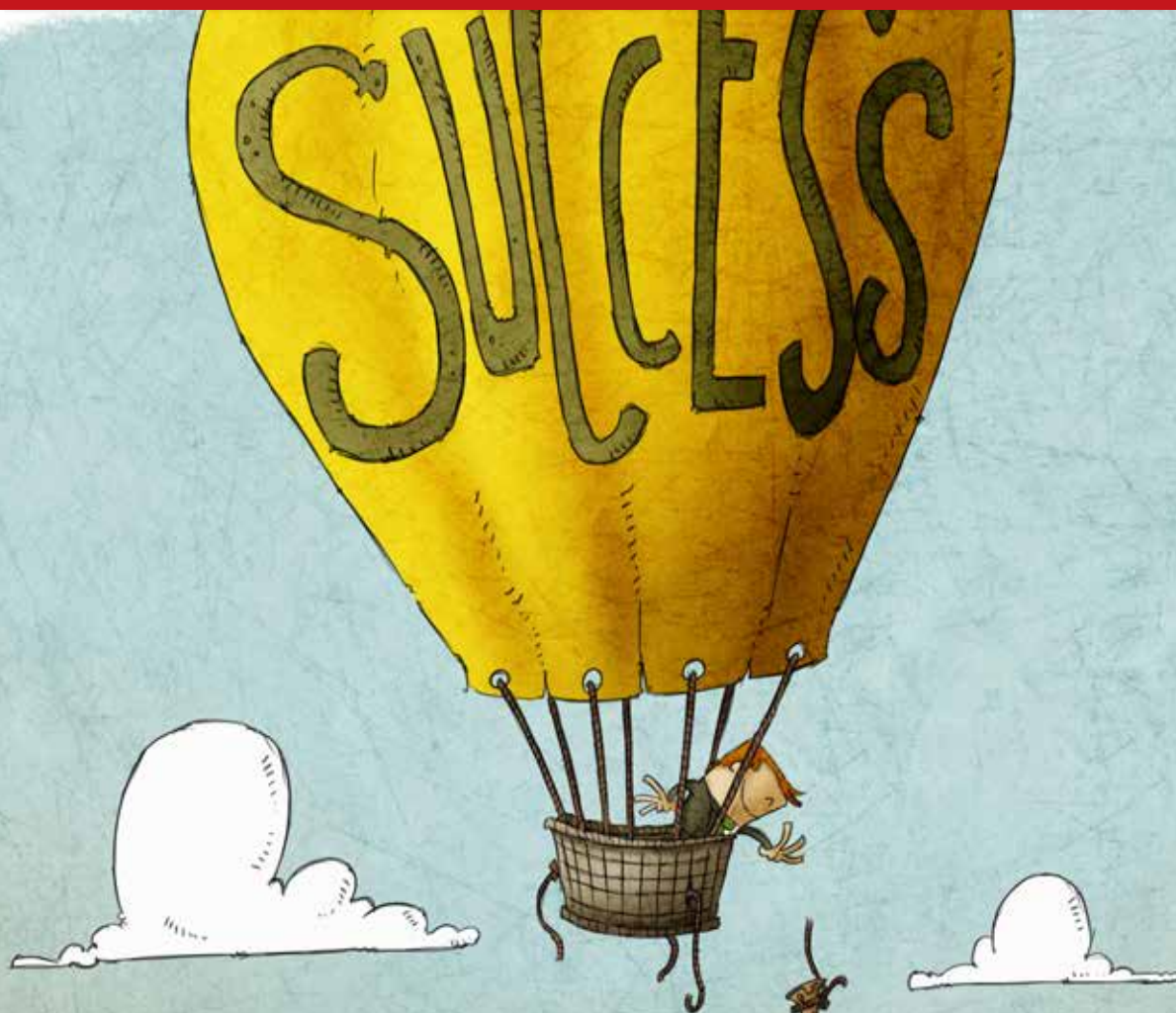


# PARTNERS

INFORMAZIONE E FORMAZIONE PER IL CANALE ICT A VALORE

N°53



## Canale e IT in trasformazione creano nuove opportunità di successo



**SPECIALE**  
Infrastrutture  
& soluzioni  
pag.45



**SPECIALE**  
**SECURITY**  
Proteggere l'azienda dagli  
attacchi informatici  
pag.20

**PANORAMI**  
Essere donna nel mondo  
della sicurezza digitale  
in Italia  
pag.16



# SICUREZZA SANITARIA E DISTANZIAMENTO SOCIALE: IL RUOLO DEL PRINTING.

Oggi le aziende devono "adattarsi" a nuove regole e rivedere le proprie strategie anche in ambito printing, per garantire il rispetto delle distanze di sicurezza, l'ottimizzazione dei costi e il rilancio della produttività.

## SOLUZIONI BROTHER:

**TECNOLOGIA CHE SI ADATTA AL CAMBIAMENTO PER RIPARTIRE IN AZIENDA!**



## BALANCED DEPLOYMENT e DECENTRALIZZAZIONE



**PRIMA**

**UNA STAMPANTE LASER A3 PER TANTI**



**DOPO**

**PIÙ STAMPANTI A4 COMPATTE**



## VANTAGGI

- RISPARMIO DI COSTI E TEMPI**  
ottimizzazione delle risorse
- SICUREZZA DI STAMPA CON SECURE PRINT+**  
a norma GDPR
- FLUSSI DI LAVORO EFFICIENTI**  
processi più snelli e veloci senza assembramenti
- ASSISTENZA DALLA STAMPANTE**  
monitoraggio da remoto dal dipartimento IT

## BENEFICI

<b>PRIMA</b>	<b>DOPO</b>
UNA SOLA STAMPANTE DI DIMENSIONI IMPONENTI	<b>PIÙ STAMPANTI, COMPATTE E PERFORMANTI</b>
FILE PER RITIRARE STAMPE	<b>MENO SPOSTAMENTI E ASSEMBRAMENTI</b>
SCRIVANIE AFFOLLATE	<b>PIÙ SPAZIO LIBERO E PIÙ DISTANZIAMENTO</b>

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

**brother**  
at your side

# CIAO GAETANO



Gaetano Di Blasio  
7 novembre 1964  
14 gennaio 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

## PARTNERS

Anno IX - numero 53

febbraio-marzo 2022

Direttore responsabile

Gaetano Di Blasio

In redazione

Riccardo Florio

Gaetano Di Blasio

Edmondo Espa

Hanno collaborato

Marco R. A. Bozzetti

Primo Bonacina

Andrea Bozzetti

Laura Rivella

Camillo Lucariello

Jacopo Bruni

Mercedes Oledieu

Grafica

Aimone Bolliger

Immagini

Dreamstime.com

Redazione

Via Gorizia 35/37

20099 Sesto San Giovanni (MI)

Tel. 0224304434

www.reportec.it

redazione@reportec.it

Stampa

A.G.Printing Srl

via Milano 3/5

20068 Peschiera Borromeo (MI)

Editore

Reportec Srl

C.so Italia 50

20122 Milano

Diffusione: 35.000 copie

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

Tutti i diritti sono riservati

Tutti i marchi sono registrati e di proprietà delle relative società

## PRIMO PIANO

CANALE E IT IN TRASFORMAZIONE

CREANO NUOVE OPPORTUNITÀ DI SUCCESSO 6

Nuovi partner per la next generation del Canale 7

L'IT post Covid si rafforza e si reinventa 11

## PRIMO DIGIT

Tempo di smart working: guida di sopravvivenza all'eccesso di riunioni

13

## PANORAMI

Essere donna nel mondo della sicurezza digitale in Italia

16

## SPECIALE

PROTEGGERE L'AZIENDA DAGLI ATTACCHI INFORMATICI 20

Indagine OAD 2021 sugli attacchi digitali in Italia 21

Dalla sicurezza alla resilienza:

come cambiano i paradigmi di protezione 26

Ransomware: il ricatto che rende 20 volte l'investimento 30

Praim dalla parte dei CISO 34

## TRANSFORM TO SUCCEED

Stampa gestita per aziende in smart working 36

Soluzioni di stampa che si adattano alla nuova normalità 38

Snom sempre più forte grazie allo smart working 42

## SPECIALE

SPECIALE INFRASTRUTTURE & SOLUZIONI 45

Dell Technologies trasforma il modo di utilizzare la tecnologia 46

Lenovo 360: il programma di Canale del futuro 48

CIE Telematica, soluzioni complete di telecomunicazioni e networking 52

Modelli standard per le infrastrutture Edge 54



# CANALE E IT IN TRASFORMAZIONE CREANO NUOVE OPPORTUNITÀ DI SUCCESSO

# NUOVI PARTNER PER LA NEXT GENERATION DEL CANALE

**In uno scenario di profondo cambiamento, accelerato dalla pandemia, i partner di Canale hanno a disposizione nuove opportunità per evolvere e crescere puntando ad avere un ruolo più incisivo nel favorire il business dei loro clienti**

di **Riccardo Florio**

**A**due anni dall'inizio della pandemia globale, con una nozione completamente nuova del termine digital transformation e un'accelerazione senza precedenti sul fronte cloud, il Canale si trova a un punto di svolta. La pandemia non solo ha alimentato la digitalizzazione e l'adozione di nuovi strumenti che guidano la trasformazione del business, ma ha anche portato a compimento una serie di trend che si protraevano da anni e che già stavano riformulando il modello del Canale, aumentandone l'importanza e aprendo la strada a significativi cambiamenti e opportunità.

Il primo di questi trend è stato il rapido passaggio verso il lavoro da remoto: un modello che tutti gli analisti concordano che non andrà più via.

Una seconda tendenza riguarda il cambiamento di ruolo che sia i VAR sia i Managed Service Provider (MSP) sono chiamati ad assumere per poter restare al passo con i tempi e con le rinnovate aspettative del mondo B2B.

Un ulteriore trend riguarda il mondo del cloud e il progressivo spostamento dei tre "grandi" - Microsoft Azure, Amazon Web Services (AWS) e Google Cloud - verso un rapporto più partecipato e collaborativo con i partner di Canale.

Nell'ultima edizione del suo report "The 2021 State of the Channel Report", Ingram Micro Cloud evidenzia quali sono le esigenze principali a cui dovranno far fronte i partner di Canale della next generation per rispondere a queste sfide.

La prima sarà di mettere a disposizione dei propri clienti strategie e tecnologie in grado di fornire a chi opera da casa il medesimo livello di prestazioni e di "user experience" che aveva in ufficio, senza pregiudicare la protezione nel ridefinito perimetro di sicurezza.

La seconda è di far evolvere il proprio ruolo per diventare un costruttore di esperienze

"channel first", un partner strategico specializzato e il promotore di un ecosistema più vasto e integrato di partner.

Infine, l'adesione a un più ampio ventaglio di programmi di certificazione che includa anche quelli offerti dai tre "big" del cloud.

### **La rivoluzione dello smart working**

Il numero di persone che lavoravano da remoto era in costante crescita anche prima della pandemia ma, l'improvviso requisito del distanziamento sociale, ha condensato in pochi mesi traguardi che altrimenti avrebbero richiesto anni. L'introduzione massiccia e pervasiva a livello globale dello smart working ha ridefinito il concetto di luogo di lavoro e le aziende si sono affrettate a connettere i loro team online, facendo crescere alle stelle la spesa per le tecnologie cloud.

Pertanto, la sostanziale valutazione positiva del cosiddetto telelavoro farà in modo che, in futuro, molte aziende decidano di adottare comunque un modello ibrido, in cui alcuni dipendenti lavorano in remoto e altri in locale oppure in cui tutti alternano lavoro da remoto e in ufficio.

Questi nuovi ambienti di lavoro remoti e ibridi genereranno, però, anche nuovi punti deboli per le aziende e richiederanno soluzioni innovative, integrate e sicure. È proprio in questo contesto che i partner di Canale troveranno nuovi spazi per duplicare l'esperienza dei lavoratori presso la sede centrale all'interno dei loro uffici domestici garantendo velocità e affidabilità della connessione ed espandendo il perimetro di sicurezza.

### **Le opportunità del cloud**

Per VAR e MSP potenziare l'esperienza di lavoro a distanza significa anche e soprattutto guidare in modo proattivo i loro clienti verso l'adozione di strategie multi-cloud e di cloud ibrido. Questo sviluppo è confermato dalle previsioni di Gartner che ha interpellato gli utenti finali per stimare il livello di crescita nel 2022 sui fronti IaaS, PaaS e SaaS (si veda immagine).

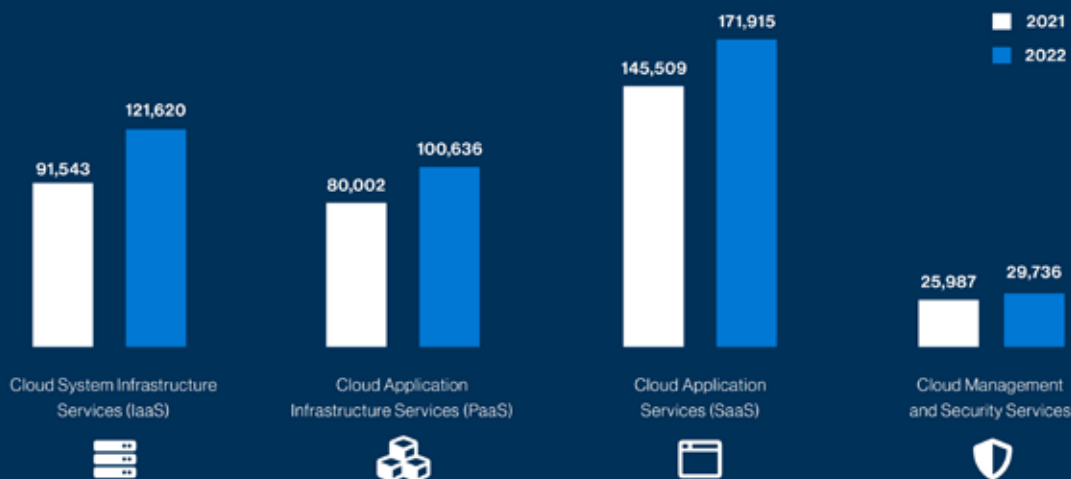
Per soddisfare questa crescente domanda, i partner dovranno sia espandere i loro ecosistemi con soluzioni basate su cloud sia investire nella formazione del proprio team in IaaS, SaaS e PaaS.

VAR e MSP dovranno, soprattutto, essere efficaci nel proporre soluzioni SaaS capaci di rispondere alle nuove esigenze di comunicazioni e collaborazione da remoto, puntando a incorporare all'interno di un'unica soluzione coesa le componenti per la messaggistica, la unified communication e la collaboration.

### **La doppia sfida della sicurezza e la crescita dell'Edge**

Il passaggio al cloud ibrido esalta anche i requisiti di sicurezza e compliance in un contesto già reso difficile dall'aumento esponenziale di attacchi e minacce.

## Previsione di spesa globale per i servizi cloud da parte degli utenti finali (in milioni di dollari)



Fonte Gartner (agosto 2021)

Peraltro, per i partner di Canale il tema è doppiamente complicato poiché devono concentrarsi sulla protezione sia dei propri clienti sia di sé stessi che sono sempre più spesso obiettivi dei cyber criminali.

Anche in questo caso il ruolo del partner è destinato a diventare più proattivo e rilevante estendendosi alla fornitura di SOC in forma di servizio. Sarà sempre più il partner di Canale a svolgere un ruolo di consulente sulla scelta e le modalità di adozione delle misure di sicurezza e di autenticazione avanzata, sulle tecnologie di rilevamento e risposta agli attacchi, sulla gestione dei rischi, l'intelligence sulle minacce e il backup e ripristino.

Anche il mercato dell'Edge computing è destinato a crescere. MarketWatch nel suo "Global Edge Computing Market Report 2021-2024", rilasciato a luglio 2021, stima per questo settore un tasso annuo di crescita composto (più comunemente noto come CAGR) del 34% tra il 2021 e il 2024.

Una delle principali difficoltà da superare in questo contesto sarà la necessità di avvicinare

le capacità di elaborazione dei dati e di delivery alla fonte di produzione e questo offre importanti opportunità ai partner che dovranno essere in grado di riconoscere e segnalare le situazioni in cui l'Edge computing possa contribuire a risolvere i problemi di rete dei propri clienti.

### L'evoluzione dei Managed Service Provider

Nel Canale in rapida evoluzione di oggi, gli MSP dovranno assumere un ruolo molto più attivo nel successo dei loro clienti. Non è più pensabile restringere la propria responsabilità alla rivendita di singoli prodotti e servizi o all'assistenza solo in base alle necessità, come è avvenuto negli ultimi due decenni.

Il moderno MSP si dovrà fare carico dell'integrazione coerente ed efficace di tutti i tasselli necessari, proponendosi come un partner strategico specializzato capace di tenere costantemente sott'occhio i punti deboli emergenti e pronto a indirizzare rapidamente i propri clienti verso le soluzioni più efficaci e

sicure. Ciò richiederà agli MSP di aggiornare i propri set di competenze aumentando anche il livello di esperienza sulla tecnologia e sui settori verticali.

Come parte di questo processo gli MSP assumeranno un ruolo sempre più centrale anche nel guidare i propri clienti verso modelli di fatturazione basati su abbonamento e consumo nel cloud e verso processi di automazione e semplificazione dei processi di fatturazione e di riconciliazione fatture.

Nella ricerca di modi per migliorare l'esperienza dei loro clienti, gli MSP moderni dovranno anche mirare a migliorare le competenze dei loro clienti e, come parte di questo sforzo, dovranno trasferirgli costantemente le più recenti "best practice" ricorrendo anche ad attività di formazione IT continue.

Ne consegue che gli MSP di maggior successo saranno, probabilmente, quelli che saranno in grado di attingere alla forza di un ecosistema ben connesso in cui convergeranno fornitori di software indipendenti (ISV), società di telecomunicazioni, distributori di tecnologia e altri MSP. È, infatti, solo dalla sinergia tra MSP, VAR e ISV che potrà nascere la capacità di affrontare in modo proattivo i diversi punti deboli di un cliente potendo disporre di tutti gli strumenti (tecnologici e non) necessari a superare le sfide del futuro.

### **I tre big del cloud e le opportunità per il Canale**

Negli ultimi anni Microsoft Azure, Amazon Web Services e Google Cloud hanno ampliato la gamma dei loro servizi cloud aumentando la loro presenza nel mondo del Canale. Per

un certo periodo di tempo gli analisti hanno previsto che la capacità di queste tre grandi aziende di portare prodotti cloud facilmente accessibili sul Canale potesse potenzialmente significare un'erosione dei prezzi per i partner, ma queste previsioni non sembrano attualmente confermate.

Invece di tentare di costruire una rete di vendita end-to-end aggressiva, i tre grandi fornitori di cloud stanno aumentando gli investimenti negli ecosistemi e nei programmi dei partner di Canale.

Microsoft sta già utilizzando in modo massiccio gli ecosistemi dei partner di Canale per vendere e distribuire le sue tecnologie ai clienti finali. AWS estende la propria presenza nel Canale soprattutto sul piano tecnico con lo sviluppo una rete di AWS Premier Consulting Partner che hanno, così, la possibilità di mettere a frutto le certificazioni e il loro accreditamento come partner AWS. Sebbene Google Cloud sia relativamente in ritardo nelle strategie basate sui partner rispetto a Microsoft e AWS, il suo piano di go-to-market è ora completamente indirizzato ai partner di Canale con una vera e propria esplosione dei partner certificati Google Cloud.

Per gli MSP di nuova generazione l'iscrizione dei propri team a programmi di certificazione Azure, AWS e Google appare, dunque, un passaggio quasi obbligato spostando l'attenzione dal margine di rivendita verso moltiplicatori di business di altro tipo offerti dai tre "grandi" del cloud. ❖

# L'IT POST COVID SI RAFFORZA E SI REINVENTA

L'accelerazione verso il digitale, alimentata dal Covid, ha determinato un incremento degli investimenti in IT che prosegue. Oggi, in una prospettiva di post pandemia, l'IT si prepara a un nuovo corso caratterizzato da nuovi servizi e tecnologie anziché dall'evoluzione di quelli precedenti, in cui le parole chiave saranno cloud, smart working e resilienza

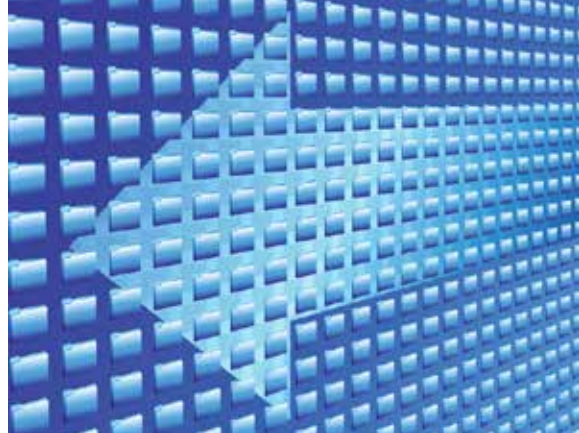
di **Riccardo Florio**

Il Covid-19 ha determinato una svolta epocale causando importanti cambiamenti. Tra questi anche un'accelerazione del processo di conversione dei canali tradizionali al digitale trasformando quella che, fino a poco tempo fa, era considerata una destinazione, in un'evoluzione in corso.

Mentre molte aziende hanno subito un forte declino, la spesa IT sta accelerando oltre le aspettative e, secondo Gartner, alla fine del 2021 raggiungerà globalmente 4206 miliardi di dollari con una crescita ri-

spetto all'anno precedente (dove già era cresciuta di circa 1%) di circa il 9%.

Le aziende e i CEO sembrano predisposti a investire in tecnologie che abbiano una diretta correlazione con i risultati di business più che in ogni altro ambito con l'obiettivo di cavalcare le opportunità offerte dalla digital transformation. Anche se molte cose sono già cambiate, tutti gli analisti ritengono che ci troviamo in una fase in cui si è appena grattata la superficie di quello che sarà il cambiamento prossimo venturo.



L'IT dopo il Covid si prospetta, quindi, differente da quello pre pandemia perché indirizzato, soprattutto, a costruire servizi e tecnologie che non esistono ancora anziché, come è stato per molto tempo, a capitalizzare sull'evoluzione di quelli precedenti. L'obiettivo diventa quello di creare nuove opportunità di differenziazione in un mercato globale sempre più affollato.

Questo passaggio vedrà un rafforzamento del settore dei servizi IT che, infatti, ha rappresentato una delle principali aree di crescita nel 2021 con forti incrementi di spesa in settori quali l'infrastruttura as a service a supporto dei carichi di lavoro "mission critical". Le parole chiave del prossimo IT saranno cloud, smart working e resilienza mentre l'IoT tende, controcorrente, a rallentare lasciando prevedere che dovremo aspettare ancora qualche anno per usufruire delle enormi possibilità che offre.

## L'Italia migliora e punta sui servizi cloud

L'Italia, per una volta, non sta a guardare. Nel Digital Riser Report 2021 redatto dallo European Center for Digital Competitiveness, che analizza come i governi hanno affrontato e gestito la transizione digitale guidata dalle tecnologie tra il 2018 e il 2020, il nostro Paese si colloca al secondo posto tra le nazioni

del G7 (preceduto solo dal Canada) e all'ottavo posto tra i Paesi del G20.

Le infrastrutture digitali svolgono un ruolo vitale per molte delle nostre attività quotidiane, dalle autostrade, alle ferrovie, alle reti elettriche e il Ministero per l'innovazione tecnologica e la transizione digitale ha, recentemente, diffuso le linee guida della strategia per rafforzare le infrastrutture digitali della Pubblica Amministrazione e favorire il passaggio al cloud dei servizi pubblici.

Con il progetto "Infrastrutture digitali e cloud" si punta ad abilitare la Pubblica Amministrazione a migliorare la qualità dell'erogazione dei servizi verso cittadini e imprese attraverso l'adozione in via prioritaria del cloud. La Strategia Cloud Italia, elaborata insieme all'Agenzia per la cyber sicurezza nazionale, prevede, tra l'altro, di: classificare dati e servizi della PA in strategici, critici e ordinari; qualificare i servizi cloud attraverso un processo di scrutinio tecnologico; realizzare il Polo Strategico Nazionale dedicato ai servizi che trattano dati strategici e critici.

### Collaborare e lavorare in modo smart

L'isolamento sociale causato dal Covid ha indirizzato cospicui investimenti delle aziende italiane anche verso soluzioni innovative a supporto della produttività.

La connessione alle risorse aziendali da remoto è ormai irrinunciabile ma è ormai evidente a molti che risulta inefficace da sola. Servono anche soluzioni che favoriscano la comunicazione tra team, la diffusione di conoscenza, nuovi strumenti di analisi per prendere decisioni più motivate, sistemi di automazione dei processi e dei flussi di lavoro da remoto, tool di digitalizzazione documentale e interfacce utente sempre più semplici.

Il tema della mobilità influenza anche i dispositivi personali, che si personalizzano sempre

	2020		2021		2022	
	Spesa (mld \$)	Crescita (%)	Spesa (mld \$)	Crescita (%)	Spesa (mld \$)	Crescita (%)
Sistemi Data Center	178,47	2,5	191,65	7,4	201,65	5,2
Software Enterprise	529,03	9,1	598,96	13,2	669,11	11,7
Dispositivi	696,99	-1,5	793,97	13,9	800,17	0,8
Servizi IT	1071,28	1,7	1176,68	9,8	1277,23	8,5
Servizi di comunicazione	1396,29	-1,4	1444,98	3,5	1481,88	2,6
Totale	3872,05	0,9	4206,23	8,6	4430,05	5,3

*DIDASCALIA: Previsione della spesa globale IT (Fonte: Gartner, luglio 2021)*

più per fattore di forma, capacità, prestazioni e sicurezza al fine di rispondere alle esigenze specifiche di ogni tipologia di lavoratore. Anche le soluzioni di stampa diventano mobili, delocalizzate ed erogate in forma di servizio. Tutto ciò sancisce definitivamente che il posto di lavoro è, ormai, un luogo privo di perimetro fisico, di contorni geografici e di orari fissi.

### Dalla sicurezza alla cyber resilienza

In questo nuovo corso anche il concetto di sicurezza IT si amplia e si afferma quello di cyber resilienza che riunisce, essenzialmente, le aree della sicurezza delle informazioni, della continuità aziendale e della resilienza organizzativa.

La cyber resilience 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).

Mentre la sicurezza informatica descrive la capacità di un'azienda di proteggersi dalle minacce informatiche, la cyber resilienza 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 da altri fattori quali, per esempio, il semplice errore umano. ❖

# TEMPO DI SMART WORKING: GUIDA DI SOPRAVVIVENZA ALL'ECCESSO DI RIUNIONI

La pandemia ha amplificato il numero di meeting, costringendo a un eccesso di impegni che, a volte, va in direzione opposta alla produttività.

Alcuni suggerimenti per sfruttare al meglio le riunioni ed evitare quelle inutili.



È un trend sempre più diffuso. Siete a casa in smart working e potreste lavorare a quel progetto a cui tenete tanto. Con calma, con qualità e senza interruzioni e invece non va così. Sempre più dipendenti, manager e imprenditori trascorrono le loro giornate in continue riunioni (in presenza o, sempre più spesso, in video), una dopo l'altra e gli studi di settore confermano che tutto ciò sta rallentando lavoro e produttività. Secondo molti, le riunioni stanno diventando una specie di "male assoluto". Quindi cosa facciamo? Le aboliamo? Le limitiamo? E come? Magari potremmo implementare dei singoli giorni "senza riunioni"?

Sì, l'idea di un giorno alla settimana in cui siano banditi i meeting appare attraente, ma un tale divieto farebbe solo spostare le riunioni in giorni differenti se prima non si affronta alla radice il problema sottostante: le aziende dovrebbero concentrarsi sulla riduzione delle dimensioni (quantità di argomenti e persone coinvolte) e durata delle riunioni, eliminando o contenendo quelle inutili e incrementando e rendendo più efficaci le rimanenti.

## Quando la riunione è un killer

Come la maggioranza degli imprenditori e manager, probabilmente iniziate la giornata guardando l'agenda e controllando quali e quante riunioni avete. Spesso noterete che ce ne sono parecchie ogni giorno, molte delle quali urgenti, importanti o impegnative. Se così è per voi, questo risulta spesso essere un killer per la vostra produttività. E soprattutto un killer del vostro umore.

di **Primo Bonacina**

si occupa d'informatica dal 1980. Con PBS - Primo Bonacina Services ([www.primobonacina.com](http://www.primobonacina.com)) fornisce consulenza e "best practice" digitali in ambito sales/marketing/HR

In effetti, le riunioni sono una delle prime cose che analizzo quando inizio a lavorare con un cliente per attività di coaching, proprio perché occupano una parte così grande della loro giornata. Quando trovo un manager che sta lottando con una raffica costante di interruzioni, gli faccio alcune domande in relazione proprio a queste riunioni.

Domande come:

- Quante riunioni hai in media al giorno?
- Devi essere proprio presente in tutte o qualcuna può essere delegata?
- Quali e quante persone sono presenti in ogni meeting? Perché proprio queste persone?
- Tutti gli incontri aggiungono valore reale? Oppure sono solo diventati routine?
- Quali incontri potrebbero essere cancellati o resi meno frequenti o più brevi?
- Quali incontri potrebbero essere sostituiti da informative scritte o da un messaggio audio o video?
- Quali riunioni devono, invece, essere aggiunte o estese o migliorate?



## Una prima risposta: concentrarsi sugli obiettivi

Il problema è chiaro. Meno chiara è la soluzione.

Diamo però una prima risposta: piuttosto che concentrarsi sulle riunioni come attività da fissare, concentriamoci sugli obiettivi di business e su come utilizzare efficacemente le nostre ore lavorative e quelle del nostro team.

Le riunioni sono uno degli strumenti della nostra cassetta degli attrezzi.

Se ben utilizzate, possono essere efficaci. Se, però, ci accorgiamo che stiamo sprestando troppo tempo in troppi meeting e ci prende un senso di fastidio, è un chiaro sintomo di qualcosa che non va, che ci deve spingere a rivedere le attività correnti e a studiare metodi per ottimizzare il tempo speso da noi e dal nostro team e il valore che otteniamo da questi meeting.

## Cinque semplici avvertenze

Certamente è bene affrontare il tema alla radice però, molto spesso, quando ci si accorge del problema, si inizia con alcune modifiche di piccolo impatto. Vi sembreranno que-

sti che seguono dei palliativi ma portano spesso a miglione sia per quanto riguarda la gestione del tempo sia per i risultati.

Ecco un primo set di cinque idee:

**1 Evitate l'agenda "spezzatino".** In pratica, allocate diverse riunioni una dopo l'altra in modo da averne alcune di fila seguite da un intervallo di tempo più ampio per concentrarsi e lavorare. Ma anche per avere del tempo libero o per visitare clienti oppure per riflettere. Questo è qualcosa che, personalmente, faccio spesso: quando devo organizzare una riunione cerco, per quanto possibile, di allocarla a mezz'ora di distanza (o, al massimo, un'ora) da un meeting già fissato, riducendo la frammentazione dell'agenda. Mi trovo quindi intere mezzegiate senza riunioni prefissate.

**2 Rivedete periodicamente l'agenda e bloccate del tempo subito dopo le riunioni chiave per affrontare il lavoro che ne deriva.**

Supponiamo che siate in smart working e in video meeting e, quindi, terminata la riunione, siete già alla scrivania. Quando incontrate

un cliente, probabilmente da quella riunione saranno uscite idee e proposte di azione. Allora è bene avere subito 30 minuti liberi per lavorarci a mente calda. Magari non gli manderete subito la quotazione e il piano di lavoro, ma, immediatamente, quando avete tutto ancora in testa, potrete stenderne una prima bozza. Questo non solo vi farà utilizzare meglio il vostro tempo, ma, soprattutto, ridurrà i tempi di futura consultazione di appunti e rifocalizzazione sull'argomento, portando quindi a una maggiore produttività in generale.

### ③ **Liberate un giorno della settimana (o due mezza giornate) dalle riunioni.**

Ciò vi consentirà, almeno in quel giorno, un lavoro più approfondito. Ci sono manager che hanno bloccato in agenda un giorno fisso alla settimana (oppure non è fisso e lo allocano di volta in volta) e quindi nessuno, salvo eccezioni fortemente motivate, può inserire appuntamenti in agenda quel giorno.

④ **Prima della riunione, fate circolare sempre un'agenda precisa.** Sembra una banalità, ma aiuta davvero. Spesso le agende o non ci

sono oppure sono approssimative e imprecise.

### ⑤ **Al termine della settimana calcolate quante ore avete dedicato alle riunioni rispetto al resto del lavoro.**

**E poi fate la media mensile.** Ancora una volta, sembra una banalità ma vi aiuta a capire l'entità del fenomeno e quanto e come usate il vostro tempo e quello dei vostri collaboratori.

### **Sette ulteriori suggerimenti**

Le precedenti idee sono semplici suggerimenti di ottimizzazione, da applicare al volo e senza pensarci nemmeno troppo.

Proviamo invece a dare 7 ulteriori suggerimenti di maggiore portata su come rendere più efficaci le riunioni:

① **Pianificate sempre le riunioni in anticipo.** Se non è stato emesso per tempo un vero ordine del giorno (forte, stringente, focalizzato) allora non tenete la riunione. Le possibilità che si vada fuori dai binari e che si perda tempo in attività che non creano valore sono alte. Rimandate l'incontro fino a quando non potrete dedicare del tempo a focalizzare un preciso ordine

del giorno

② **Evitate le riunioni ricorrenti.** Anche se è un'opinione controcorrente, evitate gli "staff meeting del lunedì" in cui ci si incontra per "fare il punto". Fare il punto di cosa? E perché proprio il lunedì? E perché non un lunedì sì e l'altro no? Insomma, diventa più un'abitudine come il tè delle 5, che una vera opportunità di far crescere il business.

③ **Iniziate puntuali, iniziate forte.** Se qualcuno arriva con 10 minuti di ritardo e tutti lo attendono, tutti perdono 10 minuti. Evitate i ritardi, entrate direttamente nell'agenda del meeting, arrivate al punto. Niente convenevoli. Non dovette per forza fare i simpatici. Il tempo di tutti è prezioso e, se spendete alcuni minuti per riscaldarvi, al termine della giornata, avrete sprecato un'ora o più

④ **Rimanete concentrati.** È facile essere sviati ed è più difficile rimanere sul pezzo. Ma, se ci riuscite, ne vale davvero la pena. Seguite strettamente l'agenda e, se vi trovate a divagare (può capitare che dalla riunione escano riflessioni sensate e utili ma non attinenti al tema del giorno), annotatelo come

possibile iniziativa futura e affrontatelo in altro momento.

⑤ **Date a tutti la possibilità di contribuire.** Fate attenzione a evitare che una o due personalità forti dirottino la riunione. Soprattutto se siete voi una di quelle persone!

⑥ **Chiarite le azioni mentre procedete.** Avete davanti una lunga riunione e non volete perdervi nulla? Allora annotate tutti gli elementi importanti mentre procedete. Chi fa cosa? Entro quando? Con quali risultati attesi? Con quali momenti di verifica?

⑦ **Riepilogate.** Al termine della riunione inviate un'e-mail riassuntiva che delinea i punti trattati e le azioni previste. Successivamente qualcuno verrà incaricato di verificare che si sia dato seguito a quanto pianificato. Soprattutto, siate produttivi. Un calendario pieno di incontri inutili non è nulla di cui essere fieri. Un calendario che contenga alcune riunioni a valore aggiunto, ben pianificate e che vi aiutino nel far progredire la vostra attività, invece sì. ❖

# Essere donna nel mondo della sicurezza digitale in Italia

*Il Rapporto "Cyber Security Women Italy (CSWI) - Il lavoro femminile nella sicurezza digitale in Italia" a cura di Andrea Bozzetti, Marco Bozzetti e Laura Rivella, pubblicato da AIPSI a Novembre 2021 evidenzia le disparità di genere.*

di **Andrea Bozzetti, Marco Bozzetti, Laura Rivella**

L'indagine CSWI 2021 ha interpellato 468 professioniste che, a vario titolo, si occupano per lavoro di sicurezza digitale: operano in aziende private e pubbliche sia lato domanda cybersecurity che lato offerta, nella formazione in ambito universitario e non, e come libere professioniste, 9,2% (freelance con partita IVA).

Il 13,8% è una imprenditrice, tipicamente di aziende dell'offerta di sicurezza digitale e l'8% opera in società di consulenza. Le rispondenti all'indagine sono prevalentemente adulte e senior: il 78,2% ha più di 35 anni e il 21,8% ha tra 18 e 34 anni. Il maggior numero di rispondenti, 36,1% è nella fascia 45-54 anni, e com-



più spesso le over 45 si attestano al 61,3%.

Il livello di istruzione delle rispondenti è alto: più dei due terzi delle rispondenti hanno conseguito la laurea, e di queste solo il 9,3% ha una laurea triennale. Le non laureate sono il 28% delle rispondenti. La grande maggioranza, 67,1% ha conseguito una laurea di tipo tecnico scientifico. Relativamente poche, il 22,7%, hanno acquisito specifiche certificazioni tecniche e/o manageriali inerenti alla sicurezza digitale e alla sua gestione.

La certificazione più diffusa tra le rispondenti è quella ITIL (8,4%), al secondo quella di Lead Auditor/ISO 27001 specifica per la sicurezza digitale (6,8%), cui seguono tutte le altre con percentuali inferiori al 5%. Solo il 2,6% ha una certificazione DPO (Digital Privacy Office).

## Essere donna nella Cybersecurity

Alla richiesta su quali siano le necessità e le prospettive di evoluzione e crescita nel prossimo futuro, quasi la metà delle rispondenti ha dichiarato di dover migliorare e approfondire le proprie conoscenze tecniche (49,4%), per il 28,57% quelle legali, per il 22,08% quelle organizzative e manageriali.

In termini di prospettive, il 43,4% intende continuare nella propria attività nella sicurezza digitale, accrescendo le sue competenze e specializzandosi ulteriormente, mentre il 27,6% intende passare, a breve o a medio termine, ad altre attività e ad altri ruoli. Quasi un quarto delle rispondenti non ha al momento idee chiare su che cosa vorrebbe fare nel prossimo futuro.

Un tema analizzato è se essere donna, nell'ambito della cybersecurity, è ritenuto dalle rispondenti un fattore negativo oppure no. Solo il 2,6% ritiene l'essere donna un aspetto favorevole per lavorare in questo campo. La maggioranza delle rispondenti, il 57,1%,

ritiene che l'essere donna sia del tutto indifferente. Il 22,1% lo giudica un elemento sfavorevole e una percentuale di poco inferiore, dichiara di non essere in grado di valutarlo, sulla base della propria esperienza sul campo.

La fascia di età 35-44 è quella che percentualmente più "soffre" nell'essere donna: è la fascia in cui la maggior parte delle donne è sposata, ha figli che vuole accudire, è a un livello di maturità e di responsabilità professionale per le quale si attenderebbe dei riconoscimenti, di carriera o economici.

Queste indicazioni, pur non avendo una valenza statistica da un campione rappresentativo della realtà femminile nel campo della sicurezza digitale in Italia, mostrano che la situazione nel nostro Paese, in termini di gender gap, è abbastanza positiva.

## Conciliare le esigenze di tempo professionali e personali

Un aspetto assai importante nell'attività lavorativa è il poter ben conciliare le esigenze di tempo per l'attività professionale con quelle per la propria persona e per la propria famiglia. Questa conciliazione è particolarmente critica per una donna, in qualsiasi tipo e ruolo lavorativo, e soprattutto per ruoli ad alta professionalità e/o dirigenziali. Conciliazione necessaria anche per le attività di sicurezza digitale, tema in rapida e continua evoluzione, e per il quale solo il 50% può operarvi a tempio pieno. L'altra metà delle professioniste deve condividere, e ben bilanciare, le attività di cybersecurity con altre attività lavorative.

Il 23,5% delle rispondenti ha dichiarato di avere, al momento, problemi nel bilanciare e conciliare attività lavorativa e attività personale e per la famiglia.

Considerando che questo problema è uno dei principali fattori

del divario di genere, si tratta tutto sommato di una percentuale inferiore al previsto.

Sono soprattutto le rispondenti nella fascia 18-34 anni che non hanno problemi nel conciliare e quelle con età superiore a 55 anni, mentre qualche problema al momento esiste nella fascia 35-54 anni.

Tra le motivazioni per queste difficoltà: la mancanza di un team di lavoro supportivo e collaborativo, la disponibilità di tempo per seguire la famiglia, la difficoltà di svolgere almeno alcune attività di cybersecurity da remoto, la frequente necessità di operare in trasferta e l'esigenza di ritagliarsi tempo per la formazione personale costante necessaria nel campo della cybersecurity.



## La disparità retributiva

Il divario retributivo è uno dei temi centrali nella disparità di genere e ha trovato riscontro anche in questa indagine, sia in Italia che in UE. Confrontando la permanenza percentuale di questo divario si evidenzia che per l'Italia è diminuito di 3 punti percentuali, mentre per l'UE, come media tra i vari Paesi, è aumentato di un punto.

Il bacino delle rispondenti di CSWI 2021 conferma che le donne tendono a essere pagate meno degli uomini, ma evidenzia una percezione meno critica del divario di genere.

Il 34,2% delle rispondenti ritiene di essere remunerata meno dei colleghi uomini, a parità di fattori quali ruolo, responsabilità, anzianità lavorativa, competenze e così via, mentre solo il 3,9% reputa di essere pagata di più rispetto agli uomini (le professioniste che ritengono di essere pagate di più si concentrano nelle fasce d'età tra 25 e 54 anni).

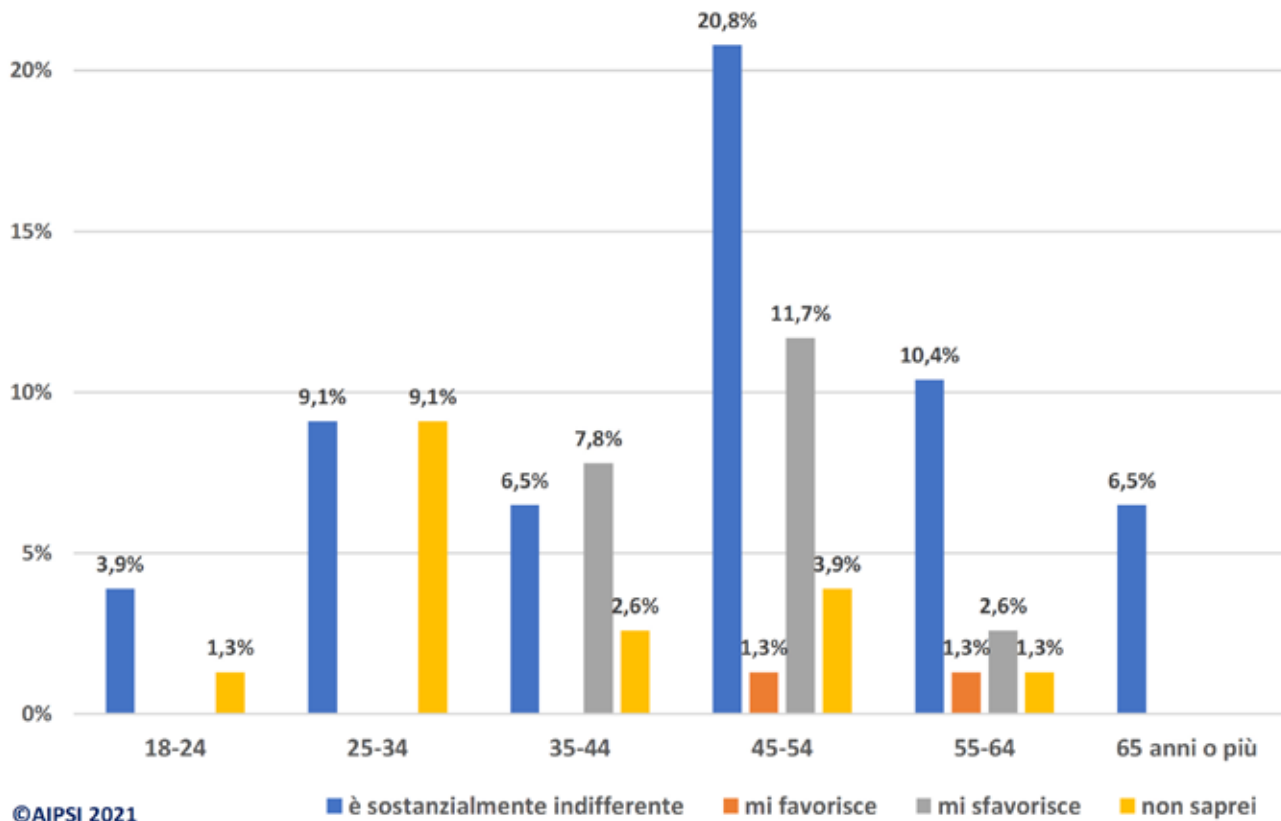
Un quarto delle rispondenti ritiene di essere pagata sostanzialmente allo stesso modo degli uomini.

La percentuale maggiore delle rispondenti, (36,8 %) dichiara di non sapere se sia pagata più o meno rispetto a colleghi; si tratta di un dato ragionevole considerando la difficoltà nel conoscere le retribuzioni dei colleghi e di riuscire a confrontare livelli retributivi a parità di ruolo, competenze ed età nel campo della sicurezza digitale, così articolato, trasversale e interdisciplinare. All'aumentare del livello di istruzione cresce la retribuzione oraria per uomini e donne, ma aumenta ulteriormente lo svantaggio retributivo per le donne.

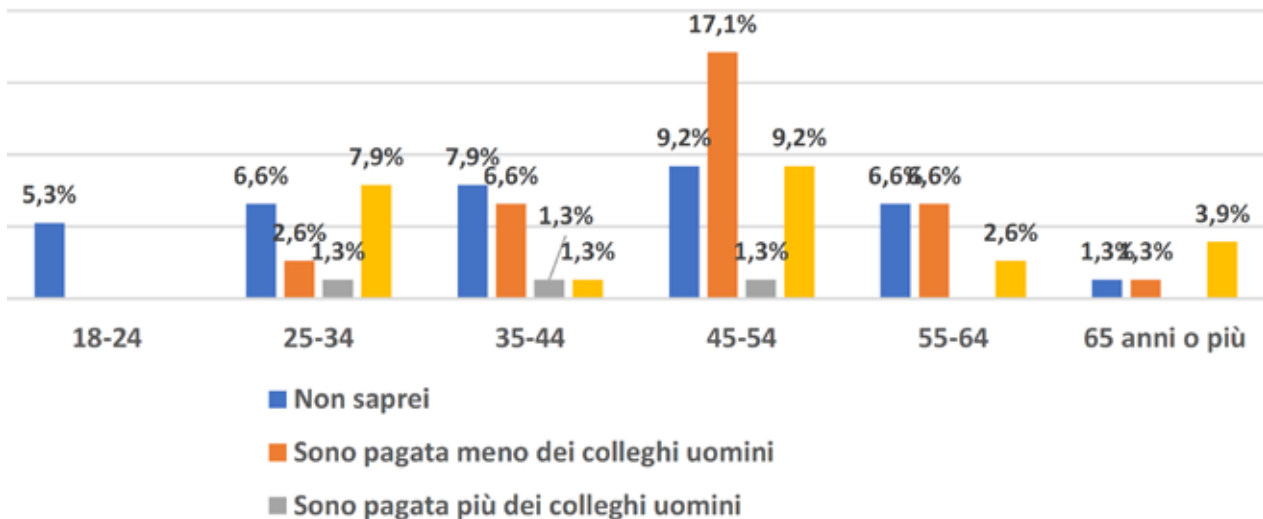
Il Rapporto AIPSI CSWI 2021 è liberamente scaricabile dal sito di AIPSI



## CSWI 2021 - La valenza del fattore "donna" nella cybersecurity per età



## CSWI 2021 - Differenza di genere nella retribuzione in funzione dell'età





# Proteggere l'azienda dagli attacchi informatici

# INDAGINE OAD 2021 SUGLI ATTACCHI DIGITALI IN ITALIA

L'anticipazione dei risultati dell'indagine che da 14 anni fotografa, con l'aiuto della Polizia Postale e delle Comunicazioni, lo scenario degli attacchi informatici nel nostro Paese ad aziende ed enti pubblici

di **Marco R. A. Bozzetti**, *Presidente AIPSI*

## **AIPSI, Associazione Italiana Professionisti Sicurezza Informatica**

AIPSI (<https://www.aipsi.org>) è la libera associazione no-profit, che raduna a livello individuale chi è interessato professionalmente alla sicurezza informatica, in qualsiasi ruolo e modalità. AIPSI è il capitolo italiano di ISSA, Information System Security Association (<https://www.issa.org/>), la più grande organizzazione analoga a livello mondiale, che conta complessivamente oltre 13mila soci. Il Socio AIPSI è contemporaneamente anche Socio ISSA. Gli obiettivi principali di AIPSI sono di aiutare i propri soci nella crescita professionale e delle competenze e di diffondere la cultura della sicurezza digitale.



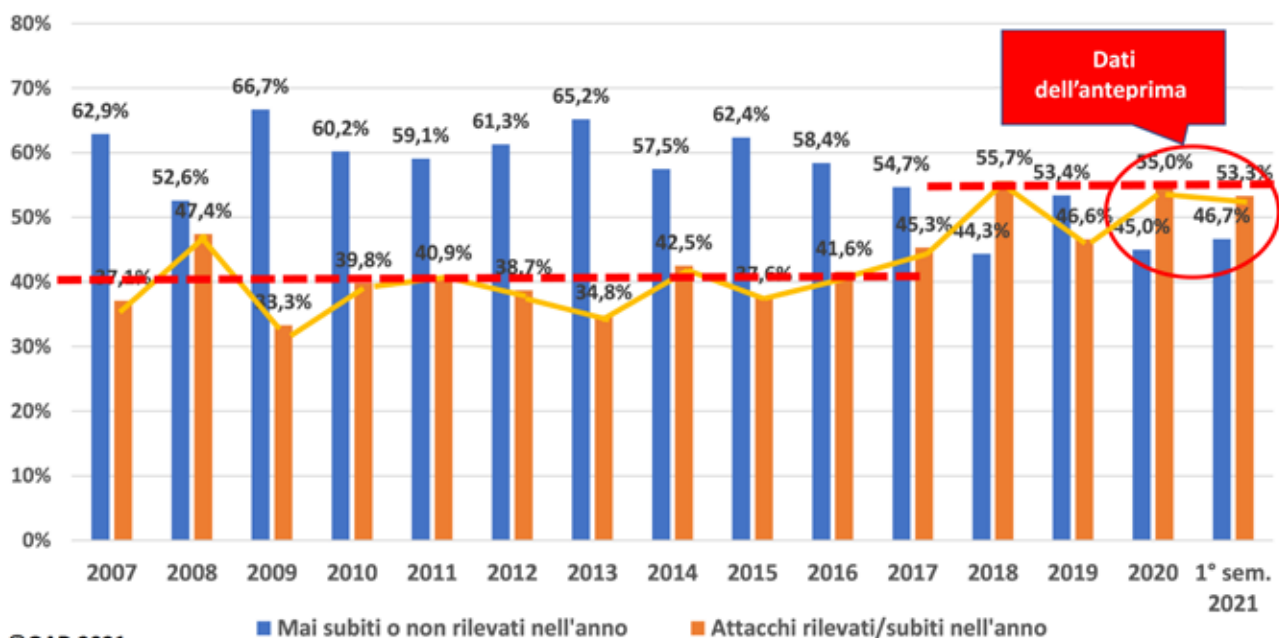
Dal 2007 AIPSI, Associazione Italiana Professionisti Sicurezza Informatica, realizza l'indagine indipendente OAD (Osservatorio Attacchi Digitali) per analizzare il fenomeno degli attacchi digitali ai sistemi informatici di aziende ed enti pubblici in Italia.

L'indagine, unica nel suo genere, si focalizza sullo scenario locale italiano fornendo indicazioni sulla tipologia e l'ampiezza del fenomeno utili per valutare i possibili rischi e attivare le misure più idonee di prevenzione e protezione.

La Polizia Postale e delle Telecomunicazioni da anni collabora con l'indagine OAD fornendo suoi dati sugli attacchi alle infrastrutture critiche, sulle frodi finanziarie online e sul cyber terrorismo. Nel 2021, inoltre, OAD è stata inclusa tra i progetti di Repubblica Digitale per la sua rilevanza in termini di comunicazione, sensibilizzazione e formazione sulla cybersecurity.

L'indagine 2021 è in fase di completamento e ve ne anticipiamo i risultati che potrebbero subire lievi variazioni. Il rapporto OAD 2021 definitivo (così come tutti quelli realizzati da AIPSI dal 2007 a oggi) può essere scaricato gratuitamente dal sito <https://www.oadweb.it>.

## Confronto risultati indagini OAD-OAI 2007-2021



### Il trend degli attacchi digitali in Italia

La quasi totalità dei rispondenti all'indagine 2021 appartiene ad aziende private e, di queste, quasi l'80% sono Piccole Medie Imprese con meno di 250 dipendenti. Un dato che rispecchia i più recenti dati Istat (2019) secondo cui, in Italia, su 4milioni e 304mila imprese, il 64,03% è senza dipendenti, il 31,65% ne ha meno di 10, il 4,22% tra 10 e 250 e solo lo 0,1% ha più 250 dipendenti. Per le PA la situazione è analoga: poche le PA di grandi dimensioni, come i Ministeri ed i grandi Comuni, e moltissime le piccole e piccolissime organizzazioni.

Un primo dato interessante è l'andamento del fenomeno attacchi digitali ad aziende ed enti pubblici in Italia dal 2007 al 2021, con un trend a onda, in una costante rincorsa tra guardie e ladri digitali a migliorare gli attacchi e potenziare le misure di prevenzione e protezione.

Nel 2018, per la prima volta, la percentuale di aziende che ha dichiarato di aver subito un attacco ha superato quella di chi lo ha negato. Negli ultimi 18 mesi la percentuale si assesta a circa il 55%.

Si tratta di una percentuale che può sembrare bassa ma che va interpretata considerando il numero prevalente di piccole e piccolissime aziende ed enti che sono stati interpellati. Le realtà piccole, infatti, non rappresentano un obiettivo di interesse specifico per i cyber criminali, soprattutto per gli attacchi mirati, potendo più facilmente essere coinvolte in attacchi di massa, come quelli basati sul phishing e sul ransomware. Questo aspetto trova conferma nell'analisi della correlazione tra attacchi rilevati e dimensioni aziendali che evidenzia una crescita molto significativa di dichiarazioni di attacchi subiti da parte delle aziende più grandi.

## Tipologie e tecniche di attacco

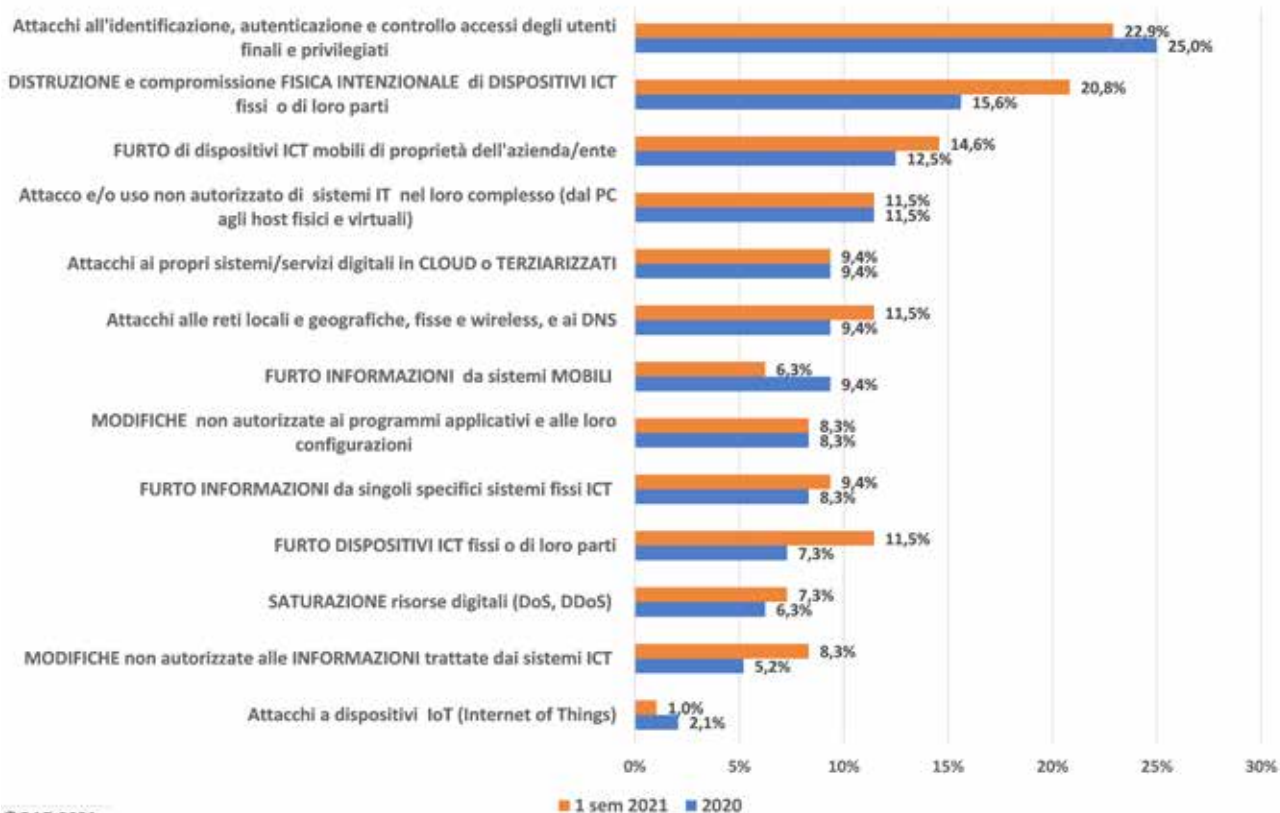
L'indagine ha considerato 14 tipologie di attacco suddivise in base all'obiettivo: il sistema digitale fisico, il suo controllo degli accessi, le sue applicazioni, la sua rete di comunicazione, i dati trattati e così via.

Al primo posto come tipologia percentualmente più diffusa si conferma quella degli attacchi ai sistemi di identificazione, autenticazione, autorizzazione: in pratica ai sistemi di controllo degli accessi ai sistemi digitali. Un primato assai critico, dato che si tratta dell'elemento chiave per sottrarre e usare in maniera dolosa l'identità di

digitale di altri utenti, sovente quelli privilegiati. Al secondo posto la distruzione fisica di dispositivi ICT o di loro parti e al terzo il furto di dispositivi mobili: quest'ultimo un attacco da tempo diffuso e in certi anni posizionato in cima alle classifiche di OAD, alla luce della semplicità di attuazione e del valore del dispositivo, in particolare per gli smartphone.

Tra tecniche utilizzate negli attacchi al primo posto si posiziona il social engineering utilizzato per raccogliere informazioni a cui seguono, a breve distanza percentuale, gli attacchi fisici e l'uso di script e malware.

OAD 2021 - Distribuzione % tipologie attacchi rilevati (risposte multiple)



©OAD 2021

## I dati dalla Polizia Postale e delle Comunicazioni

La Polizia Postale e delle Comunicazioni da anni collabora con AIPSI fornendo significativi dati sulle azioni svolte in Italia sul fronte del contrasto agli attacchi digitali e ai crimini informatici, con particolare riferimento alle infrastrutture critiche, al crimine digitale finanziario e al cyber terrorismo.

Il C.N.A.I.P.I.C. (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche) è una struttura della Polizia Postale e delle Comunicazioni incaricata in via esclusiva della prevenzione e della repressione dei crimini

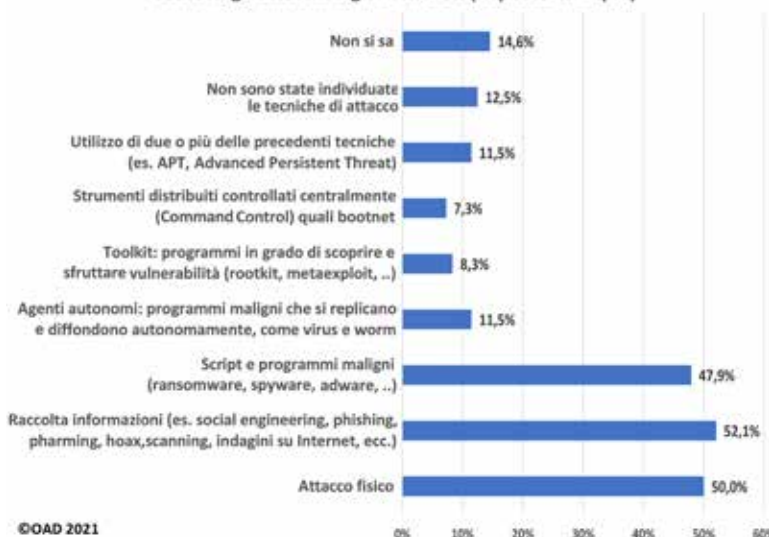
informatici di matrice comune, organizzata o terroristica, che hanno come obiettivo le infrastrutture informatizzate di natura critica e di rilevanza nazionale.

I dati relativi al primo quadrimestre del 2021 evidenziano il trend di crescita degli allarmi emanati e diramati che prosegue dal 2016.

Differente è il dato del numero di attacchi rilevati alle infrastrutture critiche, che oscilla periodicamente negli ultimi anni tra incrementi e decrementi. Oltre al ben noto inseguimento tra guardie e ladri cibernetici, ormai giocato a livello mondiale, può influire su questi dati il riposizionamento di NIS 2 (la Direttiva europea che punta a omogeneizzare gli obblighi in termini di cybersecurity per le infrastrutture critiche), con l'estensione anche del tipo di servizi essenziali e del perimetro di cybersecurity nazionale.

Un dato evidente è la forte disparità tra il numero di indagini avviate rispetto agli attacchi rilevati e, ancora più basso, il numero di persone denunciate, indagate e alla fine arrestate. Il problema di fondo è che, a fronte di centinaia di attacchi rilevati, alla fine gli arrestati si contano su una mano: il cyber crime rimane di fatto quasi impunito, nonostante l'Italia abbia adottato da anni una precisa e severa legislazione (anche in ambito penale) relativa al crimine informatico e vi sia una forza specifica di Polizia, la Polizia Postale, operante sul territorio e con il supporto di unità

OAD 2021 - Ripartizione % tecniche di attacco usate negli attacchi digitali rilevati (risposte multiple)



specializzate dell'Arma dei Carabinieri e della Finanza.

Gli attacchi digitali agli ambienti e alle transazioni finanziarie sono prevalentemente finalizzati a ottenere un illecito guadagno economico, per cui ogni transazione economica rappresenta un potenziale target. Questo tipo di crimine informatico include anche attacchi indirizzati alle piattaforme di e-commerce, ivi inclusi i relativi pagamenti online.

La buona notizia è che le transazioni finanziarie bloccate dalla Polizia Postale nell'ultimo periodo sono in aumento: se il trend dei primi 4 mesi del 2021 si confermasse arriverebbero al doppio rispetto al 2020. In aumento anche le somme recuperate, a conferma del continuo miglioramento delle capacità di contrasto da parte della Polizia Postale.

Il numero di siti Web controllati dalla Polizia Postale che, insieme ad alcune social net, sono alla base e contribuiscono al proselitismo, alla preparazione e al coordinamento di attacchi terroristici,

	gen. - apr. 2021	2020	2019	2018	2017	2016
Attacchi rilevati	282	509	1.181	459	1.032	844
Allarmi diramati	24.824	83.416	82.484	80.777	31.254	6.721
Indagini avviate	34	103	155	74	72	70
Persone arrestate	0	n.d.	3	1	3	3
Persone denunciate/indagate	0	105	117	14	1.316	1.226
Perquisizioni	n.d.	n.d.	n.d.	n.d.	73	58
Richiesta di coop. internazionale Rete 24/7 High Tech Crime G8 (Conv. di Budapest)	17	69	79	108	83	85

Attività svolte dal C.N.A.I.P.I.C. nel periodo 2016-2021 (1° quadrimestre) sulle infrastrutture critiche italiane (Fonte Polizia Postale e delle Comunicazioni)

negli anni è aumentato leggermente, e si mantiene nell'ordine di 36mila. Queste cifre forniscono una chiara indicazione della vastità e complessità del problema che quotidianamente occorre contrastare.



	gen. - apr. 2021	2020	2019	2018	2017	2016
Transazioni fraudolente bloccate	€ 20.200.000	€ 33.186.674	€ 21.333.990	€ 38.400.000	€ 20.839.576	€ 16.050.813
Somme recuperate	24.824 €	83.416 €	82.484 €	80.777 €	31.254 €	n.d.
Percentuale di recupero di somme frodate	43,07%	60,40%	84,37%	23,44%	4,14%	n.d.

Attività della Polizia Postale in contrasto al Financial Cyber Crime (Fonte: Polizia Postale e delle Comunicazioni)

# DALLA SICUREZZA ALLA RESILIENZA: COME CAMBIANO I PARADIGMI DI PROTEZIONE

Nel corso del tempo, a ogni scenario di minaccia ha fatto seguito un corrispondente modello di sicurezza. Finora è stata la sicurezza a inseguire, ma con le soluzioni di CyberRes è possibile agire in anticipo

di **Riccardo Florio**

Le tecnologie per la sicurezza informatica hanno cominciato ad affermarsi seguendo un paradigma di tipo reattivo. I tempi erano diversi e gli attacchi meno sofisticati, estremamente meno numerosi in numero e non così diversificati e, inoltre, tutto avveniva più lentamente.

La sicurezza reattiva interveniva dopo che era stato individuato un problema: un compito, peraltro, non difficile come oggi, poiché gli attacchi erano pensati per dare dimostrazione di sé. Se i tempi di ripristino erano ragionevoli i danni restavano tutto sommato accettabili. Inoltre, le aziende erano meno esposte a problematiche legate al rispetto delle normative. Le tecnologie di sicurezza non godevano di grande popolarità: erano considerate un puro costo e, da alcuni, addirittura un costo inutile.

Con il cambiare dello scenario tecnologico tutto è aumentato: i dati, i volumi di informazioni, il numero degli attacchi, il numero degli accessi alle risorse aziendali, il numero di sistemi e processi e così via. La storia recente si è riempita di stalle chiuse dopo che i proverbiali buoi sono scappati ed è apparso evidente che le perdite e i danni di un attacco andato a buon fine non erano più facilmente assorbibili e, anzi, a volte, non assorbibili del tutto, fino a decretare persino la chiusura di un'azienda.



## I limiti dei modelli preventivi e predittivi

Questo nuovo scenario ha portato a rivedere il modello della sicurezza in una rinnovata ottica di tipo preventivo.

Tuttavia, l'iniziale idea di prevenzione, basata essenzialmente sul controllo di minacce note, si è dimostrata efficace per un tempo piuttosto breve. Un tempo che ha coinciso con un contestuale mutamento nella natura del cyber crimine secondo modelli organizzati su larga scala e logiche imprenditoriali, dove l'unico obiettivo è il massimo profitto. Dal modello preventivo si è, quindi, passati a un modello predittivo in cui l'obiettivo era ancora quello di prevenire, ma con metodi che fossero un passo avanti e non uno indietro a quelli dei cyber criminali. Questo obiettivo ambizioso ha portato allo sviluppo di nuove classi di software come i sistemi SIEM (Security Information and Event Management), capaci di rilevare e gestire avvisi di sicurezza provenienti da tutte le soluzioni implementate e relativi a dati di ogni tipo. L'efficacia di questo modello di protezione richiede però un significativo contributo umano nel costante adeguamento delle impostazioni di sicu-



## Come rendere più resiliente la tua azienda

*Pierpaolo Ali, Director Southern Europe, Russia, CIS, CEE & Israel di CyberRes delinea modalità e soluzioni per aumentare il livello di resilienza*



### Cosa significa essere un'azienda resiliente?

Significa predisporre un modello integrato di governance della sicurezza pensato per garantire la continuità operativa mentre l'infrastruttura aziendale si trova a dover affrontare continue minacce e attacchi. Significa organizzare sistemi, tecnologie e processi in modo tale che sia possibile

predisporre le contromisure necessarie per bloccare attacchi, eliminare vulnerabilità e impedire minacce prima ancora che l'infrastruttura ne sia interessata.

### Perché è necessaria?

È necessaria per due ragioni fondamentali. La prima è che le minacce sono così numerose ed evolvono così rapidamente che non c'è tempo per analizzare tutti gli "alert" né per affrontarle efficacemente una volta che sono arrivate alle porte dell'infrastruttura aziendale. La seconda ragione è che il costo per una violazione della sicurezza è talmente elevato che, dopo la fase di ripristino della normalità, un'azienda può trovarsi in grande sofferenza, se non addirittura non riuscire più a riprendersi.

### Qual è il punto di partenza per rendere un'azienda resiliente?

Il primo passaggio è quello di effettuare un assessment del proprio livello di cyber resilienza, in base al quale poter effettuare una pianificazione tattica e strategica. Servono poi tecnologie innovative e automatizzate capaci di intervenire in tempo reale ma, soprattutto, una visione unitaria della sicurezza.

### Con quali tasselli si costruisce la resilienza?

Si costruisce attorno a tre principi. Il primo è predisporre la protezione da ogni tipo di minaccia informatica attraverso: una governance delle identità e modelli avanzati di autenticazione; una protezione dei dati persistente attraverso il loro intero ciclo di vita; il costante rilevamento delle vulnerabilità applicative. Il secondo principio è il rilevamento delle minacce, che deve essere accelerato attraverso soluzioni di data discovery e affiancato da tecnologie di automazione capaci di attivare risposte rapide, riducendo al minimo i falsi positivi. Infine, è necessaria una predisposizione aziendale verso una costante evoluzione, per stare al passo con minacce e rischi informatici, adottando soluzioni di sicurezza intelligenti e adattabili, modelli ibridi di distribuzione e competenze multidisciplinari. In accordo a questi presupposti, CyberRes ha sviluppato le quattro famiglie di prodotti ArcSight, NetIQ, Voltage e Fortify che abilitano una protezione efficace, predittiva e intelligente necessaria per garantire la cyber resilienza.

rezza, di gestione dell'accesso, di protezione dei dati e di definizione delle policy.

Con l'ulteriore crescita esponenziale del numero di minacce, gli avvisi di sicurezza si sono trasformati in veri e propri big data e la richiesta di capacità di analisi, di prestazioni, di competenze e risorse tecnologiche è arrivata a saturare la capacità delle aziende. Mai come negli ultimi due anni i costi per la sicurezza sono cresciuti, arrivando a un livello considerato ormai dalle aziende non più sostenibile. Oltretutto, in molte aree di sicurezza gli investimenti in nuove tecnologie si sono dimostrati inefficaci perché non si è riusciti a realizzare il livello di integrazione necessario o perlomeno non nei tempi richiesti.

### La resilienza informatica (cyber resilience)

Tutto ciò ha spostato il focus sul tema della resilienza. Parlare di resilienza aziendale significa predisporre, all'interno della propria organizzazione, le condizioni per affrontare le diverse tipologie di rischio (strategico, finanziario, operativo e informatico) per rispondere alle minacce e per riprendersi una volta subite.

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 e così via).

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, ridurre le violazioni e migliorare la reputazione. Di conseguenza, la cyber resilience svolge un ruolo fondamentale nel guidare la trasformazione digitale.

### Cyber resilience e cyber security

Il principio cardine alla base di un modello di sicurezza resiliente è l'adattabilità, con un approccio predittivo che sfrutta tecnologie di machine learning e intelligenza artificiale capaci di automatizzare i compiti di analisi e di adeguare dinamicamente e autonomamente il modello di protezione in base all'evoluzione dello scenario.

L'obiettivo è individuare in tempi più rapidi le possibili vulnerabilità, acquisire la capacità per risolverle più rapidamente, riconoscere un numero superiore di attacchi e avere le difese in atto ancor prima che l'attacco venga sferrato.

Insomma, non si tratta più di aspettare l'invasore sotto le mura del castello per difendersi, né di prepararsi sapendo che arriverà il giorno dopo, ma di spostare continuamente il castello in modo che il nemico non lo riesca mai a trovare.

Cyber security e Cyber resilience sono, pertanto, 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 informatica 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 da altre minacce come, per esempio, il semplice errore umano.

Gli aspetti che concorrono a rendere un sistema resiliente comprendono la ridondanza, la semplicità, la riduzione della superficie di attacco, restrizione

dell'accesso e capacità di coordinamento e di comprensione della situazione in corso. Il concetto riassume, essenzialmente, le aree della sicurezza delle informazioni, della continuità aziendale e della resilienza organizzativa.

### CyberRes: il nuovo brand per garantire la resilienza

CyberRes (CyberRes.com) è la nuova Business Unit che Micro Focus, uno dei principali fornitori di software enterprise al mondo, dedica in modo specifico all'esigenza di garantire la cyber resilienza e una protezione efficace di dati, applicazioni e identità digitali.

Con questa mossa strategica Micro Focus cambia i paradigmi di protezione spostando il focus dalla capacità di reagire ad attacchi e minacce a quella di essere resilienti a ogni tipo di impedimento che possa pregiudicare la normale continuità di business.

In accordo a questi presupposti, CyberRes ha sviluppato quattro famiglie di prodotti pensate per garantire la cyber resilienza: ArcSight per la protezione intelligente e automatizzata dalle minacce di ogni tipo, NetIQ per la gestione sicura di identità e accesso, Voltage SecureData per la protezione cifrata dei dati, Fortify per lo sviluppo sicuro e il test delle applicazioni.

Queste famiglie sono costituite da prodotti modulari, integrabili sia tra loro sia con soluzioni di terze parti. Inoltre, si avvalgono di tecnologie innovative quella di machine learning non supervisionato Intersect o la tecnica brevettata Hyper FPE per la cifratura dei dati anche durante l'uso. ❖

### Fortify protegge le applicazioni durante l'intero ciclo di vita

La sicurezza delle applicazioni deve partire dalla fase di sviluppo integrando strumenti di controllo e test di sicurezza direttamente nelle piattaforme di sviluppo per poi estendersi all'intero ciclo di vita. Alla protezione delle applicazioni CyberRes indirizza la consolidata gamma di soluzioni Fortify che abilitano test di sicurezza delle applicazioni in modalità statica sul codice sorgente, in modalità dinamica mentre sono in esecuzione e in ambiente mobile. Le funzionalità Fortify sono disponibili anche come servizio in cloud (Fortify on Demand).

## ArcSight per la ricerca intelligente delle minacce e il blocco degli attacchi

ArcSight è la soluzione di CyberRes di visibilità estesa per il rilevamento e relativa risposta in tempo reale alle minacce, supportata da un potente motore di correlazione (ArcSight ESM) e adatta alle esigenze delle aziende enterprise che devono analizzare in tempo reale grossi flussi di dati.

Un tassello importante nel modello di cyber resilienza proposto da CyberRes è rappresentato da ArcSight Intelligence, un software per l'analisi di sicurezza di tipo predittivo integrata con ArcSight ESM che utilizza la tecnologia Intersect di machine learning non supervisionato per effettuare analisi comportamentale degli utenti e delle entità e prevenire potenziali minacce prima che

raggiungano il loro obiettivo. Questa soluzione permette di identificare comportamenti anomali, identificare gli account compromessi, fronteggiare le minacce interne, individuare gli attacchi mirati e proteggere i computer e i dispositivi mobili. Ad accelerare ulteriormente il rilevamento e la risposta alle minacce concorre ArcSight SOAR, la piattaforma di Security Orchestration, Automation and Response integrata nella soluzione SIEM di ArcSight che consente di radunare centralmente gli avvisi sulle minacce, riducendo i tempi di indagine e attivando automaticamente azioni di risposta e ripristino.

## Il portfolio CyberRes

### Data Privacy and Protection

Individuare, proteggere e rendere sicuri i dati sensibili e ad alto valore

 Voltage

 Fortify

### Application Security

Costruire software sicuro in modo rapido e con una piattaforma di sicurezza applicativa olistica

 Intersect

### Artificial Intelligence and Machine Learning

Aumentare l'intelligenza umana con l'intelligenza delle macchine

### Identity and Access Management

Gestire centralmente le identità di utenti, dispositivi, cose e servizi

 NetIQ

 ArcSight

### Security Operations

Accelerare le attività di rilevamento e risposta efficaci a minacce note e sconosciute

## NetIQ: la protezione dell'identità digitale

Nell'attuale modello di azienda aperta e delocalizzata, dove il nuovo perimetro aziendale è definito dalle identità digitali degli utenti, la cyber resilienza richiede la predisposizione di una gestione centralizzata di identità e accesso che copra utenti, dispositivi, cose e servizi. A questa esigenza Micro Focus indirizza la famiglia di prodotti NetIQ. Le soluzioni NetIQ consentono di gestire il "chi" (dipendenti, clienti) e il "cosa" (dispositivi, servizi) accede a sistemi e dati. Conoscere i modelli normali di queste identità rende più facile identificare la comparsa di modelli anomali di comportamento.

Le soluzioni NetIQ favoriscono anche la predisposizione di un modello di sicurezza Zero Trust basato sul principio che non debbano esistere situazioni, sistemi o utenti che possano essere considerati affidabili a priori. In un modello Zero Trust tutte le attività devono essere monitorate, il livello di accesso fornito deve essere sempre quello minimo necessario allo svolgimento del proprio compito e si devono monitorare costantemente anche gli utenti con privilegi come, per esempio, l'amministratore delegato.

## Dati cifrati sempre e ovunque con Voltage

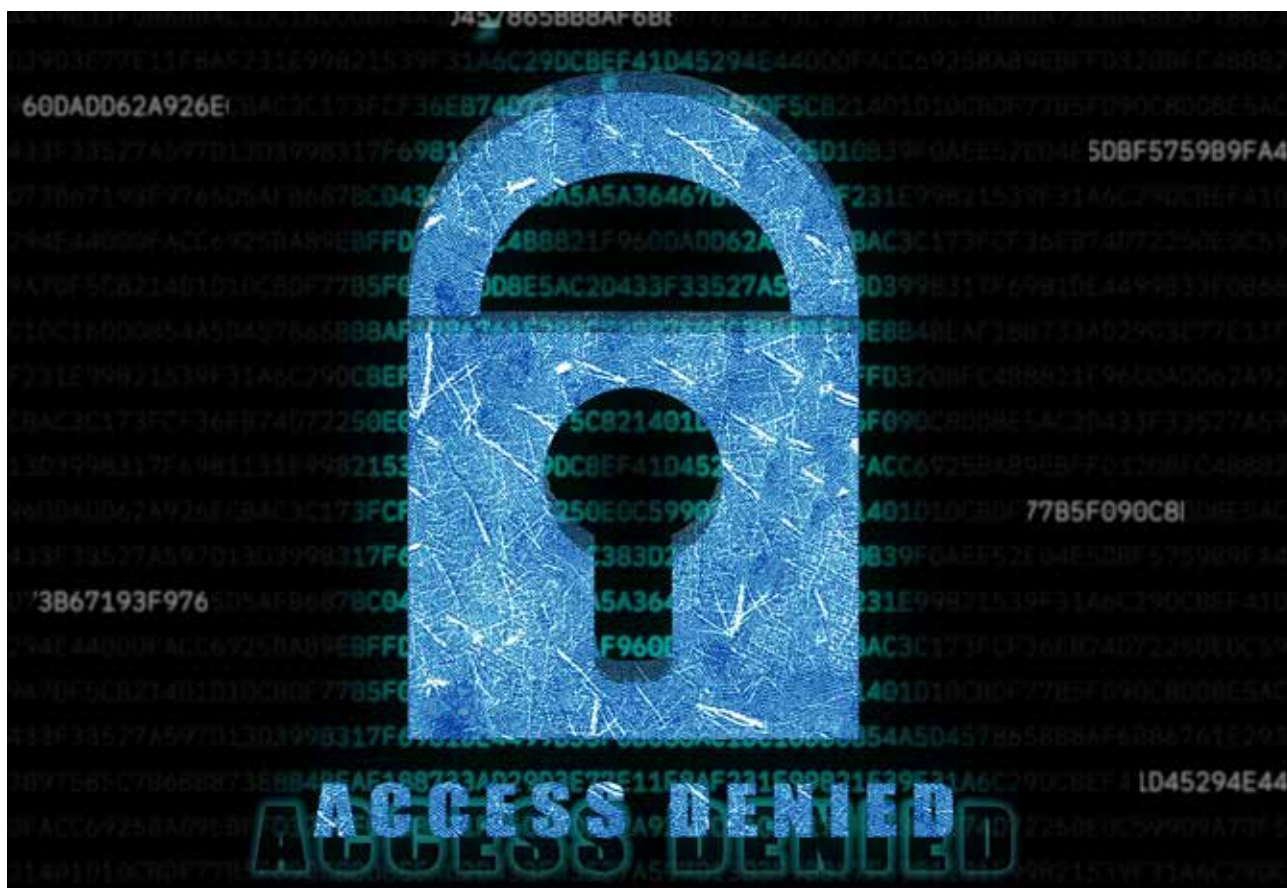
La famiglia Voltage SecureData mette a disposizione una serie di tecnologie innovative e brevettate di cifratura e di accesso sicuro per la protezione dei dati sia strutturati sia destrutturati. Alla base di queste soluzioni vi è un modello di sicurezza che prevede di implementare il meccanismo di difesa e protezione direttamente sul dato o sui sistemi che lo trattano. Con le soluzioni Voltage SecureData i dati restano sempre cifrati dal momento della loro creazione fino alla loro cancellazione sicura. Persino durante l'utilizzo, grazie a tecniche di mascheramento brevettate e uniche sul mercato, le soluzioni Voltage permettono di mantenere cifrati i dati anche all'operatore che li sta trattando.

# RANSOMWARE: IL RICATTO CHE RENDE 20 VOLTE L'INVESTIMENTO

Il rapporto dell'agenzia europea per la cybersecurity evidenzia l'incremento nel numero di attacchi, l'evoluzione delle metodologie e l'aumento dell'importo dei riscatti

di **Camillo Lucariello e Riccardo Florio**

**G**iunge alla nona edizione il Rapporto ETL (Enisa Threat Landscape, panoramica sulle minacce informatiche) realizzato annualmente dalla European Union Agency for Cybersecurity, ossia l'agenzia per la cybersecurity dell'Unione Europea, relativo allo stato delle minacce alla cybersecurity attive sul mercato nel periodo compreso tra aprile 2020 e metà luglio 2021 (disponibile all'indirizzo <https://enisa.europa.eu/publications/enisa-threat-landscape-2021>).



Il Report ha lo scopo di identificare minacce primarie e macro-tendenze osservate riguardo alle minacce, agli attori delle minacce stesse e alle tecniche di attacco, descrivendo anche le più importanti misure di mitigazione possibili.

“Fondamentalmente, Enisa raccoglie dati da fonti attendibili, quali Mitre Att&ck, Shodan e CVE (Common Vulnerabilities and Exposures) e li contestualizza per il territorio Europeo e per il periodo preciso a cui fa riferimento”, spiega Simone Fratus, cybersecurity specialist di TAG Distribuzione, azienda Italiana a capitale israeliano specializzata in cyber security.

### La piaga del Ransomware

Una delle principali e più pericolose minacce di questi ultimi anni è sicuramente costituita dal Ransomware, ossia un tipo di attacco rivolto ai sistemi informativi in cui gli aggressori cifrano i dati di un'organizzazione: per sbloccarli, serve una chiave che viene fornita solo dietro pagamento di un cospicuo riscatto (in inglese, ransom). In alcuni casi, gli aggressori possono anche rubare le informazioni di un'azienda e richiedere un pagamento aggiuntivo in cambio della mancata divulgazione delle informazioni alle autorità, ai concorrenti o al pubblico.

“Il Rapporto ETL delinea caratteristiche ed evoluzioni del Ransomware - continua Fratus -. Pur-

### Le 10 regole per fronteggiare i ransomware

- 1 Implementare strategie di backup sicure e ridondanti.
- 2 Gestire le identità e le autorizzazioni di accesso in base al principio del minimo privilegio e della separazione dei compiti.
- 3 Formare e sensibilizzare gli utenti, inclusi quelli di tipo privilegiato.
- 4 Separare gli ambienti di sviluppo da quelli di produzione.
- 5 Mantenersi aggiornati sulle più recenti tendenze del Ransomware
- 6 Monitorare costantemente i sistemi per identificare rapidamente possibili infezioni.
- 7 Utilizzare prodotti o servizi di sicurezza che bloccano l'accesso a siti di Ransomware noti.
- 8 Fare in modo che le identità e le credenziali siano emesse, gestite, verificate, revocate e verificate per dispositivi, utenti e processi autorizzati.
- 9 Testare periodicamente i piani di risposta e di ripristino in caso di Ransomware per essere sicuri che siano aggiornati rispetto all'evoluzione del ransomware.
- 10 Condividere le informazioni su incidenti o tentativi di attacco con le autorità e il mercato per contribuire a limitarne la diffusione.



troppo col tempo si sono diffuse delle piattaforme di Ransomware-as-a-Service, che consentono anche a persone senza adeguata preparazione tecnica di sviluppare rapidamente, a pagamento, attacchi Ransomware fai-da-te efficaci in modo semplice e veloce. Oggi esistono circa 16 di queste piattaforme disponibili nel mondo”.

È interessante notare che spesso, dietro questi tool di sviluppo di malware, ci sono vere e proprie multinazionali, se non organizzazioni governative. “Sono per esempio disponibili vere e proprie tabelle che indicano quali sono i reali guadagni ot-



*Simone Fratus,  
cybersecurity specialist  
di TAG Distribuzione*

tenibili con una certa piattaforma – spiega Fratus -. Per esempio, ci sono pacchetti che, con un investimento di circa 150 mila euro, garantiscono un ritorno pari a oltre 3 milioni di euro. È questo uno dei motivi che hanno fatto di queste piattaforme un vero e proprio successo, tanto che negli ultimi anni sono diventate uno standard di fatto per gli attacchi ai sistemi informativi più recenti”.

Anche perché nei “pacchetti” vengono offerti, oltre al software, i punti di accesso relativi a varie aziende che si possono scegliere come bersagli e la capacità di riprogrammare rapidamente gli attacchi, in modo da spiazzare i principali sistemi di protezione e intercettazione degli attacchi stessi.

### **I vettori di attacco più comuni**

I due vettori più diffusi per l’infezione sono l’e-mail (con tecniche di phishing) e gli attacchi “forza bruta” sui servizi Remote Desktop Protocol (RDP) in cui vengono utilizzati algoritmi automatizzati per ricavare le credenziali. Il vantaggio di questo metodo è che i criminali possono accedere alla rete sfruttando credenziali legittime e restando, in tal modo, inosservati.

Le aziende più grandi e strutturate monitorano questo tipo di attività ma la maggior parte di quelle piccole e medie non lo fa. Le possibilità di ricavare credenziali RDP sono legate all’uso di password deboli, mancanza di un sistema di autenticazione a due fattori o dell’adozione di reti VPN sicure per accedere ai servizi remoti.

### **Verso un nuovo modello di business: il Ransomware-as-a-Service**

Il Ransomware-as-a-Service (RaaS) è un servizio che prevede che un’organizzazione criminale metta a disposizione di altri soggetti criminali, in base a un modello di affiliazione, una piattaforma che fornisce tutti gli strumenti necessari per sferare un attacco Ransomware, dalla crittografia dei file, alla loro archiviazione, fino al pagamento. Il fornitore della piattaforma RaaS prende una parte dei pagamenti del riscatto ricevuti dalla vittima, mentre l’affiliato mantiene il controllo dell’azione e delle attività di comunicazione.

Le piattaforme RaaS seguono modalità identiche a quelli di un’azienda legittima, con servizio di assistenza e garanzia di qualità, e si adattano continuamente ai cambiamenti dell’ambiente per non essere rilevate dai computer e dagli strumenti di sicurezza della rete.

Il RaaS ha reso accessibili gli attacchi ransomware a qualsiasi attore malintenzionato, anche privo di conoscenze tecniche e non è un caso che l’attenzione a questi modelli di attacco sia aumentata nel corso del 2021, rendendo difficile la corretta attribuzione ai singoli attori delle minacce. Entrambi le due associazioni criminali che hanno dominato il mercato del ransomware dal punto di vista sia finanziario sia del volume di infezioni, Conti (ricavi finanziari di 12,7 milioni di dollari nel 2020) e REvil (12 milioni di dollari), forniscono piattaforme di RaaS.

Un’ulteriore tendenza negli attacchi ransomware più elaborati è anche il reclutamento attivo di dipendenti dell’azienda bersaglio per ottenere assistenza durante l’attacco. Nell’agosto 2020, un cittadino russo dipendente di Tesla è stato condannato per aver preso attivamente parte a un attacco Ransomware.

## Il livello di estorsione raddoppia

Il Rapporto ETL evidenzia come nel 2020 un tema comune negli attacchi Ransomware sia stato il doppio livello di estorsione. Questo tipo di attacco combina la tradizionale cifratura dei file sulla rete e sui sistemi della vittima, nonché la sottrazione degli stessi.

I dati sottratti vengono, solitamente, memorizzati e tenuti in ostaggio su un sito di proprietà del gruppo criminale. Mentre le trattative sono in corso, i file restano bloccati e alcune piattaforme RaaS includono persino una funzione timer per indicare il tempo rimasto a una vittima per risolvere il pagamento o negoziare il riscatto.

Di conseguenza, le vittime non sono spinte solo dall'esigenza di recuperare i propri dati ma anche dalla minaccia che la violazione venga rivelata ai propri clienti e partner.

Un ulteriore livello di estensione della minaccia prevede che gli aggressori prendano di mira anche i clienti e/o i partner delle aziende compromesse per ottenere anche da loro un riscatto e massimizzare, così, il profitto.

## L'importo del riscatto aumenta

L'importo medio del riscatto chiesto in un attacco Ransomware è raddoppiato nell'ultimo periodo: la domanda di Ransomware più elevata è passata da 15 milioni di dollari nel 2019 a 30 milioni di dollari nel 2020. L'entità del riscatto richiesta inizialmente rappresenta, spesso, il punto di partenza per una contrattazione che porterà a definire la cifra che sarà effettivamente pagata.

Continuano, in ogni caso, a essere frequenti anche attività rivolte a riscatti di piccola entità che tendono a essere pagati più facilmente e che comportano una minore esposizione pubblica per l'autore della minaccia.

Uno studio di Group-IB (Ransomware Uncovered 2020 – 2021) riporta che nel 2019 il riscatto me-

dio pagato è stato di circa 80mila dollari e che nel 2020 la cifra è salita a 170mila dollari. Secondo lo stesso studio, la media nei primi sei mesi del 2021 è stata di circa 180mila dollari.

La cripto valuta rimane il metodo di pagamento più comune.

## Aumenta anche il costo per le aziende

Durante un attacco ransomware l'obiettivo è spesso l'infrastruttura chiave di un'azienda al fine di paralizzarne l'attività verso i clienti e/o l'operatività interna. Purtroppo, tutte le statistiche indicano che anche il tempo medio di inattività delle organizzazioni è aumentato nell'ultimo anno.

È indiscutibile che un attacco Ransomware che va a buon fine implichi per l'azienda perdite elevate. Questi costi includono l'importo del riscatto, i tempi di inattività, il costo del personale e l'effettiva riparazione operativa e tecnica.

Un sondaggio condotto da Sophos in 30 Paesi (The state of ransomware - 2021) ha mostrato che il costo complessivo del ripristino a seguito di un attacco ransomware è notevolmente aumentato, da oltre 761mila dollari nel 2020 a ben 1,85 milioni nel 2021.

A seguito di un ransomware di successo, oltre ai costi relativi all'incidente, sono state osservate anche ripercussioni sulle opportunità di business e una significativa riduzione delle entrate nel periodo immediatamente successivo all'attacco. ❖



# PRAIM DALLA PARTE DEI CISO

L'azienda, che sviluppa soluzioni software e hardware per la creazione e gestione di postazioni di lavoro evolute, punta su sicurezza a più livelli e formazione

di **Jacopo Bruni**, Marketing Manager di Praim



**N**ell'ambito dell'IT c'è e ci sarà sempre un argomento che non passerà mai di moda né risulterà mai fuori luogo. Si tratta del tema della sicurezza e della protezione dei dati.

Tema caldo, quando più quando meno, e sicuramente tra i più affrontati e controversi in questi ultimi anni nei quali i CISO di tutte le aziende, piccole e grandi, hanno avuto il loro bel daffare.

Ma andiamo per gradi e poniamo delle basi.

- La sicurezza informatica di un'azienda prescinde dalle sue dimensioni e dal suo oggetto sociale. Ogni realtà organizzativa deve dotarsi dei mezzi idonei a proteggere i propri dati.
- Più è grande l'azienda e più grande sarà la perdita, ma solo in valore assoluto. In valore relativo ovviamente è tutta un'altra storia.
- La sicurezza informatica è una questione di livelli, non esiste una soluzione unica per far rilassare i CISO. Spesso l'investimento sulla sicurezza è la voce più alta del budget dell'IT.

Quanto più è grande la realtà aziendale quanto più il rischio di un attacco mirato si fa probabile. Questo non vuol dire che le realtà più piccole sono più al sicuro, ma che è più probabile che ricevano "danni minori" rispetto alle altre. Negli anni si è assistito ad un sostanziale aumento del "livello di

attenzione", anche grazie a campagne di sensibilizzazione fatte da vendor di security e non e da tutto il resto del canale (distributori, rivenditori, vendor, ecc.). Abbiamo anche assistito a una nuova presa di coscienza degli attaccanti, che ormai prediligono attacchi più mirati ma molto più efficaci. Sensibilizzazione, attività e azioni di prevenzione, casi che sono stati più volte oggetto di discussione e alcuni che hanno smosso per bene l'opinione pubblica, tutto questo ha fatto in modo di aumentare significativamente la quantità di investimenti in questo senso. Ma sarà sufficiente?

La domanda sembra ovvia e la risposta, di conseguenza, potrebbe non sorprendere più di tanto. Fatto sta che l'investimento in sicurezza informatica non sarà mai abbastanza e per quanto si possano avere i prodotti migliori o i più blasonati sul mercato, questo può non essere la garanzia del 100% di protezione.

Ecco che a mio avviso sono due le questioni sulle quali porre maggiormente l'accento:

- la sicurezza va attuata su più livelli;
- va tenuto conto che l'essere umano rappresenta un ulteriore livello.

Analizziamo meglio.

Innanzitutto, cosa vuol dire "sicurezza su più livelli"? L'infrastruttura informatica di un'azienda è un sistema complesso di hardware, software, network e storage atto a mettere in grado tutti i collaboratori dell'azienda stessa di lavorare con determinati strumenti. L'infrastruttura può essere di diversi tipi: tradizionale e proprietaria, iperconvergente, in Cloud o IaaS. Negli ultimi due casi, solitamente, l'onere della sicurezza è demandato a un Service Provider. Potrebbe essere la scelta vincente per aziende medio-piccole che scarseggiano di risorse interne per poter gestire il tutto. Negli

altri casi invece, l'onere della sicurezza, è parte integrante dell'infrastruttura stessa.

Nella maggior parte dei casi, comunque, si assiste a infrastrutture di tipo misto, nelle quali comunque un buono e cospicuo investimento in sicurezza sarebbe cosa buona e giusta.

Tornando a occuparci dei livelli, il consiglio è sempre quello di adottare soluzioni differenti e interconnesse che possano proteggere: il perimetro, gli eventuali gateway, i server (in particolar modo quello di posta), l'endpoint e i singoli account, oltre a dotare l'azienda di un ottimo sistema di backup. Tanti vendor sul mercato offrono prodotti di altissima qualità, ormai coadiuvati dalla cosiddetta "machine learning", soluzioni in continua evoluzione e aggiornamento che garantiscono una protezione praticamente infallibile a tutti i livelli infrastrutturali.

Anche le soluzioni di backup si sono evolute esponenzialmente negli ultimi anni, arrivando praticamente all'annullamento di eventuali perdite di dati, grazie a repliche sincrone e sistemi di disaster recovery che possono riabilitare un'infrastruttura danneggiata in pochi minuti.

In sostanza, un buon investimento nelle soluzioni giuste combinate in modo da ottimizzare ogni loro caratteristica è la prima cosa da fare, ma abbiamo anche detto che la persona potrebbe rappresentare, di per sé, uno di questi livelli. In che senso?

Si può anche pensare di avere l'infrastruttura più protetta del mondo, ma non si potrà mai prevedere il comportamento umano. Ed ecco che un qualsiasi collaboratore aziendale, di qualsiasi livello o preparazione, potrebbe trasformarsi nel peggior vettore di infezione di un sistema informatico: cliccando su una mail di phishing, inserendo una chiavetta USB compromessa, inviando involontariamente informazioni sensibili a soggetti non autorizzati o



navigando sul sito sbagliato. Insomma, ci sono tanti modi per cadere in trappola ed è proprio il fattore umano che dona imprevedibilità e un generoso apporto di ansia ai CISO.

Come fare per evitare tutto ciò?

La risposta anche qui sembrerà banale: formazione.

Sensibilizzare tutti i fruitori dell'infrastruttura aziendale, educare alla cybersecurity, fornire delle competenze per poter prevenire determinati disastri. Ecco come fare!

Tutto questo meglio se accompagnato con delle soluzioni complementari a quelle di security e di backup. Soluzioni in grado di "blindare" i dispositivi, creare policy personalizzate per ogni utente, bloccare la lettura di periferiche non sicure e la scrittura su disco, garantire accesso sicuro e veloce a risorse virtuali e remote e gestire tutto questo in modo semplice ed efficiente, senza perdite di tempo e limitando gli investimenti.

Prima da sempre pone basi solide per creare delle postazioni di lavoro efficienti e sicure, dando la possibilità agli amministratori IT di gestire tutte queste postazioni in modo rapido e automatizzato, sia in loco che da remoto, rendendo la vita degli ansiosi CISO un pochino più semplice. ❖

# STAMPA GESTITA PER AZIENDE IN SMART WORKING

La trasformazione digitale spinge tutti i settori dell'economia a una metamorfosi profonda, incalzando anche le aziende più piccole a riformulare i propri processi in chiave digitale per non perdere opportunità di business. Un'efficace strategia di digitalizzazione passa anche dal ridisegno dei flussi documentali che non significa, semplicemente, dematerializzare i documenti ma, invece, inserire le informazioni in un flusso capace di prevederne la migliore forma di "output" (cartacea o digitale) in ogni fase di elaborazione. Va ribadito che la spinta alla digitalizzazione non cancella la necessità di stampa delle imprese. Da questo punto di vista, i servizi di stampa gestita (detti anche Managed Print Services o MPS) possono offrire un valido aiuto fornendo alle aziende non solo una visione unificata dei processi cartacei e digitali, ma anche un modo per ottimizzare la gestione delle informazioni e garantire la continuità operativa anche a chi lavora a distanza.

L'offerta di servizi di stampa gestita è pensata per mantenere l'operatività in modalità anche da remoto garantendo elevata sicurezza e promettendo una riduzione dei costi

## I vantaggi dei Managed Print Services

In alcune attività di business le produzioni cartacee continuano a rivestire una notevole importanza e i costi associati alle infrastrutture di printing rappresentano una voce di spesa capace di assorbire fino al 3% del fatturato.

I servizi di stampa gestita sono nati per aumentare la produttività degli utenti e, contemporaneamente, ottenere una consistente riduzione dei costi associati ai processi documentali e di stampa, attraverso l'eliminazione delle inefficienze e un modello di servizio "tutto incluso" dai costi certi e prevedibili.

Si tratta di inefficienze di varia natura tra cui: l'utilizzo di parchi macchine squilibrati rispetto agli effettivi bisogni degli utenti, l'uso incontrollato del colore, il completo inutilizzo del semplice fronte-retro, il dilagare di flotte multivendor, la difficile gestione delle scorte di consumabili, la scarsa integrazione dei flussi documentali.

Inoltre, una gestione efficiente dei servizi di stampa risponde alle attuali esigenze

indotte dalla pandemia di ridurre gli assembramenti del personale e abilitare lavoro da remoto e in mobilità, grazie alle funzioni di connettività di cui dispongono le stampanti moderne.

## I servizi irrinunciabili

Le offerte di Managed Print Services non sono tutte uguali. I servizi inclusi nei diversi contratti di fornitura possono variare in modo anche molto significativo, garantendo una precisa aderenza alle esigenze aziendali o limitandosi solo ad adattare offerte di tipo standard.

In fase di valutazione è consigliabile, quindi, verificare che il fornitore scelto garantisca la presenza di alcuni servizi che vanno considerati imprescindibili.

Il primo di questi è sicuramente la rilevazione automatica dei contatori, in grado di garantire una fatturazione molto più precisa e veloce rispetto alle letture eseguite di persona.

Fondamentali sono anche le notifiche automatizzate degli errori, che migliorano notevolmente l'utilizzo dei dispositivi,

di Mercedes Oledieu

prevenendone le interruzioni. Importante, poi, la possibilità di ordinare automaticamente toner e tamburi, in modo da rendere più efficiente la gestione delle scorte ed evitare una possibile interruzione dell'attività.

La possibilità di accedere ai rapporti di utilizzo permette, invece, l'ottimizzazione dei dispositivi attraverso l'analisi dei dati raccolti, mentre la disponibilità di portali dedicati a utenti e fornitori di servizi migliora la "customer experience", incrementando i livelli di servizio.

Infine, la possibilità di gestire



da remoto gli aggiornamenti software e le configurazioni riduce significativamente i tempi di risposta dei sistemi, adattandoli più velocemente alle esigenze aziendali.

### **L'importanza della stampa in sicurezza**

Un altro tema essenziale da considerare è quello della sicurezza. La gestione della sicurezza delle informazioni in

azienda spesso si concentra esclusivamente sulle tematiche legate al flusso documentale digitale trascurando gli aspetti legati al mondo della stampa.

Documenti importanti e dati sensibili vengono spesso stampati ed è fondamentale gestire le tematiche di accesso e diffusione di queste informazioni. Si tratta di un'esigenza sempre più sentita,

soprattutto a mano a mano che le aziende si indirizzano verso soluzioni di stampa centralizzata.

Oggi, le soluzioni di stampa sicura esistono ed è solo un atteggiamento incurante che può lasciare scoperto questo rischio. Si tratta, per esempio, di soluzioni di controllo dell'accesso, di monitoraggio dell'attività di stampa per singolo utente e di controllo della produzione fisica della stampa solo quando l'utente si trova in prossimità del dispositivo e si è autenticato digitando un proprio codice. Il presupposto comune di queste soluzioni è che i processi di stampa siano inseriti in un processo di gestione del flusso documentale e affidarsi a servizi esterni di stampa gestita è il modo più semplice per affrontare la questione, evitando di dover predisporre modifiche infrastrutturali e farsi carico di un ulteriore livello di gestione. ❖

### **Le 4 principali vulnerabilità dei sistemi di stampa**

- 1 Stampe abbandonate.** Non è infrequente che la stampa di informazioni confidenziali o sensibili venga lanciata da un ufficio e lasciata sul vassoio della stampante centralizzata per molto tempo, consentendone la visualizzazione o il prelievo, inavvertitamente o intenzionalmente, da parte di persone non autorizzate.
- 2 Dati registrati su hard disk.** In tutti i dispositivi multifunzione dotati di disco fisso i documenti vengono sempre elaborati prima di essere stampati, scansionati, fotocopiati o inviati via fax. Questo passaggio rappresenta un rischio per i possibili attacchi al dispositivo sia quando è ancora in uso sia durante la gestione del suo fine vita, quando i dati archiviati possono essere facilmente recuperati.
- 3 Accesso non autorizzato alle periferiche.** Se le impostazioni delle stampanti e dei multifunzione non sono protette, i lavori in esecuzione sono suscettibili di modifiche e reindirizzamenti, mentre i documenti salvati possono essere addirittura aperti e copiati. Accidentalmente i dispositivi possono, invece, essere completamente resettati, perdendo dati e configurazioni. La loro violazione permette, infine, agli hacker di scaricare copie di documenti scansionati/inviati via email, rubando facilmente le credenziali degli utenti.
- 4 Rischi di network security.** Normalmente le stampe inviate a un dispositivo multifunzione non sono protette sui print server. Questo significa che la coda di stampa può essere copiata in qualsiasi momento, ma soprattutto che un utente esterno può facilmente accedere a informazioni riservate o infettare il dispositivo con un malware. Anche le porte di rete aperte costituiscono un pericolo, consentendo di violare le stampanti da remoto e farle diventare un target privilegiato per attacchi Denial-of-Service. Infine, se i dati inviati ai sistemi di stampa non vengono criptati, può essere facile rubarli.

# SOLUZIONI DI STAMPA CHE SI ADATTANO ALLA NUOVA NORMALITÀ

La crisi innescata dalla pandemia da Covid-19 ha reso necessario un cambiamento repentino nelle modalità di lavoro delle persone e le aziende hanno dovuto ridisegnare gli spazi di lavoro comune oppure hanno adottato lo smart working per rispettare le nuove norme di distanziamento sociale.

La velocità di risposta delle aziende nel riorganizzare le modalità di lavoro ha rappresentato un aspetto fondamentale per sopravvivere alla crisi e preservare la competitività sul mercato. In questo senso la trasformazione digitale delle aziende si è resa ancor più urgente e necessaria, poiché la tecnologia consente di avere gli strumenti necessari per assicurare l'operatività quotidiana in modo efficiente.

Tecnologie come Internet of Things, Big Data, Analytics e smart device hanno permesso di mantenere importanti vantaggi competitivi.

Nel percorso verso la trasformazione digitale un aspetto rilevante è rappresentato an-

Le nuove regole di distanziamento sociale impongono nuove modalità di gestione dell'operatività sia in ufficio sia in smart working. Brother offre soluzioni di stampa che si adattano alle nuove esigenze per non perdere competitività ed efficienza



di Paola Saccardi

che dalla gestione dei flussi documentali, con la necessità di riformulare i tradizionali cicli cartacei e integrarli in nuovi processi digitali.

### I servizi di stampa gestita

Per migliorare l'efficienza dei flussi documentali le aziende possono utilizzare i servizi di stampa gestita, un aspetto utile soprattutto in contesti lavorativi orientati allo smart working.

Parallelamente, l'approccio consolidato dei Managed Print Services consente di ridurre in modo significativo i costi e i rischi tradizionalmente associati alle infrastrutture di printing "non gestite", consentendo alle organizzazioni di sfruttare i benefici associati al modello as-a-service.

Come spiega Brother, a spingere le aziende in questa direzione è soprattutto la promessa di una riduzione

dei costi dei processi documentali e di stampa, attraverso l'eliminazione delle inefficienze: un'operazione, spiega la società, capace di generare risparmi al di sopra del 25%, con punte fino al 40%.

Un esempio di gestione inefficiente potrebbe essere l'utilizzo di parchi macchine squilibrati rispetto agli effettivi bisogni degli utenti, l'uso incontrollato del colore, il completo inutilizzo del semplice fronte-retro, la difficile gestione delle scorte di consumabili, la scarsa integrazione dei flussi documentali e così via. Una moltitudine di punti deboli che i servizi di stampa gestita sono in grado di eliminare, offrendo un servizio "All-inclusive" dai

costi certi e prevedibili. Grazie a software di print management specifici, l'offerta MPS (Managed Print Services) di Brother offre alle aziende un maggiore controllo sui costi, riducendo gli sprechi con quote massime di stampa attribuite in funzione del ruolo degli utenti e l'introduzione di alcune funzionalità specifiche: come quella di Pull Printing, che consente di produrre le stampe solo in presenza di chi le ritira.

Inoltre consente la distribuzione correttamente bilanciata dei dispositivi in base alle effettive esigenze degli utenti e contribuisce a ridurre i costi normalmente associati ai sistemi centralizzati, che per soddisfare tutte le necessità sono spesso sovradimensionati.

Il software di print management invece è in grado di attivare e monitorare le attività di printing che arrivano da tutti gli endpoint, inclusi mobile device come smartphone e tablet.

Brother assicura anche il controllo delle stampe in uscita mediante una soluzione integrata che permette di assegnare ad ogni utente funzioni di stampa differenziate, attivabili attraverso un'autenticazione con PIN o card Nfc, il cui lettore è già integrato nel dispositivo Brother.

Sempre in ambito sicurezza e prevenzione delle violazioni di documenti memorizzati sugli hard disk interni alle periferiche, buona parte dei dispositivi Brother non necessita di dischi fissi per l'esecuzione delle operazioni di stampa. Per impedire,

### PULL PRINTING

Chiamata anche 'Follow-me printing', la funzionalità di Pull Printing permette agli utenti di inviare i documenti a sistemi di stampa condivisi e stabilire, previa autenticazione, quando e cosa stampare. Questo permette di bloccare tutti gli accessi non autorizzati ai singoli dispositivi, di garantire la privacy dei documenti prodotti e di evitare stampe duplicate o non più necessarie, facendo risparmiare quindi su carta e consumabili.





invece, fughe di informazioni, le macchine laser di fascia alta sono tutte dotate delle funzionalità di sicurezza TLS/SSL.

### Soluzioni per nuove modalità di lavoro

Brother ha adattato le proprie stampanti e i multifunzione alle nuove esigenze delle aziende consentendo anche il contenimento dei costi di stampa.

Le caratteristiche di cui sono dotate le rendono flessibili e performanti, con tecnologia di ultima generazione per garantire risultati ottimali anche ai lavoratori in smart working.

La pandemia ha reso necessario modificare anche l'allocazione delle periferiche negli uffici per rispettare meglio le nuove indicazioni di sicurezza e in particolare, in Brother, applicano il processo di Balanced Deployment, una risposta concreta a questa

nuova esigenza.

In pratica grazie all'utilizzo di stampanti A4 compatte e versatili si possono sostituire le stampanti A3 che richiedevano di essere collocate all'interno degli uffici in posizioni perimetrali dove le persone potessero mettersi in coda per ritirare i documenti stampati.

Questa modalità, infatti, potrebbe essere rischiosa perché causa lunghe code e assembramenti tra dipendenti, oltre a non garantire la privacy necessaria. Con il Balanced Deployment, invece, le aziende possono rispettare meglio le normative sanitarie.

Le stampanti A4 sono compatte e collocabili in

### BROTHER PAGINE+

*Pagine+ è l'offerta MPS che Brother ha dedicato in particolare alle piccole e medie imprese. Semplici e flessibili, questi servizi di stampa gestita sono erogati in ambito output (stampanti e dispositivi multifunzione, laser e inkjet, monocromatici e a colori) e proposti al mercato in tre semplici formule. La prima prevede il pagamento di un canone periodico, comprensivo di attività d'installazione, fornitura di consumabili e assistenza tecnica, oltre a un certo numero di pagine comprese stabilito in base ai carichi medi mensili dell'azienda. Le stampe che eccedono questa quota vengono fatturate a parte e pagate in modalità posticipata.*

*La seconda formula, più propriamente "a consumo", prevede le attività d'installazione, la fornitura di consumabili e l'assistenza tecnica, con una fatturazione variabile in funzione dell'effettivo numero di pagine stampate. Di mese in mese il cliente è chiamato, dunque, a corrispondere solo ciò che realmente produce.*

*L'ultima formula, "a consumabile", prevede invece il pagamento di un canone comprensivo delle attività d'installazione e di assistenza tecnica, oltre che della fornitura di un numero predeterminato di toner o cartucce. L'eccedenza viene fatturata a parte su base periodica.*

ogni postazione, su mobiletti o scrivanie, garantendo un maggior distanziamento sociale tra i dipendenti. I dispositivi, essendo nelle immediate vicinanze di chi stampa, evitano code o assembramenti per ritirare il documento. Inoltre, questo significa anche una maggiore produttività dei dipendenti a causa di minori interruzioni dell'attività lavorativa. Brother, inoltre, garantisce che le soluzioni di stampa A4 offrono prestazioni assimilabili a quelle di una stampante A3, ma in dispositivi compatti, robusti e performanti. Le stampe sono di alta qualità e in tempi ridotti. Le funzionalità avanzate sono disponibili anche da dispo-

sitivi smart, servizi di cloud printing e display integrati per una migliore gestione e compatibilità con la rete aziendale.

In pratica, le stampanti Brother soddisfano tutte le esigenze degli uffici moderni grazie alla diversificazione del lavoro, ai punti di scansione dedicati, al numero limitato di persone connesse alla stampante. La tecnologia laser permette inoltre di ridurre il consumo energetico e le emissioni di CO2. Con la modalità eco si riduce il consumo energetico senza perdere la qualità e con la modalità risparmio toner si aumenta la capacità della cartuccia per le stampe di tutti i giorni.

## Le soluzioni per il retail

Per soddisfare le esigenze dei clienti in continuo cambiamento e supportare le aziende in ambito retail in questa sfida quotidiana Brother offre soluzioni che consentono di ottimizzare i processi e i flussi di lavoro. Con il servizio di stampa gestita Pagine+ Brother consente di ottimizzare, monitorare e gestire in modo efficiente le risorse printing in azienda e nei punti vendita. I vantaggi includono: la gestione centralizzata del parco affidata al produttore, visibilità e monitoraggio grazie a un'unica console web, assistenza completa e stampe di qualità.

Grazie alla possibilità di personalizzare le funzionalità dei dispositivi, di utilizzare la tecnologia NFC e di digitalizzare i documenti di vendita e di trasporto, ogni punto vendita può migliorare tutti gli aspetti legati alla sicurezza e alla gestione dei flussi di lavoro.

Per aumentare la visibilità nei punti vendita si possono anche utilizzare le stampanti multifunzione Inkjet A3 che consentono la stampa di grandi formati con colori vivaci e testo nero nitido per

la migliore visibilità.

Un'altra soluzione utile in ambito retail sono le etichettatrici P-touch e le stampanti di etichette con cui è possibile stampare anche codici a barre, segnaletica temporanea, informazioni di scaffale e così via. Le etichette sono pre tagliate e i rotoli consentono di creare etichette continue fino a un metro di lunghezza. Inoltre sono compatibili con pc, Mac e Android, con connessioni USB, Wifi e Bluetooth.

A questi si aggiungono i nuovi modelli di scanner Brother con molte funzionalità e dotati di connettività di rete completa, che consentono a più utenti di acquisire facilmente, memorizzare, recupera-

re, modificare e condividere documenti in una varietà di formati, senza bisogno di un pc. Grazie al sistema anti-inceppamento, all'ampia possibilità di scansione direttamente da touchscreen o dai tasti funzione programmabili, alla flessibilità nella gestione delle tipologie di carta (27-413 g/m<sup>2</sup>), il flusso di lavoro può essere gestito facilmente ottimizzando costi e tempi.

Da tenere presente sempre in ambito retail anche la gamma RJ che fa parte del mix di tecnologie mobile per questo settore. La stampante portatile RJ si integra con i sistemi gestionali aziendali della Centrale, così che ogni punto vendita possa effettua-

re il repricing senza spostare il prodotto dallo scaffale, in tempo reale, eliminando eventuali possibili errori umani e ottimizzando tutto il processo, spesso oneroso in termini di tempi e di personale.

Inoltre grazie alle opzioni di connettività USB, Bluetooth, Wifi, MFi e la compatibilità AirPrint, assieme all'ampia gamma di accessori e funzionalità offrono vantaggi a chi lavora direttamente in campo e ha necessità di stampare in qualsiasi momento della giornata. ❖



# SNOM SEMPRE PIÙ FORTE GRAZIE ALLO SMART WORKING

**C**he risultati state ottenendo in questo periodo così anomalo?

Negli ultimi mesi abbiamo dovuto affrontare alcune sfide: un aumento dei costi di spedizione che sono quasi triplicati e un incremento dei prezzi dei componenti elettronici. Nonostante queste difficoltà il 2021 ha fatto registrare una crescita del 30% a livello globale ed è stato il migliore di sempre per fatturato a livello EMEA: circa il 10% in più rispetto al nostro precedente migliore risultato.

L'Italia si conferma per Snom una delle country più importanti, con un apporto di fatturato secondo solo a quello della Germania.

**Esiste un vostro cliente tipo per dimensione o settore?**

Snom opera esclusivamente tramite Canale, con tre livelli di partnership: registrati, silver e gold.

Questo non ci consente di avere una visibilità dettagliata sui clienti ma, in ogni caso, i nostri telefoni sono utilizzati in aziende di qualsiasi dimensione, dalla micro azienda alle realtà enterprise.

Fabio Albanini, Head of international sales EMEA e Managing directory Italia di Snom, illustra risultati, progetti e strategie della multinazionale tedesca specializzata nella produzione e commercializzazione di telefoni VoIP professionali e aziendali



Fabio Albanini

**Quali sono le ragioni di questa crescita di Snom in Italia e nel mondo?**

L'esigenza, indotta dal lockdown, di dover rivedere rapidamente e completamente le modalità di gestione del business e di organizzazione interna, ha messo in evidenza come molte aziende fossero completamente impreparate e prive di strumenti adeguati a gestire la collaborazione da remoto. L'esigenza di abilitare lo smart working ha evidenziato i limiti, che noi già da molto tempo sottolineiamo, delle soluzioni di centralino tradizionali, facendo capire l'importanza del VoIP e della

unified communication e favorendo, così, la migrazione verso soluzioni tecnologicamente più evolute.

Inoltre, Snom può contare sul fatto di avere alle spalle VTech, l'azienda manifatturiera globale di telefoni cordless che l'ha acquisita nel 2016. Siamo, forse, gli unici fornitori di terminali IP a essere anche produttori dei nostri dispositivi e questo ci consente di avere un controllo totale interno e di minimizzare i tempi necessari per portare sul mercato le ultime novità tecnologiche. In questo frangente, è stato premiante sul mercato italiano il fatto di essere un'a-

di Riccardo Florio

zienda presente sul territorio con personale sia tecnico sia commerciale, per stare vicini ai nostri clienti e supportarli (sempre in lingua italiana) nei tempi e modi che si sono resi necessari. Non a caso, durante la pandemia il nostro organico in Italia è cresciuto sia nell'area tecnica sia in quella commerciale.

***Pensate di ampliare il vostro business verso nuove direzioni?***

Snom resta saldamente ancorata al suo business tradizionale. L'offerta di telefoni IP da tavolo e dei telefoni Dect IP costituisce il 96% del nostro fatturato e non siamo interessati a mercati quali, per esempio, la videoconferenza. Negli ultimi 18 mesi, sia a livello globale sia in Italia, abbiamo assistito a una significativa accelerazione nell'adozione di soluzioni Dect, soprattutto in settori quali gli ospedali, i magazzini

di grandi dimensioni e, in generale, in ogni contesto in cui è necessaria la mobilità. Ritentiamo che questo ritmo di crescita proseguirà per tutto il 2022 e probabilmente anche oltre.

Aver chiuso il 2021 in modo positivo con un fatturato in significativa crescita in Italia e all'estero ci dà nuovo slancio e prevediamo il rilascio di molti nuovi prodotti nel 2022. Puntiamo a essere un unico riferimento per tutti ciò che ruota attorno agli endpoint e, di conseguenza, abbiamo piani di investimento nel settore delle cuffie e degli speaker.

***Quali sono gli ultimi prodotti che avete rilasciato?***

A fine settembre 2021, Snom ha lanciato una nuova gamma di telefoni IP aziendali, la serie D8xx, i cui primi

dispositivi saranno disponibili sul mercato a partire da dicembre 2021.

Dopo oltre 20 anni di esperienza in questo campo, era giunto il momento di ripensare completamente il telefono fisso e le sue funzionalità.

Questa serie nasce, pertanto, con l'obiettivo di trasformare il telefono IP nel centro nevralgico di uno smart office. La serie D8xx prevede un design innovativo che pone massima attenzione alla funzionalità e all'ergonomia. Snom ha collaborato con partner ed esperti di design per sviluppare dispositivi adatti a diversi scenari d'uso, tenendo sempre presenti le esigenze degli utenti.

I nuovi telefoni prevedono tutti un rivestimento antibatterico e si caratterizzano per la presenza di display a

colori IPS di grandi dimensioni, schermo touch screen e la possibilità di ospitare fotocamere rimovibili. Queste caratteristiche rispondono alle richieste di una clientela che è diventata sempre più esigente e che è ora trasversalmente avvezza a utilizzare strumenti di videocomunicazione quali Zoom o Teams.

***Quali sono le direzioni di sviluppo a cui state lavorando?***

Con la serie D8xx ci siamo affacciati per la prima volta al mondo Android, offrendo all'utente la possibilità di scegliere il firmware per operare in ambiente Linux oppure Android.

La qualità dell'audio - oltre alla sicurezza - è, da sempre, un punto di forza delle nostre soluzioni su cui continuiamo a migliorare. Per esempio, tutti i dispositivi della serie D8xx sono dotati di sistema avanzato di soppressione del rumore e di qualità audio HD e alcuni prevedono, persino, un audio a banda ultra larga: una caratteristica che di solito si trova solo negli studi di registrazione. ❖



Telefono IP Snom serie D8xx



**VERTIV™**

**REPORT VERTIV**

## **Archetipi Edge 2.0**

Analisi approfondita delle esigenze di edge computing di diversi settori con relativi casi d'uso

Scarica gratuitamente il report su [Vertiv.com/EdgeArchetypes-IT](https://www.vertiv.com/EdgeArchetypes-IT)

Developed with STL Partners





# Speciale infrastrutture & soluzioni

# DELL TECHNOLOGIES TRASFORMA IL MODO DI UTILIZZARE LA TECNOLOGIA

Con le nuove soluzioni IT as-a-Service (APEX), l'azienda conferma il proprio impegno nel settore delle infrastrutture IT e collabora con partner come Equinix per soddisfare pienamente le esigenze di clienti che devono gestire quantità di dati in rapida e costante crescita

di **Camillo Lucariello**

L'occasione è stata offerta dall'evento Dell Technologies World: Dell Technologies (<https://www.delltechnologies.com/it-it/index.htm>) ha condiviso con clienti, partner e il mercato in generale, le ultime novità e i più recenti sviluppi nella propria offerta di soluzioni e servizi in ambito IT (Information Technology). Un particolare accento è stato posto sull'offerta infrastrutturale aaS, as-a-Service, che in casa Dell è stata identificata con APEX (<https://www.delltechnologies.com/it-it/solutions/apex/index.htm>). Ad oggi, l'offerta APEX comprende: Data Storage Services, Cloud Services, Custom Solutions e APEX Console, che rispettivamente offrono Storage-as-a-Service semplificato; servizi cloud pubblici, privati e in ambienti edge; servizi di pagamento e gestione IT flessibili con, dichiara Dell, la più ampia scelta infrastrutturale del mercato e, infine, gestione centralizzata delle soluzioni stesse. La collaborazione con Equinix (<https://www.equinix.it/>) consente

poi di estendere APEX a siti di co-location e offre ai clienti Dell la possibilità di scegliere dove implementare e scalare i servizi APEX.

## I vantaggi di Dell Technologies APEX

Dell Technologies APEX consente alle aziende che lo scelgono di implementare servizi tecnologici allo stato dell'arte più adatti alle proprie esigenze, mentre il disegno delle architetture e la gestione ottimale dell'infrastruttura è affidata a partner selezionati. In generale, si può dire che APEX fa leva sulle competenze acquisite da Dell Technologies nell'IT as-a-Service, riducendo le tempistiche e le complessità legate all'acquisizione, alla gestione, alla manutenzione e all'assistenza delle infrastrutture IT fisiche. Per i clienti che scelgono l'offerta Dell Technologies APEX vengono messi a disposizione meccanismi per aumentare la scalabilità orizzontale e verticale secondo le proprie necessità. Ad esempio, per utilizzare nuove applicazioni, avviare nuovi progetti e affrontare i cambiamenti nelle esigenze delle rispettive organizzazioni. Il tutto gestito da Dell e attraverso un'unica console.

Il risultato è quello di garantire che le organizza-



zioni possano implementare le risorse IT APEX in 14 giorni ed estenderle in 5 giorni.

Esaminando più nel dettaglio le singole nuove offerte presentate da Dell Technologies APEX - e già anticipate sopra - APEX Storage Services offre ai clienti le più avanzate tecnologie di storage fornite on-premises o all'interno di strutture di co-location, in modalità a blocchi o per file, con abbonamenti annuali o triennali, con capacità che partono da 50 Terabyte a crescere.

APEX Cloud Services offre, attraverso i sottoinsiemi APEX Hybrid Cloud e APEX Private Cloud, risorse di storage, di calcolo e di networking con supporto di applicazioni tradizionali o native cloud. È così possibile supportare workload critici come AI e VDI (Virtual Desktop Infrastructure), con velocità di deployment molto elevate.

Con APEX Custom Solutions viene reso disponibile ai clienti un ampio portfolio infrastrutturale in modalità as-a-Service. Con APEX Flex On Demand e APEX Data Center Utility, poi, i clienti possono usufruire di server, storage, protezione dati e infrastruttura iperconvergente di Dell Technologies, aggiungendo eventuali servizi gestiti e misurazione custom del proprio data center.

APEX Console, infine, offre ai clienti, spiega ancora Dell Technologies, un'esperienza self-service interattiva in cui possono gestire l'intero ciclo di vita APEX. Tramite APEX Console i clienti possono identificare e abbonarsi ai servizi APEX più adatti alle loro esigenze, lasciando a Dell il compito di sintonizzare tecnologia e servizi per offrire risultati ottimali. Console aggiunge anche la possibilità di monitorare e gestire i servizi APEX con suggerimenti pratici e funzioni di analytics predittiva. In questo modo, i clienti sono in grado di verificare, su appositi report di utilizzo e di spesa dei servizi selezionati, la reale rispondenza di questi ultimi alle proprie esigenze, effettuando le eventuali correzioni.

La collaborazione tra Dell Technologies ed Equinix, azienda specializzata in infrastrutture digitali, consente di rendere i servizi APEX disponibili attraverso i Data Center della stessa Equinix. In questo modo, Dell mette a disposizione dei propri clienti ulteriori opzioni per il deployment dell'infrastruttura, mantenendo il controllo dei dati. Dell gestirà l'infrastruttura del data center Equinix selezionato dal cliente, inserendo i costi della co-location all'interno di un'unica fattura. Grazie a questo accordo, i clienti potranno usufruire di servizi APEX con un modello di costi operativi che consentirà loro di pagare solo le risorse realmente implementate e utilizzate, per la massima efficienza ed efficacia del proprio IT.

Dell Technologies attraverso la nuova gamma di servizi APEX offre ai propri clienti tutti gli strumenti utili a realizzare il proprio futuro digitale, attraverso un portfolio, il più ampio e innovativo possibile, di tecnologie e servizi per soddisfare le esigenze più disparate di aziende di ogni dimensione. Il tutto attraverso un ecosistema di partner che rendano l'approccio alla tecnologia un processo semplice, veloce, garantendo la soddisfazione del cliente e il raggiungimento dei suoi obiettivi. ❖

# LENOVO 360: IL PROGRAMMA DI CANALE DEL FUTURO

Il nuovo programma di Canale evolve in linea con la rinnovata strategia di Lenovo che punta sempre più verso soluzioni end to end per guidare la trasformazione digitale

di **Riccardo Florio**

Lo chiama “il Canale del futuro” Cristiano Accolla, Channel leader di Lenovo, il nuovo programma di Canale denominato Lenovo 360 con cui il colosso di origine cinese si appresta a dare nuovo impulso alle modalità di relazione con i propri business partner.

Il nuovo programma evolve in linea con la rinnovata strategia di Lenovo che punta ad ampliare la portata della sua azione nel supportare le aziende verso la trasformazione digitale ed evolvere da azienda globale di dispositivi a leader tecnologico in dispositivi, soluzioni, servizi e software.

La nuova strategia di Lenovo fa leva su tutti i “building block” di cui l’azienda dispone oggi, combinandoli in soluzioni end-to-end e ha già portato

alla riorganizzazione della struttura organizzativa nelle tre business unit:

- Intelligent Devices Group (IDG) focalizzato sullo Smart IoT;
- Infrastructure Solutions Group (ISG) focalizzato su Smart Infrastructure;
- Solutions & Services Group (SSG) focalizzato su Smart Vertical e Servizi.

Una strategia di successo già tangibile nei numeri, con i risultati trimestrali

per il Q2 dell’anno fiscale 2021/2022 del Gruppo (annunciati il 4 novembre 2021) ai massimi storici sia per fatturato – pari a 17,9 miliardi di dollari, con un aumento del 23% su base annua – sia per utile netto in crescita del 65% su base annua a 512 milioni di dollari.

“Lenovo – spiega Accolla – sta passando da una visione di fornitore di prodotti ad azienda capace di erogare soluzioni end to end. Pertanto, i servizi e le soluzioni fanno parte del core business e sono importanti tanto quanto i prodotti. Nel 2021 Lenovo ha sviluppato l’organizzazione di vendita internazionale ISO (International Sales Organization) per sviluppare strategie sinergiche tra le sue business unit, proprio con l’obiettivo di massimizzare il valore sul mercato e semplificare la fornitura di soluzioni. Con il programma Lenovo 360 (che entrerà ufficialmente in vigore a partire dal 2022 N.d.R.) Lenovo si appresta ora a predisporre un ecosistema per il Canale fatto di persone, programmi e tool che consentirà di sfruttare al massimo l’intero portfolio di Lenovo”.

## I fondamenti della strategia di Canale di Lenovo

Accolla conferma che il “commitment” di Lenovo sul Canale è sempre più forte, evidenziando i punti strategici che sono alla base del rapporto con i business partner.



Cristiano Accolla, Channel leader di Lenovo

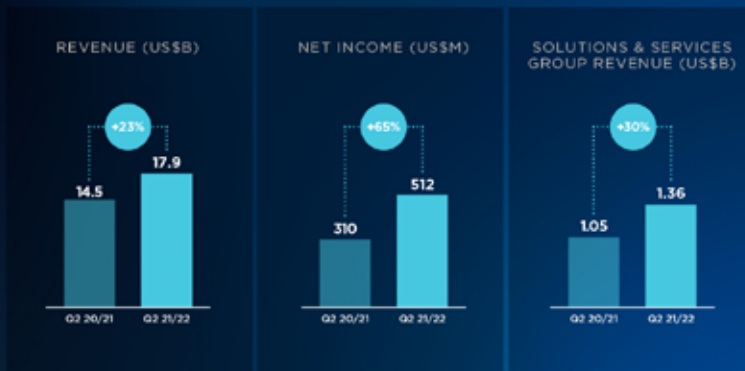
# Q2 FY 2021/22 Key Achievements & Milestones

**Lenovo**

Lenovo's New IT technology architecture of "Client-Edge-Cloud-Network-Intelligence" is gaining momentum and more accepted across the industry. Through the strong execution of our 3S strategy (Smart Devices/IoT, Smart Infrastructure, Smart Vertical), last quarter, both our net income and revenue achieved new records, and we are on track to double our net margin in three years. At the same time, our R&D investment greatly increased by almost 60%. Looking ahead, we will continue to drive to our goal to double R&D spending over three years, and further drive our service-led intelligent transformation.



Yuanqing Yang  
Lenovo Chairman and CEO



Revenue in USD:

**\$17.9B**

Net Income in USD:

**\$512M**

Pre-Tax Income in USD:

**\$742M**

Earnings per Share:

**4.42** US Cents per share

Q2 Fiscal Year 2021/22

**21%**

55G<sup>1</sup> Operating Margin

**+\$24M**

ISG<sup>2</sup> Operating Results Growth YTY

**34%**

IDG<sup>3</sup> Operating Profit Growth YTY

**AA+ Hang Seng Index**

Sustainability Rating Highest Ever

**30%**

55G<sup>1</sup> Revenue Growth YTY

**\$2B**

Record ISG<sup>2</sup> revenue

**\$89M**

Record Smartphone Operating Profit

**1 million tons**

of GHG<sup>4</sup> emissions to be removed from supply chain by FY2025/26

<sup>1</sup>SSG: Solutions & Services Group <sup>2</sup>ISG: Infrastructure Solutions Group <sup>3</sup>IDG: Intelligent Devices Group <sup>4</sup>GHG: Green House Gas

Risultati Lenovo Q2, FY 2021-2022

Il primo presupposto è quello di garantire una costante innovazione attraverso l'incremento continuo degli investimenti in ricerca e sviluppo.

Un'innovazione che contribuirà a mantenere costantemente standard qualitativi di eccellenza per i prodotti e favorire l'individuazione di nuove opportunità di business.

Un altro punto centrale, e non scontato, è ciò che Lenovo definisce "diversity" a sottolineare l'impegno nel promuovere il valore che nasce dalla convergenza di origini, esperienze e punti di vista differenti per affrontare al meglio le nuove sfide di business.

L'attenzione alla customer experience è un ulteriore aspetto fondamentale per poter realizzare soluzioni continuamente migliori e semplici da usare.

Un ultimo pilastro è "trust" ovvero la fiducia nel Canale a cui Lenovo affida la quasi totalità del proprio fatturato con la consapevolezza che, sot-

tolinea Accolla, "Lenovo può crescere solo mediante il Canale e il suo successo resta strettamente legato a quello dei suoi business partner".

## Le fasi di una trasformazione in corso

Il processo di trasformazione del Canale di Lenovo è cominciato da tempo, con una serie di iniziative e progetti costantemente tesi a favorire il lavoro dei partner.

Il primo passo è stato il processo di rafforzamento del Canale, individuando partner adeguati e fidelizzandoli attraverso opportuni programmi di premiazione come il Lenovo Partner Engage Program.

A questo ha fatto seguito un approccio sempre più orientato alla collaborazione con i business part-

ner, che ha prodotto iniziative quali, per esempio, nel 2017 quella denominata Channel 2.0 a livello EMEA e la predisposizione di strumenti quali il Lenovo Bid Portal pensato per consentire ai reseller di ottenere quotazioni particolari per i prodotti del brand.

A metà del 2020 è stata la volta del Lenovo Partner Hub, un portale di servizi personalizzati per la vendita, che ha messo a disposizione un singolo punto di accesso per ogni tipo di informazione, da quelle di prodotto a quelle di marketing.

“Oggi, con il lancio del programma Lenovo 360, che partirà a inizio del 2022 ma di cui si comincia già a vedere alcune novità, siamo giunti alla quarta fase di questi processo evolutivo – sottolinea Accolla – con la predisposizione di un ecosistema di business pensato per il Canale, che consente di proporre al meglio l’intero portfolio di Lenovo e che interpreta il passaggio verso un modello di business focalizzato su soluzioni end to end che abbraccino endpoint, infrastrutture e servizi. Inoltre, attraverso il programma Truscale, l’intero portfolio di Lenovo sarà reso disponibile anche in modalità di servizio.”

Lenovo 360 si presenta come un framework fatto di persone, programmi e strumenti.

Puntare sulle persone per Lenovo significa sfruttare in modo congiunto e coordinato le competenze interne e quelle dei business partner con una gestione unificata dell’intera forza vendita. La direzione è quella di sfruttare tutte le sinergie possibili e di avere un team unico, un obiettivo unico e una strategia unica per pc e componenti infrastrutturali.

Lenovo 360 porterà anche a un’intensificazione dei programmi di formazione, per fare crescere le competenze dei partner e accompagnarli nel

passaggio da un processo di vendita di prodotto a quello di vendita di soluzioni end-to-end, che spostano in alto l’asticella della complessità.

Altrettanto innovativi si prospettano i programmi per i business partner, attualmente in via di definizione, che avranno l’obiettivo di favorire la crescita, la redditività, la customer satisfaction e l’acquisizione di nuovi clienti.

Con Lenovo 360 resteranno invariate le suddivisioni e i requisiti per accreditarsi come partner Silver, Gold e Platinum e sarà consentito a uno stesso partner di disporre di livelli di certificazione differenti in relazione a pc/server oppure ai componenti infrastrutturali.

“Siamo nella fase in cui vogliamo costruire un Canale del futuro – ha concluso Accolla – che apra nuove opportunità per sfruttare i cambiamenti in atto all’interno di Lenovo. Lenovo 360 è il motore che creerà queste opportunità”.

### La strategia delle tre S di Lenovo

“Ci piace descrivere la nostra strategia allineata al contesto della Digital transformation all’insegna di tre S - osserva Alessandro De Bartolo, general manager, Infrastructure Solutions Group di Lenovo -. La prima sta per Smart IoT e riguarda le soluzioni che si collocano alla periferia del cloud. Comprende gli smart device che fanno parte di quella nuvola che si avvicina sempre più a noi: dagli smartphone Motorola, ai notebook, ai ta-

blet, ai dispositivi IoT. È la parte in cui presidiamo le attività di creazione e presentazione del dato. La seconda S è quella della Smart Infrastructure, con le componenti di backend e in cui si realizzano le attività di gestione, elaborazione e trasformazione del dato. La terza S è lo Smart Vertical, in cui le due S precedenti si combinano in modo sinergico per dare vita a soluzioni verticali da portare sul mercato.”

In linea con questa strategia, Lenovo si propone di risolvere i problemi aziendali dei propri clienti attraverso tre percorsi principali.

Il primo è aumentare la proliferazione di dispositivi personali sempre più intelligenti, in base al presupposto che sempre più persone richiederanno dispositivi dedicati e specifici. Lenovo si propone di offrire una gamma completa di dispositivi per ogni segmento, sviluppando nuovi fattori di forma, incorporando la connettività 5G, esplorando la realtà estesa e proponendo nuovi strumenti di collaborazione innovativi.

Il secondo è di fornire soluzioni infrastrutturali di tipo end-to-end per rispondere alle richieste dei clienti che cercano soluzioni integrate che combinino hardware, software, supporto e competenze. Per questa ragione Lenovo

mira a espandere la propria offerta in ogni tipo di ambiente: dai data center on-premise, ai cloud pubblici e privati, alle soluzioni edge to cloud.

“L’investimento di Lenovo in quest’area è molto significativo - precisa De Bartolo - sia attraverso lo sviluppo di tecnologie interne, sia attraverso un approccio aperto all’ecosistema dei leader dell’IT. Abbiamo sviluppato le soluzioni Hyper-scale computing per rispondere alle esigenze dei grandi cloud service provider mondiali e, nel contempo, continuiamo a spingere sulle soluzioni di supercalcolo HPC dove siamo leader mondiali per numero di sistemi installati. All’interno di questi due estremi si collocano le soluzioni che utilizziamo presso le aziende, incluse le PMI italiane. Le soluzioni IoT/Edge ci permettono di uscire all’esterno del data center mentre l’offerta System x fornisce i tasselli per la gestione e l’elaborazione dei dati collocati all’interno dei data center fisici. Infine, tramite la componente ThinkAgile, realizziamo il collegamento tra il data center fisico e la componente cloud per abilitare la creazione di ambienti cloud ibridi, anche attraverso soluzioni sviluppate insieme ai nostri partner tecnologici”. L’ultimo tassello prevede di porre le basi per una trasformazione intelligente puntando a sfruttare la potenza dell’intelligenza artificiale per combinare hardware e servizi e creare soluzioni di smart manufacturing, smart education, smart retail e smart city. ❖



Alessandro De Bartolo, general manager, Infrastructure Solutions Group di Lenovo

# CIE TELEMATICA, SOLUZIONI COMPLETE DI TELECOMUNICAZIONI E NETWORKING

Fondata nel 1994, CIE Telematica adotta un approccio di successo proponendosi come partner che opera a fianco dei clienti per realizzare soluzioni di alto profilo



Luigi Meregalli,  
founder e  
general  
manager di  
Cie Telematica

Molte aziende di carattere commerciale attive sul mercato ICT Italiano si propongono spesso come “box mover”, ossia come semplici venditori di tecnologia preconfezionata, spesso realizzata all'estero. Un approccio molto diverso da quello scelto da CIE Telematica (<https://cietelematica.com/>), che approccia il mercato come un consulente a tutto tondo. «Il valore aggiunto che offriamo ai nostri clienti comprende progettazione, consulenza, supporto tecnico-commerciale pre e post-vendita – spiega Luigi Meregalli, amministratore e fondatore dell'Azienda – per valutare con loro problematiche da risolvere e soluzioni, di networking o di Data Security». La missione per cui CIE Telematica è stata fondata nel lontano 1994 è quella di: «trattare tecnologia per le telecomunicazioni e il networking, sviluppata e prodotta da leader internazionali, introdurla sul mercato

Italiano per renderla disponibile a clientela di fascia medio-alta e professionale». Oggi CIE ha circa 20 collaboratori e un fatturato che si aggira sui 7 milioni di euro: «Proponiamo prodotti e sistemi che integriamo per i nostri clienti». Recentemente, CIE si è arricchita di soluzioni per reti d'accesso, rivolte soprattutto ai carrier e a grandi clienti di livello enterprise, soluzioni che comprendono switch, router ad alta affidabilità e gateway, per «poter fornire servizi di tipo TDM (Time-Division Multiplexing, una tecnologia legacy molto diffusa, ndr) sulle reti a commutazione di pacchetto odierne». I prodotti introdotti nella gamma offerta da CIE Telematica hanno «caratteristiche di robustezza e di funzionalità avanzate, in grado di operare anche in condizioni ambientali estreme. Si tratta quindi di prodotti ruggedized, sia switch che router, router 4G e via dicendo, a cui poi abbiamo aggiunto anche tutta la parte di Data Security». Tra i prodotti compresi in quest'ultima categoria, CIE offre firewall e soluzioni di connettività per l'autenticazione di utenti remoti.

di **Camillo Lucariello**

## Nuovi prodotti e nuovi clienti

«Qualche anno fa – prosegue Meregalli -, abbiamo siglato una partnership con Lenovo, che ci ha dato la possibilità di distribuire terminali, quindi la parte di pc laptop e desktop, a cui si aggiungono server e soluzioni di storage». Inoltre, la partnership con Cisco ha consentito a CIE Telematica di fornire soluzioni di collaboration, basate sulla soluzione WebEx, ottimali per la Dad (Didattica a distanza) scolastica del periodo del lockdown pandemico. «Sono state fornite ai clienti soluzioni interattive particolarmente adatte all'ambiente scolastico e alle sale riunioni virtuali».

La clientela di CIE si può suddividere in 4 aree di mercato particolari: per primi, gli operatori di telecomunicazioni, cosiddetti Tier 1, cioè i più importanti. «Per esempio, aziende del calibro di Telecom o Fastweb, che utilizzano la nostra tecnologia sia su reti d'accesso in rame e su fibra ottica, dedicate a clienti business». Per alcuni clienti, inoltre, CIE ha sviluppato soluzioni di backup su reti 4G, per connettività Vdsl o su fibra.

Un altro segmento di mercato in cui CIE Telematica vanta diversi clienti è quello dei trasporti, con clienti come RFI (Rete Ferroviaria Italiana) e Autostrade per l'Italia, «cui forniamo principalmente soluzioni di networking e telecomunicazioni – conferma Meregalli -. Si tratta di soluzioni spesso di tipo legacy, dato che molti clienti hanno ancora terminali e connessioni su rete TDM, che le nostre soluzioni aiutano a migrare sulla più recente Packet Switching, la commutazione di pacchetto». Un'altra azienda con cui CIE lavora molto in ambito trasporti è Hitachi, fornitore di dispositivi per il segnalamento ferroviario e su metropolitane. «Le nostre soluzioni di networking e teleco-

municazioni sono utilizzate anche da Leonardo, azienda di Finmeccanica», aggiunge Meregalli, soprattutto in ambito aeroportuale (controllo del traffico aereo). Sempre con Leonardo sono in corso studi per progetti legati alle smart city, come l'impiego di sensori IoT (Internet-of-Things) e gateway in tecnologia LoRa (Long Range), molto diffusa per la connessione di sensori intelligenti. Un terzo segmento in cui è attiva CIE è quello della System Integration, con clienti del calibro di Siemens, per esempio.

Infine, il quarto e ultimo segmento è quello dedicato alle Utility. «Tutte le società che forniscono luce, gas, acqua e che hanno bisogno di soluzioni di telecomunicazioni, networking, security e IT in generale. Molti si sono già dotati di contatori intelligenti, per esempio, che impiegano tecnologie LoRa o SIM cellulari e reti APN per collegare i contatori alle centrali».

E nel prossimo futuro? «Analizzando i dati del periodo pandemico più intenso, abbiamo visto un notevole aumento dell'eCommerce – conclude Meregalli -. Per questo, abbiamo appena avviato il nostro sito online dedicato appunto al commercio elettronico. Pensiamo di veicolare su questo canale soprattutto i prodotti Lenovo, oltre ad adattatori ottici, switch e router che siano abbastanza semplici da utilizzare». Infine, anche dal punto di vista dei servizi ci sarà una importante evoluzione, «che in parte è già cominciata, a causa del lockdown che ci ha costretti a rivedere le modalità di erogazione dei corsi di formazione e di assistenza tecnica ai clienti. Abbiamo implementato dei tool, che utilizzeremo sempre di più in futuro, che ci consentono di fare la diagnostica a distanza dell'installazione del cliente, consentendoci, quando necessario, di spedirgli direttamente la parte eventualmente guasta da sostituire e tutta l'assistenza remota necessaria». Una strategia che sicuramente porterà CIE Telematica a continuare a crescere anche nel prossimo futuro. ❖

# MODELLI STANDARD PER LE INFRASTRUTTURE EDGE

Vertiv propone una categorizzazione dell'infrastruttura Edge in 4 modelli pronti per l'implementazione

di Mercedes Oledieu

Il mercato dei data center, originariamente orientato verso il computing centralizzato, oggi si sta muovendo verso l'edge computing. Quest'ultimo si riferisce all'elaborazione e all'archiviazione che si trovano tra data center centralizzati e utenti finali, dispositivi o fonti di dati.

I vantaggi dell'edge computing sono molteplici, permette di sostituirsi al cloud e ai data center centrali riducendo la latenza e il costoso trasferimento di grandi volumi di dati su lunghe distanze. D'altro canto, l'edge computing è anche un fattore trainante per l'adozione del cloud. Un sito Edge può fungere da area di raggruppamento per i dati che alla fine vengono inviati al cloud per l'elaborazione, l'archiviazione o l'analisi a lungo termine. Negli ultimi due anni, l'adozione dell'edge computing è aumentata significativamente, di pari passo con la continua crescita del cloud.

Secondo una recente indagine condotta da STL Partners, il 49% delle aziende sta considerando attivamente l'edge computing e si stima che il numero totale di siti Edge crescerà del 226% entro il 2025. Tuttavia, per adottare questa modalità di calcolo, le infrastrutture fisiche devono essere progettate e implementate correttamente. Per questo motivo cresce l'esigenza di modelli infrastrutturali in grado di standardizzare design e apparati al fine di aumentarne l'efficienza riducendo i tempi e costi di implementazione.

Scegliere la giusta infrastruttura fisica è ancora



più importante quando si tratta di Edge, dato che molte implementazioni si trovano in luoghi in cui sono necessari un supporto e una protezione aggiuntivi. Questi fattori creano difficoltà per il 49% delle aziende che considerano l'implementazione dell'edge computing. Esse devono prendere decisioni su come utilizzare al meglio l'infrastruttura esistente e dove investire oggi per sostenere le esigenze di domani.

## I quattro modelli di infrastruttura Edge

Per questo motivo Vertiv ha sviluppato un framework innovativo per categorizzare l'infrastruttura Edge in modelli specifici al fine di aiutare le organizzazioni a prendere decisioni pratiche sull'implementazione dell'infrastruttura fisica e dell'elaborazione a livello di Edge.

Il recente report "Archetipi Edge 2.0" parte dalla categorizzazione dei casi d'uso Edge individuati nella ricerca condotta e pubblicata da Vertiv nel 2018 e fa compiere a tali archetipi un ulteriore passo verso la definizione di quattro modelli di infrastruttura Edge distinti, grazie ad una valutazione più dettagliata e pratica delle esigenze di edge computing di diversi settori.

Questa operazione avviene attraverso fattori quali: posizione e ambiente esterno, numero di rack, requisiti di alimentazione e disponibilità, localizzazione del sito, infrastruttura passiva, provider e numero di siti da implementare.

I quattro modelli di infrastruttura Edge individuati sono:

- **Device Edge:** l'elaborazione dei dati avviene sui dispositivi stessi, siano essi device stand-alone o integrati in architetture più ampie, come nel caso dei semafori intelligenti o dei sistemi di videosorveglianza.
- **Micro Edge:** si tratta di una soluzione stand-alone di dimensioni ridotte, che può variare da uno o due server fino a quattro rack. Potrebbe essere implementata all'interno di una organizzazione per creare piccoli data center distribuiti o presso un sito di telecomunicazioni per connettere processi e applicazioni che risiedono negli armadi di rete.
- **Distributed Edge Data Center:** possono trovarsi all'interno di un data center on-premise (che può essere un data center aziendale preesistente, una network room o una nuova struttura indipendente), oppure risiedere presso un co-locator. I data center Edge distribuiti sono già diffusi nei siti produttivi, nelle strutture sanitarie, nelle smart city e nelle reti di telecomunicazione.

- **Regional Edge Data Center:** sono strutture distanti dal data center principale, realizzate appositamente per ospitare una infrastruttura di elaborazione dati. Condividono molte funzionalità tipiche dei data center hyperscale, ad esempio in termini di condizionamento e sicurezza, per cui garantisce elevati livelli di affidabilità. Questo modello è ampiamente diffuso nel mondo del Retail e funge da sito intermedio per l'elaborazione dei dati.

Per concludere, il modello di infrastruttura Edge definito in questo report, realizzato in collaborazione con la società di analisi STL Partners, può aiutare le aziende a navigare nella gamma di soluzioni Edge disponibili e fornire indicazioni sulle scelte di infrastruttura appropriate e l'adozione dei quattro modelli consente di velocizzare l'implementazione di questi siti, accelerando il processo di go-to-market di prodotti e servizi.

Il report "Archetipi Edge 2.0" è disponibile gratuitamente su [Vertiv.com/EdgeArchetypes-IT](http://Vertiv.com/EdgeArchetypes-IT) ❖

I 4 modelli di infrastruttura Edge pronti per l'implementazione sviluppati da Vertiv



Device Edge	Micro Edge	Data center Edge distribuito	Data center Edge regionale
<ul style="list-style-type: none"> <li>• Su dispositivo</li> <li>• Da collegare o integrato</li> <li>• All'esterno (ad es. lampioni) o all'interno (ad es. attrezzature di produzione)</li> </ul>	<ul style="list-style-type: none"> <li>• Numero ridotto di server o rack</li> <li>• 0-4 rack</li> <li>• Presso il sito aziendale (ad es. punto vendita, fabbrica, armadio IT)</li> </ul>	<ul style="list-style-type: none"> <li>• Piccolo data center</li> <li>• 5-20 rack</li> <li>• Sito aziendale (ad es. magazzino), sito di telecomunicazione, parcheggi</li> </ul>	<ul style="list-style-type: none"> <li>• Data center di medie dimensioni</li> <li>• Oltre 20 rack</li> <li>• Sede regionale</li> </ul>

snom

# Perfette per ogni esigenza: le soluzioni IP di Snom

Che tu lavori da casa o dall'ufficio - le soluzioni per la telefonia IP di Snom soddisfano tutte le tue esigenze. Usando il tuo telefono aziendale anche a casa benefici di una comunicazione impeccabile in entrambe le due sedi lavorative. Approfitta ora della tecnologia flessibile, innovativa, conveniente e sicura di Snom, lo specialista della telefonia IP.

M80



M90



D785



C52 SP



D385



A190



A170

