunità per i cyber criminali, che potrebbero fissare il costo del riscatto, nel caso dei ransomware, basandosi sulle sanzioni previste dal regolamento europeo cui bisogna essere conformi dal 25 maggio prossimo.

Gli importi dei riscatti saranno sempre più ingenti, perché cresceranno gli attacchi di questo tipo mirati ad alcune imprese e preceduti da una fase di analisi e raccolta dati per "tarare" le richieste. La superficie di attacco, inoltre, cresce, rimarca ancora il manager italiano,

Le analisi di Trend Micro sulla cyber security nel 2018 preannunciano il dilagare degli attacchi informatici, con nuove forme di ricatto e la crescita di "servizi" per campagne di propaganda

perché alle tecnologie informatiche si sommano le tecnologie operative, cioè quelle tipiche di ciascun settore, finora ritenute sicure in quanto isolate nelle fabbriche o in varie strutture, ma oggi sempre più connesse e quindi a rischio. In generale una connettività sempre maggiore porterà nuove opportunità ai cybercriminali per penetrare nelle reti aziendali.

Ci sono già stati attacchi di Denial of Service (cioè servizi Internet bloccati) che hanno sfruttato infrastrutture preposte ad altro, come le videocamere per la sorveglianza usate per trasmettere dati in massa, saturando la rete e causando danni da centinaia di milioni di dollari alle imprese dell'e-commerce.



Gastone Nencini, country manager di Trend Micro Italia

9 miliardi di dollari sfumati per le "Business Email Compromise"

Attenzione particolare, Nencini la dedica agli attacchi BEC (Business Email Compromise), che purtroppo hanno ottenuto molti successi. Si tratta delle false email, confezionate con cura e spesso precedute da un'accurata fase di raccolta dati per colpire al momento giusto. Tipico è il caso della falsa email spedita dal Ceo al Cfo con una richiesta di effettuare un bonifico urgente. Qui la sicurezza è una questione di processi e di cultura aziendale. Esistono anche attacchi Business Process Compromise, che cercano di sfruttare appunto i processi, in genere del reparto finanziario, modificandoli, possibilmente tramite le vulnerabilità della supply chain (la catena di fornitura). Sono stati devastanti per Target nel 2014, ma richiedono una pianificazione a lungo termine e maggiore lavoro e in Trend Micro ritengono meno probabile che questi attacchi emergeranno nel 2018, mentre valutano che le perdite globali generate dalle truffe Business Email Compromise supereranno i 9 miliardi di dollari, dopo aver raggiunto nel 2017 i 5 miliardi.

La cyber propaganda e le fake news

In Italia si vota il 4 marzo, ma nel 2018 ci sono elezioni in diverse nazioni, compresi gli Stati Uniti: un'opportunità

di mercato per i "servizi" di cyber propaganda, le cui campagne saranno perfezionate utilizzando tecniche già sperimentate con successo in precedenza. In effetti, sembra che nel dark bleu siano disponibili pacchetti di cyber propaganda as a service.

Il triangolo delle fake news consiste in motivazioni su cui si basa la propaganda, i social network che servono come piattaforma per il messaggio e gli strumenti e servizi che sono impiegati per spedire il messaggio stesso. «Nel 2018 – spiega Nencini – ci aspettiamo che la cyberpropaganda si veicoli attraverso tecniche familiari, come quelle utilizzate nel passato per diffondere lo spam tramite e-mail e il Web».

Il manager aggiunge: «Kit software fai da te, per esempio, possono eseguire spam automatizzato sui social media. Anche l'ottimizzazione del motore di ricerca Black Hat è stato adattato per l'ottimizzazione dei social media, con una base utenti di centinaia di migliaia, in grado di fornire traffico e numeri a diverse piattaforme. Dalle e-mail spear phishing inviate ai ministeri degli Esteri all'uso plateale di documenti per screditare le autorità, al contenuto dubbio che può diffondersi liberamente e scatenare opinioni violente o addirittura proteste reali».

Azioni per la sicurezza

Dato lo scenario, gli esperti di Trend Micro suggeriscono di adottare soluzioni di cyber security per una protezione multilivello, in modo da ridurre al minimo i rischi di compromettere ogni ambito aziendale. Occorre, per questo, una visibilità su tutti i livelli, con strumenti che possano fornire rilevamento real time e protezione contro vulnerabilità e attacchi.

«Qualsiasi potenziale intrusione e compromissione degli asset verrà evitata grazie a una strategia di protezione dinamica che utilizza tecniche transgenerazionali adeguate alle varie minacce», afferma Nencini, che conclude: «È fondamentale seguire pratiche di comportamento adeguato alla sicurezza, come modificare le password predefinite, utilizzandone di complesse e uniche per i dispositivi smart, specialmente per i router; implementare la crittografia in modo da prevenire il monitoraggio e l'utilizzo dei dati non autorizzati; applicare puntualmente le patch, aggiornare il firmware alla sua versione più recente; evitare il social engineering prestando attenzione alle email ricevute e ai siti visitati in quanto potrebbero essere usati per spam, phishing, malware e attacchi mirati».



L'automazione della network security

di Gaetano Di Blasio

Dallo sniffing all'artificial intelligence: la ricerca di una rete impenetrabile e sempre più affidabile



È il caso di ricordare che la sicurezza assoluta non esiste, ma bisogna ammettere che molte delle novità su cui stanno lavorando le principali società del settore, sembrano preparare un futuro molto meno rischioso. L'ultima frontiera si basa su machine learning e intelligenza artificiale, utilizzate per rendere automatici gli interventi di protezione sulla rete. L'obiettivo è quello di rendere capaci le reti e i sistemi informatici di "aggiustarsi" da soli e di identificare i tentati di attacco prima che possano fare danni.

Più che un obiettivo sembra una chimera a tutti coloro che negli anni hanno visto i black hat vincere quasi tutte le battaglie.

Prima di farsi troppe illusioni, pensando o sperando di poter, alla fine, vincere la guerra, si deve comunque considerare che le organizzazioni cyber criminali hanno accesso alle tecnologie avanzate, spesso in anticipo: parafrasando un vecchio detto si potrebbe credere che "prima che sia fatta la nuova protezione, è già pronto un nuovo inganno". La corsa a chi realizza gli algoritmi più efficaci è già partita.

Altra nota dolente, è bene evidenziarla, riguarda il punto debole della catena, che resta l'utente finale, cui

manca una cultura sulla cyber security profonda quanto basta per evitare di compromettere le proprie credenziali, lasciandosele rubare.

Anche su questo si può lavorare, non solo sulla formazione, ma anche sul fronte della behavioral analysis. L'analisi comportamentale è fondamentale per individuare le anomalie nell'uso della rete da parte di chi ha rubato credenziali e sta svolgendo attività non coerenti con quelle solitamente svolte dal "titolare" dell'account.

Accontentati i "soliti brontoloni", lasciamo da parte i brutti presagi, perché la maggioranza delle imprese interpellate da Cisco per comporre il "Cisco 2018 Security benchmark study" sono molto fiduciose negli sviluppi di automazione, machine learning e artificial intelligence. Più precisamente, all'automation non crede affatto l'1% degli intervistati e un ulteriore 16% è scettico, mentre il 44% è positivista e il 38% completamente convinto.

Peraltro, non si tratta di fiducia, ma di ultima speranza: non ci sono alternative all'automazione della sicurezza, perché solo con gli automatismi si può mitigare l'effetto dell'errore umano.

Con il machine learning si progettano le reti che ottimizzano le prestazioni in funzione delle esigenze in tempo reale e si proteggono da sole



Le Intent based network

L'instradamento e il controllo della rete costituiscono attività critiche da sempre e da diversi anni si è cercato di automatizzarle. Inizialmente l'intenzione era soprattutto ottimizzare le prestazioni, ma ben presto, in parallelo, è cresciuta anche l'esigenza di protezione.

Concentrandoci su questo aspetto è facile comprendere le difficoltà iniziali nella gestione di log infiniti. L'intrusion detection e la successiva intrusion prevention si sono basate su motori di



correlazione che fornivano e, in molte installazioni, tuttora forniscono una sintesi dello stato infrastrutturale, utile a prendere decisioni.

Questi strumenti sono diventati sempre più sofisticati, con SIEM (Security Information Event Manager) che integrano sistemi di analytics per gestire big data e aumentare il grado di accuratezza.

Lo sviluppo delle software defined network ha aperto nuove frontiere nella gestione delle reti, alimentando un "desiderio" nella mente del

network manager: definire lo stato operativo ideale della propria rete per gli scopi che vuole realizzare e disporre di un software di orchestrazione automatizzato che implementa le policy necessarie. Sono le fondamenta per le cosiddette Intent based network, dove "intent" è l'intento che ci si prefigge, meglio traducibile come "scopo". Su tali basi è possibile, secondo Andrew Lerner, un ricercatore senior di Gartner, arrivare a realizzare la Intent Based Network Security (IBNS). Lerner sostiene che una IBNS deve

possedere quattro caratteristiche. La prima è la capacità di traduzione e validazione, cioè la capacità di tradurre i comandi degli amministratori di rete in azioni realizzate dal software. In altre parole, i network manager definiscono delle policy di alto livello, in un linguaggio semplice che si potrebbe definire "business": il software deve poter verificare se le suddette policy siano eseguibili.

Seconda caratteristica che una rete basata sullo scopo deve possedere è l'implementazione automatica: una volta che l'amministratore ha definito lo stato di rete desiderato, il software che realizza la IBNS deve poter agire sulle risorse di rete in modo da raggiungere tale stato, garantendo l'enforcement delle policy.

Terzo elemento fondamentale è l'awareness, sostiene Lerner, intendendo una capacità profonda di monitoraggio, che implica la capacità di raccogliere tutti i dati necessari per controllare la persistenza dello stato di rete preferito.

Infine, una IBNS deve possedere il trinomio di capacità: assurance, dynamic optimization e remediation.

In sostanza la capacità di assicurare costantemente lo stato desiderato. Grazie ad algoritmi di machine learning e alle suddette capacità la rete intent based è in grado di mantenere lo stato richiesto attuando le azioni correttive che di volta in volta si ritengono necessarie.

In pratica gli interventi per conservare lo stato ideale della rete sono realizzati automaticamente dal software creato ad hoc per gestire la rete.

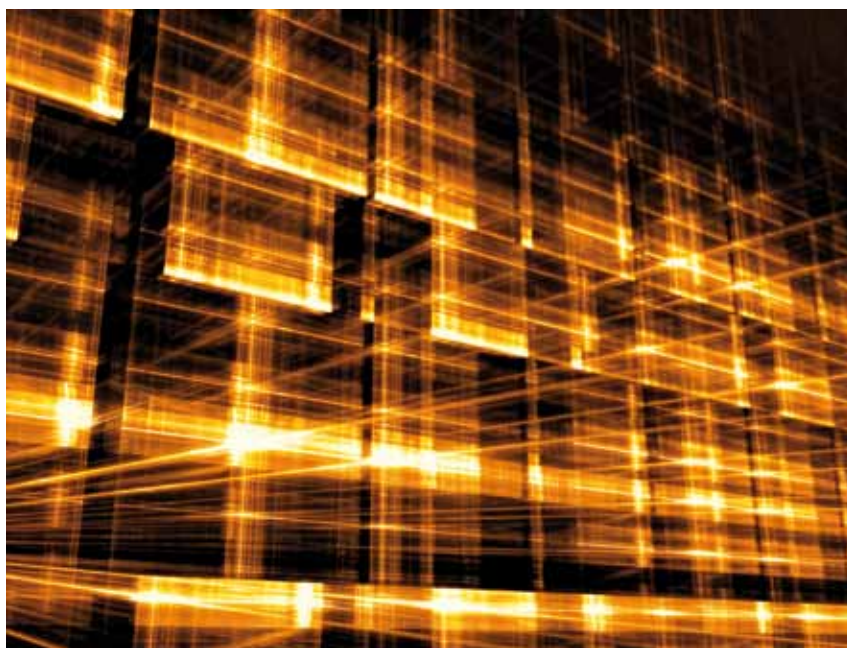
Secondo Lerner ci vorranno ancora un paio d'anni prima che le reti IBN maturino. Almeno fino a quando potranno integrare tutti i controlli e gli strumenti necessari per alimentare i sistemi di intelligenza artificiale e consentire loro di prevenire e rilevare gli attacchi eventuali. Non basta, infatti, notare che un determinato parametro esca dai limiti stabiliti, deve essere possibile capire se si tratta, per esempio, di un picco di traffico lecito che ha bisogno di un aumento temporaneo della banda disponibile oppure di un'azione diversiva, che maschera un assessment per cercare vulnerabilità con un workload pesante. Come pure si deve riuscire a osservare del codice maligno, magari spedito in tranches separate, all'interno di un attacco DDoS, su cui si concentra l'attenzione. La crescita dei flussi di dati criptati, per sacrosante ragioni di sicurezza, rende ulteriormente difficili le analisi del traffico.

Ci sono diversi produttori attivi su più fronti di ricerca, da chi è partito ponendosi come principale obiettivo la gestione automatica della rete, per poi integrare uno strato per la cyber security e chi si è concentrato sull'infrastruttura di sicurezza, che si somma alla rete.

Un ruolo importante lo gioca la virtualizzazione, su cui ovviamente si appoggiano alcuni vendor, che semplifica ed estende le capacità di gestione via software. In particolare, vanno considerati gli sforzi di VmWare, con sua la soluzione per la sicurezza delle reti software defined VmWare NSX, e di Citrix, che ha progettato un modello

architeturale di sicurezza per realizzare il Secure Digital Perimeter.

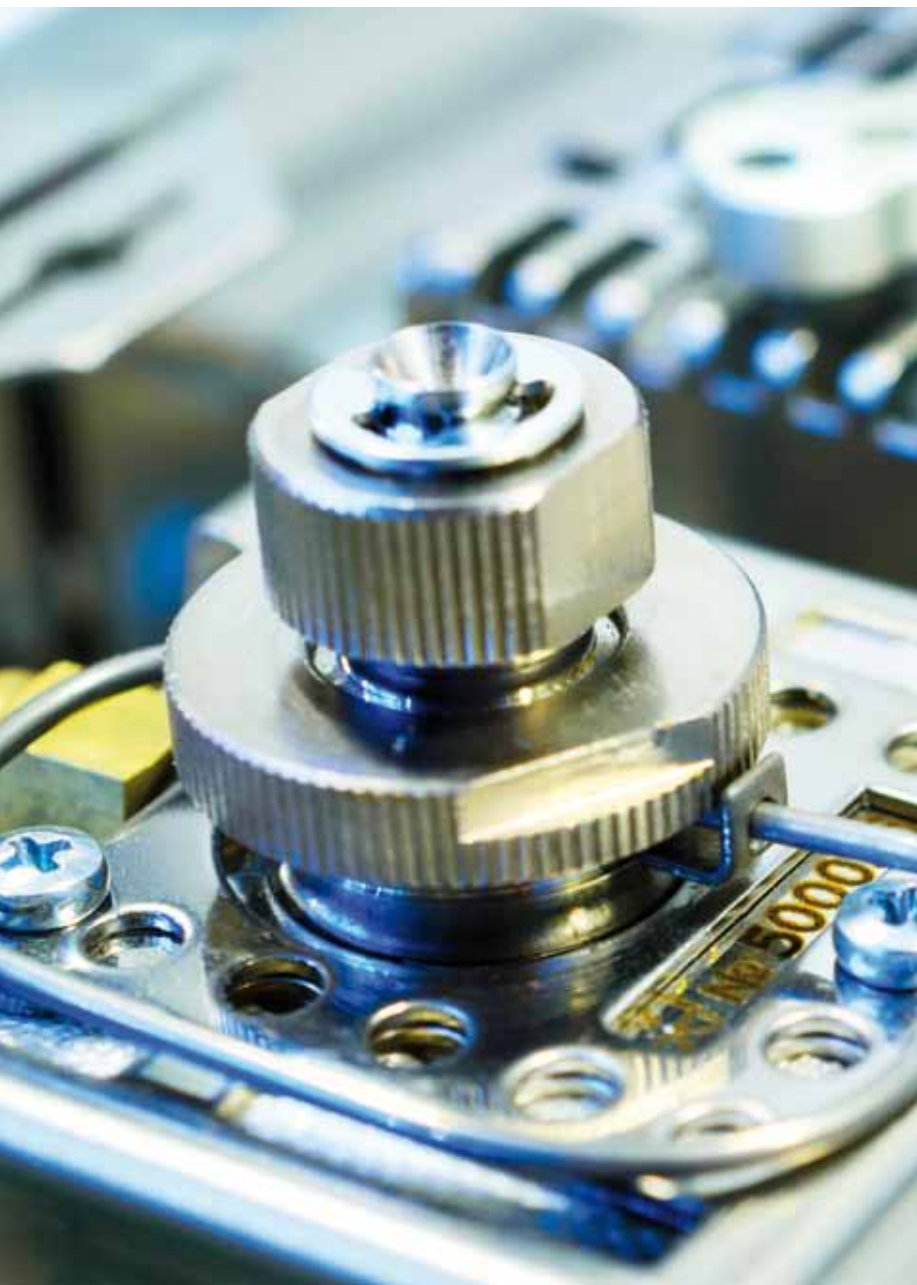
Tra le prime aziende che hanno cominciato a lavorare in questo ambito c'è Juniper Networks, che ha da subito cercato di unire prestazioni e sicurezza nell'automazione della rete. Anche Fortinet può considerarsi tra i pionieri concentrati sul fronte della security. Visto il settore non può mancare Cisco, che è certamente avanti nell'automazione per l'ottimizzazione della rete e sta facendo rapidi passi nell'integrazione della sicurezza, promuovendo, inoltre, la definizione di standard e chiamando a raccolta gli altri attori. ❖



La sicurezza per l'IoT e le infrastrutture critiche

di **Giuseppe Saccardi**

La protezione degli endpoint, come tablet e smartphone, è necessaria per preservare la sicurezza dei dati e delle applicazioni aziendali



Da qualche tempo al novero degli end-point classici quali smartphone, tablet, notebook o più convenzionali desktop si è aggiunto quanto attinente al mondo dello "smart", cioè dell'Industry 4.0 per quanto riguarda la produzione di beni materiali alla digital transformation che dal mondo office classico si è espansa sino a comprendere sempre più massicciamente il mondo dell'industria e dei fornitori di servizi essenziali, dalle reti energetiche agli acquedotti, dalle reti di trasporti su strada o su ferrovia, dal controllo del territorio tramite videocamere di sorveglianza ad alta definizione sino alla illuminazione intelligente che aumenta la sicurezza facendo allo stesso tempo risparmiare sui consumi energetici.

Il fattore comune di tutto questo è che gli oggetti che sostanziano questa trasformazione si basano su tecnologie e dispositivi smart che racchiudono al loro interno capacità elaborativa, di storage, di rete e software applicativo. Purtroppo, va però aggiunto, non sempre tra quest'ultimo annoverano quanto necessario, per non dire indispensabile, per garantire la sicurezza delle informazioni che accumulano e dei dati anche sensibili che inviano in

rete. È un problema grave che operatori di canale e system integrator nonché che eserciscono tali infrastrutture si trovano ad affrontare quando devono fornire e successivamente gestire soluzioni di tal fatta, necessità che ha portato aziende specializzate a espandere il proprio portfolio per la sicurezza in modo da rispondere a esigenze specifiche o normative.

Una sfida per gli operatori di canale

L'IoT e la sua sicurezza rappresenta una nuova e concreta sfida per il canale, oltre che fonte di business, ed è prevedibile che con il suo diffondersi, e i numeri sono da brivido, le richieste di sicurezza da parte delle aziende cresceranno quasi esponenzialmente. I dati parlano da soli. Secondo proiezioni di IDC, la spesa per l'IoT raggiungerà la cifra stratosferica di 1,3 trilioni di dollari entro il 2020, oramai dietro l'angolo, e il 43% dei dati dell'Internet of Things sarà processato a livello periferico delle reti, che dovranno garantire connettività, banda e non ultimo sicurezza. La società di analisi prevede inoltre che il numero di

oggetti connessi raggiungerà, sempre entro il 2020, i 30 miliardi, per salire a 80 miliardi nei successivi 25 anni. Lasciando a una prossima generazione il problema di cosa fare degli altri 50 miliardi di oggetti già quanto previsto per il 2020 pone le basi per notevoli opportunità di crescita per il canale a fronte dei crescenti rischi per la sicurezza e la privacy in cui sicuramente si incorrerà. A tutta prima, saranno gli integratori di rete, i Managed Service Provider e i provider con esperienza nel Software as a Service e nell'hosting che dovrebbero trovarsi nella posizione ideale per cogliere le opportunità create da queste tecnologie e dalle relative problematiche di sicurezza. Infatti, per mantenere i sistemi funzionanti in modo ottimale per i processi decisionali in tempo reale, i dispositivi IoT richiedono monitoraggio remoto e una sicurezza sia logica che fisica, aspetti su cui il canale ha in parte già accumulato una concreta esperienza ma su cui molto deve ancora essere fatto.



Protezione degli end-point e IoT

Sull'importanza della protezione di end-point IoT ha messo in guardia F-Secure, che sul garantirne la protezione ha aperto un nuovo fronte di ricerca e sviluppo e di offerta di soluzioni. L'Internet of Things (IoT) così come la si conosce, ha osservato, apre forti opportunità per quanto concerne la digital transformation e l'evoluzione verso una smart economy ma, di fatto, rappresenta una minaccia considerevole a causa di regolamenti non sempre adeguati sulla sicurezza e sulla privacy.

Milioni di dispositivi end-point installati in modo distribuito sul territorio e connessi in rete fissa o mobile o via Cloud sono già stati compromessi per essere usati come parte della botnet Mirai. E non sono pochi i produttori che immettono prodotti velocemente sul mercato senza prendere in considerazione i requisiti e le impostazioni



minime di sicurezza per questione di costi di produzione e della pressione esercitata dalla concorrenza e dalle esigenze del mercato.

Anche se milioni di nuovi dispositivi si connettono online ogni giorno, gli utenti non sono poi ancora generalmente consapevoli che i loro nuovi apparati "intelligenti" andranno online. Per esempio, già oggi è in effetti difficile trovare un modello di un qualsiasi dispositivo, come un comune apparato televisivo, che non supporti la connessione a Internet e l'WiFi e che in quanto tale non possa essere soggetto ad attacchi di hacker e la cui videocamera per i modelli che ne sono dotati non possa essere usata per spiare l'ambiente in cui si trova. La realtà, evidenzia F-Secure, è che in breve tempo miliardi di dispositivi saranno potenziali punti di attacco alla sicurezza e le aziende sembrano ignorare il problema, e sino a che gli

utenti non inizieranno a chiedere che questi dispositivi siano anche sicuri i produttori difficilmente considereranno la sicurezza come una priorità. Se F-Secure è attivamente impegna-

ta nel garantire la sicurezza degli endpoint, quello che serve, evidenzia, è che la loro parte devono farla anche i governi e gli enti di certificazione dei prodotti business e consumer, che devono preoccuparsi della qualità della tecnologia che viene messa nelle mani e nelle case degli utenti.

Sicurezza e Industry 4.0: servono dispositivi ad hoc

Il mondo industriale e in particolare l'Industry 4.0 è sempre più sotto attacco e il susseguirsi di cyber attacchi nell'ultimo anno ha portato all'attenzione il fatto che un semplice incidente informatico può avere conseguenze catastrofiche, dall'interruzione della produzione alla chiusura di interi siti produttivi, dalla perdita di dati aziendali critici al danneggiamento della reputazione di un brand.

È però assolutamente illusorio, mette in guardia Stormshield Italia, pensare

che i cyber attacchi possano essere fermati del tutto. Le aziende devono quindi rinunciare al ruolo di spettatore passivo e avviare piani per proteggere l'azienda con soluzioni adeguate, anche se questo ha di certo un costo, che però non può continuare a essere visto in modo negativo ma considerato un investimento, peraltro indispensabile e che in pratica assume il ruolo di una vera e propria polizza assicurativa.

Il problema della sicurezza permea profondamente il settore industriale. Nonostante il crescente interesse per un'Industry 4.0, in Italia il settore manifatturiero sembra ancora focalizzarsi primariamente su esigenze business quali la remotizzazione delle operazioni e del monitoraggio di sistemi esistenti, più che trasformarsi in industria di nuova generazione, e mettere in secondo piano valutazioni concernenti i rischi connessi a questa innovazione strategica.

Ne è la riprova un test condotto nel 2016 che ha rivelato che oltre 13.000 sistemi SCADA esposti su internet erano senza alcun controllo. A fronte del tipico ciclo di vita di un impianto,

è un dato che nel 2017 non dovrebbe aver subito grandi variazioni.

Il problema è dovuto in buona parte al fatto che i firewall tradizionalmente specializzati nella prevenzione di incidenti informatici in una rete aziendale non sono in grado di interpretare i protocolli SCADA, né di individuare un eventuale traffico malevolo o non autorizzato su tali protocolli, dando luogo a un quadro allarmante come quello evidenziato, ma evitabile con soluzioni di sicurezza adeguate.

Per affiancarsi e supportare tramite il canale il mondo industriale nell'affrontare in modo sicuro il processo della digital transformation e le problematiche poste dalla crescente interazione tra OT (tecnologia operativa tradizionale) e l'IT (infrastruttura informatica), Stormshield ha per esempio sviluppato un portafoglio di soluzioni che affronta la cyber security su più livelli e ambiti aziendali e con partnership con aziende specializzate nello sviluppo e nella progettazione di soluzioni per ambienti industriali che hanno portato anche alla progettazione di dispositivi ad hoc.

Mettere al sicuro Infrastrutture critiche, SCADA e IoT

L'accennato diffondersi della trasformazione digitale, l'evoluzione verso l'Industry 4.0 e la accennata realizzazione di infrastrutture e servizi pubblici a forte automazione, sta ponendo

all'attenzione di manager e autorità pubbliche il problema di come proteggere adeguatamente infrastrutture, fabbriche e servizi, che per loro natura devono essere sempre operativi e a prova di attacchi cibernetici.

Se realizzare soluzioni di protezione per l'end user, il suo pc, lo smartphone o il tablet, è relativamente semplice e le soluzioni sul mercato di certo non mancano, ben diverso si presenta il problema quando si tratta di garantire la sicurezza di impianti e servizi pubblici primari perché, mette in guardia Selta, azienda italiana specializzata nello sviluppo di soluzioni per infrastrutture critiche, questo richiede una forte esperienza impiantistica nel settore e nei relativi standard, dallo SCADA all'IoT, nonché dei dispositivi connessi.

Uno dei settori su cui si sono concentrati gli sviluppi della società è quello dell'IoT e delle soluzioni SCADA, alla base dell'Industry 4.0. La interconnessione in rete di apparati e impianti industriali e la diffusione di dispositivi IoT, se migliora produzione e time to market, osserva la società, apre però la strada ad attacchi potenzialmente disastrosi. Basandosi sull'esperienza acquisita negli anni nel settore industriale, Selta ha sviluppato soluzioni e servizi specifici per la protezione ad alto livello di ambienti SCADA, in

modo da garantirne non solo la protezione ma anche la business continuity e il disaster recovery.

L'approccio alla Cyber Security si articola, nella strategia di Selta, in due direzioni complementari: lo sviluppo di soluzioni e la fornitura di servizi di sicurezza.

La tecnologia, ritiene Selta e non è difficile essere d'accordo, da sola però non basta e in certi casi non è nemmeno il problema principale da affrontare, che il più delle volte finisce con l'essere è costituito da chi la organizza e gestisce, l'uomo.

L'assunto è semplice. Gli attacchi avvengono perché all'interno delle aziende ci sono uomini. Quindi si deve partire da una grande campagna di informazione e sensibilizzazione, oltre che dalla definizione di architetture segmentabili in modo che l'attacco possa essere individuato prima che si diffonda. Resta fondamentale comunque partire dalla strategia e dalla formazione delle persone, dopo e solo dopo intervengono le macchine e l'infrastruttura tecnologica. Anche questo è un compito in cui il canale ha un preciso compito da svolgere. ❖

La protezione fisica di ambienti Smart

di **Giuseppe Saccardi**

Proteggere gli ambienti e le persone è indispensabile quanto proteggere dati e applicazioni. Individuare un'intrusione e intervenire prontamente sono azioni fondamentali per la sicurezza ma non sempre facili da gestire



La crescente e comprensibile attenzione per l'entrata in vigore del GDPR e il come risultare compliant rischia di mettere in sordina quello che è il complementare della sicurezza logica e cioè la sicurezza fisica, intendendo con essa la sicurezza sia di persone e beni materiali, come per esempio gli ambienti di lavoro, apparati, data center e in generale quanto costituisce un asset materiale per un'azienda che può essere asportato o danneggiato.

Proteggere il business non è un qualcosa che deve limitarsi ai dati e al loro uso fraudolento da parte di hacker, ma vuol dire anche e in primis proteggere l'ambiente fisico in cui questi dati sono custoditi o fruiti, si tratti dell'ufficio o dell'ambiente domestico dove si lavora in smart working. La Sicurezza con la S maiuscola dovrebbe quindi partire dalle persone e dalle cose perché sono loro, e specialmente le prime, che costituiscono il vero asset strategico di un'azienda e come tale vanno adeguatamente protette.

Garantire condizioni ambientali adatte e sicure è un compito però non sempre facile e presenta diversi aspetti da affrontare e considerazioni da fare, a partire dalla distinzione di cosa si intende per sicurezza fisica, perché una cosa è parlare di infrastrutture che permettono di rilevare quando vi è in atto un tentativo da parte di malintenzionati di introdursi in una abitazione, ufficio o stabilimento produttivo per trafugare beni o recare danni materiali che possono anche essere molto onerosi, un'altra è parlare di soluzioni che devono permettere un rapido intervento del personale preposto privato o pubblico, per far sì che il tentativo non possa essere portato a termine con successo.

Rilevare un'intrusione non basta

Rilevazione di un'effrazione e prevenzione degli effetti sono due sono piani del tutto diversi e richiedono tecnologie, soluzioni e approccio progettuale diverso, così come diverse sono le soluzioni atte a scoraggiare atti di questo genere.

Nel primo rientrano soluzioni come sensori, rilevatori, videocontrollo, telecamere ad alta definizione e in definitiva tutto quanto permetta di rilevare che è in atto un tentativo di effrazione. Il secondo comprende soluzioni che da una parte devono allertare, tramite sistemi sicuri che non possono esser



manomessi preventivamente fuori servizio siano essi fissi o mobili, i gestori della sicurezza in modo che possano prendere le decisioni operative più opportune in base a specifici protocolli di intervento e al livello di importanza dell'area in cui è in corso un tentativo di effrazione.

Complementare a questo però devono essere disponibili barriere fisiche (vetrate o porte antisfondamento, o altri sistemi atti a ritardare l'effrazione fisica in un'area protetta) in grado di trattenere l'attaccante fisico per il tempo necessario agli addetti alla sicurezza di intervenire sul luogo e bloccare il tentativo.

L'offerta sul mercato di soluzioni che rientrano in uno o nell'altro dei campi sopra esposti è ampia ma non sempre le due cose coincidono e sono presenti nel portfolio di prodotti e

servizi della medesima azienda.

Va considerato che la sicurezza fisica richiede approcci molto specializzati e chi ha esperienza nel produrre soluzioni come le videocamere ad elevata risoluzione, brandeggiabili e con capacità di visione notturna, non necessariamente ha anche la capacità di sviluppare soluzioni fisiche antieffrazione, o software di gestione in rete, o dell'insieme di oggettistica IoT di apparati intelligenti di rilevamento delle condizioni e di controllo dell'ambiente fisico, o di soluzioni per il controllo dell'accesso a sale riservate, eccetera.

Stabilire cosa fare e come

I modi per proteggere ambienti riservati, siano essi domestici o aziendali o pubblici nel caso di aree quali parchi, giardini, strade o uffici aperti al pubblico, sono compiti non semplici. Questo sia per l'estensione delle aree che per la diversità di oggetti e numero di zone o microzone che comprendono. Ad esempio, una stanza può

comprendere una o più porte, porta, una o più finestre e se si vuole avere una segnalazione puntuale ognuna di queste deve poter essere trattata individualmente, cosa che richiede un dispositivo specifico, una segnalazione che permetta di individuare esattamente da dove un allarme è partito, eccetera. E a fronte di questo una diversa strategia di intervento, Qualunque sia l'ambiente da proteggere, il primo passo da compiere, suggeriscono gli esperti del settore, è una adeguata analisi del rischio, analisi che deve stabilire una priorità dei beni materiali, degli ambienti e delle persone da proteggere, come rilevare e segnalare quando qualcosa non va e come fare e cosa installare per far sì che la protezione fisica regga sino all'intervento risolutore. In sostanza, prima di porre mano al progetto fisico dell'infrastruttura di sicurezza si deve procedere alla analisi globale del rischio e agli obiettivi che ci si prefigge di raggiungere.

Partire con l'analisi del rischio

L'analisi del rischio è il punto chiave di una soluzione di sicurezza fisica ma non è una fase di un progetto che può essere condotto in autonomia dalla società partner nella sicurezza. Oltre che essere accurato richiede che lavorino spalla a spalla sia gli esperti del settore che i responsabili del cliente, che alla fin fine è l'unico che può dare una valutazione oggettiva del valore dei beni e delle persone da proteggere fondato sul rischio che questi, in base alle funzioni e alle mansioni aziendali, possono correre. È nel corso dell'analisi del rischio che si può fare la iniziale distinzione tra i beni immateriali come i dati e quelli materiali. I parametri da considerare sono

svariati, ad esempio se si tratta di un edificio in cui circolano solo persone interne o anche esterne, se è un edificio aperto al pubblico o è un building privato, eccetera.

C'è poi da considerare una questione di fondo. Sovente si è portati a pensare che un sistema antifurto sia atto ad evitare il furto stesso. Non è così o perlomeno non lo è se il tutto non è inserito in un approccio sistemistico corretto. Il sistema antintrusione avvisa che c'è un intruso, poi che il furto venga evitato è tutta un'altra questione e questo non sempre viene ben spiegato ma è fondamentale.

Da qui emerge l'importanza di un efficace servizio di analisi che preveda che obiettivo ci si pone, con un approccio che permetta di creare una infrastruttura che segnali l'intrusione e che allo stesso tempo resista per il tempo necessario a permettere l'intervento della Sicurezza. Naturalmente quello che vale per beni materiali vale a maggior ragione per la protezione delle persone fisiche. Se nel processo di raccolta delle informazioni, dell'analisi del rischio e della determinazione degli obiettivi manca qualcosa il sistema potrebbe, e a ragione, non funzionare.



La sicurezza dell'ambiente business e home diventa smart

Il benessere e la sicurezza dell'ambiente di lavoro in tutte le sue forme, compreso quello domestico vista la diffusione e l'interesse crescente per lo smart e l'home working, si sta imponendo all'attenzione di aziende e professionisti. Va osservato che sul mercato sono disponibili soluzioni atte a soddisfare praticamente tutte le esigenze che possono insorgere così come una rete di distributori e di installatori certificati in grado di tradurre le soluzioni in progetti concreti. Un esempio di azienda attiva nel garantire la sicurezza di ambienti Smart è CTS tramite il suo marchio SiMPNiC, società che ha tra i suoi i partner ingegneristici e distributori nazionali CIE Telematica, azienda italiana che opera da oltre vent'anni nel settore delle soluzioni e infrastrutture di rete di accesso fisse e mobili e del controllo del territorio.

La linea di prodotti dedicata al benessere ambientale e alla sua sicurezza che ha a portfolio comprende una ampia gamma di soluzioni IoT (rilevatori, sensori, attuatori, eccetera) atte a migliorare sia il comfort che la sicurezza e a rendere smart e controllabile via rete e smartphone l'ambiente in cui si vive o si opera professionalmente. La gamma di apparati e dispositivi IoT intelligenti comprende inoltre CPE

per collegamenti su reti fisse e wireless, videocamere di controllo, smart plug con diverse tipologie di presa e gateway per videocamere. Distribuiti per l'ambiente domestico o di smart working permettono di tenerlo sotto controllo, così come di controllare lo stato di accensione o di spegnimento di apparati elettronici, con il tutto che può esser gestito tramite gateway da remoto e la possibilità di ricevere

remotamente e tramite dispositivi mobili segnalazioni sul verificarsi di eventi fuori dall'usuale o potenzialmente pericolosi (ad esempio fughe di gas, effrazioni, eccetera).

Un ruolo chiave nell'erogazione del servizio di gestione lo assumono gli iCPE, che sono dei gateway IoT multiservizio che operano tramite il protocollo Z-Wave e che costituiscono una piattaforma aperta che permette di sviluppare soluzioni di smart Home/Office ad hoc.

La sicurezza si estende sino a comprendere la prevenzione di disastri ambientali dovuto al malfunzionamento di oggetti o a guasti dei servizi pubblici fruiti. Tra i controlli di prevenzione disponibili vi sono ad esempio la gestione automatizzata dell'energia, il rilevamento di perdite di gas o idriche, la rilevazione di fumi o eccessiva CO2.



Al momento della rilevazione viene automaticamente segnalato l'evento e vengono avviate in automatico le procedure di prevenzione necessarie. Della protezione di persone e beni in ambienti anche molto estesi, privati e pubblici, si è fatta carico anche RISCO, società nata col marchio Rokonet nel 1978 che specializzata nello sviluppo e commercializzazione tramite il canale di un'ampia gamma di soluzioni di sicurezza, impianti antifurto ad alte prestazioni, rivelatori e accessori. Il portfolio comprende tecnologie integrate che spaziano dalle connessioni wireless al cloud e allo smartphone e permette di proteggere le aree riservate da intrusioni e allertare immediatamente il personale di vigilanza.

Chiave delle soluzioni commercializzate è il poter realizzare una infrastruttura di protezione che può coprire l'intera azienda e le sue aree esterne, oltre a permetterne il controllo automatizzato tramite sensori, videocamere e attuatori, controllabili

da un unico centro o tramite app su smartphone mediante il cloud RISCO. Per ottimizzare controllo ed interventi l'area da proteggere può essere suddivisa in decine di microzone, costituite anche da una singola finestra o una porta, che può essere chiusa od aperta in modo automatico, o inviare un allarme se forzata.

La protezione può essere rafforzata anche tramite videocamere ad alta risoluzione e applicazioni di gestione software che permettono di evitare i falsi allarmi generati ad esempio in aree esterne ed interne dalla presenza di animali o oggetti in movimento di piccola dimensione, grazie anche a tecnologie proprietarie quali la VPT (Variable Pet Threshold), SRT (Sway Recognition Technology) e DTC (Digital Correlation Technology)

Oltre ad una gestione diretta da parte dell'utente, le soluzioni di sicurezza si prestano, per come sono state concepite e tramite il cloud, anche ad essere fruite come servizio erogato da parte di partner di canale specializzati. Diverse le soluzioni nel suo portfolio

per le svariate esigenze. ProSYS Plus è un sistema di grado 3 per grandi progetti scalabile fino a 512 zone che permette di integrare dispositivi di sicurezza cablati, radio e via RISCO Bus. È fruibile tramite un sistema di licenze studiato per ridurre il costo del progetto e permettere tramite web, smartphone e cloud di gestire e monitorare il sistema in qualsiasi momento e luogo. LightSYS 2 è invece un sistema ibrido per le PMI dotato di una centrale di grado 2 e controllabile via smartphone. Gestisce sino a 50 zone. Axeplus è invece un sistema di controllo accesso scalabile basato su cloud e personalizzabile, ideato per ambienti muti sito, senza limiti per numero di porte o utenti gestiti.

Tutte le soluzioni sono gestibili tramite SynopSYS e, tramite Cloud, con

applicazioni web e smartphone, è possibile disporre di una visione continua della situazione dei sistemi da ovunque.

Data Protection e videosorveglianza: attenti ai dati

Sempre più ampio per garantire la sicurezza fisica è il ricorso alla videosorveglianza. L'offerta di soluzioni sul mercato è vasta, ma ci sono aspetti parimenti importanti da non trascurare: dove finiscono i dati registrati che devono essere disponibili per la successiva analisi forense, sperando naturalmente che questo non sia mai necessario?

Va considerato, osserva Western Digital, che un sistema per il controllo video di un'azienda, un ufficio o una casa deve garantire la qualità delle riprese e la registrazione continua. All'esigenza di garantire la disponibilità dei dati video registrati WD ha dato una risposta con lo sviluppo delle unità WD Purple, progettate e costruite per sistemi di sicurezza ad alta definizione, destinati a funzionare ininterrottamente h24. Robuste le loro caratteristiche tecniche. Sono in grado di supportare fino a 64 telecamere e sostenere un tasso di workload (la quantità di dati trasferiti da un hard disk a un altro), che arriva fino a



180 TB all'anno, un tasso che è quasi tre volte superiore a quello tipico di un'unità desktop.

Ingegnerizzati appositamente per la videosorveglianza, sono dotati di un software di storage specifico per questa applicazione e potenziati da una tecnologia proprietaria pronta per supportare l'Ultra-HD, chiamata AllFrame 4K. Quest'ultima, ha spiegato l'azienda, migliora lo streaming ATA per limitare la perdita di fotogrammi, ottimizzare in generale la riproduzione del video e aumentare il numero di alloggiamenti di hard disk supportati all'interno di un NVR (Network Video Recorder).

Robusta anche la protezione ambientale delle unità che, per garantire l'attività anche in ambienti difficili sono realizzate con componenti anti-ossidazione.

Non ultimo, ha osservato WD, gli hard disk WD Purple sono stati progettati per la compatibilità in modo, tramite un'ampia serie di case e chipset, da consentire di aggiungere capacità al sistema di sorveglianza rapidamente e senza interruzioni.

Salvaguardare la privacy dal visual hacking

Proteggere i dati con software sofisticato e l'ufficio con sistemi anti effrazione può non essere sufficiente, soprattutto se si viaggia molto o si lavora in pubblico o in uffici molto frequentati da estranei. Il clic virtuale

e silenzioso di che fa finta di telefonare di uno smartphone e i dati sullo schermo del proprio Pc sono carpiri in un attimo. E se si tratta di user name e password sono problemi.

L'indagine intitolata "Public Spaces Interview Study", realizzata a fine 2017 dal Ponemon Institute e sponsorizzata da 3M ha rivelato che l'87% dei sempre più numerosi "mobile worker" ha sorpreso qualcuno guardare il monitor del proprio notebook da dietro le loro spalle, in uno spazio pubblico.

Il cosiddetto "Visual hacking" sta crescendo e tre su quattro mobile worker intervistati dal Ponemon Institute hanno affermato di essere preoccupati per questa minaccia, ma la consapevolezza di un problema è solo l'inizio, dopo occorre la soluzione. Eppure i motivi per preoccuparsi non mancano.

Sempre gli analisti di Ponemon, nei loro studio sul visual hacking hanno rilevato che il 91% degli attacchi visuali va a buon fine. Inoltre, il 52% dei dati sensibili di un'azienda perde la sua riservatezza poiché viene visualizzato da un impiegato interno non autorizzato.

Una protezione facile da installare l'ha ideata 3M con lo sviluppo di un'articolata gamma di filtri da applicare ai monitor di qualsiasi dispositivo, dai grandi formati per le workstation fino a tablet e smartphone.

Sono filtri, ha spiegato l'azienda, realizzati grazie a una tecnologia ottica che garantisce privacy visiva e protezione degli schermi, e forniscono una difesa dal visual hacking, fornendo allo stesso tempo protezione contro i danni fisici e l'abbagliamento dello schermo.

Funzionano in base alla tecnologia Microlouver che permette di oscurare completamente la visione laterale senza ridurre quella dell'utilizzatore, mentre il vicino o il collega indiscreto vedranno solo uno schermo nero o color oro.

Pertanto, i filtri possono essere applicati, quando serve garantire la riservatezza e facilmente rimossi quando si vuole condividere i contenuti.

3M ha reso disponibile anche una versione per i telefoni, con filtri progettati per essere usati all'occorrenza: nell'orientamento verticale garantiscono la privacy e in quello orizzontale consentono di condividere lo schermo. ❖

Il data center cambia e va nel cloud



Il data center sta mutando forma per far fronte alle esigenze di sicurezza e di business. L'iperconvergenza si sta affermando con concreti benefici

di **Giuseppe Saccardi**

In un modo che è stato inizialmente strisciante, ma con un processo che tende a velocizzarsi, stiamo assistendo alla trasformazione dei data center. A dare il via sono state le esigenze degli utilizzatori e del contesto di business in cui si muovono e, subito a seguire, chi li gestisce, e cioè il personale IT alle prese con una trasformazione digitale che in pochi anni ha proiettato il data center in uno scenario di utilizzo e un contesto architettonico del tutto nuovo.

Svariati sono i fattori che hanno portato a questo cambiamento, alcuni di natura economica e sociale, altri di natura prettamente tecnologica e organizzativa.

Tra i primi va annoverata l'esigenza da parte delle aziende di concentrarsi sul core business e di ottimizzare Capex e Opex, il che, detto in altre pa-

role, significa contenere il costo delle infrastrutture o perlomeno parametrarle ai ritorni in termini di fatturato e allo stesso tempo ottimizzare, alias ridurre, il personale preposto. Il processo di virtualizzazione dell'IT è stato in pratica un modo per contenere il Capex e utilizzare al meglio il data center. Tra i secondi la proiezione verso l'esterno dell'azienda, la crescita tumultuosa della mobility, l'esigenza di rispondere rapidamente alle richieste del mercato.

Il successo del cloud e dell'IT visto come servizio e come modo per esternalizzare la sua complessità deriva in definitiva dal fondersi di quanto sopra detto.

L'iperconvergenza è un ulteriore passo in questa direzione volta a semplificare la complessità dell'IT e in qualche modo permettere anche alle Pmi e alle aziende e agli enti pubblici in generale di poter trarre beneficio dai processi che sino a ora hanno interessato e favorito i service provider o i fornitori mondiali di servizi cloud, senza che si debbano far carico degli oneri di una complessa gestione.

Da convergenza a iperconvergenza

Ma cosa si intende per iperconvergenza, che segue quella che a questo punto si può definire come step intermedio, della convergenza?

In sostanza, pur con varianti minori, consiste nel rendere disponibili soluzioni chiavi in mano che racchiudono capacità di calcolo, di storage e di rete, il tutto in un fattore di forma compatto e predisposto per l'espansione sia locale sia geografica. Un ruolo importante in questa evoluzione lo gioca il software e in particolare quello di orchestrazione e di gestione.

Poiché l'obiettivo primario di un tale approccio è quello della semplificazione, e cioè del poter disporre di quello che a parte le dimensioni di scala si configura come un vero e proprio data center senza però doverne supportare i costi di gestione, è subito evidente che il software di gestione e orchestrazione delle risorse deve risultare molto user friendly e farsi carico di tutte quelle operazioni che in un data center convenzionale è competenza di personale specializzato che va a influire in modo massiccio sui costi di esercizio e sull'Opex.

I benefici del diffondersi di soluzioni iperconvergenti sono molteplici. Innanzitutto si apre la possibilità anche per medie o piccole aziende di disporre di soluzioni resilienti e con prestazioni facilmente espandibili, sia per uso locale che per realizzare infrastrutture di backup o di disaster recovery a costi di realizzazione e di esercizio molto contenuti. Va osservato che però nel caso di soluzione per il disaster recovery un ruolo importante è assunto da parametri quali RPO e RTO, ovvero sia il punto da recuperare e il tempo in cui lo si vuole realizzare per ritornare operativi. Tempo che naturalmente dipende dalla velocità della linea di interconnessione e che può avere un costo anche fortemente variabile. Importante è quindi anche definire una scala di priorità tra le applicazioni per stabilire quelle che devono essere recuperate e rimesse in produzione per prime, dati compresi.

Un secondo beneficio è che diventa più facile evolvere a livello di applicazioni e di elaborazione e gestione verso il cloud. Si può in tale scelta strategica spostare sul cloud attività non critiche per quanto concerne la riservatezza, così come adottare il cloud per la fase di test e sviluppo di nuove applicazioni mantenendo però una gestione e un controllo locale delle applicazioni e relativi dati aventi carattere sensibili che non potrebbero

essere trasferiti sul cloud, sia in base a scelte strategiche che a regolamenti nazionali e sovranazionali.

Un terzo punto coinvolge il canale, perché anche aziende o system integrator di medie dimensioni possono offrire servizi con un data center che può essere rapidamente attivato anche in sedi distaccate prossime ai clienti e fatto crescere in funzione del numero e delle esigenze dei clienti.

Soluzioni adatte per tutte le esigenze

L'adozione di data center di nuova concezione e in particolare iperconvergenti e con caratteristiche centrate sul software, in aderenza a quanto viene riferito come "Software Defined Data Center", ha affrontato un'ulteriore evoluzione: quella dei moduli o mattoncini di base a disposizione degli utenti.

Una prima fase di sviluppo di questo nuovo approccio, con soluzioni a rack o stand alone di configurazione fissa ha mostrato delle criticità a causa della rigidità e ha subito un adattamento progressivo per andare incontro a esigenze specifiche per quel che riguarda il solo calcolo o il solo storage.

Le prime soluzioni, peraltro abbastanza recenti, presentavano infatti il problema che se si voleva espandere il sistema perché lo spazio storage (o il tipo di storage) era esaurito o la capacità di calcolo non più in grado di gestire il crescente workload, si doveva comperare un nuovo modulo di cui poi si finiva con l'usare solo una delle componenti.

Ciò ha portato i produttori, pur mantenendo invariato l'approccio generale, a sviluppare moduli dedicati al solo storage (anche con caratteristiche diverse in termini di capacità e tipologia) o al solo calcolo.

In sostanza, quello che è possibile fare stante l'attuale situazione dell'offerta, è dotarsi di una soluzione iniziale costituita da un paio di moduli con capacità di calcolo, storage e rete per disporre in ogni caso di un sistema ridondato e poi aggiungere moduli analoghi se storage e capacità elaborativa vanno come esigenze di pari passo o aggiungere solo moduli storage o di calcolo. I benefici sono consistenti e non solo per gli utenti finali ma anche per il canale. Come evidenziato, per quest'ultimi si apre non solo la strada verso la fornitura di servizi in modalità del tutto simile (salvo la scala) al cloud messo in campo da colossi del mercato in modo proporzionale al business, ma diventa possibile farlo concentrandosi sulla gestione dei servizi erogati e sulla gestione e il supporto del cliente.

Come garantire la sicurezza dei Container

Un Container può agire come punto di diffusione per attacchi cibernetici. Come evitare questo rischio



di **Giuseppe Saccardi**

I container rappresentano la componente di una architettura per i dati che permette di rendere le applicazioni più portatili tra ambienti di sviluppo, test e produzione. In sostanza, aiutano a semplificare gli sviluppi del software e a risparmiare tempo, e di conseguenza costi di sviluppo. Proprio per la loro portabilità e il fatto che contengano in un unico contenitore tutto quanto relativo a uno specifico progetto o attività di business, ne risulta un aumento dei rischi connessi alla sicurezza. “Smarrire” o aprire la strada a un cyber criminale a un intero container non è come perderne una limitata parte.

In proposito un recente studio Forrester ha rivelato che il 53% dei decision-maker IT ha identifica-

to la sicurezza come principale freno all'adozione dei container. Le aziende che intendono adottarli dovrebbero quindi guardare attentamente al modo in cui garantirne la sicurezza, focalizzandosi su provenienza, contenuto, isolamento e fiducia.

Certificare e ispezionare il Container

La prudenza si impone. Oltre il 30% delle immagini ufficiali su Docker Hub, contengono vulnerabilità importanti secondo uno studio di BanyanOps. La certificazione con firme digitali, per esempio, aggiunge un livello di sicurezza confermando chi ha creato il container e a quale scopo.

Per aumentare la sicurezza società leader di mercato stanno lavorando per stabilire standard e practice per la certificazione dei container in modo da garantire che:

- Tutti i componenti provengono da fonti fidate.
- I container host non siano stati manomessi e siano aggiornati.
- L'immagine container non presenti vulnerabilità note nei componenti della piattaforma e nei suoi livelli.
- I container siano compatibili e operino in ambienti ospitanti certificati.

Verificare da dove viene un container è quindi importante, ma analizzare quello che c'è dentro l'immagine del container lo è ancora di più.

Come la deep packet inspection studia i pacchetti che viaggiano in rete alla ricerca di contenuti malevoli, così la Deep Container Inspection (DCI) guarda il contenuto. Avere visibilità sul codice all'interno del container è fondamentale per mantenere la sicurezza durante e dopo lo sviluppo.

Isolare per mettere al sicuro il business

Una volta che le applicazioni container-based sono composte da container sicuri, bisogna assicurarsi che non vengano compromessi da altre immagini container sullo stesso host. La realtà è che i container non contengono veramente delle applicazioni, è più corretto dire che i container pacchettizzano il codice di un'applicazione con le sue dipendenze.

Se si pensa ai container come a oggetti con delle pareti, si deve essere consapevoli che sono estremamente sottili. I contenuti malevoli in un container possono passare a un altro o al sistema operativo host. Ogni singolo processo che gira all'interno di un container parla direttamente con l'host kernel e per tutti i container su quell'host. Il kernel può in sostanza fungere da single point of failure. Una vulnerabilità all'interno del kernel Linux potrebbe permettere a coloro che accedono a un container di impossessarsi dell'host OS e di tutti gli altri container sull'host.

Per questo è fondamentale affidarsi a un host OS che venga mantenuto da kernel engineer e che sia aggiornato frequentemente con i più recenti fix di sicurezza. I containers basati su host deboli ereditano il modello di sicurezza compromesso di quell'host. Il kernel deve includere funzionalità che offrono livelli di isolamento e separazione appropriati come SELinux, Seccomp, Namespaces, e altri.

La variabile tempo gioca contro

Un'altra variabile che va considerata è quella temporale. Se nell'istante t zero l'applicazione container-based viene messa in produzione, cosa succede il giorno uno? Il giorno due? Nuove vulnerabilità vengono identificate quotidianamente e l'immagine container è sicura come il codice e le dipendenze che contiene. Ma di vulnerabilità ne è sufficiente una per compromettere il container e, potenzialmente, l'intero stack infrastrutturale.

Quello che ne deriva è che anche i container e i loro host devono essere gestiti durante l'intero ciclo di vita. Le aziende necessitano quindi di tooling policy-driven che automatizzi la gestione di versioni e upgrade, identità e accessi, sicurezza e prestazioni.

Come fare per mitigare il rischio

Anche se velocità e agilità rappresentano driver fondamentali per l'adozione dei container in azienda, non devono essere integrati a spese della sicurezza. Ecco perché una Deep Container Inspection di classe enterprise, associata a certificazioni, policy e fiducia è parte integrante dello sviluppo, deployment e gestione dei container. In sostanza, suggerisco gli operatori del settore, per trarre il massimo vantaggio dai container pur garantendo la sicurezza di questi ultimi e dei loro contenuti, l'azienda deve trovare modi più efficaci per determinarne:

- **Provenienza.** Prima di spostare un container in rete, accertarsi di sapere cosa contiene e dove ha avuto origine, nonché analizzare la tecnologia di validazione e le certificazioni relative alle fonti.
- **Isolamento.** Considerare l'isolamento del percorso di esecuzione del container e, in ambienti multi-tenant, valutare l'associazione di container con la virtualizzazione per disporre uno strato di sicurezza aggiuntivo.

Come evidenziato, non si deve poi trascurare di ispezionare regolarmente i contenuti dei container per ridurre eventuali rischi alla sicurezza per identificare ed eliminare le vulnerabilità.





DE gustare

alla scoperta dei sapori d'Italia

3 ORE AGO

ARTICOLI

LUGANA E AMICI ALLA PROVA DEL TEMPO

READ MORE

7 ORE AGO

ARTICOLI

FAUNA SELVATICA, UN SERIO PROBLEMA PER L'AGRICOLTURA

READ MORE

6 ORE AGO

EVENTI

FESTA ARTUSIANA SOTTO IL SEGNO DELLA CUCINA SOSTENIBILE

READ MORE

01 GIUGNO 2015

La Toscana di Biella

Agricoltura biodinamica

Asparago in cucina

5 ORE AGO

ARTICOLI

COCKTAIL LOW ALCOHOL, DUOMO 21 LANCIA IL NUOVO TREND

READ MORE

5 ORE AGO

ARTICOLI

TEATRO DEL G PER SCOPRIRE MEGLIO DI M

READ MORE

5 ORE AGO

WINE

SAN MIGUEL, IL GIRO DEL MONDO IN UNA BOTTIGLIA

READ MORE

5 ORE AGO

ARTICOLI

VINO E AR INSIEME P

READ MORE

DE gustare

alla scoperta dei sapori d'Italia


Alla corte del RE

www.de-gustare.it

