

# PARTNERS

INFORMAZIONE E FORMAZIONE PER IL CANALE ICT A VALORE

OTTOBRE N°55



## Vincere la sfida dell'inflazione: aumentare i prezzi senza perdere clienti



**SPECIALE**  
ANALYTICS,  
MACHINE LEARNING,  
ARTIFICIAL INTELLIGENCE



**SECURITY**  
DALLA SICUREZZA  
ALLA RESILIENZA

# PRODUTTIVITÀ, EFFICIENZA E RISPARMIO SUI COSTI: LE AZIENDE CHIEDONO, LA STAMPA GESTITA RISPONDE.

Sempre più aziende nel mondo stanno adottando soluzioni di MPS (Managed Print Services)

## PERCHÉ NASCONO I SERVIZI MPS?

Per monitorare e gestire tutte le risorse di printing in azienda (le pagine stampate, i materiali di consumo, la reportistica) seguendo un modello in cui tutti i processi risultano ottimizzati sulle esigenze produttive.



## COSA SIGNIFICA PER UN'AZIENDA RICORRERE A SOLUZIONI MPS?

Garantirsi il raggiungimento di determinati obiettivi, fondamentali per il successo nel business!

## OBIETTIVI PIÙ IMPORTANTI DA RAGGIUNGERE

In termini di parco stampa e gestione documentale, le PMI italiane si prefiggono:



**RIDUZIONE  
DEI COSTI**  
Hardware e  
consumabili




**AUMENTO DELLA  
SICUREZZA**  
Di documenti  
e stampanti




**MIGLIORE  
QUALITÀ E  
AFFIDABILITÀ  
DEI SERVIZI**

## FATTORI CHIAVE DI SUCCESSO NEL PERSEGUIMENTO DEGLI OBIETTIVI

Sono 5 i fattori di soddisfazione che determinano il successo dei servizi di stampa gestita:



**RIDUZIONE:**  
- del carico di lavoro  
sullo staff IT  
- dell'impatto ambientale



**MIGLIORAMENTO:**  
- dei flussi di lavoro  
- dei costi predittivi  
- del reporting/analytics

## LA SOLUZIONE?

### BROTHER PAGINE+

È un servizio flessibile ideato da Brother per le PMI: una soluzione di **stampa completa** che **semplifica la gestione** del parco stampa e **abbatte i costi**.



#### COSTO COPIA CERTO E COMPETITIVO

- Report dettagliato di stampa
- Tool web incluso per monitoraggio completo



#### GARANZIA PREMIUM E CONSEGNA AUTOMATICA DEI TONER ORIGINALI

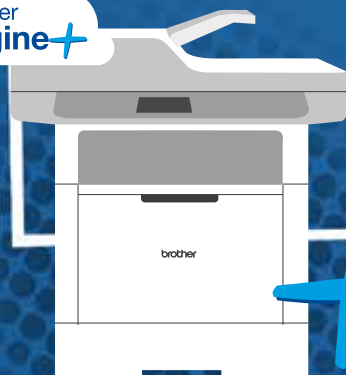
- Parco tecnologico di ultima generazione
- Funzionamento e ripristino garantiti per tutta la durata del contratto
- Consegna automatica dei toner nella sede del cliente



#### CONSULENZA STRATEGICA

- Per identificare i costi e le criticità dei processi di stampa
- Soluzione personalizzata sulle esigenze reali del cliente

Brother  
Pagine+



**brother**  
at your side

Scopri di più: [www.brother.it](http://www.brother.it)

## PARTNERS

Anno XI - numero 55

Ottobre 2022

Direttore responsabile: Riccardo Florio

In redazione: Riccardo Florio,  
Paola Rosa

Grafica: Paola Rosa

Hanno collaborato: Primo Bonacina,  
Maurizio Ferrari, Fabrizio Pincelli,  
Leo Sorge

Redazione:

REPORTEC srl

Via Gorizia 35/37

20099 Sesto San Giovanni (MI);

Tel 02 24304434;

www.reportec.it ;

redazione@reportec.it

Editore:

Reportec Srl, C.so Italia 50  
20122 Milano

Diffusione: 35.000 copie

Iscrizione al tribunale di Milano n° 515 del 13 ottobre  
2011. Stampa: A.G.Printing srl, via Milano 3/5,  
20068 Peschiera Borromeo (MI)

Immagini: Dreamstime.com

Proprietà: Reportec Srl, C.so Italia 50, 20122 Milano

Tutti i diritti sono riservati

Tutti i marchi sono registrati e di proprietà  
delle relative società

Reportec è una società fondata da:

Gaetano Di Blasio, Riccardo Florio,

Giuseppe Saccardi

## EDITORIALE

LA LOTTA PER I TALENTI CHE ALIMENTA  
IL CONSOLIDAMENTO

5

## COVER STORY

COME AUMENTARE IL PREZZO DEI SERVIZI  
INCREMENTANDONE IL VALORE

6

## SPECIALE ANALYTICS, ML, AI

L'INTELLIGENZA CHE GIRA INTORNO

12

AI E METAVERSO: ARRIVANO I SERVER IPSOR

CON CHIP SPECIALIZZATI BIREN

16

## SECURITY

DALLA SICUREZZA ALLA RESILIENZA

18

DOXING, INTIMIDIRE ATTRAVERSO LE INFORMAZIONI

21

CYBER RESILIENZA E MACHINE LEARNING:

UN BINOMIO INDISSOLUBILE

23

COME CAMBIANO I PARADIGMI DELLA PROTEZIONE

AZIENDALE

25

## CONTROCORRENTE

APPLICAZIONI CRITICHE: CLOUD VS LOCAL

28

## INTERVISTA

UN "PONTE" PER LA FORMAZIONE

32

## PANORAMI

LA STRADA VERSO LA DIGITAL TRANSFORMATION

34

INFRASTRUTTURE PER LA DIGITALTRANSFORMATION

40

AVAYA ONECLOUD: UNA PIATTAFORMA

PER L'ESPERIENZA TOTALE

42

## BUSINESS

DIMENSIONE O VELOCITÀ: IL DILEMMA  
DELL'INNOVAZIONE

44

# bizzIT.it

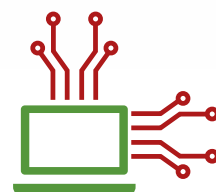
**MAGAZINE ONLINE  
DI ICT E TECNOLOGIA**



**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/>

# LA LOTTA PER I TALENTI CHE ALIMENTA IL CONSOLIDAMENTO

Una delle problematiche che interessa attualmente il mondo ICT è la **carenza di professionisti qualificati**. Tra le figure più ricercate (e più carenti) vi sono gli specialisti della sicurezza (amministratori, architetti, esperti SOC), gli sviluppatori che hanno familiarità con i nuovi modelli e tecnologie (DevOps, agile, container, cloud native) e i cosiddetti data scientist, capaci di trasformare Big data eterogenei in informazioni contestualizzate e a valore.

Questa carenza ha ripercussioni dirette sul business aziendale. Per esempio, una recente indagine di Fortinet (2022 Cybersecurity Skills Gap) ha evidenziato come il 50% delle aziende italiane interpellate consideri la carenza di competenze nell'ambito della sicurezza un significativo rischio aggiuntivo per la propria azienda.

La mancanza di figure qualificate può, inoltre, **limitare la capacità di un'azienda di intercettare opportunità di sviluppo e aumento di competitività**. Può, per esempio, inibire l'implementazione di processi di trasformazione digitale, rallentare l'evoluzione verso modelli di servitization od ostacolare un'efficace relazione e fidelizzazione dei propri clienti.

Se è difficile, da parte delle aziende, reclutare professionisti qualificati, ancora più difficile è riuscirci a trattenerli. I professionisti presenti sul mercato sono, infatti, oggetto di vere e proprie campagne acquisti simili a quelle dei calciatori.

Un aspetto centrale in questa lotta per reclutare e mantenere i talenti informatici è **l'importanza delle certificazioni che un professionista porta con sé**. Le certificazioni, infatti, sono per loro stessa natura personali e portare in azienda un

professionista che dispone di specifiche certificazioni su tecnologie e soluzioni significa, dall'oggi al domani, consentire all'azienda di fregiarsi di una certificazione. Requisito utile sia per conquistare nuovi clienti sia, a volte, per poter partecipare a una gara.

Alcuni vendor, come Microsoft, stanno modificando i processi di certificazione dei loro partner per trasferirli dalle persone alla società partner nel loro complesso. Anche così, tuttavia, la garanzia di qualità nei confronti del cliente finale è sempre fornita prevalentemente dalle persone.

È interessante osservare che, spesso, sono proprio le aziende più piccole a disporre di risorse molto valide non riuscendo, tuttavia, a sfruttarle adeguatamente perché prive della capacità di crescita. Non è un caso che **nel mondo degli MSP, dei system integrator e dei VAR si stia assistendo a un processo di costante consolidamento** in cui le realtà più grandi tendono ad acquisire le più piccole.

Si tratta di una tendenza che, almeno nel medio periodo, è destinata a proseguire poiché realizza una perfetta sinergia tra capacità complementari ed esclusive. Chi acquista ha interesse a portarsi a casa delle risorse difficili da reperire sul mercato, già pronte e capaci di portare nuovo fatturato da subito. Le aziende acquisite (che a volte mantengono la loro identità) si ritrovano all'interno di una realtà di business più grande che gli consente di crescere velocemente.

Ciò che appare incontrovertibile è che, nello scenario di mercato futuro, **i partner di Canale che non disporranno di competenze e risorse nelle nuove tecnologie saranno rapidamente sorpassati** mentre gli altri cresceranno sempre di più. Per esempio, gli analisti prevedono che nel prossimo futuro il 20% degli MSP controllerà l'80% dei guadagni del mercato dei Web service. Quelli che si troveranno al vertice della piramide non si limiteranno a fornire servizi IT, ma **assumeranno un ruolo sempre più attivo nel successo dei loro clienti**, diventando partner strategici e costruttori di nuove esperienze di business. ❖

di Riccardo Florio



# Come aumentare il prezzo dei servizi senza perdere i clienti

Cambia il mercato, aumentano i costi, cresce l'inflazione: i motivi per cui può essere necessario aumentare i prezzi sono molteplici. I rischi di perdere clienti sono alti, ma ci sono i modi per limitare al massimo i potenziali "danni"

di **Fabrizio Pincelli**



Nel mercato odierno, un termine che è sempre più spesso citato è valore. Le aziende sono alla spasmodica ricerca di un reale valore nelle proposte di service provider o system integrator, che gli permetta di ottimizzare processi e migliorare il business. Perciò, la capacità di aggiungere valore a un prodotto o a un servizio è oggi una necessità assoluta. D'altra parte, quando si riesce a creare valore per i clienti, si aumenta la reputazione e crescono i profitti. Non solo. I clienti che sentono di aver fatto un buon acquisto sono più propensi a comprare di nuovo e a condividere la loro positiva esperienza con altri.

Invece, in assenza di componenti a valore aggiunto, praticamente la vendita di qualsiasi prodotto o servizio può essere ridotta alla mera contrattazione

sul prezzo più basso. E quando la vendita è basata unicamente sul prezzo non si è mai in grado di ottenere un alto margine. Questo va a discapito della redditività, della crescita a lungo termine e del successo delle vendite. Vediamo allora come poter aggiungere valore a un prodotto o a un servizio in modo che il prezzo non rappresenti più il primo fattore di scelta.

### **1. Consulenza di esperti e livello di professionalità estremamente elevato.**

Il modo più immediato di aggiungere valore a un prodotto o servizio e di corredarlo con una consulenza. Saper consigliare cosa scegliere e come ottenere il meglio dalla scelta fatta fa una grande differenza rispetto all'acquisto di un prodotto da un listino. Tuttavia, per fornire davvero del valore, è necessario proporre un livello di consulenza significativamente più alto, più sofisticato e più prezioso di quello della concorrenza. Questo implica un ottimo livello di raffinatezza e di conoscenza di ciò che si fa.

### **2. Bundling**

Sulla falsariga di quanto accade con la consulenza, è possibile creare pacchetti accattivanti, livelli di acquisto e una serie di vantaggi aggiuntivi che hanno un significativo valore. In questo modo, un bundle risulta molto più

prezioso e stimola maggiormente l'acquisto di quanto non faccia semplicemente un prodotto o un servizio in sé.

### **3. Livelli di servizio**

Sono un fondamentale elemento di differenziazione. E questo non solo fornendo un livello di servizio più elevato, ma anche aggiungendo livelli di servizio diversi in base alle dimensioni dell'azienda acquirente, alla frequenza o all'importo degli acquisti. Per esempio, si potrebbero approntare dei livelli di servizio oro, argento e bronzo per i quali le imprese qualificate sono disposte a pagare pur di ottenere i vantaggi offerti da tali livelli di servizio.

### **4. Programmi per clienti che fanno frequenti acquisti**

È una pratica che funziona molto bene e si basa su un concetto legato al fatto che più un'azienda acquista presso un determinato system integrator o service provider, più riceve servizi, prezzi, vantaggi e articoli correlati.

### **5. Formazione**

Quando i nuovi clienti acquistano prodotti o servizi, potrebbe essere utile rendere disponibili delle persone per aiutarli a utilizzare meglio ciò che gli è stato venduto. Allo stesso modo, maggiore è la formazione relativa a tali prodotti o servizi, maggiore sarà la capacità di utilizzarli. In questo caso,

quindi, è la formazione a creare valore e a rappresentare un acquisto indispensabile.

### **6. Preferenza qualitativa**

In base al livello di acquisto, coinvolgimento o interazione di un cliente, si possono fornire prodotti di qualità superiore e magari anche un livello di servizio più sofisticato, personale e linee telefoniche dedicati e così via. Potrebbe anche essere utilizzato come esempio di valore aggiunto nei confronti dei nuovi clienti.

### **7. Velocità del servizio o del delivery**

Uno dei modi per differenziarsi è garantire la puntualità o un delivery più rapido di un servizio o di un prodotto. È risaputo che la puntualità sia una componente chiave per l'addebito del prezzo pieno o massimo. Ed essendo parte integrante della fornitura di servizi e prodotti rappresenta un valore aggiunto.

### **NON PERDERE I CLIENTI**

Quando si avvia un'attività come quella di un service provider o di un system integrator, si fa un'approfondita analisi dei prezzi e si bilancia le aspettative di guadagno con quello che il mercato può consentire. Si fanno poi delle ricerche sui concorrenti e quanto può essere importante per un cliente il valore che si può offrire.

## Aggiustamenti graduali

Se non siete in una situazione che rende indispensabile agire rapidamente, non imponete un aumento dei prezzi tutto in una volta. Se possibile, procedete per gradi. Lo svantaggio è che se applicate diversi aumenti in un breve periodo di tempo, i clienti vi possono vedere come incoerenti e possono chiedersi quando scatterà il prossimo aumento di prezzo.

Perciò, se scegliete di effettuare aumenti multipli e incrementali, separateli con un intervallo di tempo stabilito e spiegatevi attraverso un'efficace comunicazione. Molte società di servizi utilizzano aumenti annuali regolari per tenere il passo con l'aumento dei costi.

Sono quindi stabiliti dei KPI, viene definito un piano marketing e magari viene anche utilizzato un modello di prezzo freemium per scalare il mercato e ottenere rapidamente clienti. Tutto ciò permette di raggiungere l'obiettivo che ci si è posto.

Tuttavia, nel tempo il personale cresce, c'è l'inflazione, aumentano gli stipendi e il costo dei singoli prodotti che compongono il servizio. Il risultato è che i margini si riducono sempre più e così bisogna correre ai ripari. Dopo aver "tagliato" dove possibile, l'unica strada percorribile è di aumentare i prezzi. Ma di quanto? E solo su alcuni servizi e clienti o su tutti?

Ottenere il giusto risultato non significa solo trovare il prezzo da usare (o i prezzi se si hanno dei livelli di

servizio). Si tratta anche di assicurarsi che i clienti siano disposti a pagare di più. La chiave per ottenere questo risultato è comunicare come i vostri servizi contribuiscono al loro successo. Se l'aumento dei prezzi non apporta qualche beneficio al cliente, anche minimo, allora probabilmente non serve. Invece, se ben ideato, un aumento del prezzo può dare alla vostra azienda il flusso di cassa

***I clienti che scelgono solo in base al prezzo tendono a consumare molte risorse e rifiutano gli sforzi di upsell***

necessario non solo a sopravvivere ma anche a continuare a espandersi e migliorare ulteriormente.

Risulta perciò evidente che un eventuale aumento dei prezzi deve essere pianificato in modo preciso e non stabilendo in modo casuale la percentuale dell'incremento. Il punto di partenza è l'analisi del comportamento dei clienti e delle ricerche di mercato. Come nel caso del lancio di un nuovo prodotto, bisognerebbe poi assicurarsi che l'attuale flusso di cassa sia in grado di sostenere possibili cali dovuti a una nuova strategia di prezzo. In tal senso, si deve stimare il tasso di abbandono atteso, perché, almeno in un primo momento, l'aumento dei prezzi con tutta probabilità porterà una riduzione degli introiti. Infatti, i clienti che scelgono solo in base al prezzo tendono a consumare molte risorse e rifiutano gli sforzi di upsell.

Ci sono aziende che affermano di utilizzare l'analisi predittiva dei dati per calcolare l'abbandono atteso, ma spesso sono realtà che propongono servizi costosi che potrebbero non valere l'investimento.

## COME AUMENTARE I PREZZI

L'aumento dei prezzi non deve necessariamente comportare un incremento percentuale generalizzato del listino. Per esempio, si possono aggiungere nuovi livelli di prezzo o funzioni aggiuntive per i clienti che accettano il nuovo prezzo. Questo è un modo per aumentare le tariffe per alcuni e controllare il COGS (il costo dei beni venduti) per altri.

È possibile creare dei componenti aggiuntivi per coprire l'aumento di prezzo. In questo modo, i clienti che ritengono di non aver bisogno dell'aggiornamento possono continuare a usufruire del servizio, mentre gli utenti più elitari scelgono di ottenere le funzionalità aggiuntive al nuovo costo. I clienti possono continuare a pagare le loro tariffe attuali,

ma passano a un livello "base" o a un altro nuovo livello con meno funzioni. I clienti che vogliono le nuove funzionalità e possono permettersi l'acquisto effettueranno l'upgrade.

Le funzionalità premium non devono necessariamente costare molto all'azienda. Può anche trattarsi di qualche ora di consulenza in più o di un'assi-

***Si possono aggiungere nuovi livelli di prezzo o funzioni aggiuntive per i clienti che accettano il nuovo prezzo***

stenza 24 ore su 24, 7 giorni su 7 o nei fine settimana, quando alcune persone sono comunque al lavoro.

Al contrario, agire sul livello di valore può comportare che i clienti

paghino la stessa cifra, ma i vostri costi diminuiscano. Per esempio, se attualmente i clienti ricevono 20 ore di consulenza a settimana, potreste scendere a 15.

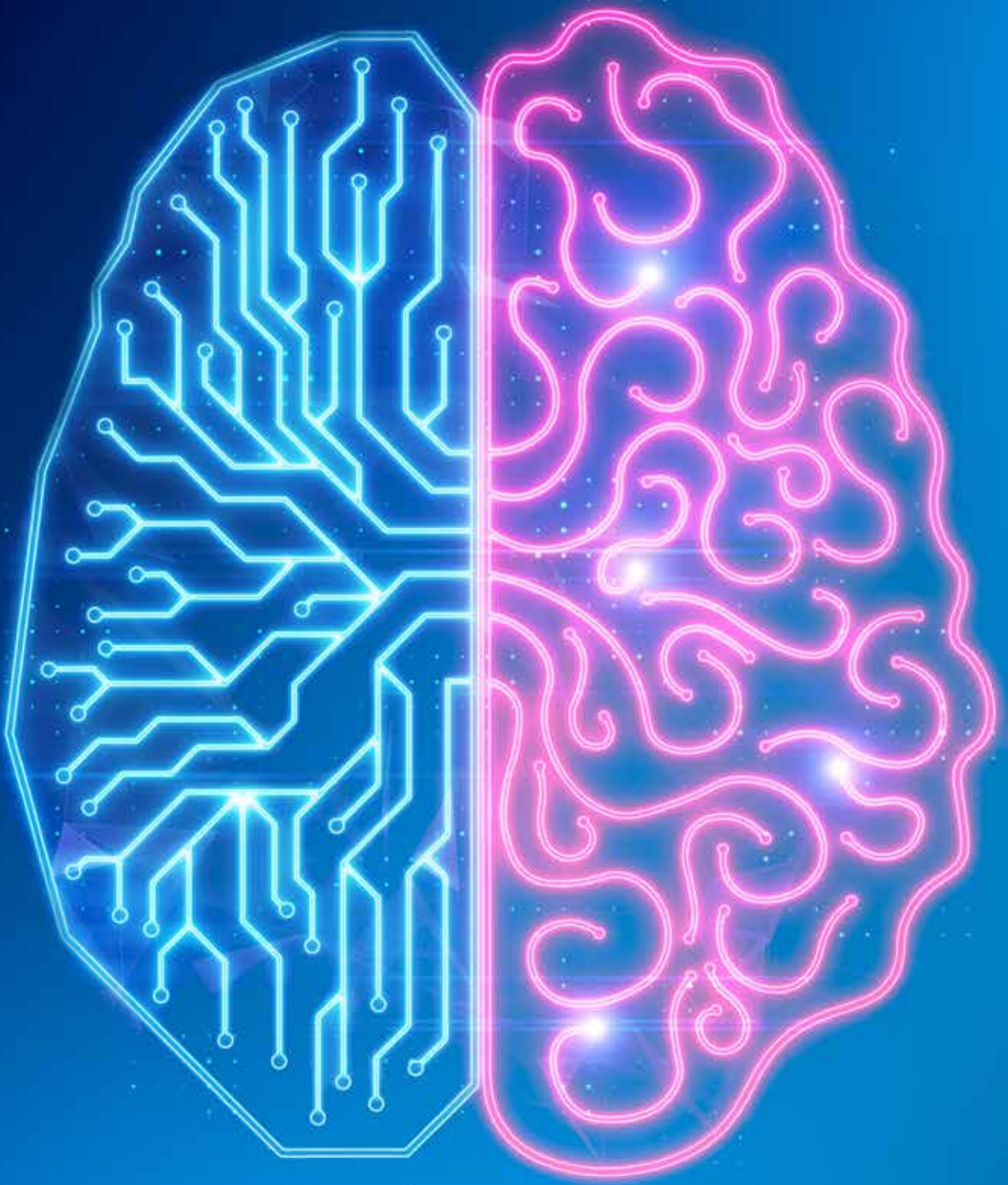
Le imprese di servizi hanno molte leve su cui agire. Provate ad aumentare le tariffe solo per i servizi che vi garantiscono i margini più ridotti, in modo da aumentare i profitti su attività che vi costano tempo senza generare grandi ricavi. Oppure, aumentate le tariffe solo per i servizi più richiesti: dato che sono quelli che vendete di più, un aumento anche minimo avrà un impatto positivo sui profitti.

L'idea alla base è fare di più con gli stessi mezzi. Quindi, o si aumentano i ricavi o si riescono a rendere operativi i costi. ❖

## Un premio per i clienti più fedeli

Considerate di usare un programma di fidelizzazione per i clienti che sono con voi da molto tempo e assicurategli la tariffa attuale, oppure offrite loro la possibilità di rinnovare il contratto a una percentuale inferiore rispetto al nuovo prezzo. Se dimostrerete di premiare la loro fedeltà, si sentiranno apprezzati e non li perderete.

In alternativa, se aumentate i prezzi su tutta la linea, ai clienti che sono con voi da un certo numero di anni offrite una funzionalità o un servizio esclusivo, come un account manager dedicato o un upgrade gratuito.



# L'intelligenza che gira intorno

AI, machine learning, reti neurali, deep analytics. Cerchiamo di capire di più sull'intelligenza al silicio che è già pervasivamente presente nella nostra vita.

di *Leo Sorge e Riccardo Florio*

**N**egli ultimi anni ci sono stati fortissimi game-changer, alcuni internazionali, altri nazionali. Tra quelli internazionali troviamo l'improvvisa sterzata sulla localizzazione del posto di lavoro e le conseguenze nel "cybermondo" dell'aggressione di Putin all'Ucraina. In Italia, a crescere, abbiamo visto le forme di contributo per la digitalizzazione, per l'industria 4.0 e il PNRR.

In questo contesto estremamente dinamico la rivoluzione digitale crea grandi opportunità per le aziende in grado di investire correttamente e, parimenti, grandi opportunità per i fornitori di software e servizi che considerino correttamente dati e sicurezza.

Tuttavia, orientarsi nel contesto delle nuove tecnologie non è facile e le aziende italiane si trovano di fronte a indicazioni contraddittorie persino a livello di terminologia.

## Una questione di terminologia

Una delle più interessanti avanguardie tecnologiche è l'intelligenza artificiale (AI) che promette rivoluzioni nella vita degli utenti e grandi opportunità per le aziende in grado di sfruttarne le potenzialità.

**Per il termine intelligenza artificiale non esistono né un dizionario comune, né un'unica definizione** e diventa, quindi, difficile coniugarlo in modo univoco con l'innovazione.

I tre aspetti che contribuiscono a generare confusione, creando ansia nei decisori di spesa, sono:

- la differenza tra AI generale e AI specifica;
- la regolarità nell'uso di AI nei vari settori;
- la valutazione del saldo nel numero di posti di lavoro in caso di adozione di una qualche forma di AI.

Partiamo da tre presupposti; il primo che l'intelligenza artificiale generale, ovvero quella che sostituisce completamente l'uomo, oggi non esiste (forse non esisterà mai); il secondo che l'adozione di tecniche commercialmente indicate come AI è molto meno regolare di altre forme di soluzioni software; che una sana strategia perseguita nel tempo porta comunque un'azienda a crescere per fatturato e numero di addetti.

### AI: la naturale evoluzione del software

La nuova componente del software, che spesso vediamo definita come AI può rientrare in numerose categorie di prodotto o servizio usate in azienda.

Tuttavia con una buona precisione potremmo comunque chiamarla "software moderno", o anche semplicemente software.

Basterebbe aggiornare la vecchia definizione di Niklaus Wirth, algoritmi + strutture dati = programmi, con algoritmi anche innovativi + tanti dati ben strutturati = programmi moderni. Certamente, rispetto al passato, si richiede la capacità di analizzare moltissime informazioni usando tecniche di deep learning.

Anche il possibile futuro della **quantum intelligence** sta proponendo, comunque, un'ottimizzazione di parametri con approcci completamente ripensati grazie al **quantum computing**.

Ne consegue che una visione più concreta e corretta delle applicazioni di intelligenza artificiale

### QUANTO VALE IL MERCATO AI?

Secondo la società di analisi Fortune Business Insight il **mercato globale** dell'intelligenza artificiale valeva 328 miliardi di dollari nel 2021, dovrebbe aumentare a 387 miliardi nel 2022 per arrivare a 1394 miliardi entro il 2029, con una crescita annuale composta stimata in oltre il 20%. Secondo altri analisti il mercato attuale ha un volume inferiore ma crescerà nel decennio a un ritmo anche doppio di quello previsto da Fortune Business Insight.

Il mercato dell'intelligenza artificiale è in **forte crescita anche in Italia**. Secondo l'osservatorio permanente sul mercato digitale di Assintel, passerà dagli 860 milioni di euro del 2021 a 1,1 miliardi nel 2022 fino a raggiungere 1,4 miliardi di euro nel 2023 con una crescita nel triennio di oltre il 40%.

è relativa a una **nuova classe di strumenti software capaci di analizzare enormi quantità di dati** (i cosiddetti Big Data) e di applicare algoritmi innovativi che permettono di **migliorare autonomamente la capacità di analizzare questi dati ed estrarre da essi informazioni utili**.

### L'intelligenza delle macchine al nostro servizio

Già oggi la nuova componente del software definita come AI può rientrare in numerose categorie di prodotto o servizio usate

diffusamente. Proviamo a fare qualche esempio. **Gli assistenti virtuali basati su machine learning (chatbot)** sono l'applicazione di AI attualmente più diffusa, capaci di imparare dai dati acquisiti per rispondere agli utenti. Durante la pandemia diverse regioni italiane li hanno utilizzati in affiancamento ai call center per indirizzare un cittadino, a seguito dei sintomi dichiarati e sulla base dei dati raccolti in precedenza, verso un medico, il pronto soccorso oppure per tranquillizzarlo.

**In ambito clinico a livello diagnostico e terapeutico** le potenzialità dell'AI sono enormi.

#### AIOPS CRESCE DEL 19% ANNUO

L'artificial intelligence for IT operations, in sigla AIOps, è l'applicazione dell'intelligenza artificiale per migliorare le operazioni IT: un mercato che Gartner stima varrà circa 2,1 miliardi di dollari a livello globale entro il 2025 (Market Guide for AIOps Platforms, 30 maggio 2022) con un tasso di crescita annuale composto del 19%.

Nello specifico, AIOps utilizza big data, analytics e le funzionalità di machine learning per raccogliere e aggregare gli enormi volumi di dati delle operazioni, distinguere in modo intelligente gli eventi significativi dal "rumore", individuare le cause e segnalarle all'IT per una risposta adeguata. In generale si parla di AIOps, indicando piattaforme e processi per prendere decisioni in modo più rapido e accurato, rispondendo subito agli incidenti di rete e di sistema.

#### RETI NEURALI E DEEP LEARNING

Al concetto di machine learning sono associati un'ampia gamma di algoritmi. Tra questi, uno di quelli che negli anni ha raccolto un vasto interesse è quello denominato rete neurale. Una rete neurale è un algoritmo di machine learning in cui le macchine sono addestrate ad apprendere utilizzando una simulazione matematica ispirata al modo con cui i neuroni sono connessi e interagiscono tra loro. I principali vantaggi delle reti neurali sono legati alla **capacità di operare correttamente anche in caso di input imprecisi o incompleti e di auto adattarsi alle modifiche dell'ambiente in cui opera**. Inoltre, l'elevato parallelismo che la caratterizza permette di processare rapidamente grandi volumi di dati. Tuttavia, sebbene siano in grado di trovare soluzioni a problemi difficili, i risultati non possono essere garantiti e sono solo approssimazioni della soluzione desiderata e un certo errore è sempre presente.

Un'altra terminologia che merita di essere ricordata è il **deep learning**.

Si tratta di un algoritmo di machine learning correlato al concetto di reti neurali nei casi in cui la rete neurale è molto grande e complessa. Queste reti neurali "più profonde" possono fare previsioni molto più complesse e i modelli di deep learning si sono dimostrati molto efficaci nell'affrontare problemi specifici, come il riconoscimento vocale o di immagini.

Tuttavia, anche nel futuro, il loro utilizzo sarà presumibilmente sempre di supporto ai medici e mai di sostituzione. A condizionarne l'affidabilità concorrono, infatti, sia l'impossibilità di avere un database di riferimento basato su dati omogenei per tipologia ma, soprattutto, problematiche di tipo etico, sociale e giuridico. Per esempio, in caso di errore la colpa sarebbe attribuibile al medico, allo sviluppatore del software, all'ospedale che provvede alla manutenzione o al venditore?

Si prevede che Machine Learning e intelligenza artificiale svolgeranno un ruolo determinante **nello sviluppo di tutte le fasi della rete 6G** (ma lo si valuta anche per il 5G attuale), dalla progettazione all'implementazione, all'operatività. Infatti, a mano a mano che la rete evolverà per supportare implementazioni native per il cloud, le funzioni di automazione basate su AI e ML risulteranno fondamentali per semplificare la gestione e l'ottimizzazione della rete.

Un altro esempio è la sperimentazione avviata in Italia nell'ambito della **sicurezza urbana preventiva** in cui l'AI è utilizzata per prevedere scippi, rapine, furti, borseggi, truffe e altri delitti di tipo cosiddetto "predatorio" che avvengono nelle città. Il sistema si basa su un protocollo tecnico e metodologico configurato per generare e impiegare strategicamente allarmi predittivi georeferenziati di possibili crimini, che vengono poi elaborati attraverso un modello previsionale di Machine Learning.

Un ruolo molto importante l'AI lo sta avendo **nella sicurezza informatica** per la sua capacità

## IL MACHINE LEARNING

Il **machine learning** è il modo di apprendimento di un'intelligenza artificiale e, proprio come gli uomini apprendono dall'esempio, dall'osservazione o dalla ripetizione, anche l'intelligenza artificiale può utilizzare più metodi di apprendimento:

L'apprendimento per esempio è il meccanismo che caratterizza i modelli che vengono detti di **machine learning supervisionato**, in cui al computer viene fornito un set di dati con "etichette" all'interno del set di dati che funge da risposta e, infine, impara a distinguere tra diverse etichette.

L'apprendimento per deduzione è il modello che caratterizza il **machine learning non supervisionato**, in cui il computer osserva schemi e, attraverso questi, impara a distinguere autonomamente nuovi gruppi e schemi. L'apprendimento non supervisionato non richiede etichette e può, quindi, essere preferibile quando i set di dati sono limitati e non dispongono di etichette.

L'apprendimento per condizionamento è il modello che caratterizza il **machine learning per rinforzo**, accade quando un programmatore istruisce un computer a individuare un certo modus operandi, ovvero a definire una serie di azioni a partire da un processo d'osservazione dell'ambiente esterno.

Idealmente, i risultati più accurati ed efficienti dell'intelligenza artificiale richiedono una combinazione di tutti i metodi di machine learning applicandoli alle casistiche a cui sono, rispettivamente, più idonei.

di individuare correlazioni nascoste all'interno dell'enorme numero di avvisi di sicurezza. AI e ML offrono un valido contributo per rilevare malware, analizzare il traffico di rete, individuare

## QUANTUM COMPUTING E AI QUANTISTICA

Il quantum computing è una tecnologia che sfrutta le leggi della meccanica quantistica per risolvere problemi troppo complessi per i computer classici.

I computer quantistici utilizzano le proprietà della fisica quantistica per archiviare dati ed eseguire calcoli.

A differenza dei computer classici che trasmettono informazioni in bit, i computer quantistici utilizzano qubit (bit quantistici). Come i bit classici, i qubit alla fine devono trasmettere informazioni come uno o zero, ma a loro differenza possono esistere in sovrapposizione ovvero rappresentare sia 1 sia 0 allo stesso tempo con una differente distribuzione di probabilità. La distribuzione di probabilità di un qubit (uno o zero) dipende dalla distribuzione di probabilità di tutti gli altri qubit nel sistema.

Per questo motivo, l'aggiunta di ogni nuovo qubit a un sistema ha l'effetto di raddoppiare il numero di stati che il computer può analizzare. L'algebra lineare quantistica fornirà un'accelerazione polinomiale, che migliorerà enormemente le prestazioni delle nostre reti neurali artificiali. L'aspettativa è, dunque, che possano eseguire miliardi di operazioni simultanee, fornendo quindi un'accelerazione alla risoluzione di problemi altamente complessi, inclusa l'intelligenza artificiale.

minacce interne tramite l'analisi sulle anomalie di comportamento degli utenti, bloccare spam e phishing, proteggere i dati mobili e le App, aiutare gli analisti della sicurezza umani in tutti gli aspetti del loro lavoro e automatizzare attività di sicurezza ripetitive. **Gli esempi possibili si estendono a moltissimi ambiti:** domotica, logistica

dei magazzini, analisi predittiva, supporto dei processi decisionali e delle esperienze di acquisto, elaborazione e interpretazione del linguaggio naturale, realtà aumentata, riconoscimento di persone, animali e cose, applicazioni di guida autonoma, robotica e altro ancora.

Ciò appare incontrovertibile è che, in un mondo sempre più digitale, che produce enormi volumi di dati e che si basa sempre più sulla loro elaborazione, intelligenza artificiale e machine learning saranno sempre più intorno a noi, in ogni aspetto della nostra vita. ❖

## INTELLIGENZA ARTIFICIALE GENERATIVA

L'AI generativa è una forma di intelligenza artificiale che apprende una rappresentazione digitale di artefatti da dati campione e la utilizza per generare nuovi artefatti originali e realistici, che mantengono una somiglianza con i dati utilizzati per l'addestramento senza però ripeterli.

Gli artefatti in ingresso possono essere contenuti (come dati, testo, codice), mentre l'output può essere nella stessa forma dell'input o in una nuova modalità (come informazioni simulate sui dati di mercato).

L'AI generativa è destinata a rimodellare molte aree dell'azienda, dai prodotti, ai contenuti e all'esperienza dei clienti, fino all'analisi, all'ingegneria del software e ai metodi di apprendimento dell'AI. Un esempio di applicazione immediata nei servizi bancari e di investimento è l'applicazione di dati sintetici per espandere i modelli di frode e rilevare frodi finanziarie e strategie di riciclaggio di denaro. Le reti neurali possono essere applicate nei casi in cui si utilizzano anche dati sintetici, poiché questa tecnica consente di individuare nuove regole.

# AI e metaverso: arrivano i server Ipsor con chip specializzati Biren

Mentre gli USA bloccano l'esportazione dei "chip per il metaverso" di AMD e Nvidia, l'azienda cinese Biren annuncia nuovi chip e punta ai server di Ipsor

di **Leo Sorge**

Il Governo degli Stati Uniti ha bloccato l'export di chip per l'AI verso la Cina. Secondo Reuters, il blocco è stato chiesto il 1° settembre a nVidia e AMD. Ma che effetto reale avranno sulla competizione mondiale, senza andar oltre?

Li chiamiamo "chip per il metaverso", ma anche "chip per l'intelligenza artificiale" e in alcuni casi anche "chip per il quantum computing". Al di là dei nomi, è evidente che esistono molte nuove tecnologie che andranno a arricchire i server per il cloud computing. Recentemente del metaverso si enfatizza il front end, un piano sul quale le differenze tra device causeranno non pochi problemi. In realtà esiste anche un back end, nel quale la visualizzazione non conta.

Visto il generale trend non stupisce che Intel, nonostante una forte attività proprietaria nello specifico settore, abbia dichiarato di voler implementare un nuovo approccio indipendente dall'hardware sottostante, dal silicio dei chip insomma, senza seguire un atteggiamento di chiusura sui suoi prodotti. D'altronde se ha nominato vicepresidente esecutivo Raja Koduri,

precedentemente a capo dell'area GPU, ci sarà un motivo.

Certamente non stupisce nemmeno che in questo mercato nVidia abbia una posizione di grande forza, di grande capacità di federazione, ma che sotto sotto si stia specializzando nella realizzazione di digital twin, un metaverso nel quale il portale è il sensore e il robot e non l'essere umano e nel quale la visualizzazione è marginale, per non dire inutile.

Anche senza voler sconfinare nel metaverso, una capacità di calcolo specifica per l'AI serve oggi in moltissimi casi.

Il settore sta crescendo moltissimo e una corretta strategia sarà essenziale per qualsiasi operatore di calcolo.

## **Biren, dalla Cina 77 miliardi di transistor per l'AI**

Almeno in parte, invece, stupisce la disponibilità quasi immediata di chip cinesi per l'AI. La cinese Biren, infatti, ha lanciato la serie 100, con un numero di transistor paragonabile, appunto circa



100 miliardi. Ed è strano che il blocco dei chip USA sia venuto pochi giorni dopo questo annuncio. Nel chip Biren vengono adottate delle tecnologie interessanti, anche se non sempre innovative, che offrono risultati molto elevati in pattern d'uso alle volte innovativi.

Le configurazioni di lancio sono due, la 100 e la 104. La base è il BR104, che offre la possibilità di mettere in comunicazione fino a tre chip. Il BR100 dichiara prestazioni esattamente doppie del 104, con collegamento fino a 8 chip grazie alla connessione proprietaria BLink™.

Biren afferma di usare la tecnologia 7n di TSMC e di aver dovuto sfruttare i chiplet e la tecnologia CoWoS 2.5D. L'espressione 7n fa riferimento alla dimensione dei singoli transistor, ma in realtà già da tempo non ha un diretto senso metrico anche se indica comunque l'avanzamento tecnologico.

Più interessante il design a chiplet, che prevede di smembrare il chip monolitico in varie unità funzionali di ridotte dimensioni, appunto i chiplet. Questi possono anche essere realizzati in tecnologie diverse. Il chip on wafer on insulator permette di impilare chip uno sull'altro in modo da ottenere ottimizzazioni incrociate per prestazioni, distribuzione di alimentazione e

superficie complessiva..

I chip Biren verranno messi su un AI server Inspur a 8 vie i cui primi campioni saranno disponibili a partire dal quarto trimestre del 2022. Inspur è un fornitore di data center cinese che Gartner colloca tra i primi tre produttori di server al mondo. I primi clienti dovrebbero essere Baidu e China Mobile.

A fine anno potremo vedere i chip Biren nei server Ipsor, sempre cinesi. A molti questo nome non dice niente, ma agli esperti dice molto, se anche Gartner ha messo questa azienda tra i primi tre produttori di server del mondo nella specifica area dei data server. Il fenomeno potrebbe non essere irrilevante neanche su scala mondiale. L'importanza della competizione nel mondo dei chip per materiali e fabbriche, ma anche vere e proprie guerre, possiamo immaginare che il panorama che ci attende metterà parecchio stress nel mondo del cloud e dei data center. Questo stress creerà nuove opportunità per pochi operatori avvenuti dentro le segrete cose e molte difficoltà in chi, per dimensioni od opacità, non vedono abbastanza lontano rispetto a quanto viene richiesto oggi e nei prossimi mesi. ❖

# Dalla sicurezza alla resilienza

Resilienza è la nuova key word per definire un nuovo modello di protezione capace di fronteggiare i rischi della trasformazione digitale

*a cura di Riccardo Florio*



La trasformazione digitale (DT) sposta sistemi, processi e dati in una direzione che è più connessa, mettendo in evidenza l'esigenza di costruire la resilienza aziendale. La resilienza aziendale è la capacità di un'organizzazione di affrontare il rischio strategico, finanziario, operativo e informativo in modo da guidare la crescita aziendale, la redditività e la modernizzazione ovvero la trasformazione digitale.

### La cyber resilienza

La cyber resilience è la componente che affronta il tema del rischio informatico per mettere un'azienda nelle condizioni di fornire in modo continuo e affidabile un risultato previsto, nonostante eventi informatici avversi (attacchi e minacce varie). La cyber resilience consente alle organizzazioni di proteggere il business, ridurre il tempo di esposizione alle minacce informatiche e ridurre l'impatto degli attacchi per garantire la sostenibilità continua.

Un'organizzazione cyber-resiliente può adattarsi a crisi, minacce, avversità e sia note sia sconosciute. L'obiettivo finale della resilienza informatica è, dunque, essere in grado di prosperare di fronte a condizioni avverse (crisi, pandemia, volatilità finanziaria, ecc.).

Conseguire la cyber resilience significa anche porre le condizioni per ridurre gli incidenti aumentando la capacità aziendale di stabilire le priorità e rispondere ai rischi. Diminuire le possibili multe e sanzioni, minor rischio di violazione e un miglioramento nella reputazione.

### I 4 pilastri della cyber resilienza

- 1** Conseguire la cyber resilienza richiede, innanzitutto, una capacità avanzata di rilevamento e risposta alle minacce note e sconosciute.
- 2** Un altro presupposto fondamentale è l'approccio Zero Trust, che realizza un modello di governance delle identità digitali e di gestione dell'accesso basato su regole, pensato per non assegnare a priori alcun tipo di fiducia e per assicurare che ogni utente (anche e soprattutto quelli con privilegi avanzati) non possa accedere a risorse che non gli sono necessarie per lo svolgimento del suo lavoro.
- 3** Il terzo pilastro della cyber resilience è il concetto di "privacy by design" per proteggere i dati sensibili (strutturati e non strutturati) durante il loro intero ciclo di vita.
- 4** L'ultimo pilastro fondamentale è l'adozione di DevSecOps ovvero di un framework che integri la sicurezza all'interno dei processi DevOps e che CyberRes realizza attraverso gli strumenti della famiglia Fortify per accelerare il processo di sviluppo e automatizzare i test di sicurezza statici, dinamici e in ambiente mobile delle applicazioni.

La cyber resilience svolge un ruolo fondamentale nel guidare la trasformazione digitale (che quindi consente la resilienza e la continuità aziendale) e, per esempio, le organizzazioni che incorporano la sicurezza informatica in modo nativo sono maggiormente in grado di guidare piattaforme di sviluppo ad alta velocità (Agile), robuste e resilienti.

### Cyber resilienza vs cyber security

I framework di sicurezza informatica esistenti come NIST e MITRE forniscono ottime linee guida per i team che si occupano di sicurezza IT ma la rapida e continua evoluzione nello scenario delle minacce, indotta anche dall'avvento della DT e del cloud, obbliga a indirizzarsi verso politiche di cyber resilience in grado di evolversi e adattarsi a questo ritmo crescente di cambiamento per garantire il necessario livello di sicurezza

Ciò che viene richiesto alle aziende è la capacità di adattarsi in modo intelligente e di focalizzarsi su protezione di identità, applicazioni e dati all'unisono fornire risultati ottimizzati che a loro volta consentono alle organizzazioni di stare al passo con il cambiamento.

Cyber security e Cyber resilience sono due concetti che hanno punti in comune ma differenti: mentre la sicurezza informatica descrive la capacità di un'azienda di proteggersi dalle minacce informatiche, la cyber resilienza in-

### Le tecnologie abilitanti

Un'efficace strategia di cyber resilience dovrebbe includere componenti di più soluzioni di sicurezza informatica che comprendono:

- **Intelligenza artificiale e machine learning:** con l'enorme volume di dati generati dalle soluzioni di sicurezza, l'uso di sistemi in grado di analizzare comportamenti e rischi e automatizzare la risposta aumenta significativamente la capacità di un'organizzazione di adattarsi in modo intelligente alle vulnerabilità e agli attacchi.
- **Sicurezza dei dati** sia strutturati che non strutturati che devono essere analizzati per rimanere conformi alla privacy e ad altre normative governative
- **Sicurezza delle applicazioni** a partire dal processo di sviluppo per estendersi all'intero ciclo di vita.
- **Identità e gestione degli accessi** per gestire chi e cosa accede ai tuoi sistemi e dati, sviluppare identità con accessi coerenti al tipo di attività svolto e conoscere i modelli normali di queste identità per identificare anomalie di comportamento.
- **Security operation** per migliorare la produttività prevedendo sistemi di orchestrazione, automazione e risposta della sicurezza (SOAR) e sistemi SIEM (Security Information and Event Management).

formatica si riferisce alla capacità di un'azienda di mitigare i danni di diversa natura (per esempio a sistemi, processi, reputazione) riuscendo a continuare a svolgere il proprio compito primario anche quando i sistemi o i dati sono stati compromessi. Inoltre la cyber resilienza copre sia gli attacchi informatici sia gli inconvenienti causati dalle minacce non contraddittorie (ad esempio, il semplice errore umano). Il concetto riunisce, essenzialmente, le aree della sicurezza delle informazioni, della continuità aziendale e della resilienza organizzativa. ❖

# Doxing, intimidire attraverso le informazioni

Dati personali allo sbaraglio pronti per essere usati per ricattare o mettere alla gogna diffondendole nel web. Ma ci si può proteggere da questi attacchi senza grossa fatica

di **Maurizio Ferrari**

I social sono diventati, inutile negarlo, parte integrante della nostra vita. In questi anni le piattaforme si sono moltiplicate, ognuna con delle caratteristiche particolari, ma tutte contengono delle informazioni che volontariamente o involontariamente abbiamo inserito. Tutto questo ci espone a quello che viene chiamato in gergo “doxing”, la pratica di diffondere informazioni, soprattutto quelle private, relative a una persona a un pubblico il più vasto possibile con lo scopo di danneggiarla. Per meglio comprendere i rischi a cui spesso ci sottoponiamo facciamo un esempio: tutti cerchiamo informazioni riguardo una persona da incontrare sul web, informazioni che noi usiamo per farci un'idea. Ma se una persona è stata fatta oggetto di doxing in rete si trovano informazioni



private riguardanti la salute, la vita privata dei figli o dei familiari o degli amici. Informazioni che l'interessato avrebbe preferito che rimanessero private e non esposte al mondo. E questo accade molto più spesso di quanto si possa immaginare. Uno studio inglese "The Impact of Online Abuse: Hearing the Victims' Voice" del giugno del 2022 realiz-

zato dall'associazione Victims' Commissioner ha evidenziato come il 19% degli intervistati è stato vittima di doxing. Le vittime vengono, attraverso la pubblicazione online di informazioni private, spaventate, messe in imbarazzo e a disagio. Perché viene fatto? Per estorcere denaro alle vittime, per creare un danno o perché chi pubblica si sente un giustiziere. Negli Usa, dove c'è un forte attrito tra i fan di Trump e il mondo liberal, c'è una vera e propria guerra combattuta con il doxing. Entrambe le parti utilizzano questo strumento per gettare nel fango i propri antagonisti politici, esacerbando gli animi di entrambe le parti. Molti hanno perso il lavoro, altri hanno dovuto cambiare casa e frequentazioni. Il doxing può avere un forte impatto sulla vita sociale di una persona, costringendola a gesti estremi, oltre a dover cambiare in modo radicale vita (lavoro, amici e allontanarsi dalla famiglia), alcune vittime sono arrivate al suicidio come un medico austriaco pro-vaccinazioni contro il Covid-19 messo alla gogna da chi credeva la pandemia una bufala. Come fare per proteggersi da tutto questo? Usando in modo intelligente i social, innanzitutto, perché tutti possiamo esserne vittime. Come regola generale può valere quella di mettere meno informazioni personali possibili online, se non ci sono sarà difficile

***Il doxing può avere un forte impatto sulla vita sociale di una persona, costringendola a gesti estremi***

trovare qualcosa da usare contro. Sui social utilizzare l'autenticazione a due fattori o più (2FA, MFA) in tutti gli account e una password forte e unica. Chiamate e videochiamate private e criptate, e bisogna sempre avere la certezza che i link che arrivano da persone conosciute o amici siano stati inviati intenzionalmente e quelli degli sconosciuti non aprirli in nessun caso. Consigli che già un pubblico adulto spesso non segue, figuriamoci le nuove generazioni. Sono loro le nuove vittime, specialmente quelli che utilizzano piattaforme di gioco online. Luoghi che sembrano accentuare questo desiderio di vendetta e rivalsa, e scatenare il doxing e anche altre forme di cyberbullismo. Le vittime di questa pratica possono reagire coinvolgendo le piattaforme dove è stato pubblicato per far rimuovere le informazioni e bloccare chi le ha usate, facendo screenshot e raccogliendo tutto il materiale per consegnarlo alle autorità competenti. Contattare la propria banca per verificare che conti correnti e carte di credito siano al sicuro. E pensare di sospendere la propria presenza sui social per un po'. Non in tutti gli ordinamenti la divulgazione di informazioni senza autorizzazione è considerato reato, ma lo sono diverse conseguenze del doxing, come le frodi finanziarie e i danni fisici alla persona. ❖

# Cyber resilienza e machine learning: un binomio indissolubile

Le soluzioni software di CyberRes aumentano il livello di resilienza sfruttando la comprovata tecnologia ArcSight Intelligence di machine learning non supervisionato.

di **Riccardo Florio**

La tua azienda ha davvero bisogno del machine learning per essere cyber-resiliente? La risposta è sì o, perlomeno, è sì per ottenere un grado di resilienza ragionevolmente elevato.

**Essere cyber resilienti significa, infatti, garantire la continuità operativa mentre l'infrastruttura aziendale si trova a dover affrontare continue minacce e attacchi.** È un obiettivo che richiede la capacità di organizzare sistemi, tecnologie e processi in modo tale che sia possibile predisporre le contromisure necessarie per identificare minacce di ogni tipo, bloccare attacchi ed eliminare vulnerabilità prima ancora che l'infrastruttura ne sia interessata. Si tratta di un compito particolarmente complesso se si considera che, ogni giorno, vengono creati migliaia di nuovi malware, che vanno da virus, adware, trojan, keylogger, ransomware a cui si aggiungono le minacce provenienti dall'interno.

## **Analizzare le anomalie di comportamento per una difesa efficace**

Nel tentativo di contrastare l'evoluzione degli attacchi, le tecnologie di protezione si sono evolute puntando su sistemi sempre più sofisticati di identificazione delle minacce

che provvedono a generare qualche tipo di avviso o evento di sicurezza. Già da tempo, questo approccio ha dato origine a veri e propri Big Data di sicurezza che richiedono sofisticati motori di analisi e correlazione per poter essere esaminati in modo automatizzato.

Molti di questi strumenti si limitano, tuttavia, a effettuare



**Pierpaolo Ali**

Director Southern Europe, Russia, CIS,  
CEE & Israel di CyberRes

un confronto con minacce già rilevate, presupponendo, implicitamente, che l'azienda possa difendersi solo nel caso in cui non rappresenti il primo bersaglio di una delle migliaia di nuove minacce citate prima. Altri strumenti prevedono tecnologie di analisi euristica che analizzano, essenzialmente, file sospetti alla ricerca di varianti di minacce note che potrebbero sfuggire all'identificazione.

Tutto ciò **lascia scoperta un'ampia gamma di minacce come quelle, per esempio, legate ad accessi effettuati tramite credenziali autentiche sottratte**, che non vengono rilevate dalle soluzioni standard proprio perché, formalmente, si tratta di accessi legittimi.

È proprio nel contrasto a questo tipo di minacce che servono sistemi di machine learning capaci di apprendere il comportamento di un utente e valutare (aggiornando costantemente i criteri di valutazione) se è anomalo oppure se rientra nelle sue abitudini.

*"L'anomalia di comportamento emerge dal confronto di molteplici fattori quali orario di accesso, località, tipo di dati acceduti, durata della connessione e così via - osserva Pierpaolo Ali, Director Southern Europe, Russia, CIS, CEE & Israel di CyberRes - ognuno dei quali, singolarmente, apparentemente trascurabile, ma che nel complesso assume un carattere di rischio significativo. Questo tipo di analisi è essenziale per restare resilienti e richiede una tecnologia di machine learning non supervisionato come ArcSight Intelligence".*

## **Il machine learning delle soluzioni CyberRes**

**ArcSight Intelligence è la tecnologia di machine learning non supervisionato** integrata nella gamma di soluzioni software CyberRes pensata per effettuare analisi di sicurezza di tipo predittivo.

Riunisce, infatti, funzionalità di analisi del comportamento



di utenti e entità (User and Entity Behaviour Analytics, in sigla UEBA) con tecnologie di machine learning per fornire analisi rapide e accurate di rilevamento delle minacce.

Si basa sull'**attribuzione di indici di rischio individuali, definiti in base all'analisi del comportamento di un utente** rispetto al suo modello esperienziale o a quello di utenti con un profilo analogo.

Gli aspetti caratteristici comprendono:

- un motore di analytics molto esteso che prevede molteplici "use case" pronti all'uso;
- un modello di elaborazione basato su una libreria di oltre 400 modelli di machine learning e analytics;
- un'architettura altamente scalabile integrabile con le più diffuse tecnologie open source per la gestione dei Big Data.

In particolare, questa tecnologia di "intelligence" o machine learning è integrata all'interno di ArcSight, la famiglia di soluzioni SIEM (Security Information and Event Management) di CyberRes. ArcSight fornisce, pertanto, una soluzione capace di riunire la capacità di analisi intelligente sulle anomalie di comportamento con quella di analizzare grandi quantità di dati in tempo reale e rilevare minacce riconducibili a casistiche note, rappresentando una formidabile difesa contro ogni tipo di minaccia. ❖

# Come cambiano i paradigmi della protezione aziendale

È sempre più complesso difendersi dalle minacce informatiche, e per limitare i rischi della sicurezza IT occorre un approccio alla security più globale. Una soluzione arriva da Stormshield.

di **Riccardo Florio**

**G**li attacchi informatici oggi rappresentano la maggiore preoccupazione per le aziende: la violazione della sicurezza rappresenta, infatti, un fermo delle funzionalità operative, la perdita di dati e la sottrazione delle credenziali più critiche. Un rischio per le aziende costrette ad affrontare nuove sfide della cybersecurity ricorrendo alle più evolute soluzioni di sicurezza informatica. Ma questo non basta, occorre urgentemente un'inversione di rotta in termini di consapevolezza verso questo tema, è necessario oggi un nuovo approccio alla sicurezza a tutto tondo.

Ne abbiamo parlato con **Alberto Brera, Country Manager di Stormshield per l'Italia**, per comprendere le evoluzioni delle minacce e i rischi per le aziende

## **Come stanno cambiando le minacce e quali sono i nuovi rischi per le aziende?**

**»** I cybercriminali hanno rapidamente adattato il loro modus operandi ai nuovi modelli lavorativi che prevedono una fruizione sempre più fluida delle risorse aziendali "from anywhere". Questo processo di estrema estensione del perimetro aziendale ad ambienti e strumenti mal protetti (pc personali, infrastrutture IT ombra per far fronte ad emergenze e simili) ha favorito l'affinamento e l'industrializzazione degli strumenti impiegati per carpire con successo credenziali di accesso alle reti, di cui gli attaccanti abusano sia per lanciare attacchi di massa, sia per infiltrare malware

che colpiscono le risorse di interesse attraverso movimenti laterali. Inoltre, gli aggressori si stanno strutturando in vere e proprie organizzazioni che commercializzano in maniera estremamente professionale l'accesso a reti compromesse (IAB - Initial Access Brokers), malware preconfezionato "as a service", strumento prezioso per cybercriminali privi di particolari competenze tecniche, e/o i dati esfiltrati nel corso di un attacco ransomware di successo. Questo sviluppo ha consolidato il primato del ransomware sulle altre minacce, seguito a ruota da attacchi mirati e sofisticati ai



Alberto Brera  
Country Manager di Stormshield per l'Italia

danni di industria, infrastrutture critiche e aziende di rilievo.

### **Le minacce dall'interno hanno un peso crescente o in diminuzione**

🗨️ In termini di cybersecurity il fattore umano è da sempre una vulnerabilità, un dato di fatto ben noto ai cybercriminali, che nel frattempo offrono via dark web laute ricompense agli addetti che forniscono il proprio accesso alle reti o dati aziendali riservati. Per non parlare di situazioni all'ordine del giorno, come i casi di leakage da parte di personale che lascia l'azienda o la perdita dei dati per furto o smarrimento dei terminali. Un quadro aggravato anche dall'irrisoria attività di sensibilizzazione di dipendenti, manutentori e collaboratori esterni verso l'igiene digitale, nonostante sia noto che un utente consapevole può evitare autonomamente molti rischi. L'impiego di strumenti di lavoro non propriamente professionali in ambienti domestici o pubblici mal protetti, pur di garantire la continuità operativa, si è rivelato un formidabile vettore accidentale di attacco, poiché ha spesso luogo al di fuori delle policy di sicurezza aziendali.

Tra le misure prese invece per ovviare alle minacce più grossolane abbiamo, da un lato, un notevole incremento del contingente di connessioni VPN attivabili (attraverso cui – ed è bene specificarlo – è comunque possibile infiltrare accidentalmente malware nella rete aziendale) e, dall'altro, un irrigidimento dei modelli Zero-Trust a discapito delle esigenze di flessibilità di postazioni di lavoro sempre più fluide.

Alla luce di un crescente peso delle minacce dall'interno, non meraviglia che si parli sempre più spesso di assegnare ai dipendenti in "smart working" computer e smartphone aziendali in linea con le policy di sicurezza e i modelli Zero-Trust, dotati di un buon livello di protezione (idealmente tramite soluzioni EDR o HIPS) e di una soluzione di cifratura dei dati (non del sistema) agnostica al tipo di piattaforma di archiviazione impiegata, come arma risolutiva. Purtroppo, però, spesso nelle PMI come nelle grandi aziende manca

la comprensione della necessità di investimenti di questa portata e di conseguenza il budget corrispondente.

### **Spostare dati e applicazioni in cloud aumenta o diminuisce il rischio?**

🗨️ Il cloud ha rappresentato "la salvezza" per i più negli scorsi due anni e mezzo, a tal punto che ha originato vere e proprie infrastrutture IT ombra (shadow IT) con cui molti IT manager fanno i conti ancora oggi. Spostare dati e applicazioni nel cloud non è un elemento di rischio in sé, bensì a fronte delle condizioni d'utilizzo. Dove sono archiviati i dati? Fino a che punto terzi (sia anche il fornitore del servizio di hosting o della piattaforma cloud) possono accedere ai dati? Quali le misure di sicurezza IT e di disaster recovery implementate? Prima di affidare i propri asset digitali e anche parzialmente la propria infrastruttura IT/TLC a operatori cloud, occorre avere risposte certe e SLA che evidenzino chiaramente le responsabilità dell'operatore, e non solo dell'utente, in caso di incidente informatico.

### **Come devono cambiare i paradigmi di protezione a livello tecnologico per fronteggiare i nuovi rischi?**

🗨️ Più che una variazione del paradigma di protezione a livello tecnologico occorre urgentemente un cambio di passo in termini di sensibilità alla tematica e di approccio alla sicurezza a tutto tondo, comprendendo che la cybersecurity non è un prodotto che si compra da uno scaffale per poi installarlo e dimenticarsene, ma un percorso indissolubilmente legato al fattore umano, ai processi, alle esigenze e alle modalità operative aziendali che va ben al di là di criteri di valutazione puramente tecnici. Un percorso che dovrebbe prevedere persino una "second line of defense". Tuttavia, fino a quando la sicurezza sarà percepita come un costo "obbligato" e non come il "business enabler" che è, CISO e responsabili IT dovranno sempre lottare per un budget che corrisponda al potenziale impatto di un attacco sulla produttività e all'effettiva superficie di attacco dell'azienda.

## **A livello strategico come dovrebbero conciliarsi ICT security e cyber-resilienza?**

☞ Come già detto, la sicurezza è un business enabler, e in quanto tale pilastro essenziale di una strategia volta a incrementare la cyber-resilienza delle imprese. Con cyber-resilienza si intende l'abilità di un dato processo o di una infrastruttura di resistere ad un attacco senza gravi ripercussioni sulla disponibilità delle risorse, sulla produttività o sull'integrità del bacino di dati. A tale scopo, la cybersecurity fornisce strumenti di analisi e risoluzione delle vulnerabilità, di segmentazione della rete, di identificazione e blocco di comportamenti anomali, di connessione sicura alla rete da remoto e di implementazione

di modelli zero-trust che si adattano automaticamente all'ambiente di lavoro (interno / privato / pubblico), allo strumento impiegato (postazione di lavoro fissa o mobile ecc.) e alle risorse aziendali autorizzate a seconda del profilo dell'utente (luogo, orario, strumento, applicazioni, diritti di accesso) in un dato momento. Naturalmente gli strumenti di cybersecurity sono per lo più preventivi, contribuiscono quindi a ridurre a priori l'impatto di un potenziale attacco, ma essenziale per la cyber-resilienza è l'irrinunciabile incremento della consapevolezza degli utenti in merito al loro ruolo quale primo baluardo di sicurezza e l'implementazione di piani accurati per il repentino ripristino dei sistemi compromessi e dei dati. ❖

### **La risposta di Stormshield**

Stormshield risponde a queste esigenze in primis attraverso un portafoglio di prodotti altamente integrati e sviluppati secondo il principio della "collaborative security" interamente in house (Francia), quindi fortemente legato alle consuetudini e alle normative europee in fatto di protezione di dati e infrastrutture. I firewall UTM/IPS hardware e virtuali Stormshield Network Security anche per ambienti industriali fungono da gateway VPN, analizzano e bloccano in tempo reale flussi di dati e/o comandi anomali, i tentativi di attacco dall'esterno come di accesso a risorse non autorizzate dall'interno e sono il punto di partenza per l'applicazione di policy di sicurezza a tutti i device presenti in azienda. Stormshield Endpoint Security Evolution è uno HIPS per computer e server che non necessita di alcuna connettività internet per funzionare. SES Evolution non solo contribuisce attivamente all'implementazione dei profili utente Zero-Trust ma, frapponendosi tra il sistema operativo e le applicazioni, impedisce che richieste anomale al sistema operativo (ad esempio l'improvvisa cifratura della macchina) si tramutino in azione. Stormshield Data Security infine assicura una cifratura dei dati punto-punto agnostica rispetto allo strumento utilizzato per visualizzare i file e alla piattaforma su cui i dati sono archiviati. Anche questa soluzione supporta le policy Zero-Trust: solo specifici addetti ai lavori possono visualizzare i dati in chiaro, che restano inintelligibili per chiunque altro. Le chiavi di cifratura restano in possesso dell'azienda che può sostituirle o invalidarle in qualunque momento, una caratteristica utile presso società con una forte fluttuazione del personale o con un ampio numero di collaboratori esterni.

Oltre ad un approccio completo alla sicurezza IT made in Europe, in Italia Stormshield dispone di una filiale che si differenzia sul mercato per il tipo di rapporto e il legame che intrattiene con i propri partner. L'azienda ha adottato sin dai suoi albori una strategia commerciale 2-tier, il canale è quindi la colonna portante del successo di Stormshield sul territorio. Per questo motivo Stormshield forma e certifica i propri partner a valore, eroga supporto pre- e post-vendita attraverso un team di tecnici locale e collabora al fianco dei partner che lo desiderano all'elaborazione e alla gestione di progetti complessi. Tutti servizi erogati per assicurare che le organizzazioni che decidono di dotarsi di una cybersecurity allo stato dell'arte intraprendano questo percorso con un partner competente e in grado di dotarli dei migliori strumenti a lungo termine.

# Applicazioni critiche: cloud vs local

È cambiato il discrimine tra cloud e on-prem, ma per saperlo la base è sempre un reale assessment. Passiamo in rassegna alcuni snodi per la scelta

di **Leo Sorge**

È cambiato il discrimine tra cloud e on-prem, ma per saperlo la base è sempre un reale assessment. Passiamo in rassegna alcuni snodi per la scelta

Il cloud rappresenta un approccio ancor oggi innovativo per affrontare la trasformazione digitale. Commercialmente mantiene una robusta accelerazione: il cloud crescerà ancora del 16% annuo, valore composto tra il 2022 e il 2030, nella valutazione di Grand View Research, non solo per le aziende grandi ma anche per le piccole e medie.

È quindi la panacea per tutti i mali? Ovviamente no: una soluzione unica non esiste mai e la nuvola non sfugge alla regola.

Ciascuna area innovativa, infatti, vede nel cloud una soluzione che scambia il controllo con la comodità: resta pur sempre un livello oltre il quale l'azienda deve mantenere un controllo totale. Se vogliamo, è proprio questo il punto centrale sulle applicazioni critiche.

E' quindi sempre lecito individuare delle aree nelle quali è preferibile il cloud, ma anche delle altre nelle quali l'on premises può essere la miglior scelta. Abbiamo scelto alcuni punti rilevanti, ma altri ne esistono e possono essere determinanti in altri settori produttivi. In linea di principio, comunque, ciascun tipo di carico può essere affrontato con un mix di soluzioni che lasciano il controllo al cloud o all'on-premises: alla base del successo c'è sempre un corretto e continuo assessment.

## 5 MOTIVI PER NON SALVARE LE APPLICAZIONI CRITICHE NEL CLOUD

Banda passante, analisi dei dati, flusso di sviluppo del software, data residency e aderenza alle normative presentano delle sfide che può convenire gestire in casa.

### 1 Serve internet di qualità

Per affidarsi al cloud serve una buona internet, secondo tutti gli schemi necessari all'azienda o all'organizzazione. Nel tempo, inoltre, questa richiesta finora è sempre cresciuta. Non tutte le aree italiane danno garanzie, ora e nell'immediato futuro, neanche valutando la geografia di crescita della rete 5G e anche l'idea di celle 5G ad uso interno.

### 2 Artificial intelligence

Parlando di AI, con un paradigma che per buona parte era valido già per la business intelligence, conviene adottare una soluzione on-prem se i risultati attesi sono molto alti e richiedono un elevato controllo in tutte le fasi, dai dati agli algoritmi, dalla privacy alla sicurezza. Per la maggior parte delle PMI, quindi, la soluzione standard applicata al proprio business andrà benissimo in cloud. Ma non per tutti.

### 3 Patch & Fix

Il cloud toglie i problemi di aggiornamento di sistema all'IT locale, ma impone i suoi. L'area softwa-

La percezione aziendale delle sfide ICT.  
Immagine Datapine su dati Flexera

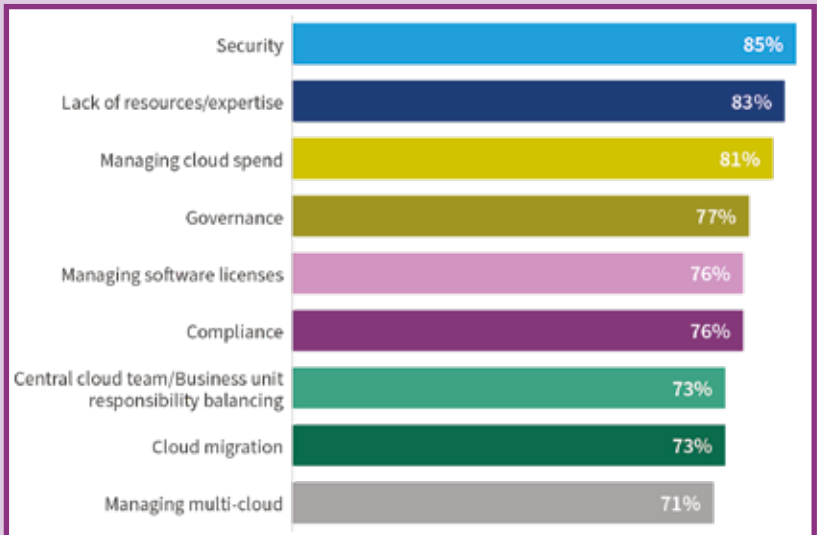
re development deve prenderne atto: patch e fix arrivano dal fornitore e alle volte hanno effetti indesiderati rispetto ad un patrimonio software che fino a quel momento funzionava egregiamente. Si tratta di uno degli aspetti legati al modello ad abbonamento, che se mal gestito rischia di portare al vendor lock-in.

#### 4 Data Residency, la certezza della posizione dei dati

In alcuni casi, il cloud non permette di avere certezza della locazione geografica nella quale sono tenuti i dati aziendali. La questione si complica con il multi-cloud. Quando è assolutamente necessario che una parte dei dati sia tenuta in una determinata area geografica, quei dati devono essere sottratti al cloud. Anche qui, un corretto assessment e stringenti policy da adottare nel tempo permettono d'individuare i dati non trasferibili, lasciando libertà sulla gestione di tutti gli altri. In questo lavoro bisogna considerare anche la shadow IT, ovvero l'insieme di servizi che operano su dati e processi ma che sono scelti dai singoli, fuori dal controllo aziendale.

#### 5 Regulatory compliance

Probabilmente questo è il punto più importante. Esiste un numero di normative molto elevate, sia tecniche sia giuridiche. La maggior parte dei casi reali non è tabellata in modo univoco, per cui in caso di problemi s'incorre in una serie di conseguenze quali blocchi, sanzioni o cause. In genere un cloud provider ha una casistica molto ampia e può



proporre iter di mitigazione più affidabili di quella della singola azienda.

#### 5 MOTIVI PER SALVARE LE APPLICAZIONI CRITICHE NEL CLOUD

Vediamo ora cinque casi nei quali il cloud in genere conviene. La sicurezza innanzitutto, che sulla nuvola trova le competenze più recenti per completare il ciclo di controlli. Poi ovviamente il controllo dei costi, Ma anche il telelavoro, che può portare anche al metaverso.

#### 1 Metaverso

Non è ancora un'applicazione critica e forse mai lo diventerà, ma gran parte dell'ICT che verrà ne sarà influenzata per i prossimi anni. E' chiaro che molti software vendor propongono universi virtuali nei quali la collaborazione è più facile e il datacenter deve adeguarsi. Non si tratta, insomma, di un semplice adattamento 3D del telelavoro, che pure è un sentito motivo di adesione al cloud. Bisogna poi considerare che il metaverso non è abitato solo da esseri umani: ci sono anche auto connesse, smart cities e fabbriche, tutto ciò per cui è previsto un digital twin, una copia digitale che possa vivere anche di vita propria.

## 2 Sicurezza

Potenza e varietà degli attacchi rende praticamente impossibile difendersi da soli su base continuativa. Inoltre la collaborazione a distanza, che sia in azienda o a scuola. Il panorama è complesso e richiede svariate soluzioni che vanno usate con attenzione. Sempre più si parla di SOAR (acronimo di Security Orchestration, Automation, and Response) per gestione delle minacce e delle vulnerabilità, risposta agli incidenti e automazione delle operazioni. Per affrontare correttamente la situazione in genere non basta un gruppo di esperti, ma si deve ricorrere ad un'ampia comunità che condivida capacità ed esperienze. L'analisi storica non può essere trascurata, ma servono anche azioni proattive, in tempo reale e preventive.

## 3 Lavoro a distanza

L'importanza di accedere alle applicazioni dell'ufficio da qualsiasi parte del mondo, purché connessi, è l'elemento che ha cambiato l'approccio al lavoro. Le attività già pronte a questa soluzione, sia nei processi, sia nei servizi, compreso lo scambio di conoscenze tra dipendenti (si pensi a Slack o Discord), si sono mostrate adatte a qualsiasi scossone sia giunto finora, dalla digitalizzazione al Covid ed oltre. Il telelavoro richiede un cambio di paradigma per perimetro di sicurezza, risorse richieste e processi aziendali e non tutte le realtà possono implementarlo in tempi utili per restare competitive.

## 4 Controllo della spesa

L'estrema variabilità dei costi, soprattutto con più vendor ciascuno con le sue politiche di vendita, è un problema che il cloud si è sempre proposto di risolvere. Non bisogna confondere il controllo della spesa con la spesa in sé. In linea teorica, infatti, l'on-premises è molto più economico del cloud già sul medio termine. Richiede però una gestione molto complessa nella quale è facile sbagliare le previsioni e uscire dal budget previsto, a parità di prestazioni ottenute. Il cloud permette di iniziare con una piccola spesa, scalare facilmente in caso di successo e poi tenere le spese sotto controllo.

## 5 Regulatory compliance

Questo punto è citato anche tra i motivi per non usare (solo) il cloud. Non c'è contraddizione: la semplificazione dei modelli sulla nuvola non è garanzia assoluta, per cui la corretta risposta alle esigenze normative dev'essere valutata in modo estremamente corretta in qualsiasi caso.

## CONCLUSIONI

Il cloud si sta adattando ad un numero crescente di situazioni, ampliando l'area comoda nella quale l'azienda cede il controllo in cambio di un esborso controllabile.

La mappa di ciò che conviene farsi in casa o comprare in cloud è molto dinamica: solo chi conosce bene la propria attività può ottenere il massimo. ❖

# 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](mailto:cem@gaiaconsulting.it)

☎ 02 24416972

**GAIA**  
Consulting & Technologies

[www.gaiaconsulting.it](http://www.gaiaconsulting.it)

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

# Un "ponte" per la formazione

Attraverso la soluzione Bridge, Applied rende disponibile una soluzione Web per realizzare sistemi di formazione adatti a realtà complesse e distribuite, mettendo a fattor comune in modo affidabile ed efficace una pluralità di soluzioni tecnologiche differenti

di **Riccardo Florio**



Caterina Castellani, head della business unit dedicata alle Digital Education Solutions di Applied

*"È importante trasmettere alle aziende il senso di urgenza per la digitalizzazione e l'innovazione; soprattutto alle PMI, che sono molto indietro nel livello di comprensione di quanto sia importante occuparsi di competenze digitale".*

È questo il primo concetto che vuole sottolineare **Caterina Castellani, "head" della business unit dedicata alle Digital Education Solutions di Applied**, azienda con sede in provincia di Bologna che supporta le imprese nel percorso di digital transformation con prodotti e servizi tecnologicamente avanzati.

Elemento caratteristico di Applied è di essere un partner tecnologico che non si limita a intervenire sugli aspetti abilitanti per la digitalizzazione dei processi aziendali dal punto di vista infrastrutturale, tecnologico e gestionale, ma che risponde in senso più esteso alle esigenze aziendali con un'offerta di soluzioni e servizi legati alla formazione delle risorse umane, al marketing, alla comunicazione, all'advertising, al post vendita e così via.

*"Applied ha creato al suo interno una business unit dedicata allo sviluppo di soluzioni digitali per il mondo education e per la funzione delle risorse umane - spiega la Castellani - che si occupa di aiutare le aziende a fare formazione digitale attraverso un catalogo formativo creato appositamente e impostato sui dettami dell'industria 4.0. Questo catalogo formativo è disponibile in modalità asincrona e permette alle aziende di diffondere cultura digitale al proprio interno in modo personalizzato."*



## Applied Bridge

Il tassello più recente dell'offerta Applied in ambito di formazione si chiama Bridge ed è una applicazione Web pensata per i responsabili delle risorse umane che può essere ospitata in cloud su directory, AWS, stoccata in docker.

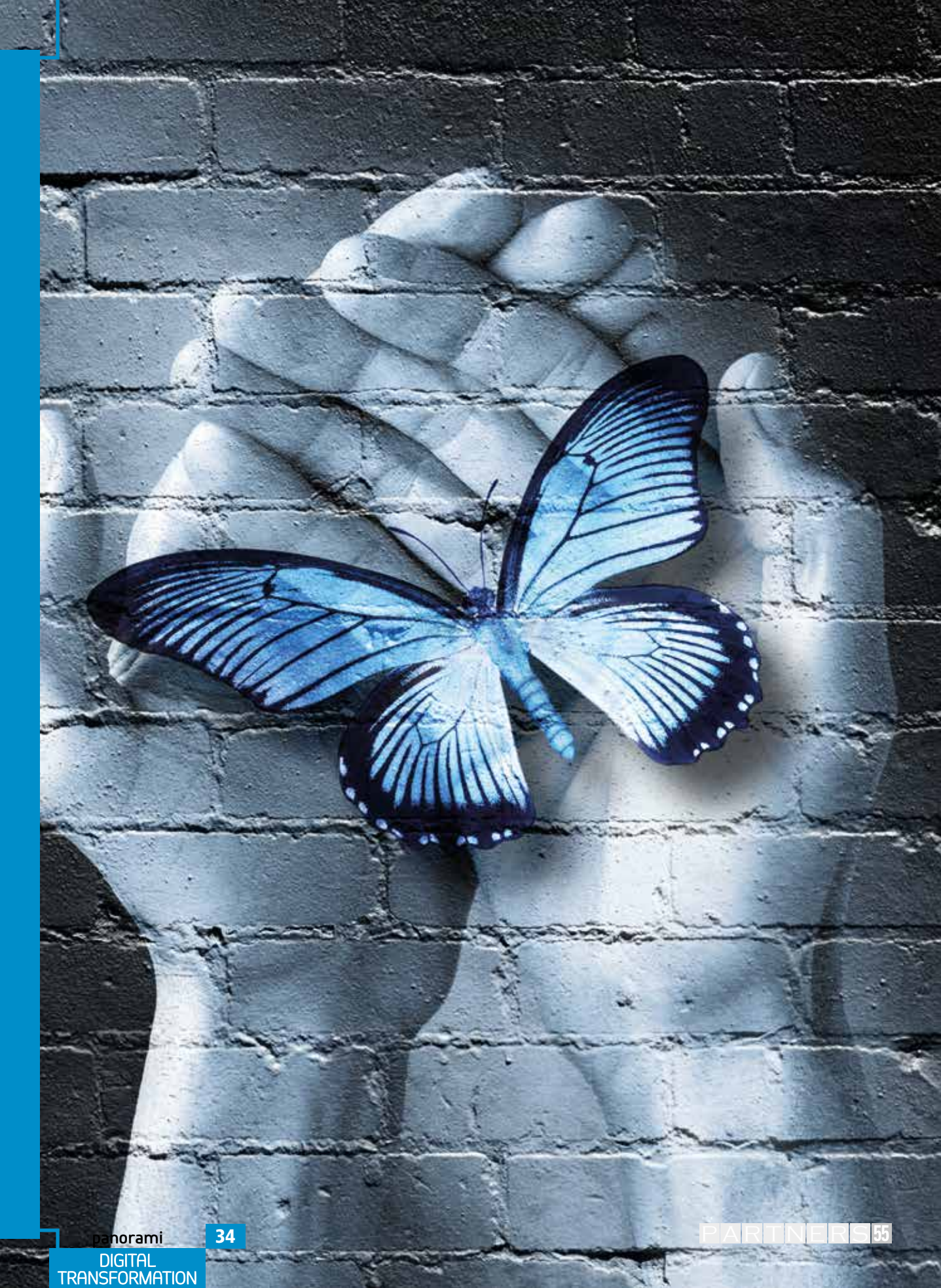
Bridge si indirizza naturalmente alla divisione delle risorse che è tipicamente responsabile delle attività di e-learning e può trovare applicazione in molti dipartimenti come, per esempio, l'ambito legale, la compliance, l'ICT, la sicurezza e così via."

Questa applicazione risponde all'esigenza di realizzare un sistema di formazione in cui gestire in modo efficace e personalizzabile molti utenti distribuiti grazie alla capacità di integrare i TMS (Talent Management System) aziendali che gestiscono anagrafiche e dati sui progressi nella formazione, con Skillgate. Skillgate è la piattaforma LMS (Learning Management System) di Applied basata su Ilias, diffusa soluzione di apprendimento completamente open source, multilingua e adatta a ogni tipologia di dispositivo, che si caratterizza anche per le funzionalità di sicurezza e per la recente introduzione di un

ampio marketplace dove trovare cataloghi online di corsi a scaffale!

Applied Bridge permette di gestire facilmente aspetti essenziali quali. Per esempio, la sincronizzazione automatica tra l'anagrafica degli utenti e la partecipazione ai corsi o di tenere conto del progresso nel processo di apprendimento. Il tutto con un approccio personalizzabile e organizzato in base alla definizione di ruoli, obiettivi formativi differenziati ed esigenze di sicurezza.

*"La tecnologia è ciò che abilita ma l'aspetto determinante per un progetto di successo è l'implementazione e uno degli scogli più difficili da superare e l'integrazione - precisa Castellani -. Applied Bridge è già stato utilizzato con successo in una realtà multinazionale come IMA Group dove siamo riusciti a predisporre un progetto di e-learning su scala enterprise con molti uffici distaccati e migliaia di postazioni. Tramite Bridge è stato possibile coniugare fusi orari diversi, così come TMS e database differenti fornendo una gestione unificata che garantisca anche la separazione dei compiti e la gestione dei ruoli su scala globale, dal Nord America all'Europa." ❖*



# La strada verso la digital transformation

La trasformazione digitale è un passaggio obbligato per un'azienda che oggi vuole essere competitiva e anche resiliente, come è stato mostrato durante la pandemia. Si tratta però di un processo che va ben oltre il dotarsi della più recente tecnologia e in cui i partner hanno un ruolo fondamentale

*di Fabrizio Pincelli*

Il digitale è stato di grande aiuto per riuscire a superare molte delle difficoltà economiche, produttive e sanitarie sorte nel periodo della pandemia. Anche quando i famigerati DPCM impedivano di recarsi in azienda, ha permesso comunque di continuare le attività.

Il digitale ha fornito quella capacità di far fronte a un evento disastroso e inatteso che è stata riassunta in un termine ormai comune a tutti: resilienza.

Tuttavia, il digitale può essere molto di più che un semplice sinonimo di resilienza. Una vera digital transformation può portare un cambiamento organizzativo capace di scardinare dalle fondamenta i processi aziendali per riproporli in una forma più efficiente con tutti i benefici

che ne conseguono in termini di attività e, più in generale, di business. In sostanza, è un modo molto efficace per affrontare le sfide indotte dai mutamenti sociali, economici e globali, riuscendo a mantenere un elevato livello di competitività.

### La strategia oltre alla tecnologia

Quando si parla di trasformazione digitale va però sottolineato un aspetto importante: la tecnologia riveste un ruolo fondamentale, ma non si deve considerare la digital transformation come una mera faccenda tecnologica. È invece una questione che considera la strategia aziendale nella sua globalità.

Affinché ci sia una reale trasformazione digitale le imprese devono adottare modelli di business che mettano i dati alla base di ogni strategia. Per ottenere i migliori risultati dal digitale si dovrebbe infatti avere un'ampia condivisione delle informazioni e delle strategie in tutta l'organizzazione. In questo modo si possono ottimizzare i processi e le attività per avere un miglioramento del business.

I dati non devono più essere un patrimonio dei singoli dipartimenti,

### Ottimizzare i processi del manufacturing

Effettuare una digital transformation nel settore manifatturiero significa avvalersi della tecnologia per massimizzare i ricavi, ridurre i costi, migliorare la qualità e aumentare la flessibilità. Il digitale può trasformare, ottimizzandoli, molti processi dall'amministrazione alla produzione fino alla supply chain. Può permeare tutta la catena del valore rendendo l'azienda più competitiva attraverso l'incremento della produttività e dei tempi di attività degli asset.

IDC prevede che nel 2025 la spesa globale per la trasformazione digitale delle aziende del settore manifatturiero ammonterà a oltre 816 miliardi di dollari. Dal canto suo, Forrester Consulting ha rilevato che oltre il 90% dei leader del settore manifatturiero ritiene che la digital transformation sia un fattore basilare per il loro successo.

Automazione dei processi e manutenzione predittiva sono sicuramente le parole d'ordine per la digital transformation nel manufacturing. Alla base ci sono l'IoT, l'intelligenza artificiale e il cloud.

## La sanità decentralizza l'infrastruttura IT

La digital transformation nella sanità è già iniziata da tempo. Lo provano per esempio pratiche consolidate come la diagnostica per immagini o il Fascicolo Sanitario Elettronico (FSE), oggi forse la massima espressione della digitalizzazione nella sanità. Tuttavia, la pandemia ha mostrato come ci sia ancora molto da fare per poter parlare veramente di digital transformation. Le ricette elettroniche e i consulti a distanza sono un chiaro esempio in questo senso. E il FSE ha mostrato i suoi limiti: è una ricca raccolta di dati eterogenei, ma è diverso da regione a regione. E lo stesso si può dire per altri processi inerenti al Sistema Sanitario Nazionale.

Risulta quindi evidente come la gestione dei dati e la loro condivisione sia ancora da affinare e come la digital transformation possa essere utile. E questo non solo per il FSE ma anche per creare un'efficiente cartella clinica elettronica e, più in generale, per riservare alle persone un efficace patient journey, ovvero navigare facilmente nel sistema sanitario, potendo gestire le interazioni di routine, come fissare un appuntamento, pagare un ticket, trovare un medico, avere risposte concrete a domande sulla salute.

Come previsto dal PNRR, che dedica 19,7 miliardi di euro all'innovazione nella "salute", deve inoltre essere effettuata una maggiore decentralizzazione della sanità. Questo significa dover attuare una vera assistenza a distanza (connected care) e creare centri periferici attrezzati. C'è bisogno di infrastrutture IT che portino sull'edge una potenza adeguata a gestire le necessità della sanità. Ma anche di sistemi volti ad assicurare la continuità dei processi e delle attività.

ma devono diventare un bene comune. Devono poi essere di qualità, ovvero corretti, coerenti e non duplicati. Chiaramente i dati comprendono informazioni di ogni tipo, dalle anagrafiche ai dati che si possono ottenere dai dispositivi IoT usati per automatizzare i processi di produzione, dalla digitalizzazione di documenti alle campagne di loyalty del retail. Gartner sostiene che "ogni anno, una scarsa data quality costi alle organizzazioni in media 12,9 milioni di dollari. Le aziende devono intraprendere azioni pragmatiche e mirate per migliorare la

qualità dei dati se vogliono accelerare la trasformazione digitale". Le aziende hanno quindi bisogno di soluzioni che consentano efficaci processi di data management e data governance. In questo diventa fondamentale il ruolo del partner che può supportare le imprese nel processo di cambiamento, la prima fase verso la completa trasformazione digitale.

### In cloud oppure on premise?

Una volta che si dispone di dati di qualità, bisogna poterli elaborare e analizzare per estrarre il valore, anche

## Finance, un digitale da aggiornare

Parlare di digital transformation nella finanza sembra quasi fuori luogo, dato che il digitale è alla base della finanza odierna. Tuttavia, il mondo della finanza è legato a schemi tradizionali e molto spesso i sistemi usati sono datati e poco funzionali. I dati sono fondamentali, ma la loro gestione è sovente a silos e la condivisione, che dovrebbe essere basilare, non è sempre agevole. Inoltre, il cloud viene approcciato in maniera molto prudente perché si deve avere la sicurezza che se delle informazioni escono dai confini aziendali devono essere più che mai al sicuro. Per questo motivo, assieme al mondo bancario, quello della finanza è stato tra gli ultimi ad avvalersi delle opportunità offerte dal cloud.

Da ciò risulta evidente come ci possano essere diverse opportunità per aiutare le aziende del finance a rendere più veloci i processi, migliorare i risultati e anche risparmiare sui costi. Tendo però sempre presente che la compliance con le normative, primo fra tutti il GDPR, è un aspetto fondamentale.

economico, che essi sono in grado di generare. È necessario quindi avere un'infrastruttura IT che consenta di lavorare in modo efficace con tali dati. La scelta può essere di avere tale infrastruttura on premise oppure di sfruttare le opportunità offerte dal cloud. Eventualmente, si possono scegliere anche entrambe le opzioni puntando sul cloud ibrido. Sta nel system integrator, che sempre più spesso può operare anche come cloud service provider, proporre la soluzione

più indicata alle singole necessità. Il cloud consente sicuramente più opzioni all'azienda, come avere le risorse necessarie on demand, pagare solo per quelle che usa e trasformare i costi da CapEx in OpEx. Non solo. Nel momento in cui sia necessario il ricorso all'intelligenza artificiale o al machine learning, il cloud è la scelta di elezione.

Per contro, per un'azienda può essere mandatorio mantenere on premise una serie di dati o applicazioni (come può accadere per una banca o una finanziaria) e quindi la scelta del cloud puro è preclusa a priori. È però possibile avere on premise gli

stessi vantaggi del cloud "affittando" un'infrastruttura IT su cui far girare le proprie applicazioni. Tale infrastruttura è sovradimensionata rispetto alle attuali esigenze, ma comunque commisurata all'eventuale necessità di incrementare la potenza di calcolo: ovviamente si pagano solo le risorse realmente usate.

Un'opportunità chiamata cybersecurity. Se da una parte la digital transformation porta una serie di benefici, dall'altra fa sorgere un problema importante:

la cybersecurity. Infatti, più articolata è l'infrastruttura IT e maggiori sono le opportunità che si offrono ai cyber criminali di sferrare un attacco. Per non parlare poi del fatto che il cloud e lo smart working estendono la rete aziendale fino ai più remoti dispositivi, i quali, quindi, dovrebbero essere adeguatamente protetti. Un discorso analogo vale per i device IoT in grado di collegarsi a Internet: rappresentano degli endpoint che possono essere facilmente attaccati.

Nasce perciò la necessità di una protezione che permetta di evitare di essere facili vittime di ransomware o di altri tipi di minacce. Se si escludono le realtà di grandi dimensioni, le aziende sono solitamente focalizzate sul core

business e non hanno una struttura interna adeguata a occuparsi dell'aspetto cybersecurity, quantomeno non in maniera sufficientemente efficace. Questo rappresenta un'opportunità per fornire un servizio di sicurezza IT in outsourcing. Molti system integrator hanno esteso il loro raggio d'azione diventando MSSP (managed security service provider). Ovviamente non ci si può improvvisare in questo ruolo perché sono necessari competenze e personale preparato. Tuttavia, chi già opera nell'ambito della sicurezza può ampliare la proposta. I vendor di soluzioni di sicurezza ormai hanno tutti a listino un'offerta per MSSP, che solitamente accompagnano anche con una formazione ad hoc. ❖

### Il cloud alla base della digital transformation della Pa

All'interno dell'ultimo Forum Pa, è emerso che negli anni la Pubblica amministrazione ha raccolto un numero enorme di dati, ma che ogni dipartimento o sede locale ha tendenzialmente sempre gestito in maniera autonoma. E spesso tali dati sono stati archiviati senza una particolare attenzione alle modalità di conservazione.

La digital transformation dovrebbe quindi partire con progetti volti a cercare di razionalizzare i dati, condividendoli tra le Pa locali al fine di farne un uso più efficiente. È un'operazione che può aiutare anche a snellire i carichi di lavoro che cominciano a diventare insostenibili per diverse infrastrutture IT della Pa. In linea anche con quanto stabilito all'interno del PNRR, la digital transformation della Pa dovrebbe prevedere anzitutto una migrazione verso il cloud, un passaggio che può fornire un sostanziale contributo per l'efficientamento delle parti infrastrutturali.

# Infrastrutture per la digital transformation

L'accelerazione nel processo di digital transformation richiede un consolidamento e un'evoluzione delle infrastrutture digitali del nostro Paese

a cura di **Redazione**

**P**arlando di trasformazione digitale è certamente importante concentrarsi su applicazioni, processi, workflow e modelli di business, ma tutto viene vanificato se le infrastrutture digitali a disposizione restano inadeguate.

## La richiesta di banda larga

Con il Piano Italia a 1 Giga il Governo italiano mira a portare, **entro il 2026, connettività ad almeno 1 Gbps in download** e 200 Mbit/s in upload alle unità non coperte da almeno una rete in grado di fornire in maniera affidabile velocità di connessione in download pari o superiori a 300 Mbps.

Tale livello di prestazioni è quello ritenuto necessaria **per supportare le reti di nuova generazione in grado di soddisfare le richieste di connettività dei nuovi servizi digitali** quali: video streaming a 4K/8K, realtà virtuale e aumentata, collaborazione

immersiva, smart working e formazione a distanza, cloud computing, online gaming, domotica avanzata, telemedicina e altri ancora. Altrettanto importante è la **connettività mobile**. I numeri forniti da Infratel, società in-house del Ministero dello Sviluppo Economico, indicano che nel 2021 la copertura del territorio italiano con reti mobili con velocità di picco in download inferiore a 30Mbit/s era ancora molto elevata (24,44%) con il 2,44% del territorio non coperto.

Gli obiettivi per il 2026 sono di portare questo dato a 13,25% con il 2,01% non coperto: certamente un miglioramento, ma che significa estromettere ancora per i prossimi 4 anni una bella fetta del nostro Paese.

Resta poi da osservare che tutti i piani e le previsioni attuali sono suscettibili di revisione (ovvero ritardi) con l'arrivo delle elezioni e un futuro prossimo che, oggettivamente, appare poco interpretabile.

## Le principali sfide del cloud computing

Assumendo che la banda sia disponibile, l'infrastruttura cloud svolge un ruolo essenziale sia per gli utenti finali che vogliono fruire dei servizi digitali, sia per le imprese che possono investire nello sviluppo di questi servizi. Anche e, forse, soprattutto, per le piccole e medie imprese del nostro Paese che possono approfittare della natura "democratica" del cloud, che ha livellato la differenza tra chi poteva permettersi di predisporre e gestire complesse infrastrutture tecnologiche e chi no.

Tra le sfide che il cloud si trova costantemente ad affrontare vi è quella della **sicurezza, un tema che negli anni si mantiene centrale** e che sta ridefinendo i propri contorni con l'affermazione di modelli ibridi e multicloud. Le questioni da affrontare sono sempre le stesse e riguardano sia temi tecnologici (legati ad aspetti quali il controllo dei dati, la compliance normativa, la gestione del ciclo di vita delle informazioni) sia l'interazione con il fornitore di servizi e le garanzie contrattuali.

Un altro tema importante per sbloccare le potenzialità della trasformazione digitale è quello della standardizzazione e dell'interoperabilità dei servizi cloud: anche in questo senso si stanno facendo passi in avanti ma il processo è ben lungi dall'essere concluso. A livello di Pubblica Amministrazione va poi affrontato anche il tema dell'autonomia tecnologica, considerando che le quote di mer-



cato delle infrastrutture cloud delle aziende europee rappresentano meno del 10% totale. Di conseguenza, l'adozione massiva di tecnologia cloud per l'erogazione dei servizi della PA potrebbe trovarsi soggetta a modifiche unilaterali delle condizioni di servizio fornite da parte di organizzazioni sovranazionali, con possibili variazioni significative degli stessi (dall'aumento dei costi all'interruzione del servizio) in ragione di intenti potenzialmente non controllabili dal Paese (il gas russo insegna).

Vale la pena, infine, sottolineare come molti modelli di trasformazione digitale e di Servitization puntino sull'affermazione delle tecnologie IoT ovvero, in una concezione più ampia, dei modelli infrastrutturali di Edge computing. In questo caso la diffusione sta procedendo più lentamente di quanto si prevedeva solo due o tre anni fa e, tra le sfide attuali, vanno ricordate sia quelle di tipo economico legate ai costi delle materie prime e alla scarsità di chip sia, ancora una volta, la standardizzazione. ❖

# Avaya OneCloud: una piattaforma per l'esperienza totale

Avaya propone una piattaforma componibile e basata su intelligenza artificiale che realizza un'interconnessione multiesperienza tra cliente, dipendente e utente

di **Riccardo Florio**

**P**er risultare vincente sul mercato è sempre più importante riuscire a differenziarsi nel modello di customer experience fornito sfruttando tutte le opportunità offerte dalle nuove tecnologie nelle strategie di marketing. La ricetta di Avaya passa per il cloud e un modello di esperienza totale.



Alessandro Catalano, Country Manager Avaya

*"L'adozione delle giuste tecnologie - osserva Silvana Suriano, Sales Engineer Manager Italy Cluster di Avaya - può consentire di prendere decisioni più informate basate sui big data, di prevedere i risultati di strategie e tattiche, di portare l'esperienza digitale contestuale nel mondo fisico. Tuttavia, le esperienze non possono essere integrate e devono, invece, essere composte. Questo significa predisporre un'esperienza che si possa distribuire senza soluzione di continuità e senza sforzo tra le App, i punti di contatto, le modalità e le persone. In altre parole, l'esperienza totale richiede un approccio di piattaforma, perché non è possibile affrontarla con un App."*

## **Il modello Avaya di esperienza totale**

Per realizzare questo modello di esperienza totale Avaya propone la piattaforma componibile e basata su intelligenza artificiale Avaya OneCloud che realizza un'interconnessione tra cliente, dipendente, utente e multiesperienza. "Avaya è presente all'interno delle infrastrutture di tutte le grandi realtà, enterprise - sottolinea **Alessandro**

Catalano, country manager di Avaya - dalle telco, alle banche, alla PA centrale. Ciò che ci differenzia maggiormente sul mercato è la percezione che i nostri clienti hanno dell'estrema affidabilità delle nostre soluzioni a cui si abbina una grandissima attenzione al cliente".

Avaya OneCloud è costruita attorno a un "core" tecnologico unificato (Avaya Media Processing Core) su cui si innestano quattro componenti strutturali erogate in forma di servizio capaci di operare congiuntamente.

La prima di queste è **Avaya OneCloud UCaaS (Unified Communications as a Service)**, che risponde alle esigenze dei nuovi modelli di lavoro remoto in costante mutamento. Integrabile con oltre 200 App, questa soluzione mette a disposizione un'unica interfaccia utente per riunire ogni esigenza di comunicazione. È possibile gestire riunioni e videoconferenze con possibilità di assegnare attività e tenerne traccia, condividere documenti e sviluppare il lavoro di team anche dopo la riunione grazie a un flusso coerente di messaggi. Altre funzionalità includono la messaggistica e i sistemi di telefonia cloud, con la possibilità di scalare facilmente nel numero di utenti a livello globale e con tutte le funzioni vocali disponibili sui telefoni tradizionali e IP. Il tutto da un'interfaccia amministrativa semplificata e con aggiornamenti di sicurezza a cadenza regolare

**Avaya OneCloud CCaaS (Contact Center as a Service)** è la componente di servizio clienti basata sul cloud che gestisce e monitora i percorsi dei clienti, le interazioni dei dipendenti con i clienti e qualsiasi altra comunicazione in entrata o in uscita attraverso canali vocali e digitali, come e-mail, chat web e messaggi di testo. La soluzione Avaya è gestita e accessibile tramite il cloud e non richiede



alcuna infrastruttura autonoma. Tramite un'interfaccia utente semplificata e da un unico browser è possibile accedere a team, risorse e informazioni del Contact Center: chiamate, messaggistica, video, riunioni, condivisione di file, gestione delle attività e altro ancora.

**Avaya OneCloud CPaaS (Communications Platform as a Service)** è la componente che automatizza e personalizza i processi aziendali integrando facilmente funzionalità di Intelligenza Artificiale e automazione sui dati, senza richiedere modifiche all'infrastruttura esistente. Per farlo sfrutta messaggi di testo, video, chiamate, e-mail, chatbot e live chat fornendo esperienze personalizzate e in tempo reale.

L'ultimo tassello è **Avaya OneCloud WSC**, la componente di Workstream Collaboration in cui si inserisce la diffusa soluzione Avaya Spaces: l'app per la collaborazione che mette in contatto le persone e gli strumenti, all'interno di un unico spazio, per incontrare, chiamare, chattare, condividere file, gestire attività. Tutto in notifiche in tempo reale. ❖

# DIMENSIONE O VELOCITÀ: IL DILEMMA DELL'INNOVAZIONE

Arriva un momento, nel ciclo di vita di un'azienda, in cui l'incremento di dimensione può inibire il ritmo dell'innovazione. Alcuni spunti e suggerimenti per affrontare il cambiamento senza limitare il processo di crescita

di *Primo Bonacina*

**S**e confrontate un coffee shop Starbucks di New York del 2012 con quello aperto recentemente a Milano in piazza Cordusio, non noterete colossali differenze (magari alcuni dettagli nell'allestimento, ma non granché nella sostanza). Ma se li confrontate con i negozi originali aperti a Seattle nel 1971, la differenza è sorprendente.

Lo stesso discorso vale per McDonald's. Passiamo a Apple: quando, nel 1984, il Mac è stato lanciato c'erano solo una dozzina di persone dedite allo sviluppo, eppure furono in grado di lanciare un prodotto che cambiò le regole del gioco.

Oggi Apple ha più di mille volte gli ingegneri di allora ma è chiaro che è facile lanciare con costanza nuovi prodotti altrettanto rivoluzionari. Lo stesso discorso vale per Google (almeno a prima vista, il motore di ricerca sembra sempre uguale, anche se sotto sotto, continua a cambiare) e altre grandi aziende.

Questo stato di cose non riguarda solo i top brand. Praticamente ogni organizzazione, prima o poi, raggiunge un punto in cui il ritmo dell'innovazione rallenta in parallelo alla crescita delle dimensioni e della storicità.



## Questo per diverse ragioni:

Il cosiddetto debito tecnico (o architetturale), ovvero il risultato di scorciatoie prese per far funzionare le cose in un certo momento. Ne consegue che il sistema non è più così espandibile in quanto buona parte dell'architettura obbedisce a parametri definiti

**1.** La complessità intrinseca nelle grandi organizzazioni. Pensiamo alla regola delle strette di mano. Se siamo in due ci stringiamo la mano (1 stretta, 2 persone, rapporto 0,5). Se siamo in 3, stringo la mano a te e poi all'altro e quindi voi vi stringete la mano (3 strette, 3 persone, rapporto 1). Proseguendo, si scopre che l'ammontare delle strette di mano necessarie è basato sul numero "n" di persone:  $n*(n-1)/2$ . Nove persone hanno bisogno di 36 ( $9*8/2$ ) strette con un rapporto strette/persone di 4, quindi 8 volte maggiore di quello

2 persone. In altre parole, un'organizzazione più complessa implica più incontri, approvazioni, coordinamento, tempo consumato ad abilitare e spiegare (e non a fare)

**2.** I clienti sono certamente il principale asset aziendale, ma anche un potenziale freno all'innovazione. Loro non hanno necessariamente piacere che l'azienda cambi continuamente lo stato delle cose. Diciamo la verità: quanti di voi si entusiasmano all'idea di passare a una nuova versione di un sistema operativo o di un'applicazione ?

**3.** Il canale dei partner, similmente ai clienti finali, ha propri obiettivi e un proprio ritmo per raggiungerli, e spesso questi partner non hanno tutta questa fretta di studiare, pensare, riprogettare, introdurre cambiamenti per loro e per i loro clienti

**4.** Le istituzioni finanziarie (banche, borsa, investitori) spesso cercano di evitare l'ignoto ("Il prodotto vende, non bruciamolo")

**5.** Il freno manageriale che si palesa quando la gestione operativa sostituisce la leadership capace di osare. Le persone vengono promosse perché sanno fare un certo lavoro: quello che stanno facendo in quel momento. E l'innovazione non è sempre un'opportunità. Al contrario, spesso è una minaccia allo status quo.

## ALCUNI SUGGERIMENTI PER GUIDARE IL CAMBIAMENTO

I punti indicati precedentemente sono reali (a volte più, a volte meno: dipende da situazioni, momenti e mercati). Ignorarli non è il modo migliore per far funzionare le cose. Così come non lo è imporre ai propri collaboratori di stravolgere il proprio approccio naturale. Servono opzioni ragionate per guidare il cambiamento.



## Di seguito tre possibili proposte alternative:

- **La continuità (crescita incrementale).**

Questo è ciò che fanno parecchi marchi noti. Nel momento in cui si è raggiunto il successo, ci si accorge che la massa dei clienti non ha grande fame di innovazione. Loro vogliono che man-

tengiate le promesse, non vogliono sorprese, bastano efficienza e prezzi ragionevoli. Magari apporterete piccoli miglioramenti al prodotto o al servizio secondo scadenze regolari e darete prevedibilità alle offerte e ai prezzi. Tutto ciò vi permetterà di raggiungere più clienti con un impatto positivo immediato. Le piccole innovazioni sono, infatti, ciò che evita alle organizzazioni di restare troppo indietro rispetto a competitor fortemente innovativi, facendo sì che per lungo tempo, anche anni, il gap non sia così rilevante. A quel punto sarete forse diventati un "follower" come Yahoo, Chrysler o Nokia (ma poco male: magari vi farete comperare da Microsoft)

- **Il rifacimento strutturale selettivo.** Create un cosiddetto "Skunk works" (letteralmente: skunk = puzzola), la denominazione ufficiale della divisione di Lockheed Martin dedicata ai velivoli sperimentali, creatrice di progetti di grande rilievo quali l'aereo spia U-2, l'SR-71 Blackbird, il caccia stealth F-117 Nighthawk, il caccia di 5ª generazione F-22 Raptor e, attualmente, il F-35 Lightning II. Nelle nazioni anglofone, il termine "Skunk works" è utilizzato per descrivere un gruppo all'interno di un'organizzazione che gode di elevata autonomia con il compito di lavorare su progetti avanzati e senza doversi preoc-



cupare troppo della burocrazia. In poche parole, un progetto quasi isolato dal resto dell'organizzazione, un manipolo di marines per conquistare quella maledetta collina. Analogamente, immaginate di essere una software house e di dover rifare da zero il codice sorgente mentre il team principale mantiene l'esistente. Oppure

ancora, isolate la vostra cash cow, la parte aziendale che produce liquidità e risorse, e staccatela dal resto dell'organizzazione, creando un team che, come sopra, riparta su qualcosa di nuovo. Forse tutto ciò all'inizio non funzionerà, ma se agirete ripetutamente alla ricerca dell'innovazione guadagnerete un'esperienza e una capacità di cambiare che, alla fine, vi ripagheranno degli sforzi

- **Le acquisizioni selettive.** Se siete grandi, potete acquisire aziende più piccole, ma dando loro autonomia operativa e di innovazione, isolandole dalle burocrazie interne e facendo in modo che la loro carica innovativa contaminino i pachidermi aziendali. Magari potrete poi, selettivamente e progressivamente, inserire le loro soluzioni nella vostra offerta, combinando l'energia e velocità delle start-up con la capacità di scala delle grandi organizzazioni

In conclusione, ho dovuto affrontare spesso queste scelte nella mia carriera, e nessuna di esse è facile né ovvia. Ma è la scelta in sé che non può essere trascurata. L'innovazione non è facile da introdurre in azienda ma è linfa vitale e imprescindibile. ❖



# INNOVATION FUTURE

copyright © Reportec 2022



# CyberRes

A Micro Focus Line of Business



## PER NOI RENDERE RESILIENTE IL TUO BUSINESS È UN GIOCO DA BAMBINI

**CyberRes** ti mette a disposizione una gamma completa di soluzioni software e tecnologie innovative per garantire che il business non si fermi mai anche in caso di crisi, pandemie e minacce informatiche



### **PROTEGGI**

le identità digitali,  
le applicazioni e i dati



### **RILEVA**

rispondi e riprenditi  
dalle minacce avanzate



### **EVOLVI**

la tua condizione di sicurezza  
per adattarti al cambiamento

### **ArcSight**

La nuova architettura evoluta Layered Security Analytics per Cyber Resilient SOC e Compliance

### **Fortify**

La suite di sicurezza applicativa leader di mercato che abilita la Security by Design senza compromessi

### **NetIQ**

Abilita la Zero Trust Security end-to-end per identità, utenti, ruoli, accessi, autenticazione, privilegi, asset, file

### **Voltage**

Soluzioni integrate per analizzare, classificare, gestire e proteggere i dati ovunque essi siano, con cifratura FPE

### **Intersect**

Aumenta l'intelligenza umana con la potenza del Machine Learning non supervisionato

Scopri su [CyberRes.com](https://www.cyberres.com) come rendere resiliente la tua azienda