N. 123

DIRECTION

LE TECNOLOGIE CHE MUOVONO IL BUSINESS

DISTRIBUITO GRATUITAMENTE CON "IL SOLE 24 ORE"

OpenText

NASCE UN COLOSSO PER LA GESTIONE SICURA DEI DATI

INTERVISTA

LA TRASFORMAZIONE SECONDO NUTANIX

SPECIALE SECURITY

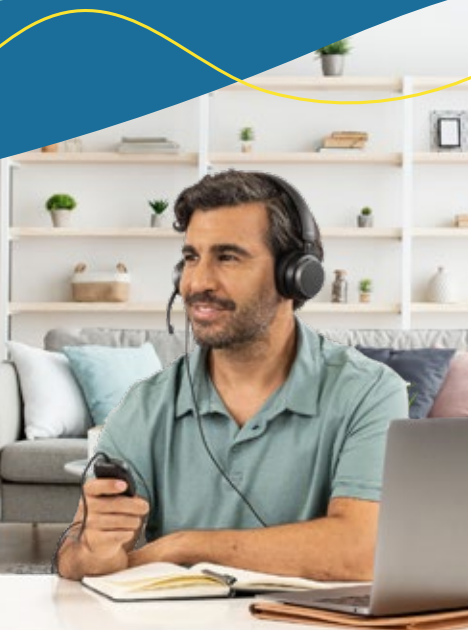
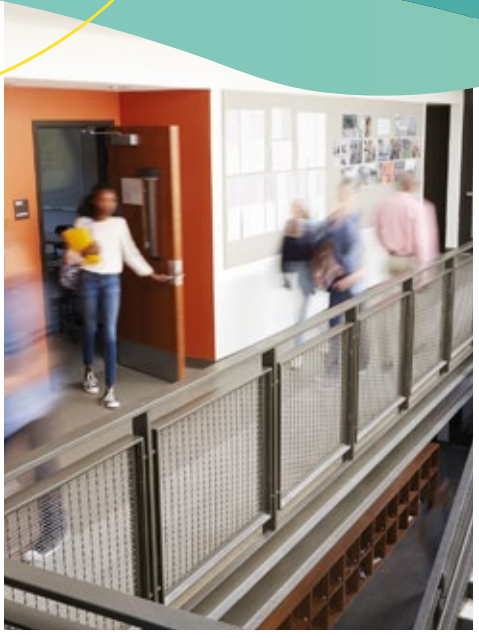
PREPARARSI PER ESSERE RESILIENTI

FOCUS RETAIL

RISOLVERE LE SFIDE DEL MERCATO



Connecting your Business


Quali che siano le esigenze o gli sviluppi della tua azienda, Snom propone soluzioni per le telecomunicazioni allineate al tuo contesto operativo. E questo da oltre 25 anni.

www.snom.com

snom

INDICE

Reportec è una società fondata da Gaetano Di Blasio, Riccardo Florio, Giuseppe Saccardi

DIRECTION REPORTEC
Anno XXI - Numero 123 - Marzo 2023
Iscrizione al tribunale di Milano n° 212 del 31 marzo 2003
Direttore responsabile: Riccardo Florio
In Redazione: Riccardo Florio; Paola Rosa
Ha collaborato: Aldo Cattaneo, Fabrizio Pincelli, Leo Sorge; Stefano Uberti Foppa
Grafica: Paola Rosa
Immagini: Dreamstime.com
Stampa: A.G. Printing Srl Via Milano 3/5; 20068 Peschiera Borromeo (MI)

Redazione: Via Gorizia 35/37 20099 Sesto San Giovanni (MI);
Tel 02 24304434; https://reportec.it; redazione@reportec.it
Editore: Reportec Srl; C.so Italia 50 20122 Milano
Amministratore unico: Riccardo Florio

Il Sole 24 Ore non ha partecipato alla realizzazione di questo periodico e non ha responsabilità per il suo contenuto

Diffusione cartacea e digitale 31.000 copie

bizIT.it

MAGAZINE ONLINE DI ICT E TECNOLOGIA

INFORMATION

COMMUNICATION

TECHNOLOGY

bizzIT.it è la rivista online che ti aggiorna con notizie, analisi, report, approfondimenti, interviste e case history dedicati all'ICT e alla tecnologia.

Continua a seguirci su:
https://bizzit.it/

IL CLOUD
NON UNA SCELTA, UN'ESIGENZA

di Riccardo Florio
• direttore responsabile •

Senza innovazione non è possibile pensare di competere nell'attuale contesto di mercato. E **non si può parlare di innovazione senza cloud**. Il cloud è l'unico modello capace, non solo di abilitare la trasformazione digitale, ma di ridefinire i modelli di business delle aziende di ogni dimensione attraverso nuove modalità d'interazione con l'utente finale, la possibilità di dispiegare applicazioni e servizi agili ai ritmi imposti dal mercato e la capacità di rispondere ai dettami di connessione dell'IoT e dell'Industria 4.0. Inoltre, risponde alle problematiche delle aziende di aggiornare costantemente l'infrastruttura tecnologica, di aumentare la flessibilità, abilitare la mobilità, individuare e proteggersi dalle minacce, di avere una previsione definita dei costi tecnologici e di ovviare alla carenza di risorse competenti e specializzate. Per questa ragione **il cloud non si può più considerare più una scelta, ma un'imprescindibile esigenza** che deve attraversare ogni decisione tecnologica e ogni strategia di business. Secondo le previsioni di McKinsey (Cloud Adoption - A Transformative Digital Solution Whitepaper, 2022) il 95% dei nuovi workload sarà distribuito su piattaforme *cloud-native* mentre, entro il 2024, l'85% delle aziende adotterà il principio *cloud-first* ovvero considererà come prima scelta l'opzione cloud a fronte di qualsiasi nuova decisione tecnologica.

Le aziende italiane sembrano aver compreso questo trend e, secondo dati Istat (Report Imprese e ICT, 2021), il 51,9% delle aziende del nostro Paese implementa già almeno un servizio cloud di livello intermedio (tipo ERP, CRM, contabilità) o avanzato (servizi quali hosting database, sicurezza, analytics, test applicativo).

L'approccio più idoneo per pianificare una migrazione verso il cloud è di **procedere per step partendo sempre da un assessment** per stabilire quale tipologia di modello sia la più idonea per ogni processo o applicazione. Per il prossimo futuro, il modello di riferimento sarà prevalentemente ibrido con la coesistenza di Private cloud e Public cloud. **Il Public cloud si sta affermando, anche in Italia, come il principale modello di rilascio di servizi IT**. Secondo Gartner (dati di ottobre 2022) la spesa mondiale degli utenti finali per i servizi cloud pubblici crescerà del 20,7% nel 2023 mentre la società di analisi IDC stima per il 2023 che in Italia la spesa aziendale per i servizi di cloud pubblico crescerà del 21,7% arrivando a sfiorare i 5,4 miliardi di euro. Di questi circa 3,24 miliardi sarà associato alla modalità Software as a Service: un dato che non sorprende considerando che la migrazione della componente applicativa è ciò che più favorisce l'evoluzione del modello di business.

di Romeo Scaccabarozzi
Amministratore Delegato di Axiante

SMART WORKING FATTO DI CASA, UFFICIO E CREATIVITÀ

Smart working non significa solo lavorare da casa, ma coordinare in modo efficace i benefici della comunicazione da remoto con gli spazi di interazione fisica in ufficio e i momenti creativi davanti alla macchina del caffè

C'era una volta l'ufficio, in cui l'ambiente di lavoro era uno spazio di produttività e il momento di ristoro presso la macchina del caffè era considerato un tempo e un luogo di non produttività. Eppure, era un luogo dove le posizioni aziendali si riequilibravano, dove era possibile proporre idee e fare commenti sfidando le separazioni gerarchiche aziendali. Oggi lo smart working è da molti considerato come un sinonimo di lavoro **da casa e tutte le statistiche confermano che, lavorare da casa, ha incrementato notevolmente la produttività degli individui (anche del 30-40%).** Tuttavia, ha "ucciso" gli spazi di creatività produttiva. Alcuni osservano che la denominazione smart è giustificata dal fatto che l'individuo, evitando il viaggio verso l'ufficio, inquina meno e può fare un uso più intelligente del suo tempo. Questo migliore uso del tempo dell'individuo non è smart working, così come non lo è lavorare unicamente da casa perdendo ogni opportunità d'interazione non strutturata. **Smart working significa bilanciare efficacemente il lavoro da casa e nello spazio di ufficio, le prestazioni dell'individuo con quelle del team, la produttività con la creatività.** Il primo vantaggio nel lavorare da casa è la possibilità di conciliare meglio le attività personali con quelle lavorative. Restare a casa non offre, però, quei momenti di discussione creativa fuori dal perimetro del ruolo e dei compiti aziendali. A questo dovrebbe contribuire lo spazio dell'ufficio che va ripensato come ruolo e funzione. **L'ufficio smart non è un luogo dove connettere il proprio PC e continuare a fare ciò che si faceva da casa:** deve prevedere meno scrivanie e più divani, meno riunioni e più interazioni. Questo è particolarmente vero per quelle realtà aziendali che, per rispondere alle proprie sfide di business, devono puntare sull'unicità e l'irripetibilità di ciò che fanno, che lavorano su progetti e che devono, ogni volta, creare e ricomporre i team di lavoro in base al progetto. Si tratta di un mondo ampio ed eterogeneo che spazia dai contractor, agli sviluppatori di software, dai professionisti del design al mondo dell'artigianato industriale. Per questo motivo, lo spazio dell'ufficio deve essere fisico e non virtuale.

Axiante (axiante.com) aiuta le organizzazioni a migliorare le performance e i processi, creando un valore reale e misurabile. Calandosi nel contesto unico di ogni realtà, opera per trovare la migliore soluzione che crei sinergia tra business, tecnologia e persone.

NUTANIX LA TRASFORMAZIONE È ANCHE MANAGERIALE

I principi del cloud suggeriscono una gestione che esce dalla nuvola e offre nuovi strumenti ai processi, sempre più innovativi

di Leo Sorge

Rajiv Ramaswami, CEO;
Sammy Zoghlami,
Senior Vice President EMEA

La gestione dell'azienda richiede competenze in continuo mutamento e con un diverso mindset nella gestione della complessità. **Il multicloud è oggi la base dell'innovazione e Nutanix è uno dei player mondiali di maggior successo.** Abbiamo affrontato l'evoluzione del management con **Rajiv Ramaswami, CEO, e Sammy Zoghlami, Senior Vice President EMEA di Nutanix.**
Trattare di GDPR, cloud e Gaia-X in Europa e in Italia è interessante, ma dalla conversazione sono usciti punti nuovi come un nuovo approccio alla gestione del talento e dell'automazione dei processi. L'ICT è sempre più la base della cultura aziendale.

D. QUALI SONO LE SFIDE DI OGGI NELLA GESTIONE DI DATI E APPLICAZIONI?

(Rajiv Ramaswami) La digitalizzazione porta alla generazione di grandi quantità di dati che l'azienda deve saper gestire. È un fenomeno generale, che tocca qualsiasi livello. Per esempio, in India è recentemente partita una piattaforma di pagamenti digitali che funziona ovunque e per qualsiasi somma, alla quale fanno riferimento persino i venditori al dettaglio che

> GRANDE ATTENZIONE AL TEMA DEI COSTI PER EVITARE IL DOPPIO COSTO PER MANTENERE LE RISORSE IN HOUSE

stanno sulla strada. I dati sono ovunque: data center, Edge, applicazioni, cloud. E la loro gestione riguarda molti aspetti: costi, sicurezza, governance, compliance e altri parametri. Inoltre, oggi, rispetto a 3-4 anni fa, c'è molta attenzione rispetto a temi quali la sovranità, la localizzazione dei dati e la privacy.
Una delle conseguenze dirette di questa situazione **è l'aumento della complessità oltre soglie facili da gestire.** È per questo che oggi è necessario **semplificare la gestione del mondo ibrido d'oggi** ed è proprio ciò che Nutanix propone.

D. HA CITATO COMPLIANCE E SOVRANITÀ DEI DATI, CHE SONO UN TEMA DI PARTICOLARE ATTENZIONE IN EUROPA. QUAL È LA VOSTRA POSIZIONE?

(Sammy Zoghlami) Governance e compliance sono componenti forti della discussione che osserviamo tra clienti e normatori, su cosa può essere fatto e come. Benché l'esigenza di compliance parta da motivazioni ragionevoli, la complessità in Europa è particolarmente elevata. In questa situazione, **l'automazione è un requisito centrale.**
Inoltre, qualche anno fa la situazione era più semplice: tutto ciò che non aveva requisiti diretti di compliance veniva spostato il prima possibile sul cloud. Ora, invece, si pone anche grande attenzione al tema dei costi per evitare di sostenere un doppio costo necessario a mantenere le risorse in house fino a quando non sono spostate nel cloud. Una situazione di questo tipo rappresenta un buon contesto per Nutanix; il public cloud è una delle risposte all'esigenza dei nostri clienti di avere più agilità, compliance e costi sotto controllo.

D. NUTANIX HA SPOSTATO IL MODELLO DI BUSINESS VERSO I SERVIZI GESTITI. QUESTA MOSSA HA SODDISFATTO LE ASPETTATIVE?

(Rajiv Ramaswami) Molte aziende stanno terminando il processo di digital transformation, che richiede servizi gestiti. Nutanix ha ormai completato un percorso durato due anni con cui ha via via rinnovato la propria offerta in modo molto soddisfacente.

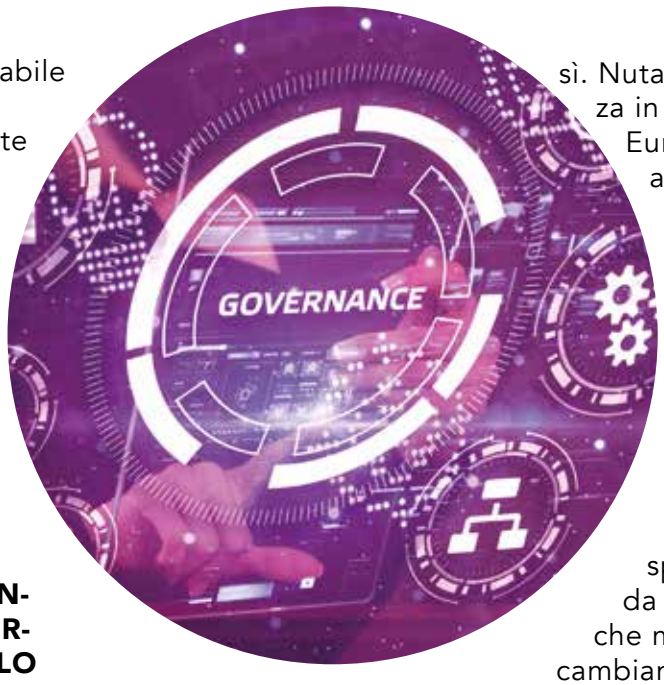
D. L'ITALIA STA AFFRONTANDO SFIDE PER MODERNIZZARE LA PROPRIA INFRASTRUTTURA ICT E NUTANIX HA ANCHE UNA PARTNERSHIP CON SOGEI. CREDE CHE LA PA ITALIANA STIA ANDANDO NELLA DIREZIONE GIUSTA?

(Sammy Zoghlami) Sono in Nutanix da oltre dieci anni e nel pubblico vedo ora una forte accelerazione, che sta cambiando anche il modo di pensare dei dirigenti e permette di superare i limiti precedenti. Ora vedo molte best practice del mondo privato che vengono applicate anche nel settore pubblico. Sogei è una iniziativa unica per la Pubblica Amministrazione e ha certamente un impatto positivo. Altri grandi Stati hanno molte iniziative ICT, ma non coordinate tra loro. Rispetto all'Italia, nazioni che non hanno alcun pregresso possono partire da zero e questo semplifica le azioni perché le transizioni sono sempre complesse.

D. GAIA-X È L'INIZIATIVA PER LA GOVERNANCE DIGITALE CHE PUÒ ESSERE APPLICATA A VARI STACK TECNOLOGICI CLOUD ED EDGE. COSA PENSA DI QUESTO APPROCCIO?

(Sammy Zoghlami) **Aumentare e uniformare la consapevolezza è un'ottima cosa** a tutti i livelli, anche politici. Non si tratta di creare l'Unione Europea dell'IT: rispetto alle iniziative nazionali, Gaia X aumenta il coordinamento. Certo creare unicgrande cloud provider europeo è possibile, ma molto difficile, e richiede tempi lunghi. Partendo da una stessa

iniziativa è molto probabile che nasceranno molte partnership con un forte substrato comune, perché ogni nazione ha le sue specificità proprio come le ha ciascun settore di mercato.



D. CREDETE CHE GDPR, LA LEGGE EUROPEA SULLA PROTEZIONE DEI DATI, RAPPRESENTI UN OSTACOLO ALL'INTEGRAZIONE DEI SERVIZI CLOUD A LIVELLO GLOBALE?

(Sammy Zoghlami) In molti casi direi di sì. **Non tutte le aziende hanno capito come adeguarsi.** Spesso la soluzione è di creare "repository" di dati per sapere sempre dove sono collocati e che è possibile cancellarli. Ne consegue che spesso vengono creati nel cloud nuovi silos di dati. A volte si parla di spostare il potere dei dati dalle grandi aziende alla gente. Questa è un'istanza filosofica dovuta anche al fatto che, storicamente, i principali cloud provider sono statunitensi e non europei.

D. CI SONO ALTRI ASPETTI CHE OSTACOLANO IL MIGLIORAMENTO DELL'ORGANIZZAZIONE DELLE AZIENDE?

(Sammy Zoghlami) Certamente due punti sono emersi su scala globale, indipendentemente sono emersi su scala globale,ui si opera: **l'elettricità e le competenze**. Qualche anno fa l'elettricità era marginale, ma ora è centrale per il business: è un problema di costo. Forse ci resterà per anni ed è diventato un problema del quale deve occuparsi il CEO. Non sempre l'IT è l'area a maggior costo energetico, ma in alcune parti sì. Nutanix ha molta esperienza in questo settore. In Europa, al momento, un altro tema centrale è quello di definire opportune strategie per la mitigazione del calore. Parlando di competenze, sono **molti i settori nei quali non ci sono abbastanza esperti** e quelli disponibili cambiano spesso lavoro, attratti da condizioni economiche migliori. Molti esperti cambiano azienda e lavoro e molte organizzazioni si trovano nella condizione di non disporre di personale a sufficienza per perseguire i loro obiettivi. La soluzione a questo problema è di intervenire per **semplificare la tecnologia, ridurre il numero di azioni umane e aumentare l'automazione.** Abbiamo alcuni clienti che sanno che perderanno i loro talenti e, di conseguenza, li formano appositamente, con programmi agili della durata di 3/6 mesi, e in grande quantità, in modo da avere continuamente a disposizione il personale necessario.

Un altro tema riguarda la **trasformazione nella gestione dei progetti.** Ogni azienda ha in corso un certo numero di progetti ma la mentalità è cambiata. Avviare nuovi progetti oggi richiede una gestione del budget differente rispetto al passato. Spesso, è necessario rassegnarsi ad accettare un progetto di portata più limitata, con un entry point più basso, ed essere pronti a cancellarlo se le cose non vanno come previsto. Se poi il progetto parte bene, allora esiste la possibilità di ampliarlo e farlo scalare verso l'alto. Sono tutti cambiamenti di gestione ai quali un'organizzazione di successo dev'essere preparata.

A seguito dell'acquisizione di Micro Focus, OpenText assume la connotazione di un nuovo colosso che punta ad avere un ruolo di leadership a supporto delle esigenze aziendali di Information Management, Digital Transformation e Cyber Resilience. Le famiglie di prodotti CyberRes si aggiungono alle soluzioni XDR, IAM, network detection e di analisi forense di OpenText per comporre una rinnovata e ampliata offerta di protezione.

di Riccardo Florio

OPENTEXT UN NUOVO COLOSSO PER LA GESTIONE SICURA DEI DATI

Con la recente acquisizione di Micro Focus per un prezzo di circa 5,8 miliardi di dollari la dimensione e la portata di OpenText, azienda nata in Canada nel 1999 , assumono i contorni di un nuovo protagonista assoluto nel panorama dell'Information Management. OpenText si propone ora come "la piattaforma delle piattaforme" per la gestione delle informazioni, ponendosi la rinnovata missione di aiutare le organizzazioni di tutte le dimensioni ad accelerare la loro trasformazione digitale e con l'obiettivo dichiarato di diventare leader nella gestione sicura dei dati.
Per abilitare una trasformazione digitale efficace in linea con questi trend l'azione di OpenText si articolerà per il futuro attorno ai seguenti mercati chiave:

- **Cybersecurity** per bloccare le minacce sul nascere con una sicurezza resiliente che protegge, rileva, risponde e ripristina;
- **Gestione delle "Digital operations"** per ottimizzare le operazioni digitali e la gestione dei servizi IT;
- **Servizi indirizzati ai contenuti** per incrementare la produttività, eliminare i silos e favorire l'automazione;
- **Esperienza digitale** per trasformare le relazioni e alimentare le interazioni digitali tra clienti, partner e dipendenti;
- **Rete business** per semplificare la connettività dell'ecosistema aziendale e integrare la supply chain;
- **Application Delivery Management** per consentire alle aziende di accelerare la distribuzione delle applicazioni.

OPENTEXT CYBERSECURITY: TUTTO CIÒ CHE SERVE PER LA RESILIENZA AZIENDALE

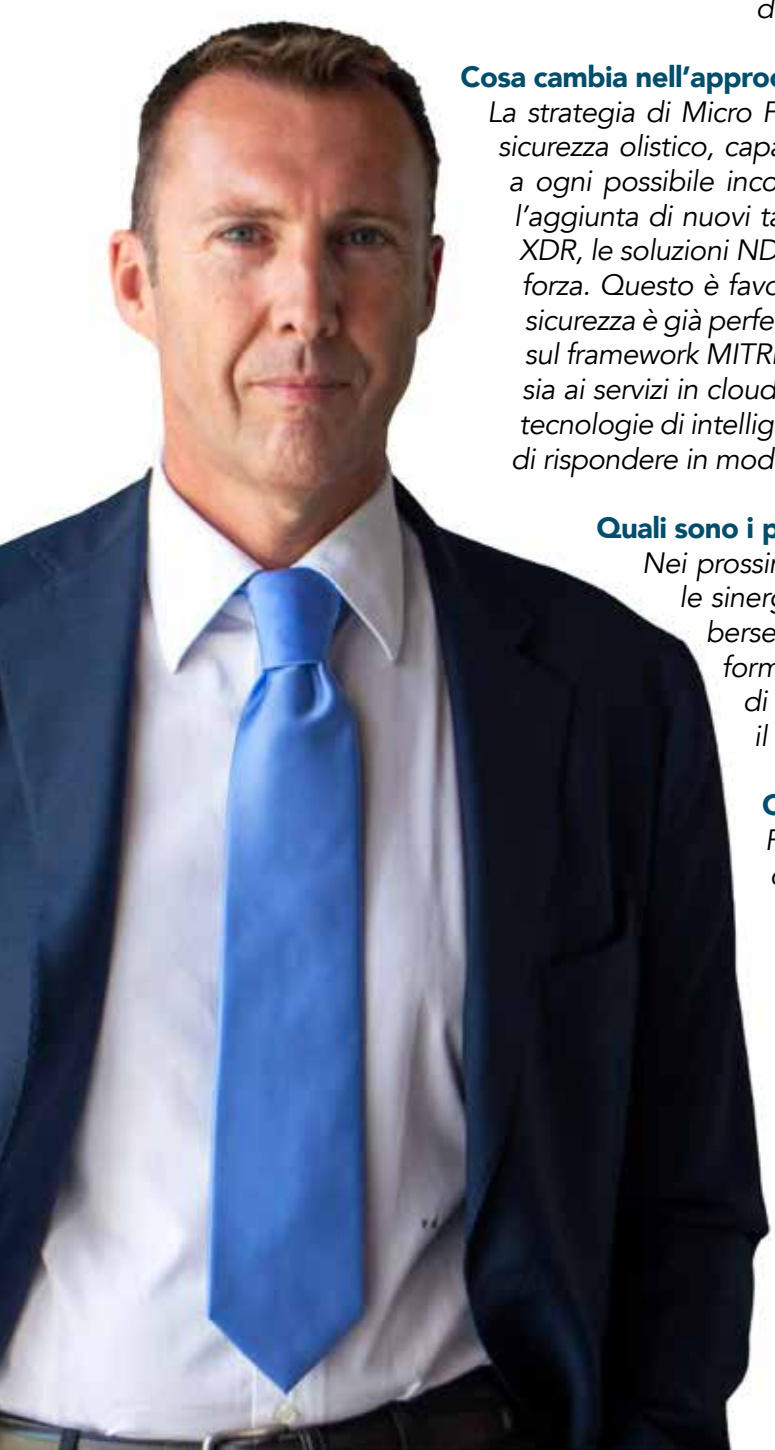
Resilienza e gestione sicura dei dati sono le parole chiave di OpenText Cybersecurity, la business unit dedicata a security e resilienza che sarà guidata in Italia, Sud Europa, CIS e CEE & Israel da Pierpaolo Alì e in cui confluisce la famiglia di soluzioni Micro Focus CyberRes (ArcSight, Fortify, NetIQ, Voltage) pensate, come dice il nome, per

OPENTEXT RIUNISCE INFORMATION MANAGEMENT, CYBERSECURITY E GESTIONE DEI DATI IN UNA VISIONE UNICA E COERENTE

garantire la cyber resilienza.
"OpenText Cybersecurity mette oggi a disposizione delle aziende probabilmente il portafoglio più ampio del mercato di soluzioni per la resilienza, il rilevamento delle minacce e la gestione intelligente e sicura delle informazioni – ha commentato **Pierpaolo Alì, Director Southern Europe, CIS, CEE & Israel di OpenText Cybersecurity** -. *Mettiamo, infatti, a disposizione delle aziende un'offerta completa per la cyber security e la resilienza adatta a rispondere alle nuove aree chiave di trasformazione dell'impresa, incentrate sui rinnovati modelli di business e di lavoro e basate e sui nuovi paradigmi digitali".*
Dalla prevenzione delle minacce al rilevamento e alla risposta, dalla gestione dell'accesso alle indagini forensi, dalla protezione delle applicazioni alla cifratura dei dati, l'offerta di sicurezza di OpenText permette di protegge le informazioni e i processi critici attraverso endpoint, reti, cloud, e-mail, Web-server, firewall e log.
Più precisamente, OpenText Cybersecurity punta ad abilitare la resilienza in base ai seguenti presupposti tecnologici:

- implementare il modello Zero Trust su tutte le superfici di attacco in continua espansione per prevenire e rispondere in modo proattivo alle minacce;
- ridurre al minimo i rischi di downtime dovuti a minacce come il Ransomware;
- mantenere la privacy e la sicurezza informatica in modalità conforme alle richieste normative;
- rilevare e rispondere alle minacce in pochi minuti su tutti i vettori IT, compresa qualsiasi fonte di log, endpoint, reti, server, e-mail e firewall, attraverso le funzionalità XDR (eXtended Detection and Response);
- acquisire, contestualizzare e visualizzare il traffico di rete totale per sapere sempre cosa sta succedendo e rispondere immediatamente a ogni inconveniente;
- monitorare e raccogliere dati da remoto, grazie a una visibilità completa sugli endpoint;
- raccogliere, elaborare, analizzare e produrre report di analisi forense per ottenere risultati più rapidi e approfonditi;
- governare l'accesso alle risorse aziendali attraverso sofisticati sistemi di gestione dell'identità;
- rilevare in modo automatizzato qualsiasi tipo di minaccia e attacco, utilizzando le tecnologie di machine learning per individuare qualsiasi comportamento anomalo inclusi quelli provenienti dall'interno;
- proteggere le applicazioni durante il loro intero ciclo di vita, a partire dalla fase di sviluppo e testarle costantemente per verificare ogni possibile vulnerabilità;
- proteggere qualsiasi tipo di dati grazie a tecnologie brevettate di crittografia e mascheramento, che seguono i dati sempre: a riposo, in movimento e persino durante l'uso.

4 DOMANDE A PIERPAOLO ALÌ, SOUTHERN EUROPE, CIS, CEE & ISRAEL DI OPENTEXT CYBERSECURITY



Con l'acquisizione di Micro Focus da parte di OpenText cosa cambia per gli attuali utilizzatori delle soluzioni di sicurezza CyberRes?

Per gli attuali utenti delle soluzioni CyberRes non cambia nulla in relazione ai prodotti che stanno utilizzando. Vengono garantiti gli Investimenti e gli aggiornamenti di prodotto con lo stesso ritmo, un miglioramento del supporto e le persone di riferimento restano le stesse.

Cosa cambia nell'approccio strategico verso la sicurezza?

La strategia di Micro Focus CyberRes, che puntava a un modello di sicurezza olistico, capace di garantire la resilienza aziendale rispetto a ogni possibile inconveniente o avversità, non cambia. Anzi, con l'aggiunta di nuovi tasselli di sicurezza come le soluzioni OpenText XDR, le soluzioni NDR quelle per l'analisi forense si estende e si rafforza. Questo è favorito dal fatto che l'approccio di OpenText alla sicurezza è già perfettamente allineato a quello di CyberRes: basato sul framework MITRE ATT&CK, aperto sia agli ambienti on-premise sia ai servizi in cloud, improntato al modello Zero Trust, sorretto da tecnologie di intelligence per una protezione in tempo reale capace di rispondere in modo intelligente e dinamico.

Quali sono i prossimi piani per l'Italia?

Nei prossimi mesi il lavoro si concentrerà nell'ottimizzare le sinergie di prodotto sia all'interno dell'offerta di cybersecurity, sia rispetto alle soluzioni OpenText di information e data management. Ci sarà poi una fase di integrazione tecnologica per sfruttare al meglio il bacino ampliato di tecnologie a disposizione.

Cosa accade del brand CyberRes?

Prevediamo di mantenere il brand delle famiglie di soluzioni ArcSight, Fortify, Voltage e NetIQ che faranno parte delle soluzioni OpenText Cybersecurity. Il brand CyberRes scompare per lasciare spazio a OpenText Cybersecurity a testimonianza di una gamma di soluzioni che interpretano il tema della security nel modo ampio che serve oggi ovvero capace di coniugare rilevamento delle minacce, protezione efficace, risposta rapida ma anche resilienza di fronte a qualsiasi evento e gestione sicura dei dati e dell'accesso.

XDR PER LA PROTEZIONE DEGLI ENDPOINT

La rapida evoluzione del panorama delle minacce informatiche sta riducendo l'efficacia dei tradizionali sistemi di sicurezza perimetrali e basati sulle firme. Inoltre, i team di sicurezza sono sovraccaricati con avvisi che minano la loro capacità di analizzare, dare priorità e rispondere alle minacce prima che si verifichino danni irreparabili o perdite di dati. Per affrontare queste sfide, le organizzazioni devono ottenere una migliore visibilità sugli endpoint.
OpenText dedica due famiglie di soluzioni alla protezione dei dispositivi individuali connessi in rete, i cosiddetti endpoint, che sono coinvolti in pressoché ogni tipologia di attacco,
OpenText EnCase Endpoint Security è una soluzione di rilevamento e risposta per gli endpoint (EDR), che consente agli analisti della sicurezza di rilevare, convalidare, analizzare, gestire e rispondere rapidamente agli incidenti. Completamente allineata al framework MITRE ATT&CK (una base di conoscenza accessibile a livello globale di tattiche e tecniche avversarie basata su osservazioni del mondo reale), questa soluzione opera tramite un singolo Agent molto leggero compatibile con la maggior parte i server, workstation e dispositivi. EnCase Endpoint Security affronta in modo completo gli attacchi più avanzati agli endpoint, siano essi provenienti da minacce interne oppure esterne e permette alle aziende di proteggersi dal Ransomware.
La seconda soluzione è **Webroot Business Endpoint Protection**, che sfrutta il cloud computing e il machine learning per monitorare e adattare in tempo reale le difese degli endpoint alle minacce. La protezione Webroot di nuova generazione opera in più fasi che, non solo è più efficace contro le minacce moderne, ma riduce anche la possibilità di falsi positivi. Non ci sono mai firme o definizioni da aggiornare, poiché la prevenzione delle minacce avviene in tempo reale dal cloud.

ARCSIGHT

Un aspetto rilevante della cyber resilience è la capacità di anticipare un attacco prima che avvenga. A questa esigenza OpenText indirizza le soluzioni **ArcSight** in grado di accelerare **la rilevazione delle minacce e la capacità di risposta**. ArcSight è una soluzione SIEM che permettono di individuare efficacemente ogni tipo di minaccia sfruttando la tecnologia di machine learning non supervisionato per identificare anomalie rispetto ai comportamenti abituali e identificare in modo intelligente le aree di rischio maggiore.

GESTIONE DELL'**ACCESSO** E DELL'**IDENTITÀ** ANCHE IN CLOUD

Il nuovo perimetro aziendale non è più definito dall'infrastruttura di rete, ma dalle identità digitali degli utenti e dei sistemi. OpenText Cybersecurity permette di gestire in modo efficace queste identità in ogni contesto e ambiente IT. **OpenText Identity and Access Management (IAM)** è un sistema di gestione delle identità e degli accessi basato sul cloud che comprende tecnologie cloud-native, framework di sicurezza integrati e processi digitali per garantire la massima scalabilità per l'accesso delle terze parti. Disponibile come servizio, questa piattaforma mette a disposizione un'architettura a microservizi con scalabilità automatica per sviluppare rapidamente applicazioni e soluzioni di gestione dell'identità personalizzate in un ambiente DevSecOps. La famiglia di soluzioni **OpenText NetIQ** mette a disposizione gli strumenti per realizzare una gestione Zero Trust dell'identità e dell'accesso secondo un approccio adattativo che utilizza l'analisi del comportamento per verificare costantemente che il profilo di rischio di un utente sia adeguato al livello di accesso di cui dispone. Queste soluzioni sono adatte per le aziende che vogliono di raggiungere i propri obiettivi di compliance mantenendo un ambiente sicuro e allineato agli obiettivi aziendali.

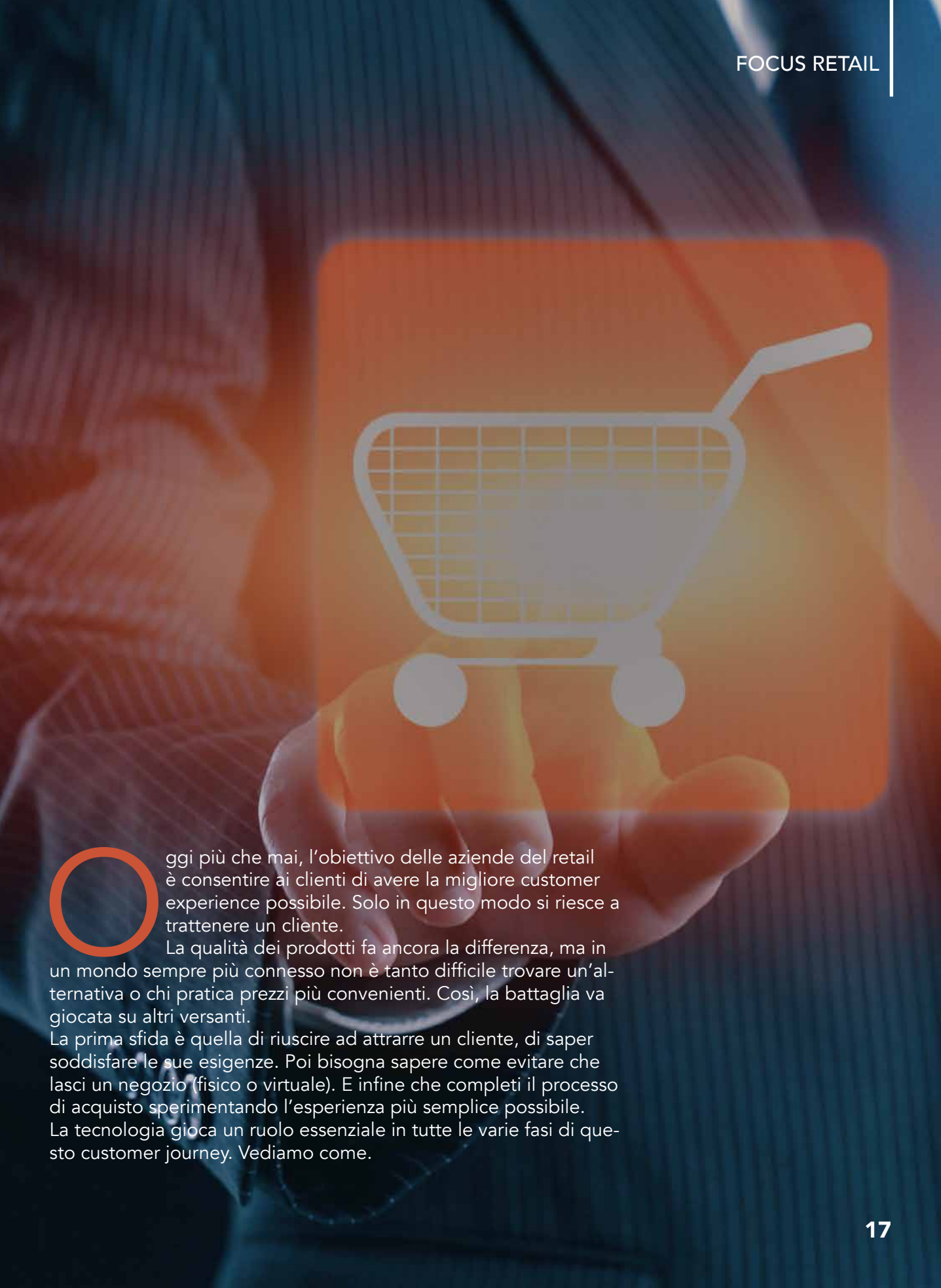
PROTEGGERE DATI E APPLICAZIONI NEL CICLO DI VITA: LE SOLUZIONI **VOLTAGE** E **FORTIFY**

Alla protezione e la privacy dei dati si indirizzano le soluzioni della famiglia **Voltage** che forniscono gli strumenti per garantire la cifratura dei dati durante l'intero ciclo di vita, in ambienti ibridi e anche quando sono contenuti in file destrutturati. Le tecnologie esclusive e brevettate di Voltage consentono anche di mantenere i dati protetti anche durante l'uso, ma mascherandone la natura ma mantenendo però l'usabilità e l'integrità referenziale necessarie per le operazioni di elaborazione, le applicazioni e i servizi.
Per proteggere le applicazioni durante il loro intero ciclo di vita OpenText mette a disposizione la famiglia di software **Fortify**. Queste soluzioni mettono a disposizione strumenti per integrare in modo trasparente e automatizzato l'analisi di sicurezza e identificare i difetti del software nel momento stesso in cui viene scritto. Inoltre, consentono di effettuare test di sicurezza in ogni ambiente e su ogni tipologia di software, inclusi quelli commerciali, sia in modalità on-premise in on-demand (Fortify on Demand).

LE SFIDE CHE DEVE AFFRONTARE OGGI IL RETAIL E COME RISOLVERLE

Più che per i prodotti, un cliente oggi si affeziona a un marchio per l'esperienza d'acquisto che tale marchio gli permette di vivere. Il modo più efficace per soddisfare al meglio i sempre più mutevoli ed esigenti consumatori è ricorrere alla tecnologia

di Fabrizio Pincelli



Oggi più che mai, l'obiettivo delle aziende del retail è consentire ai clienti di avere la migliore customer experience possibile. Solo in questo modo si riesce a trattenere un cliente.

La qualità dei prodotti fa ancora la differenza, ma in un mondo sempre più connesso non è tanto difficile trovare un'alternativa o chi pratica prezzi più convenienti. Così, la battaglia va giocata su altri versanti.

La prima sfida è quella di riuscire ad attrarre un cliente, di saper soddisfare le sue esigenze. Poi bisogna sapere come evitare che lasci un negozio (fisico o virtuale). E infine che completi il processo di acquisto sperimentando l'esperienza più semplice possibile.

La tecnologia gioca un ruolo essenziale in tutte le varie fasi di questo customer journey. Vediamo come.

Tutte le più attuali strategie del mondo retail sono caratterizzate da un aspetto comune: il cliente è al centro. In sostanza, l'obiettivo è soddisfare al meglio le esigenze e aspettative del cliente cercando di conoscerlo più possibile.

In questo senso, il customer relationship management (CRM) assume un ruolo ben diverso da quello che aveva qualche tempo fa, quando era principalmente indirizzato a offrire un servizio di supporto. Oggi il CRM è parte integrante del marketing della relazione su cui si basa la promozione di attività in linea con il profilo dei clienti. L'obiettivo è instaurare una relazione di lungo periodo che poggi su un servizio appagante e su un'esperienza d'acquisto personalizzata tagliata sulle peculiarità dei singoli e a cui si possono affiancare sconti o promozioni mirati.

Questa linea strategica richiede di avere un CRM che fornisce più dati possibili inerenti ai clienti, sui loro gusti loro preferenze, sulle loro abitudini di acquisto. Ma anche di carattere demografico, sulle caratteristiche finanziarie e sulle attività online. I dati mobili provenienti da dispositivi come i telefoni possono poi mostrare dove vivono i clienti, a quale distanza dal punto vendita, nonché i loro movimenti abituali. Per massimizzarne l'efficacia, tali dati vanno combinati e analizzati con sistemi di intelligenza artificiale (IA) e machine learning (ML). Così facendo si ottengono analisi evolute da cui è possibile estrarre informazioni che consentono di prendere decisioni più intelligenti ottimizzare le operazioni per aumentare le vendite e offrire servizi migliori e più in linea con le aspettative.

CRM E PROFILAZIONE
proposte e servizi sono sempre più personalizzati

Ovviamente, i dati devono essere adeguatamente protetti in termini di cyber security e conservati secondo le normative previste dal GDPR.

Usare i social per analizzare i pareri dei **CONSUMATORI**

Volete saper cosa pensano i vostri clienti di voi? Usate la sentiment analysis. Si tratta di un processo automatizzato che analizza un testo per estrarre i pareri contenuti.
La sentiment analysis si basa su un motore di intelligenza artificiale che usa il ML ed elaborazione del linguaggio naturale (NLP) per estrarre le informazioni. Più in dettaglio, il ML consente al software di apprendere in modo autonomo e diventare più preciso nel prevedere il risultato dell'analisi senza essere programmato per uno scenario esplicito migliorandosi nel tempo. La tecnica NLP analizza invece il linguaggio umano e il significato che sta dietro ad esso.
Solitamente, la sentiment analysis è usata per esaminare i post dei clienti, come tweet, commenti, feedback e qualsiasi comunicazione relativa a prodotti o servizi, pubblicati su siti o social. In tal modo si può tenere traccia degli argomenti pubblicati in relazione a un determinato brand o ai suoi prodotti. Questo consente di apprendere di eventuali problemi, avendo un chiaro quadro della situazione e poter, quindi, fornire ai clienti una soluzione efficace.
I risultati della sentiment analysis possono essere usati per individuare tendenze oppure per progettare un nuovo prodotto o migliorare la qualità di un servizio. Ma anche per identificare gli strumenti e i modi più adatti per evitare che i clienti abbandonino un marchio.

Ottimizzare magazzino e logistica con l'**IOT**

L'uso dell'IoT nel settore della vendita al dettaglio è strettamente connesso alle tecnologie GPS e RFID che aiutano a tracciare i prodotti attraverso l'intera supply chain. Viene così consentito ai rivenditori di monitorare il movimento del prodotto, le sue condizioni e tracciarne la posizione, oltre a prevedere tempi di consegna precisi. L'IoT nei centri commerciali e nei negozi offre ai rivenditori i dati di cui hanno bisogno per ottimizzare la progettazione delle loro strutture. Utilizza i dati dell'esperienza in negozio per organizzare al meglio il layout del punto vendita, ottimizzare il tempo trascorso nei camerini, creare un sistema di suggerimenti intelligenti e spingersi fino a sostituire il personale umano con la tecnologia automatizzata, ove possibile. Un altro esempio di impiego dell'IoT nella vendita al dettaglio sono gli scaffali intelligenti. I rivenditori dedicano tempo ed energia a tenere traccia degli articoli per assicurarsi che non siano mai esauriti e anche a garantire che gli articoli non vengano smarriti sugli scaffali. Gli scaffali intelligenti automatizzano entrambe queste attività, rilevando anche potenziali furti. Dotati di sensori evoluti e tag RFID possono scansionare i prodotti per informare i dipendenti quando gli articoli si stanno esaurendo o quando sono posizionati in modo errato. In alcuni negozi i tag RFID sono oggi usati anche per velocizzare le operazioni di pagamento, senza dove passare lo scanner sui singoli prodotti.

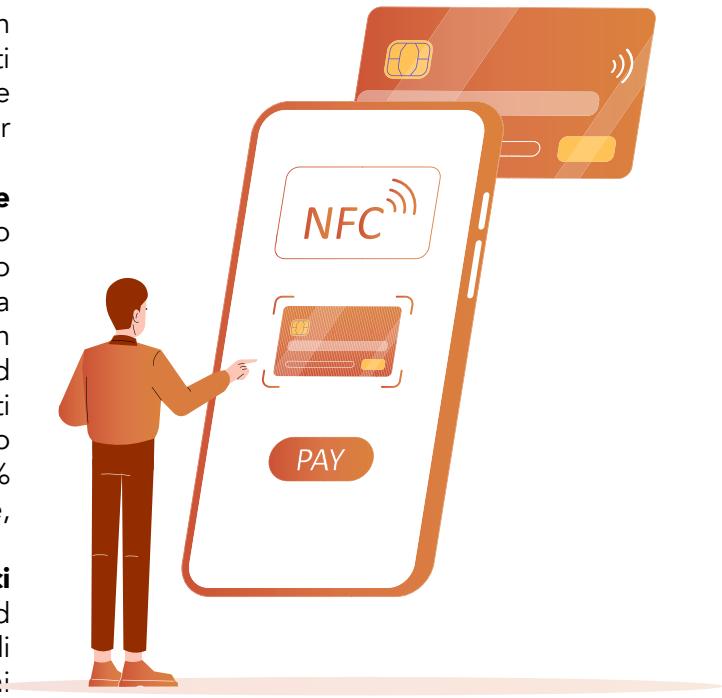
Un nuovo modo di vendere: l'**OMNICANALITÀ**

La vendita al dettaglio omnicanale è una strategia commerciale che crea un'esperienza di acquisto senza soluzione di continuità su più piattaforme. Mentre i consumatori si spostano tra spazi fisici e digitali, sperimentano una **conversazione coerente e organica con il brand** perché ogni punto di contatto è connesso e i loro dati sono sempre unificati. Alcune aziende utilizzano un'unica piattaforma, gestendo un negozio fisico oppure online, altre offrono un'esperienza multicanale, consentendo ai clienti di effettuare acquisti attraverso più canali separati. Però, siccome queste piattaforme non sono collegate tra loro, isolano le esperienze del cliente.

Nella vendita omnicanale, le aziende offrono le stesse esperienze su tutti i canali che sono uniti per dar vita a una fluida customer experience. Questa connessione mantiene i clienti coinvolti e li indirizza verso l'acquisto.

Con un numero di canali e dispositivi in continua crescita, anche la tecnologia che consente esperienze omnicanale prosegue nello sviluppo e così aumentano anche le aspettative dei consumatori. Le app dei social media, per esempio, sono diventate popolari canali di acquisto perché hanno aggiunto la possibilità di effettuare acquisti in-app.

La realtà aumentata (AR) amplia ulteriormente l'offerta multicanale fornendo una serie di vantaggi per il settore della vendita al dettaglio perché consente esperienze di acquisto più fluide senza doversi recare in un punto vendita fisico. L'AR consente infatti di provare virtualmente qualsiasi prodotto, dall'abito all'arredamento, prima di effettuare un acquisto. Un effetto eclatante è che può ridurre il numero di resi che nel 2021 ha portato i rivenditori a emettere rimborsi per un totale di 4,4 miliardi di dollari.



I pagamenti sono sempre più **CONTACTLESS**

Garantire un percorso di acquisto al cliente fluido e piacevole è sempre stato un punto focale per i retailer che, spinti dalla rapida adozione della tecnologia, sempre più si avvalgono di strumenti alternativi per l'accettazione dei pagamenti.
I rivenditori iniziano quindi sviluppare **strategie per integrare i pagamenti digitali** nella loro proposta di valore. Tra queste strategie troviamo anche i **pagamenti contactless** tramite carta di credito/debito, smartphone o smartwatch attraverso servizi come Apple Pay, Android Pay o Google Wallet. Questi, secondo i dati dell'Osservatorio del Politecnico raggiungono **il 64% del totale transazioni digitali** (il 69% se consideriamo anche quelle via mobile, smartwatch e altri device).
Alla base dei **pagamenti senza contatto ci sono la tecnologia RFID o NCF** (Near Field Communication). Quest'ultima consente di trasmettere e ricevere in modo sicuro informazioni a corto raggio (di solito a una distanza non superiore a 4 cm) attraverso smartphone o dispositivi indossabili. In pratica, NFC è un aggiornamento della tecnologia RFID che combina in un unico dispositivo sia il lettore sia l'interfaccia della smart card.
Il processo di pagamento è molto semplice: quando i lettori e i dispositivi di pagamento sono vicini e attivati, **si verifica uno scambio di dati crittografati tra i chip NFC**, che completano il pagamento. Tale processo rende il flusso di cassa velocissimo, facendo così dei pagamenti NFC uno dei metodi di pagamento più sicuri e convenienti.

Diverse app di pagamento e wallet digitali utilizzano NFC **per aumentare la sicurezza poiché i portafogli digitali comunicano con i lettori NFC solo quando l'utente sblocca l'app sul dispositivo** e seleziona la carta da utilizzare per il pagamento.
Inoltre, NFC consente di archiviare più carte di debito e di credito sui propri dispositivi mobili, eliminando quindi la necessità di portare tali carte nel proprio portafogli.
La più recente tendenza nell'ambito dei pagamenti contactless è di poter usare app per trasformare un qualsiasi smartphone in terminale per il pagamento, così da semplificare ulteriormente la conclusione del processo di acquisto ovunque i cliente si trovi in negozio evitando code e senza obbligare il retailer a ricorrere a dispositivi dedicati.

PREPARARSI PER ESSERE **RESILIENTI**

di Riccardo Florio

ESSERE RESILIENTI SIGNIFICA PENSARE ALLA PROTEZIONE IN MODO DIVERSO E PASSANDO DA UN PARADIGMA IMPRONTATO A IMPEDIRE LA RIUSCITA DI UN ATTACCO A QUELLO IN CUI SI ACCETTA DI RESTARNE, PRIMA O POI, VITTIMA E SI PUNTA A PREDISPORRE LE MISURE PER RITORNARE ALLA NORMALITA IN TEMPI RAPIDI E COL MINORE IMPATTO SUL BUSINESS. SIGNIFICA ANCHE FOCALIZZARSI SUL TEMA DEL BUSINESS E PREPARARSI PER FRONTEGGIARE LE CONSEGUENZE DI CRISI ENERGETICHE, PANDEMIE, GUERRE E CROLLI FINANZIARI.

I cyber attacchi rappresentano certamente una delle principali minacce per la continuità del busiess aziendale ma non sono l'unica.
L'esperienza degli ultimi anni ha messo in evidenza quanto le aziende, in realtà, non fossero pronte ad affrontare le conseguenze sul business indotte da scenari di crisi come quelli creati da pandemie, guerre, crisi economiche globali. Avere predisposto un piano di disaster recovery, capace di ripristinare le risorse di un data center in caso di terremoto, non è servito a supportare le aziende nel predisporre modelli di lavoro da remoto, a contrastare l'incremento dei costi dell'energia, la carenza di chip e componenti elettronici, la mancanza di grano causata dalla guerra in Ucraina e un mercato azionario colato a picco negli ultimi due anni.
Essere resilienti significa essere preparati.
Esiste una resilienza che potremmo definire "aziendale" che deve occuparsi di tutto che ha impatto sul business e che richiede idonei approcci strategici.
Vi è poi la resilienza informatica o cyber resilienza, in cui il focus è di predisporre le condizioni per cui un'organizzazione possa continuare a operare anche durante un attacco informatico.
Si tratta di un obiettivo che richiede non solo scelte e azioni tecnologiche, ma anche di tipo organizzativo e culturale. Vediamo alcuni spunti.

ALCUNI SPUNTI PER LA CYBER RESILIENZA

- **Proteggersi "fuori casa"** In uno scenario di azienda aperta è essenziale preoccuparsi non solo del proprio livello di sicurezza, ma anche di quello dei partner e dei fornitori a cui un'organizzazione espone le proprie risorse. Ricordiamo, per esempio, l'attacco SolarWinds del 2020 alla supply chain, in cui è stata sfruttata un'applicazione software per attaccare le aziende che la utilizzavano.
- **Proteggere lo sviluppo applicativo** Se il buongiorno si vede dal mattino, la sicurezza delle applicazioni si vede dal momento del loro sviluppo. Predisporre controlli sulle vulnerabilità mentre il codice di un'applicazione viene scritto è un sistema efficace per prevenire compromissioni delle applicazioni.
- **Non fidarsi mai.** Prediligere l'approccio Zero Trust, in base al quale nessun privilegio viene assegnato a priori e se non direttamente legato ai requisiti del proprio lavoro.
- **Proteggere ogni aspetto dell'IT** Dati, software, applicazioni, infrastruttura, sistemi, cloud e IoT. Rafforzare le soluzioni di sicurezza scegliendo tecnologie avanzate, aggiornate costantemente, orchestrate e opportunamente configurate, prendendo anche in considerazione l'opzione di delegare all'esterno la gestione della sicurezza.
- **Predisporre opportune misure di risposta, ripristino e remediation** per riportare la situazione alla condizione normale il prima possibile e col minimo impatto per il business.
- **Creare una cultura di sicurezza** Introdurre all'interno dell'azienda una cultura di sicurezza è un requisito indispensabile per conseguire un elevato livello di cyber resilienza. Come minimo i dipendenti devono essere formati su come identificare le minacce informatiche mirate, considerando che il phishing è il principale metodo di infezione.
- **Restare aggiornati sullo scenario delle minacce** Se non si conoscono il mondo degli hacker, le vulnerabilità e le minacce esistenti, non è possibile predisporre un'efficace gestione del rischio e contromisure adeguate
- **Comprendere i propri processi** Sapere la catena di dipendenza è essenziale per interpretare correttamente le vulnerabilità e le possibili conseguenze della compromissione di un sistema o un processo.
- **Gestire identità e accesso** Un controllo indispensabile che richiede soluzioni automatizzate e sorrette da tecnologie di intelligenza artificiale capaci di analizzare le anomalie di comportamento degli utenti.

PREPARARSI AL RANSOMWARE

Il Ransomware rappresenta, oggi, una delle minacce più diffuse e in rapida crescita. Secondo IDC il numero di attacchi Ransomware al mondo nel 2022 è stato superiore a 600 milioni. Con questi numeri in gioco e considerando che non esiste una tecnologia in grado di prevenire l'agire incompetente e superficiale delle persone, è meglio pensare a come agire quando se ne resterà inevitabilmente vittime anziché credere di riuscire a evitarlo per sempre. Essere resilienti al Ransomware significa intervenire essenzialmente su due aspetti. Poter disporre di una copia "pulita" dei propri dati e di un piano di ripristino alla normalità che possa minimizzare l'impatto sul business. Non è però un compito facile. Spesso il tempo che intercorre tra quando un sistema viene infettato e quello in cui il codice nocivo entra in azione per cifrare i file è molto lungo. Per questo motivo, ripristinare semplicemente una copia di backup potrebbe significare reintrodurre sui sistemi aziendali il malware dormiente. Servono soluzioni tecnologiche specifiche, che sono disponibili sul mercato, pensate per predisporre costantemente copie pulite dei dati e mantenerle in condizioni isolate e inattaccabili e per effettuare azioni efficaci di "remediation".

UNA PIATTAFORMA PER LA **PROTEZIONE DEL CLOUD**

La sicurezza nel cloud è essenziale e richiede un approccio strategico pensato per estendere la protezione a ogni livello, inclusi ambienti ibridi e multi cloud. La risposta a questa esigenza di SentinelOne si chiama Singularity.

di Riccardo Florio

Il 2022 ha dimostrato che il cyber crimine è un'azienda più florida che mai, che continua a investire in nuove tecniche in risposta alle contromisure dei team e dei software di sicurezza e ad aggiornare i metodi e gli strumenti di attacco. Tra i rischi in più rapida crescita, accanto al ransomware, vi sono quelli legati alla rapida diffusione del cloud computing e alla presenza di ambienti ibridi e multi cloud, che richiedono idonee strategie di cybersecurity. *"È essenziale predisporre strumenti innovativi per la difesa dei dati e delle applicazioni critiche che si trovano nel cloud così come dell'infrastruttura sottostante* - osserva **Paolo Cecchi, Regional Sales Director Italy di SentinelOne** -. *Nel cloud possono risiedere informazioni sanitarie personali, di identificazione personale o i dati delle nostre carte di credito, che potrebbero essere sottratti per essere rivenduti o per avviare un attacco ransomware. La maggior parte degli attacchi al cloud può essere ricondotto a tre modalità di accesso iniziale, rispetto alle quali è, pertanto, opportuno adottare opportune misure di protezione."*

I TRE PRINCIPALI VETTORI DI ATTACCO SUL CLOUD

Il primo tipo di vettore di accesso è rappresentato dagli **errori nella configurazione delle risorse** e, nello specifico, delle risorse cloud

Paolo Cecchi, Regional Sales Director Italy di SentinelOne

rese pubblicamente accessibili a Internet. Per esempio, se si utilizza un bucket S3 (contenitore online per gli oggetti archiviati in Amazon S3), un cluster di nodi Elasticsearch o un altro tipo di database cloud e, per errore, lo si configura in modo che sia pubblicamente accessibile da Internet (quando non dovrebbe esserlo), sarà violato in pochi minuti, perché i cyber criminali scansionano continuamente Internet alla ricerca di qualsiasi tipo di risorsa esposta.

Un secondo modo classico in cui le organizzazioni subiscono violazioni nel cloud è la **compromissione delle chiavi di accesso** per accedere agli account cloud. Accanto alle chiavi di accesso costituite dal binomio username/password vi sono quelle dei sistemi di Identity and Access Management per impostare l'accesso in base al ruolo anziché all'utente.

Il terzo rischio più comune che le organizzazioni devono affrontare nel cloud è rappresentato dalle **vulnerabilità delle applicazioni Web** messe a disposizione dai cloud provider, che possono essere sfruttate in vari modi. Per esempio, un'azienda potrebbe sfruttare una versione di WordPress che presenta un plug-in corrotto oppure un modulo della sua applicazione che è suscettibile ad attacchi del tipo "SQL injection".

I RISCHI DEGLI AMBIENTI IBRIDI E MULTI-CLOUD

Nuovi problemi di sicurezza sono posti anche dalla complessità legata ad ambienti ibridi, in cui il cloud pubblico si coniuga con l'esecuzione di applicazioni on-premise, e multi-cloud dove si utilizzano più fornitori di cloud per i carichi di lavoro host come, per esempio, AWS, Google cloud e Azure.

"Un aspetto interessante dal punto di vista della sicurezza - spiega Cecchi - *è* ***sottolineare che gli incidenti informatici possono iniziare in ambiente on-premise e poi spostarsi nel cloud o viceversa.*** *Al momento, direi che la maggior parte delle soluzioni di sicurezza si concentra solo sulla sicurezza del cloud o solo sulla sicurezza on-premise. A causa di questa focalizzazione separata, molte soluzioni non riescono a realizzare il salto tra ambienti on-premise e cloud e questo limita la capacità di comprendere davvero la portata di un attacco o di un incidente. Per garantire una sicurezza efficace è importante ricomporre tutti i "pezzi" in una visione unificata che comprenda sia gli ambienti on-premise sia quelli cloud".*

Un esempio tipico è quello di un utente aziendale che potrebbe, accidentalmente, inserire le proprie credenziali in un sito Web compromesso a seguito di un'e-mail di phishing. L'attaccante potrebbe utilizzare tali credenziali per accedere al suo computer e da lì, utilizzando tecniche di escalation dei privilegi, acquisire credenziali di amministrazione oppure trovare credenziali di amministrazione esistenti sul computer compromesso. Se tali credenziali fossero di amministrazione del cloud l'attaccante potrebbe

anche accedere al cloud e crearsi un proprio account utente a cui assegnare le autorizzazioni necessarie per procedere con ulteriori attività malevoli nel cloud.

SENTINELONE SINGULARITY

Per fornire una risposta efficace a questo tipo di problemi SentinelOne ha sviluppato **Singularity, una piattaforma modulare che fornisce funzionalità di ricerca, rilevamento e risposta alle minacce** unendo, all'interno di un unico flusso di lavoro e di un'unica architettura (che include agenti e piattaforme), funzioni e componenti che solitamente di trovano separate in molteplici prodotti quali: funzioni di previsione, prevenzione, rilevamento e risposta per gli endpoint (anche in modalità gestita); controllo dell'IoT; protezione dei carichi di lavoro; firewall; controllo dei dispositivi; blocco, quarantena e isolamento; inventario delle applicazioni; integrazione; visibilità e controllo della rete.

"Rilevare le minacce è solo la prima parte di una strategia di protezione - sottolinea Paolo Cecchi -. *Servono efficaci misure per rispondere ed eventualmente ripristinare la situazione alla normalità nel caso di attacchi andati a buon fine, nel minor tempo possibile e minimizzando i danni. Questo è ciò che fa la piattaforma Singularity di SentinelOne, che è stata progettata per il SOC e le operazioni IT, capace di proteggere endpoint, carichi di lavoro, ambienti cloud di ogni tipo e dispositivi IoT con protezione, rilevamento e risposta basati sull'intelligenza artificiale"*.

Singularity Cloud è la componente della piattaforma dedicata in modo specifico alla protezione dei carichi di lavoro cloud, capace di combinare ricerca delle minacce con rilevamento e risposta degli endpoint per proteggere anche gli ambienti cloud più complessi. Integra, infatti, funzioni di classe enterprise di rilevamento e risposta in tempo reale per gli endpoint, specificamente progettate per le macchine virtuali AWS, Azure e Google Cloud. Singularity Cloud prevede anche l'implementazione automatica di funzioni per la sicurezza dei container assicurando protezione, rilevamento e risposta per EKS, AKS, GKE e Kubernetes.

L'IMPORTANZA DI PROTEGGERE L'**ACTIVE DIRECTORY**

Semperis promuove un modello di Identity Threat Detection e Response che si focalizza sulla cifratura e sulla garanzia di integrità a livello di Active Directory

di Riccardo Florio

Coley Burke
Chief Revenue Officer di Semperis

Nata in Israele da un programma incubatore di Microsoft, Semperis è un brand recente nello scenario della cybersecurity che si **focalizza su quello che l'azienda definisce Identity Threat Detection e Response (ITDR) per la sicurezza dell'Active Directory in ambienti on-premise e ibridi**.
L'offerta prevede una serie di strumenti per proteggere l'infrastruttura di identity management legata ad Active Directory (AD) in ambienti on premise, Azure e ibridi; si distingue da quella delle molte aziende che operano all'interno del contesto della gestione dell'identità dell'utente finale, proprio per questa focalizzazione sulla componente di infrastruttura dell'identità.
Semperis si indirizza oggi, soprattutto, verso realtà enterprise ma sta ampliando progressivamente la sua penetrazione verso il mercato delle realtà di media dimensione, veicolando le proprie soluzioni tramite operatori del Canale come Avanade e Deloitte.

FOCUS SU IDENTITÀ E INTEGRITÀ

Active Directory non è stata costruita per resistere alle minacce odierne e proteggere sia l'AD on-premise che l'Azure AD in un ambiente ibrido è un compito difficile. Inoltre, gli aggressori spesso si spostano dall'on-premise al cloud (o viceversa) alla costante ricerca di privilegi elevati (come nel caso dell'attacco SolarWinds).

Peraltro, la percentuale delle organizzazioni che migrerà completamente a breve dall'Active Directory on-premise verso un servizio di identità basato sul cloud appare ancora limitato: solo il 3% entro il 2025 secondo il report Active Directory in Transition: Gartner Survey Results and Analysis, pubblicato a ottobre 2021. In linea con questa previsione **il survey realizzato da Semperis "Evaluating ITDR Solutions"** mostra come AD sia un bersaglio di riferimento per i cybercriminali essendo coinvolta nel 90% dei cyber attacchi e come solo il 4% degli intervistati dichiari di non utilizzare AD o Azure AD; il 16% dichiara che l'AD on-premise rappresenta il loro archivio di identità principale e l'80% che utilizza AD on-premise sincronizzato con Azure AD oppure diversi sistemi di identità. Per questo motivo Semperis rimarca come **la protezione della sicurezza dell'Active Directory in ambienti ibridi debba rappresentare un obiettivo prioritario di sicurezza** per le aziende e pone al centro della sua offerta identità e integrità dell'identità di AD. *"Stiamo assistendo a un grande scambiamento nelle aziende rivolto verso un approccio Zero trust* – ha osservato **Coley Burke Chief Revenue Officer di Semperis** – *per riuscire a fronteggiare efficacemente anche le minacce interne. L'identità digitale rappresenta il nuovo perimetro e i sistemi di identità zero trust sono i soli che possono assicurare la protezione degli endpoint. Semperis attraverso il suo approccio all'Identity Threat Detection e Response consente ai team di sicurezza di proteggere gli ambienti ibridi e multi-cloud e di assicurare l'integrità e la disponibilità dei servizi critici per le directory aziendali a fronte di ogni tipo di minaccia. La tecnologia brevettata di Semperis, creata appositamente per la sicurezza dell'Active Directory, protegge le identità da cyberattacchi, violazioni di dati ed errori operativi. Permette di rilevare vulnerabilità delle directory, intercettare i cyberattacchi in corso ed eseguire rapidamente il ripristino delle operazioni in seguito a ransomware e ad altre emergenze che compromettono l'integrità dei dati"*.

I COMPONENTI PER LA SICUREZZA DELL'ACTIVE DIRECTORY

La piattaforma Semperis di Identity Threat Detection e Response è suddivisa in due componenti.

Directory Services Protector (DSP) è la soluzione di sicurezza pensata per impedire ai criminali informatici di accedere ad AD e Azure AD e intercettare e correggere eventuali modifiche illecite.

Permette di effettuare la **valutazione della vulnerabilità**, attraverso monitoraggio continuo degli indicatori di esposizione e di effettuare il **ripristino automatico** creando notifiche sulle modifiche agli oggetti e agli attributi AD sensibili, con l'opzione di annullare automaticamente le modifiche selezionate. Inoltre abilita il **tracciamento AD** per intercettare le modifiche anche se la registrazione di sicurezza è disattivata, se i log di registro sono stati eliminati, se gli agenti sono disabilitati o se le modifiche sono inserite direttamente in AD. Le funzioni di **rollback granulare** consentono di ripristinare le modifiche a qualsiasi punto nel tempo di singoli attributi, membri di gruppo, oggetti e contenitori;

Active Directory Forest Recovery è, invece, la componente di ripristino che permette di effettuare diverse funzioni di ripresa.

Questa componente abilita il **ripristino di AD** su qualsiasi hardware virtuale o fisico, in sede o nel cloud.

Garantisce un **ripristino "pulito"** per prevenire la reintroduzione di rootkit e altre minacce informatiche partendo da un sistema operativo Windows pulito e ripristinando solo ciò che è necessario per il server (controller di dominio, server DNS e così via).

Mette a disposizione funzionalità di **automazione avanzata** dell'intero processo di ripristino, compreso il ripristino e la ri-protezione dei controller di dominio, la ricostruzione del catalogo globale, la pulizia dei metadati e dello spazio dei nomi DNS, la ristrutturazione della topologia del sito e altro ancora.

SEI PREOCCUPATO DEI RISCHI DA ESPOSIZIONE A CAMPI ELETTROMAGNETICI SUL POSTO DI LAVORO O A CASA?

Se preferisci l'approccio scientifico contatta Gaia Consulting & Technologies

Effettuiamo da 20 anni misurazioni di campi elettromagnetici ELF e RF, con approccio scientifico, personale specializzato laureato in Fisica, strumentazione certificata e di livello professionale, verificando il rispetto dei limiti per i lavoratori ai sensi del D.Lgs. 81 e per l'esposizione della popolazione.

CONTATTACI PER UN PREVENTIVO GRATUITO

cem@gaiaconsulting.it

02 24416972

GAIA Consulting & Technologies

www.gaiaconsulting.it

GAIA Consulting & Technologies S.r.l.
Sesto San Giovanni (Milano)

HYBRID WORKING
LA SFIDA TECNOLOGICA

Snom ribadisce l'importanza delle soluzioni di comunicazione aziendale nel lavoro ibrido, capaci di garantire più sicurezza e privacy rispetto al BYOD

Il lavoro ibrido si sta sempre più affermando come **modus operandi irrinunciabile in ambito professionale**. Secondo i dati della società di analisi Statista, ad aprile 2021 il 16,8% dei professionisti italiani stava lavorando in modalità ibrida e il 14,8% da remoto, per un totale di ben 7,3 milioni di persone. Sebbene per il 53,6% dei lavoratori sotto i 34 anni il lavoro da casa fosse causa di disagi per via di postazioni di lavoro sprovviste di un equipaggiamento tecnico professionale, il 62,4% dei lavoratori totali si dichiarava soddisfatto della modalità operativa. Dal 1° settembre 2022, attraverso la legge 81 del 2017, è possibile regolamentare la pratica del lavoro ibrido definendo un accordo individuale tra il dipendente e il datore di lavoro, al fine di ridurre la burocrazia e rendere più agevole questa opzione lavorativa. Il datore di lavoro ha la possibilità sia di fornire al lavoratore gli strumenti di comunicazione necessari oppure di richiedere ai dipendenti di utilizzare i propri dispositivi personali, in accordo al principio BYOD (Bring Your Own Device).
Questa condizione crea una dualità che rende difficile garantire la sicurezza, può sfociare in problemi di privacy e, non in ultimo, creare costi aggiuntivi al dipendente. Nella transizione verso il lavoro ibrido o smart working, le aziende spesso trascurano l'importanza di **adottare dispositivi tradizionali dedicati per la telefonia aziendale che, meglio di quelli privati, possono garantire comunicazioni sicure** e rispettare la privacy dei dipendenti.

Fabio Albanini, *Head of International Sales, EMEA di Snom e Managing Director di Snom Italia*

Snom Technology offre una vasta gamma di terminali cablati e cordless basati su SIP, accessori inclusi, per fornire una connessione affidabile al centralino telefonico, migliorare la sicurezza e, soprattutto, garantire una qualità della voce cristallina per ogni tipo di comunicazione aziendale. La gamma comprende telefoni da tavolo connessi tramite Wi-Fi, terminali IP-DECT, cuffie e speakerphone professionali multiuso nonché soluzioni portatili per conferenze, per un utilizzo flessibile e indipendente dal luogo di lavoro. *"Gli ambienti in cui viviamo la nostra vita privata e professionale si stanno progressivamente aggregando* - commenta **Fabio Albanini, Head of International Sales, EMEA di Snom e Managing Director di Snom Italia** -. *Per questo, spetta a noi offrire soluzioni ottimali che si adattino alla nuova realtà".*

WORKPLACE X BROTHER
STAMPA SU MISURA

Brother mette a disposizione un'ampia gamma di soluzioni di stampa e scansione, abbinati a servizi a valore aggiunto che aiutano i team aziendali a lavorare in modo sicuro, veloce ed efficiente in qualsiasi contesto

di Aldo Cattaneo

Con Workplace X Brother, l'azienda vuole offrire alle aziende delle soluzioni flessibili e di facile implementazione di stampa e scansione, per garantire processi di lavoro sicuri e altamente produttivi, nonché efficienza e velocità, anche grazie al costante supporto che Brother assicura ai propri clienti. La gamma di stampanti e multifunzione adotta, infatti, sia la tecnologia laser sia quella inkjet, fornendo così un'ampia possibilità di scelta agli interessati. Tutti i modelli sono progettati, inoltre, per essere sostenibili e al passo con le nuove esigenze aziendali.

SICUREZZA

Le printer, per esempio, utilizzano tecnologie che garantiscono un **triplice livello di sicurezza**: reti, documenti e dispositivi sono protetti, in modo da dare alle aziende la certezza che i loro asset saranno sempre tutelati. I dispositivi, infatti, sono progettati per monitorare automaticamente qualsiasi attività irregolare sulla rete e arrestare il sistema in caso di rilevamento di processi dolosi, garantendo la **sicurezza dei dati e del dispositivo e impedendo che questo possa essere usato come punto di accesso** alle reti protette.

COSTI SOTTO CONTROLLO

Workplace X Brother permette poi di migliorare la produttività e l'efficienza dei costi attraverso piani di pagamento personalizzati, ottimizzazione dei consumi e monitoraggio continuo di tutte le periferiche di stampa. Grazie a questi servizi, Brother è in grado di creare un ambiente di stampa semplificato e facilmente scalabile, così da essere in grado di **progettare e installare un'infrastruttura di stampa dimensionata sui corretti volumi,** consigliando al tempo stesso il prodotto e la soluzione migliore per la propria attività.

SOSTENIBILITÀ

La sostenibilità è un altro pilastro su cui è stata costruita l'offerta Workplace X Brother: questa viene ottenuta grazie a prodotti efficienti, durevoli nel tempo, che dispongono di funzioni di risparmio energetico e che sono progettati per essere riparati con una idea di economia circolare. La modularità del design dell'hardware, infatti, agevola l'approvvigionamento e la sostituzione delle singole parti, e ciò contribuisce **a estendere la vita utile dei prodotti e a realizzare gli obiettivi di riduzione dei rifiuti dei clienti.** Anche per questo le cartucce sono totalmente riutilizzabili o riciclabili, garantendo l'azzeramento dei rifiuti conferiti in discarica.

UNA GAMMA COMPLETA

Sicurezza, servizi a valore aggiunto e sostenibilità si appoggiano ad una gamma completa di soluzioni. È possibile scegliere, per esempio, uno dei modelli di **stampanti laser a colori professionali**, che garantiscono una velocità di stampa fino a 40 ppm, vassoi di alimentazione da 520 fogli, un toner con durata fino a 15.000 pagine e un lettore NFC integrato.
Nell'offerta di printer laser a colori, Brother ha previsto anche una linea per le aziende che abbinano elevate velocità di stampa con minima manutenzione a materiali di consumo di lunga durata, per assicurare operatività e produttività senza interruzioni.
Rimanendo nell'offerta con tecnologia laser, Brother, con **stampanti e multifunzione monocromatici**, mette a disposizione una serie di prodotti pensati per chi ha necessità di produrre elevati volumi di stampa e di raggiungere altissime velocità, con dispositivi che richiedono una minima manutenzione, con anche una gamma progettata per i gruppi di lavoro.
Brother peró vuol dire anche **tecnologia inkjet**: una linea di printer a getto d'inchiostro pensata per le aziende che stampa a colori, anche in formato A3, con elevata qualità e con la massima attenzione alla riduzione del consumo energetico e delle emissioni. La famiglia Workplace X Brother si completa infine con un'ampia offerta di **scanner desktop per documenti,** che aiutano a velocizzare i processi aziendali offrendo un'esperienza semplice e intuitiva, in spazi ridotti.
Workplace X Brother è il frutto della lunghissima esperienza che Brother ha maturato nel settore della stampa, e della profonda conoscenza degli ambienti aziendali, delle loro esigenze e della loro costante evoluzione.

TECNOLOGIE RESPONSABILI PER FARE BUSINESS IN UNA SOCIETÀ CHE CAMBIA

Accanto a giusti obiettivi di contenimento costi, le imprese iniziano a guardare allo sviluppo e alla proposta tecnologica secondo modelli di maggiore responsabilità. Una recente ricerca del MIT Technology Review Insights descrive quanto le aziende percepiscano oggi la criticità di una società in cui le tecnologie presidiano e guidano ambiti sempre più delicati e complessi.

di Stefano Uberti Foppa

Il concetto di "Tecnologia responsabile", come sta avvenendo per le strategie di sostenibilità ambientale, va ormai oltre il solo aspetto etico. **Un approccio responsabile alla tecnologia, alla sua implementazione e utilizzo genera, infatti, nuovo valore, potenziale sviluppo di business, considerazione e fidelizzazione da parte degli utenti** e conseguenti margini di crescita.

Ma cosa significa oggi seguire percorsi di innovazione tecnologica ponendo attenzione agli impatti che questa può avere su persone, benessere individuale e sociale?

Come sviluppare il business attraverso una digitalizzazione che rispetti valori e avvenga attraverso l'uso di pratiche responsabili?

Quanto e in quali modalità i business leader oggi stanno implementando policies, modelli e strategie che concretizzino obiettivi di sviluppo tecnologico responsabile?

LA RICERCA DEL MIT

Una ricerca realizzata dal **MIT Technology Review (azienda media indipendente fondata dal Massachusetts Institute of Technology)** in collaborazione con la società di consulenza tecnologica internazionale **Thoughtworks**, illustra quanto le aziende percepiscano oggi la criticità di una società in cui le tecnologie presidiano e guidano ambiti sempre più delicati e complessi, dalla medicina alla finanza, dalle infrastrutture critiche a una digitalizzazione diffusa in tutti i settori di mercato e sia a livello sociale sia individuale, con impatti continui sulle nostre interazioni quotidiane.

> INTEGRARE TECNOLOGIA, CULTURA E VALORI UMANI GARANTENDO MASSIMA INCLUSIVITÀ FA BENE ANCHE AL BUSINESS

Accanto quindi a giusti obiettivi di contenimento costi, **le aziende iniziano a guardare allo sviluppo e alla proposta tecnologica secondo modelli di maggiore responsabilità,** sia nell'utilizzo interno aziendale sia nell'offerta sul mercato, per evitare contraccolpi sul fronte normativo, ridurre criticità nel rapporto con i propri clienti, attrarre nuove competenze e talenti, creare modelli che supportino un nuovo sviluppo di business.

Tra luglio e agosto 2022 sono stati coinvolti per questa indagine **550 senior executive e direttori di aziende operanti nei principali settori merceologici, a livello mondiale con fatturati annuali di almeno 500 milioni di dollari.** Sono inoltre state effettuate interviste approfondite a responsabili di tecnologia all'interno di un significativo panel di aziende utenti del campione oltre ad esperti di gestione dati, data ethics, digital privacy, matematici, CTO, analisti delle strutture degli algoritmi, realtà aumentata e intelligenza artificiale.

UNA SENSIBILITÀ AL TEMA MOLTO ALTA

Definire il concetto di tecnologia responsabile non è banale. Può considerarsi l'insieme di **elementi tecnologici hardware, applicazioni**

software e prodotti analogici diventati smart, integrato con riferimenti culturali e valori umani rispettosi di alcuni aspetti oggi vitali nell'utilizzo digitale (per esempio, la protezione dei dati e la privacy), **favorendo la massima inclusività.**

In questo sviluppo tecnologico è, pertanto, essenziale evitare che vi siano velocità diverse di accesso, potenziali discriminazioni, condizionamenti occulti, vantaggi e svantaggi intrinseci alla struttura stessa del prodotto e alla sua diffusione, in modo che garantisca un utilizzo ottimale anche sul piano etico. Non semplice!

A oggi le aziende, prima di tutto per salvaguardarsi, vedono in un utilizzo tecnologico rispettoso di quanto definito dalle normative il proprio riferimento primario (59%) ma è importante notare come la sensibilizzazione su questo tema sia già molto alta in chiave di sviluppo business: per il 73% del campione l'importanza assegnata a questo tema in un futuro prossimo è analoga agli aspetti di business o finanziari **(fig. 1)**.

Più di un utente ritiene, infatti, che **la guida normativa non sia sufficiente** a garantire che i processi di implementazione e diffusione tecnologica assicurino un pieno rispetto etico e non nascondano, anche inconsapevolmente, elementi di discriminazione.

LE RAGIONI PER UN APPROCCIO TECNOLOGICO RESPONSABILE

Ma quali sono le principali motivazioni delle aziende nel perseguire un approccio responsabile alle tecnologie?

Ben il 52% lo vede come il driver primario per **migliorare la percezione della propria azienda sul mercato.**

Segue la motivazione di **essere sempre più attrattivi per investitori e partner** (49%) e dalla possibilità (43%) di riuscire a innescare un "circolo virtuoso" con il mercato che consenta di **sviluppare prodotti sempre più inclusivi e adatti ai propri clienti.**

Considerando il livello "executive" dei rispondenti, si può quindi desumere come questo tipo di approccio possa già oggi essere potenzialmente attuato dai business leader per indirizzare verso obiettivi di inclusività, tecnologie responsabili e sostenibilità le proprie strategie aziendali.

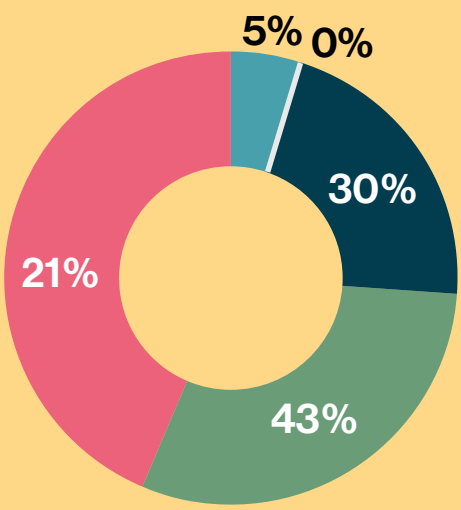


Fig. 1 La tecnologia responsabile diventerà un fondamentale aspetto del business

Source: MIT Technology Review Insights survey, 2022

Interessante sottolineare un importante aspetto psicologico che riguarda le giovani generazioni in ingresso oggi nel mondo del lavoro: esiste, oltre alle giuste aspettative economiche, **un idealismo legato alla partecipazione alla mission dell'azienda per cui si lavora,** dove non solo il tema del profitto e

Fig. 2 Best practice delle tecnologie responsabili

Source: MIT Technology Review Insights survey, 2022

del business viene considerato predominante. Per esempio secondo Linda Leopold, responsabile dell'area AI & Data di **H&M Group**, testimonial citata nel Report: *"Una AI etica unita a modalità corrette sono oggi uno dei fattori attrattivi per giovani talenti e devono essere diffuse dal basso all'interno delle organizzazioni, garantendo globalmente lo stesso livello di priorità di utilizzo"*.

Ralf Sigmund, responsabile tecnologico di **Moia**, un'azienda tedesca che si occupa di mobilità condivisa dice: *"Abbiamo circa 217 persone che lavorano al disegno, sviluppo e produzione di servizi in Moia; tutti hanno accettato il lavoro soprattutto per essere parte di una mission che vede la tecnologia come strumento per cambiare e migliorare lo stato delle cose"*.

Una priorità che viene confermata dalla quarta voce di scelta dal campione per motivare l'adozione di uno sviluppo tecnologico responsabile: ben il 42% ha l'obiettivo di **rafforzare la fidelizzazione dei propri dipendenti e mantenere alto l'interesse dei propri talenti.**

ATTENZIONI, RISCHI E PROBLEMI

Il tema delle tecnologie responsabili non è filosofico bensì si concretizza in una serie di "practice" ben precise da seguire per evitare una serie di problemi e il raggiungimento di determinati obiettivi di cui le imprese sono ben consapevoli **(fig. 2)**.

Tra le priorità da dare a queste tecnologie vi è ad esempio un disegno che garantisca **accessibilità semplice e inclusività (57%), rispetto di data privacy e security, sostenibilità ambientale** e, interessante da notare in relazione alla diffusione di tecnologie smart sempre più embedded nei prodotti, **l'eliminazione dei "bias" negli algoritmi di Intelligenza Artificiale**, cioè di tutte quelle potenziali discriminazioni che i sistemi di machine learning all'interno di soluzioni di AI, possono autonomamente determinare nella correlazione e apprendimento di determinati data set, indipendentemente dalla volontà di chi ha inizialmente progettato il sistema.

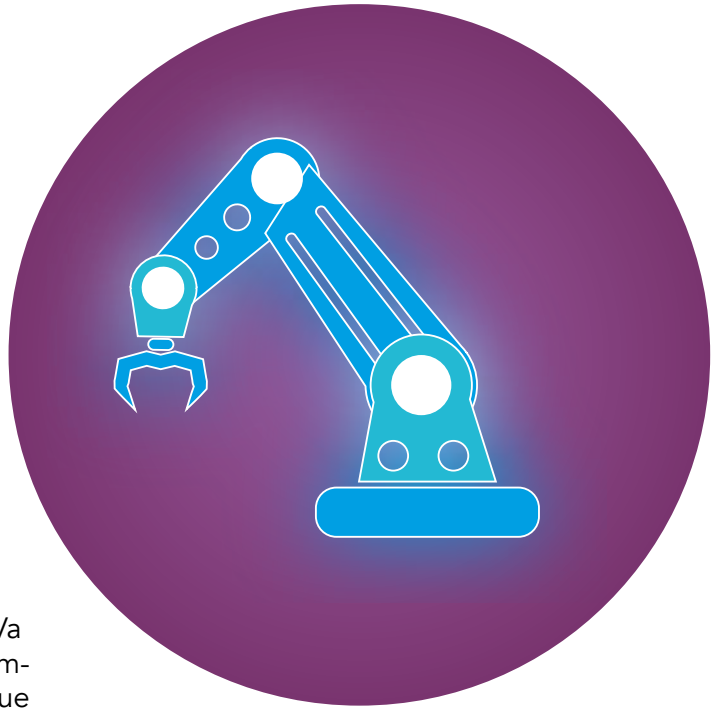
Un accenno, infine, ai problemi che, in questo caso, sono spesso di natura più sfumata e che devono essere affrontati secondo prospettive più ampie, di tipo culturale, soprattutto.

Ecco infatti, come voce primaria nelle barriere da superare per lo sviluppo di tecnologie responsabili, la **mancanza di consapevolezza** nei livelli senior delle organizzazioni aziendali (52%), una **resistenza al cambiamento** che potremmo definire strutturale a ogni processo di innovazione (46%) e la scarsa attenzione alle tecnologie responsabili (35%).

DALL'INDUSTRY 4.0 ALL'**INDUSTRY 5.0**

IL CORONAVIRUS È STATO UNO STRESS TEST MOLTO FORTE SULLA STRADA DELLA TRANSIZIONE ENERGETICA. ALL'INTERNO DELL'ENERGIA TROVIAMO ALTRE FACCE DELLA STESSA MEDAGLIA: INFORMATIZZAZIONE (DIGITALE), ROBOTICA (COBOT, INTELLIGENZA ARTIFICIALE, DIGITAL TWIN), AMBIENTE (CON INFILTRAZIONI DALLE ENERGIE FOSSILI), NUOVO MERCATO DEL LAVORO.

di Leo Sorge



Il concetto di industria 4.0 nasce in Germania nel 2011, in un documento del Fraunhofer Institut, che riguardava esclusivamente la situazione tedesca. Il quadro generale ha fatto presa un po' ovunque nel mondo e quindi sono stati varati piani analoghi in Cina, negli States, in altri Paesi europei. Insieme ad altri programmi ha fornito, con differente penetrazione, un rinnovamento che potesse irrobustire le fondamenta di una nuova economia. Va sempre ricordato che per le Nazioni che li implementano questi piani generano comunque un debito diretto e una ridefinizione del valore complessivo.

IL 5.0 IN UNIONE EUROPEA

Nel 2022 l'Unione europea ha iniziato a diffondere il progetto Industria 5.0. Presentato come un complemento del precedente 4.0, il progetto aumenta la competitività delle organizzazioni che riescono ad adottarlo. Il piano di riferimento propone delle azioni concrete incentrate esclusivamente sulla forma mentis europea, con democrazia, diritti e competitività dati per scontati mentre non lo sono assolutamente.

"Per rimanere il motore della prosperità", dice il documento, "l'industria deve guidare le transizioni digitale e verde". Che l'Europa sia oggi motore della prosperità è tutto da dimostrare: pensando ai mercati dell'energia, della mobilità, dell'industria, dei chip, del cloud (e più in generale del software) i nostri governanti sembrano invece in una fase di affannoso inseguimento di benessere, lavoro ed introiti fiscali per troppo tempo lasciati ad altre macroaree.

L'industria 5.0 può però rappresentare un punto di svolta, permettendo che produzione e lavoro tornino sul nostro territorio. La forma che prenderanno sarà diversa da quella alla quale siamo abituati, perché la trasformazione è in atto ed è forte. "Questo approccio", continua il documento UE, "fornisce una visione dell'industria che va oltre l'efficienza e la produttività come unici obiettivi e rafforza il ruolo e il contributo dell'industria alla società".

IL LAVORO DEL FUTURO E LA GESTIONE DEL TALENTO

Oltre alla valenza tecnica, con Industria 5.0 si cerca di governare un cambiamento anche sociale per la conservazione delle risorse tramite filiere corte, locali e circolari, in un forte cambiamento climatico e alla ricerca della stabilità sociale attraverso un diverso ciclo di gestione dei talenti (lavoro, formazione, smart working). Inoltre l'intero sistema viene reso più resistente all'attacco di pandemie delle quali il Covid-19 potrebbe essere stato solo l'avanguardia.

La situazione mondiale varia in maniera molto più impegnativa di quanto previsto dall'Unione europea: non solo quando generò le 6 priorità del piano 2019-2024, ma anche e soprattutto quando fu formulato il Recovery Plan for Europe, ispirato dal Covid-19, con il piano 2021-2027.

DIGITAL TWIN
il processo in tempo reale

Ogni nuova ondata tecnologica richiede un vocabolario comune per i termini più usati. "Digital twin" è un termine già noto da tempo, sul quale quindi esiste un ampio consenso. Questo termine viene usato in molti diversi modi, per scopi di controllo in tempo reale e di simulazione di modifiche di flusso. La sua adozione richiede un assessment molto più dettagliato di quello che di tanto in tanto viene proposto dai fornitori ICT e mal digerito dalle aziende. Al di là dei nomi, avere la completa descrizione digitale della produzione in tempo reale è un risultato straordinario che possiamo chiamare "modello informativo del digital twin". Il punto centrale è nella qualità e sintesi dei dati veramente utili.

FILTRARE IL RUMORE DAL SEGNALE UTILE

Oggi le componenti utili di qualsiasi flusso lavorativo sono sommerse in un enorme rumore di fondo fatto di dati mal raccolti, inutili e dannosi. Filtrare le componenti utili richiede una mentalità nuova per identificare i dati effettivamente rilevanti, in genere sommersi da infinite inefficienze affastellatesi nel tempo. È certo molto scenografico, poi, visualizzare il twin in modalità grafica, ma si tratta di una funzionalità generalmente poco significativa. Se nella rappresentazione digitale si inserisce anche un'area, il digital twin viene meglio definito spatial twin, gemello spaziale. Il gemello promette dei miglioramenti operativi che consentano di migliorare le prestazioni del prodotto o l'efficienza del processo.

INFORMATIVO, DIGITALE, FISICO

Organizzativamente parlando, per sviluppare un digital twin si applicano sempre le stesse tre componenti: definizione digitale dell'aspetto fisico, esperienza fisica acquisita digitalmente e modello informativo. La definizione digitale dell'aspetto fisico si occupa della configurazione del gemello, generalmente generata da CAD, PLM, ALM e altre fonti di dati di progettazione. L'esperienza fisica acquisita digitalmente descrive la sequenza temporale delle attività del gemello, come eventi, istantanee IoT e procedure eseguite. Ambiente ed eventi vengono analizzati attraverso un modello informativo, che guida un percorso basato su ruoli e attività. In alcuni casi per la stessa attività servono più twin, ad esempio per le attività in prima linea e per l'analisi della flotta, nel qual caso è il modello informativo a guidare le due analisi ed integrare i risultati relativi. Parametric Technology Corporation (PTC), società statunitense di digital transformation ed industria 4.0, ha definito con precisione il concetto di digital twin in gran parte riportato in questo articolo. PTC ha anche proposto un'indagine sul modello statunitense. I risultati sono molto interessanti. Nel 2022, i progetti di digital twin sono stati per lo più (86%) un investimento ad alto costo, da oltre 1M$/y per azienda. Probabilmente, queste aziende sono ancora solo nella fase di sviluppo di ricerca e sviluppo e semplicemente non hanno raggiunto gli alti costi associati all'approvvigionamento dei dati, alla modellazione dei dati e alla democratizzazione dei dati. Il lato positivo, tuttavia, è che una volta che i gemelli digitali sono operativi, possono e produrranno un ritorno sull'investimento (ROI) positivo.

La **RIVOLUZIONE** delle operazioni

Il modello 5.0 ha come obiettivo una nuova gestione dei processi. La tradizionale distinzione tra IT e OT sta subendo una forte disruption già da molti anni, arrivando a comprendere il tempo reale e la coesistenza tra robot ed umani.
Attraverso la raccolta di big data da fonti informatiche e da sensori si può operare sia su base storica, sia in tempo reale, con quest'ultima modalità a rappresentare il nuovo paradigma. Le operations sono quindi diventate un concetto fluido.

L'AUTOMAZIONE DELL'AI

Il concetto di tempo reale non vive forzatamente nell'ambito di 1-10 microsecondi, ma va adattato al tipo di necessità. Si può operare in tempo reale a distanza breve (private 5G, edge e non cloud computing) e maggiore (satelliti, cloud). Il sistema complessivo può essere automatizzato ed ottimizzato grazie all'AI.
Allargando lo sguardo, si nota che maggiore è la tecnologia generale, più potenti sono gli attacchi informatici; all'aumentare dell'interconnessione e della virtualizzazione, la cybersecurity richiede reazioni in pochi millisecondi, quando non proattivamente attivate.

SPAZI PER UOMINI E COBOT

L'industria 5.0 integra uomini e macchinari. Già conosciamo magazzini, fabbriche e agricoltura migliorati da robot, droni e veicoli autonomi, sistemi già noti, mentre cresce l'uso dei cobot, collaborative robot, che si alternano con gli operatori umani in uno stesso spazio, spesso angusto.

Questa organizzazione del lavoro promette di rendere resistenti a pandemie, inquinamento e mutazioni sociali. Analogamente, l'adozione del 5.0 aumenta le probabilità di successo e di durata delle organizzazioni.
In ciascuno di questi elementi è quindi evidente la centralità delle operations, ormai fluide. Abbiamo già visto negli ultimi dieci anni l'enorme rimescolamento di IT ed OT nella sorridente rivoluzione dei DevOps e del modello agile, quell'approccio iterativo infinito che sotto sotto dovrebbe essere il motore dell'industria 5.0. Questo approccio è già passato all'automazione ottenuta tramite intelligenza artificiale, quell'AiOps oggi essenziale anche nella cybersecurity già ristrutturata dai DevSecOps.

ATTENZIONE AI CHIP

Già il 5G, nell'attuale versione, rende le celle dei data center con blade server ed AI a bordo. Nel 5G sembra configurarsi il rischio di una forte incidenza di celle 5G private, ad uso delle singole aziende e non inserite nella rete nazionale ed internazionale.
Nelle reti satellitari l'Europa è forte nella sensoristica ma debole nella trasmissione dati, dove gli statunitensi sono avanti. Nella produzione di chip, affidata a Taiwan e Sud Corea, il reshoring europeo sembra meno potente di quello statunitense, in attesa di quello giapponese (partito con l'iniziativa Rapidus) e delle mosse della Cina (e più in là anche dell'India). Senza chip, ricordiamolo, non c'è IT.

IL LAVORO COME LO CONOSCIAMO OGGI HA UN FUTURO?

Automatizzare è importante, ma se si automatizza tutto si sceglie una strada che non permette di distinguersi dalla concorrenza. Meglio puntare su una sinergia virtuosa tra Intelligenza artificiale ed estro umano.

di Primo Bonacina

Una delle caratteristiche salienti del contesto imprenditoriale degli ultimi anni è stata la necessariamente accresciuta attenzione delle aziende verso i dipendenti. La loro salute, i loro valori e le convinzioni, le loro capacità di essere performanti, le loro preferenze su quando, dove e come lavorare, sono fattori saliti a livello di importanza nelle agende dei manager.

Però, con le segnalazioni di riduzioni della forza lavoro ormai all'ordine del giorno - Salesforce, Amazon e Goldman Sachs sono tra coloro che hanno recentemente annunciato significativi tagli - vale la pena di chiedersi: la preoccupazione delle aziende per i desideri e il benessere dei dipendenti diminuirà con l'aumentare della debolezza del mercato del lavoro?

Un nuovo rapporto appena pubblicato da Deloitte (2023 Global Human Capital Trends) offre una nuova visione sul motivo per cui il cambiamento potrebbe essere inferiore a quanto suggerito dalla brutale economia di mercato. Secondo Deloitte, **è proprio la natura e forma fondamentale del lavoro che sta cambiando** e, di conseguenza, le organizzazioni dovranno abbandonare l'illusione di poter avere un controllo completo poiché i lavoratori assumeranno sempre maggiore influenza e responsabilità per i risultati organizzativi e sociali.

Al centro di questo cambiamento, afferma il report, c'è un

allontanamento dalla nozione di lavoro (ruolo), inteso come insieme predefinito di responsabilità funzionali assegnate a un lavoratore. Ciò aveva senso in un momento in cui il cambiamento era lento e i lavoratori erano come ingranaggi di una macchina industriale. Ma, nel mondo di oggi, comincia a imporsi un approccio basato sulle competenze nella gestione del lavoro e dei lavoratori. Un grado di autonomia e flessibilità molto più elevato è essenziale affinché le aziende producano il massimo valore. In estrema sintesi: il lavoro non lo fa più chi era preposto a farlo (parola chiave: ruolo) bensì chi ha gli skill per farlo (parola chiave: competenze).
La variazione non è banale.
Oggi come oggi …

- Chi deve registrare una fattura? Il contabile!
- Chi deve installare il PC? Il tecnico IT!
- Chi deve supportare un'azienda in una causa? Il legale!

Tutti ragionamenti basati su ruoli. Ma magari il legale in azienda non c'è e ci si rivolge a un avvocato esterno. Magari il tecnico IT in azienda non c'è e ci si rivolge a un service provider. Magari il contabile c'è però le fatture vengono automaticamente registrate dal sistema ERP e il contabile fa *controllo di gestione (quindi un task più pregiato rispetto al pedissequo inserimento di una fattura).* E magari non è più necessaria una divisione dei ruoli così rigida. Anche perché, con il cambiare delle esigenze dell'azienda e del mercato, le organizzazioni sono in continua turbolenza e riorganizzazione, che è pratica in sé molto costosa in quanto riorganizzare vuol dire raddrizzare una barca che sta andando fuori rotta, il tutto con gran dispendio di energie.
Una delle conclusioni più interessanti del rapporto di Deloitte è che mentre la maggior parte dei CEO delle grandi aziende americane riconosce la necessità di questo cambiamento (il 93% dei leader aziendali intervistati concorda sul fatto che un allontanamento dall'attuale struttura del lavoro è importante per il futuro successo delle organizzazioni), solo il 20% di loro crede che loro stessi e le loro aziende siano pronti ad affrontarlo. Insomma, la reinvenzione del lavoro è davvero agli inizi.
Potete trovare il report in rete ma le idee che vorrei qui far passare sono soprattutto 3:

1. Il ruolo dei dipendenti nell'equazione del valore aziendale sta aumentando. Una temporanea recessione economica può causare alcuni cambiamenti a breve termine nel rapportarsi delle aziende con i dipendenti. Ma a lungo termine, l'effettivo coinvolgimento del personale, sfruttando al massimo le sue competenze e disponibilità, non farà che aumentare di importanza e diventerà fattore chiave del successo aziendale. Parliamo quindi di skill matching, formazione, recruiting, onboarding, retention, piani incentivi (il tema è davvero ampio!)
2. In un mondo che cambia, il lavoro lo fa chi sa (o ha l'inclinazione per) farlo, non sempre e solo chi è preposto a farlo. Questo richiede uno sforzo organizzativo non banale. Anche e soprattutto per avere in casa o nel proprio perimetro di partnership le giuste competenze, quando e come servono. E per liberarsi, purtroppo, delle risorse che non servono più
3. In un mondo che cambia, la flessibilità è sempre una chiave vincente, sia a livello tattico (tenersi flessibili aiuta a rispondere meglio ai cambiamenti), sia strategico (nessuno è in grado di predire tutti i cambiamenti). Stare (ed essere organizzati per essere) flessibili aiuta a rispondere agli accadimenti, siano essi a impatto positivo o negativo

Tre concetti chiave, forse non facili da digerire subito.

VERTIV.

Architects of Continuity™

Soluzioni power e cooling per garantire continuità operativa alle infrastrutture digitali critiche.

Scopri di più su:

Vertiv.com/ChiSiamo

brother
at your side

WORKPLACE X BROTHER

Soluzioni di stampa su misura per la tua azienda

Negli odierni luoghi di lavoro si fa sempre più affidamento sulla tecnologia. I team accedono rapidamente alle informazioni e le condividono come mai prima d'ora.

La tecnologia connessa, però, ha portato a crescenti sfide per la sicurezza aziendale. Per soddisfare le nuove esigenze di Security, i dispositivi Brother forniscono un triplice livello di sicurezza: proteggono i dispositivi di stampa, assicurano la riservatezza dei documenti e impediscono agli hacker di accedere alle reti.

Inoltre, Brother aiuta le aziende ad ottimizzare l'infrastruttura di stampa, offrendo visibilità e controllo dei costi, anche per le configurazioni più complesse.

Infine, Brother sviluppa prodotti efficienti e durevoli dotati di funzioni di risparmio energetico. I toner sono totalmente riutilizzabili o riciclabili, garantendo l'azzeramento dei rifiuti conferiti in discarica. Insieme ai nostri Partner e ai nostri Clienti perseguiamo un futuro più sostenibile, a zero emissioni.

Questo è il Workplace X Brother

Scopri le soluzioni Brother per la tua azienda

brother.it