

# DIRECTION

Reportage

LA DIGITAL ECONOMY AL SUPPORTO DEL BUSINESS

Distribuito gratuitamente con "Il Sole 24 Ore"



**Reagire e ripartire col digitale**

# OAD 2020

L'iniziativa OAD, Osservatorio Attacchi Digitali in Italia, con il 2020 è alla 12° edizione, con 12 anni consecutivi di indagini sugli attacchi digitali intenzionali ad aziende ed enti pubblici in Italia.

OAD è l'unica iniziativa in Italia per l'analisi sugli attacchi, realizzata tramite una indagine anonima con un questionario compilabile on line, indirizzata a tutte le aziende e alle Pubbliche Amministrazioni di ogni settore merceologico e dimensione. OAD collabora con la Polizia Postale e delle Comunicazioni, che fornisce significativi dati sugli attacchi digitali che costituiscono crimini informatici. Obiettivo principale di OAD è fornire reali e concrete indicazioni sugli attacchi ai sistemi informatici che possano essere di riferimento nazionale, autorevole e indipendente, per la sicurezza ICT in Italia e per l'analisi dei rischi ICT. La disponibilità di dati "locali all'Italia" sugli attacchi digitali intenzionali rilevati, sulla tipologia e sull'ampiezza del fenomeno è fondamentale anche per le organizzazioni di piccole e piccolissime dimensioni per valutare i possibili rischi e attivare le misure più idonee di prevenzione e protezione, così come richiesto da numerose normative nazionali ed internazionali, non ultimo il GDPR, il regolamento europeo sulla privacy. OAD, con la sua indagine e con lo stretto supporto di AIPSI, Associazione Italiana Professionisti Sicurezza Digitale (Capitolo italiano della mondiale ISSA), intende inoltre contribuire alla sensibilizzazione e alla consapevolezza, in Italia, sulla sicurezza digitale del personale a tutti i livelli, dai decisori di vertice agli utenti. Quest'ultimo obiettivo è particolarmente importante per creare una più diffusa cultura in materia di sicurezza digitale, che va oltre il mondo tecnico-informatico e toc-

ca anche i vertici dell'organizzazione e tutti coloro che decidono requisiti e budget della sicurezza digitale nei processi organizzativi delle proprie strutture.

Per la prima volta nell'edizione 2020, chi completa il questionario on line avrà anche in tempo reale una valutazione di sintesi di come le misure di sicurezza digitale indicate rispondano effettivamente alle esigenze di sicurezza digitale indicate per l'azienda/ente ed il suo sistema informatico: una macro valutazione qualitativa (e gratuita) del livello di sicurezza digitale del sistema informatico oggetto delle risposte fornite provè nel rispondere al questionario.

Per motivare il rispondente, a conclusione delle risposte fornite al questionario on line, oltre alla valutazione di cui sopra, è possibile scaricare gratuitamente il numero di maggio 2020 di ISSA Journal, la rivista mensile riservata ai soci AIPSI-ISSA, che tratta la crittografia quantistica, e l'intero volume "Information Security e Data Protection", pubblicato da Reportec, che è anche Publisher e Media Partner per OAD.

Il Rapporto finale di OAD 2020 è previsto per fine novembre 2020, e sarà scaricabile gratuitamente da parte di tutti gli interessati. Più compilazioni del questionario si avranno, provenienti dai vari settori merceologici e dalle Pubbliche Amministrazioni Centrali e Locali, più analitico, dettagliato, accurato e autorevole potrà essere il rapporto finale.

*Si prega pertanto il lettore di questa nota di compilare, o di far compilare dai suoi tecnici, il questionario on line disponibile alla pagina: <https://www.oadweb.it/lime-survey2020/index.php/574592?lang=it>*



## 4 LA PANDEMIA COVID NON DEVE ABBATTERE LE AZIENDE E I LAVORATORI

6 Pollo e uova di Salvador Dalì 1931, particolare

8 Lavorare in ufficio e in sicurezza nonostante il Covid-19

10 L'UCC as a service si diffonde in Europa

13 Il mondo dei dati è diventato la linfa vitale che supporta ogni business, a patto che sia supportato dalle infrastrutture

14 La gestione efficiente del dato ovunque esso sia

16 Come collaborare da remoto in modo sicuro

18 La sicurezza informatica è costantemente sotto pressione a causa di una vera e propria industrializzazione degli attacchi che colpiscono senza pietà

20 Le best practice per la cyber security

22 Il ruolo dell'Enterprise Mobility nella ripartenza al tempo del Covid-19

24 Rischio sopravvivenza in metà delle aziende italiane

27 Il mercato Industry 2020 si avvia alla chiusura con un aiuto dal digitale

29 Per ottimizzare le telco aziendali serve una consulenza di alto livello

30 La digitalizzazione nel futuro delle PMI del comparto manifatturiero

Direttore responsabile: Gaetano Di Blasio  
In redazione: Giuseppe Saccardi, Gaetano Di Blasio, Paola Saccardi, Edmondo Espa  
Grafica: Aimone Bolliger  
Immagini Dreamstime.com  
Redazione:  
via Marco Aurelio, 8 - 20127 Milano  
Tel 0236580441 - fax 0236580444  
www.reportec.it  
redazione@reportec.it

Direction Reportec • anno XVII • numero 116 - novembre 2020

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

Editore: Reportec Srl, via Marco Aurelio 8,  
20127 Milano

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

Presidente del C.d.A.: Giuseppe Saccardi  
Iscrizione al tribunale di Milano  
n° 212 del 31 marzo 2003  
Diffusione (cartaceo ed elettronico)  
50.000 copie  
Tutti i diritti sono riservati;  
Tutti i marchi sono registrati e di proprietà delle relative società.

# La pandemia Covid non deve abbattere le aziende e i lavoratori





È il momento di rendere più efficienti i processi, sfruttare il tempo "sciolto" dal lockdown per esplorare nuove forme di business basate sul digitale.

Non solo app, ma anche strumenti di realtà aumentata o virtuale, machine learning, industry4.0, IoT, AI

# POLLO E UOVA

di  
Salvador

Dalì

1931

*particolare*





La situazione che il mondo sta vivendo a causa del Covid può apparire surreale, ma affrontandola con coraggio e ricordando quante minacce, pur dolorose si sono superate possiamo guardare a un nuovo rinascimento, guidato dalla rivoluzione digitale in tutti i campi

# Lavorare in ufficio e in sicurezza nonostante il Covid-19

Per chi non può lavorare da casa, Brother ha realizzato soluzioni intelligenti che consentono di abbattere il rischio di contagio da contatto

**N**on occorre ricordare quanto siano diffuse attività che richiedono la carta, come per documenti legali, garanzie o, con il lockdown, le certificazioni che occorre esibire per svolgere alcune attività lavorative o per uscire dal proprio appartamento avendone diritto. Gli esperti di Brother hanno quindi progettato soluzioni che consentono di utilizzare la stampante in ufficio e in sicurezza.

In particolare la soluzione Secure Print+ affronta l'importante problema del contagio da coronavirus attraverso le superfici.

Il virus si diffonde principalmente attraverso il contatto con le goccioline che si espandono propagano tramite il respiro, gli starnuti, la tosse delle persone che lo hanno contratto. Peraltro, secondo le informazioni ufficiali del Ministero della Salute il virus può sopravvivere alcune ore su qualunque superficie, ecco perché è stato consigliato di non toccare con le mani le superfici degli oggetti posti in spazi comuni, come i pannelli delle stampanti. Una soluzione esiste, poiché, spiega in Brother: Secure Print+ consente a ogni dipendente di ritirare i propri lavori di stampa senza dover toccare la stampante. Infatti non occorre digitare sul display, in quanto la soluzione prevede l'utilizzo di una card NFC personale, avvicinando la quale che, se avvicinata al lettore integrato nel dispositivo, consente l'autenticazione e l'avvio della stampa.

Si tratta di una soluzione che garantisce anche la privacy dei documenti, che non rischiano di essere dimenticati o di essere letti da chi passa vicino alla stampante. Si riducono anche le code davanti al dispositivo rispettando il distanziamento sociale.

Va considerato che una parte dei lavoratori, presto o tardi a riprenderà a rientrare, rientrerà in ufficio, dove troverà cambiamenti, a cominciare dal posizionamento delle stampanti, non più situate in un reparto ma dislocate in più punti, per garantire il distanziamento sociale e il rispetto delle norme di sicurezza.

La card NFC è quindi utile anche da questo punto di vista, poiché l'autenticazione tramite tale dispositivo è rapida, semplice e sicura

**brother**  
at your side

**BROTHER È AL TUO FIANCO PER SUPPORTARTI NEL CAMBIAMENTO.**  
Il mondo cambia e con lui cambia anche il modo in cui tutti siamo abituati a vivere e lavorare.

**PRIMA**

ASSENZA DI REGOLE

- ATTESA PROLUNGATA CON CODE
- ASSEMBRAMENTI DI PERSONE
- NESSUNA PRIVACY DEI DOCUMENTI STAMPATI

**ADESSO**

NUOVE NECESSITÀ E NORMATIVE

- RIDUZIONE DEI CONTATTI TRA I COLLEGGHI
- ELIMINAZIONE DEGLI ASSEMBRAMENTI
- RISPETTO DELLE DISTANZE DI SICUREZZA
- RILANCIO DELLA PRODUTTIVITÀ E OTTIMIZZAZIONE DEI COSTI

**LA TECNOLOGIA ADATTA PER RIPARTIRE IN AZIENDA!**

**PRIMA**

STAMPANTE A3 PER UFFICI

**PROBLEMI**

- NO PRIVACY
- ASSEMBRAMENTI
- CODE

**ADESSO**

BALANCED DEPLOYMENT E DECENTRALIZZAZIONE

STAMPANTE A4 COMPATTA PER GRUPPI DI LAVORO

**BENEFICI**

- DISTANZIAMENTO
- AUTONOMIA
- A NORMA DI LEGGE

**LE FUNZIONALITÀ DELLE STAMPANTI A4 OFFRONO DIVERSI VANTAGGI:**

**RISPARMIO DI COSTI E TEMPI**  
ottimizzazione della risorsa

**SICUREZZA DI STAMPA CON SECURE PRINT+**  
a norma GDPR

**FLUSSO DI LAVORO EFFICIENTI**  
processo più snello e veloce senza assembramenti

**ASSISTENZA DIRETTAMENTE DALLA STAMPANTE**  
monitoraggio da remoto dell'equipaggiamento IT

**LE SOLUZIONI BROTHER PER LO SMART WORKING**

**MFL-L1000**  
MFL-L1000 Serie  
MFL-L1000 Serie  
MFL-L1000 Serie  
MFL-L1000 Serie

**MFL-L1000**  
MFL-L1000 Serie  
MFL-L1000 Serie  
MFL-L1000 Serie  
MFL-L1000 Serie

**MFL-L1000**  
MFL-L1000 Serie  
MFL-L1000 Serie  
MFL-L1000 Serie  
MFL-L1000 Serie

**MFL-L1000**  
MFL-L1000 Serie  
MFL-L1000 Serie  
MFL-L1000 Serie  
MFL-L1000 Serie

**MFL-L1000**  
MFL-L1000 Serie  
MFL-L1000 Serie  
MFL-L1000 Serie  
MFL-L1000 Serie

e, inoltre, tranquillizza i dipendenti che non gradiscono di toccare superfici sporche, come sarebbe non devono più toccare il touchscreen della stampante, evitando qualsiasi rischio.

La semplicità è assicurata dal fatto che non è necessario ricordare un PIN o una password spesso composta da numeri, lettere minuscole, maiuscole e caratteri speciali, su un'interfaccia utente e talvolta piccola, con l'inconveniente di commettere errori di digitazione, ma basta avvicinarsi alla stampante con la card. È anche una soluzione flessibile, poiché è possibile creare specifici profili utente che forniscono accesso ad alcune o a tutte le funzioni della stampante.

### **Sicurezza in un Open space**

Come accennato, il ritorno in ufficio dovrà essere accompagnato da una riconfigurazione degli spazi. Un ufficio open space con stampanti A4 posizionate vicino alle postazioni garantisce maggiore sicurezza per i dipendenti grazie a: meno contatti tra colleghi, nessuna possibilità di assembramenti, rispetto delle norme sul distanziamento ed eliminazione delle code. Utilizzando una card NFC si ottiene anche un importante vantaggio per il reparto IT, i cui amministratori devono gestire le operazioni legate alle password, quali cambiare le password o sbloccare gli account; inoltre viene eliminato il rischio che un utente sia spiato quando inserisce la password. D'altro canto le card NFC presentano molti meno rischi, evidenziano gli esperti di Brother. Infatti

non vengono scambiate fra colleghi e difficilmente possono essere duplicate o hackerate.

Gli amministratori IT, invece, possono aggiungere o rimuovere in pochi e semplici passaggi fino ad un massimo di 200 utenti, ciascuno dei quali può essere registrato con il suo profilo distinto.

È, poi possibile abilitare account individuali che danno accesso ad alcune o a tutte le funzioni della stampante.

È altresì possibile impostare un tempo limite massimo entro cui i documenti devono essere stampati e ritirati. Questo limite costituisce un elemento di sicurezza, poiché se i dati rimangono più a lungo del tempo impostato, vengono automaticamente cancellati.

### **Prepararsi al rientro con il balanced deployment**

Tutti questi mesi di smart working per molti hanno rappresentato una novità che ha svelato un nuovo modo lavorare e di collaborare all'interno delle aziende. Grazie a strumenti adeguati, molti professionisti hanno potuto essere produttivi, connessi e digitali.

Nella lista sono comprese anche le stampanti.

In ogni ciclo di vita aziendale il mantenimento di un archivio documentale è sempre stato uno dei processi vitali per le attività di business e amministrative, e anche da remoto le stampanti rappresentano il complemento indispensabile per tutti i professionisti operativi da casa e per i quali i processi di stampa mantengono una valenza chiave.

Quando l'allentamento delle restrizioni lo permetterà molti lavoratori tori rientreranno in ufficio dopo diverso tempo. Per ripartire a pieno regime è però necessario modificare la cultura organizzativa a cui ci si è assuefatti, mettono in guardia in Brother.

La vita in ufficio si adatterà a nuove abitudini, procedure e accorgimenti ideati per tutelare la salute degli impiegati, riducendo la probabilità di altri contagi. In questa fase il document management giocherà un ruolo importante, perché saranno studiate strategie ad hoc volte a mantenere il distanziamento sociale, senza però pregiudicare l'efficienza delle attività aziendali. Una di queste strategie è rappresentata dal balanced deployment, che consiste nel suddividere in modo ottimale e più minuzioso il carico di lavoro all'interno degli uffici, sostituendo le grandi stampanti A3 con più unità in formato A4 compatte, performanti ma soprattutto più vicine alle singole postazioni di lavoro. Così si evitano lunghi percorsi attraverso altre aree, come nel caso degli open space, per andare a recuperare le stampe, evitando le attese. L'aggiunta di scanner è un altro elemento di bilanciamento, perché chi deve fare solo la scansione di un documento non deve necessariamente attendere la conclusione delle stampe dei colleghi e viceversa.

A ciò si aggiunge la decentralizzazione, che consiste nel posizionare più stampanti all'interno dello stesso reparto, sfruttando le scrivanie vuote per il distanziamento degli impiegati. ❁

# L'UCC as a service si diffonde in Europa

di  
Gaetano  
Di Blasio

## Avaya Cloud Office spinge il new normal dell'UCC in cloud

Una nuova soluzione di Unified Communications in cloud byRingcentral di Avaya sarà utilizzabile sul mercato italiano a partire dal prossimo dicembre 2020. Subito a seguire la soluzione sarà disponibile in altri quattro fra i maggiori mercati europei: Austria, Belgio, Germania e Spagna. Vanno anche ricordati quelli di Irlanda e Olanda, attraverso Rig Central. In questo modo Avaya Cloud Office consolida e amplia la propria presenza a livello globale, raggiungendo un totale di dodici paesi dal lancio negli USA, risalente a marzo e altri ne arriveranno. Afferma infatti Massimo Palermo, Country Manager di Avaya Italia: «il lancio di Avaya Cloud Office conferma la nostra volontà di portare l'innovazione del cloud, del software e dei servizi as a service ad una platea sempre più ampia di clienti offrendo una soluzione all-in-one, semplice, che indirizza totalmente i bisogni di comunicazione e collaborazione fondamentali in questo momento critico particolare».

Il manager ha quindi commentato: «Avaya Cloud Office è in grado di offrire la flessibilità e l'agilità che le aziende italiane, soprattutto le piccole e medie imprese, richiedono per assicurare la continuità delle proprie attività in questo particolare contesto storico, ma anche per assecondare il crescente bisogno di lavorare e, guardando in prospettiva, una volta terminata la fase emergenziale, per portare a termine il processo di trasformazione digitale, innovare il proprio modello di business e affrontare le sfide del di quello che sarà il New Normal».

Palermo, inoltre ha evidenziato come, grazie a questa nuova soluzione di Avaya, si aprono nuovi scenari per i 200, attualmente partner che: «potranno ampliare il proprio business e la loro value proposition offrendo un'innovativa ed efficiente soluzione di cloud pubblico». A questo si possono aggiungere le molte potenzialità di integrazione.



Massimo Palermo, Country Manager di Avaya Italia

Oggi è difficile fare previsioni economiche, ma il 2021, tra "rimbalzi e vaccini che sembrano pronti, fa sperare bene.

Un aiuto arriva dal consolidamento dei modelli as a service per rinnovare il

business di chi rivende UCC. Attraverso il cloud si diffondono modelli basati su abbonamenti che garantiscono ricavi ricorrenti.

A questo si possono aggiungere ulteriori servizi d'integrazione che rappresentano un valore aggiunto da fornire al cliente.

Ovviamente, come ammette Palermo ciascuno dei partner Avaya dovrà valutare la propria posizione con il parco clienti, ma il punto di arrivo è ormai segnato.

Avaya Cloud Office, sostengono gli esperti di Avaya, aiuta a ridurre l'incertezza associata alle fluttuazioni economiche grazie a scalabilità, strumenti di migrazione, migliore supporto per i dispositivi, gestione avanzata della telefonia e altre nuove funzionalità.

Una recentissima analisi di Frost & Sullivan del mercato europeo UCaaS rileva che le aziende europee saranno sempre più distribuite geograficamente a fronte di un numero sempre crescente di dipendenti che lavorano in remoto e in mobilità, dell'allargamento della base clienti, dell'aumento dei canali dei rivenditori e dell'espansione delle catene di fornitura in più paesi e regioni. Secondo quanto riferisce Elka Popova, Vice

President - Information & Communications Technologies, Frost & Sullivan che aggiunge: «Questa tendenza guiderà la domanda di modelli flessibili di utilizzo della tecnologia, mobilità e strumenti di collaborazione avanzati. Infatti, l'83% dei responsabili delle decisioni di investimento, che operano all'interno di aziende IT o di telecomunicazioni e che hanno risposto al nostro sondaggio, prevede che entro il 2021 le proprie aziende avranno migrato in cloud gran parte o perfino l'intero carico di lavoro legato alla telefonia aziendale. Avaya Cloud Office offre valore aggiunto alle aziende che desiderano adottare soluzioni cloud flessibili e ricche di funzionalità per garantire la business continuity e migliorare la collaborazione tra i team distribuiti».

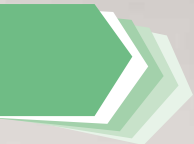
Oltre alle funzioni già disponibili, i clienti di Avaya Cloud Office potranno utilizzare nuove funzionalità, tra cui: una esperienza utente migliorata, un tema di fondo scuro che semplifica la visualizzazione, l'integrazione con Microsoft O365 e i contatti Google, che facilitano la comunicazione e gli aggiornamenti del telefono desktop migliorato. Nuove funzionalità di chiamata:

permetteranno agli utenti di passare da una chiamata vocale a una chiamata audio con un solo clic, rispondere alle chiamate indirizzate ad altri utenti e impostare l'overflow della coda verso gli interni in modo che un numero maggiore di chiamate ricevano una risposta e non siano dirottate alla segreteria telefonica.

Altri miglioramenti riguardano l'esperienza e la sicurezza delle riunioni video.

Gli utenti partecipanti avranno a disposizione i controlli di amministratore, host e moderatore e una protezione attraverso password. Inoltre, i partecipanti al meeting avranno la possibilità di cambiare la visualizzazione della galleria video e scegliere tra uno dei due nuovi layout: Film Strip e Active Speaker.

Con il Covid che ci accompagnerà ancora per un po', l'esperienza delle riunioni è critica. Le funzionalità nuove e i miglioramenti permetteranno di accrescere l'esperienza e la Sicurezza. ❁



# Il mondo dei dati è diventato la linfa vitale che supporta ogni business, a patto che sia supportato dalle infrastrutture

Governo e aziende possono sfruttare questo momento storico per dare una svolta di innovazione per la ripresa



# La gestione efficiente del dato ovunque esso sia

di  
Gaetano  
Di Blasio

Hitachi Vantara unifica la gestione del cloud con un portafoglio di infrastrutture iperconvergenti aggiornato

---

**L'**avvio della quarta rivoluzione industriale (Industry 4.0), attraverso la trasformazione digitale, e le recenti criticità legate al Covid-19 hanno determinato un repentino sviluppo della collaborazione aziendale in ottica distribuita e remota e hanno comportato anche un nuovo approccio interpretativo del business così da condizionarne il modello stesso.

In questo contesto, le aziende hanno la necessità di evolvere le proprie tecnologie informatiche, rendendole sempre più data-oriented e applicando metodologie di memorizzazione ed analisi di grandi quantità di dati con caratteristiche di agilità, efficienza e velocità, e distribuite in ottica hybrid-cloud.

Le imprese hanno però la possibilità di sfruttare questa situazione per rendere più efficienti i processi aziendali e le relative capacità di offerta sui diversi mercati facendo leva sulle tecnologie digitali e grazie alla loro capacità di gestione ed estrazione del valore dai dati.

Hitachi Vantara, azienda consociata del gruppo Hitachi Ltd., si colloca come una delle poche realtà presenti sul mercato in grado di supportare la trasformazione digitale dei propri clienti facendo leva su tecnologie e competenze data-driven che permettono di accelerare la digitalizzazione e la relativa adozione di modelli dinamici edge-to-core-to-cloud.

Tutto ciò è sicuramente frutto delle caratteristiche innovative delle soluzioni Hitachi Vantara, ma anche della capacità di collaborazione all'interno di Hitachi Ltd., gruppo industriale da 95 miliardi di dollari di fatturato con competenze di eccellenza in numerosi e strategici domini industriali. «L'appartenenza al gruppo Hitachi - sottolinea Salvatore Turchetti, Country manager di Hitachi Vantara Italia -, ci consente di raccogliere e capitalizzare le competenze verticali di ogni singolo mercato in cui siamo presenti, toccando con mano le esigenze di innovazione per accelerare la digitalizzazione». Nel 2020 Hitachi Ltd è stata riconosciuta da BGC come una delle 50 aziende più innovative al mondo.

Hitachi Vantara sta continuando ad investire nello sviluppo delle proprie soluzioni e ha recentemente presentato nuove tecnologie che vanno a potenziare il portafoglio di soluzioni infrastrutturali a partire dallo Storage, al Software-Defined, alla Convergenza (CI), all'Iperconvergenza (HCI) che si aggiungono a soluzioni che forniscono la capacità di automazione dell'intero data center. In questi ultimi due ambiti ricade l'evoluzione della piattaforma Hitachi Unified

Compute Platform (UCP). In buona sostanza, si tratta di una soluzione pre-ingegnerizzata che consente di rendere più efficienti i processi operativi del data center mediante l'applicazione di funzioni di automazione. Come ci spiega il Country Manager di Hitachi Vantara Italia: «UCP consente di abbattere il cosiddetto time-to-market riducendo al massimo la distanza fra le esigenze di business e il mondo IT facilitando l'adozione di modelli dinamici per far eseguire i carichi applicativi in maniera ottimale e senza interruzioni tra le piattaforme infrastrutturali indipendentemente che queste siano presso il



Salvatore Turchetti,  
Country manager di  
Hitachi Vantara Italia

proprio data center, sul cloud o in multicloud».

Più nel dettaglio, fra i numerosi vantaggi offerti dalle nuove soluzioni Hitachi Unified Compute Platform spiccano: l'applicazione di tecnologie di automazione ed auto-apprendimento per la gestione delle risorse informatiche ed il loro controllo proattivo, l'integrazione con nuove tecnologie come l'NVMe per il raggiungimento di altissime prestazioni, l'impiego di Kubernetes per la gestione multi-cloud di applicazioni containerizzate.

A corredo dell'offerta tecnologica, Hitachi Vantara offre ai propri clienti un modello di acquisizione flessibile come EverFlex, che consente di spostare gli investimenti aziendali dall'acquisizione del bene al consumo dello stesso in modalità Cloud-like, allineando gli investimenti IT alle nuove esigenze di business.

### Supportare la nuova normalità

Senza dubbio quindi l'adozione di nuovi modelli organizzativi lascerà un segno duraturo su come le persone in tutto il mondo fanno affari e vivono la loro vita quotidiana. Questo significa che ogni azienda deve accelerare il processo di trasformazione digitale per supportare una forza lavoro mobile, con necessità di accedere ad applicazioni e dati in modalità continuativa e distribuita, garantite da una completa resilienza delle applicazioni e quindi delle infrastrutture massimizzando la sicurezza informatica, come

evidenza Turchetti, che aggiunge: «La missione di Hitachi Vantara è quella di supportare l'innovazione e le capacità di crescita dei nostri clienti attraverso soluzioni agili e distribuite tramite le quali è possibile ottimizzare l'impiego delle risorse che queste siano nei Data Center delle aziende o sul Cloud attivando processi di trasformazione, analisi e monetizzazione delle informazioni generate da qualunque tipo di fonte dati. In questi giorni inoltre si è aggiunto un nuovo riconoscimento oltre a quelli delle nostre soluzioni infrastrutturali che il mercato ed i più importanti analisti mondiali ci riconoscono da tanti anni: Gartner ha nominato la piattaforma IoT Lumada di Hitachi leader di mercato grazie alla sua capacità di integrare OT (Operational Technology) e IT completando la nostra visione "From the Edge to the Cloud, to the Core"».

Hitachi supporta la capacità di gestione del dato a tutto tondo: «Poiché è l'unico vero elemento, per le aziende che avranno la capacità di estrarne il valore nel rispetto delle regole di Governance e Compliance, che è e sarà in grado di supportare la crescita delle aziende. Grazie a questa visione e capacità di supportare il mercato, in Italia stiamo crescendo anno su anno a doppia cifra in modo omogeneo sulle varie soluzioni indipendentemente dai settori di business» conclude Salvatore Turchetti. ✨



# Come collaborare da remoto in modo sicuro

di  
Giuseppe  
Saccardi

Lo smart working è uno dei punti chiave per affrontare la pandemia in corso, ma serve la garanzia di farlo in modo sicuro.

Il come lo suggerisce CIE Telematica

---

**N**ello scenario aziendale che si prospetta appare saliente il tema del come lavorare in team quando i partecipanti sono distribuiti su più sedi o in mobilità o presso la propria abitazione, e quali strumenti lo rendono possibile in modo sicuro.

Risolvere il problema dei dispositivi può infatti non essere sufficiente perché entrano in gioco anche altri fattori. Quella degli strumenti adatti, evidenzia Luigi Meregalli, general manager della società di ingegneria CIE Telematica (cietelematica.it), è di certo una condizione sine qua non per procedere, ma puntare solo su quello non basta. Assieme a un buon dispositivo serve anche quanto permette ai sistemi di collaborazione distribuiti di essere sempre operativi, ed esserlo in modo garantito, ed esenti da attacchi da parte di cyber criminali.

Se enunciare un principio è facile, i problemi con cui si scontrano i responsabili IT nel passare alla pratica sono consistenti. In primis c'è il fatto che sovente si dispone di personale di supporto limitato o non ancora formato sugli strumenti utilizzati, e poi la gamma di aspetti che devono essere considerati a corollario, come il garantire la sicurezza remota, l'aggiornamento dei software, la manutenzione, la gestione, la garanzia del funzionamento e cos' via.

Apparati che smettono di funzionare nel mezzo di una conferenza, o una qualità della connessione insufficiente, o il mancato aggiornamento della sicurezza, sono aspetti che possono far perdere i benefici di un'evoluzione che ha permesso di affrontare l'attuale momento di criticità e lasciato intravedere un nuovo modo di lavorare e cooperare.

In pratica, si rischia di far seguire a una fase di entusiasmo una fase di disillusione. Inevitabile o quasi che a quel punto scatti la ricerca del colpevole, che inevitabilmente tende sempre ad essere considerato il responsabile IT, al quale sino a poco prima si negavano le risorse necessarie.

Per superare questi problemi e il fatto che si è spesso restii ad affidarsi ai suggerimenti di un produttore per il timore di incorrere in un lock-in tecnologico, CIE Telematica ha sviluppato una proposta risultante da una analisi terza del mercato che si è concretizzata in un portfolio di prodotti e servizi che ritiene adeguati a rispondere alle sfide che si prospettano.

## Cooperazione flessibile e nel cloud

Cominciando dallo smart working e dalla collaborazione, grazie ad un'accordo con Lenovo, che a sua volta ha in corso una partnership con Microsoft, si è identificato uno strumento adatto per l'ambiente aziendale in Microsoft Teams, una piattaforma che permette di cooperare tramite chat, video meeting, file storage, abilita l'integrazione di applicazioni e che è disponibile in 26 lingue.

Aspetto saliente, osserva Meregalli, è che oltre a connettere in modo efficace gli utilizzatori in diverse modalità è una soluzione integrata anche con Microsoft Office 365 ed è integrato con app e servizi usati quotidianamente quali Word, Excel, PowerPoint, OneNote, SharePoint, Stream e PowerBI.

Semplificato, ha aggiunto Meregalli, e motivo della sua scelta, è anche l'editing simultaneo e in tempo reale con altri utenti di documenti, cosa che permette di evitare invii e reinvi di successive versioni via mail per la loro messa a punto.

## La rilevanza dei servizi di security

Un secondo aspetto a cui porre attenzione è quello della garanzia di funzionamento e di sicurezza della soluzione adottata.

Le criticità derivano da diversi aspetti quali il dispositivo usato dagli utenti finali (aziendale o personale), i rischi connessi ai sistemi operativi dei dispositivi mobili, il malware e il phishing che hanno

come obiettivo i social media e il rischio intrinseco all'utilizzo di software di terze parti.

La soluzione che CIE Telematica ha identificato e suggerisce nell'ambito delle proprie attività di società di ingegneria e in qualità di silver partner di Lenovo, è ThinkShield, uno strumento sviluppato da quest'ultima e che è utilizzabile per proteggere dati, i dispositivi, la identità e le attività on-line.

I servizi di protezione estesa di ThinkShield derivano dalla considerazione che un'azienda non può permettersi di subire violazioni della protezione.

ThinkShield rappresenta sotto questo punto di vista una piattaforma di protezione personalizzabile che ha l'obiettivo di proteggere un'azienda nel suo complesso, dai dispositivi ai dati alle connessioni



Luigi Meregalli, general manager di CIE Telematica

di rete, e dai criminali informatici sempre più agguerriti, anticipandone le mosse e bloccandone in modo preventivo e dinamico gli attacchi.

«Abbiamo verificato sul campo che Thinkshield è uno strumento estremamente efficace per la data security e la protezione dei dati, sia per quanto concerne l'utilizzo che viene fatto di un pc che nelle modalità di accesso ad Internet, con in aggiunta la possibilità di riconoscere reti wifi affidabili a cui connettersi, e dotata di funzioni di autenticazione a più fattori ed encryption», ha evidenziato Meregalli.

Ideato per il supporto e la gestione del personale che lavora da remoto è anche il servizio Premier Support, sottoscrivibile anche per un solo anno, che prevede l'accesso all'help-desk per i prodotti della famiglia Think di Lenovo. Unico requisito è che il dispositivo deve essere coperto dalla garanzia Onsite. Tra quello che prevede vi e anche il supporto hardware e software, un singolo punto di contatto e la reportistica standard sui livelli di servizio.

«CIE, come solution provider, è poi in grado di fornire assistenza nello sviluppo di soluzioni più complesse, non limitandosi solo ai prodotti Lenovo ma aggiungendo altre tecnologie utili a promuovere lo smart working, quali threat prevention su qualsiasi dispositivo (pc, smartphone e cloud), ottimizzazione della banda con soluzioni SD-WAN e strumenti di collaborazione software e hardware», ha evidenziato Meregalli. ❁



# La sicurezza informatica è costantemente sotto pressione a causa di una vera e propria industrializzazione degli attacchi che colpiscono senza pietà

Le dinamiche, le indagini, la situazione, che richiede un atteggiamento 0 trust. In sostanza si tratta di diffidare e comunque controllare sempre prima di fare qualcosa, così come ispira il quadro di De Chirico "Le muse inquietanti"

---



# Le best practice per la cyber security

di  
Giuseppe  
Saccardi

Paolo Lossa, Country Sales Manager di CyberArk Italia, suggerisce i cinque punti critici della cyber security nell'era del Covid-19 e dello smart working

---

**C**i si sta avviando alla fine del 2020, un anno di certo difficile per le aziende, che hanno dovuto ricorrere allo smart working e così facendo a dover rispondere ai problemi intrinseci nel lavoro da remoto, soprattutto nel caso di utenti privilegiati i cui dati sono tra i più ambiti dai criminali cibernetici.

La crisi sanitaria, evidenzia Paolo Lossa, Country Sales Manager di CyberArk Italia ([cyberark.com](http://cyberark.com)), ha influenzato e influenzerà in modo significativo la nostra vita quotidiana e ci ha spinti a un utilizzo sempre più intenso delle tecnologie. È una combinazione di fattori che ha stimolato la creatività dei cyber criminali che hanno sviluppato nuove tecniche di attacco volte a catturare i nostri dati sensibili, la cui vendita sul dark web è molto redditizia.

Cosa suggerisce Lossa a tal proposito? Innanzitutto che gli utenti devono conoscere i rischi informatici in cui potrebbero incorrere al fine di adottare l'approccio più appropriato per proteggere se stessi e i propri dispositivi. Molti aspetti della nostra vita quotidiana possono infatti diventare un punto di accesso per i cyber criminali, ma non tutti ne sono consapevoli.

Cinque i consigli suggeriti da Lossa per incrementare il livello di protezione. Vediamoli in sintesi:

- 1. Non fidarsi degli estranei:** non bisognerebbe mai aprire messaggi o cliccare su link ricevuti da persone che non si conoscono, che si tratti di e-mail, messaggi su Slack, Teams o Google Chat.
- 2. Monitorare la salute va bene, farsi rubare i dati, no:** Fitness tracker e orologi "intelligenti" sono un modo semplice per tenere sotto controllo la propria forma fisica, purtroppo però raccolgono molti dati personali. Chi li utilizza deve quindi assicurarsi di sapere esattamente come vengono utilizzati, archiviati e protetti i dati personali dalle differenti aziende.
- 3. Non raccontare troppo sui social network:** Se questi canali permettono di condividere le passioni e i bei momenti con le persone care, bisogna fare attenzione a non condividere informazioni personali che potrebbero essere utilizzate per determinare password e domande di sicurezza, indicare un luogo o prevedere il comportamento.
- 4. Proteggere lo smartphone.** I cellulari hanno assunto il ruolo di assistente

personale, sia in ambito privato che professionale, ma sono vulnerabili agli attacchi. Pertanto, è importante verificare a quali dati ogni applicazione ha accesso. Inoltre, processi di autenticazione come l'autenticazione a più fattori aiutano a garantire che gli smartphone non vengano sfruttati dagli aggressori per rubare dati personali.

**5. Proteggere l'Internet of Things.** Nei prossimi dieci anni, ogni consumatore avrà almeno 10 dispositivi collegati e, se non sono sicuri, ognuno di essi rappresenterà un modo per rubare dati sensibili. I dispositivi IoT, come le smart TV e i contatori collegati, sono sicuramente utili, ma richiedono molte informazioni e connessioni per funzionare correttamente. Per metterli in sicurezza e chiudere tutti gli accessi alla rete, è necessario fidarsi solo di produttori rinomati, applicare ogni patch di sicurezza disponibile e aggiornare le loro password di default.

«La tecnologia sta entrando sempre più nelle nostre abitudini e gran parte delle nostre attività nel tempo libero, acquisti o operazioni amministrative ora includono la navigazione online. Pertanto, la protezione dei nostri dati personali e la prova della nostra identità saranno al centro di tutto ciò che facciamo fino al 2030. E, chissà, forse il nostro frigorifero connesso saprà più cose su di noi di noi stessi», mette in guardia Lossa.

## La criticità di ambienti SaaS

Le criticità per gli utenti e soprattutto gli utenti privilegiati, sono enfatizzate anche dal fatto che gli attacchi e i rischi continuano a crescere anche in ambienti SaaS considerati sicuri. È con questo dato di fatto che CyberArk ha esaminato la tecnica di intrusione preferita dagli aggressori: il phishing. Si prendano, per esempio, gli attacchi di phishing di Office 365. Negli ultimi mesi si è osservato che questo approccio mira a token temporanei (aka access token) generati per consentire il Single Sign-On per Microsoft 365 e tutte le applicazioni Microsoft.

Rubando e utilizzando questi token temporanei, gli aggressori possono bypassare l'autenticazione multifattore (MFA) e persistere in rete



Paolo Lossa, Country Sales Manager di CyberArk Italia

"legittimamente" aggiornando il token. Inoltre, anche se un utente cambia la propria password, il token rimane valido e non può essere revocato.

Le applicazioni video e chat - come Microsoft Teams, Slack, WebEx, Zoom e Google Hangouts - sono diventate il nuovo volto dell'organizzazione in questo periodo di lavoro a distanza.

All'interno di queste applicazioni SaaS, si possono rubare le credenziali e compromettere le identità digitali dei dipendenti, in particolare di utenti privilegiati, accedere ai dati sensibili inclusi in questi strumenti di collaborazione, report giornalieri e dati finanziari.

A queste problematiche CyberArk ha risposto rendendo disponibili le proprie soluzioni di security tramite Cloud dal Marketplace Microsoft Azure. In pratica, i clienti Microsoft Azure hanno accesso alla soluzione di protezione degli accessi privilegiati di CyberArk e possono fruirne per definire le strategie aziendali

«La soluzione CyberArk Privileged Access Security, offre un approccio esaustivo alla sicurezza e all'efficienza operativa nel cloud attraverso il rilevamento continuo e la protezione degli account privilegiati; funzionalità just-in-time per un accesso flessibile ai sistemi Windows sia in cloud che on-premise, un rilevamento e risposta alle minacce in grado di prioritizzare gli avvisi in base a comportamenti potenzialmente rischiosi, nonché la possibilità di prendere il controllo rapidamente degli account pericolosi», ha spiegato Lossa. ✨

# Il ruolo dell'Enterprise Mobility nella ripartenza al tempo del Covid-19

Per garantire uno smart working efficace le aziende devono mutare l'approccio nella gestione e protezione dei dispositivi mobili. I suggerimenti di MobileIron

**S**ono passati oltre sei mesi da quando è iniziato il lockdown a seguito del Covid-19 e oggi le aziende stanno cercando di riorganizzare le attività e i processi interni. In questo processo che ruolo avrà l'Enterprise Mobility?

Le aziende hanno reagito chiedendo ai dipendenti di lavorare da casa su dati e apparecchiature aziendali con tempistiche molto strette. Devono però rivedere le strategie per la sicurezza e individuare se e quali protocolli siano stati violati. In più le aziende, osserva Riccardo Canetta, Regional Sales Director Mediterranean Area di MobileIron ([www.mobileiron.com](http://www.mobileiron.com)), a cui abbiamo chiesto quali ritiene siano i punti critici e come farvi fronte, devono rispondere a domande come: quali apparecchiature aziendali sono state utilizzate a domicilio e da chi? Quali dati contenevano? Dove si trovano adesso? Quali dipendenti utilizzano i propri dispositivi e quali sono le loro vulnerabilità?

Una forza lavoro più distribuita avrà bisogno di dispositivi ma l'introduzione di nuovi device non gestiti di varia provenienza comporta sfide inedite per l'IT. Un esempio è lo Shadow IT, un problema serio che lo diventa ancor più con le nuove condizioni lavorative.

Le aziende devono in pratica fornire supporto ai dipendenti per i dispositivi che non controllano direttamente, ma in che modo possono farlo?

## Cambiare la gestione IT per migliorare la sicurezza

«La gestione IT deve essere rivoluzionata. Molte tecniche e tecnologie perfezionate dalle aziende negli ultimi 30 anni non saranno più così efficaci. Probabilmente il sistema di prevenzione delle intrusioni non sarà eliminato del tutto ma non sarà più in grado di proteggere le risorse fondamentali o addirittura la maggior parte di esse», sottolinea Canetta.

In sostanza, l'IT dovrà ridefinire le esigenze di mobilità degli utenti. Ciò significa che dovrà conoscere molto bene il settore delle app e offrire soluzioni approvate che permettano di accedere facilmente ai servizi cloud. Inoltre, mettendo a disposizione uno spazio aziendale approvato i team IT saranno in grado di proteggere

i dipendenti e i loro dispositivi, sia personali che aziendali.

«I dispositivi mobile in dotazione ai dipendenti, sia in azienda che a casa, sono già predisposti per rendere questa esperienza ancora più semplice. In molte aziende, l'hardware dei dispositivi consentirà di eliminare password complesse che creavano problemi e rischi per la sicurezza. L'autenticazione mediante tecnologia biometrica integrata li trasformerà in una sorta di ID. I dispositivi mobile utilizzati dai dipendenti diventeranno quindi il principale strumento di autenticazione», evidenzia Canetta.

### Preservare la sicurezza e garantire le prestazioni con il cloud

«In MobileIron, abbiamo vissuto il cambiamento in prima persona perché i nostri clienti si sono rivolti a noi per richiedere assistenza su come accedere alle loro applicazioni e ai loro dati in modo sicuro. Dunque, qual è stato l'effetto del lockdown sulla mobilità aziendale e quali i problemi che vanno affrontati?» osserva Canetta.

Un primo problema che MobileIron ha rilevato è che circa uno su tre dei propri clienti ha chiesto alle persone di accedere alle risorse aziendali dai loro dispositivi personali. Ciò ha però creato problemi di sicurezza perché i dati aziendali e personali tendono a "mischiarsi". Inoltre, le aziende non potevano avere alcun controllo sui dispositivi personali.

«Il nostro software le ha aiutate a risolvere questo problema delimitando aree sicure riservate al

lavoro e controllate dall'azienda sui dispositivi mobili dei dipendenti e preservando la privacy personale di questi ultimi e la sicurezza del datore di lavoro», ha spiegato Canetta. Una volta online, MobileIron ha rilevato che gli attacchi di phishing e di malware connessi al Covid-19 sono aumentati, una criticità che interessa soprattutto gli utenti di device che leggono le e-mail aziendali da questi strumenti con schermi relativamente piccoli.

«Per contenere i rischi abbiamo offerto ai nostri clienti funzionalità di sicurezza per dispositivi mobile che monitorano le attività sospette a livello, rete e applicazione. Inoltre, la nostra tecnologia anti-phishing è stata rinnovata per rilevare e porre rimedio ad attacchi di phishing su tutti i canali pericolosi, tra i quali: messaggi di testo e SMS, messaggi istantanei, social media e altre modalità di comunicazione diverse dalle semplici e-mail aziendali», ha spiegato Canetta.

Le aziende hanno anche dovuto affrontare un altro problema: i colli

di bottiglia nella rete e nelle VPN, che sono di norma configurate in modo da gestire un numero medio di collegamenti.

Le aziende che avevano già migrato le loro applicazioni e i loro dati nel cloud sono state in grado di far fronte all'aumento della domanda della rete in modo più efficiente e si sono adattate con facilità al grande flusso di nuovi lavoratori remoti.

«Le abbiamo aiutate mettendo loro a disposizione il nostro software per collegare in sicurezza i loro dispositivi mobile direttamente al cloud dalle loro posizioni remote senza dover instradare il traffico attraverso le loro reti aziendali. Ciò ha ridotto la pressione sui loro sistemi aziendali», ha spiegato il manager.

In questo mutamento però anche le modalità di accesso devono cambiare. Le password erano già obsolete ma in un mondo che deve convivere con un nuovo coronavirus gli utenti che lavorano da remoto avranno sempre meno voglia di digitare password su una tastiera.

«Occorrono meccanismi di accesso più efficaci che adottino soluzioni più pratiche come i dati biometrici basati sul telefono, l'autenticazione multifattore e gli accessi in base al contesto per semplificare il lavoro da remoto con i dispositivi mobile. Al momento solo il 10% circa delle aziende lo sta facendo. Riteniamo che il restante 90% inizierà a farlo presto. Una cosa è però certa: il posto di lavoro non sarà più lo stesso», ha considerato Canetta.\*



Riccardo Canetta, Regional Sales Director Mediterranean Area di MobileIron

# Rischio sopravvivenza in metà delle aziende italiane

Un 46% dei manager teme i rischi indotti dall'industrializzazione del cyber crime

**L'**impatto economico che il Covid ha determinato s'incrocia con le problematiche di sicurezza che sono tornate prepotentemente sul tavolo dei decisori aziendali. Ciò, in particolare, a causa dell'ampliarsi degli attacchi e, al contempo, delle difficoltà che le società incontrano nell'occuparsi adeguatamente della cybersecurity. Si evidenzia, osservano gli esperti di Bitdefender, che hanno diffuso una nuova indagine sui fenomeni legati alle violazioni dei dati, una superficie d'attacco maggiore, attraverso la quale il cybercrime ha così potuto proliferare nel 2020.

Se risulta difficile per tante aziende integrare i tool e le pratiche per combattere le minacce, ancor più critico è portare in azienda le competenze, sempre più eterogenee, che occorrono per contrastare le attività malevole e sviluppare i processi che migliorano la sicurezza.

Purtroppo, ci svela Denis Cassinerio, Director Regional Sales Director SEUR di Bitdefender: «Sono molti i recenti attacchi, anche sul piano nazionale che hanno mostrato le carenze delle imprese, quali Geox e Carraro oppure Bonfiglioli, cui va il merito dell'aver avvisato il mercato relativamente a come l'attacco subito avrebbe potuto far danni sulla filiera». In tale contesto, pertanto, non stupisce che il 46% delle società italiane coinvolte in un sondaggio da Bitdefender abbia dichiarato di temere per la sopravvivenza della propria azienda.

D'altro canto, rivela ancora il manager: «Gli attaccanti continuano ad attrezzarsi con incredibile velocità, già nella prima parte dell'anno si era notato un evolversi delle minacce ransomware, che maturavano di sette volte, secondo la telemetria di Bitdefender, sfruttando i temi del Covid».

È andato crescendo inoltre, l'uso di tecniche avanzate per entrare nei sistemi della vittima, per esempio cercando e crittografando i backup in modo da impedirne il ripristino e rendere efficaci le richieste di riscatto.

Attacchi di questo genere sono tanti, il che, evidenzia Cassinerio, dà l'idea dell'industrializzazione sviluppatasi con il RaaS ovvero ransomware as a service.



Denis Cassinerio, Regional Sales Director SEUR di Bitdefender

## La Nuova Normalità tra le minacce previste per il 2021

Il report "Business Threat Landscape" realizzato dagli esperti di Bitdefender illustra il quadro delle minacce indirizzate alle aziende, le quali comprendono attacchi alle vulnerabilità, che fanno leva sulle patch mancanti, e la crescita di attacchi noti, alcuni dei quali sempre più condotti anche attraverso la filiera degli MSP (Managed Service Provider). Le imprese avranno l'opportunità di imparare e adattarsi a una nuova normalità in quanto saranno costrette ad affrontare i cambiamenti nel panorama minacce e le molte che saranno riutilizzate, come, per esempio quelle che sfruttano vulnerabilità non risolte. «Configurazioni errate, attacchi mirati commissionati a pagamento, attacchi di tipo 0-day per cui non sono ancora disponibili patch, aumento delle tattiche di esecuzione "stealth" sono solo la punta di un iceberg.

La telemetria di Bitdefender mostra che il 63,63% di tutte le vulnerabilità segnalate e non ancora identificate coinvolge falle di sicurezza note più vecchie del 2018, segnalando che le aziende hanno, potenzialmente, un'ampia superficie di attacco che gli hacker potrebbero sfruttare. Se l'apice delle minacce opportunistiche nel 2020 si è focalizzato intorno alle email di spear-phishing che sfruttavano i temi della pandemia, è probabile che le vulnerabilità non ancora identificate finiranno sotto i riflettori nel 2021.

Quindi le aziende devono adottare rapidamente soluzioni di

mitigazione e patch management che valutano lo stato dei dispositivi in dotazione ai dipendenti, per diminuire la crescente esposizione al rischio di un attacco di tipo cyber.

## Rivalutazione dello stack di sicurezza aziendale

Durante la fase di esecuzione degli attacchi, l'uso di comandi e script PowerShell rimane la sotto-tecnica preferita dai criminali informatici: rappresenta infatti ben il 42,52% di tutte le sotto-tecniche segnalate. Gli hacker prediligono quelle tattiche che si muovono al di sotto delle soglie di rilevazione delle soluzioni di sicurezza tradizionali, perciò è probabile che le aziende dovranno rivalutare il loro stack di sicurezza per il 2021 e includere soluzioni efficaci che non si limitino a fornire funzionalità antimalware.

## Contro misure per gli hacker APT "in affitto" - Focus sulle PMI

Uno dei più grandi cambiamenti nel panorama internazionale delle minacce riguarda la comparsa di hacker APT "in affitto", che ha costretto le aziende di tutte le dimensioni e settori a rivalutare le minacce che si trovano ad affrontare. Mentre gli attacchi APT tradizionali erano rivolti contro enti governativi e settori industriali specifici, oggi gli attacchi in stile APT da parte di hacker mercenari cambiano totalmente il paradigma della sicurezza per ogni azienda. Nel caso delle PMI, che sono maggioranza in Italia, sottolinea Cassinerio, le aziende devono cambiare l'approccio con cui disegnano i

modelli di minaccia. Finora, per la maggior parte, le violazioni APT, facevano parte degli attacchi alla filiera, ma, spiegano in Bitdefender, ora, questa nuova dinamica potrebbe significare attacchi continui, con la conseguenza del dover alzare il livello di sicurezza con strumenti di visibilità sia a livello di endpoint che di rete. Per esempio, gli strumenti di rilevamento automatico a livello endpoint e di risposta che mettono in evidenza gli avvisi di sicurezza pertinenti, indicativi di una tattica o di una tecnica comunemente utilizzata dai gruppi APT, potrebbero facilmente segnalare potenziali intrusi. Inoltre, la mancanza di personale di sicurezza qualificato potrebbe essere affrontata rivolgendosi a team di rilevamento e risposta gestiti o come team specializzato per la ricerca di minacce su eventi sospetti. Questi servizi, che includono gli stack tecnologici necessari di tipo Endpoint Detection and Response (EDR), prendono il nome di Managed Detection and Response (MDR). Sia le soluzioni EDR che MDR sono diventate accessibili alle piccole e medie imprese, offrendo una sicurezza di tipo SOC che solo le grandi aziende possono normalmente permettersi, ma a una frazione del costo e con il beneficio di una partnership efficiente e specializzata.

## La cyber war è una minaccia per il 71% dei Ciso secondo Bitdefender

Uno studio di Bitdefender, che ha coinvolto anche manager italiani, evidenzia la crescita di nuove minacce ransomware, problemi

di comunicazione e mancanza di competenze.

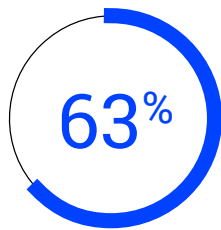
Una serie di problemi che vanno affrontati e che imporranno importanti cambiamenti nei prossimi mesi e anni.

Il 63% dei professionisti della sicurezza informatica a livello mondiale (47% in Italia) tra cui un 71% di Ciso nel mondo, ritiene che la guerra informatica sia una minaccia per la loro azienda, peraltro, solo il 22% degli esperti nel mondo e il 32% degli italiani) ammette di non avere una strategia in atto per mitigare questo rischio.

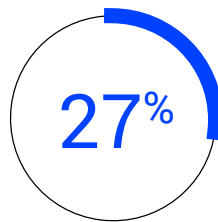
Ciò è allarmante in un periodo di sconvolgimento globale senza precedenti, affermano i manager di BitDefender poiché la metà dei professionisti della sicurezza informatica (dato globale 50% ma in Italia il 53%) concorda sul fatto che l'inasprimento di una guerra informatica danneggerà l'economia nei prossimi 12 mesi.

I CISO e i professionisti della sicurezza informatica stanno comunque rafforzando le loro difese - come sostengono il 48% dei rispondenti a livello mondiale e del 43% in Italia.

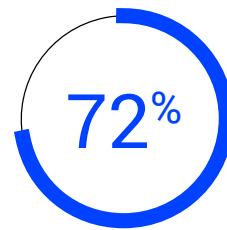
Questi e altri risultati sono raccolti nello studio internazionale "10 in 10" di Bitdefender.



believe that the **state of cyberwarfare** is a threat to their organisation



of companies **don't have a strategy** to protect against cyberwarfare



believe that there is a **need for a more diverse skill set** in cybersecurity



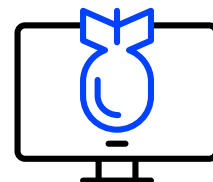
28%

CISOs and CIOs



22%

infosec professionals



50%

believe that the skills gap will be seriously disruptive



38%

Reputational damage



36%

Increased downtime and business continuity disruptions



35%

The personal impact on people (customers, staff, vendors)



33%

Loss of revenue



30%

Increased cost of cyber insurance



29%

Paying to have the ransomware deactivated



27%

Legal fines and penalties



0%

Other



3%

Don't know

## La metodologia dello studio

In particolare ha preso in considerazione i punti di vista e le opinioni di oltre 6.700 professionisti del settore, tra cui CISO, CSO e CIO, in diversi Paesi: Regno Unito, Stati Uniti, Australia/ Nuova Zelanda, Germania, Francia, Italia, Spagna, Danimarca e Svezia. Gli intervistati rappresentano un ampio spaccato di aziende che vanno dalle PMI fino a imprese quotate in borsa con 10.000 e oltre dipendenti in un'ampia varietà di settori, tra cui quello finanziario, governativo, sanitario e della tecnologia.



# Il mercato Industry 2020 si avvia alla chiusura con un aiuto dal digitale

**C**on il 2020 che si avvia alla chiusura in una situazione pandemica tornata critica viene da chiedersi con quali numeri e andamento potrà chiudere il mercato dell'Industry. Una indicazione viene dal Politecnico di Milano, che ha prima analizzato il consuntivo per l'Italia del 2019 come punto di partenza per meglio comprendere l'andamento in corso.

In sostanza, dalle analisi emergeva che nel 2019 il mercato dell'Industria 4.0 in Italia aveva raggiunto un valore di 3,9 miliardi di euro, in crescita del 22% rispetto all'anno precedente e praticamente triplicatosi in 4 anni.

Di questa consistente cifra 2,3 miliardi di euro, il 60%, è stato dedicato a progetti di connettività e acquisizione dati (Industrial IoT), cifra suddivisa a sua volta tra Analytics (630 milioni), Cloud Manufacturing (325 milioni), Advanced Automation (190 milioni), Additive Manufacturing (85 milioni) e tecnologie di interfaccia uomo-macchina avanzate (55 milioni). A questo vanno poi aggiunte le attività di consulenza e formazione per progetti Industria 4.0: pari a circa 255 milioni di euro, con un +17% rispetto al 2018.

Per il 2020, originariamente si prevedeva una crescita in linea con il trend 2019, con un incremento compreso tra il 20 e il 25%. Poi è scoppiata la pandemia di Covid-19 e quello che si prospetta è uno scenario di grande incertezza, le cui previsioni,

**Nel mercato dell'Industry, il 60% è relativo all'Industrial IoT, il 16% all'Industrial Analytics e quasi il 10% al Cloud Manufacturing con una media di 4,5 applicazioni per azienda**



legate all'effettivo superamento dell'emergenza, alla ripartenza della domanda e ai possibili stimoli agli investimenti, variano da uno scenario ottimistico di chiusura dell'anno quasi in linea con il budget iniziale a uno pessimistico di contrazione del fatturato 4.0 nell'ordine del 5-10%. Nel medio-lungo termine il sentimento verso l'industria 4.0 rimane comunque positivo, rafforzato dalla considerazione che l'emergenza abbia accelerato la trasformazione digitale.

### Cloud e analitiche per la supply chain

Sempre nel 2019 sono incrementate le applicazioni 4.0. Il 40% ha investito più del 2018 e in media oggi se ne contano 4,5 per azienda, con una forte accelerazione in soluzioni cloud e analytics per la supply chain, oltre che IoT per le fabbriche, mentre si evidenziano le prime applicazioni di Artificial Intelligence. Ad oggi, riporta l'analisi condotta, quasi un terzo delle aziende sta riconvertendo la sua produzione o sta valutando di farlo e per il 25% di queste sono considerate fondamentali tecnologie 4.0 come l'IoT e cloud.

Il futuro e la chiusura del 2020 sono tuttavia incerti e nel complesso degli ultimi mesi e per la fine dell'anno e oltre gli investimenti si preannunciano ridotti. Indicativamente, oltre un quarto delle aziende posporrà almeno metà di quelli originariamente pianificati e circa un quarto si concentrerà su Industrial-IoT, Analytics e Advanced HMI.

Nell'incertezza, le imprese auspicano incentivi per non fermare la

“scalata digitale”, in particolare una riduzione delle imposte sui prossimi esercizi contabili e una diminuzione del costo del lavoro per operatori di fabbrica.

Un terzo gradirebbe anche, osserva la ricerca, di rilanciare il Super e Iper ammortamento per beni strumentali, di gran lunga più desiderato rispetto al credito d'imposta per ricerca e sviluppo, agli incentivi per beni immateriali o a quelli per assunzione e formazione.

### Il ruolo del digitale nel far fronte alla pandemia

Così come a livello di aziende e uffici, oltre all'adozione di pratiche di smart working per il personale indiretto, nell'emergenza sanitaria le tecnologie digitali sono diventate strumenti per reagire alla crisi. Peraltro, aiutano anche a comprendere le direzioni dell'Industria 4.0 in quella che si prospetta essere la nuova normalità.

Le tecnologie IoT permetteranno infatti di migliorare il distanziamento sociale nei luoghi di lavoro, localizzando e tracciando i percorsi, oppure utilizzando veicoli a guida autonoma nella logistica interna. Per esempio, modelli e simulazioni attraverso dati in real time permetteranno di realizzare analisi per rispondere all'incertezza. Piattaforme di teleconferenza consentiranno la gestione da remoto di riunioni, trattative commerciali, revisioni e collaudi. Piattaforme di design collaborativo, simulazioni di processo si diffonderanno nello sviluppo prodotto. Soluzioni di Advanced Human Machine Interface, di virtual commissioning e di teleconferenza

permetteranno l'esecuzione da remoto di attività operative come interventi manutentivi, installazioni e collaudi al cliente.

In sostanza, le tecnologie digitali permetteranno di potenziare le capacità di monitoraggio, controllo e presa di decisioni nei sistemi produttivi e logistici.

Quello dove si evidenzia una certa lacuna è invece l'organizzazione dei progetti 4.0. Un quarto delle imprese porta avanti progetti sparsi, senza una roadmap, un programma strategico o un coordinamento; 4 su 10 perseguono diversi progetti in modo coordinato, ma senza una roadmap o un programma strategico complessivo; e quasi un quarto segue una roadmap generale. Solo una percentuale limitata di circa il 10% ha un programma globale che guida in modo strutturato l'identificazione e la gestione dei diversi progetti.

«Per un approccio sistemico ai progetti 4.0 serve inquadrarli in ampi programmi di digitalizzazione, con una visione strategica dei vantaggi e del ruolo delle persone nei processi operativi - osserva Raffaella Cagliano, docente Ordinario di People Management e Organization al Politecnico di Milano -, coinvolgendo più funzioni, dipartimenti e livelli gerarchici, insieme agli utenti per raccogliere proposte di miglioramento. Inoltre, serve un approccio basato su metodologie agile e di design thinking, con un'attenzione particolare al Change Management, dedicando se possibile figure specifiche a supporto del progetto e facendo leva su culture aziendali orientata al miglioramento continuo».



# Per ottimizzare le telco aziendali serve una consulenza di alto livello

HiSolution risponde da 15 anni alle esigenze consulenziali e di integrazione con servizi che potenziano e ottimizzano gli asset Telco e IT delle aziende

**O**ttimizzare gli asset telco aziendali per favorire smart working, collaborazione e sicurezza è tra gli obiettivi principali delle aziende. Il problema è con l'aiuto di chi farlo.

Un supporto concreto si è proposta di darlo HiSolution ([hisolution.it](http://hisolution.it)), che ha come mission quella di affiancarsi alle aziende per ottimizzarne valori economici e performance.

L'azienda, che ha sede a Vecchiano (PI), opera da 15 anni per supportare le imprese di medie e grandi dimensioni con servizi volti a gestire le aree TLC, networking, data center e security tramite un servizio di consulenza e progettazione che identifica le soluzioni ottimali in base alle specifiche esigenze. Il target è costituito da grandi clienti che devono gestire un'alta complessità di telco e IT, hanno numerose sedi, anche estere, e molti dipendenti anche in mobilità.

Due le divisioni con cui opera: la *Technology*, che ha accordi con Carrier, compreso Fastweb e Wind, e la *Consulting*, che affianca le aziende nella fase di Negoziazione, nel Management day-by-day, e nel



Luca Coturri, CEO di HiSolution

Controllo e Governance.

Gli ambiti e le modalità in cui l'azienda opera con un'esperienza consolidata sono: *Telco*, con un team certificato e specializzato; *Security*, con soluzioni che condividono i dati di intelligence in tempo reale; *Networking*, con la progettazione di rete e wi-fi; *Data center*, supportando le aziende nella scelta di investimento in co-location o in facility.

L'azienda dispone anche di un servizio di Help Desk & NOC centralizzato H24, con interventi on-site o da remoto e operando come Single Point of Contact.

Tra gli altri gli aspetti qualificanti la società spiccano: il mix di servizi di consulenza e

software volti ad ottimizzare i diversi aspetti delle telco, dai valori economici a quelli prestazionali; la riduzione sensibile della spesa telco tramite la collaborazione e la negoziazione con i diversi operatori con risparmi stimabili tra il 20 e il 60%, con possibilità di garantire un minimo a seguito di una pre-analisi, l'acquisizione della governance dell'asset telco tramite tool di monitoraggio, Help Desk dedicato e benchmarking di mercato. Inoltre, sia che si tratti di SDWAN, CLOUD, VOIP o di integrazione con Microsoft Teams, viene disegnata congiuntamente la soluzione tecnologica e infrastrutturale più adatta, reinvestendo anche parte del saving.

«Nel 2020 sono stati attivati oltre 80 progetti in ambito technology cui si vanno a sommare le iniziative relative ai nuovi clienti dei servizi consulting e quelli già consolidati. Il totale è un parco clienti di oltre 300 aziende in costante crescita. Il successo del nostro approccio è confermato dai risultati economici, con un target per il 2020 di 3,6 milioni di euro di fatturato e una crescita del 30% rispetto al 2019», ha evidenziato Luca Coturri, CEO di HiSolution. \*

# La digitalizzazione nel futuro delle PMI del comparto manifatturiero

La scelta di soluzioni agili, flessibili e altamente funzionali consente un notevole risparmio in termini di costi e tempi di implementazione

---

**L**a pandemia in corso ha evidenziato come la digitalizzazione sia uno dei prerequisiti indispensabili per consentire alle aziende di rimanere sul mercato. Ma in assenza di una tecnologia adeguata è impossibile progettare un percorso di crescita.

Le PMI, in particolare, spesso hanno sistemi gestionali obsoleti e i percorsi di innovazione non sempre sono in linea con le esigenze di sviluppo del business. La varietà dei settori e di tipologie aziendali implica poi da parte di un fornitore di tecnologie o del consulente la capacità di erogare servizi atti a rispondere alle specifiche esigenze, senza che però questo incida sulla flessibilità e sui costi. «Le PMI del manifatturiero, su cui concentriamo le nostre attività di consulenza, devono affrontare un processo di innovazione di per sé articolato che va a incidere non solo nel profondo della loro organizzazione, ma soprattutto sui processi caratteristici del proprio business. Una metodologia di implementazione strutturata su un'analisi specifica dei requisiti e dei processi dell'azienda, con una loro precisa mappatura, è l'approccio che un system integrator moderno deve avere per supportare l'implementazione di un nuovo sistema gestionale», osserva in proposito Paolo Aversa, Managing Director di Ally Consulting (allyconsulting.it). Esperienze reali evidenziano come in un progetto di implementazione di un ERP mediamente l'80% del tempo sia dedicato alla mappatura e revisione dei processi, al migliorare l'organizzazione e alla formazione degli utenti. In questo, il software deve essere considerato un tool a supporto degli utenti per la gestione dei flussi e dei dati per il controllo del processo.

A parte la scala dimensionale, va considerato che le PMI si trovano ad affrontare le stesse problematiche delle grandi aziende, ma a farlo avendo meno risorse. Per questo motivo, osserva Aversa, hanno bisogno di un sistema gestionale con una ampia copertura dei processi, ricco di funzionalità ma allo stesso tempo flessibile e capace di adattarsi al modello di business dell'azienda.

Oltre che nell'implementazione del sistema gestionale la flessibilità si deve riflettere anche nel prodotto stesso. Per esempio, spiega il manager, CloudSuite Industrial di Infor è una soluzione ERP end-to-end per l'industria manifatturiera

e la produzione discreta; una piattaforma che include estensioni di analisi predittiva, collaborazione, strumenti di lean production e opzioni di integrazione.

Le imprese che lo adottano possono in sostanza disporre di tutte le funzionalità, tipiche di settore, necessarie per migliorare il servizio offerto, aumentare la produzione e migliorare la qualità, coordinando meglio gli aspetti legati alla manutenzione e all'assistenza "aftermarket".

Le funzionalità insite nel prodotto limitano anche la necessità di customizzazioni, che rendono le applicazioni rigide e meno adattabili a nuove esigenze, in antitesi con la flessibilità che oggi viene richiesta dal mercato.

Va infatti considerato che soluzioni customizzate tendono ad aumentare il TCO, laddove invece il costo del software e dell'implementazione di una soluzione deve essere accessibile, e non sfruttare tutte le funzionalità delle soluzioni è in contrapposizione con questo tipo di approccio.

«La digitalizzazione è un processo a cui le PMI del manifatturiero discreto non possono più sottrarsi. Tuttavia, gli ostacoli che incontrano oggi le imprese sono molteplici, a partire dalle risorse economiche ridotte, ma con la richiesta, comunque, di strumenti performanti e con alti livelli di copertura funzionale per continuare a fare della flessibilità la loro arma vincente», ha osservato Aversa.

Tre i valori principali dell'approccio adottato da Ally Consulting per permettere alle PMI di essere

vincenti: innovazione, flessibilità e concretezza.

- Innovazione, attraverso l'uso di tecnologie moderne, per estendere l'uso del sistema gestionale a tutta la fabbrica e non solo in ufficio.
- Flessibilità nell'implementazione di un sistema gestionale e nel supporto ai clienti che devono adattarsi velocemente a scenari competitivi e dinamici.
- Concretezza, perché le aziende che intraprendono un percorso di implementazione di un sistema gestionale ERP, devono raggiungere in tempi ragionevoli i risultati che gli vengono proposti.

### Strategie e partnership per il manifatturiero

A un anno dalla nascita, e in soli 12 mesi, ha evidenziato Aversa, Ally ha raggiunto buoni risultati,



Paolo Aversa, Managing Director di Ally Consulting

accresciuto i clienti e consolidato il rapporto con Infor fino a diventare il partner di riferimento in Italia per la soluzione CloudSuite Industrial.

L'azienda prevede di chiudere il 2020 con un fatturato di 3 milioni di euro, con una forte crescita rispetto all'anno precedente (pari a 1 milione di euro), superando le aspettative in un periodo segnato da una forte crisi economica.

La sua crescita è testimoniata anche e soprattutto nelle competenze e i clienti, il cui parco è alla data composto da più di cento aziende in Italia e all'estero con diversi progetti di innovazione per le PMI e la gestione di oltre 2.000 utenti Infor.

L'obiettivo dichiarato è quello di consolidare la propria presenza sul mercato e garantire alle PMI del manifatturiero un affiancamento a 360° in tutti i processi del complesso percorso di digitalizzazione.

Il Partner Network di Ally, oltre a Infor, vede poi ad oggi anche la collaborazione con molte realtà quali: Jps e Twin Group come Consulting Partner e Netsurf, AR-XIvar, Overlog, Plannet e FasThink come Solution Partner.

Per rispondere all'espansione del business e alle richieste del mercato la società ha investito anche in nuove assunzioni nelle sue sedi di Milano e Ravenna.

Il team di specialisti è cresciuto del 15% portando a 38 i suoi professionisti, con la previsione di ulteriori ingressi di Business, Application e Technical consultant. ❁

# 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



A4

## BENEFICI

PRIMA

UNA SOLA STAMPANTE DI  
DIMENSIONI IMPONENTI

DOPO

**PIÙ STAMPANTI,  
COMPATTE  
E PERFORMANTI**

FILE PER RITIRARE  
STAMPE

**MENO SPOSTAMENTI  
E ASSEMBRAMENTI**

SCRIVANIE  
AFFOLLATE

**PIÙ SPAZIO  
LIBERO E PIÙ  
DISTANZIAMENTO**

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

**brother**  
at your side