

# Insieme contro i rischi: l'eccellenza di una sinergia Made in Italy

*Attacchi sempre più sofisticati e pervasivi alle aziende e alle Pubbliche amministrazioni: la sfida si supera solo offrendo servizi "su misura" e costruendo relazioni durature con i clienti*

Dai primi virus informatici degli anni Sessanta al cambio di scenario che si è avuto con l'ingresso in scena di Internet come strumento di comunicazione di massa, per arrivare fino all'impennata di minacce e di attacchi negli ultimi anni, la cybersecurity ha assunto un ruolo via via sempre più cruciale, assestandosi in una posizione prioritaria nell'agenda IT di ogni azienda, indipendentemente dalle sue dimensioni, dalla sua categoria merceologica e dalla sua collocazione geografica.

Tanto per avere un'idea della scala economica del fenomeno, stiamo parlando di un giro d'affari complessivo che, soltanto in Italia, nel 2023, ha superato i 2,15 miliardi di euro, con un incremento del +16% rispetto al 2022 che sembra essere destinato a essere ribadito anche nel prossimo biennio, secondo quanto emerge dai dati appena pubblicati dall'Osservatorio Cybersecurity & Data Protection della School of Management del Politecnico di Milano.

L'esperienza di numerosi manager del tech italiano insegna, poi, che la pandemia ha portato significativi cambiamenti nel contesto della sicurezza informatica, con un aumento delle minacce e una conseguente e rinnovata attenzione nei confronti del comparto, resa ancora più rilevante dai numeri dell'adozione di dispositivi IoT (*Internet of Things*) e delle relative vulnerabilità.

Il tutto si ritrova ben incastonato in un quadro generale ancora più ampio in cui le normative sulla protezione dei dati, come il GDPR in Europa o il CCPA negli Stati Uniti, impongono agli enti di adottare misure di sicurezza più rigorose e di proteggere adeguatamente i dati personali.

Ciò ha prodotto l'emergere di tante realtà che sono impegnate quotidianamente nell'offrire a PMI e grandi imprese il



Fabio Naccazzani, CEO Akito



Alessio Aceti, CEO HWG Sababa

supporto necessario a fronteggiare in modo efficace i nuovi e i vecchi pericoli provenienti da intrusioni esterne e a garantire l'incolumità delle infrastrutture e delle informazioni, combinando in modo fruttuoso le tecnologie più avanzate di sicurezza informatica con le *best practice* più attuali nella formazione del personale e nelle strategie di vigilanza continua.

#### *Minacce e protezione dei dati*

"Partiamo dal fatto che gli attacchi *ransomware*, il *phishing* e il *social engineering* sono diventati sempre più sofisticati, mirati e diffusi - spiega Fabio Naccazzani, CEO di Akito, system integrator con sede a Perugia, una filiale romana, e una lunga storia di expertise nella cybersicurezza - e sono sempre

più mirati, con truffatori che utilizzano tecniche ingannevoli per ottenere accesso a informazioni sensibili o per introdurre malware nelle reti aziendali". A ciò si aggiunge la specificità del tessuto aziendale del nostro Paese, con la sua conformazione estremamente eterogenea, fatta - da un lato - di un numero assai elevato di piccole o anche piccolissime imprese sparse su tutto il territorio che scontano il limite della scarsa consapevolezza dei rischi cyber, e da grandi imprese o nodi strategici di filiere critiche molto attenti al tema, dall'altro.

Su quest'ultimo aspetto, Alessio Aceti, CEO di HWG Sababa, cybersecurity player italiano (sede legale a Milano, e filiali a Roma, Torino, Genova, Verona, Bergamo e Bari), ma con una presenza

anche al di fuori del nostro Paese (da Dubai, a Vilnius, fino a confini dell'Asia) tiene a mettere l'accento: "Per proteggere correttamente l'ecosistema nazionale dobbiamo pensare alla protezione di tutto il tessuto produttivo e istituzionale. Abbiamo osservato diversi attacchi che prendono di mira la *supply chain*, direi in due 'macro modalità': colpire un grande fornitore di servizi IT o di prodotti software per fermare un vastissimo numero di altre aziende, creando ripercussioni e problemi per diversi settori; oppure attaccare numerose PMI (per esempio, i clienti di un software gestionale) andando a bloccare intere catene di approvvigionamento e produzione".

Il 2024 segnerà un momento-chiave per la cybersicurezza anche per un altro

aspetto: l'ingresso in scena della *Direttiva NIS 2* che, dopo essere stata recepita ha cominciato il suo iter di adozione da parte degli Stati membri dell'Unione Europea. Il provvedimento consente di stabilire e adottare le misure necessarie a garantire un elevato livello comune di cybersecurity nel Vecchio Continente, in modo da migliorare il funzionamento del mercato interno.

"Il recepimento della Direttiva - aggiunge Aceti - andrà ad ampliare il panorama delle aziende che forniscono servizi considerati critici e, certamente, la compliance alle nuove norme fungerà da stimolo all'attenzione per i rischi cyber e per lo sblocco di investimenti in tale direzione, sensibilizzando i board delle aziende che non hanno ancora preso veramente sul serio la questione".

#### *Parola d'ordine: fiducia*

Akito e HWG Sababa sono un caso emblematico, la materializzazione di un modello vincente che insegna come "fare sistema" sia essenziale in un contesto complesso e variegato com'è quello della sicurezza informatica e del mercato che sta alle sue spalle.

A una delle estremità di questa sinergia si colloca l'approccio consulenziale di Akito, che si basa soprattutto sulla sua capacità di instaurare con i clienti relazioni durature nel tempo. Il come lo spiega il suo CEO: "Chi si affida a noi sa che proponiamo soltanto tecnologie in cui crediamo e che può contare su un supporto olistico, attento e competente".

A un livello complementare si colloca la *proposition* tecnologica di HWG Sababa. "Ho sempre considerato la squadra di Akito - gli fa eco Aceti - come la migliore in assoluto nel comparto, soprattutto per la grande attenzione che ha saputo dimostrare nella qualità e nei dettagli. Per entrambi, è fondamentale fornire servizi di altissimo livello e co-

struire un rapporto di estrema fiducia e trasparenza con il cliente, diventando non solo fornitori ma advisor fidati in tema di cybersecurity".

La fiducia: è lei la grande keyword che fa la differenza nel settore: "Oltre alla qualità - chiosa Naccazzani - il cliente ha la necessità di avere qualcuno vicino a lui, che già conosce e di cui si fida, nonché di avere partner tecnologici che sappiamo calare i loro servizi sulle specifiche esigenze, allo stesso modo con il quale un sarto confeziona i suoi vestiti tailor made".

Con una collaborazione roduta, i due gruppi rispondono alle esigenze di sicurezza di imprese medio grandi del settore pubblico e privato che, come sottolineato in precedenza, in un periodo storico sempre più sfidante in tema di attacchi *cyber*, si trovano a gestire ambienti IT, OT e IoT complessi.

"Sì, c'è un grande bisogno di una maggiore visibilità sulla propria infrastruttura, per rilevare in anticipo anomalie e potenziali vulnerabilità. Ma anche di monitoraggio continuo di tutti gli asset e di tutti i dati aziendali", interviene Akito. A tale proposito, vale la pena aggiungere che il SOC (*Security Operations Center*), le strutture dove vengono centralizzate tutte le informazioni sullo stato di sicurezza dell'IT di un'azienda o di un'intera filiera, *nda*) di HWG Sababa ha già avuto un ottimo riscontro in numerosi clienti del settore automotive e in ambito Sanità, che ne hanno apprezzato l'efficacia nel rilevamento di potenziali minacce e la flessibilità del team di lavoro".

Clienti che, conclude Aceti: "Richiedono sempre più spesso di affiancare al servizio gestito anche la presenza di esperti sul territorio che possano essere disponibili *on site* in breve tempo in caso di necessità. Assieme ad Akito, siamo in grado di garantire anche questa operatività ai massimi livelli disponibili nel contesto italiano. E non solo...".