

PARTNERS

INFORMAZIONE E FORMAZIONE PER IL CANALE A VALORE



Internet of Things trasforma i dati in decisioni aziendali

INCHIESTA

L'IMPORTANZA DELLA FORMAZIONE TECNICA E DELLE CERTIFICAZIONI



INTERVISTA

- ▶ ADESSO.IT PARTNER PER LO SVILUPPO AGILE

PROFILI

- ▶ OVH E NEXID UNA SINERGIA CHE CREA LA TRASFORMAZIONE DIGITALE

SICUREZZA

- ▶ OPENTEXT: SOLUZIONI PER AFFRONTARE LE MINACCE INTERNE
- ▶ WITHSECURE: TECNOLOGIE E SERVIZI PER LA SICUREZZA A MISURA DI MID-MARKET

03. EDITORIALE

Autofagocitosi delle informazioni: l'AI che si nutre di sé stessa

05. FOCUS TECNOLOGIE

Internet of Things: trasformare i dati in decisioni aziendali

La tecnologia che abilita la potenzialità dell'IoT

12. PROFILI

OVH e **NEXiD**, un motore di trasformazione digitale

16. Cips Informatica spiega la NIS2 nel suo roadshow

22. CYBERSECURITY

OpenText: ArcSight Intelligence e CrowdStrike Falcon insieme contro le minacce interne

25. SentinelOne aiuta a proteggere le identità

27. WithSecure: rafforzare la cybersecurity puntando al mid-market

29. TECNOLOGIE

Microservizi: vantaggi, sfide e best practice

33. INTERVISTA

Carmen Palumo di WithSecure



36. INTERVISTA

Francesco Micotti di Adesso.it

39. CANALE

VMware-Broadcom: quale futuro per la virtualizzazione

42. TECNOLOGIE

Formlabs rivoluziona la stampa 3D con Form 4

44. INCHIESTA CANALE

Conoscenza e competenza premianti sul mercato

PARTNERS

Anno XIII - numero 62
Giugno 2024

Direttore responsabile: Riccardo Florio
In redazione: Riccardo Florio, Paola Rosa

Hanno collaborato: Maurizio Ferrari, Fabrizio Pincelli, Leo Sorge

Redazione:

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

Editore:

Reportec Srl, C.so Italia 50 | 20122 Milano

Diffusione: 35.000 copie 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



RICCARDO FLORIO
DIRETTORE RESPONSABILE

Autofagocitosi delle informazioni: l'AI che si nutre di sé stessa

L'autofagocitosi delle informazioni è un fenomeno emergente nel contesto dell'intelligenza artificiale che si verifica quando **i contenuti generati da AI vengono poi utilizzati come dati di addestramento per ulteriori algoritmi di AI**. Questo ciclo può potenzialmente portare a una serie di complicazioni, tra cui la riduzione della diversità informativa e il rischio di amplificazione degli errori iniziali.

Quando l'AI genera contenuti basati su dati raccolti da Internet, che a loro volta sono stati prodotti da altre AI, si crea un ciclo di retro alimentazione che può essere sia positivo sia negativo. Da un lato, questo processo può affinare la capacità degli algoritmi di produrre risultati sempre più accurati e pertinenti. Dall'altro lato, se i dati iniziali contengono bias o errori, questi possono essere perpetuati e amplificati, portando a contenuti distorti o fuorvianti.

Uno dei rischi maggiori di questa autofagocitosi informativa è **l'omogeneizzazione dei contenuti**. Se gli algoritmi di AI sono costantemente alimentati e addestrati con dati derivanti da un pool limitato di fonti, la diversità dei contenuti prodotti può drasticamente diminuire.

L'impatto sull'originalità e l'espressione creativa

Nel settore creativo, l'autofagocitosi delle informazioni **può limitare l'innovazione**. L'intelligenza artificiale ha il potenziale di trasformare radicalmente i campi creativi, dalla scrittura alla musica, dall'arte visiva al design. L'AI può analizzare enormi quantità di dati e identificare



schemi che possono essere replicati o combinati per creare nuove opere. Questo può risultare in una produzione più rapida e in una maggior quantità di contenuti creativi, ma solleva dubbi sulla loro originalità.

L'AI che genera **contenuti artistici** basandosi su opere preesistenti può tendere a produrre lavori che riflettono stili e temi già noti, senza introdurre elementi veramente innovativi, venendo a mancare quel tocco unico e personale che è la firma di un vero artista.

In ambiti come il **giornalismo**, l'omogeneizzazione dei contenuti potrebbe ridurre la pluralità delle prospettive e delle voci, essenziale non solo per un'informazione di qualità ma anche per alimentare un sano dibattito critico.

Nel campo della **letteratura**, l'AI è già significativamente utilizzata per supportare gli autori nella fase di brainstorming e nella strutturazione delle trame e persino per generare testi narrativi completi basati su parametri definiti dagli scrittori.

Insomma, se le opere sono generate principalmente da algoritmi che tendono a seguire formule basate su ciò che è stato popolare in passato, ciò potrebbe limitare la diversità stilistica e tematica, portando a una saturazione del mercato con opere simili, riducendo l'interesse e il valore percepito dell'arte e della letteratura, diminuendo il valore dell'informazione.

Emerge, da quanto detto, la necessità di approntare una **diversificazione delle fonti di input usati per addestrare per l'AI**. Alimentare gli algoritmi con un ampio spettro di input creativi provenienti da diverse culture e sottoculture può evitare la ridondanza e promuovere una maggiore diversità nei contenuti generati. Questo non solo arricchirà l'output dell'AI, ma assicurerà anche che il risultato delle elaborazioni dell'AI risulti influenzato da una gamma più vasta di esperienze e prospettive umane.



Internet of Things: trasformare i dati in decisioni aziendali

I dispositivi intelligenti dell'IoT si ritrovano ormai in ogni settore perché hanno la capacità di portare innovazione migliorando i flussi di lavoro e incrementando la competitività. Tutto questo grazie alla capacità di estrarre preziose informazioni dagli innumerevoli dati raccolti, che aiutano a prendere decisioni migliori per il business

di Fabrizio Pincelli

Il mondo intorno a noi è sempre più interconnesso grazie alla crescita dell'Internet of Things, una vasta rete di oggetti fisici, dispositivi e macchine dotati di sensori, software e connettività Internet. Questi dispositivi intelligenti raccolgono e scambiano dati, potendo prendere decisioni autonome e svolgere compiti per migliorare la nostra vita quotidiana.

Non stiamo parlando di robot, ma di device capaci di integrarsi perfettamente nelle nostre esperienze quotidiane. Questo può essere il caso di un'abitazione dove luci,

elettrodomestici e sistemi di sicurezza sono interconnessi e controllabili tramite un'applicazione per smartphone. Oppure di una città con infrastrutture intelligenti che ottimizzano il traffico e risparmiano energia. L'IoT permette di creare un **ecosistema connesso in cui convenienza, efficienza e sostenibilità coesistono** armoniosamente.

IoT, un impatto a tutto tondo su ogni settore

L'impatto dell'IoT è tale che sta trasformando molteplici settori, rivo-

luzionando le tradizionali procedure e aprendo nuove opportunità. Per esempio, nel caso del **manifatturiero, il ricorso all'IoT consente di creare fabbriche intelligenti**, dove le macchine comunicano tra loro ottimizzando i processi produttivi in tempo reale. Questo migliora le operazioni, riduce i costi e aumenta la qualità del prodotto, portando a maggiori efficienza e competitività.

L'IoT rivoluziona anche il settore **sanitario connettendo dispositivi medici**, monitorando i dati dei pazienti a distanza e permettendo consulenze remote. In tal modo si migliora l'assistenza, si può fornire una diagnosi precoce e più precisa e si aumenta l'efficienza complessiva della cura medica.

Anche i **trasporti e la logistica** possono trarre benefici dal ricorso all'IoT. Si possono infatti creare sistemi di trasporto intelligenti, permettendo il monitoraggio in tempo reale dei veicoli, l'ottimizzazione delle rotte e il miglioramento della sicurezza. Inoltre, l'IoT riveste un

ruolo critico nella **gestione della supply chain**, tracciando l'inventario, migliorando le operazioni logistiche e riducendo le interruzioni. L'IoT non è però pensato solo per il mondo industriale. Anche l'**agricoltura**, un settore che sempre più spesso si avvale di infrastrutture IT, può avvantaggiarsi dell'Internet of Things. Il suo impiego, per esempio, può potenziare le coltivazioni di precisione, raccogliendo dati sulle condizioni del suolo, sui modelli meteorologici e sulla salute delle colture. Questo approccio ottimizza l'impiego delle risorse, migliora i raccolti e promuove pratiche sostenibili.

Nell'ambito del **retail, l'IoT può migliorare la customer experience**, consentendo marketing personalizzato, gestione intelligente dell'inventario e processi di pagamento fluidi. Inoltre, può offrire preziose informazioni sul comportamento dei clienti, aumentando la soddisfazione e le vendite.

È il momento di puntare sull'IoT

Il mondo dell'IoT sta evolvendo rapidamente e i benefici che la sua adozione può comportare sono molteplici. È il momento di agire. Le aziende che non seguono il trend rischiano di rimanere indietro rispetto ai concorrenti. E sembra che ne siano ben consapevoli. Prova ne è che il mercato dei dispositivi IoT sta conoscendo un periodo di importante crescita. **IDC stima che le imprese europee dovrebbero investire circa 260 miliardi di dollari** in soluzioni le-



L'APPROFONDIMENTO

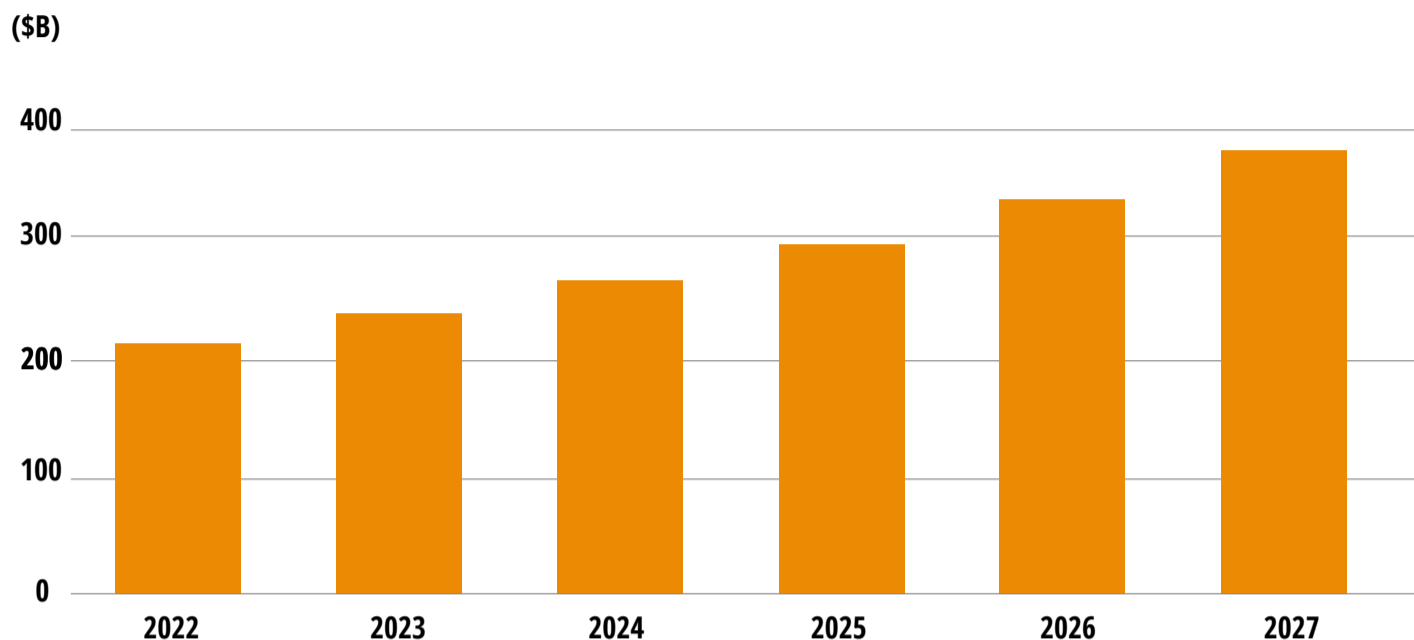


La tecnologia porta la sostenibilità nei campi

[+ continua a leggere](#)

PREVISIONI DI SPESA IOT IN EUROPA 2022-2028

Fonte: IDC



gate all'Internet of Things nel 2024. Dopo una leggera decelerazione negli ultimi due anni, causata dagli effetti degli eventi geopolitici e macroeconomici sull'economia europea, IDC prevede che la spesa IoT riprenderà gradualmente slancio nel 2024, registrando un tasso di crescita annuale composto (CAGR) quinquennale dell'11,8%, arrivando a sfiorare i 368 miliardi di dollari entro il 2027.

Secondo i più recenti dati dell'Osservatorio Internet of Things del Politecnico di Milano, **in Italia nel 2022 il mercato dell'Internet of Things è arrivato a toccare 8,3 miliardi di euro**, con un aumento del 13% rispetto all'anno precedente. Un ulteriore segnale che le aziende iniziano a intravedere il potenziale legato ai dati resi disponibili dai dispositivi intelligenti. Questo si traduce in un vantaggio competitivo ottenuto attraverso l'offerta di prodotti e servizi innovativi, grazie

anche al fatto che disporre di una grande quantità di dati "azionabili", permette di prendere decisioni informate, basate su fatti concreti e non solo su intuizioni. L'IoT consente anche il monitoraggio e l'analisi in tempo reale, ottimizzando i processi, riducendo i tempi di inattività e migliorando l'efficienza complessiva. Questo si traduce in risparmi sui costi e nell'aumento della produttività.



L'APPROFONDIMENTO



IT-OT: l'integrazione che guida l'industria 4.0



continua a leggere

Un aspetto cruciale: la sicurezza di dati e privacy

Assieme ai tanti vantaggi che comporta l'aumento dell'utilizzo dei dispositivi IoT, c'è anche un importante aspetto negativo: spesso i sistemi IoT presentano vulnerabilità, sia software sia hardware.

I dispositivi IoT spesso utilizzano software e firmware obsoleti non aggiornati con le ultime patch di sicurezza. I produttori devono dare priorità agli aggiornamenti e alle patch regolari del software, mantenendo così i dispositivi protetti contro le minacce emergenti.

Le pratiche di codifica inadeguate rappresentano un ulteriore problema, poiché lasciano il codice aperto agli exploit. Gli sviluppatori devono seguire le migliori pratiche, includendo test regolari e gli aggiornamenti necessari per garantire la sicurezza del software. Inoltre, alcuni dispositivi IoT possono avere backdoor inserite nel firmware per scopi di debug, ma queste possono essere sfruttate dai cyber criminali. È fondamentale eliminarle una volta terminata la fase di sviluppo.

Analogamente, l'insufficienza dei test durante lo sviluppo può far passare inosservati bug che diventano evidenti solo durante l'uso reale, rendendo inefficaci le misure contro gli attacchi zero-day. Procedure di test rigorose e continue sono necessarie per migliorare la sicurezza.

Un rischio chiave è l'uso di password predefinite o deboli, che rende i dispositivi facili bersagli per gli hacker. La mancan-

za di crittografia nei trasferimenti di dati espone informazioni sensibili, rendendole vulnerabili agli attacchi. È essenziale implementare protocolli di crittografia robusti per proteggere i dati sia trasmessi sia archiviati. Inoltre, l'accesso condiviso tra dispositivi intelligenti connessi amplia la superficie di attacco e implementare meccanismi di autenticazione forti, come l'autenticazione a più fattori o i certificati digitali diventa cruciale per garantire la sicurezza delle reti. Infine, l'incoerenza degli standard di sicurezza tra le diverse regioni rappresenta una sfida globale. I produttori devono collaborare con associazioni di settore ed enti normativi per sviluppare standard comuni basati sulle best practice, promuovendo una maggiore coerenza nelle leggi globali sulla cyber security.

Questo dovrebbe valere anche per la privacy. Infatti, la raccolta massiccia di dati che consentono i dispositivi dell'Internet of Things aumenta il rischio di violazioni della privacy degli utenti. In tal senso, esistono delle normative che inducono già a una sorta di standardizzazione, che si traduce nell'obbligo per tutti di rispettare le leggi vigenti, come per esempio il GDPR. Però, di nuovo, anche se perseguono il medesimo fine, non sono esattamente uno standard a livello globale.

La tecnologia che abilita la potenzialità dell'loT

È innegabile che oggi il ricorso all'loT abiliti innumerevoli applicazioni che erano impensabili solo poco tempo fa. Un ruolo basilare nell'ottenere questi risultati lo riveste l'evoluzione tecnologica, soprattutto la disponibilità del 5G e dell'edge computing, ma anche l'integrazione dell'intelligenza artificiale e del machine learning

di Fabrizio Pincelli

All'esplosione del ricorso all'Internet of Things ha sicuramente contribuito l'evoluzione tecnologica. In particolare, la disponibilità delle **reti 5G e le tecnologie di edge computing hanno consentito connessioni più veloci**, sbloccando nuovi casi d'uso in vari settori. Inoltre, l'impiego dell'intelligenza artificiale e del machine learning ha fornito la possibilità di eseguire analisi avanzate e di ottenere capacità predittive.

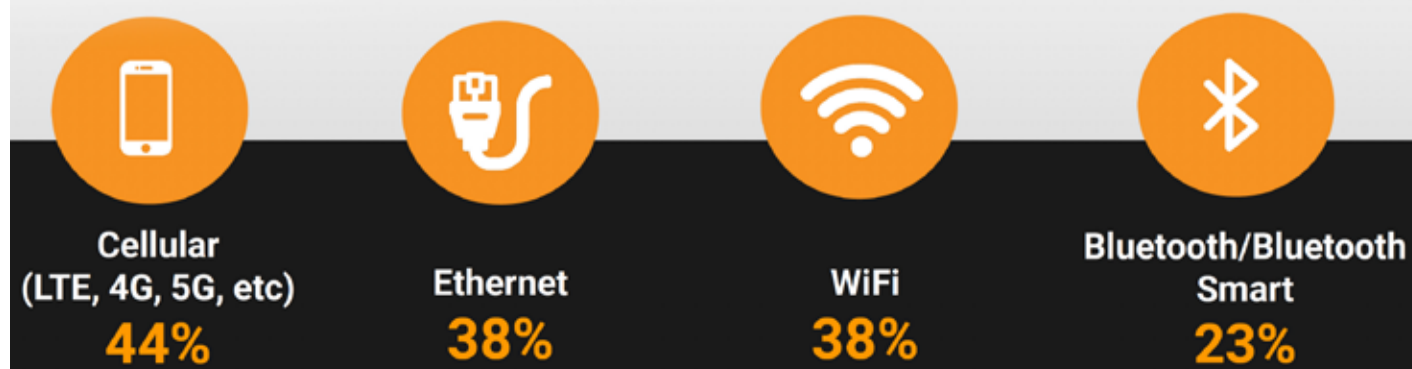
La potenza del 5G e dell'edge computing

L'emergere delle reti 5G e delle tecnologie di edge computing ha accelerato la connettività loT, garantendo bassa latenza, connessioni rapide ed elaborazione immediata

dei dati. Questi progressi stanno alimentando la crescita e il potenziale delle applicazioni loT, consentendo collegamenti più veloci e affidabili, una maggiore larghezza di banda, download più rapidi e una minore latenza dei dispositivi. Inoltre, la connettività è più affidabile e la copertura viene estesa anche ad aree che potrebbero non avere un'infrastruttura wireless adeguata. Questa migliore connettività apre la via a nuove possibilità per le applicazioni loT, dalle infrastrutture delle città intelligenti alle soluzioni sanitarie avanzate fino alle applicazioni nell'ambito dell'agricoltura intelligente. Dal canto suo, l'edge computing consente l'elaborazione dei dati più vicino ai dispositivi loT, migliorando ulteriormente latenza,

Principali tecnologie di connettività utilizzate

Fonte: Eclipse Foundation



sicurezza e scalabilità. Distribuendo le risorse di elaborazione vicino all'utente finale, l'edge computing riduce la distanza che i dati devono percorrere, con tempi di risposta più rapidi e utilizzo ottimizzato della larghezza di banda. Questo approccio decentralizzato migliora anche la sicurezza e la privacy, poiché i dati vengono elaborati e analizzati ai margini della rete, attenuando le minacce e le vulnerabilità.

L'integrazione di intelligenza artificiale e machine learning

A estrarre utili indicazioni dalla grande quantità di dati che consente di raccogliere l'IoT ci pensano **l'intelligenza artificiale (IA) e il machine learning (ML)**. Sono queste tecnologie che si fanno carico di effettuare analisi sofisticate, che rendono disponibili funzionalità predittive e che permettono di avere processi decisionali intelligenti. Elaborando e analizzando l'enorme mole di informazioni generate dai dispositivi IoT, IA e ML sbloccano nuove intuizioni e opportunità, stimolando l'innovazione e trasformando i modelli di business tradizionali.

Questo abilita molteplici applicazioni, come, per esempio, la manutenzione predittiva, ovvero la possibilità di rilevare segnali anomali dai macchinari e prevenire guasti inattesi. Questo permette di **intervenire in momenti in cui il fermo non impatta** in modo sostanziale sul flusso di lavoro e anche di avere macchine sempre al massimo dell'efficienza. In modo analogo, ma agendo in tutt'altro ambito, i

dati raccolti dai sensori possono consentire di **intuire le preferenze di un consumatore in fase di acquisto** e quindi suggerirgli i prodotti potenzialmente di maggiore interesse. L'insieme di intelligenza artificiale e machine learning potrebbe poi essere impiegato per avere un'efficace gestione del **traffico all'interno di una smart city**. In tal senso, con le informazioni ricevute dalle telecamere intelligenti i software di video analytics possono rielaborare le immagini e riconoscere situazioni di pericolo, segnalandole. Le applicazioni IoT e di machine learning stanno rivoluzionando diversi settori, dalle auto a guida autonoma agli elettrodomestici intelligenti, fino all'automazione industriale. Sfruttando le tecnologie di intelligenza artificiale e di apprendimento automatico, i dispositivi IoT possono imparare dall'ambiente circostante, adattarsi alle preferenze degli utenti e prendere decisioni intelligenti.

La fusione di intelligenza artificiale e machine learning con i sistemi IoT consente alle organizzazioni di prendere decisioni informate, aumentare l'efficienza operativa, migliorare l'esperienza degli utenti, garantire la sicurezza e promuovere la sostenibilità. Questa sinergia è fondamentale per promuovere l'innovazione e massimizzare il potenziale delle applicazioni IoT.

Il futuro dell'IoT

Come denotano le previsioni degli analisti, per l'Internet of Things si prospetta una crescita sostenuta,

grazie a un sempre più rapido ed efficace progresso tecnologico. Questo si traduce in un potenziale senza limiti apparenti nel migliorare l'efficienza, la sostenibilità e la qualità della vita. Con l'evoluzione e la maturazione delle tecnologie IoT, emergeranno nuovi casi d'uso e applicazioni che porteranno innovazione e trasformeranno molteplici settori. Questo, negli anni a venire, porterà facilmente l'IoT ad assumere un ruolo cruciale nel plasmare il nostro mondo, abilitando nuove possibilità e ridefinendo il nostro modo di vivere e lavorare.

Standardizzazione e interoperatività ancora difficili

Con la costante espansione dell'IoT (IDC prevede che il numero di dispositivi connessi raggiungerà i 41,6 miliardi entro il 2025), l'interoperabilità è diventata essenziale per il suo sviluppo. Permettere a dispositivi e sistemi diversi di comunicare e lavorare insieme senza ostacoli offre numerosi vantaggi sia per le aziende sia per i consumatori.

Tuttavia, oggi mancano precisi standard per l'IoT e ciò rappresenta una sfida significativa per aziende e organizzazioni perché comporta complessità inutili, costi elevati e rischi per la sicurezza. Un'indagine della Eclipse Foundation ha rilevato che il 40% degli sviluppatori IoT considera la mancanza di standard una sfida importante nello sviluppo di applicazioni IoT. Però rendere sistemi IoT interoperabili non è semplice. Uno dei principali problemi è di natura tecnica. Esistono molteplici dispositivi e sistemi

IoT, che spesso per comunicare usano protocolli e standard differenti. Questo causa facilmente incompatibilità e quindi impedisce ai dispositivi stessi di funzionare in modo cooperativo senza mostrare problemi. Un'altra sfida è di tipo commerciale. I produttori spesso impiegano protocolli e standard proprietari, mostrando una limitata disponibilità a collaborare tra loro. Va da sé che ciò rappresenta un ulteriore ostacolo per l'interoperabilità tra dispositivi e sistemi. Anche i diritti di proprietà intellettuale e le questioni di licenza possono limitare l'uso di alcuni protocolli e standard, complicando l'interoperabilità. Per superare queste sfide sono necessarie collaborazione e cooperazione tra le parti interessate, che possono non essere solo aziende e organizzazioni industriali, ma anche governi. Però, superare queste difficoltà è fondamentale per sfruttare appieno il potenziale dell'IoT e trarne i più ampi benefici. Secondo un rapporto di McKinsey, l'interoperabilità può ridurre i costi di sviluppo e implementazione fino al 30%, generando un valore potenziale globale tra 1.800 e 4.000 miliardi di dollari all'anno entro il 2025.

Va sottolineato che ci sono sviluppi positivi in questo campo, con diverse organizzazioni e consorzi industriali che lavorano per creare standard IoT in modo da facilitare l'interoperabilità. La Open Connectivity Foundation (OCF), per esempio, ha sviluppato uno standard che permette l'interoperabilità tra piattaforme ed ecosistemi diversi. Allo stesso modo, l'Industrial Internet Consortium (IIC) ha creato un'architettura di riferimento per lo sviluppo di sistemi IoT interoperabili.

CLICCA
QUI

Un motore di trasformazione digitale

di Riccardo Florio

La trasformazione digitale richiede il supporto di aziende affidabili e innovative come NEXiD, in grado di combinare una vasta esperienza sul campo con il sostegno di partner tecnologici strategici come OVHcloud.

Avviare un percorso di trasformazione digitale non è un compito facile. Le aziende italiane, soprattutto quelle di piccole e medie dimensioni, devono affrontare numerosi ostacoli come la carenza di risorse, la competitività globale, budget ridotti, infrastrutture obsolete, problemi di sicurezza e la necessità di rendere i processi aziendali più agili ed efficienti. Riuscire a compiere questo passaggio richiede la collaborazione di partner specializzati e affidabili, che possano fornire le competenze e le soluzioni tecnologiche necessarie a raggiungere il successo.

Un ruolo da protagonista per la trasformazione digitale

Tra le aziende che si distinguono nel supportare la trasformazione digitale in Italia c'è NEXiD.

Fondata nel 2018, **NEXiD** all'insegna del motto "Digital - Composable - Smart" offre soluzioni tecnologiche

avanzate per aiutare le imprese a modernizzare concretamente i loro processi.

«NEXiD nasce dall'unione di una piccola azienda attiva in ambito mobile e pmi e di un'azienda attiva nel settore bancario e assicurativo - spiega **Umberto Migliore, Partner & CTO NEXiD** -. Oggi l'azienda conta una cinquantina di persone che ne fanno una realtà sufficientemente grande per avere una capacità di ricerca e sviluppo interna, ma con dimensioni tali da garantire la massima agilità e flessibilità nell'affrontare progetti altamente personalizzati. La combinazione di queste doti ha permesso a NEXiD di essere riconosciuta **tra le 1000 aziende europee a più alta crescita nel 2022** da parte di Statista e di Financial Times».

Un elemento a valore aggiunto di NEXiD è la sua capacità di combinare le competenze interne con le soluzioni tecnologiche di partner e, tra questi, un posto di rilievo spetta a **OVHcloud, il principale provider europeo di servizi cloud**. La partnership con OVHcloud consente a NEXiD di sviluppare e implementare progetti innovativi a costi competitivi, mantenendo un focus specifico sul mercato europeo e garantendo sia la piena sovranità dei dati sia una gestione trasparente delle infrastrutture.

«Collaboriamo con OVHcloud da più di 15 anni - osserva Migliore - ed è stato il primo provider europeo



Umberto Migliore, Partner & CTO NEXiD

con server in Europa. Tuttavia, **garantire la sovranità dei dati non significa semplicemente avere data center sul territorio europeo** ma, invece, essere un'azienda sottoposta alla giurisprudenza europea anziché, per esempio, a quella americana come avviene per i tre grandi hyperscaler. Inoltre, nel tempo OVHcloud si è dimostrato un partner accessibile quando si sono presentate situazioni che richiedevano un maggior livello di supporto come, invece, non avviene nel caso degli hyperscaler».

Il valore della semplicità e della trasparenza

La collaborazione tra NEXiD e i suoi partner, come OVHcloud, si basa su valori di fiducia e trasparenza, attraverso un approccio flessibile e collaborativo che è fondamentale per sviluppare soluzioni che rispondano alle esigenze specifiche dei clienti garan-

tendo, al contempo, un elevato livello di supporto e una gestione efficiente delle infrastrutture. Il tutto all'insegna di un approccio che eviti qualsiasi forma di lock-in tecnologico.

«La semplicità è una cifra distintiva della nostra offerta - spiega **Dionigi Faccenda, Partner Program manager di OVHcloud** -. Sul Public Cloud di OVHcloud, per esempio, è possibile attivare una piattaforma di intelligenza artificiale ed effettuare operazioni di training e deployment con pochi click: il tutto in un contesto di massima sicurezza e privacy. Mettiamo anche a disposizione un'interfaccia di gestione semplice e accessibile che consente agli utenti di effettuare attività di gestione e controllo in autonomia e di ottenere reportistica dettagliata sulla qualità del servizio e sui costi. Nei confronti dei partner come NEXiD, l'approccio non prevede vincoli sul fatturato perché l'elemento chiave della collaborazione è la fiducia reciproca e la voglia di fare business insieme. Inoltre, supportiamo i nostri partner anche attraverso attività congiunte di marketing, Webinar e persino laboratori di formazione sulle modalità di vendita».

Soluzioni tecnologiche all'insegna dell'innovazione

L'offerta di NEXiD prevede un'ampia gamma di soluzioni tecnologiche che spaziano dallo **sviluppo di applicazioni Web e mobili** per



Dionigi Faccenda,
Partner Program manager di OVHcloud

il settore consumer e aziendale, alle **piattaforme di automazione della forza lavoro** e dello smart working. Un esempio significativo è l'**app Immagini** sviluppata per supportare i medici dell'**Istituto Europeo di Oncologia (IEO)** fondato da Umberto Veronesi, che garantisce alti standard di sicurezza e privacy. Inoltre, NEXiD è attiva tradizionalmente nell'ambito dei **sistemi IT a supporto di banche e assicurazioni**, oltre che nell'**Industria 4.0** con l'integrazione di tecnologie che aumentano la produttività degli impianti e soluzioni specifiche quali l'applicativo **4th Dimension** che permette di gestire database on-premise connessi a macchinari industriali.

«NEXiD opera in completa trasparenza con i propri clienti - precisa Migliore - offrendogli la possibilità di conoscere i fornitori e di controllare i costi dell'infrastruttura pro-

posta. Questo perché **il nostro obiettivo non è vendere tecnologia** ma, piuttosto, accompagnare i nostri clienti in un processo di trasformazione che avrà un impatto importante su tutti gli ambiti aziendali: tecnologico, operativo, strategico. Il nostro lavoro è sempre guidato da una forte dedizione ai **bisogni dei nostri clienti perché la loro soddisfazione è il nostro business**».

L'attività di NEXiD si estende anche alle tecnologie di frontiera. L'azienda **con sede a Milano** sviluppa, infatti, algoritmi di AI e Machine Learning, gestisce e integra dispositivi IoT, sviluppa sistemi di realtà virtuale e aumentata e rende la blockchain, i token e gli NFT accessibili a chiunque. Tra le esperienze recenti si possono ricordare il progetto in ambito **metaverso a supporto del lancio di alcune autovetture Nissan**, il primo **marketplace italiano di certificati di CO₂** chiamato **Carbon Planet** e lo sviluppo di assistenti basati su **AI per aziende operanti nel settore delle criptovalute**.

«Questi progetti - conclude Migliore - dimostrano la capacità di NEXiD di integrare tecnologie avanzate per creare soluzioni personalizzate e ad alto valore aggiunto per i propri clienti. Il cloud è l'ambiente irrinunciabile per supportare questi progetti ed è essenziale che l'ambiente Public Cloud scelto metta a disposizione la scalabilità e la flessibilità necessarie per adeguare dinamicamente il livello di prestazioni alle esigenze che cambiano nel tempo oltre che garantire una gestione facile e trasparente. Per tutte queste esigenze abbiamo sempre trovato in OVHcloud il partner ideale di riferimento».

NEXiD Metide è una soluzione di Digital Governance completamente modulare basata su Big Data, IoT, sistemi esperti e AI. Permette la gestione integrata e il monitoraggio dei dati attraverso sensori IoT in uffici, edifici, luoghi di produzione e spazi esterni complessi. Può essere utilizzata come sistema di monitoraggio e controllo di impianti elettrici, acquiferi, di condizionamento, di riscaldamento e fotovoltaici al fine di ottimizzare il risparmio energetico. È attualmente in uso da parte di un primario Gruppo Bancario italiano.



Scopri di più su
NEXiD Metide

Radio Maria Play è una piattaforma multicanale sviluppata da NEXiD per usufruire di contenuti digitali in continuità tra desktop, app mobile, CarPlay, Android Auto e Smart TV. Attraverso un unico Login è possibile restare sempre connessi e raggiungere tutti i contenuti salvati. Questa soluzione opera su scala globale fornendo contenuti e streaming in più di 80 Paesi nel mondo. Per l'internazionalizzazione e la personalizzazione dei contenuti, NEXiD ha utilizzato una tecnologia basata sull'intelligenza artificiale.



Scarica l'app
da Google Play o da App Store

Cips Informatica spiega la NIS2 nel suo roadshow

di Fabrizio Pincelli

Attraverso un evento itinerante, il distributore Cips Informatica ha voluto sensibilizzare partner e utenti finali sulla direttiva che diventerà effettiva il prossimo 17 ottobre. Protagonisti sono stati N-able, Netwrix, Sangfor e Notalia che, vestiti gli abiti di consulenti, e coadiuvati dall'avvocato Giuseppe Serafini, hanno affrontato il tema NIS2 a tutto tondo

Il 17 ottobre 2024 sarà una data importante per la cybersecurity in Europa: diventerà effettiva la normativa NIS2. Una direttiva che introduce diverse importanti novità nella lotta contro il cybercrime, a partire dal fatto che, rispetto all'attuale NIS, estende notevolmente il numero di realtà interessate. Senza contare che avrà importanti riflessi anche sulle relative filiere.

Ma quali sono le aziende coinvolte e, soprattutto, **cosa comporta in termini pratici questo adeguamento?** A queste e ad altre domande relative alla nuova normativa ha voluto dare risposta il distributore **Cips Informatica** attraverso il roadshow Road to NIS2. L'evento, che ha toccato quattro città (Genova, Milano, Padova e Roma), ha avuto come protagonisti tre vendor (N-able, Netwrix e Sangfor) e un service provider (Notalia). Questi, smessi i panni commerciali e indossati quelli di consulenti, e coadiu-

vati dal supporto dell'avvocato casazionista Giuseppe Serafini, hanno offerto un approfondimento a tutto tondo sul tema NIS2.

Cosa è la NIS2 e che novità porta

La **NIS2 è una versione aggiornata della direttiva sulla sicurezza delle reti e dei sistemi informativi dell'Unione Europea** (NISUE 2016/1148), introdotta nel maggio 2018. Creata per garantire un alto livello di sicurezza delle reti e dei sistemi informativi in tutta l'UE, tale direttiva si rivolge agli operatori di servizi essenziali per prevenire gli effetti dannosi che attacchi alle infrastrutture strategiche avrebbero potuto causare. Tuttavia, col passare del tempo, la NIS ha mostrato dei limiti sia nella sua implementazione sia nel concetto stesso di sicurezza IT.

Di conseguenza, l'Unione Europea ha deciso di modificare la direttiva e ha proposto la NIS2. Dopo un iter legislativo di due anni, nel maggio 2022 è stato raggiunto un accordo sulla NIS2, che è entrata in vigore il 16 gennaio 2023. **Gli Stati membri**

devono recepire la direttiva nelle loro legislazioni nazionali entro il 17 ottobre 2024.

Quale evoluzione della NIS, la NIS2 chiarisce le responsabilità del management aziendale e i tempi di notifica degli incidenti. Prevede che le aziende segnalino incidenti significativi entro 24 ore, considerando come significativi gli incidenti che possono causare gravi perturbazioni operative o rilevanti perdite finanziarie. Inoltre, obbliga il management aziendale all'attuazione e alla supervisione della conformità alla legislazione. Qualora si trasgredisca si va incontro a sanzioni che includono multe e, in casi gravi di non conformità, la sospensione temporanea dalle funzioni manageriali.

Le aziende devono anche adottare misure di protezione basate su un approccio che includa politiche di analisi dei rischi, gestione degli incidenti, continuità operativa, sicurezza della supply chain e altre disposizioni. Queste misure devono essere implementate da soggetti che devono saperne valutare l'efficacia e promuovere la formazione in materia di cybersecurity.

La direttiva si estende anche alla sicurezza della supply chain, richiedendo alle aziende di considerare le vulnerabilità dei propri fornitori e adottare misure correttive quando necessario. Gli Stati membri devono coordinare valutazioni dei rischi per la sicurezza delle supply chain critiche e promuovere l'adozione di misure correttive in caso di non conformità.



La NIS2 introduce poi una regola di dimensionamento (devono adeguarsi le realtà con un minimo di 50 dipendenti e un fatturato annuo superiore a 10 milioni) che operano nella categoria dei servizi essenziali già prevista dalla NIS (energia, trasporti, banche, mercati finanziari, sanità, acqua potabile, acque reflue, infrastrutture digitali, servizi ICT business-to-business) e nella nuova categoria dei servizi importanti (poste e corrieri, gestione rifiuti, lavorazione e distribuzione sostanze chimiche, fornitori di servizi digitali, ricerca e fabbricazione di dispositivi medici e diagnostici computer, prodotti di elettronica e ottica, apparecchiature elettriche; autoveicoli, rimorchi, semirimorchi e altri mezzi di trasporto).

La responsabilità è personale

Attraverso la NIS2, la UE intende fare in modo che le aziende che costituiscono l'attuale tessuto socio-economico siano in qualche modo affidabili. In tal senso, la NIS2 si colloca all'interno di una serie di norme, come sono anche il Data Act, l'Artificial Intelligence Act o DORA, che caratterizzano un panorama che sta cambiando in maniera sostanziale. *«Viviamo un momento in cui la normazione pervade il fenomeno cibernetico perché il fenomeno cibernetico pervade la nostra vita – ha affermato l'avvocato Giuseppe Serafini –. In questo senso la direttiva di fatto riconosce grande importanza al fenomeno cibernetico e individua strumenti specifici di analisi del comportamento delle organiz-*



Avv. Giuseppe Serafini

zazioni». In pratica, la NIS2 afferma che in ogni Paese UE deve esserci un'autorità di controllo che possa imporre audit periodici da parte di terze parti e che i costi di questi audit siano a carico del soggetto che li subisce, salvo situazioni specifiche in cui la mancata attribuzione del costo è giustificabile. Se sono riscontrate irregolarità, qualcuno ne deve rispondere. *«Il legislatore dell'Unione ha rafforzato il concetto di governance – ha aggiunto Serafini – appuntando precisamente una responsabilità personale di chi ha la gestione dell'organizzazione. Questo è uno shift significativo perché finora il soggetto sanzionato era solo l'organizzazione stessa»*.

Avere le armi adatte ed essere conformi alla NIS2

«La cybersecurity è cambiata perché sono cambiati gli attacchi, si sono modernizzati – ha sostenuto Matteo Brusco distribution manager per Italia e Spagna di N-able –. Se vogliamo contrastare certe attività dobbiamo usare gli strumenti giusti. Ricordiamo che l'intelligenza artificiale è nata per le organizzazioni cri-



Matteo Brusco,
N-able

minali, che la usano da anni. La NIS2 vuole spingere a operare sullo stesso piano o perlomeno al meglio delle proprie possibilità».

L'Italia è formata per il 90% da PMI le quali non hanno un IT manager e cercano di affidarsi a qualcuno che gestisca per la sicurezza. «Questo mostra l'importanza di system integrator, partner e vendor in grado di aiutarle – puntualizza Brusco -. Tuttavia, chi offre tale servizio tipicamente ha le credenziali di accesso del proprio cliente. E in quanto tale, diventa un punto vulnerabile per il cliente stesso, perché se è vittima di un attacco può subire il furto di tutte le credenziali. Ecco perché chi vuole continuare a lavorare con soggetti che rientrano nella NIS2 deve a sua volta adeguarsi alla normativa». E, molto probabilmente, col tempo, la richiesta della certificazione NIS2 diventerà un prerequisito per ogni contratto, a prescindere dal fatto che sia davvero necessaria.

Una più semplice gestione della sicurezza

Oggi i dipendenti di un'azienda devono poter lavorare sempre e do-

*vunque in sicurezza. «Chi si occupa di cybersecurity deve preoccuparsi che gli endpoint siano protetti e che gli utenti possano lavorare in maniera sicura e funzionale – ha dichiarato **Francesco Addesi, country manager di Sangfor Italia** -. Le tecnologie che proteggono dai rischi di sicurezza non devono diventare un ostacolo per la produttività. Bisogna rendere pratico e funzionale ciò che il cliente vede come complesso».*

In passato si parlava di antivirus, poi di EDR (Endpoint Detection and Response), quindi di MDR (Managed Detection and Response). Oggi si parla di SASE (Secure Assess Service Edge). «Non è nulla di nuovo – ha precisato Addesi -, è la crisi di tutte le precedenti tecnologie, un unico agent per semplificare la gestione della sicurezza. Ma c'è bisogno di un consulente che aiuti in questo percorso. Sempre di più i system integrator diventeranno consulenti, sempre di più i vendor individueranno i trend di mercato per proteggere al meglio gli utenti finali. I vendor devono essere i consulenti dei propri partner nel seguire questa strada, in conformità alle normative».



Francesco Addesi,
Sangfor Italia

Tutto parte da un assessment

Maurizio Taglioretti, esperto di cybersecurity e Regional Manager SEUR di Netwrix, ha ripreso quanto detto da Addesi per rimarcare il valore del risk assessment: «È fondamentale. Tutto parte da lì: non si può rendere sicuro ciò che non si conosce o non si sa di avere. Questo vale per l'hardware e per il software, ma soprattutto per i dati. Nonostante la spesa in sicurezza aumenti, gli attacchi crescono vertiginosamente. Quindi le tecnologie ci sono, ma probabilmente non si utilizzano nella maniera corretta oppure non dialogano tra loro o non si riescono a configurare adeguatamente. La soluzione è l'assessment. Non è solo uno dei punti cardine della NIS2, ma anche del GDPR e di tutte le normative». Taglioretti ha consigliato di leggere con attenzione **l'articolo 21 della NIS2, dove in 10 punti viene precisato cosa si deve fare per adeguarsi**, sia per il fornitore sia per l'utente finale. «Un assessment potrebbe portare a scoprire che molte delle richieste sono già implementate e, quindi, per essere compliant con la norma basta un numero limitato di



Maurizio Taglioretti,
Netwrix



GLI APPROFONDIMENTI
DI BIZZIT



Protezione dei dati: best practice e compliance

I dati sono tanto preziosi quanto esposti a nel mirino globale del cybercrime. Tra sfide tecnologiche e normative, serve un approccio coerente che garantisca la protezione del patrimonio digitale durante l'intero ciclo di vita.

[+ continua a leggere](#)

interventi. Per esempio, le politiche di analisi dei rischi di sicurezza sono le stesse previste dal risk management dell'ENISA. Lo stesso vale per la gestione degli incidenti che è la medesima prevista dalla ISO 27.000. Per cui, se un'azienda è certificata, dovrebbe già seguire tali politiche».

La NIS2 obbliga un ampio numero di aziende ad **affrontare in modo più consapevole il problema della cybersecurity, definendo chiare responsabilità**. In tal senso, rappresenta un'ottima opportunità per il canale, in particolare per i system integrator e gli MSP, che avranno l'occasione di instaurare un rapporto duraturo e proficuo con le imprese che saranno obbligate a soddisfare le richieste della normativa, mantenendo nel tempo il massimo livello di protezione consentito. Tuttavia, per poter cogliere tale opportunità, bisognerà essere adeguatamente informati e formati sul tema NIS2, essendo in prima persona compliant.

CIPS, quando la distribuzione non è una questione geografica

Con una sede decisamente inusuale per un'azienda IT, a Città di Castello, in un palazzo d'epoca all'interno di una delle zone più medievali dell'Umbria, dal 1991 Cips Informatica si occupa della gestione e della sicurezza delle infrastrutture informatiche. Nel 2023 ha registrato un fatturato di 8,3 milioni di euro (in crescita del 10,6% rispetto ai 7,5 milioni di euro del 2022). Annovera circa 600 partner dislocati in tutta Italia, molti dei quali sono MSP.

Nata come Value Added Distributor (VAD), oggi propone un listino composto da prodotti tecnologicamente complementari in modo da offrire ai partner soluzioni complete preconfezionate. L'attività dell'azienda ruota infatti attorno allo scouting tra brand meno noti a livello globale. Le soluzioni selezionate sono testate nei laboratori di Cips e ne viene verificata l'aderenza alle normative (prima fra tutte il GDPR). Ai partner viene anche fornita una valutazione del go to market attraverso la definizione di un modello commerciale.

Per Cips Informatica la formazione e l'informazione rivestono un ruolo essenziale. E il road show sul tema NIS2

va visto in questo senso. Tuttavia, non è che la più recente di una serie di attività organizzate dall'azienda, alcune delle quali volte proprio a incontrare i partner direttamente sul territorio. Inoltre, il distributore offre frequenti webinar tecnici, marketing e commerciali. In quest'ultimo periodo, grande attenzione è data al mondo dell'MSP, in particolare per fornire le competenze adatte a trasformare il modello di vendita da prodotto a servizio.

Cips Informatica, per intensificare l'attività di informazione, ha allestito due siti con contenuti pratici e utili all'attività lavorativa:

Cipslegal, che propone testi scritti da esperti dell'informatica forense;

Digital Channel Forum, spazio dove i partner possono trovare notizie ad ampio spettro sul mondo IT.

ArcSight Intelligence e CrowdStrike Falcon insieme contro le minacce interne

di Riccardo Florio

La combinazione tra la capacità AI di ArcSight Intelligence e le funzionalità EDR di CrowdStrike garantisce un'eccezionale capacità di rilevamento delle minacce sperimentata con successo da Bernicia Homes



Le minacce interne sono le più difficili da individuare e bloccare proattivamente. Per fornire una straordinaria capacità di prevenzione l'associazione abitativa Bernicia Homes ha combinato due soluzioni leader di mercato per fornire una straordinaria capacità di rilevare le minacce: **CrowdStrike Falcon** mette a disposizione una imponente ricchezza di dati che **ArcSight Intelligence** utilizza per individuare le anomalie.

L'esperienza di Bernicia Homes che gestisce 60mila di clienti

Bernicia Homes fornisce case e servizi di qualità alle persone nel nord-est dell'Inghilterra da oltre 50 anni, essendosi guadagnata la reputazione di una delle principali associazioni abitative del Paese. Le associazioni edilizie sono proprietari senza scopo di lucro che forniscono case e assistenza a circa sei milioni di persone in tutta l'Inghilterra.



Bernicia si trova a dover **gestire dati sensibili di oltre 60.000 clienti** rendendo la sicurezza informatica una priorità per l'azienda.

«La sicurezza informatica è al primo posto nel nostro profilo di rischio – spiega **Adam Watson, responsabile della sicurezza e dell'infrastruttura di Bernicia** – a dimostrazione di quanto siamo consapevoli, a tutti i livelli dell'organizzazione, del potenziale danno reputazionale che può derivare da una violazione della sicurezza di qualsiasi tipo. Per questo motivo abbiamo implementato una serie di misure di sicurezza informatica ma negli ultimi anni gli attacchi sono diventati molto più sofisticati. Abbiamo quindi ritenuto di dover adottare un approccio proattivo indirizzato ad **augmentare la visibilità del nostro ambiente in modo da poter rilevare i movimenti laterali e i potenziali comportamenti sospetti**».

Bernicia ha effettuato un'analisi di mercato valutando sei potenziali soluzioni, tra cui **ArcSight Intelligence**. La soluzione di OpenText Cybersecurity fornisce un rilevamento avanzato delle minacce, supportato da una sofisticata tecnologia di machine learning non supervisionato. ArcSight Intelligence crea profili di rischio per ogni utente, macchina, URL ed entità, imparando a riconoscere i comportamenti normali specifici di ogni organizzazione. In tal modo, riesce a sintetizzare le informazioni lega-

te a miliardi di eventi di

sicurezza in pochi indizi molto affidabili, da sottoporre a ulteriori indagini.

ArcSight Intelligence fornisce indicazioni mirate sulle minacce

Bernicia gestisce un'infrastruttura desktop virtuale (VDI) in un ambiente cloud privato e ha apprezzato particolarmente il fatto che **ArcSight Intelligence offra un'integrazione diretta con CrowdStrike**.

«La nostra piattaforma **CrowdStrike Falcon fornisce un'ampia gamma di dati sulla sicurezza, che ArcSight Intelligence riutilizza per individuare anomalie specifiche che altrimenti passerebbero inosservate** – spiega il responsabile della sicurezza di Bernicia -. Non abbiamo dovuto preoccuparci di distribuire altri agenti sugli endpoint, in quanto i dati di CrowdStrike erano già presenti nel cloud, ottenendo una distribuzione "zero-footprint" che ha semplicemente richiesto di impostare l'integrazione con ArcSight Intelligence all'interno dello store di CrowdStrike».

Durante un proof of concept durato 45 giorni, ArcSight Intelligence ha analizzato oltre 100 milioni di eventi di sicurezza provenienti da centinaia di endpoint.

La gestione di questi dati ha rappresentato l'aspetto distintivo di ArcSight Intelligence rispetto alla concorrenza come precisato da Adam Watson

«ArcSight Intelligence ci ha fornito un'interfaccia user-friendly che rende facile trovare le informazioni di cui abbiamo bisogno. Siamo un piccolo team e **il servizio di threat hunting**



BERNICIA GROUP

Housing People, Helping People

per la cybersecurity che completa ArcSight Intelligence è stato prezioso per noi. Riceviamo un report esecutivo con un numero selezionato di potenziali comportamenti anomali che riusciamo a gestire. I dati sono presentati in modo visuale ed è estremamente facile individuare trend in uno specifico periodo di tempo. Dopo un'indagine più approfondita, fortunatamente non abbiamo trovato nulla di grave e certamente nulla di dannoso, ma ArcSight Intelligence ha evidenziato comportamenti interessanti in alcune delle nostre applicazioni che ci hanno fornito informazioni preziose. Avere una visione approfondita di come il nostro personale utilizza l'ambiente ci dà l'opportunità di individuare comportamenti anomali e, auspicabilmente, di fermare una minaccia sul nascere».

La caccia alle minacce riduce lo stress da allerta

Dopo il successo della proof of value, il team di Bernicia è passato in produzione con ArcSight Intelligence. Adam e il suo team sono stati messi in contatto col team di cybersecurity threat hunting per concordare la modalità operativa da adottare. Un "touchpoint" settimanale discute i risultati di alto livello, mentre è stato impostato un flusso di lavoro per gestire gli avvisi critici che devono essere attivati immediatamente da Bernicia.

ArcSight Intelligence rileva, collega i punti e visualizza il percorso di un attacco. Grazie a questo contesto, ArcSight Intelligence è in grado di evidenziare gli attacchi nel momen-

to in cui si verificano. In questo caso, Bernicia viene

immediatamente avvisata potendo visualizzare gli incidenti e i flussi di lavoro al fine di consentire una convalida e abilitare azioni di indagine e di risposta.

«Oggi il rischio che l'account di un utente venga compromesso espone le aziende a rischi potenziali con un elevato impatto di tipo finanziario e operativo – spiega **Pierpaolo Ali, Director Southern Europe di OpenText Cybersecurity** -. La combinazione tra la tecnologia avanzata di machine learning non supervisionato di ArcSight Intelligence unitamente alla capacità di fornire dati sulla sicurezza affidabili della piattaforma Falcon di CrowdStrike **realizzano una sinergia vincente** che permette di identificare proattivamente ogni tipo di minaccia, incluse quelle provenienti dall'interno. Questa capacità di threat hunting si avvale di analisi e correlazioni estremamente sofisticate che non sono presenti nei tradizionali strumenti di cybersecurity, consentendo alle aziende di concentrare le proprie risorse sugli eventi davvero importanti e riducendo lo stress da allerta».



LEGGI ANCHE

Ransomware: le soluzioni di OpenText Cybersecurity



Pierpaolo Ali Director Southern Europe di OpenText Cybersecurity



SentinelOne aiuta a proteggere le identità

di Maurizio Ferrari

Le soluzioni SentinelOne per il mondo delle Active Directory aiutano a scoprire e contrastare gli attacchi a questo sistema e a proteggere le identità.

Io sono. Affermazione filosoficamente molto forte, ma nel settore della cybersecurity può essere molto debole. Specialmente se non si sono prese le giuste precauzioni, perché rubare identità o crearne di nuove, con privilegi e permessi, può aprire le porte a dati e informazioni delle aziende, spesso senza che queste si rendano conto di essere sotto attacco, tranne quando è troppo tardi e il danno è stato fatto.

Salvatore Di Biasi, system engineer di SentinelOne, ha illustrato come attaccare le credenziali possa essere proficuo per gli hacker, che con uno "sforzo" minimo possono, se hanno la giusta pazienza, portare a casa una grossa mole di dati e informazioni. Al centro dell'attività degli hacker ci sono le **Active Directory, il punto focale da cui diventa possibile controllare tutto il sistema.**

Strategie di protezione e controllo delle identità

Allo stato attuale il perimetro di una azienda si è ampliato, ma non tutto è stato reso sicuro e impene-trabile dagli attacchi esterni: ci sono una moltitudine di sistemi che sono poco protetti ed esposti a Internet. Lo strumento più usato per penetra-re è il malware, in secondo piano gli attacchi di forza bruta o gli exploit. Una volta entrato l'attaccante opera con calma e cerca di recuperare più informazioni possibile sul sistema, di prendere possesso di credenziali privilegiate e, attraverso esse, rima-nere all'interno dell'Active Directory il più a lungo possibile per pianifi-care l'esfiltrazione dei dati e delle informazioni desiderate. Operando in modo invisibile, come se fosse un utente autorizzato a farlo, questo tipo di attacco può causare molti danni, soprattutto perché **quando emerge il problema della fuga dei dati il danno è fatto**. Soprattut-to considerando il costo che deve essere sopportato per il ripristino di Active Directory compromesse, spesso il backup non è sufficiente, ma diventa necessario ricominciare da zero. SentinelOne ha in portafoglio una soluzione completa di **Identity Threat Detection & Response (ItDr)** che consente ai responsabili della sicurezza di controllare che nelle Active Directory tutto sia nor-male e che nessuno operi in modo sospetto. Attraverso **Singularity Identity** e **Ranger AD** si è in grado di proteggere l'Active Directory da ogni tipo di attacco. Grazie a un leggero agente tutta la foresta vie-

ne controllata: i pacchetti vengono analizzati in modo da intercettare e bloccare tecniche di attacco avan-zate basate sull'identità. Questa so-luzione, inoltre, consente di avere sotto controllo, in modo dettaglia-to, tutti i profili degli utenti presen-ti nell'Active Directory: in questo modo diventa possibile osservare anomalie, come spostamenti verti-cali e orizzontali. Questa soluzione ItDr permette anche di creare pro-fili "trappola" cui attirare l'attac-cante e bloccarlo. Grazie al costante controllo sull'Active Directory e sulle utenze a esse connesse diventa im-possibile per l'attaccante mantene-re un basso profilo e raccogliere in-formazioni per esfiltrare i dati in un secondo tempo. Tra le funzionalità di questa soluzione c'è anche l'ana-lisi di oltre 200 vulnerabilità critiche in Active Directory e Azure Active Directory riducendo la superficie di attacco a disposizione dei cybercri-minali. SentinelOne con Identity e Ranger AD aiuta a verificare che chi dice "lo sono" sia realmente chi dice di essere.



L'APPROFONDIMENTO

SentinelOne: protezione multilivello, integrata e guidata dall'AI

Un approccio strategico alla sicurezza basato su un modello di protezione multilivello che affronta le minacce informatiche in maniera comprensiva, dalla prevenzione al rilevamento e alla risposta.

[+ continua a leggere](#)

Rafforzare la cybersecurity puntando al mid-market: la direzione di WithSecure

A Sphere 2024, l'evento annuale di WithSecure, l'azienda specializzata in soluzioni di sicurezza afferma la dedizione verso il mid-market e annuncia interessanti novità a supporto della "threat detection"

di Riccardo Florio

Il costante e rapido sviluppo tecnologico rende le aziende più vulnerabili ed esposte a minacce come il ransomware. A soffrire maggiormente di questa condizione sono le piccole e medie imprese che si trovano ad affrontare questa situazione senza le risorse necessarie restando, così, senza scelte praticabili, convenienti e realizzabili.

È proprio **al mid-market che WithSecure, azienda globale specializzata in soluzioni per la cybersecurity, ha deciso di ind-**

irizzare la propria offerta, con una strategia recentemente ridefinita per rispondere in pieno alle esigenze di questo settore.

L'obiettivo dell'azienda finlandese è quello di mettere a **disposizione anche delle realtà più piccoli gli strumenti necessari per disporre di un elevato livello di sicurezza** a un costo accessibile e, soprattutto, con un livello di semplicità tale da non richiedere competenze che risultano tanto avanzate quanto difficili e costose da reperire.

A **Sphere 2024**, l'evento annuale in cui la società finlandese raccoglie attorno a sé partner, clienti e media, WithSecure ha annunciato alcune interessanti novità che rispondono a questa strategia: nuove funzionalità di Exposure management, supporto per la gestione dell'identità, una gamma di servizi di sicurezza gestiti e Luminem un assistente per la gestione degli incidenti basato su AI.

Le novità annunciate a Sphere 2024

La nuova funzionalità **Exposure Management** aumenta la resilienza adottando una modalità di analisi dell'ambiente simile a quello degli attaccanti per fornire un assessment continuo sull'esposizione alla minacce. Dal punto di vista pratico, Exposure Management si presenta come una nuova dashboard accessibile dal pannello di controllo di **WithSecure Elements Cloud** (la piattaforma che riunisce i servizi XDR, XM e Co-security) ed è pensata per favorire il passaggio da un modello di sicurezza reattiva a una proattiva. Questa soluzione si adatta alle esigenze dei clienti del mid-market poiché presenta viste semplificate sulle minacce relative alla superficie di attacco aziendale, **fornendo contestualmente le indicazioni pratiche** sugli asset, le priorità e le modalità con cui intervenire per ridurre il livello di rischio.

WithSecure ha anche esteso le funzionalità di Detection & Re-

sponse con **Elements Identity Security for Entra ID** che integra, per la prima volta, funzionalità di gestione dell'identità e dell'accesso all'interno della sua piattaforma tramite il supporto per il servizio basato su cloud Microsoft Entra ID. Nel futuro, l'azienda prevede di stabilire nuove partnership per estendere la gestione dell'identità a un bacino più ampio di soluzioni di terze parti.

Per contribuire a ripristinare la fiducia digitale WithSecure ha rilasciato una serie di **nuovi servizi di sicurezza gestita con funzionalità di rilevamento e risposta alle minacce** erogati attraverso i propri partner. In tal modo, le aziende più piccole che non dispongono delle risorse sufficienti, potranno decidere di esternalizzare le attività di sicurezza a partner dedicati e costantemente aggiornati dal punto di vista tecnologico e dell'analisi delle minacce.

L'ultima novità annunciata riguarda l'introduzione di un **nuovo assistente basato su AI generativa denominato Luminem**, che viene integrato in WithSecure Elements Cloud e reso disponibile ai clienti della piattaforma senza costi aggiuntivi.



Leggi l'articolo integrale


```

177 return(c[a] < d[a] ? -1 : c[a] > d[a] ? 1 : 0
178 };
179 }
180 function performance(a, b, c) {
181   if (0 >= b.length) {
182     var d = 100, f = 0;
183     for (c = c ? 1 : b.length;;) {
184       if (f = a.indexOf(b, f), 0 <= f) {

```

Microservizi: vantaggi, sfide e best practice

Sono uno dei modelli per lo sviluppo e la gestione delle applicazioni in più rapida diffusione per i vantaggi in termini di scalabilità, manutenibilità e flessibilità tecnologica. Non vanno però trascurate le tematiche inerenti alla complessità gestionale e la sicurezza.

di Riccardo Florio

Nel panorama tecnologico attuale, le architetture software tradizionali stanno cedendo il passo a soluzioni più modulari e scalabili, tra cui spiccano i microservizi.

Questa transizione non è solo una moda, ma una necessità dettata dalla crescente complessità delle applicazioni e dalla necessità di rispondere rapidamente alle esigenze del mercato.

L'architettura a microservizi rappresenta un paradigma in cui un'applicazione viene suddivisa in una serie di servizi piccoli e indipendenti. Ogni microservizio esegue una funzione specifica e comunica con gli altri servizi tramite API ben

definite. Questa frammentazione consente una gestione più granulare delle funzionalità e una maggiore flessibilità nel ciclo di sviluppo e manutenzione del software.

I vantaggi dei microservizi

Uno dei principali vantaggi dei microservizi è la **scalabilità**. In un'architettura monolitica, scalare un'applicazione significa replicare l'intera base di codice, con un notevole spreco di risorse. I microservizi, invece, permettono di scalare solo i componenti che necessitano di più risorse, ottimizzando così l'uso delle infrastrutture. Per esempio, se un modulo di pagamento ha un carico

maggiore rispetto agli altri componenti dell'applicazione, è possibile scalare solo quel servizio senza dover scalare l'intero sistema. Questo approccio non solo riduce i costi operativi, ma migliora anche le prestazioni dell'applicazione, garantendo una risposta rapida alle variazioni della domanda.

Inoltre, ogni microservizio è autonomo e, di conseguenza, gli sviluppatori possono aggiornare o sostituire singoli servizi senza timore di interrompere l'intero sistema. Questo livello di modularità contribuisce anche a **ridurre i tempi di sviluppo**, poiché i team possono lavorare in parallelo su servizi differenti senza interferenze. Inoltre, poiché i microservizi sono generalmente più piccoli e più focalizzati rispetto ai codici monolitici, il **codice è più facile da comprendere e da gestire**: una caratteristica particolarmente utile in ambienti di sviluppo dove la velocità di iterazione e la capacità di rispondere rapidamente ai cambiamenti sono fondamentali. I microservizi forniscono un maggiore livello di flessibilità dal punto di vista tecnologico, consentendo alle aziende di scegliere la tecnologia più adatta per ogni servizio specifico, senza essere vincolate a un unico stack tecnologico. Per esempio, un'azienda può utilizzare **Node.js** per servizi che richiedono una gestione efficiente delle I/O asincrone, mentre può scegliere **Python** per i servizi che richiedono elaborazioni complesse di dati.

Node.js



Python



Questa libertà di scelta offre alle aziende la possibilità di utilizzare le migliori tecnologie disponibili per ogni specifico caso d'uso, migliorando così l'efficienza complessiva del sistema.

Le sfide dei microservizi

Nonostante i numerosi vantaggi, l'implementazione dei microservizi non è esente da sfide. La prima riguarda la **gestione della complessità**. Dividere un'applicazione in molti servizi indipendenti, infatti, richiede una gestione accurata delle comunicazioni e della coerenza dei dati. In assenza di una pianificazione adeguata, il rischio è quello di creare un sistema difficile da mantenere e monitorare. Le comunicazioni tra microservizi, solitamente basate su protocolli come HTTP/REST o gRPC, devono essere ben progettate per evitare inefficienze e colli di bottiglia. Inoltre, la **gestione della coerenza** dei dati diventa più complessa poiché i dati potrebbero essere distribuiti su diversi servizi, rendendo necessario implementare specifici accorgimenti. Uno di questi è la cosiddetta **eventual consistency**, che prevede che le modifiche ai dati possano non essere immediatamente visibili a tutti i nodi o servizi ma garantisce che, una volta propagati tutti gli aggiornamenti, i dati diventeranno consistenti. Un altro modo per gestire la coerenza dei dati è l'**event sourcing**, che tratta la registrazione di tutte le modifiche ai dati come una sequenza di eventi che descrivono il cambiamento avvenuto e che vengono memorizzati in

un log ordinato cronologicamente. Con molti servizi in gioco un'altra sfida significativa è rappresentata dalle operazioni di **deployment e di monitoraggio continuo**. Assicurarsi che tutti i servizi funzionino correttamente e siano ben integrati richiede, infatti, un'infrastruttura di monitoraggio robusta e una strategia di logging efficace.

Microservizi e sicurezza

La sicurezza rappresenta un altro aspetto critico.

Il fatto che nei microservizi ogni servizio comunichi con gli altri attraverso la rete, amplia la superficie di attacco. Ogni API esposta rappresenta un potenziale punto di ingresso per gli attacchi, aumentando la complessità della gestione della sicurezza. Garantire la **sicurezza delle comunicazioni tra microservizi** è cruciale per prevenire attacchi come l'intercettazione di dati sensibili, attacchi man-in-the-middle e spoofing. Per questo motivo, tutte le comunicazioni tra i microservizi dovrebbero essere cifrate utilizzando protocolli sicuri come TLS (Transport Layer Security). Questo assicura che i dati trasmessi siano protetti da intercettazioni e modifiche non autorizzate. Inoltre, l'uso di certificati SSL/TLS validi e aggiornati è essenziale per garantire la sicurezza delle connessioni. Tuttavia, in un'architettura a microservizi, anche la **gestione delle identità e degli accessi** diventa più complessa. Ogni servizio può avere requisiti di accesso diversi e garantire che solo gli utenti e i servizi autorizzati possano

accedere alle risorse appropriate richiede un sistema di gestione delle identità robusto e flessibile. L'uso di **OAuth2** e **OpenID Connect** può semplificare la gestione delle identità, consentendo di delegare l'autenticazione a provider esterni affidabili. L'implementazione di politiche di accesso granulari e l'uso di token di autenticazione come **JWT (JSON Web Token)** possono aiutare a mitigare i rischi.

Va poi ricordato che i microservizi spesso necessitano di accedere a

Strumenti la gestione delle identità e degli accessi

OAuth2



OpenID Connect



Json Web Token



credenziali, chiavi API e **altri dati segreti** per funzionare correttamente. La gestione sicura di queste informazioni è fondamentale per prevenire fughe di dati e accessi non autorizzati. Per limitare tali problemi è possibile utilizzare soluzioni di "secret management" come **HashiCorp Vault** o **AWS Secrets Manager** per archiviare, distribuire e accedere ai dati riservati in modo sicuro.

La segmentazione della rete con l'**isolamento dei microservizi critici** è una strategia chiave per limitare l'impatto di eventuali violazioni di sicurezza. Ogni servizio dovrebbe operare in un ambiente isolato, utilizzando tecnologie come i con-

Soluzioni di secret management

HashiCorpo Vault 

AWS Secrets Manager 

tainer Docker e orchestratori come Kubernetes. Questo approccio riduce il rischio che una compromissione di un servizio si propaghi agli altri servizi del sistema.

Best practice per l'implementazione

Integrare **pratiche DevOps** è un requisito pressoché irrinunciabile per facilitare l'automazione del deployment e del monitoraggio dei servizi. DevOps favorisce la collaborazione tra i team di sviluppo e operativi, accelerando il ciclo di vita del software e migliorando la qualità del prodotto finale. Strumenti di Continuous Integration/Continuous Deployment (CI/CD) come **Jenkins**, **GitLab CI** e **CircleCI**, permettono di automatizzare il processo di build, test e deploy dei microservizi, riducendo così il rischio di errori e migliorando l'efficienza del team. L'uso di **container, come Docker**, può semplificare notevolmente la gestione dei microservizi. I container offrono un ambiente isolato e coerente per l'esecuzione dei servizi, indipendentemente dall'infrastruttura sottostante. Questo facilita il deploy e la scalabilità, riducendo al contempo i problemi di compatibilità. I container possono essere orchestrati tramite piattaforme come

Kubernetes, che gestisce il deployment, la scalabilità e il funzionamento continuo delle applicazioni containerizzate.

Questa combinazione di tecnologie assicura che i microservizi possano essere eseguiti in modo efficiente su qualsiasi ambiente, sia on-premise sia cloud. **Implementare un API Gateway** è un'altra best practice. Un API Gateway funge da punto di ingresso centralizzato per tutte le richieste ai microservizi, migliorando la gestione del traffico e la sicurezza. Permette di applicare politiche di autenticazione e autorizzazione in modo più efficiente e di monitorare le API in tempo reale. Soluzioni come **Kong**, **NGINX** o **Amazon API Gateway** offrono funzionalità avanzate per la gestione delle API, come il bilanciamento del carico, la limitazione della velocità, e la trasformazione delle richieste e delle risposte. Un API Gateway può anche aiutare a implementare "circuit breaker" e "retry policy", migliorando la resilienza complessiva del sistema. Infine, è fondamentale dotarsi di strumenti di **monitoraggio e logging adeguati**. Soluzioni di monitoraggio come **Prometheus** e **Grafana** forniscono visibilità in tempo reale sulle prestazioni dei microservizi, aiutando a identificare e risolvere rapidamente i problemi. Un sistema di logging centralizzato come **ELK Stack (Elasticsearch, Logstash, Kibana)**, permette di aggregare e analizzare i log provenienti da tutti i microservizi, facilitando così il debug e la risoluzione dei problemi.



**Carmen
Palumbo**



Il mercato chiede oggi servizi di cybersecurity gestiti per contrastare attacchi sofisticati e colmare il divario di competenze. WithSecure ha recentemente aggiornato il portafoglio a Sphere 2024.

L'intervista alla country sales manager Carmen Palumbo.



WithSecure, servizi di cybersecurity serenamente europei

di **Leo Sorge**

Il mondo della cybersecurity, che è sempre più sfidante, sta cambiando pelle. I fornitori di soluzioni e servizi devono seguire questi cambiamenti e quando possibile anticiparli. Di questo abbiamo parlato con **Carmen Palumbo, country sales manager di WithSecure Italia.**

L'obiettivo 2024 dell'azienda è una crescita a due cifre alte, ovunque nel mondo e quindi anche in Italia. Lo strumento di questa crescita è nei servizi, perché le soluzioni stanno diventando una commodity e quin-

di si lavora pesantemente sul prezzo, una politica tattica ma non certo strategica.

«WithSecure sta seguendo con attenzione il cambiamento del mondo cyber: vendere soltanto soluzioni a un tot al chilo non va più bene: gli attacchi hacker sono sempre più sofisticati e la situazione geopolitica aiuta gli attaccanti», spiega Palumbo.

L'incontro è avvenuto a latere del tour per i partner italiani. «Comunichiamo ai partner la nostra evoluzione verso i servizi: all'interno del nostro portafoglio ne abbiamo sempre di più, per dare una mano ai partner e agli utenti finali nel contrastare gli attacchi hacker».

Si parla quindi di servizi pensati appositamente per il canale, in modo che possano andare dall'utente finale e proporre le soluzioni e servizi.

Certo la cybersecurity è esplosa, ma mancano le competenze, c'è skills shortage sul personale tecnico. Le aziende, sia i partner sia l'utente finale, sperimentano un dilemma: assumendo un giovane e formandolo, c'è grande rischio che a fine formazione venga assunto altrove con stipendio più alto.

«I nostri servizi risolvono spesso questo problema: a partner e utenti finali diciamo che affidandosi al partner o a noi, quando serve subentriamo e diamo una mano», senza complesse

gestioni del personale fuori orario. «Abbiamo tre nuovi servizi: co-monitoring, Countercept MDR e un nuovo servizio, di tipo MDR light, che ancora non ha un nome ufficiale. Il co-monitoring è un servizio correlato alla nostra soluzione EDR, che sfrutta l'intelligenza artificiale per supportare partner e utente finale».

L'AI è al massimo dell'hype del mercato: WithSecure la cavalca da tempo. «Noi parliamo di intelligenza artificiale da sette otto anni, con il progetto Blackfin: non è che ci abbiamo pensato adesso perché è di tendenza! Crediamo nell'AI, ma contrariamente ad altri vendor non la spingiamo al 100%, non facciamo automazione totale: per noi l'intervento umano è ancora fondamentale. Ovviamente l'AI aiuta, perché toglie il rumore di fondo, ma poi le scelte deve farle l'uomo. Un nostro nuovo cliente ha avuto il blocco delle casse in tutta Italia per una scelta automatica, un fatto che con le nostre soluzioni non sarebbe successo».

Dalla soluzione al servizio

Il quadro prodotti/servizi è chiaro e la grande novità, già in preparazione, è il cambiamento di approccio alla vendita: «la nostra piattaforma di intelligent Exposure Management permetterà di gestire da un unico punto tutte le nostre soluzioni: per WithSecure è un punto di svolta rispetto

alla pura vendita di soluzioni. Siamo in procinto di lanciare anche un altro tipo di servizio sul co-monitoring, legato alle soluzioni EDR: noi diamo supporto 24/7, quindi se l'utente finale non ha un proprio servizio tecnico, ci pensiamo noi o i nostri partner». L'abbonamento dura un anno.

Un'altra formula di abbonamento è l'out of the office: «se il cliente ha skill interni ed è coperto durante le ore di ufficio, feriali lunedì-venerdì 9-17, fuori da questi slot ci pensiamo noi».

Per dimensione di aziende, il core di WithSecure è dalle 200 alle 1.000 postazioni a livello italiano, che possono gestire anche a livello di supporto e consulenza. Il co-monitoring è perfetto fino a 600 postazioni e copre la gran parte delle proposte. Dalle mille postazioni in su la consulenza diventa un po' più articolata: «in alcuni casi ci è capitato di far riferimento ai colleghi di Helsinki per mantenere una gestione ottimale».

«Salendo nelle prestazioni, nella fascia Enterprise il classico servizio MDR che noi chiamiamo Countercept opera dalle mille postazioni in su. Per meglio servire anche la fascia tra 600 e 1.000 ci mancava una via di mezzo, un mix tra il co-monitoring e il countercept, un MDR Light».

Perché scegliere WithSecure

«Oggi il mondo della cybersecurity è un po' il cavallo vincente, il carro sul

quale tutti cercano di salire. I vendor sono tantissimi, con prodotti più o meno uguali ma con storie di lunghezza diversa. Noi non siamo arrivati da poco: ci lavoriamo dal 1988!»

L'innovazione è un fattore essenziale che spesso viene valutato sull'aggressività del marketing più che sui reali risultati. «Noi facciamo un marketing tradizionale: in tantissime cose siamo anche stati pionieri, però la nostra anima è finlandese, non lanciamo slogan».

Per i finlandesi il marketing e la comunicazione non vanno gridati come in altri modelli promozionali: se il prodotto è buono andrà bene, dicono loro. «Abbiamo da sempre delle realtà tecniche che potevano essere proposte con maggior enfasi, ma per scelta non le spingiamo più di tanto: al massimo diciamo che una certa feature della quale si parla tanto è nella nostra roadmap».

Scegliere WithSecure vuol dire essere europei. «Siamo finlandesi, quindi siamo europei, convinti di esserlo. I vendor europei non due o tre». In questo periodo, particolarmente, è importante essere europei: «Gdpr, Pnrr e in particolare Nis2 sono solo una spinta ulteriore: un cliente che sta in Europa è giusto che si affidi a un player europeo e i nostri data center sono in Finlandia e in Polonia».

Adesso.it è la “digital factory” italiana del gruppo internazionale Adesso, specializzata in progetti di modernizzazione delle applicazioni core, garantendo la continuità di business e promuovendo approcci allo sviluppo basati sul metodo Agile. L'intervista al CEO Francesco Micotti. »»



Francesco Micotti



Adesso.it partner per lo sviluppo Agile

di Riccardo Florio

Adesso.it è il nuovo brand di Webscience, software house fondata nel 2000 dallo spin-off di un centro di ricerca del Politecnico di Milano e confluita nel Gruppo tedesco Adesso, una realtà internazionale che ha registrato un fatturato di 1,14 miliardi di euro nel 2023. Adesso.it oggi funge da avamposto del Gruppo sul territorio italiano, proponendo progetti di sviluppo e di modernizzazione applicativa basati sul metodo Agile. **Francesco Micotti, CEO di Adesso.it**, ci guida alla scoperta dell'azienda e del suo valore aggiunto.

Cominciamo ricordando il core business di Adesso.it

Siamo specializzati nella modernizzazione applicativa utilizzando tecnologie all'avanguardia, sia per quanto riguarda l'aggiornamento di applicazioni esistenti sia per lo sviluppo di nuove soluzioni da zero.

Cosa è cambiato nel passaggio da Webscience ad Adesso.it?

Adesso è un gruppo molto importante, anche se poco conosciuto in Italia, e siamo stati scelti da loro nel 2022, cosa di cui siamo molto orgogliosi.

Adesso è presente in tutti i settori industriali e opera sulle principali tecnologie come SAP, ServiceNow, Salesforce e Microsoft, prevedendo anche attività

di sviluppo “custom” che attinge al codice open source. In Italia Adesso.it si configura come la “digital factory” deputata a promuovere un approccio allo sviluppo Agile in contrapposizione alla metodologia Waterfall. Entrare a far parte di un gruppo internazionale, che oltretutto sta crescendo mediamente a ritmi del 25%, ci conferisce maggiore autorevolezza e ci sta aprendo la strada verso clienti che, per politiche aziendali, preferiscono affidarsi a partner di dimensione maggiore e di caratura internazionale.

Qual è il vostro approccio al mercato italiano?

Il nostro obiettivo è introdurre in azienda un nuovo “mindset” per l’approccio allo sviluppo del software, che rappresenta un investimento strategico per molte imprese. L’approccio tradizionale allo sviluppo applicativo si basa sulla definizione di un contratto monolitico al cui interno vengono specificate tutte le caratteristiche e le funzionalità che il software dovrà avere. Questa modalità fa in modo che il fornitore e il committente si incontrino solo all’inizio del progetto e poi al momento della consegna e ha sempre causato problemi. Infatti, il periodo che intercorre da quando si defini-

sce il capitolato tecnico a quando si consegna il software può durare mesi e persino anni. Durante questo tempo, l’azienda cresce, evolve e, a volte, cambia persino modello di business. Il rischio è che il prodotto finale, al momento della consegna, non risponda più alle esigenze attuali dell’azienda.

Come è possibile ovviare a ciò?

Adottando una metodologia di sviluppo Agile.

Agile mira a consegnare al cliente, in tempi brevi e frequentemente, software funzionante e di qualità attraverso uno sviluppo iterativo e incrementale, con una pianificazione adattiva. Il team Agile è composto da tutte le persone necessarie per terminare il progetto software e prevede il coinvolgimento diretto e continuo del cliente nel processo di sviluppo. Agile richiede una roadmap operativa, la definizione dei tempi e delle metriche per misurare la produttività e l’adozione di strumenti per la pianificazione delle successive release e degli item rilasciati iterazione per iterazione. Abbiamo reso questo approccio ancora più pragmatico e oggi siamo in grado di gestire progetti che coinvolgono fino a 62 sviluppatori che operano contemporaneamente sulla stessa “core base”.

Qual è il principale ostacolo che vi trovate a dover affrontare con i clienti?

Il nostro target è costituito da aziende di livello enterprise in settori molto diversi tra loro, dai trasporti al retail, dai servizi finanziari al manufacturing. Alcune grandi aziende sono caratterizzate da una gestione tradizionale, con un'impostazione gerarchica del controllo del budget che si scontra con le richieste dinamiche del modello Agile. A volte dobbiamo vincere la resistenza del cliente che si trova più a suo agio con un approccio allo sviluppo tradizionale.

In cosa si realizza il valore aggiunto di Adesso.it?

Il nostro valore aggiunto si manifesta principalmente nei progetti di modernizzazione applicativa, che sono diventati negli anni il nostro core business. Consentiamo alle aziende clienti di intervenire sul portafoglio legacy e farlo evolve nel tempo, mantenendo in ogni istante la continuità di business. Ci piace dire che riusciamo a "cambiare il motore durante il volo". Questo aspetto è molto apprezzato dai clienti perché, quando si lavora sul core business, non è possibile fermarlo e l'attività deve proseguire indisturbata.

Come garantite questa continuità di business?

Per esempio, riscriviamo le applicazioni da zero in modo che possano entrare in produzione parallelamente a quelle preesistenti, insistendo sul medesimo database. La nuova applicazione è disponibile senza rallentare quella vecchia e senza interrompere la continuità di business.

Quindi, nella fase intermedia, gli utenti possono utilizzare due applicazioni per svolgere il medesimo compito?

Nella fase di transizione, gli utenti avranno a disposizione entrambe le applicazioni e, una volta implementate e testate tutte le funzionalità della nuova, sarà possibile disattivare l'applicazione precedente e passare senza soluzione di continuità alla nuova, avendo già avuto modo di utilizzarla e acquisire familiarità.

Si tratta di un processo che richiede tempo poiché interviene sul core business e deve gestire anni di modifiche e customizzazioni stratificate del software, che rappresentano la ricchezza del software del cliente ma lo rendono complesso e difficile da riunificare in uno sviluppo coerente. Per questo è importante adottare tecniche di co-design e interagire costantemente con il cliente, lavorando per iterazioni incrementali, come previsto dal metodo Agile.



Quale futuro per la virtualizzazione

di Fabrizio Pincelli

A sei mesi dall'acquisizione di VMware da parte di Broadcom, facciamo un po' il punto della situazione per capire cosa è successo (e sta succedendo) nel mondo della virtualizzazione, da cui dipende il business di molte aziende, sia clienti sia partner



Hock Tan
Ceo di Broadcom



Sono ormai trascorsi sei mesi dall'acquisizione di VMware da parte di Broadcom e una domanda permea ancora il mondo IT: quale sarà il futuro della virtualizzazione? Ma, soprattutto, la virtualizzazione avrà un futuro? A chiederselo sono in molti, tra clienti e partner di VMware, che, a vario modo, sulla virtualizzazione avevano basato il proprio business. E se lo domanda anche la commissione Antitrust della UE, che ha di recente chiesto chiarimenti a Broadcom a seguito delle lettere di protesta inviate da alcune associazioni di settore, come quella dei service provider europei (CISPE), e di clienti VMware, preoccupati di come sta procedendo la gestione del licensing, del supporto e degli accordi con le terze parti. In particolare, i clienti avrebbero denunciato gli improvvisi cambiamenti di policy e di prassi da parte di Broadcom, che avrebbero portato a forti aumenti di prezzo, al re-bundling delle licenze, al

divieto di rivenderle e al rifiuto di mantenere le condizioni di sicurezza per le licenze perpetue. Mentre, il CISPE (che vede tra i suoi membri anche Amazon e 26 cloud provider europei) si sarebbe lamentato del fatto che Broadcom avrebbe annullato i termini di licenza per i software di virtualizzazione essenziali. Particolarmente eclatante è il caso di Amazon che, a fronte di una decisione unilaterale di Broadcom, **non può più rivendere VMware Cloud on AWS**, nemmeno tramite i partner di canale. In un post sul blog aziendale, il **Ceo di Broadcom Hock Tan** ha precisato: «*I clienti che in precedenza avevano acquistato VMware Cloud on AWS da Amazon, per rinnovare i loro abbonamenti ed espandere i loro ambienti ora si rivolgeranno direttamente a Broadcom o a un suo rivenditore autorizzato*».

Leader indiscusso di mercato

Prima dell'acquisizione, quello della virtualizzazione era un settore florido: secondo **Research & Markets**, il mercato globale del software di virtualizzazione nel 2022 ha fatto registrare un giro d'affari **57,3 miliardi di dollari**. Considerando i trend degli anni precedenti, la società di ricerca stimava che il mercato potesse raggiungere i 190,7 miliardi di dollari entro il 2028, con un tasso di crescita (CAGR) del 20,53% annuo. All'interno di tale mercato, VMware era leader indiscusso con uno share globale circa del 45%, ma in determinati settori raggiungeva addirittura picchi superiori all'80% (come

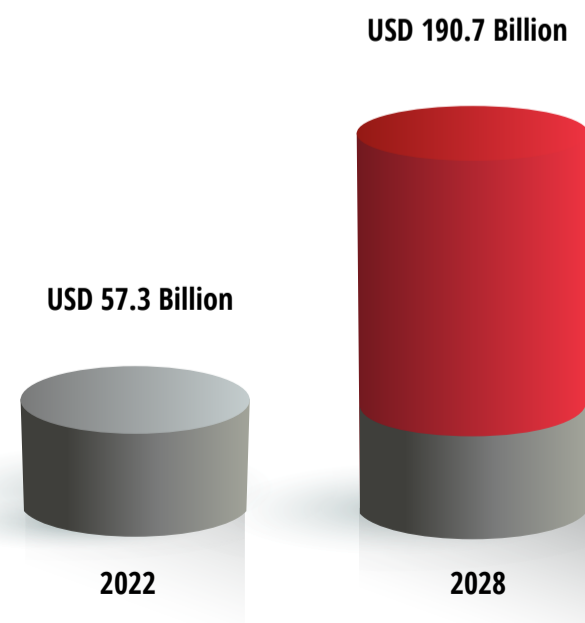
per esempio nel caso dell'uso di vSphere nell'ambito hypervisor).

Virtualizzazione, un futuro incerto

L'acquisizione di Broadcom ha però portato uno stravolgimento al mercato. Infatti, notizie relative alle strategie di integrazione di VMware e della gestione del suo patrimonio tecnologico non solo non hanno fornito efficaci assicurazioni sul futuro della virtualizzazione, ma hanno portato a una destabilizzazione di partner e clienti. Immediatamente dopo l'acquisizione, VMware ha subito una significativa riorganizzazione, che ha portato al licenziamento del Ceo e di oltre 2.000 dipendenti. Inoltre, l'azienda è stata segmentata in quattro parti. Il Ceo Hock Tan aveva precisato che tali mosse erano parte di una strategia basata sulla consolidata capacità della stessa Broadcom di far crescere con successo le organizzazioni acquisite. Tuttavia, espe-

MERCATO GLOBALE DEL SOFTWARE DI VIRTUALIZZAZIONE

Fonte: Research & Markets



rienze pregresse di acquisizioni, come sono state quelle di Symantec e CA, hanno mostrato risultati decisamente differenti da quelli prospettati da Hock Tan.

Un solo programma per i partner

Esempi che hanno fatto nascere una fondata preoccupazione tra clienti e partner di VMware. A poco sono valse le rassicurazioni della **vice president Global Partner e Commercial Sales di Broadcom, Cindy Loyd**, che in un post ha invitato i 18.000 partner attivi di VMware ad aderire al Broadcom Advantage Partner Program. Tuttavia, non è ben chiaro come tra gli oltre 25.000 partner che dichiarava VMware, ne siano stati selezionati 18.000. Loyd ha promesso miglioramenti per i partner selezionati, con una maggiore coerenza nelle offerte e semplificazioni in prezzi e sconti. Però è arrivata anche la decisione dell'azienda di seguire direttamente i primi 2.000 clienti (in termini di importanza e fatturato).

Offerta ridotta e rinnovata

Broadcom ha semplificato l'offerta eliminando diversi prodotti e piattaforme VMware, inclusi vSphere+, Aria Suite e NSX, oltre all'hypervisor gratuito ESXi. Oggi il listino prevede due soluzioni: **VMware Cloud Foundation (VCF) e VMware vSphere Foundation (VVF)**. Inoltre, è stata ceduta al fondo KKR l'unità di computing "end-user" di VMware, che comprende le offerte Workspace ONE e Horizon. È stata

poi interrotta la vendita di licenze perpetue, spingendo i clienti verso un modello di supporto su abbonamento.

Il nuovo ruolo del canale

In un recente post, Tan ha sottolineato l'importanza dei partner nel successo con i clienti ma ha anche annunciato modifiche significative. Tan ha affermato che *«i clienti devono essere liberi di spostare i loro carichi di lavoro tra i data center e i fornitori di cloud, e tra diversi fornitori di cloud»*.

Per garantire condizioni uniformi per tutti i fornitori di cloud, è stata introdotta la standardizzazione dei prezzi e delle licenze per il VCF. Broadcom ha inoltre imposto anche la standardizzazione dello stack tecnologico di VCF per i partner, al fine di agevolare la transizione dei carichi di lavoro tra ambienti on-premises e cloud.

Anche la strategia per i partner è stata rivista per accogliere una gamma più ampia di provider, anche i fornitori di servizi più piccoli che non soddisfano ancora i criteri del Premier Tier.

Tan ha infine assicurato il supporto per le licenze perpetue di VMware vSphere e la disponibilità, secondo le attuali politiche di abbonamento, patch di sicurezza zero-day anche per le versioni non più supportate. Mosse importanti, ma che non lasciano del tutto tranquilli delle aziende che hanno puntato sulla virtualizzazione. E le richieste dell'Antitrust UE ne sono una dimostrazione.

Formlabs rivoluziona la stampa 3D con Form 4

di Maurizio Ferrari

Questa stampante a resina liquida, grazie al rinnovato motore di stampa, è il nuovo punto di riferimento per il mercato della prototipazione e non solo



La stampante 3D Form 4 di Formlabs

L'ultima fatica di Formlabs, Form 4, è destinata a dare uno scossone al mercato della stampa 3D. Si tratta di un **modello a resina liquida** (SLA), caratterizzato da una nuova tecnologia che permette alla Form 4 di essere veloce, precisa e affidabile. Questa stampante è la nuova tappa di un viaggio iniziato da un gruppo di studenti del MIT nel 2012 con la prima Form 1, da allora di passi in avanti ne sono stati fatti molti, portando Formlabs da "garage" a una realtà presente in tutto il mondo. La Form 4 è già disponibile dai **partner di Formlabs che operano sul mercato italiano: 3DIItaly, Solid-Manufacturing, 3DZ, Manufat e Ciano Shapes**. Sono loro l'interfaccia tra i clienti e la Formlabs; si tratta di realtà che hanno acquisito competenze specifiche nel mondo della stampa 3D e nella prototipazione.

Velocità uguale risparmio

Questo modello utilizza un potente motore di stampa, denominato **Low Force Display**, in grado di velocizzare il processo di solidificazione della resina. La tecnologia sviluppata da Formlabs ha permesso di ridurre la chimica all'interno delle resine e, così, renderle meno costose. Questa potenza si traduce anche in maggiore velocità; rispetto al modello precedente, per la stampa di uno stesso pezzo, per esempio un alloggiamento per componentistica elettronica, si passa da circa 10 ore e 35 minuti a 2 ore. Questo significa che i tempi di ricerca e sviluppo, e di design vengono ridotti in modo sensibile e diventa possibile disegnare e prototipare in giornata.

Sensori per massima efficienza

La Form 4 è ricca di sensori che permettono di avere il totale controllo del lavoro, automatizzando quasi tutto. È pronta a stampare in pochi minuti, basta inserire il vassoio e la cartuccia della resina scelta e grazie al programma PreForm la pianificazione del lavoro sarà semplice, le strutture di sostegno le calcola in modo automatico il software. Nel caso fosse necessario intervenire per cambiare qualche componente, la Form 4 si autocalibra e torna immediatamente operativa. **Sono disponibili diverse resine, adatte a ogni tipologia di utilizzo, dal meccanico al biomedico**, per quest'ultimo caso Formlabs propone un modello ad hoc specifico per il mondo degli **odontotecnici e delle componenti medicali**. Form 4 è

in grado di stampare un modello di arcata dentale in soli 49 secondi, cioè 9 minuti per una piastra completa, prima per una piastra ci voleva 1 ora e 32 minuti. La soluzione si completa con il sistema di lavaggio automatizzato Form Wash e nel caso di applicazioni biomediche con Fast Cure per la polimerizzazione post-stampa.

La stampa 3D va (quasi) in produzione

Oggi il divario tra prototipazione e produzione si è ristretto, soprattutto quando è necessario realizzare pochi componenti od oggetti personalizzati. Un esempio è la **collaborazione tre Formlabs, Unilever e Serioplast per velocizzare il processo di design e prototipazione** dei flaconi di plastica per detersivi. L'uso di stampanti SLA di Formlabs ha permesso di realizzare degli stampi modulari idonei alla produzione di flaconi con la tecnologia SBM (stiro e soffiaggio) da parte di Serioplast. Il risultato finale è stato un prodotto di test con una qualità paragonabile a quella della produzione standard con tempi e costi ridotti.



L'APPROFONDIMENTO



Il violino di Paganini creato da 3DItaly

Dalla scansione 3D al prodotto finito sono bastati solo tre giorni.



continua a leggere



Conoscenza e competenza premianti sul mercato

In un momento dove la mancanza di personale formato è tangibile, le aziende ICT puntano a far crescere i propri dipendenti e i propri partner così da essere sempre allineati con l'evoluzione tecnologica.

di Maurizio Ferrari

Scientia potentia est! Oggi questo aforisma di Francesco Bacone e Thomas Hobbes è più che mai attuale. Il mondo ICT italiano sta affrontando, da diversi anni ormai, un vuoto di conoscenza e di competenze. L'evoluzione tecnologica è stata più veloce e rivoluzionaria rispetto alle capacità formative del Sistema Italia e nel giro di poco tempo il divario tra domanda e offerta si è ampliato in modo preoccupante, sino a diventare un problema serio in questo periodo. L'Italia, in realtà, soffre da sempre di un deficit di competenze digitali; come segnalato dal **Digital Decade Country Report 2023** della

Commissione Europea, nel nostro Paese solo il 46% della popolazione possiede quelle di base. Da questo punto di vista siamo pericolosamente arretrati, gli obiettivi del 2030 saranno difficili da raggiungere, nonostante gli sforzi fatti con il PNRR. La media europea dei laureati in materie ICT è del 4,2%, in Italia crolla all'1,5%. Percentuale insufficiente per il mercato italiano: **il 77% delle aziende, secondo una ricerca di Manpower, ha problemi a trovare personale IT con le giuste competenze.** Per la Commissione Europea l'Italia dovrebbe intensificare gli sforzi per le competenze digitali, in par-

ticolare per l'aggiornamento e la riqualificazione della forza lavoro. Secondo la ricerca **Previsioni Dei Fabbisogni Occupazionali e Professionali in Italia a Medio Termine** per il periodo 2024-2028 di Unioncamere le competenze digitali verranno sempre ricercate, nel prossimo quinquennio si stima, nello scenario migliore, che saranno circa 2,1 milioni gli occupati, meno del 59% del fabbisogno totale. L'incremento degli investimenti in tecnologia ICT, favorito anche dai fondi del PNRR, determina una domanda elevata di nuove figure professionali, capaci di operare su cloud, mobile, big data analytic, cyber security, IoT, sviluppo software, intelligenza artificiale e robotica. Diventa fondamentale per le società che operano nel settore dell'ICT aumentare il livello di competenza del proprio personale, sia attraverso il mercato del lavoro sia ricorrendo alla formazione continua dei dipendenti. In questo panorama abbiamo chiesto ad alcune aziende

come operano per avere personale formato sulle ultime tecnologie, e il valore aggiunto che porta avere figure certificate in casa.

A rompere il ghiaccio è **Romeo Scaccabarozzi, amministratore delegato di Axiante**, che mette sul tavolo la propria esperienza e sottolinea l'importanza di avere dipendenti costantemente formati sulle ultime tecnologie. *«Come per tutte le aziende che operano nel settore ICT, per Axiante l'asset più importante è rappresentato non dalle tecnologie, ma dalle conoscenze e competenze delle persone. Queste devono essere costantemente aggiornate per soddisfare le esigenze dei clienti. Mentre le tecnologie sono in continua evoluzione, le metodologie cambiano a un ritmo meno elevato: i fondamentali sono spesso costanti, ma c'è bisogno di farli conoscere a chi entra per la prima volta in azienda. Ecco perché ci concentriamo molto sull'attività di formazione dei nuovi assunti e di coloro che cambiano di ruolo all'interno dell'organizzazione. Al contrario di quelle metodologiche, le conoscenze tecnologiche vanno invece aggiornate costantemente con un mix di pratica e teoria: in Axiante promuoviamo corsi specifici legati alle singole tecnologie e cerchiamo di fare in modo che quanto appreso venga applicato il prima possibile su progetti esterni o interni. In quest'ottica, il conseguimento di*



Relazione 2023 sullo stato del decennio digitale

La relazione sullo stato del decennio digitale fa il punto sui progressi compiuti dall'Unione europea verso una trasformazione digitale riuscita, come stabilito nel programma strategico per il decennio digitale 2030

[+ SCARICA LA RELAZIONE](#)

una certificazione rappresenta il momento formale in cui viene misurato il percorso di apprendimento delle persone che lavorano in Axiante. La sfida per noi è dunque quella di fidelizzare i nostri collaboratori, in modo che le certificazioni restino in azienda. Il know how sta nelle persone ed è un elemento di motivazione e sviluppo delle competenze, più che un risultato da esibire. Come Axiante crediamo fortemente nell'aggiornamento delle conoscenze, come fattore di crescita delle persone e di conseguenza anche dell'organizzazione».

Il costante aggiornamento è un punto focale anche per **Fabio Buccigrossi, country manager di ESET Italia**, ma devono essere sempre sul pezzo tutti, sia i propri dipendenti sia i partner. «Per ESET, investire nello sviluppo di percorsi



di formazione e certificazione è essenziale. Le risorse interne nel settore della sicurezza informatica devono rimanere costantemente aggiornate sia commercialmente sia tecnicamente per offrire soluzioni al passo con le reali esigenze dei clienti. In particolare, per i cybersecurity specialist che gestiscono i servizi MDR a livello locale, ESET fornisce corsi di ethical hacking e training sul monitoraggio e la risposta agli incidenti di sicurezza, garantendo loro la preparazione necessaria per affrontare efficacemente le sfide quotidiane del

SOC. Per i partner, ESET ha sviluppato un completo percorso di formazione e certificazione. Attraverso il portale dedicato e il supporto dei distributori, che agiscono come Centri di Formazione Autorizzati (ATC), vengono offerti corsi aggiornati sulle soluzioni ESET, disponibili gratuitamente online o a pagamento in aula. L'obiettivo di questi percorsi è elevare la cultura e la consapevolezza sulla sicurezza informatica, affiancando i partner nella gestione delle sfide di sicurezza dei clienti. Questo approccio consente ai partner di acquisire competenze sulle tecnologie ESET e di affrontare le minacce attuali, garantendo un servizio di sicurezza informatica completo e di qualità. ESET riconosce che la formazione continua è essenziale per mantenere standard elevati di sicurezza e protezione dei dati in un ambiente sempre più complesso e in evoluzione».

Secondo **Imma Cinquegrana, People Specialist HR Department in FAR Networks Group**, il miglior biglietto da visita per il mercato è avere personale formato e aggiornato sull'evoluzione tecnologica. «In FAR Networks Group, per assicurarci che il team sia sempre aggiornato sulle ultime tecnologie, adottiamo una strategia di formazione continua. Definiamo annualmente interventi formativi ad hoc per ogni gruppo professionale, delineando le esigenze con i rispettivi manager, in continuità con il per-





Previsioni dei fabbisogni occupazionali e professionali in Italia a medio termine (2024-2028)

Gli scenari futuri del mercato del lavoro in Italia

[+ SCARICA IL DOCUMENTO](#)

corso di carriera dei colleghi. Garantiamo l'accesso a riviste specializzate e a piattaforme di e-learning, promuoviamo, organizziamo e partecipiamo a eventi del settore per apprendere direttamente dagli esperti e fare networking. Prevediamo attività di mentorship e coaching interno attraverso le quali le risorse esperte guidano i membri dei team meno esperti. Secondo la nostra esperienza, le certificazioni influenzano positivamente la percezione dei partner perché dimostrano il nostro costante impegno alla qualità e all'aggiornamento professionale. Aiutano, inoltre, a distinguersi in un mercato competitivo, infatti, le certificazioni confermano ufficialmente le competenze e le conoscenze nel settore e migliorano le prestazioni lavorative: ciò che si impara durante la formazione per una certificazione può essere applicato direttamente sul lavoro. Un'azienda con personale costantemente aggiornato non acquisisce solo un valore per sé, ma mostra ai suoi partner e clienti quanto tiene alla qualità

dei suoi prodotti e servizi e quanto importante sia ogni persona e ogni team».

Formare su tutto e tutti, personale e partner, è la strada che percorre Cohesity, come spiega **Matteo Ghielmi, channel development Southern Europe and emerging di Cohesity**.

«In Cohesity crediamo nel valore delle competenze, sia per il team interno sia per l'ecosistema di canale, come strumento fondamentale per il raggiungimento degli obiettivi di business. Ecco perché i partner Cohesity



possono accedere a diversi programmi, progettati per renderli autonomi durante tutto il ciclo di vendita: si va dalle Accreditation Sales e Presales, presenti sul nostro Partner Portal, fino alla PS Authorization, che permette di formare competenze identiche a quelle dei nostri professional service. Questa certificazione autorizza i partner a effettuare servizi di installazione e implementazione autonomamente, così da poter incrementare la marginalità legata ai progetti. Da poco abbiamo, inoltre, lanciato l'ACE Program, un programma dedicato alla prevendita dei partner, che prevede tutta una serie di vantaggi. Tra le altre cose, permette, al conseguimento della certificazione, di poter accedere a demo lab da usare con clienti e prospect. A livello italiano, abbiamo affiancato alle iniziative corporate due progetti dedicati alla formazione dei nostri partner: il primo prende il

nome di "Cohesity Pills" e consiste in una serie di webinar con cadenza mensile dedicati a temi tecnici verticali; il secondo progetto si concretizza negli "ACE Summit", eventi semestrali dedicati alla comunità degli ACE italiani, che prevedono sessioni dedicate all'approfondimento di tematiche di natura tecnica e workshop, per portare dalla teoria alla pratica quanto condiviso durante la giornata».

L'importanza di avere partner formati e di aiutarli a raggiungere questo risultato è al centro dell'intervento di **Alessandro Riganti, country manager per l'Italia di D-Link**. «Le tecnologie si evolvono costantemente. Per rimanere al passo con le ultime novità, è importante garantire la corretta formazione sia al personale interno sia a tutti i partner di canale,



che rappresentano i nostri "avamposti" sul mercato. Il successo di D-Link come

fornitore di soluzioni di networking e di connettività si fonda sul costante impegno nel creare valore per i partner, soprattutto in termini di formazione e certificazione. I corsi di certificazione di D-Link sono strumenti di formazione, online o on-site, che permettono ai partner di canale di maturare tutte le conoscenze sulle soluzioni D-Link e ottenere il massimo dalle tecnologie proposte. Migliorando le competenze del proprio team, i partner hanno la possibilità di intervenire e di rispondere

tempestivamente alle esigenze in costante mutamento dei clienti. La formazione D-Link prevede approfondimenti sales e tecnici ed è focalizzata su tecnologie specifiche: switching, wireless, nuclias e soluzioni industriali. I corsi D-Link Sales Specialist (DSS) sono ideati per i professionisti sale e si focalizzano su identificazione delle opportunità di mercato e comprensione delle esigenze dei clienti, definizione dei vantaggi delle soluzioni D-Link, valore, proposta e posizionamento del prodotto. I corsi D-Link Certified Specialist (DCS) sono dedicati ai team tecnici e forniscono le conoscenze necessarie per implementare al meglio le soluzioni D-Link e offrire il corretto supporto ai clienti, nelle fasi pre e post vendita».

L'importanza dei partner certificati è sottolineata anche da **Luca Besana, senior channel business manager della Mediterranean Region di SentinelOne**. «Per assicurare che il nostro team e i partner siano sempre all'avanguardia sulle ultime tecnologie a

portfolio, abbiamo implementato un rigoroso processo di validazione delle partnership, per cui solo i partner certi-



ficati possono vendere le soluzioni di SentinelOne. Questo non solo garantisce una conoscenza approfondita dei prodotti e servizi, ma contribuisce anche a mantenere uno standard qualitativo elevato. Abbiamo poi deciso di dare accesso gratuito a tre percorsi formativi ai part-

ner, distinti tra commerciale, prevendita e tecnico, che sono progettati per fornire conoscenze approfondite su come promuovere, presentare e supportare efficacemente le nostre soluzioni. A supporto di ciò, è stato inoltre dedicato un team specifico alla formazione del canale, un team che si impegna attivamente a sviluppare e aggiornare con sessioni di formazione sia online che in presenza, con l'obiettivo di garantire che il canale sia sempre ben informato sulle ultime novità. Riconosciamo che il canale è la nostra vetrina e che la soddisfazione del cliente dipende in gran parte dalla qualità dei nostri partner. È per questo motivo che investiamo in modo significativo nella formazione e, le certificazioni, giocano un ruolo fondamentale nel processo di aggiornamento del nostro canale. Le certificazioni influenzano positivamente anche la percezione dei nostri partner: essere certificati suggerisce un impegno verso l'eccellenza e un alto livello di professionalità, elementi che i clienti apprezzano ulteriormente».

Mirko Rinaldi, chief technology officer di Quanture, ha messo in evidenza come la formazione sia centrale per il business e per essere all'avanguardia è necessario investire per aumentare le competenze del proprio personale e anche dei partner. «La formazione del personale tecnico è cruciale nel settore ICT e in Quanture. Data la rapida evoluzione del settore, riteniamo che l'apprendimento conti-



nel settore ICT e in Quanture. Data la rapida evoluzione del settore, riteniamo che l'apprendimento conti-

Conoscenza e abilità nel cuore di Arrow

Michele Puccio, country manager Italia di Arrow, sottolinea l'importanza della formazione continua e delle certificazioni, che rappresentano per l'azienda il perno fondamentale per garantire servizi di eccellenza. L'investimento costante in queste aree è essenziale per mantenere aggiornati sia i team interni che i partner,



permettendo loro di affrontare con competenza le rapide evoluzioni del settore ICT. «Arrow Enterprise Computing Solutions svolge da anni il ruolo di distributore a valore nell'aiutare i partner a supportare i processi di digitalizzazione del paese. Siamo un "advisor" capace di coordinare i più importanti player e mettiamo a fattor comune le nostre specificità per elevare il valore della partnership. Al centro di tutto, il nostro know how e le competenze delle persone su cui continuiamo a investire in modo significativo. Infatti, la qualità e l'ampiezza della gamma di servizi da noi offerti ha ricevuto molteplici riconoscimenti dal mercato, basti pensare al premio di fine 2023 dove Training Industry, società di ricerca per i leader della formazione aziendale a livello internazionale, ci ha selezionato come una delle 20 migliori aziende di formazione del 2023. Il premio conferma la nostra leadership nella formazione IT verso i reseller e riafferma il fatto che in un contesto in cui le aziende si avvalgono di molteplici soluzioni IT, l'offerta formativa di Arrow, sempre più completa e in evoluzione, consente alle imprese di gestire efficacemente gli ambienti complessi e di rimanere competitive. Con i nostri servizi siamo in grado di supportare il partner in ogni fase, dalle attività di pre-sales alla consulenza post-vendita e al training on the job. Non manchiamo infine di aggiornare i partner sulle ultime novità tecnologiche, vedi il recente annuncio sulla formazione offerta ai rivenditori per accelerare le opportunità con Copilot di Microsoft 365».



GLI APPROFONDIMENTI
BIZZIT



Trasformazione digitale:
soluzioni, tecnologie e servizi

[+ continua a leggere](#)

nuo sia essenziale per garantire servizi di alta qualità ai nostri clienti. Per perseguire questo obiettivo, abbracciamo un approccio dinamico. Destiniamo una quota annuale significativa, pari al 20% dei nostri utili, alla formazione del personale. Organizziamo regolarmente una grande varietà di iniziative, dalle più tradizionali come corsi e materiale manualistico, alle più moderne e mirate come eventi, workshop e confronti interni. In particolare, questi ultimi fungono da catalizzatori per lo scambio di conoscenze e il confronto di best practice tra i nostri Senior Engineer/Architect e i membri più giovani del team. Questa condivisione ci consente di rimanere al passo con le ultime tendenze e di adattare rapidamente le nostre soluzioni alle esigenze dei clienti. Le certificazioni, seppur impegnative, rappresentano un importante riconoscimento di qualità. Sottolineano il nostro impegno nel fornire soluzioni efficienti, a beneficio dei clienti. La nostra selezione rigorosa dei partner tecnologici, limitata a un

numero ristretto, ci consente di concentrarci sullo sviluppo di competenze altamente specializzate e verticali. Questo approccio ci permette di tradurre tali competenze in servizi innovativi e su misura, perfettamente allineati alle moderne esigenze di business delle imprese».

Silvana Suriano, sales engineering leader Italy cluster di Avaya, ha spiegato che per aggiornare le competenze del proprio personale e dei partner ricorre sia a risorse interne sia esterne per offrire sempre il meglio.

«L'aggiornamento delle competenze di dipendenti e partner è da sempre elemento di grande attenzione per

Avaya; infatti, siamo convinti che supportare il cliente con competenze specialistiche certificate sia un modo per aggiungere ulteriore valore ai nostri servizi e prodotti. Le attività di aggiornamento tecnico e certificazione sui nostri prodotti e servizi, e su quelli dei nostri partner tecnologici sono realizzate fissando obiettivi su base annuale, sulla base dei quali sono definiti programmi di training e certificazione differenziati in base al ruolo (progettazione/pre-vendita, vendita, postvendita). I training sono erogati attraverso risorse interne quali Avaya Learning, accessibile anche ai nostri business partner, e risorse esterne, quali, ad esempio la formazione offerta da LinkedIn o su Academy di partner tecnologici. Il possesso di certificazione specialistica, in particolare per i business



delivery partner, è un requisito mandatorio per Avaya e ci permette di mantenere il livello di elevata qualità che da sempre ci contraddistingue. La formazione dei partner è completata anche attraverso l'erogazione di sessioni di approfondimento con gli esperti di Avaya. Per il cliente il possesso di una certificazione in ambiti specialistici, quali la sicurezza, il project management o l'amministrazione di prodotti e servizi dovrebbe essere un requisito imprescindibile nella scelta di un partner tecnologico».

La filosofia adottata durante il processo di assunzione del personale da **Miguel del Moral, channel sales director Southern Europe di Vertiv**, considera, oltre alle competenze, la voglia di crescere e la curiosità, perché un candidato deve dimostrare di comprendere le esigenze del cliente. «Come responsabile di un



team di vendita e appartenendo a una multinazionale che produce soluzioni per le infrastrutture digitali critiche e le soluzioni di continuità delle imprese, ritengo che il principale ingrediente per lo sviluppo del business ruoti proprio intorno alle persone. Infatti, durante le fasi di recruiting, non ho considerato solo le imprescindibili conoscenze tecniche e commerciali dei candidati, ma ho cercato di valutare la loro "curiosità",

la capacità di mantenere sempre un costante desiderio e interesse a imparare, a scovare le reali esigenze dei clienti e a riconoscere il valore che la tecnologia può apportare a ogni processo di business. Ovviamente questo non è sufficiente, dobbiamo poi essere in grado di fornire gli strumenti adeguati ad aiutare non solo i dipendenti, ma anche i nostri partner ad apprendere e a perfezionare le conoscenze. È per questo motivo che abbiamo messo a disposizione sul Vertiv Partner Portal una sezione dedicata dove sono disponibili corsi di formazione sulle nostre tecnologie e soluzioni. Inoltre, a seconda del livello di partnership, offriamo livelli di certificazione per formare i partner nella maniera più completa possibile. Il nostro obiettivo è rendere i partner veri e propri "ambasciatori" di Vertiv per qualsiasi tipo di soluzione e servizio tecnologico, affinché siano capaci di guidare e supportare i clienti durante il lungo e, a volte complesso, percorso necessario per la trasformazione digitale delle aziende».

La formazione continua è dunque fondamentale per riuscire a cavalcare sempre l'onda. Questa va ad aggiungersi alle conoscenze acquisite durante il percorso scolastico; queste ultime servono per entrare nel mondo del lavoro, ma poi è necessario continuare a crescere assieme all'evoluzione delle tecnologie.

bizzIT.it

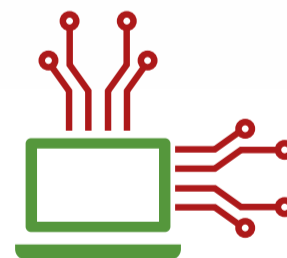
MAGAZINE ONLINE
DI ICT E TECNOLOGIA



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/>