

PARTNERS

INFORMAZIONE E FORMAZIONE PER IL CANALE ICT A VALORE



Per l'AI, Microsoft rinnova il partner program

MONDO CANALE

GLI MSP ITALIANI EVOLVONO PUNTANDO SUI SERVIZI GESTITI

SICUREZZA

RANSOMWARE IN ITALIA: STRATEGIA E COMPETENZE SECONDO VEEAM

TECNOLOGIE

- ▶ INFRASTRUCTURE AS A CODE
- ▶ PFU PUNTA SULLA VIDEOCONFERENZA
- ▶ INTENT BASED NETWORKING

snom

I vostri vantaggi come Partner Snom



Il Programma Partner Snom offre
molti vantaggi - e questo
gratuitamente e senza impegno

- Cashback a partire da un determinato fatturato
- Accesso all'Help Desk
- Certificazioni e formazione (Accademia Snom)
- Condizioni speciali per progetti
- e molto altro ancora



SOMMARIO

AGOSTO/SETTEMBRE 2023 • N. 58

04. EDITORIALE

L'ascesa e le sfide del riconoscimento emozionale, tra AI e psicologia

07. PARTNER PROGRAM

Per l'AI, Microsoft rinnova il partner program

10. MONDO CANALE

Gli MSP italiani evolvono puntando sui servizi gestiti

14. CLOUD COMPUTING

African Queens of cloud computing

17. DIGITAL TRANSFORMATION

Red Hat guida la transizione digitale

20. TECNOLOGIE

PFU punta anche sulla videoconferenza

23. Infrastructure as a Code: rivoluzione digitale

27. Intent Based Networking porta innovazione e automazione nelle reti aziendali

33. BUSINESS

L'inevitabile scelta dell'open innovation

37. SICUREZZA

Strategia e competenze: la ricetta Veeam per la protezione delle aziende

39. Secure enclave: le tecnologie di protezione dei dati a livello di chip

44. Il principio del minimo privilegio e il modello Zero Trust



PARTNERS

Anno XI - numero 58
Agosto/Settembre 2023

Direttore responsabile: Riccardo Florio

In redazione: Riccardo Florio, Paola Rosa

Grafica: Paola Rosa

Hanno collaborato: Stefano Uberti Foppa, Fabrizio Pincelli, Leo Sorge

Redazione:

REPORTEC srl | Via Gorizia 35/37
20099 Sesto San Giovanni (MI);
Tel 02 24304434 | www.reportec.it |
redazione@reportec.it

Editore:

Reportec Srl, C.so Italia 50 | 20122 Milano

Diffusione: 35.000 copie digitali

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

Immagini: Dreamstime.com

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

Tutti i diritti sono riservati

Tutti i marchi sono registrati e di proprietà delle relative società

Reportec è una società fondata da:

Gaetano Di Blasio, Riccardo Florio, Giuseppe Saccardi



L'ascesa e le sfide del riconoscimento emozionale, tra AI e psicologia

I rilevamento e riconoscimento delle emozioni (Emotion Detection and Recognition o EDR) è un campo di ricerca in rapida evoluzione che sfrutta l'intelligenza artificiale, la psicologia e altre discipline per identificare, analizzare e interpretare le emozioni umane.

Le tecnologie EDR stanno diventando sempre più prevalenti in una varietà di campi, inclusi la sanità, la guida autonoma, la customer experience e il settore pubblicitario. A fronte delle opportunità entusiasmanti offerte da queste tecnologie, vanno però valutate attentamente anche le conseguenze di tipo etico associate.

In sintesi, l'EDR si propone come metodo per affinare l'interazione tra gli esseri umani e i dispositivi tecnologici, non solo per migliorare la facilità d'uso delle interfacce utente, ma anche per offrire meccanismi di feedback più sensibili e intelligenti. Tuttavia i temi dello sfruttamento inconsapevole e del controllo aperti da queste tecnologie sono dietro l'angolo.

Ciò che appare incontrovertibile è che si tratti di un mercato in forte crescita nel prossimo quinquennio, con previsioni che collocano il valore dell'industria EDR a quasi 5 miliardi di dollari entro il 2028 (Fonte: Exactitude Consultancy).

Questa crescita è alimentata dal crescente interesse in diverse settori, per l'uso dell'EDR come strumento per raccogliere dati preziosi sui comportamenti dei consumatori e migliorare l'interazione con



gli stessi. Anche l'adozione su larga scala di queste tecnologie come parte di iniziative e riforme strategiche in vari settori, sta dando un forte impulso alla crescita del mercato: per esempio, le forze dell'ordine e altre agenzie governative stanno implementando l'uso di telecamere di sicurezza abilitate all'IA per esigenze di sorveglianza.

Un mercato in rapida evoluzione

Il mercato EDR comprende le tecnologie di **riconoscimento facciale, riconoscimento vocale e l'uso di biosensori**. Soprattutto il riconoscimento facciale è una delle tecnologie in più rapida diffusione, per il suo uso come forma di controllo dell'accesso e di autenticazione per smartphone e altri dispositivi intelligenti connessi.

A livello tecnologico, il mercato EDR si avvale sia di machine learning sia di intelligenza artificiale. Attraverso l'analisi delle immagini del volto umano, le tecnologie di machine learning sono in grado di riconoscere le emozioni e comprenderne l'intensità; l'intelligenza artificiale, attraverso algoritmi di deep learning, analizza le espressioni facciali per ricavare una visione più ricca delle emozioni umane. Anche le soluzioni basate sulla voce stanno registrando un aumento costante della domanda: secondo Google il 20% di tutte le ricerche Web di oggi sono vocali e la percentuale sale al 65% nel caso di Amazon Echo o Google Home. Oltretutto, chi sceglie la voce come strumento principale d'interazione mostra grande riluttanza a tornare all'input da tastiera.

I principali settori in cui queste tecnologie possono trovare un utilizzo efficace comprendono gli enti governativi, le organizzazioni di assistenza sanitaria, il retail, l'intrattenimento, i trasporti. In **ambito sanitario**, per esempio, l'EDR può caratterizzare dispositivi indossabili intelligenti e smartphone per il monitoraggio continuo dei pazienti. Anche l'industria dell'**intrattenimento** se ne può avan-



taggiare e il gioco rappresenta un'area importante nell'alimentare la domanda di rilevamento delle emozioni al fine di migliorare l'esperienza del giocatore in ambiti come la realtà virtuale.

Un altro ambito di utilizzo riguarda il **marketing** al fine di migliorare la soddisfazione del cliente e, nel contempo, acquisire maggiori informazioni sui consumatori. Per esempio, questa tecnologia in ambito retail viene già utilizzata per offrire un'esperienza personalizzata ai clienti nel punto vendita nonché per la prevenzione del taccheggio. Kairos ha rilasciato una telecamera plug-and-play che offre sia la possibilità di rilevare l'identità dei clienti sia le loro emozioni. Anche l'**industria dei trasporti** sta sfruttando la tecnologia di riconoscimento delle emozioni. Aziende che operano nel settore automotive hanno sviluppato una tecnologia del cruscotto che controlla le emozioni del guidatore e del passeggero con l'obiettivo di migliorare la sicurezza.

Il mercato è oggi consolidato nelle mani di un numero limitato di brand poco noti al grande pubblico come Emotient, Tobii AB, Realeyes UO, Affectiva, Noldus e Kairos.

Oggi è il Nord America l'area geografica in cui si concentra la quota di mercato EDR più rilevante (40% del totale sempre secondo Exactitude Consultancy) ma la crescita più elevata nel prossimo futuro la si aspetta dalla Cina. Il governo cinese ha imposto la scansione del volto per ottenere la connessione a Internet e la tecnologia di riconoscimento del rilevamento delle emozioni è collegata al suo sistema di credito sociale in modo che il governo possa potenzialmente punire o premiare i cittadini, in base al fatto se il loro comportamento possa essere ritenuto accettabile o non accettabile. Altre applicazioni che il governo cinese sta sperimentando riguardano l'uso di queste tecnologie per prevedere il comportamento di un individuo riconoscendo il suo stato emotivo.

Per l'AI, Microsoft rinnova il partner program

di Fabrizio Pincelli

L'intelligenza artificiale è stata protagonista di tutti gli annunci fatti da Microsoft all'ultimo evento Inspire, a partire dal nuovo programma di canale AI Cloud Partner Program. Di rilievo anche l'accordo con Meta per l'impiego privilegiato della famiglia di LLM Llama 2 su Azure



Satya Nadella
CEO di Microsoft



Non c'è alcun dubbio. Il grande protagonista del recente **Microsoft Inspire**, l'evento annuale che la società di Seattle dedica ai partner, è stata l'intelligenza artificiale (AI). Nel suo keynote, il **CEO, Satya Nadella**, ha sottolineato *“le immense opportunità che l'AI offre al settore IT”*. Nadella ha detto di ritenere che l'IA sarà trasformativa come lo è stata l'interfaccia grafica. *“Siamo nel bel mezzo di un enorme cambiamento di piattaforma – afferma il CEO – e la nuova generazione di IA trasformerà praticamente ogni settore e ogni categoria del mondo del computing”*.

Un partner program all'insegna dell'IA

Per consentire al canale di poter

sfruttare al meglio le opportunità offerte dall'AI, Microsoft ha lan-



SCOPRI IL NUOVO AI CLOUD PARTNER PROGRAM

ciato il nuovo **AI Cloud Partner Program**. Come ha precisato Satya Nadella, il nuovo programma riunisce tutti gli aspetti dell'intero lifecycle del partner, dall'onboarding alla formazione, dal go-to-market agli incentivi fino al co-selling. Oltre ad avere tutti i vantaggi del programma precedente, i partner potranno avere accesso a nuove offerte e benefici specifici per l'AI.

Non c'è alcuna azione da intraprendere per passare al nuovo programma: Microsoft afferma di aver già trasferito tutti i partner esistenti nel nuovo programma con effetto immediato. Saranno mantenuti i benefici e le designazioni esistenti.

La chat per il business

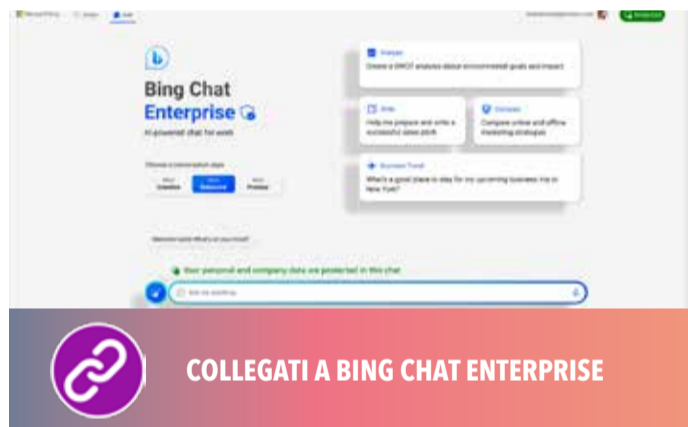
L'evento Microsoft Inspire è stato anche l'occasione per nuovi annunci in termini di soluzioni volte a supportare la crescita del canale



GUARDA IL VIDEO BING CHAT ENTERPRISE: YUSUF MEHDI AL MICROSOFT INSPIRE 23

e delle aziende, con particolare riferimento all'impegno nell'accelerare la trasformazione dell'AI.

Tra le più rilevanti c'è sicuramente **Bing Chat Enterprise**, una chat per il business basata sull'IA. **Jared Spataro, Corporate Vice-president Modern Work & Business Application**, ha sostenuto che *"tutte le informazioni in uscita e in entrata sono protette. I dati della chat non vengono salvati e Microsoft non vi ha accesso. Questo signi-*



fica che nessuno li può vedere. I dati non vengono nemmeno utilizzati per addestrare i modelli. Che si tratti di ricerche per degli approfondimenti, per analisi o semplicemente come fonte di ispirazione, Bing Chat Enterprise offre risposte migliori, maggiore efficienza e nuovi modi di essere creativi".

Spataro ha precisato che Bing Chat Enterprise **verrà incluso senza costi aggiuntivi in Microsoft 365 E3, E5, Business Standard e Business Premium**. In futuro, sarà anche disponibile come offerta standalone al prezzo di 5 dollari al mese per utente. Il manager ha

anche reso noti i prezzi di Microsoft 365 Copilot: costerà 30 dollari al mese per ogni utente di Microsoft 365 E3, E5, Business Standard e Business Premium.

Microsoft è partner privilegiato di Meta

Altra novità di rilievo annunciata da Nadella è la **partnership tra Meta e Microsoft** in relazione al supporto della famiglia di modelli linguistici di grandi dimensioni Llama su Azure e Windows. L'accordo prevede che Microsoft sia il partner privilegiato di Meta nel rilasciare per la prima volta la nuova versione di Llama 2 ai clienti commerciali. Questa col-



laborazione consentirà ai clienti di mettere a punto e distribuire i modelli Llama 2 da parametri 7B, 13B e 70B in Azure. Inoltre, Llama sarà ottimizzato per fun-



TI POTREBBE INTERESSARE:



Microsoft porta l'AI in tutte le funzioni aziendali

Con il nuovo Microsoft Dynamics 365 Copilot, che fornisce assistenza interattiva e basata sull'AI in tutte le funzioni aziendali, le organizzazioni possono dotare i propri dipendenti di strumenti pensati per i ruoli di vendita, assistenza, marketing, operations e supply chain.



continua a leggere

zionare localmente su Windows. Microsoft ha colto l'occasione di Inspire per annunciare anche **nuove funzionalità per Sales Copilot** direttamente all'interno di Dynamics 365 Sales (come per esempio il riepilogo delle opportunità generato dall'AI, le bozze di e-mail contestualizzate e la preparazione delle riunioni) e **nuove funzionalità di AI per Power Automate Process Mining**, che offre ai clienti insight per ottimizzare i processi esistenti e aumentare l'efficienza attraverso l'automazione low-code.

Gli MSP italiani evolvono puntando sui servizi gestiti

Continua il processo evolutivo dei managed service provider italiani verso servizi a maggiore valore aggiunto, con un'attitudine più votata all'outsourcing e che insegue i vantaggi dei ricavi ricorsivi. La carta di identità messa a punto da Achab nel suo report periodico.

di Fabrizio Pincelli

Sono stati oltre 450 gli MSP che hanno partecipato (più di 350 in presenza e un centinaio in remoto) all'**MSP Day**, l'evento organizzato lo scorso giugno da **Achab** per chiamare a raccolta i fornitori italiani (attuali o futuri) di servizi IT gestiti. E il successo di questa quinta edizione è stato tale che la durata ha dovuto essere prolungata. Il tradizionale giorno non bastava più per consentire ai sempre più numerosi partecipanti di assistere

agli speech e di condividere in modo

appropriato idee ed esperienze nei momenti di networking. Ma, soprattutto, un giorno non era più sufficiente per lasciare un adeguato spazio ai 36 sponsor tecnologici che hanno voluto essere parte della manifestazione.

L'MSP Day è anche l'occasione per Achab di raccontare agli operatori del settore **come sta evolvendo il mondo dei managed service provider in Italia**. Infatti, il distributore milanese ogni anno a primavera raccoglie i dati per redigere un report sugli MSP nel nostro Paese, i cui risultati sono poi pre-



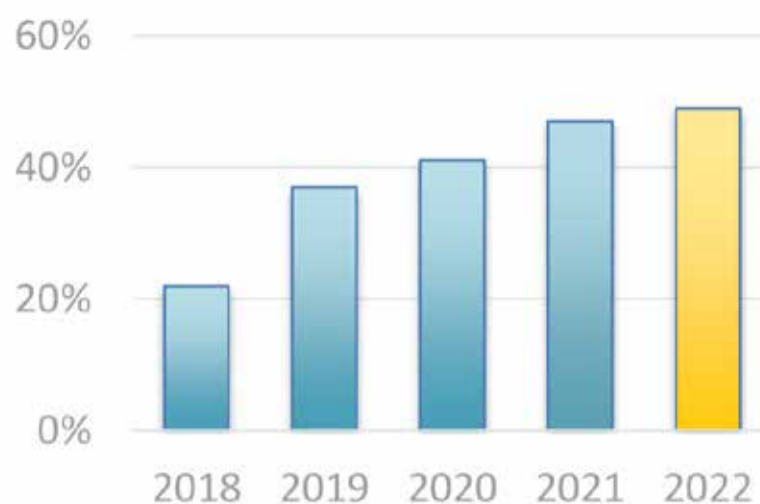
COLLEGATI
AD ACHAB

sentati all'evento di Riccione. Il campione è costituito da aziende clienti di Achab e, quindi, qualcuno potrebbe osservare che il report fornisca una visione parziale del settore. Un'osservazione più che lecita, tuttavia, oggi è l'unica indagine che tenta di valutare a che punto è il mercato degli MSP evidenziando le evoluzioni in atto, i trend, le sfide e le prospettive per il futuro. E in quanto tale assume quindi particolare valore.

L'identikit dell'MSP

Dal Report MSP 2023 di Achab, emerge che **i service provider italiani sono in massima parte realtà medio piccole**. Sta però gradualmente diminuendo il numero delle microaziende e sta invece aumentando quello delle realtà di dimensioni maggiori. Iniziata tre anni fa, questa tendenza sta comportando un cambiamento sia nel numero di addetti impiegati sia nella percentuale delle

MSP con più di 100 clienti



aziende service provider che superano il milione di euro di fatturato (sono il 43%). Anche tra le piccole realtà, la maggior parte (il 54%) si trova comunque a dover gestire un parco macchine con 500 o più endpoint mentre il 30% ne gestisce oltre 1.000. In pratica, quello delle 500 machine rappresenta oggi il limite che distingue gli MSP che lavorano in maniera ancora "artigianale" da quelli che invece si strutturano per erogare servizi gestiti. Si tratta di un punto critico che dovrebbe portare a ripensare il proprio business. E questo pone anche **nuove sfide in termini organizzativi**: anzitutto tro-

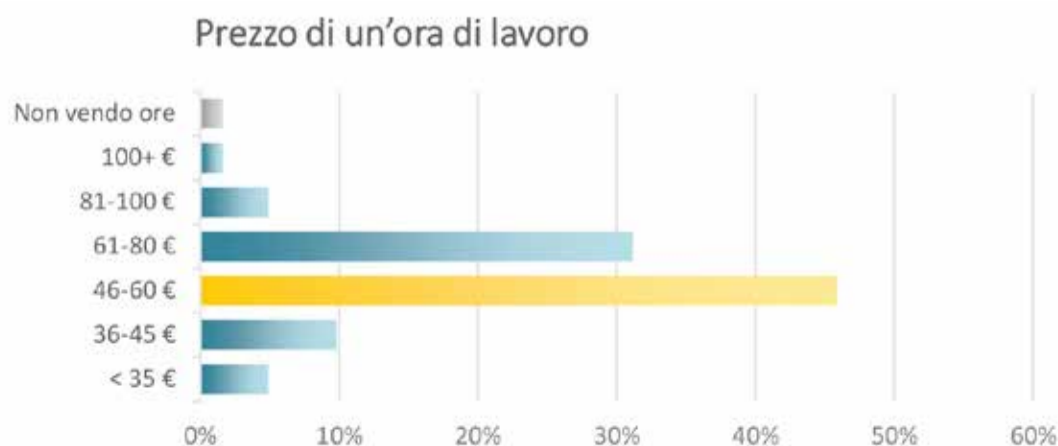
MARKETING E MSP, UNA RELAZIONE DA COSTRUIRE

Uno dei punti deboli dell'attività dell'MSP è il marketing. Infatti, sembra che le idee non siano molto chiare. Prova ne è che il 44% degli MSP sostiene che l'aspetto più problematico del marketing sia generare lead. Tuttavia, poi, quando si chiede qual è la principale attività svolta per la lead generation si scopre che pochi agiscono in modo organizzato, la maggior parte si avvale del passaparola (53%) e il 16% non fa addirittura nessuna attività di lead generation. E il 40% degli MSP non destina al marketing più dell'1% del fatturato.

vare nuovi tecnici competenti (lo ha citato il 50% del campione) e poi amministrare la crescita rendendo più efficiente l'azienda (40%). Il report evidenzia anche un altro aspetto di rilievo: è in costante aumento il numero di fornitori che gestiscono oltre 100 clienti.

Dal break fix all'IT in outsourcing

L'indagine di Achab conferma il processo di evoluzione in atto da qualche anno che porta ad abbandonare il vecchio modello di business reattivo, o break fix (il 17% dei rispondenti lavora ancora in questa modalità), in favore di un modello secondo cui l'erogazione dei servizi in maniera gestita la fa da padrone a fronte del pagamento di un canone ricorrente, nel 70% dei casi di durata annuale. Il 72% degli MSP lavora offrendo servizi IT in outsourcing, con un aumento dell'11% rispetto al 2022. Il sistemi di controllo remoto (33%) e le piattaforme RMM (66%), strumenti ormai indispensabili per un MSP, stanno rendendo un ricordo gli interventi presso i clienti (1%). In aumento anche il numero di fornitori che



TI POTREBBE INTERESSARE:



Da system integrator a managed service provider

[+ continua a leggere](#)

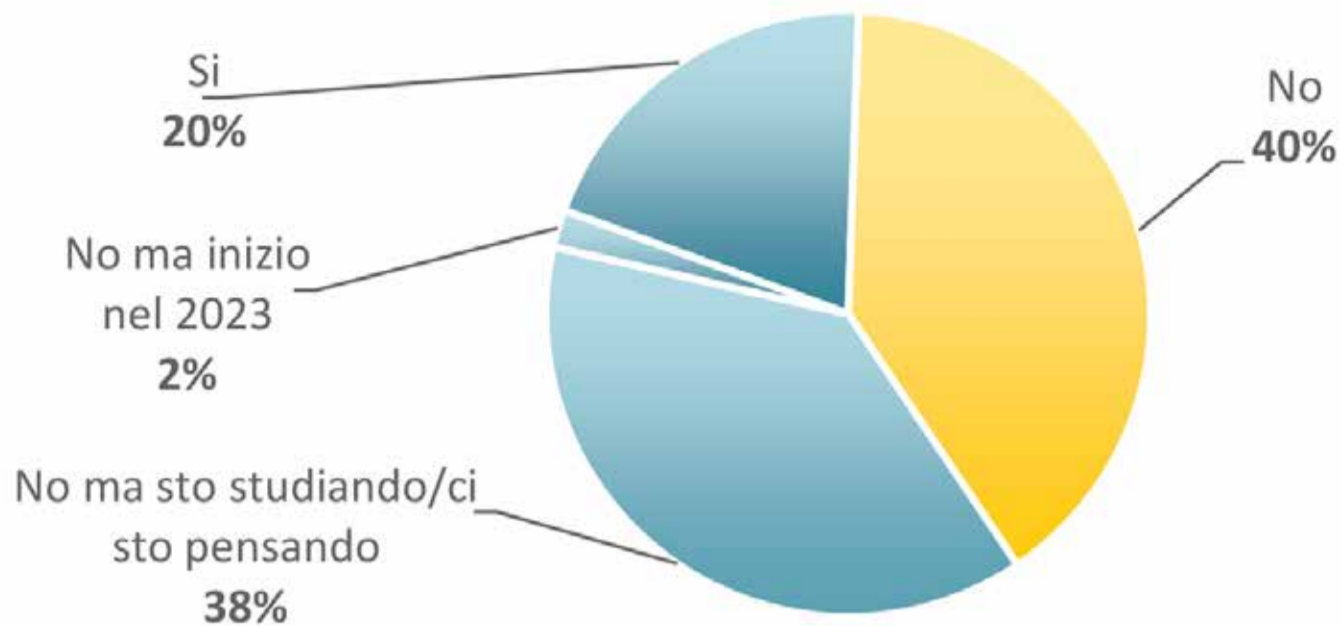
usano strumenti di PSA (Professional Software Automation) e di ticketing per la gestione del help desk (70%), mentre il 61% dei rispondenti all'indagine dichiara di utilizzare software di Networking Monitoring & Management e il 50% strumenti professionali di documentazione IT. Per i servizi che esulano dal contratto annuale, la tariffa oraria media praticata oscilla in prevalenza fra i 46 e i 60 euro (46%), ma molti (32%) puntano invece un po' più in alto, tra i 61 e gli 80 euro.

In quali settori operano gli MSP

Secondo i dati del report, la grande maggioranza degli MSP (89%) ha clienti che operano nell'ambito della produzione, mentre l'81% ha

come focus gli studi professionali. Questi dati evidenziano una maggiore efficienza operativa perché specia-

MSP che adottano soluzioni di Zero



lizzarsi in un settore permette di fornire lo stesso pacchetto di servizi a un ampio numero di clienti. **La formazione è basilare per l'MSP** che nel 53% dei casi dedica dal 6% al 10% del proprio tempo a informarsi e aggiornarsi. Ma il 26% del campione arriva anche al 20%. Gli argomenti che gli MSP cercano di approfondire sono la **cybersecurity, l'organizzazione dei processi aziendali e le attività di sales & marketing.**

La mancanza di consapevolezza dei clienti rispetto alla cybersecurity ha costretto nel 2022 il

42% degli MSP a porre rimedio ai danni provocati da attacchi ransomware, mentre il 72% ha avuto clienti colpiti da attacchi di phishing, spear phishing o Business Email Compromise. E il 24% di questi ultimi ha avuto perdite di almeno 10.000 euro. Nonostante ciò, è in controtendenza rispetto al trend globale l'impiego dello Zero Trust. Mentre nel mondo è sempre più diffuso, gli MSP italiani ne hanno ridotto l'impiego perché le limitazioni che impone possono avere un importante impatto sulle aziende.

QUANTO RENDE FARE L'MSP?

Il 63% del campione di MSP analizzato da Achab nel 2022 ha aumentato il proprio fatturato e solo il 3% lo ha diminuito. Tra chi è cresciuto, il 42% ha aumentato del 15% o più. Analogamente ha avuto il margine: il 68% degli intervistati lo ha aumentato e, tra questi, il 32% di oltre il 20%. Valutando l'anno in corso, il 73% degli MSP è convinto di poter incrementare ulteriormente il fatturato, segno che il mercato dei servizi IT è un settore in fermento e che il modello di business "as a service" aiuta a crescere anno su anno.

AFRICAN QUEENS OF CLOUD COMPUTING

Il mercato africano dei data center e dei servizi cloud sta crescendo significativamente anche in Paesi interni. Cercano connettività, bassa latenza, consulenza. E forse normativa.

di Leo Sorge

Medusa, il sistema di cavi sottomarini in fibra ottica che si estenderà per 8.700 km, è un progetto strategico per migliorare la connettività tra i Paesi dell'Unione Europea, per questo motivo la Commissione Europea ha concesso all'ATMED-DG (Atlantic -Mediterranean Data Gateway) il progetto da 7,79 milioni di euro per finanziare l'installazione di una coppia di fibra spenta tra Lisbona, Zahara de los Atunes, Barcellona, Marsiglia e Mazara del Vallo.



**COLLEGATI AL
PROGETTO MEDUSA**

Può sembrare un evento marginale, ma forse non lo è. Mentre Cina e India crescono imperiosamente, l'Europa impone normative su tecnologie che non padroneggia e cerca Nuovi Mondi sui quali far valere le proprie qualità. Orbene, la prima area di riferimento sembra essere proprio l'Africa.

L'African Cloud cresce veloce

La situazione è già molto strutturata, ma lascia ancora grandi spazi di manovra. I grandi blocchi geografici sono già organizzati,

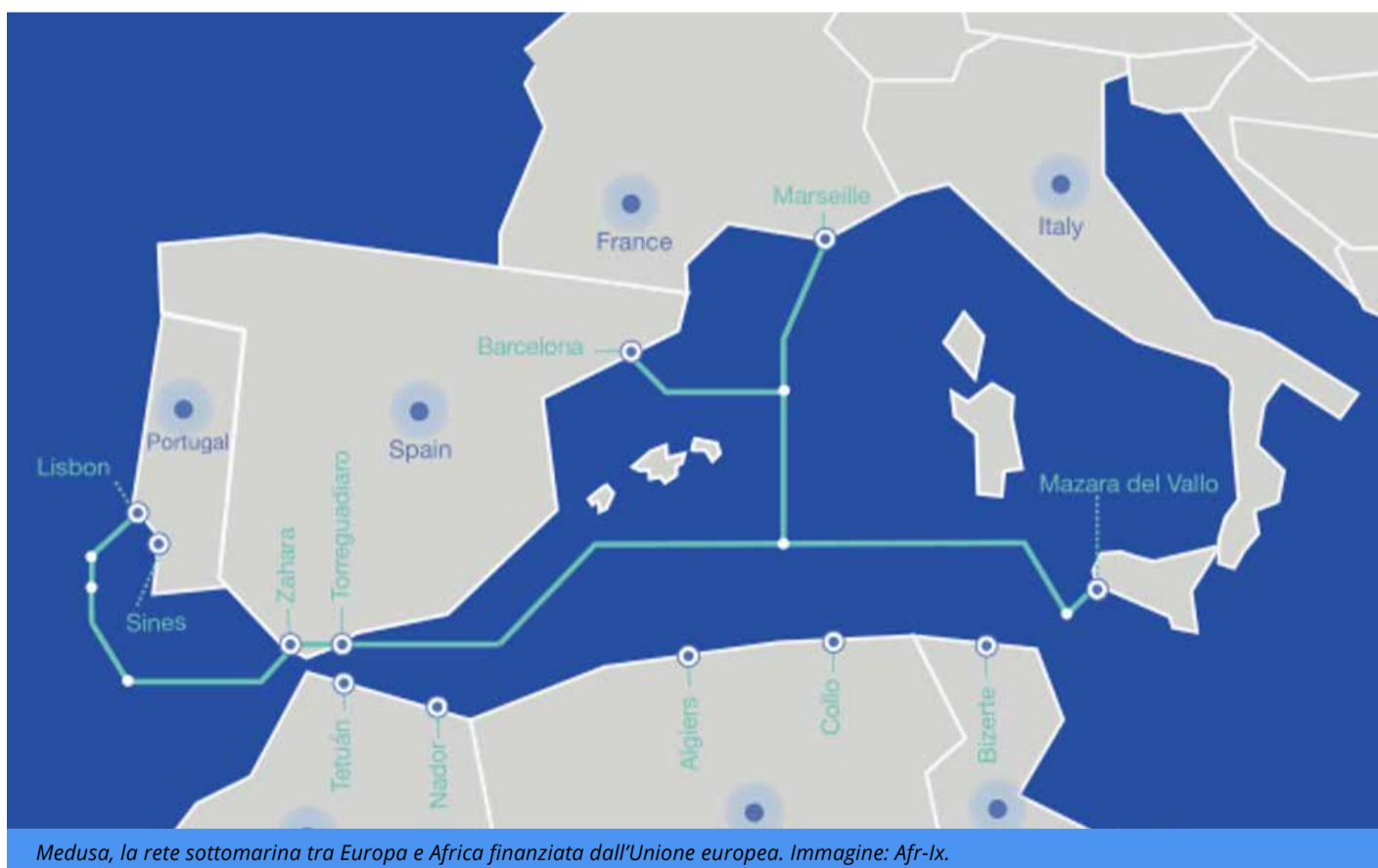
per cui Maghreb, Corno d’Africa e soprattutto Sudafrica fanno ormai storia a sé, con i loro fornitori storici. Negli ultimi anni anche Meta e Google hanno investito direttamente nella connettività e nei data center specifici di nazioni più piccole.

Secondo **ResearchAndMarkets**, il mercato africano dei soli data center (qualsiasi tier) dovrebbe crescere a un CAGR del 10,70% per superare 1,4 B\$ di dollari entro il 2028, rispetto a 0,76 B\$ nel 2022. Queste stime, che potrebbero anche richiedere un aggiornamento, aumentano di molto se si parla dei servizi. *“Una nuova generazione di data center*

in più rapida crescita al mondo”, scrive **Alexis Akwagyiram, analista per la BBC, la Reuters e il Financial Times**, facendo riferimento alla previsione relativa al 2026 (5B\$) secondo stime dell’ADCA, Associazione dei Data Center dell’Africa.

Se nel recentissimo passato l’emergere di data center locali ha alimentato un’esplosione del cloud computing in alcune delle più grandi economie dell’Africa (Nigeria, Kenya, Egitto, Sud Africa e Marocco), è giunto il momento della crescita di economie più piccole.

“Il cloud africano è un’interessante opportunità commerciale da



sta sorgendo nelle economie più piccole dell’Africa, alimentando un’opportunità di mercato di 5 miliardi di dollari nel continente

miliardi di dollari, in crescita a un tasso annuo tra il 25 e il 30%”, dice l’introduzione di The Rise of the African Cloud, il report di Xalam;

“è anche un mercato dinamico complesso, dove gli hyperscaler competono e collaborano con una serie di operatori di telecomunicazioni e fornitori di data center e specialisti del cloud”. La lunghezza dei cavi determina lunghe latenze e basso livello di servizi che si cerca di migliorare, in primis nell’area finanziaria.

Alla ricerca di talenti

Va sottolineato che l’Africa, con la sua creatività diversa da quella europea, statunitense o orientale, è un continente estremamente complesso e fortemente sconnesso, almeno in termini informatici. Molte aree non sono servite da reti fisse né mobili, e molte altre ancora hanno reti 2G e 3G, per cui si punta molto sul 5G ma anche sui cavi sottomarini e il traffico con gli altri Continenti.

I principali fornitori sono cinesi, ma per motivi storici, sono molti gli africani esperti di computer science che trovano modo di lavorare sia all’interno del loro Continente, sia al di fuori (America, Europa). Riuscire a impostare un’attività informatica di supporto alla crescita potrebbe rivelarsi un fattore di stabilizzazione geopolitica altrettanto forte di altre infrastrutture come ponti, dighe

e acquedotti e porti, in qualche modo controbilanciando altri poteri tribali o coloniali nella ricerca di un equilibrio maggiore di quello attuale.

Per motivi geografici e politici, l’African Cloud è un segmento ad alto rischio. Come visto, però, prevede una crescita alta e potenzialmente esplosiva. Non solo nel fatturato: si pensi alla guerra ai talenti che in Europa e Italia, ma anche negli States, stanno perdendo rispetto ad aree più popolose e giovani come Cina e India.

Va infine pensato che si potrebbe provare a esportare in questo enorme bacino anche il nostro impianto normativo, certo scontrandosi con usi, costumi e costi molto variabili. Uniformare aspetti come sicurezza, privacy e uso dell’IA potrebbe essere un volano formidabile per quelle economie e anche per chi le supporta.

**RIMANI AGGIORNATO
ISCRIVITI ALLA NEWSLETTER**





Red Hat guida la transizione digitale

La società americana vuole essere protagonista in questa fase, dove il mercato digitale in Italia mostra una forte crescita, con le proprie soluzioni in grado di coprire ogni esigenza in ambienti cloud privati o pubblici ed edge

di Maurizio Ferrari

La sfera di cristallo di **Red Hat** ha mostrato il (un) futuro. **Questo futuro è fatto di open source, automazione, intelligenza artificiale, cloud ed edge.** In un momento particolare, dove l'economia mondiale subisce pressioni da diversi punti, alta inflazione, la guerra in Ucraina, le tensioni commerciali tra Usa/Europa/Cina/Russia, diventa fondamentale continuare a innovare. Un percorso di innovazione dove gli investimenti devono essere fatti in modo oculato, per non disperdere risorse in progetti irrealizzabili.

I capisaldi dell'offerta

L'impegno di Red Hat e dei suoi partner è di mettere a disposizione dei propri clienti una infrastruttura in costante evoluzione, capace di intercettare i cambiamenti e le innovazioni tecnologiche e renderle subito disponibili.

L'offerta si basa dunque su questi capisaldi:

- **Framework per sviluppare applicazioni** in grado di trarre il meglio dalle architetture cloud ed edge (container, micro-servizi, machine learning, intelligenza artificiale);
- Strumenti per costruire ambienti cloud e ibridi;
- **Soluzioni per il monitoraggio** e l'automazione delle infrastrutture;
- **Soluzioni sempre più sicure** per prevenire problemi derivati da attacchi informatici;
- **Flessibilità e agilità** nell'acquistare tecnologie e servizi offerti che possono essere gestiti on premise o attraverso hyperscaler.

Soluzioni per ogni problema

L'offerta della società americana vuole rispondere così alle esigenze e ai problemi che i clienti stanno affrontando, dalla mancanza di competenze alla necessità di ridurre la complessità, dalla ridu-



TI POTREBBE INTERESSARE:



Red Hat introduce un nuovo modello di sottoscrizione gratuito per i partner

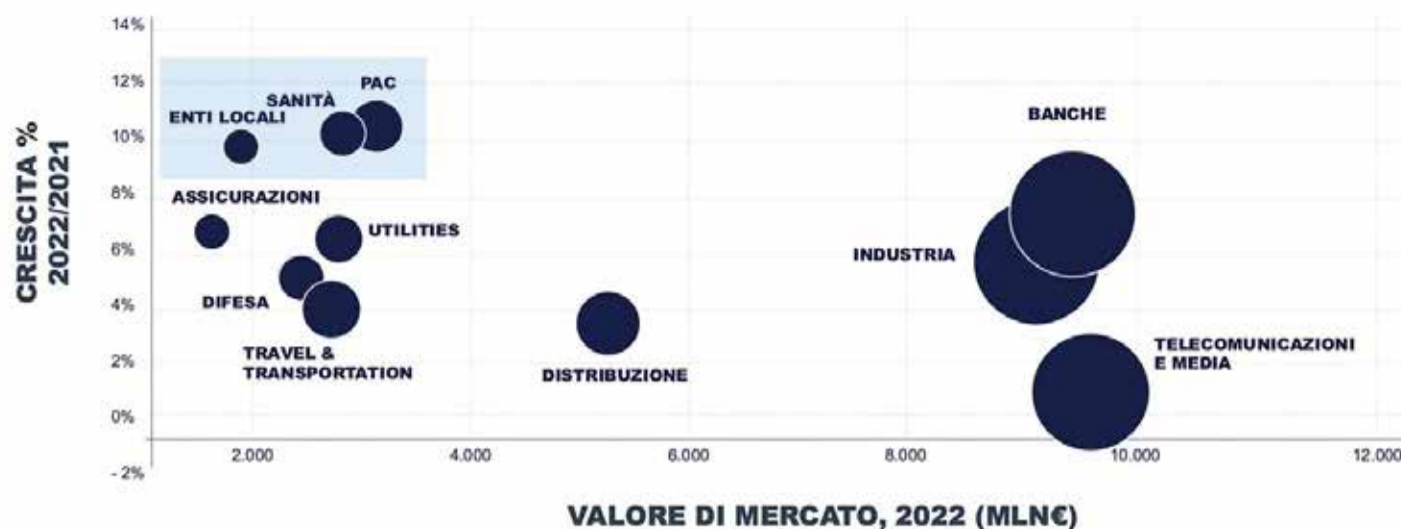
Red Hat Partner Subscriptions offre ai partner l'accesso gratuito all'intero portfolio open hybrid cloud di Red Hat

[+ continua a leggere](#)

zione dei tempi di sviluppo alla sicurezza, sino ad arrivare a soluzioni per la sostenibilità. Per ogni problema Red Hat ha una soluzione, per esempio il **Progetto Kepler**, che riguarda la sostenibilità, è in grado di analizzare le prestazioni delle Cpu e di altri parametri per stimare il consumo energetico dei Kubernetes Pods così da calcolare l'impronta di carbonio e agire in modo da ridurre (per esempio migliorando l'efficienza del codice, piantando alberi o mettendo nuovi pannelli solari per alimentare i data center).

Mercato italiano in crescita

Un approccio che ha permesso alla società americana di ritagliarsi importanti spazi nel mercato. Si sono affidati alle sue



Fonte: NetConsulting cube, 2023

soluzioni realtà diverse come Airbus, La Banque Postale (le poste francesi), Grupo Pinero (turismo spagnolo), Clalit (sanità israeliana), Akbank (banca turca), mentre in Italia troviamo per esempio Conad, Istat, Italgas. In Europa e in Italia le operazioni di Red Hat sembrano dare i loro frutti, ma la società americana non rilascia ancora numeri precisi (l'ultimo bilancio italiano disponibile è del 2021).

Analizzando con attenzione la situazione italiana, salta all'occhio il ruolo della **pubblica amministrazione che è diventata il maggior investitore** e traino in questo processo di innovazione. In questo momento tutti gli indicatori evidenziano come **il mercato digitale italiano stia crescendo più del Pil**: la stima per il 2023 vede il Pil crescere dello 0,9%, mentre questo settore farà segnare un più 3,1%.

I trend evidenziano come nel 2026 il Pil dovrebbe crescere dell'1,1%, mentre il mercato digitale del 5,5% e passare dai 79,4 miliardi di euro del 2023 ai 91,7 del 2026. L'Italia sta cercando di colmare il divario che ha con altre economie mondiali sul fronte tecnologico.

Intelligenza artificiale nel futuro

L'offerta di soluzioni firmate Red Hat permette dunque alla società della California di proporsi come player di riferimento per creare infrastrutture che vanno dal bare metal sino all'edge, passando per il cloud privato o pubblico con i principali Hyperscaler. Nel futuro prossimo di Red Hat ci sarà sempre più spazio a servizi e soluzioni che sfrutteranno l'intelligenza artificiale generativa, già presente in **Ansible Automation Platform**, così da semplificare il lavoro degli sviluppatori e degli It manager.

PFU punta anche sulla videoconferenza

di Fabrizio Pincelli

In arrivo la nuova gamma **Smart Meeting Device** di dispositivi pensati per migliorare la comunicazione durante le riunioni online. Saranno marchiati Ricoh ma venduti a livello europeo da PFU, che amplia così l'offerta al di là della "tradizionale" gestione documentale



Massimiliano Grippaldi
Regional Sales Manager di PFU



PFU annuncia la nascita della nuova categoria di prodotti **Smart Meeting Device**. Come vuole chiaramente far intuire il nome, si tratta di dispositivi intelligenti audio-video pensati per migliorare le riunioni. I primi a vedere la luce sono i **monitor portatili Ricoh 150BW e 150**, ma entro la fine dell'anno è previsto verranno lanciate altre soluzioni.

*"Grazie anche al lavoro ibrido, le riunioni online sono in continuo aumento - ha affermato **Massimiliano Grippaldi, Regional Sales Manager di PFU** - e i nostri nuovi monitor si integrano perfettamente in questo scenario".*

Un prodotto molto verticale

Grippaldi ha riconosciuto che non sono numeri enormi, ma questo perché si tratta di un prodotto che sod-

disfa un'esigenza particolare e si indirizza in modo esplicito a precise categorie professionali che hanno la necessità di un monitor portatile perché operano in mobilità o perché devono mostrare determinati contenuti ai clienti.

Il nuovo monitor ha uno schermo OLED touch da 15,6" con risoluzione 1.960x1.080 sul quale si può anche scrivere usando una penna dedicata. Può connettersi a un computer o replicare lo schermo di uno smartphone o di un tablet (iOS o Android) collegandosi tramite USB (sono disponibili due prese) oppure wireless (tramite una connessione wi-fi dedicata). Le sigle 150BW e 150 definiscono il tipo di connettività: wireless la prima, USB la seconda. **Il modello 150BW** usa una batteria che consente un'autonomia di 3 ore, ma che fa anche aumentare un po' il peso: 715 g contro 560 g del modello wired. In entrambi l'alimentazione è via USB.

Integrato nello chassis c'è un comodo supporto che consente di



Il nuovo monitor portatile Ricoh 150



TI POTREBBE INTERESSARE:



Scanner documentali: PFU presenta fi-8040, il primo a marchio Ricoh

Primo tra gli scanner documentali parte del "nuovo corso" di PFU, che mantiene una propria autonomia anche nel gruppo Ricoh, fi-8040 è indirizzato all'impiego in piccoli gruppi di lavoro e si contraddistingue per la versatilità nei collegamenti e per la semplicità d'uso



continua a leggere

posizionare il monitor sia orizzontalmente (secondo svariate inclinazioni) sia verticalmente. Il prezzo di listino è di 775 euro per il modello wireless e di 575 euro per l'altro. La penna costa 70 euro.

I primi effetti dell'acquisizione

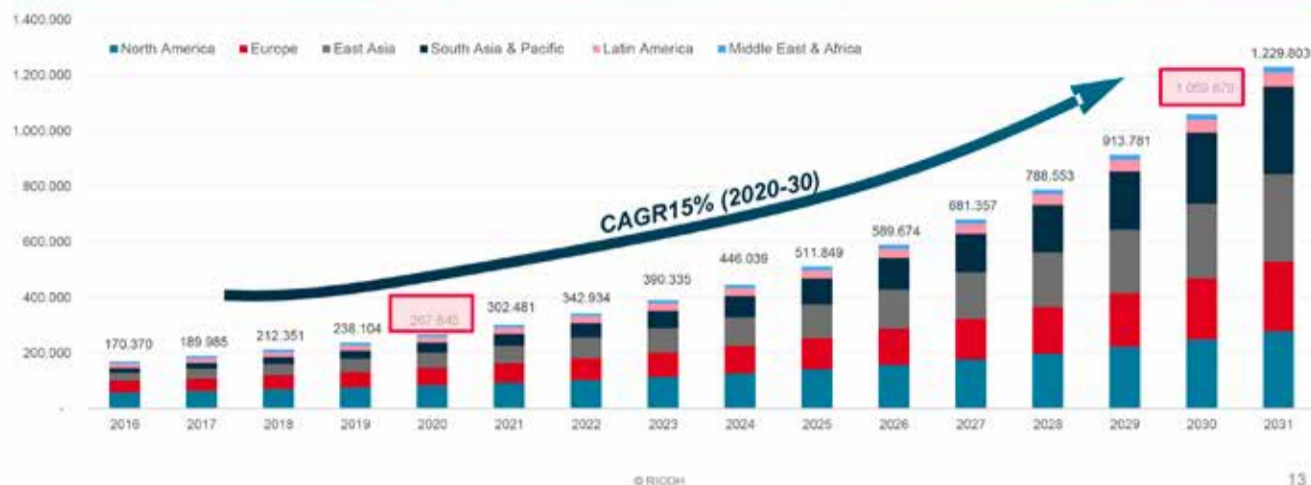
"Essere entrati nel gruppo Ricoh – ha precisato Grippaldi – ci offre la possibilità di accedere a una serie di prodotti diversi e aggiuntivi rispetto alla nostra offerta tradizionale, che consisteva in massima parte negli scanner, a cui si aggiungeva una limitata proposta di tastiere specializzate". Così, mentre Ricoh Italia e Ricoh Europe continuano a vendere le loro multifunzione e altri prodotti per la smart com-

La richiesta di monitor portatili è in crescita, trainata dall'evoluzione degli stili di lavoro

Unità vendute nel 2022:
343.000

Unità vendute nel 2030:
1.060.000

Il mercato dei monitor portatili
CAGR del 15%



munication, **PFU è stata incaricata di promuovere e commercializzare sul mercato italiano ed europeo la nuova categoria di device per rendere le riunioni più intelligenti.**

Il ruolo strategico del canale

In merito a tale scelta Grippaldi ha osservato: *“crediamo che la nostra strategia commerciale abbia avuto un ruolo centrale nella decisione. PFU ha una distribuzione molto capillare sul territorio perché da sempre usa una modalità di vendita indiretta tramite distributori e rivenditori. Questo ci permette di arrivare anche a reseller che operano in paesi o aree limitate e che sono in grado di soddisfare l'esigenza del piccolo studio*

professionale, che difficilmente può essere servito da Ricoh Italia o dai suoi corporate partner”.

Se da una parte è il canale l'elemento che ha fatto la differenza, dall'altra parte questa per il canale di PFU è una nuova opportunità. *“Con gli Smart Meeting Device andiamo a colpire un nuovo settore e quindi estendiamo oltre l'ambito documentale le possibilità di business che offriamo ai partner – ha sostenuto Grippaldi –. Ritengo sia un valore aggiunto molto importante. Oggi parliamo di un prodotto specifico, ma ne lanceremo altri, due entro l'anno, fino ad avere una categoria completa, che offrirà ai nostri partner anche la possibilità di effettuare vendite cross selling”.*

Infrastructure as Code

RIVOLUZIONE DIGITALE

L'Infrastructure as Code rappresenta un cambio di paradigma nella gestione delle infrastrutture IT, rendendo possibile una gestione più efficiente, scalabile e sicura delle risorse, attraverso l'automazione e la codificazione. Questo approccio facilita la ripetibilità dei processi, la tracciabilità delle modifiche e la velocità di risposta ai cambiamenti, che sono elementi fondamentali in un panorama IT sempre più dinamico e complesso.

di Riccardo Florio

L'Infrastructure as Code (IaC) rappresenta una delle maggiori innovazioni nel panorama della gestione delle infrastrutture IT, proponendo un approccio rivoluzionario basato sull'automazione e la codifica. Rappresenta un risultato diretto dell'evoluzione tecnologica dell'ultimo decennio, radicata nel bisogno sempre più pressante di velocità, efficienza e scalabilità nell'era del cloud computing.

Questa metodologia **tratta le infrastrutture IT esattamente come se fossero codice software**. Pertanto, gli ambienti informatici, le configurazioni, le reti e i server vengono definiti e gestiti attraverso codici scritti in linguaggi specifici. Ciò significa che tutte le operazioni che, normalmente, richiederebbero un intervento manuale, come l'installazione e la configurazione

di un server o la creazione di un ambiente di rete, vengono eseguite tramite codice.

Il processo evolutivo tecnologico

La modalità tradizionale per la gestione delle infrastrutture

IT è un processo manuale o, nella migliore delle ipotesi, semiautomatico basato su script ad hoc. Questo approccio si dimostra estremamente lento, richiedendo un tempo significativo per la configurazione e la manutenzione delle risorse IT. Inoltre, è soggetto a un elevato tasso di errori, poiché l'intervento umano nelle attività di configurazione può portare a inconsistenze e problemi di sicurezza. Infine, questo modello è scarsamente scalabile, poiché richiede lo stesso impegno lavorativo per gestire un piccolo numero di risorse o una grande infrastruttura.

L'avvento del cloud computing ha portato a un aumento esponenziale della complessità e della dimensione delle infrastrutture IT. Questo ha reso ancora più evidente la necessità di un approccio sistematico, automatizzato e scalabile alla



TI POTREBBE INTERESSARE:



Come migliorare il processo di application modernization

Partire dalla cultura per arrivare a costruire un team che condivida i dettami DevOps e, solo a questo punto, occuparsi della tecnologia. È l'approccio con cui Axiante supporta le aziende nel processo di modernizzazione di applicazioni e processi.

[+ continua a leggere](#)

gestione delle infrastrutture. L'laC è nato proprio per soddisfare questa necessità.

Anche **la diffusione della metodologia DevOps** ha contribuito alla diffusione dell'laC. Ricordiamo che DevOps è una filosofia di lavoro che mira a unire le operazioni di sviluppo (Development) e di gestione IT (Operations) allo scopo di accelerare i cicli di rilascio del software, migliorare la qualità del prodotto e promuovere la collaborazione tra team.

L'laC si inserisce perfettamente in questo quadro perché i team DevOps possono definire e gestire



TI POTREBBE
INTERESSARE

Agile e DevOps:
i modelli per uno
sviluppo collaborativo



continua a leggere

le infrastrutture usando lo stesso approccio usato per lo sviluppo del software.

Ciò significa che possono sfruttare i vantaggi del controllo versione, del testing automatizzato e della distribuzione continua anche per le infrastrutture, riducendo il tempo di rilascio e migliorando la qualità del servizio.

I vantaggi offerti dall'Infrastructure as Code

Il vantaggio principale è che questo codice **può essere scritto, testato, aggiornato, distribuito e riutilizzato, proprio come qualsiasi altro software**. Inoltre, il codice può essere salvato in "repository" di codice sorgente, come Git, consentendo la tracciabilità e la riproducibilità delle modifiche, rendendo il processo di gestione delle infrastrutture molto più veloce.

In termini di efficienza, l'automazione che l'IaC introduce **riduce notevolmente il tempo necessario per la configurazione e la gestione delle infrastrutture**.

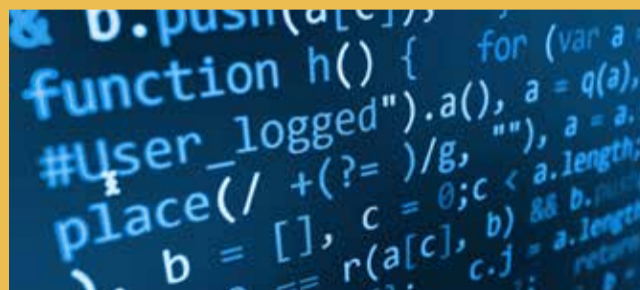
Questo permette di liberare risorse preziose che possono essere riutilizzate per altre attività all'interno dell'organizzazione.

Parallelamente, l'IaC contribuisce in modo significativo alla **riduzione degli errori** legati alla gestione manuale delle

infrastrutture e che possono compromettere la sicurezza e l'affidabilità. Utilizzando il codice per la gestione delle infrastrutture, l'IaC minimizza l'intervento umano, limitando così la possibilità di errori. La **scalabilità** è un altro aspetto fondamentale che l'IaC migliora. In un ambiente aziendale dinamico e in continuo cambiamento, la capacità di adattarsi rapidamente alle esigenze del mercato è cruciale. L'IaC facilita questo processo permettendo di **creare, modificare o eliminare intere infrastrutture con un semplice aggiornamento del codice** (cosa particolarmente utile nell'ambito del cloud computing, dove le risorse possono essere scalate su richiesta).



TI POTREBBE INTERESSARE:



DevSecOps, la sicurezza deve essere un prerequisito dello sviluppo

La metodologia DevOps è sempre più diffusa ma troppo spesso non si considera in modo adeguato l'aspetto sicurezza. Fortify permette di incorporare la sicurezza nel software sin dalle prime fasi del ciclo di sviluppo.



continua a leggere

Inoltre, l'laC **assicura la ripetibilità delle operazioni** dato che il codice utilizzato per configurare e gestire le infrastrutture può essere riutilizzato per creare ambienti identici. Ciò è estremamente vantaggioso in fase di testing e di distribuzione di nuove applicazioni, poiché consente di replicare facilmente gli stessi parametri in diversi contesti, garantendo coerenza e riducendo il rischio di anomalie o malfunzionamenti.

Le opportunità di business per le aziende

L'laC apre molteplici opportunità di business per le aziende. Innanzitutto, permette di **ridurre i costi operativi** legati alla gestione delle infrastrutture e poi, grazie alla sua scalabilità, **favorisce una rapida espansione** in linea con le opportunità che si aprono sul mercato. L'laC **facilita la digital transformation** perché le aziende possono sfruttare la sua flessibilità per migliorare la loro efficienza, innovare i loro prodotti e servizi e creare nuove opportunità di business. Tra gli esempi di strumenti che abilitano laC possiamo ricordare il **codice open source Terraform** oppure il servizio **AWS CloudFormation**, per creare una raccolta di risorse AWS e di terze parti correlate, fornirle

e gestirle in modo ordinato e prevedibile. Questi strumenti permettono di scrivere codice che descrive la configurazione desiderata delle infrastrutture e di applicare questa configurazione in modo automatico.

TERRAFORM

Terraform, sviluppato da HashiCorp, consente di definire, creare e gestire l'infrastruttura come codice. Con Terraform, è possibile descrivere le risorse infrastrutturali desiderate utilizzando il linguaggio specifico HCL, e poi utilizzare il codice per automatizzare il provisioning e la gestione delle risorse su una varietà di piattaforme, tra cui cloud provider e ambienti on-premises.



COLLEGATI
A TERRAFORM

AWS CLOUDFORMATION

AWS CloudFormation è anche esso un servizio che consente la modellazione, il provisioning e la gestione di risorse AWS e di terze parti trattando l'infrastruttura come codice.



COLLEGATI A AWS
CLOUDFORMATION

INTENT BASED NETWORKING PORTA INNOVAZIONE E AUTOMAZIONE NELLE RETI AZIENDALI

L'Intent-Based Networking (IBN) sta rivoluzionando la gestione delle reti aziendali. Scopriamo come funziona, i benefici, le sfide e i prossimi sviluppi di questa innovativa tecnologia

di Riccardo Florio

L'evoluzione delle reti informatiche è sempre stata guidata dalla necessità di adattarsi a un contesto in rapido cambiamento. L'**Intent-Based Networking (IBN)** si sta affermando come un nuovo paradigma che promette di semplificare la gestione della rete, migliorare l'efficienza e garantire sicurezza. Si tratta di **un approccio alla gestione della rete** in cui un amministratore invece di configurare manualmente ogni dispositivo, definisce l'intento, ovvero ciò che si desidera ottenere dalla rete e il sistema si occupa di implementarlo automaticamente traducendo questi intenti in configurazioni di rete automatiche e dinamiche. L'IBN trova impiego in una vasta gamma di scenari ed è particolarmente utile per le organizzazioni che gestiscono grandi reti, come data center, fornitori di servizi di rete e grandi imprese. Grazie alla sua capacità di migliorare l'efficienza e l'automazione della rete, l'IBN può contribuire a ridurre gli erro-

ri umani e a velocizzare la distribuzione dei servizi.

Questo modello di gestione si basa su tre principi cardine.

Traduzione e validazione dell'intento

Il primo passo nell'IBN è la definizione dell'intento, ovvero delle esigenze di business che la rete dovrebbe soddisfare. Questo intento può essere espresso in termini di prestazioni, sicurezza, compliance o qualsiasi altro obiettivo aziendale: per esempio, garantire la connessione ininterrotta tra due punti della rete oppure prevedere che gli utenti del dipartimento vendite possano avere accesso alle risorse X e Y ma non alla risorsa Z.

Il sistema IBN traduce queste politiche in configurazioni di rete specifiche che potrebbero includere la configurazione di VLAN, la definizione di regole del firewall, la configurazione di percorsi di routing e così via. Un passaggio importante è costituito dal processo di validazione, in cui il sistema verifica che le configurazioni di rete tradotte corrispondano all'intento originale prima di implementarle.

In questo modo gli amministratori di rete devono specificare solo ciò che vogliono ottenere e non come ottenerlo, indipendentemente dalla complessità o dal

numero di dispositivi coinvolti. La generazione automatica di configurazioni oltre ad accelerare il processo, riduce il potenziale di errori umani che sono una delle cause principali di problemi di rete.

Monitoraggio continuo della rete

Una volta implementato l'intento, il sistema IBN non si ferma. È incaricato di monitorare continuamente la rete per garantire che queste configurazioni rimangano efficaci e pertinenti nel tempo sfruttando sensori e agenti incorporati nei dispositivi di rete che raccolgano un'ampia varietà di dati (da metadati del traffico a log di sicurezza e prestazioni del sistema).

I dati raccolti vengono analizzati e correlati per generare un quadro completo dello stato della rete e in questa fase è possibile utilizzare algoritmi di machine learning e altre tecniche avanzate di analisi dei dati. Se viene rilevata una discrepanza tra l'intento e lo stato della rete, il sistema può prendere una serie di azioni correttive che possono variare da semplici notifiche agli amministratori fino a modifiche automatiche alla con-

**RIMANI AGGIORNATO
ISCRIVITI ALLA NEWSLETTER**



figurazione della rete.

Il sistema acquisisce così la capacità di validare in tempo reale se la rete sta effettivamente operando secondo gli intenti dichiarati. Inoltre, monitorando la rete in tempo reale, il sistema può identificare potenziali problemi prima che diventino criticità per predisporre una risoluzione proattiva dei problemi.

Capacità di adattamento dinamico

Mentre la traduzione dell'intento e il monitoraggio continuo della rete forniscono i fondamenti per stabilire e mantenere la configurazione della rete è la capacità di adattamento dinamico che rende una rete IBN veramente reattiva e resiliente ai cambiamenti abilitandone il pieno potenziale

In un ambiente aziendale in rapida evoluzione, con requisiti di rete che possono cambiare frequentemente, avere una rete rigida e statica può essere un ostacolo significativo. L'adattabilità è cruciale per affrontare sfide come fluttuazioni nel carico di lavoro, modifiche delle politiche di sicurezza e nuove integrazioni tecnologiche.

Utilizzando i dati forniti dal monitoraggio continuo, il sistema IBN è **in grado di rilevare eventi** che potrebbero richiedere un adattamento. Questi eventi possono es-

sere variazioni nel traffico, errori di configurazione, o anche modifiche nelle politiche aziendali.

Una volta rilevato un evento, il sistema IBN **valuta le opzioni per la migliore strategia di adattamento**. Questo processo può beneficiare di algoritmi avanzati e machine learning per prevedere l'impatto di diverse scelte.

Dopo aver preso una decisione, il sistema procede **all'implementazione delle modifiche necessarie**. Questo può significare riallocare risorse, aggiornare regole di sicurezza o, in casi estremi, riprogettare dinamicamente la topologia della rete. Le modifiche dinamiche alla configurazione della rete devono essere **gestite in modo sicuro** per evitare potenziali vulnerabilità.

Infine, il sistema **verifica che le nuove configurazioni siano efficaci e conformi** all'intento originale, assicurando che il sistema permanga in uno stato di ottimizzazione continua.

I vantaggi dell'IBN

Una delle caratteristiche più desiderate in qualsiasi infrastruttura tecnologica moderna è **l'agilità** poiché l'IBN consente alle organizzazioni di reagire rapidamente ai cambiamenti, sia che si tratti di una modifica della strategia aziendale, di requisiti normativi o di condizioni del mercato. Sup-

poniamo che un'azienda voglia espandersi in un nuovo mercato; con IBN, la configurazione della rete può essere aggiornata e scalata rapidamente per soddisfare nuove esigenze, tutto senza richiedere interventi manuali complessi da parte del team IT.

Le reti sono complesse e anche un piccolo errore nella configurazione può avere conseguenze disastrose. IBN riduce la necessità di interventi manuali, **minimizzando così il rischio di errori umani**. Gli strumenti di IBN possono monitorare costantemente la conformità delle politiche di **sicurezza**, segnalando o correggendo automaticamente le violazioni. Si consideri il caso in cui esigenza di dover implementare nuove regole di sicurezza in seguito a una minaccia emergente: IBN può automaticamente applicare queste politiche attraverso la rete, eliminando la possibilità di errori che potrebbero rendere l'organizzazione vulnerabile.

Le reti tradizionali richiedono spesso sovradimensionamento per far fronte ai picchi di carico. IBN, con il suo monitoraggio continuo e la capacità di adattamento dinamico, **permette un utilizzo più efficiente delle risorse**. Per esempio, durante periodi di alta domanda, IBN può riallocare dinamicamente risorse per garantire che le applicazioni critiche

abbiano la larghezza di banda di cui hanno bisogno.

L'IBN porta **l'automazione a un livello più avanzato**, permettendo alle organizzazioni di implementare politiche complesse con semplici dichiarazioni d'intento riducendo notevolmente il tempo e gli sforzi necessari per le operazioni di rete. Per le aziende che devono aderire a rigidi requisiti normativi, IBN può automatizzare la conformità, facilitando l'audit e riducendo il rischio di sanzioni.

IBN offre una **migliore visibilità sullo stato e le prestazioni della rete**, il che è vitale sia per la gestione operativa che per la pianificazione strategica. Con una visione chiara del traffico e dei pattern di utilizzo, le organizzazioni possono prendere decisioni più informate su come ottimizzare la rete. La capacità di adattarsi a eventi imprevisti rende anche la rete più **resiliente a guasti e interruzioni**, migliorando così la continuità aziendale.

Le sfide da affrontare

Mentre l'Intent-Based Networking (IBN) continua a ridefinire il panorama della gestione delle reti aziendali, emergono anche nuove sfide che devono essere affrontate per sfruttare appieno il potenziale di questa tecnologia. Dal mantenimento della sicurezza alla gestione della crescente

complessità, esaminiamo le principali sfide che si prospettano per l'IBN nel prossimo futuro.

Tuttavia, l'adozione dell'IBN non è priva di sfide. Il passaggio a un approccio basato sull'IBN comporta un **cambiamento radicale nel modo in cui le organizzazioni gestiscono le reti**. Inoltre, l'implementazione dell'IBN richiede una comprensione approfondita delle politiche di rete e delle capacità di traduzione dell'intento in configurazioni di rete. Infine, rimangono ancora alcuni problemi da risolvere, tra cui **l'integrazione con le infrastrutture esistenti** e l'interoperabilità tra diverse piattaforme di IBN.

Nonostante queste sfide, i futuri sviluppi dell'IBN sono promettenti.

Con l'automazione e l'adattabilità come alcune delle sue caratteristiche fondamentali, l'IBN è intrinsecamente esposto a **rischi di sicurezza** come intrusioni, manipolazioni e attacchi DDoS. La progettazione di algoritmi di apprendimento automatico e IA per rilevare e prevenire attacchi in tempo reale potrebbe essere un passo nella giusta direzione. Tuttavia, la sicurezza sarà sempre una gara tra attaccanti e difensori.

Con la crescente adozione di servizi cloud, IoT e altre tecnologie emergenti, la rete sta diventando

sempre più complessa. **Questa complessità potrebbe superare la capacità di IBN di gestirla in modo efficace**. Una formazione continua e specializzata per gli amministratori di sistema e gli ingegneri di rete potrebbe essere necessaria per gestire queste reti sempre più complesse.

L'IBN è ancora una tecnologia relativamente nuova e **l'assenza di standard industriali** può ostacolare la sua adozione su larga scala. Lo sviluppo e l'adozione di standard aperti possono facilitare l'integrazione con altre piattaforme e tecnologie, rendendo IBN più accessibile e versatile.

L'implementazione di IBN può **richiedere investimenti significativi** in hardware e software, e non tutte le organizzazioni possono essere pronte a sostenere questi costi **senza una chiara comprensione del ritorno sull'investimento (ROI)**. Strumenti di valutazione del ROI più precisi e casi studio ben documentati possono aiutare le organizzazioni a prendere decisioni informate sull'adozione di IBN.

Con l'automazione avanzata, potrebbero emergere **problemi legati alla governance dei dati e alla conformità normativa**, specialmente in settori altamente regolamentati come la sanità e la finanza. Le funzionalità di audit e tracciabilità avanzate possono es-

sere integrate nell'IBN per garantire che tutte le operazioni siano conformi ai requisiti normativi.

Gli sviluppi futuri

L'Intent-Based Networking (IBN) ha già ridefinito la gestione delle reti, offrendo automazione, agilità e una semplificazione delle operazioni IT. Ma il viaggio dell'IBN è appena iniziato. Guardando al futuro, si intravedono diverse aree in cui l'IBN potrebbe svilupparsi, migliorando ulteriormente le prestazioni, l'efficienza e la sicurezza delle reti aziendali. Esaminiamo alcune delle tendenze emergenti e dei possibili sviluppi futuri in questo campo.

L'IBN potrebbe trarre vantaggio **dall'integrazione con l'IA e il Machine Learning** per analizzare e interpretare grandi volumi di dati di rete. Questo miglioramento consentirebbe alle reti di adattarsi più rapidamente e in modo più intelligente ai cambiamenti fornendo miglioramenti nella prevenzione degli attacchi di sicurezza, ottimizzazione del traffico in tempo reale e capacità di anticipare i problemi di rete prima che si verifichino.

Con la crescente adozione delle infrastrutture cloud, l'IBN potrebbe svilupparsi per **gestire in modo più efficace ambienti multi-cloud**, fornendo una gestione e un'automazione coerenti

su diversi fornitori di servizi cloud. **Le implicazioni sono:** migliorata portabilità e scalabilità delle applicazioni; gestione semplificata delle politiche di sicurezza e conformità su diverse piattaforme cloud.

L'IBN potrebbe **evolvere verso un modello di sicurezza più proattivo**, integrando funzionalità avanzate di threat hunting e risposta automatica a incidenti. Questo porterebbe a una riduzione del tempo di esposizione a minacce informatiche e a una minore necessità di intervento manuale in caso di incidenti di sicurezza.

L'IBN potrebbe estendere il suo ambito d'intervento e di **automazione all'intero ciclo di vita** delle applicazioni, dalla distribuzione alla manutenzione, fornendo una vista olistica che va oltre la sola rete. Le implicazioni sarebbero di una distribuzione più rapida delle applicazioni e di monitoraggio e ottimizzazione delle prestazioni delle applicazioni in tempo reale. Un'ulteriore prospettiva riguarda **l'interazione e l'integrazione con l'IoT** poiché con l'aumento dell'uso dei dispositivi IoT, l'IBN dovrà gestire una maggiore complessità e variabilità delle reti permettendo una migliore gestione del carico di rete e di definire politiche di sicurezza specifiche per i dispositivi IoT.

L'inevitabile scelta dell'open innovation

di Stefano Uberti Foppa

Uno studio Capgemini offre uno spaccato importante di cosa è oggi e soprattutto sarà nei prossimi anni il ricorso delle imprese a ecosistemi di innovazione per reggere la complessità competitiva. Crederci, con investimenti e trasformazioni di processo e culturali verso un'integrazione vera, rappresenta l'unica via per raggiungere flessibilità e capacità di reggere le disruption.

Era il 2003 quando il professor Henry Chesbrough, dell'Università della California, coniò il termine "open innovation". Da allora si è usata questa espressione per definire la capacità di un'impresa di creare innovazione in modo collaborativo e sinergico con soggetti al di fuori del proprio perimetro aziendale. I modelli studiati e applicabili sono innumerevoli, ma certo è un elemento importante nella capacità innovativa dell'impresa saper integrare soggetti differenti nel proprio modus operandi, affrontando così meglio le disruption del mercato che via via si presentano e dando velocità alla propria risposta. È diventato un fenomeno strutturale alle aziende. Da quelle che perseguono una open innovation più tradizionale, svolta in prevalenza attraverso feed back continui con clienti e fornitori, a realtà che

attraverso una galassia di partner, molto eterogenei per settori, cultura, anche generazione, creano ecosistemi in grado di stimolare l'azienda all'innovazione continua. Una ricerca Capgemini svolta a livello mondiale a febbraio e marzo 2023 su un campione di 2.000 senior executive di 1.000 grandi imprese (con fatturato oltre 1 miliardo di dollari) dei principali settori merceologici che hanno in corso iniziative di open innovation, ci fornisce qualche elemento di riflessione. Lo studio ha compreso nell'analisi anche quei soggetti, 500 tra start up, università, aziende di venture capital e realtà non profit, che rappresentano il bacino di riferimento del sistema esterno dell'innovazione di impresa.

Crederci e agire con decisione

Il sistema di open innovation acquista importanza strategica soprattutto in momenti di forte volatilità e di discontinuità come quello attuale. Tuttavia la messa a punto di un sistema sinergico virtuoso è tutt'altro che semplice, complice le strutture organizzative e culturali delle imprese, spesso rigide e refrattarie ai cambiamenti e cresciute nella logica a silos autoreferenziali poco collaborativi. Per contro se la caratteristica primaria dei soggetti esterni preposti all'innovazione è la velocità e la destrutturazione organizzativa, unitamente a una

diffusa debolezza finanziaria, il rischio che questi soggetti vengano intesi come elementi esterni e soprattutto sperimentali e non siano avviati verso un reale processo di integrazione per la realizzazione di prodotti e servizi innovativi, è molto alto e diffuso. Corporate accelerator, incubatori, corporate venture capital, venture clienting, crowdsourcing, sono alcuni approcci adottati dalle aziende per sondare estensioni del proprio business in aree nuove e potenzialmente rischiose, ma la fotografia che emerge dalla ricerca traccia un quadro a velocità diverse. Da un lato esistono approcci più tradizionali con circa il 45% delle aziende che ha dichiarato risultati soddisfacenti di innovazione facendo ricorso ai continui feed back dei propri clienti e un 40% provando a innovare insieme ai fornitori. Dall'altro lato, le percentuali si riducono quando vengono analizzati processi di innovazione realizzati attraverso soggetti diversi quali università (33%), cross collaboration con aziende in segmenti diversi o competitor (31%) ed enti no profit (25%). Tuttavia quella minoranza (il 22%) che ha dichiarato risultati eccellenti e buoni (c'è un altro 31% "sopra la media") ricorrendo a ecosistemi, afferma come la vera leva strategica sia un approccio deciso alla collaborazione con realtà esterne. Cosa significa? Esplorare

partnership non convenzionali; ricercare un'innovazione attraverso la contaminazione di processi, tecnologie e culture; collaborare con competitor su aree pre competitive (cosa che fa circa il 50% dei leader contro il 36% degli "altri"); lavorare sui processi interni riadattandoli e non solo seguire la tradizionale e più sicura via di rafforzare l'attività della unit R&D che persegue un'innovazione spesso incrementale e lineare.

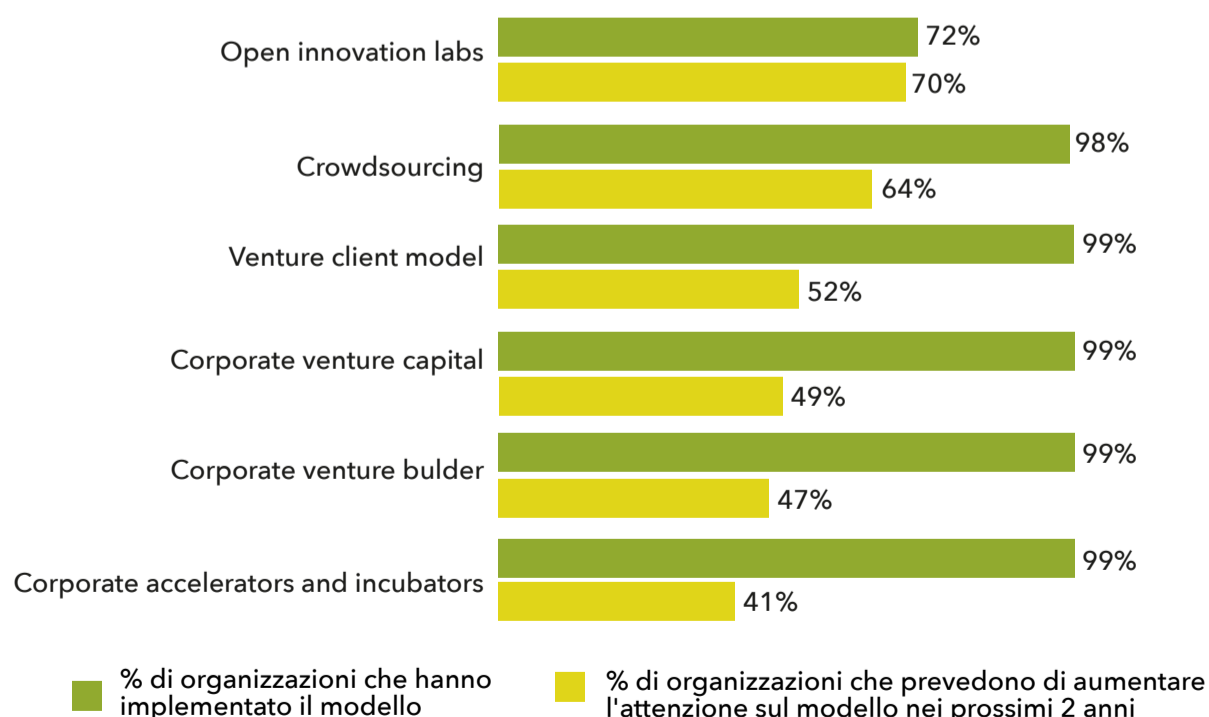
Questo approccio "deciso", segnala spartiacque tra un'azienda che affannosamente cerca di rispondere all'attuale complessità competitiva e una che invece vuole creare e cavalcare innovazione disruptive, ripensando le proprie strategie di business, trasformando le proprie supply chain, perseguendo strade di innovazione sconosciute quali,

ad esempio, la grande corsa oggi in atto verso il raggiungimento di obiettivi di sostenibilità e, attraverso questi, essere in grado di innovare e innovarsi.

Come fare per avere successo

Gran parte delle imprese è d'accordo sull'imprescindibilità di un'innovazione open. Il 75% ha affermato essere cruciale per affrontare le complesse sfide di business, tant'è che circa il 71% prevede di aumentare gli investimenti nei propri ecosistemi. I driver di questa decisione derivano dalla necessità di migliorare la propria offerta e di svilupparne di nuova; disegnare nuovi modelli di business; rendere più efficiente la spesa della propria R&D. E l'evidenza di questi obiettivi ha riguardato ben il 55% del campione, che ha dichiarato di aver incrementato

COME PENSATE CHE SI EVOLVERÀ L'ATTENZIONE DELLA VOSTRA ORGANIZZAZIONE VERSO CIASCUN MODELLO DI OPEN INNOVATION NEI PROSSIMI 2 ANNI?



Fonte: Capgemini Research Institute 2023

la propria velocità di innovazione; circa il 62% ha migliorato la flessibilità della propria forza lavoro mentre il 60% ha migliorato i propri risultati finanziari con maggiore fatturato ed efficienza operativa. Le difficoltà non mancano.

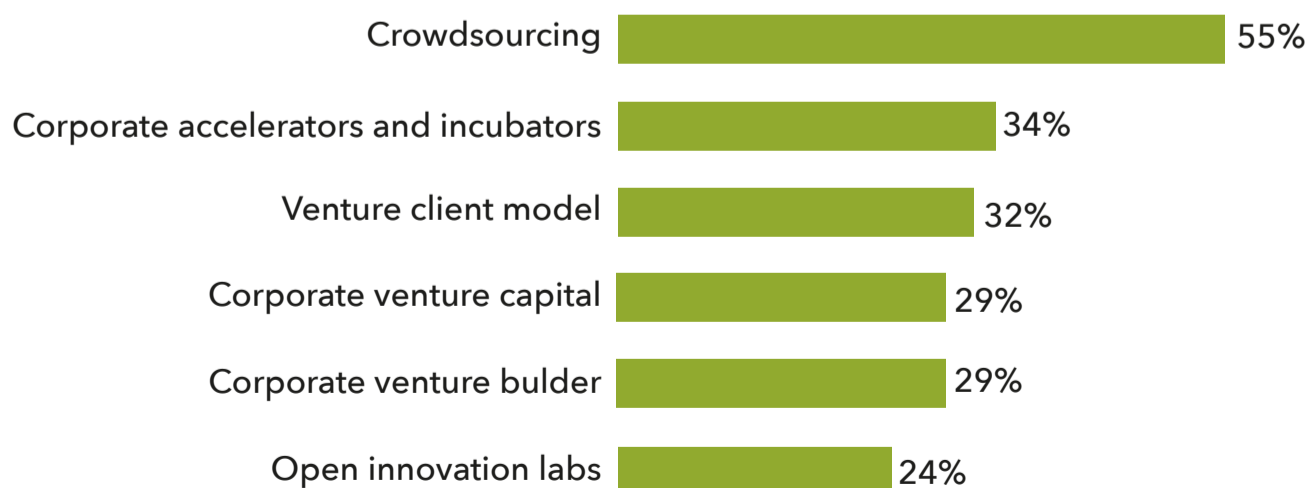
Soprattutto nell'integrazione operativa tra soggetti tanto diversi e aziende strutturate con processi consolidati. Tant'è che se da un lato il crowdsourcing (hackathon, progetti open source per la raccolta di idee su specifiche problematiche) viene preferito, per il 55%, come strumento per sondare le opportunità ma senza un grande coinvolgimento dei processi e delle strutture di impresa, dall'altro lato gli open innovation labs (innovation hub, centri di eccellenza, spazi di co-creazione in cui confluiscono su progetti congiunti startup, clienti e rappresentanti dell'impresa)

comportano difficoltà di gestione. È infatti un modello citato come preferibile da un 24% ma che ha difficoltà a tradursi in business outcome proprio perché questi laboratori operano in modo verticale e spesso disallineati alle priorità di business dell'impresa.

È quindi importante avere la forza di attuare scelte di reale trasformazione quali, ad esempio, adottare approcci diversificati per ogni tipologia di partner; definire e controllare di continuo le metriche che fissano parametri di successo; assicurare la partecipazione attiva, fin dall'inizio del processo di open innovation, dei business team; sviluppare percorsi di inserimento rapido in azienda dell'innovazione derivante dai partner; utilizzare tecnologie di analisi e di collaboration per diffondere nell'intera azienda i risultati di successo.

QUANTO SONO STATI EFFICACI PER LA VOSTRA ORGANIZZAZIONE I MODELLI DI OPEN INNOVATION?

(% DI ORGANIZZAZIONI CHE VALUTANO IL MODELLO COME EFFICACE)



Fonte: Capgemini Research Institute 2023

Strategia e competenze: la ricetta Veeam per la protezione delle aziende

di Riccardo Florio

Il rilascio del Report Ransomware 2023 da parte di Veeam è stata l'occasione per interrogarsi su come aggiornare la strategia aziendale e i relativi processi, insieme a Elena Bonvicino, Channel Manager Italy di Veeam.



Elena Bonvicino
Channel manager Italy di Veeam



Il ransomware è un attacco ai dati aziendali molto articolato, che spesso parte da un precedente, invisibile attacco ai file di backup che l'attaccante copia, cifra e spesso rivende sul mercato nero. La strutturazione mette a dura prova i processi dell'azienda attaccata. Sono moltissime le aziende, soprattutto italiane, che non hanno un approccio strategico a questo problema, confidando nella fortuna.

Questa è una grave colpa, che mina il futuro e mostra l'inadeguatezza dei processi. Ma ormai è chiaro che gli attacchi si ripetono più volte nel tempo e quindi la sopravvivenza dipende dalla capacità strategica dell'azienda.

"Noi siamo un'azienda 100% di canale, quindi ragioniamo in quest'ottica - spiega Bonvicino - e al di là dei numeri nelle aziende italiane non c'è competenza, al-

meno non quella necessaria". Può sembrare un'affermazione forte, ma non lo è: sappiamo bene che il numero di esperti di ICT e sicurezza in Italia cresce molto meno del necessario e che il grosso degli addetti ha un'età non più giovanissima.

Le competenze sono in costante aumento

Veeam ha una rete di partner variegata, che copre l'intero spettro dimensionale dalle aziende piccole a quelle più grandi.

"Quest'anno abbiamo ridisegnato l'area competenze, mostrando che la maggiore preparazione aumenta soddisfazione e retention del cliente, il fatturato per cliente, il numero di clienti e il cross selling anche interno a nuove LOBs, lines of business".

La necessità di aggiornare le competenze non solo aggiungendo informazioni, ma anche modificando la struttura di riferimento, deve essere modulata all'interno della rete di canale, rinsaldandone le maglie.

"Veeam ha saputo interpretare questo cambiamento senza snaturare la normale capacità dei nostri partner, grazie al programma Partner With Partner - , dettaglia la Channel Manager -. Il nostro portafoglio offre white labels o altro che anche un partner pubblico

può inserire in una soluzione CSP che porta miglioramenti immediati ma anche a medio/lungo termine". Questo è un esempio per piccole e medie aziende, ma Partner With Partner propone soluzioni anche per le grandi aziende. "Nel mercato enterprise i clienti hanno forti competenze e si presentano già con assessment, possibili soluzioni sia tecniche sia commerciali: è questo terreno del VASP che si confronta su pianificazione, tempificazione, project management".

Alla ricerca dell'immutabilità

Nell'ambito tecnico del backup la parola chiave è immutabilità, la tecnica che rende i dati non corrottibili su device (nastro o disco) o sul generico cloud. Parlando di immutabilità, una delle possibilità è il cloud, all'interno di un modello ibrido. *"Tra i tanti partner di Veeam non c'è nessuno che abbia fatto una trasformazione completa, ma con le giuste competenze il cloud è diventato un forte punto di "cross-selling". D'altronde il 3-2-1-1-0, regola d'oro del backup, dice che delle tre copie (su due media) una va off-site, una offline e una ha 0 errori, e l'1-1-0 è il campo di gioco proprio del cloud.*



**COLLEGATI
A VEEAM**



Secure enclave: le tecnologie di protezione dei dati a livello di chip

Le tecnologie di sicurezza a livello di chip creano un ambiente sicuro e isolato dedicato alla protezione delle informazioni. Ognuna di queste tecnologie offre un approccio unico per proteggere i dati ma, tutte, condividono un obiettivo comune: migliorare la sicurezza nel mondo digitale.

di Riccardo Florio

Nel mondo sempre più digitalizzato in cui viviamo, la protezione dei dati sensibili è diventata una priorità assoluta. Al centro di questa battaglia per la sicurezza si colloca una serie di tecnologie generalmente indicate come “secure enclave” che forniscono un’efficace protezione a livello di chip. Queste tecnologie creano regioni protette all’interno del processore

di un dispositivo ovvero aree fisicamente e logicamente separate dal resto del sistema in cui è possibile gestire dati e operazioni particolarmente sensibili. Questa separazione fornisce un livello di protezione elevato, in grado di resistere anche ad attacchi sofisticati.

L’ambito d’uso

Le tecnologie secure enclave tro-

vano impiego in diversi settori, dalla salvaguardia dei dati aziendali alla protezione delle transazioni finanziarie e sono anche diventate strumenti indispensabili nell'ambito dell'Internet of Things.

Per queste ragioni il mercato delle secure enclave sta conoscendo una crescita esponenziale e, secondo un'analisi di Markets and Markets, il mercato globale della sicurezza a livello di chip dovrebbe raggiungere un valore di **\$36,4 miliardi di dollari entro il 2025**.

Alle aziende, l'adozione di queste tecnologie può portare a una serie di benefici significativi. Oltre a garantire la sicurezza dei dati, possono favorire il raggiungimento degli obiettivi di conformità normativa, ridurre il rischio di violazioni dei dati e rafforzare la fiducia dei clienti nella gestione dei loro dati personali.

Analizziamo, di seguito, alcune delle principali tecnologie secure enclave.

Hardware Security Module (HSM)

Hardware Security Module (HSM) è un dispositivo fisico dedicato che gestisce, elabora e immagazzina informazioni sensibili, quali chiavi crittografiche, algoritmi e certi-

ficati digitali. Gli HSM sono considerati secure enclave perché offrono un ambiente isolato e protetto, separato dal software e dall'hardware general-purpose, in cui è possibile eseguire operazioni crittografiche senza rischio di esposizione a possibili minacce.

Gli HSM sono progettati per resistere a tentativi fisici di effrazione e manipolazione. Sono spesso ospitati in gusci inviolabili e possono includere meccanismi di autodistruzione delle chiavi in caso di tentativi di apertura forzata.

Gli HSM forniscono un ambiente isolato in cui le chiavi crittografiche sono separate da altri sistemi. Questo è particolarmente utile quando si trattano dati altamente sensibili, come le informazioni finanziarie o i dati dei pazienti.

Questi dispositivi sono ampiamente utilizzati nell'industria finanziaria per la protezione di transazioni e la gestione delle chiavi crittografiche e sono in grado di gestire in modo sicuro la creazione, lo storage e l'utilizzo delle chiavi utilizzate nelle operazioni di pagamento, come anche nella generazione di firme digitali per le transazioni. In un'infrastruttura a Chiave Pubblica (PKI), gli HSM possono es-

sere utilizzati per proteggere la Root CA e altre CA subordinate oppure possono essere utilizzati per memorizzare le chiavi utilizzate nell'autenticazione dei dispositivi IoT.

Physical Unclonable Function (PUF)

Physical Unclonable Function (PUF) è una tecnologia che sta guadagnando crescente attenzione per l'identificazione sicura e l'archiviazione di chiavi segrete. Le PUF utilizzano le irregolarità e le variazioni fisiche inevitabili che si verificano durante la produzione di dispositivi semiconduttori come base per generare una impronta digitale hardware unica e intrinseca per ciascun dispositivo. Ogni PUF è unica grazie alle minute variazioni fisiche nel materiale di cui è composta, come siliciumi o polimeri. Questa unicità è analoga all'unicità delle impronte digitali umane.

La struttura fisica di una PUF è tale che è praticamente impossibile da clonare, anche con l'accesso fisico al dispositivo e questo rende le PUF ideali per applicazioni che richiedono alti livelli di sicurezza.

Possono essere utilizzate per fornire un meccanismo di identificazione e autenticazione per

dispositivi in una rete e, dato che ogni PUF è unica e non clonabile, può servire come una forma affidabile di identità hardware.

Le PUF possono essere utilizzate per generare e archiviare chiavi crittografiche in modo sicuro: poiché la "chiave" è intrinsecamente legata alla struttura fisica del dispositivo è estremamente difficile da estrarre o duplicare. Le PUF possono anche essere utilizzate in soluzioni di Digital Rights Management (DRM) per garantire che solo dispositivi autorizzati possano accedere a contenuti protetti.

Trusted Platform Module (TPM)

Trusted Platform Module (TPM) è un chip di sicurezza hardware che fornisce funzioni crittografiche e di archiviazione sicura per un'ampia gamma di applicazioni e sistemi operativi. Si tratta di un componente hardware che può essere integrato direttamente nella scheda madre di un computer o fornito come un modulo esterno.

Le funzioni di base del TPM includono la generazione di chiavi crittografiche, la cifratura e la decifratura, la firma digitale e la creazione di hash. Questi servizi crittografici sono essenziali per

una varietà di applicazioni di sicurezza come l'autenticazione, l'integrità dei dati e la confidenzialità delle informazioni.

Una delle funzioni più importanti del TPM è fornire una "root of trust" hardware. Questo significa che il chip può generare e conservare chiavi crittografiche in modo sicuro all'interno di un ambiente hardware protetto. Queste chiavi possono essere utilizzate per avviare una "catena di fiducia" che si estende attraverso il sistema operativo e le applicazioni, garantendo che solo software e dati verificati possano essere eseguiti o acceduti.

TPM può essere utilizzato per garantire l'integrità del sistema: quando il sistema si avvia, il TPM può verificare che il bootloader, il sistema operativo e le applicazioni siano stati firmati digitalmente e siano integri prima di permetterne l'esecuzione. Questa funzione è particolarmente utile in scenari in cui la sicurezza è di importanza critica, come in sistemi bancari o di assistenza sanitaria.

Secure Element (SE)

Secure Element (SE) è una soluzione hardware avanzata che funge da cassaforte elettronica all'interno di un dispositivo

più ampio, come uno smartphone o una smart card. Questa sorta di fortezza digitale è progettata per isolare e proteggere dati e applicazioni sensibili da potenziali minacce, sia hardware sia software. Uno dei punti di forza del Secure Element è il suo isolamento hardware dal resto del sistema. Questa separazione fisica rende estremamente difficile per malware o altri attacchi compromettere i dati protetti. Allo stesso tempo, tutte le operazioni eseguite all'interno del Secure Element sono criptate. Le chiavi crittografiche utilizzate in questo processo sono spesso generate e memorizzate nel SE stesso, impedendo quindi la loro esportazione e l'accesso da parte di entità non autorizzate.

Il Secure Element è anche dotato di robusti meccanismi di integrità e autenticazione che assicurano che i dati e le applicazioni al suo interno siano ciò che dicono di essere. Questo è reso possibile grazie a un microcontroller dedicato che esegue un sistema operativo specializzato, spesso capace di gestire applicazioni come le applet Java Card in un ambiente di esecuzione rigorosamente controllato.

Questo concentrato di sicurezza trova applicazione in una varietà di settori. Negli smartphone e nelle carte di pagamento, per esem-

pio, gestisce informazioni critiche come numeri di carte di credito, mentre nei passaporti elettronici e nelle carte d'identità è utilizzato per memorizzare dati biometrici come impronte digitali. Le sue applicazioni si estendono anche al mondo dell'IoT, all'industria 4.0 e ai sistemi di sicurezza automobilistici.

Security Enhanced Linux (SELinux)

Security-Enhanced Linux, o più comunemente conosciuto come SELinux, rappresenta un esempio di secure enclave nel contesto del sistema operativo Linux. In un sistema Linux tradizionale, il controllo degli accessi è fondamentalmente regolato dai permessi utente e dai gruppi, che determinano chi può accedere a quali risorse e in che modo. Tuttavia, questa configurazione lascia spazio a diverse vulnerabilità, specialmente se un utente o un'applicazione riesce ad acquisire privilegi elevati, compromettendo di fatto l'intero sistema. SELinux entra in gioco per mitigare questo tipo di rischi. Nel modello SELinux ogni processo e ogni oggetto all'interno del sistema è etichettato con un'etichetta di sicurezza e l'interazione tra essi è governata da una serie di politiche di sicurezza altamente configu-

rabili. Queste regole definiscono comportamenti permessi e non permessi, restringendo l'ambito di ciò che processi e utenti possono effettivamente fare. Per esempio, anche se un'applicazione dovesse riuscire ad elevarsi a "root" (l'utente amministratore in un sistema Linux), SELinux potrebbe impedirle di compiere azioni che sono al di fuori della sua politica di sicurezza configurata, isolando così il danno potenziale.

Questa filosofia di "minimo privilegio" realizza una forma di enclave sicura all'interno del sistema operativo. I processi sono limitati a una "gabbia" di operazioni e risorse, circoscritta dalle politiche SELinux, e non possono uscire da questa gabbia senza un'autorizzazione esplicita che, in molti casi, non può essere concessa nemmeno dall'utente root. Questo è particolarmente utile in scenari come i server web, dove un'applicazione potrebbe essere esposta a un numero elevato di minacce esterne. SELinux è anche progettato per essere flessibile e configurabile: gli amministratori di sistema possono creare e modificare politiche di sicurezza per adattarle alle esigenze specifiche di un determinato ambiente, offrendo una combinazione di sicurezza e flessibilità che è difficile da raggiungere con approcci tradizionali.



Il principio del minimo privilegio e il modello Zero Trust

Non fidarsi di nessuno ed evitare di concedere a chiunque privilegi che non siano assolutamente necessari per svolgere il proprio lavoro: questi i principi necessari per garantire una protezione efficace dell'accesso

di Riccardo Florio

Il minimo privilegio è uno dei fondamenti della sicurezza Zero Trust, basato su una strategia di sicurezza focalizzata sulla garanzia che identità, persone e processi abbiano il minimo livello di permessi necessari per essere produttivi o svolgere la loro funzione.

Nel documento di "Introduzione alla sicurezza delle informazioni 800-12R1", del National Institute of Standards and Technology

(NIST) sono evidenziate i principali problemi risolvibili con il minimo privilegio.

SCARICA "INTRODUZIONE
ALLA SICUREZZA DELLE
INFORMAZIONI 800-12R1"



Tra questi vi sono gli attacchi provenienti dall'interno ed effettuati da fornitori, dipendenti e addirittura amministratori e tutti i livelli di management. Il minimo privilegio consente in queste condizioni

di limitare l'ambito del danno o degli abusi che queste figure possono infliggere a un'organizzazione.

La protezione risulta efficace anche quando il danno proveniente dall'interno non è di tipo volontario ma legato a un comportamento negligente da parte di operatori che, pur non avendo cattive intenzioni, commettono errori che espongono le loro organizzazioni al rischio. Un esempio di comportamento negligente è rappresentato dagli errori di configurazione che inavvertitamente potrebbero interrompono servizi digitali importanti o esporre informazioni sensibili al Web.

Il furto di credenziali è un'altra casistica in cui l'approccio del minimo privilegio si dimostra efficace. In questo caso, più ampio e più esteso è l'accesso di un account, maggiore è il potenziale danno per l'organizzazione: il motivo per cui gli "executive" vengono sempre più presi di mira.

Le principali cause dell'eccesso di privilegi

L'eccesso di privilegi si verifica quando un utente accumula diritti oltre quelli giustificati dal suo ruolo all'interno dell'organizzazione. Di solito, questa situazione si verifica gradualmente nel tem-

 TI POTREBBE INTERESSARE:



Cybersecurity: in Italia il livello di maturità è ancora troppo basso

 [Leggi il Report Cybersecurity Readiness Index 2023](#)

po e colpisce spesso le organizzazioni che devono proteggere le loro informazioni regolamentate o sensibili. Quando gli individui cambiano ruoli, i permessi vengono spesso concessi rapidamente per rendere le persone produttive ma, poiché le responsabilità possono persistere, i diritti precedenti vengono spesso mantenuti. Anche con richieste e approvazioni automatizzate, l'eccesso di privilegi è ancora un rischio potenziale

Le tipologie di risorse dove è necessario valutare il minimo privilegio includono: applicazioni e servizi core, dati non strutturati, sistemi e piattaforme. Spesso l'eccesso di privilegi si accumula a mano a mano che le dinamiche aziendali divergono dalle politi-

che di governance definite. I flussi di lavoro dei permessi tendono a espandersi mentre le organizzazioni si trasformano e le responsabilità si spostano.

Alcune delle fonti più comuni di eccesso di privilegi includono:

- **Approvazioni:** Gli approvatori, preferibilmente i proprietari delle informazioni, non valutano accuratamente le richieste di permessi. Gli approvatori occupati potrebbero non dedicare il tempo necessario per capire esattamente chi è l'utente che fa la richiesta e quali sono le sue esigenze.
- **Processo di revisione inadeguato:** Comprende la mancanza di revisioni regolari o quelle condotte da persone non attrezzate per valutare adeguatamente o valutare la correttezza delle richieste di accesso.
- **Utenti ad alto rischio:** Ci sono alcuni utenti per cui è molto possibile che accumulino un livello di diritti nel tempo che rappresenta un rischio inaccettabile per l'organizzazione. Ciò accade quando l'utente assume temporaneamente vari

progetti e ruoli che richiedono diritti per eseguire e tali diritti vengono successivamente mantenuti.

L'aumento progressivo dei privilegi viola uno dei principi fondamentali del modello Zero Trust.

Zero Trust

Zero Trust è un concetto di sicurezza che adotta un approccio proattivo, verificando continuamente dispositivi, servizi e individui, invece di fidarsi ciecamente di essi. Il modello Zero Trust si basa sull'assunto di un'azienda che tutto ciò che è collegato al suo sistema necessita di verifica, che provenga da qualcuno o qualcosa, all'interno o all'esterno dell'organizzazione.

Mentre la sicurezza di rete tradizionale si è concentrata su limitare l'accesso a identità esterne alla rete, la sicurezza Zero Trust coinvolge il monitoraggio continuo di tutte le identità per verificare l'accesso e i privilegi. È, in ultima analisi, un elemento fondamentale della trasformazione digitale delle aziende che cercano di migliorare la loro sicurezza informatica.



TI POTREBBE
INTERESSARE

Zero Trust per rendere
sicura tutta la supply
chain



continua
a leggere

Di conseguenza, una rete Zero Trust si basa sulla filosofia secondo la quale, poiché gli aggressori possono trovarsi sia all'interno sia all'esterno della rete, nessuna identità dovrebbe avere accesso automatico.

Alcuni componenti chiave per implementare un modello Zero Trust sono i seguenti:

- **Autenticazione Multi-Fattore (MFA):** richiede vari modi per confermare un'identità prima di concedere l'accesso; tale conferma può includere domande di sicurezza, conferma via email, messaggi di testo e altro ancora.
- **Monitoraggio in tempo reale:** valuta costantemente una rete per rilevare intrusi e limitare i danni che possono essere causati se un sistema è compromesso. Il monitoraggio in tempo reale è fondamentale per mitigare i danni quando le misure preventive non hanno funzionato e bloccare gli spostamenti laterali
- **Microsegmentazione:** questa tecnica entra in gioco quando un sistema è stato penetrato e consiste nel creare piccoli segmenti di ogni parte della rete. Creando diversi perimetri all'interno della rete, un hacker non può accedere alla rete oltre il piccolo microsegmento

che è stato penetrato.

- **Zone di Fiducia e Audit dei controlli di accesso predefiniti:** le reti possono essere suddivise in zone di sicurezza o di fiducia come parte del TIC 3.0 per consentire agli utenti di condividere dati all'interno della zona. Questo aiuta ulteriormente a prevenire che gli intrusi accedano a dati aggiuntivi. Ovviamente, le zone di fiducia sono efficaci solo se tutte le richieste di accesso ai sistemi e alle zone sono crittografate e autorizzate come parte dell'accesso predefinito.

Le sfide dell'implementazione Zero Trust

L'architettura Zero Trust può senza dubbio migliorare la sicurezza della tua azienda, ma ci sono alcune sfide nell'implementare questo concetto di sicurezza.

Innanzitutto va evidenziato l'elevato livello di impegno richiesto. I controlli predefiniti e l'accessibilità devono essere monitorati e aggiornati regolarmente e questo include quando gli utenti passano a nuovi ruoli e necessitano di accesso a parti diverse della rete. Le aziende devono avere una visione completa di tutte le identità e dei requisiti di sicurezza, e aggiornare immediatamente i cambiamenti. Qualsiasi ritardo

nell'aggiornamento dei controlli potrebbe lasciare dati sensibili vulnerabili a terze parti.

Alcune applicazioni essenziali (come i sistemi HR) sono necessarie per il funzionamento quotidiano di un'azienda, ma sono generalmente escluse dal modello di sicurezza Zero Trust. I sistemi più vecchi che sono già in uso spesso non possono essere protetti dai sistemi di verifica. Di conseguenza, le app preesistenti possono rappresentare un punto debole nel sistema di sicurezza e ridurre il vantaggio del passaggio a Zero Trust. Quando si adottano soluzioni Zero Trust, le app precedenti potrebbero dover essere sostituite o rielaborate, il che potrebbe aumentare i costi della transizione.

Infine, alcune aziende potrebbero avere difficoltà a dimostrare la compliance se non sono in grado di rendere i dati accessibili. Le regolamentazioni sono state lente a cambiare per tener conto dello Zero Trust, ma dovrebbe essere solo questione di tempo.

Implementare un'architettura Zero Trust

La transizione allo Zero Trust è un processo continuo, e tutti gli utenti devono essere consapevoli di questo fatto. Sapere che sono in corso cambiamenti può aiu-

tare tutti gli utenti a metterli in pratica rapidamente per evitare interruzioni nel flusso di lavoro.

Di conseguenza, per implementare un modello Zero Trust lo si dovrebbe render un compito organizzativo, coinvolgendo tutti i manager e aiutandoli a informare adeguatamente i loro team e a avviare una discussione su quali parti della rete dovrebbero essere prioritarie nella transizione.

Una valutazione accurata del sistema è necessaria per identificare i dati sensibili e i sistemi e prendere consapevolezza dei gap di sicurezza nell'infrastruttura esistente. È essenziale mappare dove si trovano i dati importanti e quali utenti devono essere in grado di accedervi, prendendo anche nota di come i dati e gli asset sono condivisi e resi sicuri e della loro compatibilità una volta implementata la microsegmentazione.

Infine è essenziale rendere Zero Trust parte della trasformazione digitale complessiva. Man mano che le aziende si spostano verso il cloud e incorporano l'IoT, è ragionevole che decidano di passare a un modello Zero Trust perché così facendo forniranno un livello di sicurezza migliorato all'ecosistema e copriranno anche le tecnologie legacy durante la transizione.

bizzIT.it

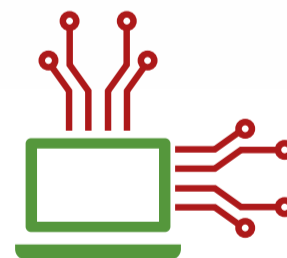
MAGAZINE ONLINE
DI ICT E TECNOLOGIA



INFORMATION



COMMUNICATION



TECHNOLOGY

bizzIT.it è la rivista online che ti aggiorna con notizie, analisi, report, approfondimenti, interviste e case history dedicati all'ICT e alla tecnologia.



Continua
a seguirci su:
<https://bizzit.it/>