

DIRECTION

ReportTec

LA DIGITAL ECONOMY AL SUPPORTO DEL BUSINESS

Distribuito gratuitamente con "Il Sole 24 Ore"

**Sicurezza informatica:
in anteprima i dati 2021
dell'Osservatorio Attacchi
Digitali in Italia**

**Servizi di stampa gestita:
una soluzione adatta alle
PMI per ridurre i costi e
aumentare la sicurezza**

**Da cyber security a cyber
resilience: come cambiano
i modelli di protezione**

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

**Verso
nuovi modelli
di lavoro
e di protezione**



VERTIV™

REPORT VERTIV

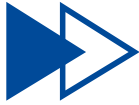
Archetipi Edge 2.0

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





INDICE

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

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

Gaetano Di Blasio

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.

- 4 Indagine OAD 2021 sugli attacchi digitali in Italia
- 8 Essere donna nel mondo della cybersecurity
- 9 Ransomware: il ricatto che rende 20 volte l'investimento
- 12 Machine learning per una resilient security
- 14 Praim dalla parte dei CISO
- 16 Dalla sicurezza alla resilienza: come cambiano i paradigmi di protezione
- 20 Modelli standard per le infrastrutture Edge
- 22 Cloud ibrido: il motore della trasformazione digitale
- 24 Stampa gestita per aziende in smart working
- 26 I servizi MPS di Brother
- 28 Tempo di smart working: guida di sopravvivenza all'eccesso di riunioni



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

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.

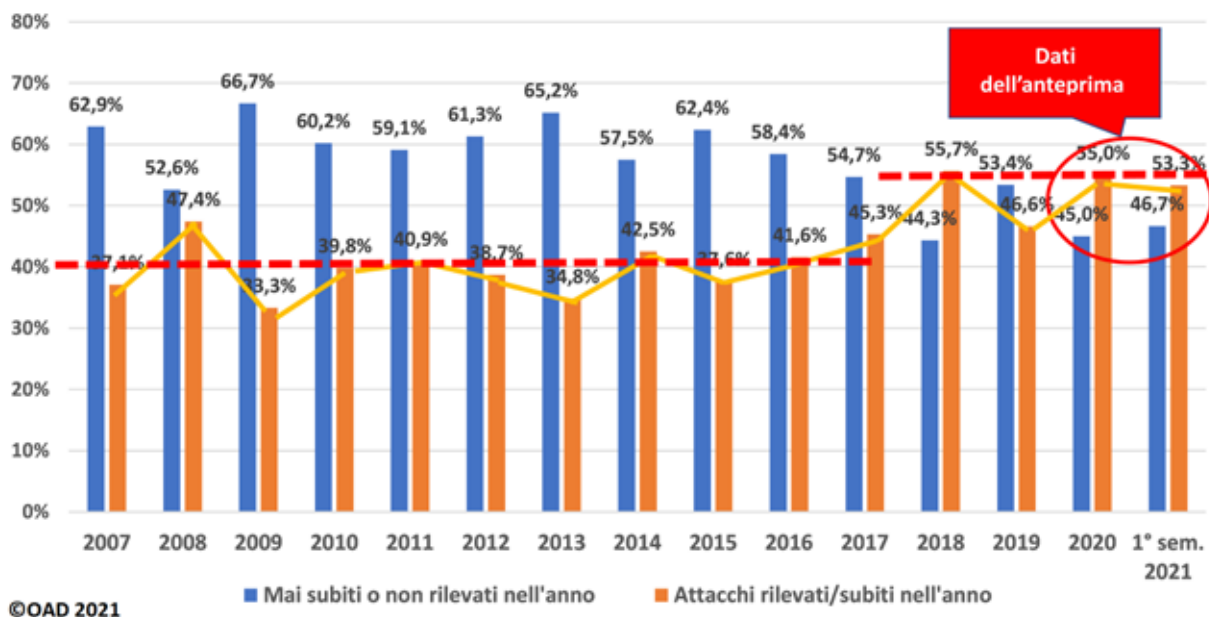
AIPSI, Associazione Italiana Professionisti Sicurezza Informatica

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.



Confronto risultati indagini OAD-OAI 2007-2021



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>.

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 4 milioni e 304 mila 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 di 250 dipendenti. Per la 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.

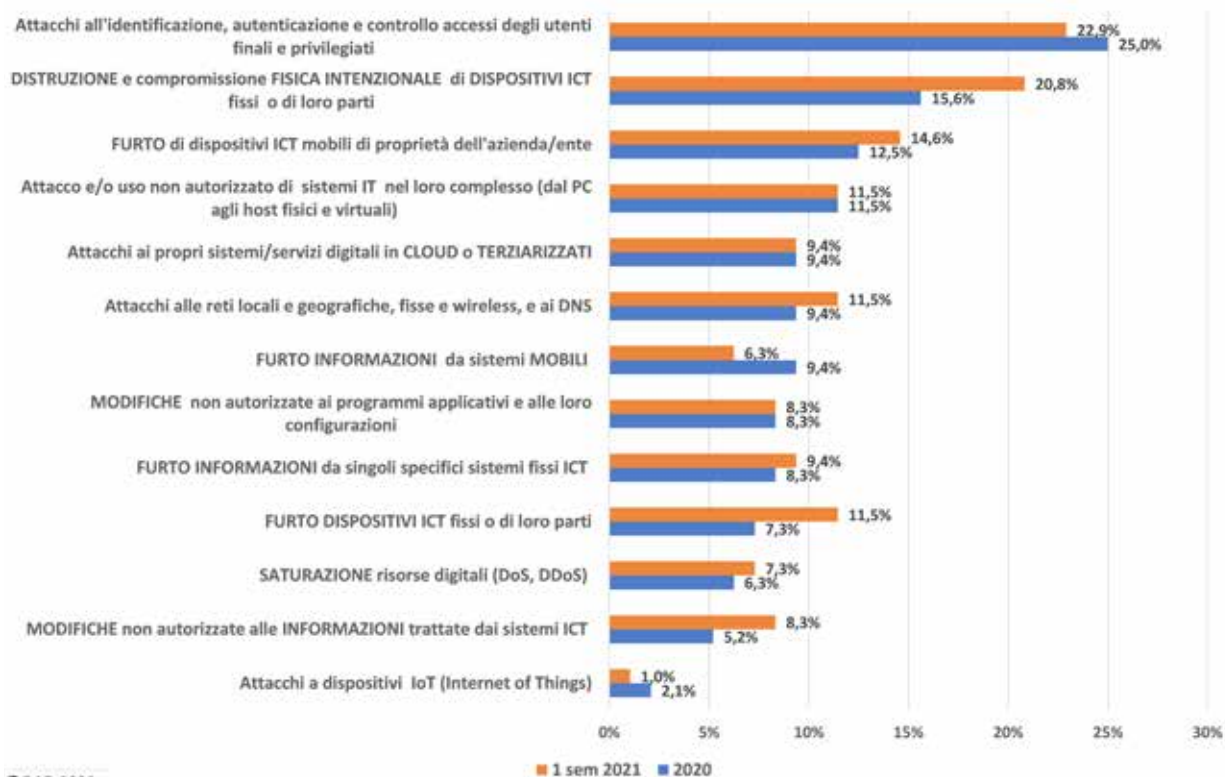
Tipologie e tecniche di attacco

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

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



©OAD 2021

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.

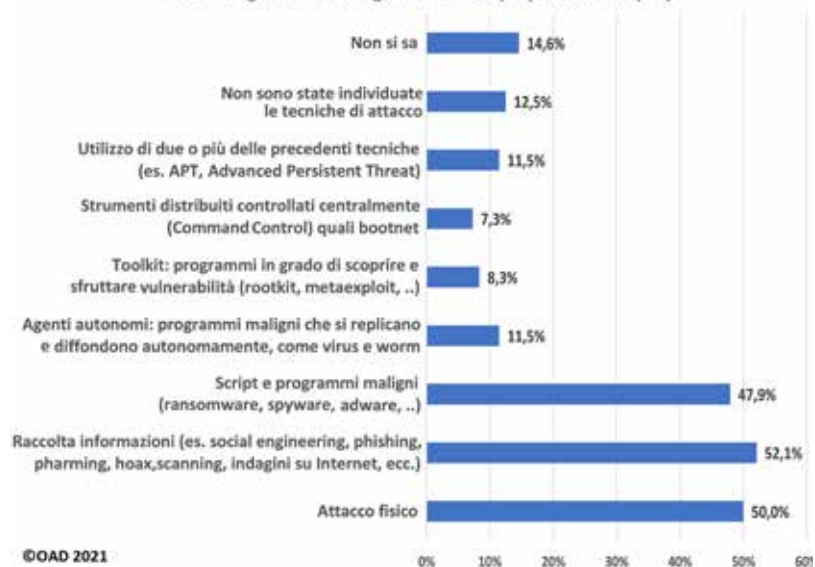
I dati dalla Polizia Postale e delle Comunicazioni

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

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



©OAD 2021

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

	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)

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 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, 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)



Essere donna nel mondo della cybersecurity



Il Rapporto “Cyber Security Women Italy (CSWI) - Il lavoro femminile nella sicurezza digitale in Italia” pubblicato da AIPSI fa il punto sulla diversità di genere tra i professionisti della sicurezza informatica

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

L'indagine CSWI 2021 ha interpellato 468 professioniste donne che, a vario titolo, si occupano per lavoro di sicurezza digitale: operano in aziende private e pubbliche, nella formazione in ambito universitario e non e come libere professioniste. 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. Più dei due terzi delle rispondenti ha una laurea (solo il 9,3% di tipo triennale) e, di queste, il 67,1% è di tipo tecnico scientifico.

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% (concentrato soprattutto nella fascia di età 35-44) lo giudica un elemento sfavorevole e una percentuale di poco inferiore, dichiara di non essere in grado di valutarlo.

Un aspetto importante nell'attività lavorativa è poter ben conciliare le esigenze di tempo per l'attività professionale con quelle personali e per la propria famiglia. Il 23,5% delle

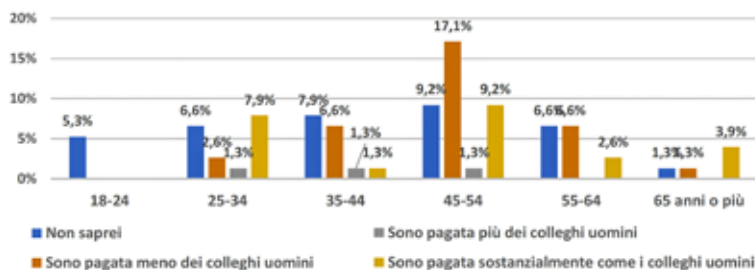
rispondenti ha dichiarato di avere problemi nel bilanciare attività lavorativa e personale: si tratta di una percentuale inferiore al previsto, che si concentra nella fascia di età 35-54 anni. Tra le motivazioni per queste difficoltà: la mancanza di un team di lavoro supportivo, poco tempo per seguire la famiglia, l'impossibilità di svolgere alcune attività di cybersecurity da remoto, la frequente necessità di operare in trasferta e l'esigenza di ritagliarsi tempo per la formazione costante necessaria nel campo della cybersecurity.

Il divario retributivo è uno dei temi centrali nella disparità di genere e ha trovato riscontro anche in questa indagine. 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 (questa percentuale si concentra nella fascia d'età tra 25 e 54 anni). Un quarto delle rispondenti ritiene di essere pagata sostanzialmente allo stesso modo degli uomini.

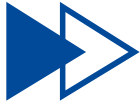
La percentuale maggiore delle rispondenti (36,8%) dichiara di non sapere se sia pagata più o meno rispetto a colleghi. All'aumentare del livello di istruzione cresce la retribuzione oraria per uomini e donne, ma aumenta ulteriormente lo svantaggio retributivo per le donne.

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

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



© AIPSI 2021



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

Giunge 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 sblocarli, 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 –. Purtroppo 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 ottenibili 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.



Simone Fratus, cybersecurity specialist di TAG Distribuzione

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 sferrare 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 quelle 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

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.



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

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.



Machine learning per una resilient security



**Il machine learning
offre alle aziende
nuove opportunità
per risolvere
problemi di sicurezza
che i loro team non
riescono più ad
affrontare**

di Riccardo Florio

Le aziende sono ormai piene di strumenti di monitoraggio e gli eventi di sicurezza generano veri e propri big data che arrivano ai team di sicurezza, impegnandoli in continue cacce al tesoro o intrappolandoli in labirinti, nel tentativo di impedire una violazione. Ci sono molte strade da percorrere, ma non tutte porteranno alla soluzione di cui il team ha bisogno. Alla fine, questo processo si traduce in un compito estenuante e dispendioso (vedi a lato).

Resilient security oltre l'analytics predittiva

Le tecnologie di analytics possono fornire un importante contributo alla risoluzione di questi problemi. L'approccio di analytics più comune oggi nella sicurezza riguarda modelli predittivi, per identificare possibili rischi all'interno di grandi quantità di dati. In breve, la modellazione predittiva combina i dati storici con il comportamento in tempo reale per comprendere o prevedere l'evoluzione futura.

Con questo tipo di analisi possiamo rispondere alla domanda "Cosa succede dopo?".

L'analisi predittiva è, tuttavia, solo un tassello di un puzzle più esteso. L'approccio analitico ideale dovrebbe combinare sensori intelligenti e fonti di dati distribuiti (desktop, server, dispositivi mobili, cloud, social network, IoT) con molteplici forme di analisi avanzata: analisi comportamentale e delle minacce, analisi forensi, modellizzazione dei rischi, rilevamento di anomalie, ottimizzazione comportamentale e di risposta e altro ancora.

Grazie agli strumenti di machine learning è possibile andare oltre un rilevamento avanzato delle minacce per fornire indicazioni su come la minaccia potrebbe essere prevenuta o contenuta: in definitiva, identificare la migliore azione di risposta possibile, prima ancora che la minaccia si sia

presentata alle porte della propria azienda. In altre parole, consente di rispondere ad altre domande chiave, come: "Quante minacce ci sono?" e "Qual è la migliore reazione possibile?". Questo approccio definisce i contorni di un modello di "resilient security" capace di adattare costantemente il livello di protezione in modo intelligente e dinamico all'evoluzione delle minacce.

Il contributo del machine learning

Le aziende hanno oggi bisogno di tecnologie di machine learning per risolvere i problemi che i loro team di sicurezza devono affrontare perché i processi esistenti non hanno la capacità di scalare a piacere e non riescono a far fronte efficacemente alle nuove esigenze di protezione.

Gli strumenti di machine learning e analytics possono semplificare e accelerare notevolmente il processo di identificazione e analisi di trend importanti, favorendo l'identificazione delle vere minacce. Il machine learning mette a disposizione strumenti per filtrare tutte le informazioni in arrivo, identificare i posti giusti dove cercare e identificare le risposte idonee rilevare le minacce in termini di minuti e ore, anziché in giorni e settimane (se non addirittura mesi o anni). Questi nuovi strumenti sono applicabili non solo ai processi che coinvolgono le macchine, ma consentono di analizzare le vulnerabilità associate agli utenti e al loro comportamento che rappresentano un rischio

molto elevato all'interno dell'azienda, soprattutto quando si tratta di utenti che godono di accessi privilegiati a informazioni business critical.

Gli strumenti di intelligenza artificiale permettono di effettuare analisi avanzate basate su sofisticate correlazioni combinando dati provenienti da ogni fonte e ogni dispositivo di controllo, sintetizzando i risultati e proponendoli all'utente in modo coerente all'interno di una dashboard e consentendogli di comprendere rapidamente la situazione associata a un'entità, un utente, un file, un dispositivo client, un server, un indirizzo IP o un altro componente



IT. Se i professionisti della sicurezza hanno a disposizione tutte queste informazioni all'interno di una dashboard intuitiva e interattiva possono analizzare in modo approfondito i motivi per cui le caratteristiche, i modelli di utilizzo e i comportamenti di un'entità sono da considerare a rischio più elevato di altri.

È una condizione che permette di dedicare meno tempo alla raccolta dei dati e più tempo alla comprensione di un attacco così come di ridurre le risorse e il budget speso per l'analisi, che favorisce la comprensione dei processi aziendali, dei modelli di comportamento degli utenti e delle relazioni tra le entità dimostrando abilitante per la predisposizione di strategie e metodi di security governance capaci di adattarsi dinamicamente al rischio.*

Un processo frustrante e dispendioso

In uno scenario per nulla inusuale in molte imprese il team di sicurezza nota un avviso e assume che sia rilevante e meriti di essere seguito. A questo punto controlla il contesto nei dashboard del Security Operations Center (SOC) per avere un'idea generale di cosa stia succedendo e quindi le informazioni di sicurezza e il sistema di gestione degli eventi (SIEM) e trova due indirizzi IP. Per ogni indirizzo IP, il team controlla un'altra console per scoprire a quali sistemi corrisponde l'indirizzo IP. Esegue una ricerca sul Web per determinare chi possiede l'indirizzo e se si tratta di un indirizzo IP buono o cattivo, quindi controlla l'inventario delle risorse per scoprire se si tratta di un'applicazione legittima e chi la possiede. A questo punto viene inviata un'email ai proprietari per i dettagli, perché le informazioni sull'inventario delle risorse sono probabilmente obsolete o incomplete.

Successivamente, il team controlla una console per scoprire quando è stata eseguita l'ultima scansione del sistema di avviso, una per scoprire se il sistema è stato aggiornato dopo la scansione e un'altra ancora per verificare se è stato eseguito il backup del sistema. Il processo continua all'infinito con più email, più controlli della console, più percorsi da seguire. E alla fine del processo, due ore dopo l'inizio, la risposta è che l'allerta era un falso allarme. Nel frattempo sono arrivati centinaia di altri avvisi che richiedono attenzione; quindi il team di sicurezza ne sceglie un altro da esaminare e ricomincia il processo da capo. Solo i professionisti della sicurezza che hanno affrontato questo processo possono veramente capire quanto possa essere frustrante e dispendioso in termini di tempo.



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



Nell'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 da fare.

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 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 particolare 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. ❁



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 proverbiai 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 sicurezza, 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



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.

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 **Interset 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.

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.

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

Il portfolio CyberRes

Data Privacy and Protection

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

Voltage

For

Interset

Identity and Access Management

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

NetIQ

ArcSight

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.

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 resilience 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 resilience 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 riunisce, essenzialmente, le aree della sicurezza delle informazioni, della continuità aziendale e della resilienza organizzativa.

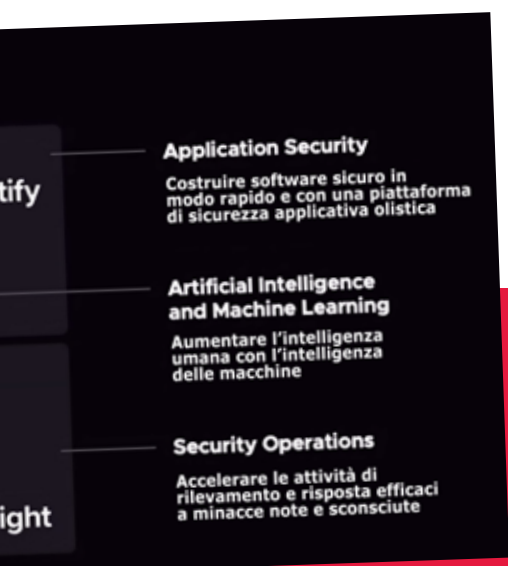
CyberRes: il nuovo brand per garantire la resilienza

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 resilience 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 resilience: 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

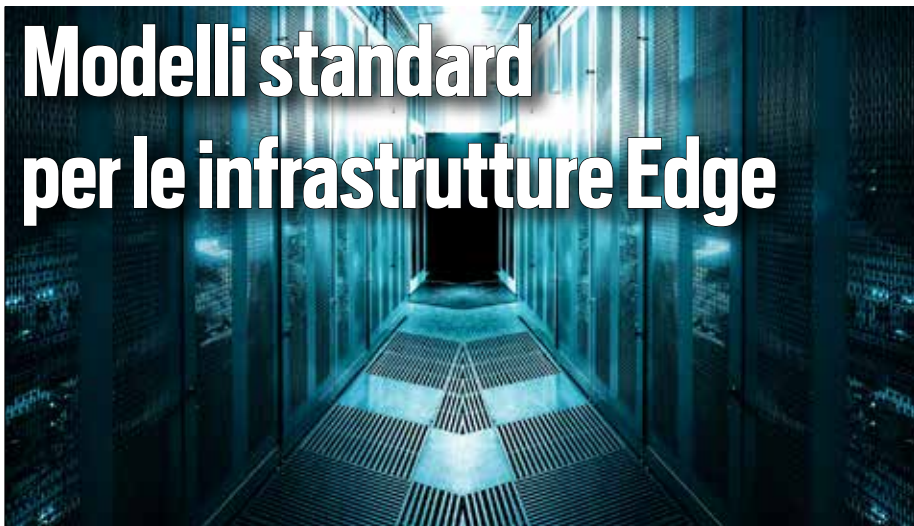
La sicurezza delle applicazioni deve partire dalla fase di sviluppo integrando strumenti di controllo e test di sicurezza direttamente nelle piattaforme di sviluppo per poi estendersi all'intero ciclo di vita. Alla protezione delle applicazioni CyberRes indirizza la consolidata gamma di soluzioni Fortify 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).



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

di Mercedes Oledieu

Modelli standard per le infrastrutture Edge



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. Condivide 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 *



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

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



Cloud ibrido: il motore della trasformazione digitale

L'approccio verso un modello di cloud ibrido conquista sempre più consenso per rispondere alle esigenze di digital transformation e di riduzione del Total Cost of Ownership dell'infrastruttura

di Mercedes Oledieu

La crisi conseguente alla pandemia ha accelerato il processo di trasformazione digitale che molte realtà avevano già intrapreso, aprendo la strada a nuove opportunità per accrescere la resilienza aziendale.

Nel processo di digital transformation la migrazione verso il cloud rappresenta un passaggio fondamentale e un approccio ibrido tra soluzioni cloud-based e on-premise offre innanzitutto maggiore agilità con la possibilità di adattarsi e cambiare rapidamente direzione: un principio fondamentale di un business digitale.

Hybrid cloud e digital transformation

Un'architettura ibrida permette di approcciarsi in modo graduale verso il cloud, beneficiando da subito dell'agilità offerta da questo ambiente, ma migrando contenuti e applicazioni sulla base di ritmi ed esigenze specifici.

Con una configurazione ibrida è possibile utilizzare un mix di risorse private e pubbliche per eseguire i carichi di lavoro in modo ottimizzato ed effettuare analisi ovunque, indipendentemente da dove si trovano i dati. Inoltre permette di spostare i carichi di lavoro nell'ambiente cloud di tua scelta, pubblico o privato e di prevenire il lock-in verso uno specifico fornitore.

Alle caratteristiche di agilità, elasticità e facilità d'uso dei





cloud pubblici affianca una piattaforma multidisciplinare che unifica metadati, sicurezza e governance in tutti gli ambienti. Inoltre, diventa più semplice assicurare che i dati siano archiviati correttamente in relazione ai corretti requisiti di governance e di gestione dei costi. Il cloud semplifica l'accesso e la creazione dei contenuti, nonché l'interazione con clienti e business partner; ed è proprio attraverso un approccio moderno alla gestione dei contenuti che è possibile accelerare gli obiettivi di trasformazione digitale e di accelerazione del business. Le aziende che utilizzano il cloud ibrido possono, così, conseguire vantaggi in relazione ad aspetti quali cicli di vendita più veloci, migliore livello di collaborazione, customer satisfaction, usabilità, flessibilità e anche sicurezza.

Un modello che aumenta la cyber resilienza

La resilienza informatica può essere descritta come la capacità di un'organizzazione di continuare a eseguire efficientemente i propri processi mentre si trova a dover fronteggiare una minaccia informatica.

Di conseguenza, raggiungere la resilienza informatica significa, per un'organizzazione, essere in grado di identificare le proprie risorse, valutare e gestire il rischio dell'infrastruttura e sviluppare capacità di risposta alle minacce in modo tale che i processi di business continuino a funzionare durante una crisi e si riprendano rapidamente. Garantire la resilienza significa anche apprendere da tutto ciò che succede e migliorare continuamente i piani e le strategie esistenti.

Raggiungere questi obiettivi richiede adattamento e reinvenzione continui e il cloud ibrido è il candidato ideale per rispondere a questo tipo di esigenze.

Inoltre, il processo di modernizzare nella gestione dei contenuti favorito dal cloud porta verso l'automazione dei processi chiave che contribuisce a ridurre il rischio di errore umano e di perdita di informazioni.

Convertirsi al digitale puntando sul cloud può rivelarsi anche fondamentale per affrontare le nuove minacce informatiche che, con il diffondersi di modelli di lavoro da remoto, rendono i dispositivi ancora più vulnerabili, esponendo i dati conservati su desktop, laptop e tablet a ransomware, errori umani, perdita e furto di dati.

Hybrid cloud e TCO

Un'altra esigenza molto sentita dalle aziende è di riuscire a ottimizzare i costi dell'infrastruttura puntando a

utilizzare solo le risorse necessarie e a pagarle il costo minore possibile.

Anche in tal caso l'utilizzo di un'architettura che coniughi cloud pubblico e privato si dimostra una scelta efficace verso cui si orientano sempre più aziende. Nel rapporto "Cloud Trends in 2020: The Year of Complexity, and its Management", per esempio, la società di ricerche 451 Research evidenzia come il cloud ibrido stia emergendo come scelta strategica predominante per la gestione informatica e la trasformazione digitale. Le architetture ibride stanno guadagnando sempre più consenso come approccio più idoneo a favorire la riduzione del costo totale di proprietà (TCO).

Sebbene il cloud pubblico fornisca un accesso immediato a risorse teoricamente infinite, la sua struttura di prezzo ha un impatto diretto sul budget che porta a un costante aumento del TCO. Di conseguenza, i costi dell'infrastruttura continuano a crescere, drenando i risultati aziendali e consumando il budget per l'innovazione.

Un'architettura ibrida risponde meglio all'esigenza di ottimizzare i costi dell'infrastruttura perché mette a disposizione piattaforme cloud pubbliche e private unificate in un ambiente operativo e un framework di gestione comuni. Negli ambienti ibridi, per esempio, le istanze del database possono essere eseguite in un cloud privato e le applicazioni front-end possono essere eseguite in un cloud pubblico. Ciò consente alle aziende di gestire le proprie piattaforme (pubbliche e private) utilizzando un unico insieme di strumenti e processi, consentendo un'unica visione di gestione coerente tra le piattaforme e di avere gli stessi processi per il provisioning su entrambe le piattaforme. ❁



Stampa gestita per aziende in smart working



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

di Mercedes Oledieu

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.

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, 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.



I servizi MPS di Brother



**Un'offerta flessibile
di Managed Printing
Services adatti
anche alle PMI, che
favorisce la riduzione
dei costi e aumenta
la sicurezza**

di Riccardo Florio

L'offerta di servizi di stampa gestita di Brother mette a disposizione delle aziende, innanzitutto, un approccio per rivedere in ottica digitale la gestione dei flussi documentali che comprendono la stampa.

Grazie a software di print management e l'introduzione di alcune funzionalità specifiche, è possibile abilitare un maggiore controllo sui costi, riducendo gli sprechi.

L'attribuzione di quote massime di stampa attribuite in funzione del ruolo degli utenti unitamente a una distribuzione dei dispositivi correttamente bilanciata in base alle effettive esigenze degli utenti permette di ridurre i costi normalmente associati ai sistemi centralizzati che, per soddisfare tutte le necessità, sono spesso sovradimensionati rispetto alle attività svolte dai diversi reparti.

Funzionalità per ridurre gli sprechi

Una serie di funzionalità consente di gestire il consumo energetico. Quando la macchina non riceve un lavoro di stampa per un certo periodo di tempo entra automaticamente in modalità di sospensione (Sleep) e, se il tempo di inattività si estende, passa in modalità Deep Sleep con un'ulteriore riduzione dei consumi. Un'ulteriore fase di inattività porta allo spegnimento automatico, che richiede la pressione del tasto di accensione/spegnimento sul pannello di controllo per la riattivazione.

Grazie alla funzionalità di Pull Printing i documenti da stampare vanno in una coda virtuale sicura e per produrre l'output di stampa è necessario che l'utente sia pronto al ritiro della stampa e si trovi in prossimità del dispositivo. Questo permette non solo di bloccare tutti gli accessi non autorizzati ai singoli dispositivi, ma anche di garantire la privacy dei documenti prodotti e di evitare stampe duplicate, abbandonate o errate, facendo risparmiare quindi su carta e consumabili.

Stampe sempre protette

Il Pull Printing è una funzionalità avanzata che permette di stampare documenti riservati con la massima sicurezza in ogni fase di stampa.

Un'ulteriore opzione di sicurezza delle stampe in uscita proposta da Brother è il Secure Print+ che permette di assegnare a ogni utente funzioni di stampa differenziate, attivabili previa un'autenticazione con scheda di identificazione NFC oppure mediante PIN.

Per prevenire i rischi associati a violazioni di documenti memorizzati sugli hard disk interni alle periferiche, buona parte dei dispositivi Brother non necessita, poi, di dischi fissi per l'esecuzione delle operazioni di stampa, mentre per impedire fughe di informazioni le macchine laser di fascia alta sono tutte dotate delle funzionalità di sicurezza di rete TLS/SSL.

Alcune serie di stampanti sono in grado di bloccare a distanza chiunque acceda al dispositivo tramite la rete, filtrando gli indirizzi IP e sfruttando il controllo protocolli, che consente agli amministratori di disattivare i protocolli non necessari senza bloccare completamente l'accesso a tutte le funzioni, come FTP o SMTP.

Brother Pagine+ porta le PMI nell'era dell'As a Service

Pagine+ è l'offerta MPS di Brother pensata soprattutto per le piccole e medie imprese che include la fornitura di stampanti e dispositivi multifunzione, laser e inkjet, monocromatici e a colori.

Tre sono le formule disponibili con l'obiettivo di fornire ai clienti il massimo del valore a fronte del minimo impatto implementativo.

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 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 è più propriamente a consumo e 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 cartucce o toner. L'eccedenza viene fatturata a parte su base periodica.

Qualunque sia la formula scelta l'implementazione avviene in tre fasi.

La prima prevede un'analisi approfondita dell'ambiente di stampa e dei flussi documentali per identificare costi e criticità.

La fase successiva è quella d'implementazione dell'infrastruttura gestita, che viene progettata sugli effettivi bisogni del cliente.

L'ultima fase è quella di un processo continuo di ottimizzazione per garantire l'aderenza costante del servizio alle necessità aziendali (che possono variare nel tempo) e richiedere, quindi, una diversa distribuzione dei carichi sulle periferiche installate.

Tra i servizi offerti da Pagine+, Brother include anche l'accesso a un portale Web per monitorare i dispositivi di

output e i costi associati. Lo stesso portale consente ai rivenditori, nella parte a loro riservata, di creare in pochissimi clic un'offerta MPS, selezionando dispositivi e condizioni contrattuali in modo agile e snello.

Stampanti per aziende in smart working

Le soluzioni di stampa di Brother rispondono all'esigenza di mantenere invariata la produttività, in ufficio e in casa, durante l'emergenza pandemica garantendo, nel contempo, il rispetto delle normative sanitarie.

Attraverso la fornitura di stampanti, multifunzione e scanner dalle dimensioni compatte e ad alta velocità di stampa dotate di connettività completa (USB, WiFi, rete cablata), App di stampa o scansione per i dispositivi mobile e funzionalità di sicurezza avanzata per i documenti anche fuori dall'ufficio diventa, infatti, possibile lavorare in smart working evitando code ed assembramenti in ufficio e riducendo le interazioni tra i dipendenti.

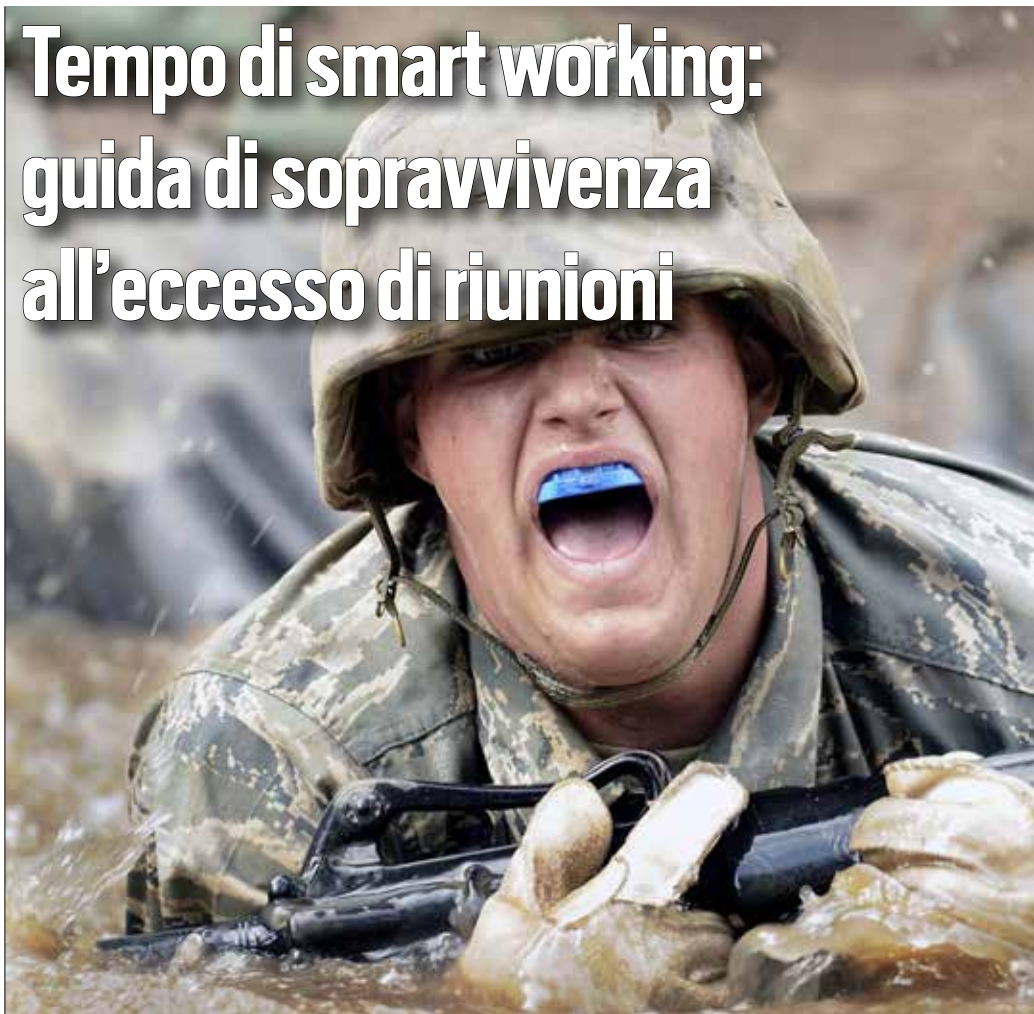
L'offerta contempla tre opzioni:

- **Silver**, prevede la fornitura di stampante multifunzione 4 in 1 monocromatica, con toner inclusi, funzionalità fronte-retro, scanner ad alta velocità e alimentatore automatico di documenti (ADF) da 50 fogli;
- **Rainbow**, con stampante multifunzione 4 in 1 a colori anche nel formato A3, stampa fronte-retro e cartucce XL incluse per un'elevata capacità di gestione della carta;
- **Premium**, con stampante professionale multifunzione 4 in 1 monocromatica oppure a colori, invio automatico dei toner XL fino a 12mila pagine incluso, assistenza da remoto e software di "security printing". ❁



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.



di Primo Bonacina *

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.

** Primo Bonacina si occupa d'informatica dal 1980. Con PBS - Primo Bonacina Services fornisce consulenza e best practice digitali in ambito sales, marketing e HR*



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. 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 sprecando 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 questi che seguono dei palliativi ma portano spesso a miglie 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 mezzeggiornate) 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 dovete 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. ✨



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

PRIMA		DOPO
UNA SOLA STAMPANTE DI DIMENSIONI IMPONENTI	>	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

brother
at your side

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