

DIRECTION

LE TECNOLOGIE CHE MUOVONO IL BUSINESS



THE INTERNET OF THINGS

SPECIALE IOT

LE SOLUZIONI IOT PER
LA TRASFORMAZIONE DI
VODAFONE BUSINESS

SECURITY

RAFFORZARE
L'IDENTITÀ CON
SEMPERIS

SECURITY

LA BANCA SCEGLIE
FORTIFY PER AVERE
UN **CODICE SICURO**



Architects of Continuity™

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

Scopri di più su:
Vertiv.com/ChiSiamo



INDICE

5 Editoriale

IT e OT due mondi che convergono

6 Business

Axiant: Performance management per le strategie di business

8 SPECIALE IOT

Internet of Things. Tutto pronto per connettere il mondo

IOT: più sicurezza per conquistare il mercato

Per i servizi IOT la connettività sarà senza confini

L'Edge computing, chiave per soluzioni IOT efficienti

Le soluzioni IOT per la trasformazione di Vodafone Business

20 MERCATI VERTICALI

PA e formazione? Una piattaforma per ogni campanile

Proiezioni e interventi per la PA prossima ventura

La PA punta sul public cloud

27 Tecnologie

Il Quantum Computing italiano è una questione di fisico

30 Security

Il tuo sistema di identità è sicuro? Le indicazioni di Semperis

32 La banca sceglie Fortify per avere un codice sicuro

35 La sicurezza ha bisogno di competenza

38 Il settore energetico chiede cybersecurity

40 SCENARI

Digitale e sostenibilità: risparmio con sviluppo del business

45 Riflessioni

Il digital divide generazionale

47 La Striscia IF by Errefe

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

DIRECTION

Anno XXI - numero 124

Giugno 2023

Direttore responsabile: Riccardo Florio

Coordinamento editoriale: Paola Rosa

Ha collaborato: Primo Bonacina, Aldo Cattaneo, Maurizio Ferrari, Leo Sorge, Stefano Uberti Foppa

Immagini: Dreamstime.com

Redazione: Via Gorizia 35/37 20099 Sesto San Giovanni (MI);

Tel 02 24304434; <https://reportec.it>; redazione@reportec.it

Stampa: A.G. Printing Srl Via Milano 3/5; 20068 Peschiera Borromeo (MI)

Editore: Reportec Srl; C.so Italia 50 20122 Milano

Amministratore unico: Riccardo Florio

Iscrizione al tribunale di Milano n° 212 del 31 marzo 2003

Diffusione cartacea + digitale 32.500 copie

Tutti i diritti sono riservati

Tutti i marchi sono registrati e di proprietà delle relative società

bizzIT.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/>



IT E OT

DUE MONDI CHE CONVERGONO

di Riccardo Florio

• direttore responsabile •

Information Technology (IT) e Operational Technology (OT) rappresentano due mondi che sono rimasti a lungo tempo separati e che comprendono l'uso di hardware e software con caratteristiche e requisiti specifici. La tecnologia operativa si occupa di monitorare e controllare processi fisici, macchinari e infrastrutture in ambito industriale mentre l'informatica sovrintende prevalentemente la riservatezza, l'integrità e la disponibilità di sistemi e dati. In passato, gli ambienti industriali non sentivano l'esigenza di interagire col mondo esterno; i macchinari erano tipicamente di tipo proprietario, con software di controllo sviluppati ad hoc dal produttore e molto poco versatili. Anche i dati acquisiti si limitavano allo specifico dispositivo e si muovevano su una rete che non era connessa a Internet. Tutto ciò è cambiato e sta cambiando sempre più. A richiedere una progressiva convergenza tra le reti IT e OT concorrono i temi della trasformazione digitale, la progressiva affermazione di modelli di produzione basati sui dettami dell'industria 4.0, la crescente diffusione dell'IoT e i recenti progressi dell'intelligenza artificiale. I dati, acquisiti e analizzati, diventano sempre più elemento indispensabile per ottimizzazione ed efficienza e per abilitare decisioni automatizzate in processi sempre più interconnessi che escono al di fuori dell'ambiente di produzione: sistemi di approvvigionamento, manutenzione predittiva, interazione tra produzione e logistica, efficientamento energetico basato su intelligenza artificiale, ottimizzazione dei consumi

di materie prime, sicurezza dei lavoratori, interazione tra ritmi di produzione e marketing, smart building e altro ancora. Uno dei temi tecnologici a maggior impatto nella convergenza tra reti OT e IT è quello della sicurezza perché l'ambito OT, che in passato era sostanzialmente isolato, oggi è anch'esso esposto alle minacce esterne e ai cyberattacchi. Le tecnologie OT sovrintendono ad ambiti quali il controllo delle infrastrutture critiche (acquedotti, linee di fornitura energetica, sistemi di controllo del traffico aereo e così via) e, di conseguenza, la portata degli effetti legati a un attacco andato a buon fine in ambito industriale potrebbero avere esiti devastanti e portata molto ampia. Per questo motivo, oggi, le soluzioni di sicurezza OT comprendono un'ampia gamma di tecnologie di sicurezza condivise con il mondo IT. A questa convergenza tecnologica deve, però, fare seguito anche una convergenza delle professionalità che si devono occupare della loro gestione. Infatti, i responsabili IT che si occupano dell'infrastruttura di rete e dei data center non dispongono di conoscenze specifiche sul mondo OT che è stato finora appannaggio di figure specializzate quali i direttori di stabilimento, il personale addetto alla manutenzione degli impianti e gli ingegneri addetti alla produzione; figure che, a loro volta, non sono mai state specializzate in informatica. Forse è presto per parlare di nuove professionalità, ma sicuramente non lo è per un'estensione e una ridefinizione degli ambiti di competenza.



PERFORMANCE MANAGEMENT PER LE **STRATEGIE DI BUSINESS**



Marcello Visalli, *Leader della Business Unit Stream di Axiante*

Le aziende necessitano di dati per analizzare le performance e pianificare lo sviluppo. Il Corporate Performance Management (CPM) offre soluzioni per gestire e analizzare le informazioni aziendali, favorire una cultura del dato e migliorare l'efficienza dei processi.

di Marcello Visalli

Più dati, più informazioni. Per restare competitive sul mercato e crescere in modo sostenibile, le aziende hanno bisogno di dati che le aiutino ad analizzare le proprie performance e a pianificare le future strategie di sviluppo. Gestire una così ampia mole di informazioni però



non è semplice, soprattutto quando si tratta di organizzazioni di grandi dimensioni.

Complice la scarsa cultura finanziaria di filiali e finance team periferici, sono molte le aziende, soprattutto se gestite in un'ottica di gruppo, che faticano ad acquisire i dati necessari per le attività di consolidation reporting, pianificazione e budget.

Al crescere dell'azienda, cresce infatti anche la complessità gestionale. Nei processi di acquisizione, sistemi dati sorgenti e regole di contabilità sono spesso differenti per ciascuna realtà produttiva e, a ridosso di scadenze mensili o trimestrali, il fattore tempo amplifica le difficoltà di reperimento dei dati.

Anche in assenza di una crescita improvvisa, i modelli di business cambiano nel tempo e con essi anche i dati operativi e finanziari necessari a misurare tali modelli.

Per orientarsi in uno scenario sempre meno prevedibile, ogni organizzazione ha bisogno di avere informazioni dettagliate e aggiornate sull'andamento dei dipartimenti aziendali e di poterle analizzare in maniera semplice e veloce. Ecco perché sta aumentando l'interesse delle organizzazioni nei confronti delle soluzioni di **Enterprise o Corporate Performance Management (CPM)**, costituite da un unico applicativo su cui confluiscono tutti i dati, le pianificazioni e i documenti funzionali a monitorare e gestire le performance aziendali per tutte le linee di business.

IL RUOLO DEL CPM PER SVILUPPARE UNA NUOVA CULTURA DEL DATO

Avviare un progetto di Corporate Performance Management non significa solo dotarsi di nuovi strumenti tecnologici, ma sviluppare all'interno delle aziende una cultura finanziaria nuova. È quella che in Axiante chiamiamo "intelligent finance": grazie a una piattaforma innovativa, flessibile e scalabile, è oggi possibile portare dentro a un unico database tutte le informazioni necessarie, di alto livello e di dettaglio, per supportare le decisioni operative.

In questo modo il finance team è libero dalla gestione delle anagrafiche e dal lavoro più amministrativo e può concentrarsi sull'analisi dei dati, per fornire al management le informazioni utili a pianificare investimenti e mettere in campo nuovi progetti. I tempi di sviluppo sono molto brevi: superate la prima fase di adeguamento al nuovo sistema di validazione dei dati, le operazioni diventano immediatamente più semplici e veloci e il progetto di Corporate Performance Management si conclude in pochi mesi.

Adottare soluzioni intelligenti vuol dire anche dare avvio a un cambiamento più ampio: una volta sperimentati i vantaggi di una piattaforma di intelligent finance, è facile infatti che le organizzazioni si rendano conto della necessità di migliorare i propri processi di acquisizione dati in altri ambiti, dalle fatturazioni ai trasporti. Ciò aiuta a sviluppare una nuova cultura del dato, basata su qualità e chiarezza delle informazioni e focalizzata sulle performance.



INTERNET OF THINGS TUTTO PRONTO PER CONNETTERE IL MONDO

LE TECNOLOGIE ALLA BASE DELL'IOT
STANNO CONVERGENDO VERSO
SOLUZIONI IN GRADO DI GARANTIRE
OVUNQUE SICUREZZA
E CONTINUITÀ DEI SERVIZI

di Maurizio Ferrari

Silenziosamente, in modo quasi invisibile, l'Internet of Things (IoT) ci sta circondando. Dispositivi, sensori di diversa natura – non computer, smartphone e affini – connessi a Internet o, meglio, a delle reti, in grado di interagire e rilevare quello che ci circonda. Registrano, elaborano e trasmettono grandezze fisiche e chimiche, posizione e così via: una mole di dati che serve al pubblico e al privato per erogare servizi, per controllare linee di produzione, per telemedicina, per gestire trasporti e traffico e molto ancora. Gli ambiti di utilizzo dei dispositivi IoT sono innumerevoli e il limite sembra essere proprio solo la fantasia. Ma è così veramente?

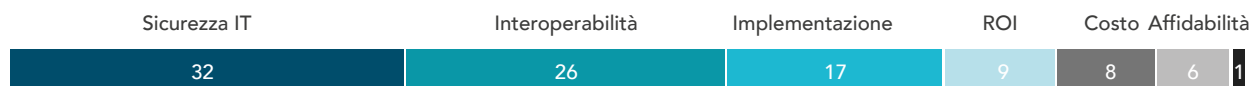


IOT: PIÙ SICUREZZA PER CONQUISTARE IL MERCATO

FAR CONVERGERE SIN DALLE PRIME
FASI SICUREZZA E SERVIZI IOT
PUÒ SBLOCCARE GLI INVESTIMENTI
IN QUESTO SETTORE

Uno dei punti critici per l'adozione di soluzioni Internet of Things è la sicurezza. I dati trattati dai dispositivi IoT sono innumerevoli e questi devono essere protetti e garantiti, dalla fonte allo storage sino all'elaborazione finale. Oggi, tuttavia, spesso non è la stessa realtà aziendale a occuparsi della sicurezza e della progettazione di soluzioni IoT: avere due responsabili crea dei problemi perché per avere soluzioni sicure con il livello di prestazioni richiesto è necessario iniziare a far convergere sicurezza e sistemi IoT sin dalle prime fasi di progettazione. Non si possono avere falle o posticipare gli interventi perché, quando la complessità si amplifica, è molto difficile intervenire a posteriori per introdurre elementi a protezione dei dati. Inoltre, considerando la natura dei dispositivi IoT c'è da tenere conto sia della sicurezza fisica sia di quella informatica. In specifiche applicazioni, per esempio nelle automobili connesse di nuova generazione, l'accesso alla centralina che controlla tutti i sensori non deve essere possibile né fisicamente collegando un cavo né da remoto se non si è autorizzati. Far convergere il mondo della sicurezza, in particolare quello dalla cybersicurezza e quello dei sistemi IoT può incrementare l'adozione di soluzioni Internet of Things da parte delle industrie e non solo. Una ricerca McKinsey (Cybersecurity for the IoT: How trust can unlock value) ha evidenziato come questa convergenza permetterebbe di sbloccare un mercato da centinaia di milioni di dollari. Secondo questa ricerca entro il 2030 il mercato

Per i buyers la sicurezza informatica è il maggiore ostacolo per l'adozione e la spesa dell'Internet of Things B2B



Fonte: McKinsey B2B Internet of Things Survey, 117 buyers, Q3 2022

mondiale dei servizi IoT dovrebbe raggiungere i 500 miliardi di dollari. In uno scenario in cui sicurezza e IoT convergono l'incremento degli investimenti può aumentare tra il 20 e il 40 per cento, raggiungendo così un valore che oscilla tra i 625 e 750 miliardi di dollari. Avere progetti IoT che garantiscono la richiesta

di digital trust diventa fondamentale per permettere un'evoluzione significativa delle soluzioni sia a livello B2B sia B2C: è indispensabile per avere una vera esperienza IoT senza interruzioni, con i dati che potranno fluire ininterrotti dall'origine sino all'utilizzo finale. Anche se in questo caso c'è una discrepanza

Le opinioni dei buyers e dei providers di IoT su questioni come il ritmo di adozione, la digital trust e il processo decisionale, divergono, probabilmente ostacolando la crescita del mercato

Sentiments di Internet of Things (IoT), % di intervistati

L'adozione di IoT maturerà ≤3 anni, % degli intervistati che concordano



Importanza della digital trust nei sistemi IoT



Importanza della privacy nei sistemi IoT



La suddivisione in Silos e la cybersecurity sono la causa della rapidità di adozione dell'IoT, % degli intervistati che concordano



Fonte: McKinsey B2B Internet of Things Survey, 208 intervistati (117 buyers e 91 providers), Q3 2022

di opinioni: sempre secondo McKinsey, la "fiducia digitale" è importante solo per il 30% dei fornitori, mentre per gli utilizzatori, questa percentuale raddoppia. In questo

gioco di rimpiazzino, secondo i fornitori (per l'81% è così) le difficoltà nell'adottare soluzioni IoT sicure risentono della separazione tra i gruppi IoT e quelli di cybersecurity, che, come detto, spesso agiscono in modo separato rallentando il processo decisionale e scegliendo anche percorsi divergenti. Tra gli acquirenti, invece, solo il 42% ritiene che vengano prese decisioni

È FONDAMENTALE REALIZZARE PROGETTI CHE TENGANO CONTO DEGLI ASPETTI DI SICUREZZA FISICA E DIGITALE

separate. C'è dunque un problema a livello di management che si riverbera durante la fase di progettazione. Realizzare progetti che tengono conto di tutti gli aspetti di sicurezza

in modo che i dati raccolti siano riservati, integri e disponibili è necessario per soddisfare ogni tipologia di esigenza dalla telemedicina alla linea di produzione, dalle smart car alle smart city. Avere la certezza che i dati su cui si deve lavorare sono protetti, sia dalle intrusioni sia nella costante disponibilità, è quindi uno dei cardini per guidare i futuri investimenti IoT.

I FATTORI PER AVERE UNA ESPERIENZA IOT SENZA PROBLEMI

La progettazione di un servizio di Internet of Things, sia per il mondo business sia per quello consumer, che funzioni senza problemi si basa su cinque fattori chiave.

- ▶ **Integrazione.** Tutto nei dispositivi IoT deve essere integrato e semplice da gestire: registrazione praticamente immediata, dispositivi autogestiti con aggiornamenti over-the-air, più standard di connettività a piattaforme e sistemi di back-end.
- ▶ **Sicurezza e fiducia.** Sfruttare tutte le ultime tecnologie per realizzare un sistema di sicu-

rezza dinamico, capace di garantire riservatezza, integrità e disponibilità dai dati è fondamentale. L'uso di intelligenza artificiale e machine learning permetterà di avere una gestione della sicurezza automatizzata.

- ▶ **Connettività.** Ogni dispositivo deve essere in grado di connettersi a diversi standard, così da realizzare con facilità lo scambio di informazioni e dati senza nessuna interruzione.
- ▶ **Mobilità.** Dispositivi e reti dovranno richiedere una manutenzione minima con batterie a elevata efficienza.
- ▶ **Personalizzazione.** Il sistema si adatterà alle esigenze dei diversi utilizzatori, permettendo di personalizzare l'esperienza a seconda degli scenari in cui si trova a operare, come il passaggio dall'ufficio a casa e durante il tragitto.



PER I SERVIZI IOT LA **CONNETTIVITÀ** SARÀ **SENZA CONFINI**

NEL PROSSIMO FUTURO LE APPARECCHIATURE SARANNO IN GRADO DI COMUNICARE TRA LORO, ATTRAVERSO SATELLITI, RETI CELLULARI O ALTRE RETI RADIO SENZA INTERRUZIONI

I sistemi IoT sono oggi a un bivio: esistere come isole a sé stanti o come un unico sistema interconnesso. Come spiegato da una ricerca Idc per conto di Eseye, i vantaggi di diventare un unico sistema sono innumerevoli. Per esempio, un container durante il suo viaggio attraverso il mondo sarà in grado di fornire sempre informazioni sulla sua posizione, sulla temperatura al suo interno, indicare quando passa da un mezzo di trasporto a un altro. Sulla carta è tutto fantastico, ma quante reti diverse incontrerà questo container? A quali si potrà connettere? Di quali tecnologie dovranno essere dotati i sensori IoT? Dovrà avere una connettività sicura, affidabile, performante ed economica. Non importa quale, anche se le tecnologie candidate sono innumerevoli. La tendenza attuale è quella di dotare i sistemi IoT di più accessi radio (Rat) e reti per fornire più opzioni: alle comunicazioni cellulari si associano altri protocolli



il roaming ovunque; attraverso le eSim diventa possibile selezionare da remoto gli operatori migliori a garanzia di una connettività efficace e senza interruzioni. Nel precedente esempio i container del futuro prossimo venturo potranno utilizzare dispositivi con connessioni satellitari, multi-Rat ed eSim per girare il mondo rimanendo sempre connessi. In determinati ambiti applicativi stanno prendendo piede anche modelli di connettività basati sul crowdsourcing, in cui sono gli stessi dispositivi a diventare fornitori di connettività per quelli vicini. Una soluzione del genere ha una importante valenza per progetti IoT con una mobilità limitata, circoscritta a un'area ben precisa: poiché ogni dispositivo fornisce anche la connessione, si possono creare reti virtualmente senza confini, garantendo la necessaria copertura per cancellare zone d'ombra e azzerare le interruzioni del servizio. Logistica, telemedicina, smart city possono trarre enormi benefici da questa soluzione. Il 5G, poi, sarà il collante di tutto. Quando sarà sufficientemente pervasivo, con un mix di reti pubbliche e private basate su questa tecnologia, il mondo IoT potrà avere un'ulteriore spinta sul mercato. L'interoperabilità tra reti pubbliche e reti private dovrà essere messa al primo posto, in modo che la creazione di un "mondo" interconnesso attraverso diverse tecnologie permetta la realizzazione di nuovi servizi e il potenziamento di quelli già esistenti.

wireless, tra cui Wi-Fi, Bluetooth, Zigbee, Thread e

LoRaWan. Diversi fornitori di semiconduttori stanno già realizzando soluzioni multi-Rat per semplificare la progettazione delle apparecchiature. Un ulteriore canale di comunicazione, che sta attirando l'attenzione del mondo IoT, è quello satellitare: una nuova generazione di costellazioni di satelliti a basso costo in orbita terrestre bassa (Leo) sta cambiando l'economia e la fattibilità delle comunicazioni satellitari da dispositivo a cloud. Inoltre, l'utilizzo di eSim al posto di quelle fisiche amplia di molto il range d'azione dei dispositivi. Niente più accordi con un singolo operatore, con la necessità di ulteriori accordi con altri per avere

L'EDGE COMPUTING CHIAVE PER SOLUZIONI IOT EFFICIENTI

ELABORARE I DATI IN PROSSIMITÀ
DELLA FONTE RIDUCE LA LATENZA
E PERMETTE DI AVERE RISPOSTE IN
TEMPO REALE PER GARANTIRE SERVIZI
EFFICACI E PUNTUALI

Parlare di progetti IoT è un discorso molto ampio dal punto di vista delle tecnologie e delle applicazioni: sotto questo cappello stanno innumerevoli soluzioni con richieste di banda diverse e apparecchiature con una capacità di elaborazione differente. Per l'IoT il cloud non è sempre la soluzione migliore per elaborare i dati raccolti dai dispositivi e dai sensori, perché in alcune applicazioni la latenza tra invio delle informazioni e la loro elaborazione può essere troppo elevata. L'elaborazione locale diventa fondamentale per il successo dell'IoT, basti pensare alle auto di nuova generazione, con sistemi di guida autonoma: tutti i rilevamenti devono essere elaborati in loco per permettere al sistema di funzionare correttamente e in modo sicuro; la parte che viene inviata in tempo reale ai data center delle case automobilistiche non serve per la guida. Secondo una ricerca Gartner

nel 2025 circa il 75 per cento dei dati saranno processati fuori dai data center, direttamente alla fonte o nelle immediate vicinanze. In telemedicina un dispositivo per il controllo del cuore e dei parametri vitali deve essere in grado di dare indicazioni in tempo reale sullo stato di salute al personale in loco. I dati acquisiti, però, possono essere usati sia in locale sia da remoto: per esempio una rete semaforica "intelligente" può rilevare le condizioni di traffico e modificare la durata del verde di conseguenza, con la possibilità di sovrascrivere questa modalità da remoto se fosse necessario creare un'onda verde d'emergenza. La chiave per l'automatizzazione di molti servizi è, quindi, l'utilizzo di machine learning e intelligenza artificiale unite a soluzioni di Internet of Things ed edge computing. La realizzazione di reti ibride, pubbliche/private, basate sulla tecnologia 5G, consentirà di realizzare "mini" data center locali, impegnati a gestire flussi di dati da elaborare in loco, anche con modalità di pay per use, sbloccando capacità di calcolo e applicativi solo all'occorrenza. Tutto questo avrà ripercussioni su diversi settori, tra cui quello della manutenzione predittiva o l'ottimizzazione dei processi di produzione. Il mercato delle soluzioni di Internet of Things è dunque in costante crescita, con prospettive ancora più interessanti nel momento in cui l'interoperabilità tra le reti e i sistemi, e la sicurezza diventeranno elementi fondanti della loro progettazione.

LE SOLUZIONI IOT PER LA TRASFORMAZIONE DI VODAFONE BUSINESS

VODAFONE BUSINESS PROPONE ALLE AZIENDE DEL SETTORE MANIFATTURIERO E DELLA LOGISTICA UN MODELLO DI TRASFORMAZIONE DIGITALE BASATO SULL'IOT, L'INTERCONNESSIONE E LA GESTIONE INTELLIGENTE. TRA I PUNTI DI FORZA: LA PIATTAFORMA DI CONNETTIVITÀ, IL 5G, L'AMPIA GAMMA DI MODULI FUNZIONALI E L'ELEVATO LIVELLO DI COMPETENZA RAFFORZATO DA PARTNERSHIP STRATEGICHE.

di Riccardo Florio

Vodafone Business si conferma sempre più come punto di riferimento per supportare le aziende nella trasformazione digitale, grazie a una rinnovata proposizione strategica, un'offerta tecnologica in costante espansione e una serie di partnership strategiche con aziende del calibro di Cisco, Microsoft e SAS.

La strategia di Vodafone Business è strutturata per rispondere alle quattro sfide fondamentali della trasformazione digitale: **ottimizzare le operation, abbracciare la trasformazione dei modelli di lavoro, garantire protezione e resilienza, accelerare la crescita del business.**

All'interno delle sfide che interessano le operation si inseriscono le soluzioni IoT, un mercato in cui Vodafone riveste oggi un ruolo di leadership come fornitore di servizi di connettività.

Le soluzioni IoT di Vodafone trovano collocazione in un'ampia gamma di settori quali PA, retail, sanità, manufacturing e logistica. L'obiettivo è di rinnovare i processi puntando sull'analisi dei dati e sull'implementazione di una "intelligence" capace di attivare azioni di risposta in modo autonomo.

Queste soluzioni permettono, per esempio, di concretizzare i modelli di Industria 4.0 e di abilitare un'integrazione a valore tra il settore manifatturiero e un nuovo modo (più intelligente e connesso) di interpretare la logistica che alcuni già chiamano logistica 4.0.

IL VALORE DELLA CONNETTIVITÀ

Al centro della proposta IoT di Vodafone Business si colloca la **Global Data Service Platform (GDSP)**

che rappresenta il fondamento tecnologico per sviluppare in sicurezza progetti di automazione o per favorire l'interconnessione e la flessibilità in ambienti eterogenei.

GDSP costituisce l'offerta di connettività gestita di Vodafone grazie all'integrazione delle SIM con una piattaforma di gestione e diagnostica in grado di portare valore aggiunto a ogni tipologia di progetto IoT. Un elemento di ulteriore valore aggiunto nell'offerta di connettività di Vodafone è quello di essere un provider di **reti mobili basate sulla tecnologia 5G** che si dimostra particolarmente adatta ad accompagnare la trasformazione digitale in ambito industriale, grazie alla sua natura di rete "elastica", virtualizzata e, pertanto, modellabile in base alle specifiche esigenze dei diversi impianti, oltre che alle indubbie doti prestazionali.

Il 5G è un elemento che rafforza ulteriormente le soluzioni Vodafone di **Mobile Private Network (MPN)** che permettono di creare reti di interconnessione capaci di superare in termini di flessibilità, prestazioni e numero di connessioni le tradizionali reti Wi-Fi.

VODAFONE INDUSTRIAL CONNECT

Il fulcro tecnologico della piattaforma IoT di Vodafone Business è Vodafone Industrial Connect (in sigla VIC), la piattaforma end-to-end che permette di interconnettere sensori sfruttando connettività mobile a banda larga e di trasferire il flusso di dati nel cloud per abilitare attività di monitoraggio, controllo, automazione, analisi dei dati di impianto, gestione efficiente del consumo energetico e così via. In altre parole, fornendo tutti i tasselli necessari per realizzare una smart factory, dalla connettività all'analisi avanzata dei dati. Le attività di analisi sono ulteriormente rafforzabili tramite la soluzione specifica **IoT Data Analytics** mentre attraverso **IoT Device Management** è possibile proteggere, monitorare, gestire e aggiornare da remoto i dispositivi connessi.

VODAFONE SMART LOGISTICS

Al tema della logistica Vodafone dedica una soluzione dedicata denominata Vodafone Smart Logistics, pensata per un'integrazione ottimale con i processi manifatturieri. Tramite diversi moduli funzionali,

questa soluzione permette di ottimizzare tutte le operation di un magazzino, dall'ingresso delle merci, alla movimentazione, allo stoccaggio fino alle operazioni di uscita. Altre tematiche gestite riguardano gli aspetti di controllo di produzione e di tracciamento degli asset, per estendersi fino alla sicurezza fisica associata a cose e persone.

I benefici ottenibili sono molteplici e si concretizzano in termini di efficienza di movimentazione dei prodotti, di ottimizzazione delle consegne, automazione delle attività ripetitive, monitoraggio remoto di macchine, diminuzione dei tempi di fermo del magazzino e riduzione dei rischi per la sicurezza degli operatori.

AUMENTARE L'EFFICIENZA ENERGETICA

Al tema estremamente attuale dell'efficienza energetica Vodafone Business indirizza **Energy Data Management**, una soluzione che permet-

LEADER NELLA CONNETTIVITÀ IOT

Gartner posizione Vodafone nel punto più alto del quadrante dei leader del suo Magic Quadrant 2023 per il mercato dei "Managed IoT connectivity services". Un segmento che comprende le soluzioni che abilitano la connettività, la raccolta e l'analisi dei dati e i servizi decisionali aggiuntivi necessari per le soluzioni connesse. Gartner conferma che, alla fine di giugno 2022, Vodafone aveva fatto registrare 158,9 milioni di connessioni IoT gestite in 190 Paesi, ottenendo il primato sia per il maggior numero di connessioni IoT tra i fornitori valutati nel Magic Quadrant sia per il più alto tasso di crescita delle connessioni su base annua (+22%). Tra i punti di forza rimarcati dalla società di analisi americana vi è il fatto che Vodafone sia uno dei pochi fornitori di servizi di connettività IoT a vantare un'esperienza nella fornitura di connessioni IoT gestite basate su servizi Mobile Private Network (MPN) 5G/4G, compresi progetti di successo al di fuori del proprio Paese.



te non solo di monitorare il consumo energetico e di controllare i parametri associati, ma anche di predisporre azioni correttive automatizzate guidate dall'intelligenza artificiale. Questa soluzione trova il suo utilizzo ideale nella gestione dei consumi associati ai sistemi di riscaldamento, ventilazione e condizionamento dell'aria, i cosiddetti HVAC (acronimo di Heating, Ventilation and Air Conditioning) che, in un edificio commerciale medio, possono rappresentare fino al 50% del consumo energetico totale.

VODAFONE BUSINESS FLEET ANALYTICS

Vodafone Business Fleet Analytics è la piattaforma modulare proposta da Vodafone Business per raccogliere dati operativi e ottenere informazioni sui veicoli della flotta e sui conducenti, al fine di ridurre il consumo di carburante, massimizzare

le prestazioni dei veicoli e mantenerne il valore nel tempo, migliorare il servizio offerto ai clienti e aumentare la sicurezza dei dipendenti su strada.

Questo sistema digitalizzato di gestione della flotta è utilizzabile via app o Web ed è adatto a un'ampia gamma di settori industriali che comprendono: organizzazioni di noleggio e leasing di veicoli, edilizia e mezzi pesanti, spedizioni, food and beverage, trasporti e logistica, servizi pubblici, car sharing, municipalità, scavatori e mezzi agricoli.

Vodafone Business Fleet Analytics consente di acquisire dati provenienti da più veicoli fornendo:

- informazioni in tempo reale su viaggi, velocità e percorsi, disponibili 24/7/365;
- visibilità completa sulla posizione del veicolo e le fermate, con reportistica immediatamente disponibile;
- manutenzione predittiva grazie alla diagnostica dei veicoli e ai dati di GPS;
- monitoraggio dei comportamenti di guida, per garantire la sicurezza dei dipendenti, in conformità con il GDPR;
- analisi multidimensionale in tempo reale con accesso ai dati storici e possibilità di personalizzare i report direttamente dal portale Web;
- accesso ai dati attraverso il portale web (My Vodafone Fleet) e la mobile app per conducenti (Vodafone Fleet Drive) con funzionalità avanzate di reporting e la possibilità di impostare regole e notifiche personalizzate.

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)

PA E FORMAZIONE? UNA PIATTAFORMA PER OGNI CAMPANILE

IL RINASCIMENTO CONTINUA A PERSEGUIARCI, AMPLIFICANDO LE DIFFERENZE ED IMPEDENDOCI DI DIVENTARE UNA VERA NAZIONE. DIFFERENZIAZIONE E FRAMMENTAZIONE SONO FRATELLI-COLTELLI. LA FRAMMENTAZIONE DERESPONSABILIZZA E CONDANNA ALL'IMMOBILITÀ E AL VITTIMISMO.

di Leo Sorge

Da che PNRR è PNRR, stiamo assistendo ad una girandola d'iniziative senza precedenti. Questo approccio non sta risolvendo i classici problemi strutturali come la mancanza di visione sulla PA e sugli italiani. Replicando all'infinito una storia già vista fin dal Medioevo, ciascun valvassino replica un intero ecosistema, senza cercare di federarsi con altri in modo da assicurarsi il successo: ne è esempio la corsa ai portali di formazione. Ma il personale è poco e di bassa qualità. Nella nuova competizione tra enti e con il privato le figure tecniche e i professionisti della gestione mancano sempre di più. Cerchiamo di valutare le prospettive future.



LA FORMAZIONE? UN GIORNO ALL'ANNO

Durante il Forum PA 2023 è stata presentata la Ricerca sul Lavoro pubblico, a cura di FPA. L'indagine ha presentato dati aggiornati al 31 dicembre 2021 e valutazioni per il 2022 della La Ragioneria dello Stato. A fine 2021 i dipendenti pubblici erano 3.239.000, dopo l'ennesimo anno in sostanziale pareggio tra uscite (184 mila) ed entrate (178 mila). La Ragioneria aveva fatto una valutazione per il 2022, ipotizzando un incremento di circa 27.000 unità. Prime la Scuola (14.400, +1,2%) e la Sanità (9.000, +1,3%).

La formazione, qualunque cosa voglia dire, è ferma al palo. Secondo i dati finali del Conto Annuale della Ragioneria dello Stato, i 3,2 milioni di lavoratori hanno ricevuto nel 2022 un totale di 2,9 milioni di giorni di formazione, ovvero meno di uno a testa. Anche l'idea che per attivare un dipendente, purché laureato, basti una qualche sporadica formazione aggiuntiva, va ripensata. Quasi tutti gli Enti pubblici ci sommano dati trionfali sulla formazione da loro erogata, al contempo lamentando inefficienza e mancanza di personale. Ma i trionfi restano sulla carta.

MOCHI SISMONDI: LA PA PUÒ ATTRARRE TALENTI

Resta il fatto che il settore pubblico in Italia non è attrattivo. L'indagine del ForumPA mostra chiaramente che anche nel settore pubblico pesa la trasformazione del mercato del lavoro già emersa nel privato.

*"Da un lato, oggi i lavoratori danno meno importanza al posto fisso in favore di aspetti come benessere, motivazione, formazione o lavoro agile - ha spiegato **Carlo Mochi Sismondi, Presidente di ForumPA** - dall'altro, in una scarsità di personale*



Carlo Mochi Sismondi
Presidente di ForumPA

qualificato, si osserva una nuova competizione tra pubblico e privato sui profili tecnici e tra amministrazioni, a causa dell'ingorgo di concorsi". In queste condizioni, come può la PA diventare attrattiva? "Acquisendo nuovi strumenti di employer branding e presentando ai candidati un'offerta completa di welfare aziendale, smart working, possibilità concrete di crescita professionale e retributiva".

Alcune iniziative di federazione delle forze in termini moderni e qualitativi, comunque, esistono. In questa direzione va la 3-I, che prende nome dalle iniziali delle tre entità che l'hanno generata, ovvero Inps (49%), Inail (30%) e Istat (21%). Inizialmente spinta da Mario Draghi, lo scorso 28 novembre 2022 ha visto la nomina del direttore generale Claudio Anastasio da parte del Governo in carica. Viste competenze, dimensioni e provenienze, dovrà giocoforza avere un ruolo centrale nella costruzione della PA.

Il quadro è chiaro, ma probabilmente non realistico. A nostro avviso è piuttosto dubbio che persone preparate scelgano la PA e non le aziende private: pensate a sviluppatori, modellatori di processo, esperti di cybersecurity. Se occasionalmente può accadere, è difficile che possa verificarsi con la frequenza di cui la PA avrebbe bisogno.

IL CONFRONTO IN EUROPA

L'Italia continua ad avere un numero totale di impiegati pubblici nettamente inferiore a quello dei principali Paesi europei, in proporzione sia alla popolazione sia agli occupati. Nel confronto con la popolazione il Belpaese occupa 5,5 impiegati pubblici ogni 100 abitanti: sono 6,1 in Germania; 7,3 in Spagna; 8,1 in UK; 8,3 in Francia. Guardando gli occupati, in Italia sono 14 ogni 100, ma 16,9 in UK, 17,2 in Spagna e ben il 19,2 in Francia.

Popolazione vecchia e mal formata, idolatria di lauree arcaiche, dipendenti ancor più vecchi e male aggiornati, incapacità di sviluppare da zero processi efficaci che sfruttino l'ICT per ampliare i servizi: questa, in impietosa sintesi, è la situazione quasi ovunque in Italia e quasi ovunque anche nella PA. Non si può più seguire questa strada.

In un quadro di rinnovamento è importante osservare l'anzianità dei dipendenti pubblici. Nonostante le assunzioni, **nel 2021 l'età media del personale stabile è 50,7 anni (49,9 anni per gli uomini, 51,4 per le donne). Nel 2001 era di 44,2 anni.** L'età media di entrata è passata in vent'anni da 29,3 a 34,3 anni. Gli impiegati pubblici con meno di trent'anni sono il 4,8%. Nei Ministeri siamo al dramma: solo lo 0,7% ha meno di 30 anni, nella scuola siamo vicini al limite di valutazione statistica (0,3%).

Bisogna operare una discontinuità. Non fosse altro perché entro il 2030, saranno 700.000 i dipendenti pubblici che andranno in pensione (proiezioni di FP CGIL). Potrebbe essere necessario assumere più personale di quello che lascerà. Se la PA non è attrattiva, sostituire i partenti sarà molto difficile, trovare gli 1,2 milioni che si ipotizza sarà impossibile.

LA TRASFORMAZIONE DIGITALE È ANCORA POSSIBILE

La domanda sorge spontanea: possiamo davvero farcela? In aggiunta ai dati presentati dal ForumPA è disponibile un'altra analisi indipendente, Lo stato di conformità delle Pubbliche Amministrazioni alle Linee Guida AgID presentata in marzo da Anorc, Associazione Nazionale Operatori e Responsabili della

PROIEZIONI E INTERVENTI PER LA PA PROSSIMA VENTURA

NUOVE TECNOLOGIE, NUOVI PROCESSI E NUOVO PERSONALE SONO LA CHIAVE PER LA TRASFORMAZIONE DIGITALE DEL SETTORE PUBBLICO. IL PERCORSO APPARE TORTUOSO.



IN-HOUSE PROTAGONISTE DELLA PA

Le in-house tecnologiche potrebbero essere al centro della nuova res pubblica digitale. Certamente le cose apparesentate quando Colao era ministro sono state oggetto di revisione. Il nuovo Governo punta sul cloud federato incentrato sulla collaborazione con le società in house qualificate.

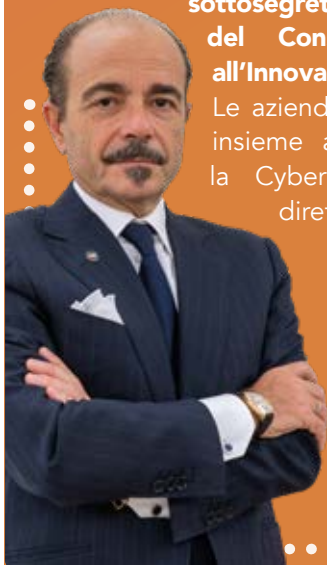
Su questo argomento Assinter ha organizzato il convegno "Le in-house ICT pubbliche patrimonio tecnologico del Paese e protagoniste dell'innovazione della PA", del 24 gennaio 2023.

Assinter comprende una ventina di aziende interne, tra cui Aria Lombardia, Lazio Crea, Csi Piemonte, Liguria Digitale, l'ombra PuntoZero e Sicilia Digitale.

"Per il Polo Strategico Nazionale ci sarà discontinuità", ha detto **Alessio Butti**,

sottosegretario alla Presidenza del Consiglio con delega all'Innovazione Tecnologica.

Le aziende dovrebbero essere insieme all'Acn, Agenzia per la Cybersicurezza Nazionale, diretta da Bruno Frattasi.



Alessio Butti,
sottosegretario
alla Presidenza del
Consiglio con delega
all'Innovazione
Tecnologica

CUSTODIA DI CONTENUTI DIGITALI

Il campione Anorc di 288 PA ha compreso aziende sanitarie, presidenza del Consiglio dei Ministri e tutti i Ministeri, agenzie fiscali ed enti locali. Orbene, uno scarso 10% è pienamente in regola con gli adempimenti. Se questi dati sono

generalizzabili, la trasformazione digitale della PA italiana è una chimera.

Secondo **Andrea Lisi, presidente di Anorc, al fondo di tutto c'è un problema di competenze.**

Quel 10% mostra che in alcuni casi il risultato è stato raggiunto. Per tutti gli altri, pare che la panacea sia una bella piattaforma di telelearning. È una soluzione gettonatissima: pochi mesi fa anche Anitec-Assinform ha lanciato la sua (Fòrmati con noi).

SYLLABUS E CONCORSI CON TE

Sempre **notando il forte skill mismatch del dipendente pubblico medio, anche il Ministero della PA s'è fatto la solita domanda: come fare per risolvere questo problema?** Tra le soluzioni troviamo... una piattaforma di formazione, **Syllabus**. Gli ambiti tematici sono quelli relativi alla transizione digitale, ecologica e amministrativa e allo sviluppo delle cosiddette "soft skills".

Da tempo, FP CGIL si è fatta la stessa domanda e si è data la solita risposta: la piattaforma **ConCorsi Con Te**. Supporta studenti, concorrenti e dipendenti non solo nell'apprendimento, ma anche nell'aggiornamento e nello sviluppo professionale. È un punto di riferimento sui nuovi bandi di concorso, anche per prepararsi alle prove.

IL DIGITALE POSSIBILE: AGENZIA DELLE ENTRATE

Buone notizie, ad esempio, arrivano da **Domenico Bifulco, Capo Ufficio Reingegnerizzazione dei processi presso Agenzia delle Entrate**: "La scelta dell'Agenzia è tenere la conservazione documentale vicina ai processi". Oggi l'Agenzia può dire che i suoi archivi documentali ospitano il 100% dei documenti informatici.

IL DIGITALE POSSIBILE: INPS

Un esempio di trasformazione digitale andata nella giusta direzione è quella dell'Inps. Per fare qualche esempio sui risultati raggiunti prendiamo quelli riguardo al PNRR. Su un totale di 105

obiettivi 2022-2023, a marzo 2023 ne restavano da completare solo tre. Parlando di formazione, nel 2022 era atteso l'aggiornamento di 4.250 dipendenti e sono stati 7.199. Per l'anno in corso, delle 8.500 formazioni attese, a fine marzo ne erano state già erogate 7.337.

Tra gli obiettivi futuri di Inps citiamo un esempio di semplificazione reale: la realizzazione di un unico hub operativo e informativo per la gestione delle domande di integrazione salariale semplificherà il lavoro di aziende, lavoratori e della stessa Inps.



LA MISSIONE DI INSIEL CON PAI

La Missione 4 del PNRR è rivolta al potenziamento dei Competence Center e a 37 nuovi Edih (European Digital Innovation Hubs). Ne fa parte il progetto Pai (Public Administration Intelligence) per la digitalizzazione dei servizi pubblici e di quelli sociali (Oes). Pai

è uno sportello unico per l'intera durata della transizione digitale ma anche ambientale, per questo unica in Europa. Opera all'interno della rete Europea di Edih, quindi accede ai servizi aggiuntivi offerti da altri Edih e reti europee (European Enterprise Network, StartUp Europe).

A coordinare Pai c'è Insiel, la in-house per l'Ict della Regione Friuli Venezia Giulia. Nell'ambito del progetto, Insiel ha il compito di coordinare una ventina di partner, comprese altre in-house regionali. Gli Edih forniscono servizi gratuiti o scontati per la diffusione di competenze digitali avanzate (Intelligenza Artificiale, blockchain) e la loro implementazione, corsi avanzati di riqualificazione delle competenze digitali e corsi aperti online di massa. Anche pianificazione e finanziamenti sono tra le possibilità affrontate dagli Edih.



SANITÀ: POTREI MA NON VOGLIO

La ricetta elettronica o dematerializzata è un classico esempio di cosa si potrebbe fare con il digitale e cosa invece non si fa. La ricetta immateriale era disponibile

da tempo, ma solo con la pandemia si è fatto un salto concettuale permettendone l'uso ampio. Successivamente, questo uso è stato confermato, per cui attualmente è ancora attivo. Dietro alla ricetta dematerializzata, però, il mondo che c'era prima, fatto di infiniti, irrazionali passaggi all'interno di un processo che si stenta a definire tale, è rimasto lo stesso. Quel che è cambiato è il software gestionale. Ripensare il processo porterebbe dei veri vantaggi in termini di servizi, economie, progettazione del futuro, ma è del tutto al di fuori della mentalità italiana che non prevede di uscire da quella via della seta di dazi ed assalti che è il sistema attualmente in piedi. Si basti pensare che in uno Stato diviso in 20 Regioni esistono 21 sistemi regionali, perché Trento e Bolzano fanno entità a sé. Con buona pace del Fascicolo Sanitario Elettronico, altro strumento che garantirebbe vantaggi immediati e a lungo termine in una nazione che invecchia, ma sul quale non si vuole fare sul serio.

LA PA PUNTA SUL PUBLIC CLOUD

L'ADOZIONE DEI SERVIZI CLOUD RESTA UN TRAGUARDO ANCORA LIMITATO, OSTACOLATO ANCHE DAL MODELLO A CONSUMO CHE, INVECE, È UN DRIVER PER LE AZIENDE

di Riccardo Florio

Migrare al cloud è l'unica via che consente di affrontare e risolvere le nuove sfide della trasformazione digitale. Il public cloud è diventato il principale modello di rilascio di servizi IT anche in Italia, con una spesa che IDC stima arriverà a 5,37 miliardi di euro nel 2023.

Oggi la Pubblica amministrazione italiana focalizza gli investimenti sul cloud pubblico prevalentemente sulle soluzioni di collaborazione (come e-mail, piattaforme di videoconferenza, applicazioni e strumenti per il lavoro da remoto e la condivisione di file) e sui servizi IaaS (archiviazione, virtualizzazione, backup e computing), con una limitata propensione a orientarsi al cloud per applicazioni verticali di settore, CRM, storage e sicurezza. Per migliorare il livello complessivo della digitalizzazione della Pubblica amministrazione italiana è, invece, indispensabile promuovere l'uso di un cloud più pervasivo. Secondo il Digital Economy and Society Index (DESI) della Commissione Europea, nel 2022 l'Italia era solo al 25° posto (su 27) nell'Unione Europea nella percentuale di cittadini

che interagiscono online con la PA. Una criticità che limita lo sviluppo della data economy, fatta dal connubio tra Internet of Things, cloud e digitalizzazione, e che appare ancor più evidente se correlata alle stime di Assolombarda secondo cui la burocrazia costa alle medie aziende italiane il 2% del fatturato e alle piccole aziende il 4% del fatturato.

BENEFICI E OSTACOLI

L'obiettivo della Pubblica amministrazione è di fornire vantaggi ai cittadini e il cloud può contribuire in due modi: migliorando l'efficienza della macchina amministrativa e ampliando la digitalizzazione dei servizi. Questi benefici sono riconducibili ad alcuni aspetti fondamentali. Innanzitutto, la semplificazione amministrativa, favorendo l'interoperabilità, la scalabilità e la personalizzazione dei servizi. Altri benefici conseguibili sono l'ampliamento del livello di digitalizzazione, l'ottimizzazione dei servizi, la riduzione della burocrazia e dei costi interni per le imprese. Inoltre, è centrale anche il tema "once only" ovvero la riduzione della duplicazione delle richieste a cittadini e imprese. Permangono però alcuni ostacoli importanti da superare a cui si spera il PSN potrà fornire rimedio. Il primo è che i tempi delle gare pubbliche non sono compatibili con la velocità con cui oggi i prodotti tecnologici di ultima generazione arrivano sul mercato rischiando di rendere già obsoleti gli acquisti in corso. Il modello di fornitura a consumo del cloud va inserito in bilancio come spesa operativa (OPEX) e questo, che è invece uno dei tipici vantaggi per le imprese, crea problemi sia di gestione amministrativa sia di tipo politico (perché le amministrazioni preferiscono spendere su asset che restano nel tempo). Un ulteriore ostacolo è la preoccupazione delle PA verso il pericolo di lock-in e di essere obbligati a rinnovare con lo stesso provider anche a fronte di costi eventualmente superiori per garantire la continuità delle attività.

IL QUANTUM COMPUTING ITALIANO È UNA QUESTIONE DI FISICO

L'Italia dei quanti ha le idee chiare ed è pronta alla crescita. Che dipenderà molto dall'intelligenza delle aziende

di Leo Sorge

Un'infrastruttura di rete fissa per la QKD e una rete geografica di distribuzione delle chiavi crittografiche, in una logica di collaborazione pubblico-privato: sono questi gli elementi necessari allo sviluppo di una filiera quantistica nazionale competitiva discussi in occasione dell'evento "Quantum computing e Quantum Secure Communications: un'agenda per l'Italia", organizzato da Anitec-Assinform.

Di quantum computing si parla già da vent'anni e nel tempo i passi in avanti ci sono stati. Si tratta di un settore che partendo da una nuova matematica sviluppa una filiera di prodotti innovativi che non potranno sostituire l'elaborazione classica, della quale saranno un arricchimento.

La formazione è al centro di qualsiasi attività, ma molto di più in aree rivoluzionarie come la fisica dei quanti, diversa dalle altre competenze d'oggi. Sul fronte specifico **saranno richiesti profili come Quantum Scientist, Quantum Engineer, Quantum Developer e specialisti in crittografia.** Questo cambiamento non può partire dopo l'Università, ma deve comprendere anche nuovi piani didattici sul fronte STEM, fin dalle scuole.

Va sottolineato che quanto più ci avviciniamo alla figura del fisico, tanto più l'Italia mostra di essere all'altezza: serve però proseguire nella costruzione di sistemi completi che competano con il resto del mondo. In questi comparti **possiamo competere sia per tenere i nostri talenti sia per attrarre quelli altrui**. Poi però bisogna dare prospettive future.

Il QC (Quantum Computing) è un settore a sé che comprende, per semplificare, hardware, software e comunicazioni. **Francesca Galli del Miur** ha raccontato le iniziative italiane nella sfera della micro/nanoelettronica nell'ambito dell'imminente Chips Act, che dovrebbero comprendere anche l'hardware per il QC e che vedono iniziative per il carburo di silicio nella STM siciliana. Per quanto riguarda il rapporto tra ricerca e industria l'Italia è ancora indietro e siamo ancora all'assessment di ciò che c'è.

L'AZIENDA ITALIANA DEVE CREDERE NEL QC

Nel mondo, l'ecosistema Quantum è un settore in forte crescita, con un valore stimato di oltre 500 miliardi di dollari a maturità tecnologica (stime The Boston Consulting Group).

L'Italia ha una grande opportunità di sviluppo in questo campo, ma le aziende non ci credono ancora. Secondo i dati dell'Osservatorio Quantum Computing & Communication del Politecnico di Milano, **al momento solo il 14% delle grandi aziende italiane ha avviato una o più sperimentazioni in ambito Quantum Computing**. Attualmente, il Governo italiano ha annunciato progetti e programmi di formazione. Nello scorso mese di luglio ha dato il via a un investimento di 320 milioni di euro per tre anni nella tecnologia quantistica attraverso la **costituzione del Centro Nazionale su HPC, Big Data e Quantum Computing presso il Tecnopolo di Bologna**, con il varo di Leonardo, tra i più potenti al mondo e inserito nella strategia europea.

Bisogna però ricordare che altre nazioni, come

Francia e Germania, investono cifre ben più alte su periodi che vanno oltre il triennio.

PROPOSTE PER UNA FILIERA ITALIANA

Durante l'evento sono stati presentati due white paper. **Paolo Comi, del Comitato R&S&I di Anitec-Assinform e coordinatore su Quantum Secure Communications**, ha fatto il quadro della situazione, elencando le proposte di policy per lo sviluppo della tecnologia QKD in Italia.

Due i capisaldi, con alcune raccomandazioni.

Un'infrastruttura di rete fissa per la QKD è alla nostra portata, con reti QKD metropolitane (reti in fibra ottica, collegamenti ottici terrestri e satellitari).

Anche una rete geografica di distribuzione delle chiavi crittografiche come servizio di sicurezza è molto vicina.

Un prerequisito è l'applicazione puntuale delle indicazioni previste dalla Misura #22 del Piano di

I MATERIALI SONO DISPONIBILI ONLINE

L'evento "Quantum computing e Quantum Secure Communications: un'agenda per l'Italia", organizzato da Anitec-Assinform ha tratteggiato con grande dettaglio tecnico e programmatico la situazione italiana.

Durante l'incontro sono stati presentati i White Paper "Il Quantum Computing a supporto della Trasformazione Digitale Italiana" e "Tecnologie Quantistiche per la sicurezza delle Comunicazioni

Digitali" realizzati da Anitec-Assinform in collaborazione con il CNR.

Prossimamente dovrebbero essere resi disponibili anche i video degli interventi.



SCAN ME



Implementazione della Strategia Nazionale di Cybersicurezza 2022-2026 in relazione all'uso della crittografia fin dalla fase di progettazione di reti, applicazioni e servizi.

Per raggiungere questi obiettivi, ovviamente, bisognerà realizzare una filiera quantistica nazionale. Sulla messa a sistema l'Italia ha da sempre fatto fatica, per usare un eufemismo.

IL QUANTUM A SUPPORTO DELLA TRASFORMAZIONE

"Le tre sfide del QC sono la realizzazione dell'unità di elaborazione (il qubit), la sua programmazione (del tutto diversa da quella standard) e l'adozione da parte delle aziende", ha detto **Federico Mattei, coordinatore su QC a supporto della Trasformazione Digitale Italiana**; *"è questo il momento per creare partnership e collaborazioni tra grandi player tecnologici, le autorità nazionali e le più importanti realtà industriali".*

POCHE MA BUONE LE AZIENDE NEL QC

La tavola rotonda, moderata da **Marina Natalucci, direttore dell'Osservatorio Quantum Computing & Communication del PoliMi**, ha presentato una rassegna -frutto di tanto lavoro- di grandi aziende italiane che già da tempo investono nel QC: **Eni per l'energetico, Dom-**

pè per il farmaceutico, Intesa Sanpaolo per la finanza. Queste aziende sviluppano attività e fanno anche grande opera di semina in accordi e formazione. *"Ci candidiamo a guidare l'ecosistema",* ha detto **Davide Corbelletto, Quantum Specialist di Intesa**, dopo un ampio quadro dell'impegno dell'azienda.

"QKD è vendibile ed è già sul mercato", gli ha fatto eco **Tommaso Occhipinti, Co-Founder e CEO di QTI**. La sua opinione è rilevante, in quanto rappresenta un'azienda di grande rilevanza mondiale nel QC, fondata nell'ottobre 2020 come spin-off ufficiale dell'Istituto Nazionale di Ottica del Consiglio Nazionale delle Ricerche (CNR-INO). *"Siamo affamati di business",* ha continuato Occhipinti, *"e stiamo già sviluppando le soluzioni che andranno sul mercato tra due e tre anni".* Per quanto riguarda il Chips Act, QTI è interessata alla fotonica integrata.

Un ambiente di applicazione di questo tipo di comunicazione va oltre la terra ed entra nel mare, quei **seawater quantum channel dei quali si parla da anni per applicazioni commerciali** ma anche militari. Anche in questo campo, QTI c'è.

A conclusione dell'incontro di studio resta una sensazione fortemente positiva, allineata con il resto del mondo avanzato e che però richiede molta attenzione sia da parte del Governo e del Ministero sia da parte delle aziende medio-grandi, che devono investire nel futuro senza che la casella del ROI blocchi il CFO miope. **Una spinta a tutti i nostri ricercatori è di espandere la loro attività a più tipologie di quantum computing.**

"È necessario pianificare per formare nuove competenze specialistiche, per disporre di infrastrutture e soluzioni nei settori dell'informatica quantistica e della sicurezza delle comunicazioni quantistiche", ha concluso **Eleonora Faina, Direttrice Generale di Anitec-Assinform**; *"i fisici li abbiamo, non lasciamoli scappare!"*.

IL TUO SISTEMA DI IDENTITÀ È SICURO?

Proteggere identità e credenziali utente è fondamentale: phishing, password deboli e furti di identità sono solo alcuni dei vettori di attacco più usati nelle violazioni di dati.

di Dan Lattimer



Dan Lattimer, Vice President Regno Unito & Irlanda, Semperis

Secondo il report “Cost of a Data Breach 2022” di IBM, quasi il 19% delle violazioni ha origine da credenziali compromesse, con un costo per incidente che oscilla da 4,4 a 9,4 milioni di dollari. E stando al “Data Breach Investigations 2022” di Verizon, le credenziali e i dati personali sono l’obiettivo principale degli attacchi di phishing. Oggi, tutto, dalle applicazioni online ai server fino ai sistemi per archiviare i file, si trova nel cloud. In un mondo così connesso la sicurezza dei sistemi di identità ha assunto una nuova rilevanza.

STRATEGIE E TRIANGOLO DI SICUREZZA

Per il 2025, Gartner prevede che più del 40% delle aziende userà analisi e risultati ottenuti da soluzioni di governance e gestione delle identità (**IGA**) per ridurre i rischi nei sistemi di gestione delle identità e degli accessi (**IAM**). Inoltre, in 7 casi su 10, le nuove distribuzioni di questi sistemi consisteranno in piattaforme IAM convergenti. Le strategie di difesa si incentrano su 3 funzionalità: **IGA**, gestione degli accessi con privilegi (**PAM**), autenticazione Single Sign-On (**SSO**) o multifattore (**MFA**), che formano il cosiddetto triangolo di sicurezza.

IGA: consentono alle aziende di automatizzare creazione, gestione e certificazione utenti, account di rete e relativi ruoli e diritti di accesso, riducendo i rischi legati alle identità. L’obiettivo è semplificare il provisioning utenti, la gestione delle pw e il controllo degli accessi.

PAM: proteggono le aziende dagli attacchi alle risorse aziendali più importanti grazie a monitoraggio, rilevamento e prevenzione degli accessi con privilegio non autorizzati. Con il mix fra esperienza dei singoli team, processi e tecnologie

dedicati, le aziende possono ottenere informazioni più approfondite, sapere cosa fa un utente, quando è connesso e limitarne il numero che accede alle funzioni amministrative.

SSO e MFA: SSO e MFA sono utili per garantire la sicurezza di una configurazione IAM specifica: l'autenticazione SSO è pensata per agevolare l'accesso utente, l'MFA predilige la sicurezza.

UNA PICCOLA FALLA PUÒ MANDARE A PICCO L'INTERO SISTEMA

Spesso le aziende che adottano le 3 soluzioni credono di aver posto basi per una sicurezza solida ed efficace, ma non è sempre così. In realtà, quasi tutti i sistemi di identità si ricollegano a Microsoft Active Directory (AD), utilizzato dalla maggior parte delle aziende. AD è il baricentro del triangolo, il fulcro per l'attendibilità delle identità; se non è sicuro, non lo sono neanche le soluzioni ai lati. AD è uno strumento datato, sviluppato 20 anni fa, quindi non attrezzato per contrastare i sofisticati attacchi informatici moderni. AD è stato progettato per gestire e monitorare direttamente un ampio numero di utenti e consentire l'accesso "come e quando". Questa eredità rende AD un obiettivo particolarmente appetibile per i malintenzionati. Molto spesso, nei programmi di sicurezza l'AD viene sottovalutato, lasciando tantissime vulnerabilità pronte a essere sfruttate, con il problema più grande, che resta la mancanza di consapevolezza. Anche le aziende che adottano sistemi su cloud, come AAD (Azure AD), non sono esenti dalle vulnerabilità. Nove volte su dieci, AAD estrae le autorizzazioni da AD in locale, che continua a essere il sistema principale per la maggior parte delle aziende. Non deve stupire che utenti malintenzionati utilizzino AD per infiltrarsi in Azure AD e viceversa.

QUATTRO MOSSE PER MIGLIORARE LA PROTEZIONE DI AD

AD è spesso un punto cieco nelle strategie di sicurezza. Le aziende sono consapevoli delle minacce, ma non di come sono collegate ad AD, e credono che i propri sistemi di identità siano al sicuro sebbene abbiano falle gigantesche. Anche l'adozione di soluzioni che rafforzano le strategie di sicurezza, come lo Zero Trust,

sono insufficienti dal momento in cui un attaccante viola AD e accede al sistema. Poiché tutte le identità sono raccolte in AD, le aziende devono impegnarsi per migliorare la resilienza informatica e la visibilità. Ecco quattro semplici mosse:

1. Analisi. Le aziende devono capire il livello di sicurezza dell'ambiente AD e se sono presenti indicatori di esposizione o compromissione. Grazie a tool sviluppati dalle community di utenti, es. Purple Knight di Semperis, è possibile ottenere un quadro della sicurezza di AD: informazioni chiave come errori di configurazione che possono esporre ad attacchi e segni di possibili compromissioni in atto.

2. Backup. I backup giornalieri o settimanali che di solito vengono eseguiti per AD sono problematici poiché su una rete possono verificarsi moltissime modifiche al giorno che rischiano di andare perse in caso di compromissione. Inoltre le aziende raramente testano i processi di backup, che possono rivelarsi inutilizzabili quando servono. In caso di ripristino da backup di stato o bare-metal c'è anche il rischio di reintrodurre il malware. Per evitare tutto ciò, le aziende devono avere backup specifici per AD in tempo reale in modo da eseguire restore puliti. Solo con processi verificabili il recupero può avvenire in tempi rapidi e senza intoppi.

3. Monitoraggio. Le aziende devono agire sul fronte dell'integrità di AD. Per valutare come cambiano esposizione e livelli di rischio è importante monitorare le configurazioni di AD nel tempo, in modo da rivedere le impostazioni e apportare le modifiche necessarie per mantenere un livello di sicurezza ottimale.

4. Test. Infine i test, che non devono essere eseguiti nell'ambiente AD di produzione ma in ambienti distinti per evitare interruzioni indesiderate.

Tutti questi step sono fondamentali per la sicurezza di AD, in qualsiasi strategia di protezione dei sistemi di identità. Per modernizzare l'infrastruttura IT, bisogna sempre partire dall'AD e per quanto sia uno strumento datato è un'applicazione di cui non si può fare a meno: se AD non funziona, si ferma tutto.

LA BANCA SCEGLIE FORTIFY PER AVERE UN CODICE SICURO

Un importante Gruppo di Credito italiano, con il supporto di Join Business Management Consulting, sceglie le soluzioni Fortify di OpenText per rafforzare la sicurezza dello sviluppo applicativo, eliminare le vulnerabilità del codice e per conformarsi ai prossimi obblighi normativi previsti dal Regolamento DORA

di Riccardo Florio

Molti sono i requisiti normativi a cui devono ottemperare gli operatori del settore finanziario.

Tra i più recenti vi è il **Digital Operational Resilience Act (DORA)**, il regolamento dell'Unione Europea sulla resilienza operativa digitale che promuove la convergenza a livello europeo in merito ai requisiti che gli enti finanziari devono adottare per innalzare la sicurezza dei propri sistemi digitali. Si applica non solo agli enti finanziari tradizionali quali banche, imprese di investimento e assicurazioni, ma anche alle aziende che trattano servizi di cripto-asset e a chi fornisce servizi cloud alle aziende sopra indicate. Entrato in vigore il 16 gennaio 2023 lascia 24 mesi agli stati membri per il suo recepimento.

DORA fornisce strumenti per la classificazione e segnalazione degli incidenti, ma punta anche sugli aspetti di sicurezza preventiva introducendo il Capo IV: Test di resilienza operativa digitale che **richiede l'esecuzione di una serie completa di test adeguati, tra cui individuazione e valutazione delle vulnerabilità, analisi open source, esami del codice sorgente**. Inoltre, prevede che le entità finanziarie effettuino valutazioni della vulnerabilità prima di ciascuna introduzione o reintroduzione di servizi nuovi o già esistenti e che sottopongano a test tutte le applicazioni e i sistemi critici con cadenza almeno annuale.

LE ESIGENZE DEL GRUPPO DI CREDITO ITALIANO

Un importante Gruppo di Credito italiano aveva l'esigenza di integrare, all'interno del proprio ciclo di sviluppo del software, strumenti di test adeguati al fine di **aumentare il livello di resilienza delle proprie soluzioni software e predisporre alla conformità al regolamento DORA.**

Per supportarlo in questo compito, il Gruppo bancario ha deciso di affidarsi a **Join Business Management Consulting, boutique di consulenza strategica e manageriale italiana** nata nel 2013 e classificata negli ultimi 5 anni dal Financial Times e da Il Sole 24 Ore tra le realtà in più rapida crescita in Europa.

*"Abbiamo, inizialmente, effettuato un'analisi di mercato per identificare le soluzioni che rispondevano ai requisiti del cliente, come l'esigenza di introdurre meccanismi di analisi statica del codice all'interno del ciclo di vita delle applicazioni – spiega **Maurizio Garofalo Head of Risk, Compliance e Cybersecurity Practice di Join Business Management Consulting** -. Tra queste **abbiamo identificato Fortify by OpenText come la migliore soluzione per le esigenze del Gruppo bancario.** Infatti, oltre a rispondere ai criteri cercati, Fortify risultava preferibile*

Maurizio Garofalo, Head of Risk, Compliance e Cybersecurity Practice di Join Business Management Consulting



alle altre soluzioni sotto molteplici aspetti. Innanzitutto, per il superiore livello di affidabilità e ricchezza di funzionalità che provengono dal fatto di essere una soluzione consolidata, riconosciuta come leader di mercato da tutti gli analisti: Gartner, Forrester, IDC e G2. Altri aspetti che sono stati rilevanti nella scelta sono stati l'elevato numero di linguaggi supportati e la possibilità di utilizzare il servizio di test sia in modalità on-premise per un agevole inserimento nell'infrastruttura del ciclo di sviluppo sia come servizio flessibile in cloud. Tutto ciò a un costo non superiore a quello di soluzioni meno performanti".

Fortify by OpenText è la suite di soluzioni inclusiva ed estensibile per la protezione delle applicazioni che vanta due decenni di esperienza e miglioramento continuo. Le soluzioni Fortify consentono di gestire il ciclo di vita delle applicazioni mettendo a disposizione funzionalità di test statico (**Static Application Security Testing o SAST**), test dinamico (**Dynamic Application Security Testing o DAST**) e di **Software Composition Analysis o SCA** (queste ultime indispensabili per garantire la sicurezza dei componenti open source).

Grazie a una sofisticata tecnologia di intelligenza artificiale, Fortify permette di eseguire controlli di sicurezza automatizzati sul codice mentre viene scritto, suggerendo le modifiche richieste per inibire la presenza di possibili vulnerabilità. *"Fortify by OpenText è una famiglia di soluzioni pensata per proteggere in modo automatizzato, concreto ed efficace le*

Pierpaolo Ali, Director Southern Europe, CEE & Israel di OpenText Cybersecurity



applicazioni, partendo dal momento stesso del loro sviluppo, per estendersi fino al termine del loro ciclo di vita - spiega **Pierpaolo Ali, Director Southern Europe, CEE & Israel di OpenText Cybersecurity** -. Questo livello di protezione favorisce l'applicazione di modelli di sviluppo DevSecOps e il rispetto della conformità normativa in molteplici ambiti, incluso quello finanziario”.

carte di debito/credito/prepagate. Il Gruppo di Credito si avvale anche della soluzione per la cifratura e tokenizzazione dei dati dei pagamenti **Voltage SecureData Payments**, semplificando la conformità ai requisiti PCI e proteggendo i dati delle carte di credito nelle applicazioni di e-commerce e nei pagamenti via Web e da dispositivo mobile.

IL PROGETTO

L'avvio del progetto ha previsto l'utilizzo della soluzione Fortify on Demand (FoD) per poi prevedere l'acquisizione di una serie di licenze della soluzione on-premise al fine di integrare nel processo di sviluppo applicativo le funzionalità di controllo automatizzato del codice con correzioni in tempo reale di Fortify. Il livello di adozione si è progressivamente ampliato fino a raggiungere **una settantina di licenze della soluzione in versione on-premise e oltre cento “gettoni” per attivare test tramite FoD**. A oggi la soluzione ha pienamente risposto alle aspettative del Gruppo di credito che sta considerando la possibilità di affiancargli alcune soluzioni della famiglia Voltage by OpenText per la sicurezza dei dati.

La soluzione Fortify svolge oggi un ruolo centrale nei tre diversi ambiti di sviluppo che interessano il Gruppo di Credito. Il primo è quello relativo allo **sviluppo delle applicazioni di home banking** e della relativa App che viene utilizzata per l'accesso tramite dispositivo mobile. Il secondo ambito di utilizzo riguarda lo **sviluppo delle applicazioni che regolano il sistema informativo** del Gruppo e che forniscono l'operatività a 180 Istituti collegati. La “terza fabbrica di sviluppo” in cui viene utilizzato Fortify è relativa alla **componente di monetica** ovvero legata al mondo delle

FORTIFY ON DEMAND PER FAVORIRE LA RELAZIONE CON I FORNITORI ESTERNI DI SOFTWARE

Attualmente, Fortify sta contribuendo a **mettere in sicurezza il Gruppo di Credito italiano verificando e correggendo ogni componente software che viene sviluppato**, prima che questo entri in produzione. All'interno delle tre fabbriche di sviluppo interne, in cui vengono utilizzati linguaggi di sviluppo predefiniti, il Gruppo di Credito utilizza Fortify in modalità on-premise.

La versione on-demand FoD viene, invece, utilizzata per tutto ciò che riguarda le restanti componenti applicative e nei confronti dei software che provengono da fornitori esterni o commerciali.

FoD semplifica le procedure di fornitura di software da parte di soggetti esterni, costituiti, spesso, da piccole software house specializzate sul settore bancario. Il Gruppo di Credito, infatti, ha la possibilità di offrire ai fornitori esterni di software alla banca l'accesso ai test FoD per effettuare una scansione di sicurezza. Questo consente alla banca di ottenere una certificazione di sicurezza indipendente sul livello di sicurezza e vulnerabilità del software conforme ai propri requisiti, senza dover richiedere al fornitore di interagire col codice sorgente che costituisce una proprietà intellettuale protetta.



LA SICUREZZA HA BISOGNO DI COMPETENZA

L'Italia ha mostrato di essere in difficoltà sul fronte della cybersecurity e per togliersi il bersaglio dalla schiena deve formare esperti e affidarsi a soluzioni avanzate in grado di semplificare la difesa

di Maurizio Ferrari

In occasione dei recenti Security Days è stato possibile fare con Fortinet, e alcuni ospiti, il punto sullo stato della **sicurezza informatica in Italia e sulle prospettive per il futuro**. Quello che è emerso è un quadro problematico, il nostro Paese è terreno di caccia per cybercriminali di tutto il mondo. Per contrastare il fenomeno, per Fortinet è necessario semplificare la complessità e aumentare le competenze nell'ambito della sicurezza. Secondo **Massimo Palermo, country manager di Fortinet**, il 2022 è stato un anno nero per la cybersecurity nel nostro Paese. L'Italia è nel mirino. **Il 7,6% degli attacchi a livello mondiale del 2022 hanno avuto noi come obiettivo**, mentre nel 2021 questa percentuale era del 3,4 (fonte Rapporto 2023 del Clusit). Altri indicatori segnano incrementi anche a tre cifre percentuali, segno di una attenzione elevata da parte del mondo del cybercrime. Ciò è da attribuire probabilmente al fatto che l'Italia sta pagando lo scotto dell'assenza di serie politiche di sicurezza e la mancanza di competenze all'interno di tutti i settori produttivi e della pubblica amministrazione. Come ha sottolineato Palermo, **oggi i criminali informatici hanno a disposizione un'ampia superficie d'attacco** e molti strumenti per fare danni. Nel dark

Massimo Palermo,
country manager Fortnet



web è possibile trovare di tutto, anche realtà che offrono "ransom as a service".

RIDURRE LA COMPLESSITÀ

Le competenze necessarie per fare danni sono drasticamente scese, mentre quelle per proteggersi sono al contrario cresciute, soprattutto alla luce della aumentata complessità delle attuali infrastrutture informatiche e tecnologiche. Cloud, smart working, integrazioni reti tecnologiche, iperconvergenza, digitalizzazione dei servizi e l'elenco potrebbe essere ancora molto lungo, ma ogni voce significa un possibile punto di accesso per gli attacchi. Questa complessità è gestita da tanti diversi attori, ma secondo Palermo, ci dovrà essere una semplificazione, necessaria per riuscire a proteggere l'integrità dei dati e la loro gestione. Chi saranno questi attori? Per Palermo saranno «*il mercato e la sua*

COMPETENZE AL POTERE

Fortinet ha annunciato i risultati del report "2023 State of Operational Technology and Cybersecurity" che fotografa lo stato della sicurezza delle tecnologie operative (OT) ed evidenzia le buone pratiche per proteggere le aziende dalle minacce IT/OT in continua espansione. Anche le industrie Ot sono prese di mira, lo scorso anno ben tre realtà su quattro sono state attaccate, in particolare malware e phishing l'hanno fatta da padrone e circa un terzo ha subito un attacco ransomware. L'esplosione di dispositivi OT connessi alle reti Ip amplifica il rischio e il team della sicurezza deve far fronte a minacce sempre crescenti.

Molte aziende pensano di dotarsi di un Ciso (Chief information security officer) a cui affidare la responsabilità della sicurezza informatica Ot, così da aumentare il livello di efficienza.

Tra le buone pratiche che le aziende dovrebbero adottare il report mette sotto la lente le politiche Zero Trust, l'implementazione della tecnologia Nac (Network access control), lo sviluppo di una strategia di sicurezza collaborando con i vendor, ma soprattutto rendere consapevoli i dipendenti che loro sono il primo elemento della sicurezza della azienda.



evoluzione a stabilirli, ma sicuramente uno sarà Fortinet». Questa fiducia nasce dalla consapevolezza che la soluzione Fortinet Security Fabric è una piattaforma di cybersecurity tra le più complete e con un elevato livello di automazione, in grado di gestire tutto il fronte esposto ai possibili attacchi da un unico centro di controllo.

FORMARE FIGURE COMPETENTI

Potrebbe sembrare sufficiente dotarsi degli strumenti hardware e software giusti per colmare il divario tecnologico dell'Italia in termini di sicurezza, ma purtroppo non è così. Nel nostro Paese mancano figure competenti nell'ambito della cybersecurity e ne mancano parecchie: per rendere "sicura" l'Italia sono necessari oltre 100mila esperti. Per formarli, secondo **Alessandro Curioni, presidente Di.Gi. Academy**, saranno necessari molti anni. Le sue riflessioni dicono che prima del 2038 non le avremo a disposizione; chiaramente nel frattempo muteranno le esigenze del mercato e sarà necessario adeguare questa formazione.

LE OPPORTUNITÀ PROFESSIONALI

Gennaro Boggia, professore ordinario di telecomunicazioni e direttore del Dipartimento di Ingegneria Elettrica e dell'Informazione, Politecnico di Bari, ha anch'egli sottolineato come sia necessario formare per il presente e anche, e soprattutto, per il futuro. Boggia ha evidenziato come, da quando è attiva dal 2017 la collaborazione con Fortinet Academic Partner Program e i relativi corsi per il conseguimento delle Certificazioni Nse, gli esperti formati usciti da questo corso di Laurea hanno trovato immediatamente lavoro, anche con condizioni economiche interessanti. Boggia ha rimarcato come in Italia ci sia fame di laureati nell'ambito Stem e, in particolare, con competenze digitali avanzate. Fortinet, con il suo programma di formazione, ha spiegato

Cesare Radaelli, senior channel director Italy and Malta, vuole formare in cybersecurity un milione di persone entro il 2026 in tutto il mondo. Nasce da questo la collaborazione con il Politecnico di Bari, dove gli studenti potranno "farsi le ossa" sulle soluzioni Fortinet acquisendo in modo rapido le competenze richieste dal mercato. Nel prossimo futuro per garantire la sicurezza delle infrastrutture sarà necessario avere tecnologie meno complesse da gestire, persone formate per amministrarla e persone educate nell'evitare tecniche di ingegneria sociale per ridurre il fattore umano come falla di sicurezza.

LA PIADINERIA

Piadina, prosciutto, squacquerone e cybersicurezza: è questo il mix vincente per La Piadineria. Questa realtà in costante crescita - a oggi ci sono oltre 350 punti vendita in tutta Italia, di diverse dimensioni - ha bisogno di gestire in modo sicuro la mole di dati che giornalmente viene comunicata tra i punti vendita e la sede centrale. «A febbraio - come ha spiegato Filippo Minini, responsabile It de La Piadineria - abbiamo iniziato a "mettere in sicurezza" i nostri punti vendita e le comunicazioni con la sede centrale. Abbiamo scelto la soluzione di Fortinet perché ci garantisce la scalabilità necessaria per coprire ogni nostra esigenza. Per noi l'integrità dei dati è fondamentale, attraverso l'analisi di questi siamo in grado di ottimizzare gli ordini e la gestione del personale, anche in funzione dei carichi di lavoro che cambiano durante le giornate». Entro la fine dell'anno tutti i punti vendita di questa catena saranno protetti con i dispositivi Fortinet.

IL SETTORE ENERGETICO CHIEDE CYBERSECURITY

Il Security Summit Vertical - Energy & Utilities 2023, la tavola rotonda organizzata da Clusit con AIPSA e Utilitalia, ha messo in luce come la transizione energetica, la guerra ucraina e l'andamento dei prezzi delle fonti fossili abbia generato criticità nei sistemi IT delle aziende del settore energia

di Aldo Cattaneo

La transizione energetica è un percorso inevitabile e il Green Deal europeo attraverso il pacchetto "Pronti per il 55%" mira a tradurre in normativa gli obiettivi di questa transizione, procedendo a tappe forzate verso gli obiettivi fissati al 2030. La crisi tra Russia e Ucraina si è innestata in questo scenario e ha aggiunto criticità a un quadro di ripresa già ampiamente messo sotto pressione, soprattutto per il settore gas, nel periodo post pandemico dalla "rincorsa alla ripresa" delle principali economie mondiali. E ben prima della scadenza del 2030 si collocano gli obiettivi previsti dal programma "REPowerEU" per rendere l'Europa indipendente dai combustibili fossili russi.

In questo quadro si trovano a operare anche i principali attori del settore energetico in Italia, sia nel segmento dell'upstream che in quelli del mid e downstream.

ANALIZZARE LO SCENARIO

Per analizzare tendenze, necessità e favorire percorsi verso una transizione energetica cyber resiliente, **Clusit, Associazione Italiana per la Sicurezza Informatica**, con **AIPSA, Associazione**

Italiana Professionisti Security Aziendale e Utilitalia, Federazione delle imprese idriche, energetiche e ambientali, organizza la terza edizione di *Energy & Utilities Security Summit*. Un appuntamento pensato come approfondimento confronto dedicato a un settore fondamentale per la sicurezza di dati e informazioni di aziende e cittadini. *Energy & Utilities Security Summit* si sviluppa a partire dall'esperienza ultradecennale di *Security Summit* per creare uno spazio di approfondimento sui rischi cyber e sulla necessità di gestire gli stessi attraverso un approccio olistico con i protagonisti del mercato.

IL RAPPORTO CLUSIT

L'incontro è stato introdotto da alcuni dati del rapporto Clusit 2023 sulla sicurezza ICT in Italia e nel mondo **Il numero di attacchi che hanno colpito il settore Energy & Utilities andati a buon fine è raddoppiato negli ultimi 4 anni**. A livello mondiale, quasi metà delle vittime (45%) sono basate in Europa, sia sul campione 2022 che nel Q1 2023. **Il malware è stato e resta la principale causa di**



attacco, passando dal 47% al 78%, con un 66% di crescita in valore assoluto.

Estremamente rilevante il 13% di incidenti 2022 che hanno come "punto di ingresso" la presenza di vulnerabilità. Gli incidenti con impatto Critical passano da oltre metà a quasi due terzi. Si noti la totale assenza di incidenti con impatti bassi. Da notare la rilevanza di attacchi a matrice Information Warfare del 2022, che nel 2023 va azzerandosi; al contrario, nel Q1 2023 raddoppiano gli attacchi a matrice Hacktivism.

Queste variazioni non devono stupire, in quanto nell'analisi di un incidente la fase di attribution è sempre tra le più complesse; rispetto a fenomeni come l'Information Warfare ovviamente il rischio di operazioni "undercover", per spostare su altri l'attribution, è sempre un rischio concreto.

Dal dialogo tra i vari manager è emerso come in questo scenario di transizione e di conflitti che impattano sulla distribuzione e il costo dell'energia **il settore energetico è rimasto tra quelli più esposti alla possibile "weaponization"** con il contestuale, potenziale ricorso all'arma cibernetica da parte dei diversi attori, statuali e non, per ampliare ancor più l'instabile assetto geopolitico venutosi a creare e questo rappresenta una grande sfida. I piani di cyber resilience giocheranno un ruolo fondamentale nelle strategie di business delle Società in un contesto normativo e regolatorio in continua evoluzione.

IL RUOLO DEL PNRR

In questo contesto **il PNRR può e deve essere l'occasione per rafforzare la resilienza cibernetica delle infrastrutture dei servizi essenziali del nostro Paese** e accompagnare tutto il settore

industriale delle PMI lungo un percorso di maggiore sicurezza dei sistemi IT e OT. Gli interventi hanno sottolineato come questo inevitabile passaggio debba essere graduale e soprattutto tenendo conto della dimensione delle varie aziende e come l'introduzione di una normativa dedicata possa aiutare questa transizione, proprio perché anche le piccole e medie imprese saranno costrette a fare i conti con i nuovi rischi e con la necessità di garantire la sicurezza informatica della propria azienda. Sicuramente si tratta di una sfida che tocca tutta la comunità europea, ma nella quale ogni singolo Paese deve fare la sua parte e per questa ragione è stato apprezzato che, per la prima volta in Italia, nel nuovo Codice degli Appalti sia stato inserito un riferimento alla cybersecurity e che verrà premiato il soggetto che saprà garantire le migliori procedure di sicurezza cibernetica a difesa delle infrastrutture o della gestione dei servizi essenziali. Passaggio graduale del sistema paese.

ENERGY & UTILITIES SECURITY SUMMIT

Hanno aperto i lavori della tavola rotonda, trasmessa in streaming il 25 maggio, Alessandro Manfredini, Presidente di AIPSA e Alessio Pennasilico, Membro del Comitato Scientifico Clusit. L'evento è stato moderato da Andrea Chittaro, Senior Vice President Global Security & Cyber Defence di Snam e ha visto la partecipazione di Francesco Ceraso, Head of Security Cyber Intelligence di ENI; Massimo Cottafavi, Global Security & Cyber Defence Dpt., Head of Cyber Security & Resilience di Snam Spa; Alessandro Marzi, CISO del Gruppo A2A; Alessandro Menna, Chief Security Officer, Italgas; Franco Picchioni, Head of Information & Cyber Security del Gruppo Hera; Simonetta Sabatino, Head of Cyber Security & Workplace Management di Saras e Mattia Sica, Direttore del Servizio Reti dell'Energia di Utilitalia.



DIGITALE E SOSTENIBILITÀ: RISPARMIO CON SVILUPPO DEL BUSINESS

LE IMPRESE STANNO TROVANDO NELLA SOSTENIBILITÀ AMBIENTALE UN PARAMETRO DI RIFERIMENTO PER ALLINEARE MODELLI ORGANIZZATIVI, COMPETENZE E TECNOLOGIE VERSO UNA NUOVA CAPACITÀ COMPETITIVA. DAL RISPARMIO ENERGETICO, AL CONTROLLO DEI COSTI ATTRAVERSO TECNOLOGIE E ARCHITETTURE SMART FINO A NUOVI MODI DI FARE BUSINESS. MA LA TRASFORMAZIONE NON È COSA SEMPLICE

Alle prese con una "disruption" continua dovuta a un insieme di complessità economiche, culturali, sociali, nonché a revisioni geopolitiche in atto su scala mondiale e alle recenti difficoltà indotte dalla pandemia, le imprese sono oggi alla disperata ricerca di modelli di riferimento sui quali orientare le proprie strategie di sviluppo del business. Una risposta concreta, già confermata dai primi numeri positivi, viene dall'**allineamento delle scelte strategiche di impresa con i modelli di sostenibilità**. Perché se l'evidenza di una crisi climatica spinge verso una transizione ecologica che ridefinirà, oltre che le nostre abitudini comportamentali, anche i modelli produttivi, logistici e di consumo, è già in essere la messa a punto di modelli di sviluppo di business sostenibili per creare nuova competitività.

di Stefano Uberti Foppa





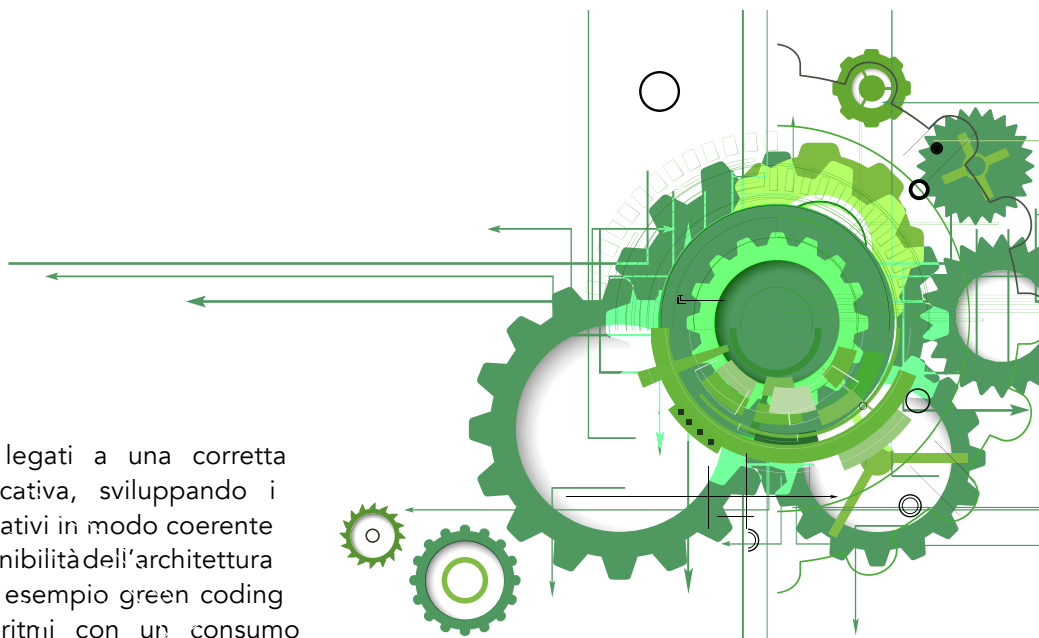
Un quadro nel quale l'IT gioca un ruolo di primo piano a partire da rinnovati criteri di efficienza energetica dei sistemi, verso modelli di utilizzo applicativo e sistemi di analisi dati orientati all'eliminazione delle inefficienze, fino a una visione di business globale basata sulla sostenibilità.

È un percorso che necessita di tappe di avvicinamento con Kpi e risultati misurabili per trasformare quella che già nelle aziende più illuminate è oggi una visione integrata nelle strategie di business in concrete evidenze di migliori performance, presidio di nuovi mercati, miglioramenti nel controllo dei costi, finalizzazione mirata degli investimenti. **Capgemini** ha svolto a fine 2022 uno studio a livello globale presso numerose grandi imprese di tutti i settori (2.004 partecipanti provenienti da 668 organizzazioni con fatturati oltre il miliardo di dollari) per sondare le loro strategie di sostenibilità e verificarne i risultati concreti. L'elemento di

riferimento che emerge fin da subito risiede nei **risultati di business raggiunti proprio grazie all'implementazione di practice sostenibili**, a ogni livello dell'impresa, dallo sviluppo strategico del business, al ripensamento organizzativo, al ridisegno dei processi, alla scelta tecnologica. Queste imprese hanno rilevato in media l'83% in più di fatturato per addetto tra il 2020 e il 2021 rispetto ad aziende senza questo tipo di strategia. Sono imprese che stanno compiendo la **transizione, anche culturale, del loro modo di operare**, investendo, ad esempio, in tecnologie innovative, quali software AI e sensori IoT per monitorare l'impatto ambientale delle loro infrastrutture tecnologiche e produttive. Aziende guidate in questa trasformazione da un top management convinto nel dare alla sostenibilità una priorità di business (Ceo); una parte Finance (Cfo) che favorisce gli investimenti in progetti di innovazione sostenibile attraverso tutte le unit dell'impresa; un Marketing (Cmo) che spinge all'adozione di protocolli di reale implementazione evitando il diffuso "green washing"; una Ricerca & Sviluppo dove il chief design officer progetta "by design" concetti e funzioni di sostenibilità nei nuovi prodotti e servizi; un supply chain officer che si fa garante di partner in grado di operare secondo reali criteri di sostenibilità; un Cio che rivede alcuni fondamenti architettonici dei sistemi informativi lavorando sulla costante eliminazione del costoso e impattante legacy hardware e software presente nei silos aziendali; un Hr che lavora davvero alla ricerca di quelle nuove competenze necessarie a sostenere questa difficile transizione.

EFFICIENZA ENERGETICA DEI SISTEMI INFORMATIVI...

Sono i sistemi informativi che possono accelerare un vero cambiamento e dare immediata evidenza di risparmi e vantaggi. A cominciare dal ridisegno di architetture legacy verso modelli meno "energivori", razionalizzando i parchi applicativi, identificando terze parti più ecosostenibili. Servirà controllare

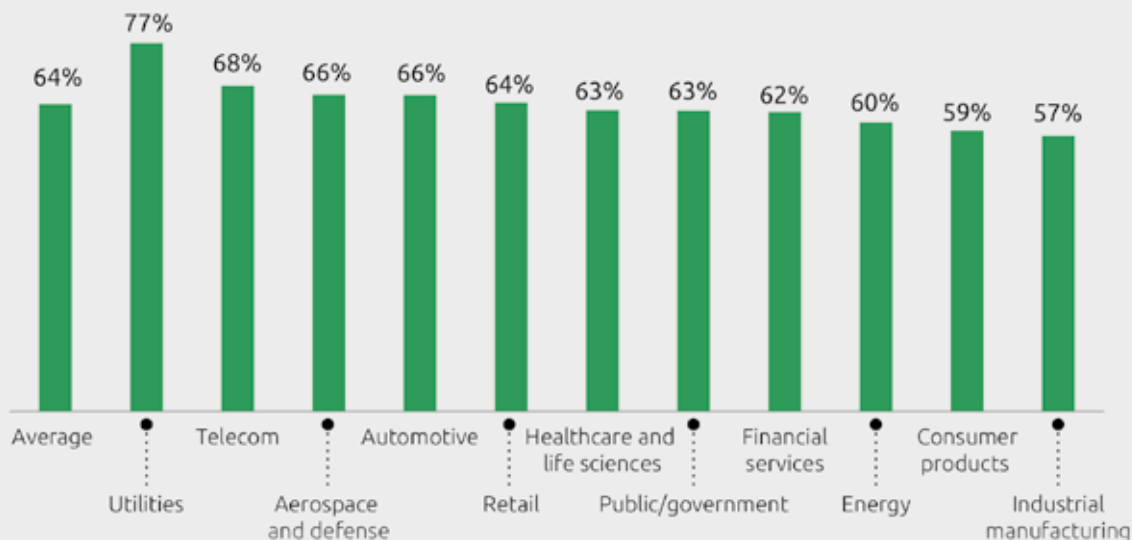


i costi energetici legati a una corretta distribuzione applicativa, sviluppando i nuovi moduli applicativi in modo coerente con i principi di sostenibilità dell'architettura generale. Usare ad esempio green coding per produrre algoritmi con un consumo energetico ottimizzato; utilizzare software "smart" (AI, IoT, analytics, A/R, V/R, digital twins) per una governance architeturale e applicativa evoluta, orientata alla riduzione del consumo energetico. Numerose iniziative di ottimizzazione energetica si sono concentrate negli ultimi anni attorno al nucleo primario di un sistema informativo: il datacenter, laddove l'architettura informativa preveda server e mainframe on premise (cioè installati in azienda) in confronto a scelte che privilegiano l'utilizzo di servizi esterni in cloud, dove i datacenter sono invece in carico al fornitore cloud.

Ci sono differenze architetture fondamentali tra i moderni datacenter, i mainframe/server di oggi con processori e componenti vari pensati "by design" in un'ottica funzionale di efficienza energetica, rispetto a quelli di solo un decennio fa, con tolleranze fisiche inferiori e maggiore dispersione di calore. Tuttavia il sistema centrale resta sempre "energivoro", e oggi, con richieste elaborative e di gestione di dati e applicazioni in costante aumento, lo è ancora di più. Serve quindi un costante lavoro di monitoraggio e riduzione d'impatto orientato all'ottimizzazione d'uso di questi sistemi. Sono tecnologie delicate e costose, che lavorano 24x7 su cui, attraverso l'analisi continua dei dati, è possibile giungere a livelli ottimali di raffreddamento (e quindi di consumo

energetico) in rapporto a un utilizzo sempre più efficiente. Ciò significa anche **capire i reali utilizzi di questi datacenter che spesso lavorano a richieste elaborative** che potrebbero essere soddisfatte in determinate ore del giorno o della notte, dove il costo energetico è minore/maggiore (decidendo quindi le priorità dei task da assegnare al sistema in funzione della loro criticità). O addirittura sono sistemi impegnati in task provenienti da applicazioni obsolete, a grande carico elaborativo ed energivoro, ma che in molti casi potrebbero essere persino eliminate per quanto poco vengono usate in azienda. Un'analisi del parco applicativo che talvolta porta a un consolidamento su un numero più contenuto di server e di mainframe, ridotto traffico di rete e minore utilizzo di storage, con evidenti risparmi e maggiore efficienza operativa (magari accoppiando tutto ciò con un ripensamento del layout del posizionamento dei sistemi per ottimizzare la ventilazione dei corridoi di raffreddamento e di uscita del caldo). Tutto questo, infine, lo si potrebbe trasferire, come requisito richiesto in fase di accordo contrattuale, al proprio fornitore di servizi cloud, forzando quindi un approccio sostenibile anche sui propri partner.

% dei rispondenti che afferma che le strategie di sostenibilità sono ormai presenti nelle agende dei C-level



Fonte: Capgemini Research Institute, Sustainability Transformation Trends Survey, Agosto-Settembre 2022

...E STRATEGIE GLOBALI DI SOSTENIBILITÀ AZIENDALE

La ricerca Capgemini fa emergere una dura realtà: la difficoltà di questa trasformazione ma anche l'inevitabilità del passaggio. **Ben oltre la metà dei rispondenti (il 64%) afferma che strategie di sostenibilità sono ormai presenti nelle agende dei C-level.** Tuttavia **solo il 37% sull'intero campione sta concretamente intervenendo sulla revisione dei propri modelli di business** e solo lo 0,91% del fatturato delle imprese censite è destinato oggi a questa transizione. Tuttavia i tempi cambiano e l'IT risulta fortemente impegnato in questo passaggio: il 48% afferma che la propria impresa usa architetture cloud a basso consumo energetico e i migliori performer in termini economici hanno

implementato diffusamente smart system di controllo del consumo energetico spingendo inoltre verso un'attività di smart working dei propri dipendenti allo scopo di ridurre l'impatto energetico aziendale. In conclusione, secondo le aziende censite, l'impatto ambientale e l'utilizzo di pratiche sostenibili sarà uno dei trend più "disruptive" nell'industria IT dei prossimi tre anni. E se non si vorrà subire questa tendenza bensì farla diventare un'opportunità di business, servirà non solo avviare una trasformazione di processi, organizzativa e tecnologica, ma anche accompagnare questo percorso con una condivisione culturale diffusa. Per definire nuovi modelli comportamentali di tutti i componenti dell'impresa in grado di creare una nuova identità allineata a un mondo in grande trasformazione.

IL DIGITAL DIVIDE GENERAZIONALE

di Primo Bonacina



Avete mai sentito l'espressione Digital Divide? Il Digital Divide (in italiano: Divario o Divaricazione Digitale) è un concetto che descrive la disparità nell'accesso e nell'uso delle tecnologie digitali tra persone, comunità o regioni, e parla delle differenze socioeconomiche e geografiche che influenzano la nostra capacità di utilizzare efficacemente le tecnologie digitali. Il fenomeno può manifestarsi in diverse forme:

- È correlato all'accesso fisico alle infrastrutture tecnologiche, come la mancanza di connessione a Internet ad alta velocità, in alcune aree svantaggiate. Ci sono infatti ancora comunità che non hanno un accesso affidabile a Internet o che sono escluse dalle principali reti di comunicazione digitali a causa di limitazioni infrastrutturali o mancanza di risorse finanziarie
- Riguarda anche le competenze e l'alfabetizzazione digitale. Anche se le persone avessero accesso alla rete, potrebbero non possedere le competenze necessarie per utilizzare efficacemente le tecnologie digitali. Questa mancanza può essere influenzata da diversi fattori socioeconomici e anche da età e livello di istruzione

- Può riguardare l'accesso alle risorse e servizi online, come l'e-commerce, l'e-government, l'istruzione online e le opportunità di lavoro, limitando così le possibilità di apprendimento, partecipazione sociale ed economica, miglioramento delle condizioni di vita.

Quando si parla di Digital Divide si pensa quindi a una situazione di inferiorità, di costrizione. Non a una scelta o un approccio voluto. Si pensa che, se tutti avessero le stesse possibilità, questa divaricazione non esisterebbe. Tutto ciò è certamente vero ma, in aggiunta al Digital Divide forzato ne esiste uno naturale, che è quello generazionale.

UN NUOVO STUDIO DI DELOITTE SUL CONSUMO DI MEDIA DIGITALI

Sappiamo tutti che la pandemia ha fornito un forte impulso al consumo di media digitali. Meno noto è il grado in cui è cambiata la natura stessa di questo consumo, fornendo non solo intrattenimento, ma anche significato e appagamento, secondo un nuovo report di Deloitte (Q2 2023) che mostra le dimensioni di questo cambiamento, soprattutto per i giovani. Lo studio divide i consumatori in generazioni (Boomer, Gen X ...) raggruppandole poi in 2 macro-fasce: fino

a 40 anni di età e oltre. Ecco alcuni punti salienti:

- Il 50% dei consumatori della Gen Z e Millennial negli Stati Uniti (14-40 anni) concorda con l'affermazione *Le esperienze online sostituiscono in modo significativo quelle di persona*. Solo il 19% dei Gen X, Boomer e anziani (dai 41 anni in su) la pensa allo stesso modo (A livello di nota personale, mio nipote mi ha detto: *perché dovrei andare a visitare il Duomo di Milano se lo posso vedere su YouTube?*)
- Ben il 48% dei giovani consumatori (*ma solo il 20% dei più anziani*) afferma di *passare più tempo a interagire con gli altri online che nel mondo fisico*
- Guardare programmi TV o film rimane attività importante per la maggior parte del pubblico di oltre 41 anni (55%), meno per i più giovani: solo il 30% di loro afferma di apprezzare soprattutto programmi TV e film. Sono invece importanti i videogiochi (19%), i contenuti generati dagli utenti (19%), la musica (16%)
- I più giovani affermano di sentirsi connessi a una comunità di persone quando interagiscono ai videogiochi (19%) e guardano contenuti generati dagli utenti (27%) rispetto un numero molto inferiore di consumatori più anziani (videogiochi: 5%, contenuti: 11%)
- Per chi tratta media digitali, ecco un altro spunto: mentre l'88% dei consumatori censiti ha pagato per un abbonamento digitale, la metà di questi (44%) ne ha anche annullato almeno uno negli ultimi sei mesi. E la cancellazione è molto più comune tra la Gen Z (57%) e i Millennial (62%) rispetto alla Gen X (43%) e ai Boomer (24%)

ALCUNE RIFLESSIONI

Chi scrive è un *Boomer* ma vorrei cercare di portare alla vostra attenzione, se ci riesco, alcune riflessioni generali:

- Ci sono cose che i Boomer non capiscono o non apprezzano o magari capiscono ma fanno fatica a interiorizzare. Il gap generazionale è sempre esistito. Fin dai tempi dell'Impero Romano ci furono

imperatori che condannarono la dissolutezza dei costumi moderni. Marco Aurelio (2° secolo d.C.) era famoso per l'impegno morale contro la dissolutezza delle nuove generazioni, mentre Teodosio I (4° secolo d.C.) promosse leggi per la repressione di nuove pratiche immorali. Però, se non ce l'hanno fatta gli imperatori, probabilmente non ce la faremo neanche noi: impariamo a convivere!

- I giovani di oggi saranno, banalmente, gli adulti di domani. Oggi non compriamo più candele per illuminare bensì per profumare. Non compriamo più giornali cartacei bensì abbonamenti media. Oggi si vendono (in percentuale) meno autovetture mentre aumentano quelle noleggiate (trend: passaggio da bene a servizio). Ogni giorno siamo costretti a ripensare i modelli di business e questo nostro sforzo, verosimilmente, dovrà continuare in futuro
- In ottica di recruiting di talenti, i valori e le abitudini delle nuove generazioni sono differenti da quelli delle precedenti. È inutile lamentarsi che non troviamo giovani con le giuste competenze (cit.) o che i giovani d'oggi non hanno voglia di lavorare (cit.) o che i giovani stanno solo sul divano a spendersi il reddito di cittadinanza (cit.). Se questo è il mercato dei candidati, adeguiamoci. Come possiamo interessare, ingaggiare, rendere produttive le nuove generazioni?

I TREND. CHE FARNE?

Ci sono 3 tipi di aziende:

- 1. Le aziende dominanti impongono i trend.** Ce ne sono di note e globali (Apple, Amazon, Netflix, Boeing) ma può essere dominante anche il gelataio di quartiere con la fila fuori mentre gli altri vedono pochi clienti
- 2. Le aziende smart cavalcano i trend** (imposti da altre aziende o da fattori esterni o dal mercato). Li capiscono, li fanno propri, li anticipano. Ripensano i modelli di business affinché siano funzionali ai nuovi trend
- 3. Le aziende perdenti subiscono i trend.** Si lamentano. Mostrano la propria frustrazione. Senza capire il problema. Senza affrontarlo e risolverlo.





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

