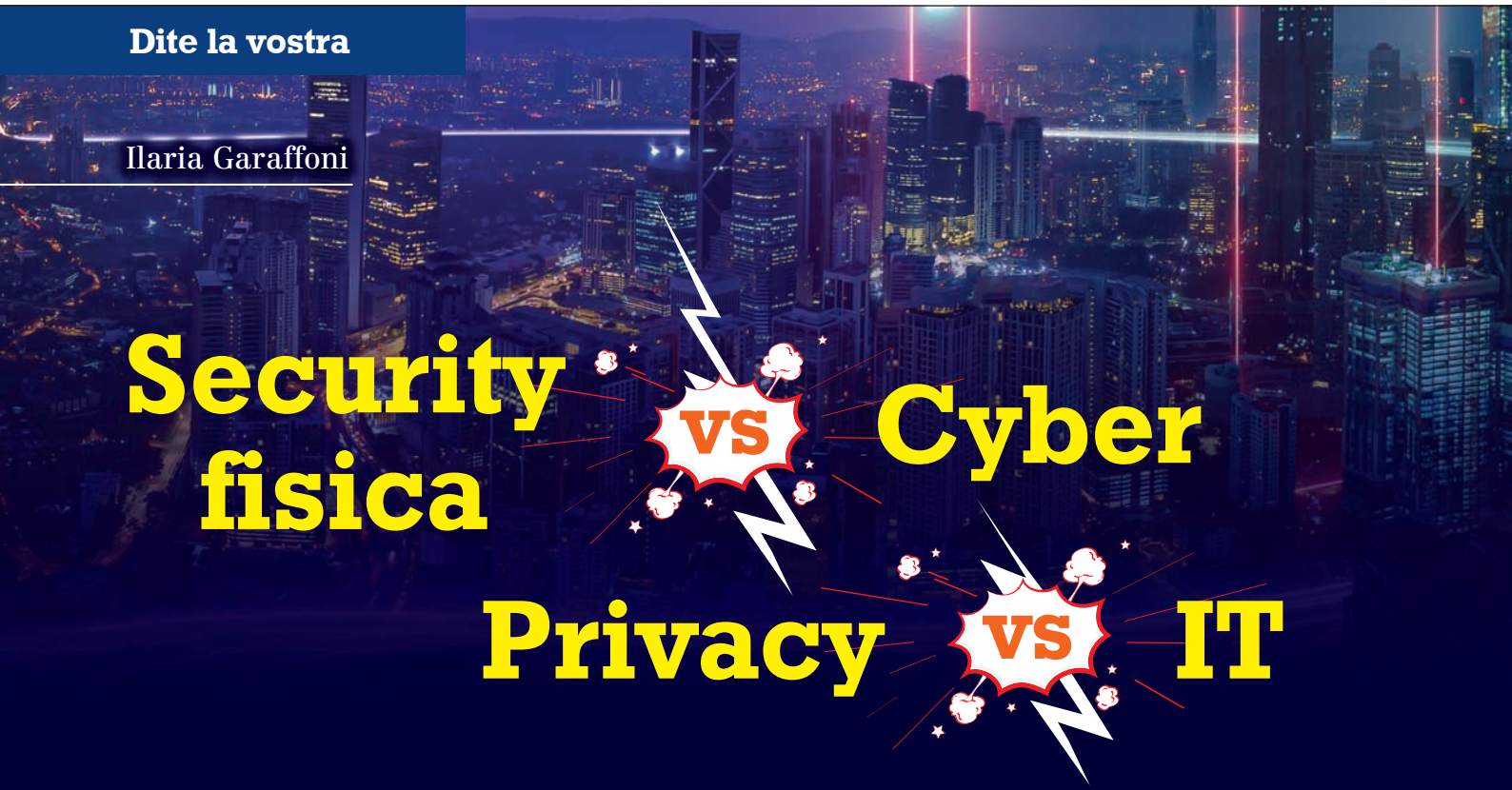
Ilaria Garaffoni




# sicurezza = comunicazione

**Il team che si occupa di sicurezza fisica spesso si scontra con il team che si occupa di sicurezza informatica:** ognuno è geloso del proprio orticello (e del proprio già risicato budget) e non di rado la mentalità è opposta (l'IT vorrebbe vedere "tutto aperto" mentre la security fisica, ma anche cyber, vorrebbe tutti sistemi chiusi e blindati). Ma da tempo ormai le due discipline devono viaggiare a braccetto perché di fatto sono due facce della stessa medaglia. **Stessa relazione conflittuale si verifica in materia di protezione dei dati tra il team che si occupa di compliance (privacy) e il team IT.** Oltre ad una fisiologica difficoltà di comprensione lessicale tra legali e tecnici, resta il fatto che se un attacco informatico non comporta data breach, il team privacy in genere non viene coinvolto, con ulteriori rischi per la protezione dei dati. Come uscire dall'impasse? L'abbiamo chiesto ad esperti dei tre ambiti professionali per capire come conciliare le posizioni per fare vera sicurezza.

*le domande*

1. Il team che si occupa di sicurezza fisica spesso si scontra con il team che si occupa di sicurezza informatica anche se sono due facce della stessa medaglia. Qual è la vostra esperienza?
   Stessa relazione conflittuale si verifica in materia di protezione dei dati tra il team che si occupa di compliance (privacy) e il team IT. Come migliorare le cose?

2. Parliamo di cloud, ormai super usato anche nella sicurezza fisica: quali garanzie di sicurezza cyber possono essere offerte in tal senso?

# Dite la vostra

## Marco Bavazzano

**CEO Axitea - www.axitea.com**

**La cybersecurity è troppo spesso ancora considerata un servizio accessorio all'interno degli investimenti IT, raramente accompagnata da budget dedicati. Il confine tra sicurezza fisica e informatica è sempre più sottile: ad esempio, con la crescente adozione dei sistemi IoT e dell'edge computing, aumenta la minaccia di infiltrazioni e attacchi diffusi ad entrambi i domini, coinvolgendo non solo l'organizzazione stessa, ma anche partner e terze parti. Ad esempio, nella gestione delle patch, è essenziale che il team IT esegua regolarmente aggiornamenti per correggere vulnerabilità, mentre il team di cybersecurity deve verificare che ciò avvenga in modo continuo e puntuale, indicando se necessario le priorità di intervento. In questo scenario, diventa essenziale un cambio di approccio basato su una chiara separazione dei ruoli e da processi interni definiti che coinvolgano i giusti referenti. La relazione conflittuale tra i team di compliance privacy e IT è un'altra sfida da superare. DPO e CISO dovrebbero collaborare strettamente per affrontare le nuove minacce informatiche e applicare efficacemente le normative emergenti. Tuttavia, lacune organizzative e mancanza di formazione spesso portano queste due figure a viaggiare su binari separati. La promozione di una cultura proattiva sull'importanza della sicurezza dei dati, che coinvolga il team privacy fin dalle fasi iniziali della progettazione, e definisca chiaramente ruoli e responsabilità, è cruciale per evitare conflitti e garantire un controllo indipendente".**

## Elisa Ballerio

**Marketing Director di CybergON - https://cybergon.com**

**Nella nostra esperienza il team IT, più che vedere tutto "aperto", vorrebbe vedere tutto predefinito. La security è, invece, un processo in evoluzione e richiede un adattamento nel corso del tempo (basti pensare all'evoluzione continua di metodi di attacco, vulnerabilità, tecnologie). Per soddisfare ambo le parti, occorre impostare una collaborazione molto stretta fin dal principio, specialmente sulla parte identità, accessi e privilegi. Questo aiuta a gettare solide fondamenta in ottica di collaborazione continua e a creare un framework di partenza per eventuali modifiche. Consigliamo un interlocutore fisso nella parte IT del cliente che riesca a contestualizzare e implementare tutti gli elementi di security che emergono nel corso di un progetto. Con i clienti del nostro datacenter noi lo facciamo tramite un gruppo specifico di tecnici che, nell'ambito di un processo ben consolidato, si interfaccia con il SOC per analizzare le problematiche di security e l'impatto che possono avere sui clienti e per proseguire con la messa in sicurezza. Per quanto riguarda privacy e dati, non è sempre come da voi rilevato. Nella nostra esperienza il team privacy viene sempre coinvolto prima dei data breach, proprio nell'attuazione di processi di gestione e messa in sicurezza del dato. Quando questo non accade assistiamo a delle carenze evidenti in termini di configurazione, mancata compliance con il gdpr e altri aspetti".**

## Nicola Lopatriello

**Penetration Tester GFM Group - https://gfm.cloud**

**Eventuali elementi di conflitto tra team IT Security e team di sicurezza fisica all'interno di un'azienda dipendono, prima che dal budget, dalla mancanza di una solida cultura aziendale e quindi di una visione comune. Diffondere a tutti i livelli aziendali l'importanza della protezione dei dati è essenziale affinché i team lavorino in armonia. Questo può essere realizzato attraverso sessioni di formazione condivisa e workshop dove tutti possono comprendere meglio le rispettive esigenze. Altrettanto conflittuale è il rapporto tra team privacy e team IT Security, con l'aggravante dell'effettiva differenza culturale e lessicale tra i due. In questo caso, il primo è interessato alla protezione dei dati personali e a garantire l'effettivo rispetto dei diritti a livello legislativo, il secondo si concentra sulla protezione dei sistemi informatici e dei dati in esso contenuti. Penso che tale gap possa essere colmato solo in parte dalla costruzione di una cultura aziendale, che poi dev'essere necessariamente supportata dall'adozione di uno strumento in grado di riportare sempre le giuste ed essenziali informazioni ad ogni team".**

Dite la vo

## Augusto Fedriani

**Head of Cyber Security Governance Hwg-Sababa - www.hwgsababa.com**

**"La relazione conflittuale tra il team privacy e il team IT è un problema comune a molte organizzazioni, frutto di una difficoltà di comprensione che può portare a mancanza di collaborazione. Tra le strategie utili a mitigare questa contrapposizione vi sono attività di formazione incrociata tra due team, per costruire e promuovere comprensione reciproca, il coinvolgimento del team privacy nei progetti IT critici, partendo dalle fasi di pianificazione e sviluppo per evitare possibili conflitti successivi, e un'attenta definizione delle responsabilità di ciascun team in relazione alla protezione dei dati. È altresì utile un monitoraggio continuo volto ad identificare potenziali rischi per la sicurezza dei dati, una collaborazione strutturata tra i team per discuter sviluppi e sfide, nonché una comunicazione aperta e trasparente, per affrontare eventuali conflitti in modo tempestivo. Infine, è importante identificare obiettivi comuni per i team e attuare valutazioni periodiche finalizzate a determinare l'efficacia delle strategie adottate. Affrontare la complessità della protezione dei dati richiede collaborazione tra team legali e tecnici. Implementando queste strategie, sarà possibile migliorare la comprensione e rafforzare la sicurezza dei dati".**

## Domenico Dominoni

**Director of Sales South Europe Claroty - https://claroty.com**

**"In questo scenario, i vendor ricoprono un ruolo chiave per sensibilizzare i responsabili OT sull'importanza della sicurezza informatica. IT e OT parlano lingue differenti e spesso i referenti dei diversi dipartimenti non parlano tra loro, per questo un vendor efficace deve comprendere la natura dell'OT /IoT e fungere da trait d'union per far capire che una soluzione di sicurezza OT è la chiave per portare valore aggiunto al business. A tal fine, è indispensabile adottare un approccio pragmatico basato su tre punti: visibilità, valutazione dei rischi e raccomandazioni su come arginarli. Il primo passo è quello di identificare il cuore del business, mentre lo step successivo consiste nell'aiutare le aziende ad avere piena visibilità sui device collegati alla rete e capire come comunicano tra loro. Una volta raggiunta la piena visibilità è possibile effettuare una simulazione di decrescita del rischio, stilando una serie di "recommendation" che permettono alle aziende di scegliere quali azioni implementare e a quali dare priorità. È fondamentale, inoltre, che tutte le informazioni scaturite dalle analisi OT vengano presentate e condivise in modo chiaro anche con CEO e CIO, per dare loro la visione completa di quali sarebbero i potenziali rischi causati da un attacco senza una protezione adeguata. Solo la piena comunicazione, infatti, può portare a decisioni efficaci ed efficienti".**

## Cesare D'Angelo

**General Manager Italia Kaspersky - www.kaspersky.it**

**"Un approccio di sicurezza ideale combina l'efficacia delle misure fisiche tradizionali con l'intelligenza delle tecnologie digitali. Garantendo l'adeguata sicurezza, si evita che i dispositivi di videosorveglianza diventino un possibile punto di ingresso per attacchi informatici, contribuendo così alla protezione globale del sistema. L'implementazione di protocolli di sicurezza affidabili, l'isolamento delle reti di videosorveglianza e la formazione dei dipendenti sull'uso sicuro di tali dispositivi sono essenziali. A queste misure è importante affiancare una soluzione di sicurezza efficace. Basata su SaaS, la nostra proposta fornisce gli strumenti per identificare, analizzare e rispondere rapidamente alle minacce progettate per eludere la protezione endpoint. La soluzione contiene due strumenti: il primo permette di raccogliere e correlare i dati provenienti da più livelli di sicurezza come endpoint, app, e-mail, cloud e reti, riducendo al minimo il tempo medio di rilevamento e risposta - aspetto fondamentale per combattere le minacce complesse e gli attacchi mirati, dove la rapidità di reazione riduce le possibilità degli aggressori di raggiungere l'obiettivo con conseguenti danni finanziari o reputazionali per l'organizzazione. Il secondo offre, invece, una protezione gestita continua 24 ore su 24, 7 giorni su 7 e ricerca automatizzata delle minacce per garantire elevati livelli di rilevamento, consentendo alle aziende prive di risorse e competenze specifiche di individuare automaticamente le minacce che eludono i sistemi di sicurezza e prevenzione esistenti".**

# Dite la vostra

## Gianluca Lombardi

**Amministratore Unico GL Consulting - www.glconsulting.com**

"La mia opinione è che chi si occupa di sicurezza fisica, chi si occupa di sicurezza IT e chi di compliance/privacy, persegue lo stesso fine, ossia: proteggere l'azienda dai rischi che essa corre nei vari ambiti. L'unico vero problema è che, spesso, manca la comunicazione tra questi soggetti. **Per agevolare la comunicazione tra di loro è necessario che ci sia una regia gestita da chi conosce i tre ambienti e sa raggiungere lo scopo della protezione finale mediando le esigenze** di ognuno. E' necessario, però, un approccio olistico, possedendo competenze trasversali da mettere in gioco e non solo verticali su uno dei tre ambiti. Nella nostra esperienza in questo campo, di quasi 30 anni, è possibile creare una road map di attività, comune alle tre aree, che porti ad obiettivi condivisi, con soddisfazione di tutte le parti e con ritorno positivo per tutta l'azienda. Per guidare questo processo, a volte, non basta una singola persona, ma un team di professionisti, con competenze diverse e complementari ma con l'abitudine a lavorare assieme e, quindi, in grado di introdurre misure tecniche ed organizzative che tengano conto delle esigenze dei vari ambiti".

## Bruno Cordioli

**CEO di Muscope - www.muscope.com**

"Nel nostro approccio al tema, vediamo la sicurezza come un concetto unico che richiede un'analisi olistica. **La distinzione tra sicurezza fisica e sicurezza informatica, sebbene necessaria per specializzazione e focus, non deve portare a silos operativi.** I malintenzionati che mirano all'integrità fisica delle nostre risorse hanno motivazioni e metodi diversi rispetto a coloro che orchestrano attacchi da remoto. Questa differenza giustifica l'esistenza di team specializzati, ognuno con sensibilità e competenze distinte, ma è fondamentale che questi team operino in sinergia, condividendo conoscenze e strategie per una difesa integrata. Contrariamente a quanto si possa pensare, la mentalità dei due team non è opposta. Il settore IT ha evoluto la propria visione, comprendendo che limitare l'esposizione e mantenere un perimetro di attacco ristretto e ben difeso è cruciale. **La minimizzazione del perimetro di attacco e la protezione dei punti di ingresso critici sono principi che guidano entrambe le discipline verso un obiettivo comune:** la salvaguardia dell'organizzazione sotto ogni aspetto".

## Alberto Fuccello

**Amministratore ValueDataTrust - https://primatoo.cloud**

"Entrambi i team si occupano di valutare e gestire rischi: l'IT Security protegge il sistema informativo in generale, la Privacy si focalizza sulle misure di sicurezza da garantire ai trattamenti dei dati personali. Due ambiti che esigono un contesto e un dizionario comune, esigenza a cui abbiamo risposto con un modulo che integra le soluzioni privacy con le valutazioni di sicurezza IT. Per dare un'idea di quanto possa essere dannoso questo mancato connubio, rammento la vulnerabilità di Apache Log4j di fine 2021: una libreria Java apparentemente inoffensiva e diffusissima diventata un potenziale canale per promuovere attacchi informatici anche gravi lato web server. **Al mondo Privacy manca una "traduzione" di questi eventi estremamente "tecnici" che, in modo efficiente e diretto, faccia emergere le possibili conseguenze sulle attività di trattamento di dati personali fin dalla scoperta di una vulnerabilità, indipendentemente dal fatto che l'attacco occorra.** È necessario cioè uno sforzo per consentire al mondo Privacy di esercitare meglio il controllo del proprio dominio in qualunque caso, meglio se attraverso evidenze contestuali. La tecnologia può agevolare uno scambio di informazioni più tempestivo e sinergico".

# Dite la vostra

## Nicola Bernardi

**Presidente di Federprivacy - www.federprivacy.org**

**"Chi si occupa di protezione dei dati nelle organizzazioni pubbliche e private ha a che fare con una materia trasversale e multidisciplinare che abbraccia vari ambiti: ciò comporta che esperti di tematiche diverse debbano interagire tra loro, con il rischio però di incontrare difficoltà di comunicazione. Spesso infatti il linguaggio e l'approccio dei professionisti della privacy e di quelli della cybersecurity viaggiano su binari paralleli che raramente si incontrano. Per comprendere quali siano le maggiori difficoltà che incontrano gli addetti ai lavori e per individuare possibili soluzioni per colmare il gap e aiutarli a cooperare meglio, l'Osservatorio di Federprivacy - principale associazione di riferimento in Italia dei professionisti della privacy e della protezione dei dati personali - ha condotto un sondaggio dal quale sono emersi vari spunti interessanti. Il primo è che i legali esperti di compliance e i professionisti della cybersecurity incontrano effettive difficoltà ad interagire a causa dei differenti background, pur riconoscendo (91,53%) che le diverse competenze costituiscono un valore aggiunto per il team, e che nel caso in cui non fossero coperte tutte le competenze l'azienda sarebbe esposta a rischi di sanzioni e violazioni dei dati (60,31%). Tali difficoltà emergono anche dalle risposte fornite da oltre la metà degli esperti (57,2%), i quali hanno indicato gli aspetti organizzativi come quelli più importanti per un team che si occupa di protezione dati, ma anche quelli più sottovalutati nel 48,4% dei casi, denotando la necessità di implementare le strategie di governance dei dati in modo da superare le difficoltà riscontrate dal 56,06% degli intervistati nel conciliare compliance normativa e sicurezza dei dati. Gli addetti ai lavori sono tuttavia ottimisti sui margini di convergenza (53%) e ritengono di poter attenuare i gap trovando maggiori convergenze e collaborando a stretto contatto con esperti che hanno un background diverso (62,2%), approfondendo temi diversi dalla propria specializzazione (57,44%) e partecipando ad eventi formativi che non rientrano direttamente nelle proprie competenze (52,85%). Gli stessi addetti ai lavori - informatici e giuridici - vorrebbero essere inoltre coinvolti nelle riunioni del vertice aziendale che trattano questioni sulla protezione dei dati (66,67%) e sul mercato ricercano corsi di formazione trasversale (75,88%). Questi temi, non a caso, sono stati al centro della prima edizione di cyber & privacy forum, che ha registrato un forte successo a Verona il 29 Novembre 2023".**

**Queste ed altre tematiche sono state approfondite al cyber & privacy forum (Verona, 29 Novembre 2023)**

## 2 Parliamo di cloud, ormai super usato anche nella sicurezza fisica: quali garanzie di sicurezza cyber possono essere offerte in tal senso?

Risposte domanda 2

### Andrea Ciappesoni

**DPO di Adeguamenti Privacy - www.adeguamentiprivacy.it/**

**"E' consigliabile individuare correttamente i fornitori preferendo le aziende strutturate e affidabili soprattutto se dichiarano di eseguire frequenti test di sicurezza. Diffidare delle offerte a basso costo, poiché è probabile che trascurino gli aggiornamenti di sicurezza nel tempo (e l'evoluzione delle minacce informatiche rende necessario un costante adeguamento delle misure di sicurezza). Quello che originariamente potrebbe essere stato concepito per garantire la sicurezza fisica può inoltre diventare un'opportunità se trascurato digitalmente. L'approccio alla sicurezza deve essere olistico, comprensivo sia degli aspetti fisici che quelli informatici. La vulnerabilità di un sistema informatico è intrinseca alla sua natura dinamica, quasi sempre legata al software non solo del sistema operativo, ma anche software a basso livello integrato nei componenti elettronici. Nel corso del tempo, le falle possono essere individuate dagli hacker e diffuse nelle loro community: una volta individuato il dispositivo debole, i software d'attacco sapranno già come agire. Quali test fare? Vulnerability Assessment - identificazione delle vulnerabilità (scansione del sistema per individuare i punti deboli: può rivelare falle nella configurazione di sicurezza, errori di programmazione o altri bugs) e Penetration Test (simula attacchi reali per testare la capacità del sistema di resistere a intrusioni. Si basa sullo sfruttamento delle vulnerabilità applicando vere tecniche d'attacco per stabilire se il sistema può essere compromesso)".**

### Dario Marchese

**Security Manager BIP CyberSec, Privacy & Security**

**"L'adozione del cloud ha trasformato radicalmente l'approccio alla sicurezza informatica. Avendole già integrate nei nostri processi, promuoviamo presso i nostri clienti l'adozione delle certificazioni ISO 27017 e 27018, che stabiliscono standard severi per la gestione e la protezione dei dati nel cloud. Queste normative sottolineano che la sicurezza dei dati trascende la mera tecnologia, enfatizzando l'importanza di una gestione responsabile e trasparente dei dati. La nostra missione ci spinge a integrare l'expertise tecnica con la competenza legale e le pratiche di ethical hacking per creare soluzioni adatte alle complesse sfide del cloud. Il progresso tecnologico porta con sé nuove minacce, richiedendo soluzioni creative: l'intelligenza artificiale, ad esempio, apre possibilità incredibili per rafforzare la sicurezza, ma introduce altresì rischi inediti. Un aspetto fondamentale per garantire la sicurezza di servizi su cloud è l'implementazione di regole tecniche per i service cloud provider che rispettino i framework di riferimento. Assicurare che le soluzioni cloud aderiscano a questi standard è essenziale per affrontare proattivamente le minacce emergenti".**

## Piermaria Saglietto

**CEO Compet-e srl - www.compet-e.com**

"Uno dei principali ostacoli nel contesto del cloud risiede nell'applicazione, da parte dei fornitori o degli utenti, di principi e paradigmi di progettazione ancorati al modello on-premise. In questo modello, tutti i sistemi sono confinati all'interno della rete aziendale, beneficiando di livelli sofisticati e precisi di protezione. Tuttavia, quando ci si trova **nel contesto del cloud, è essenziale adottare misure di sicurezza adeguate a un ambiente intrinsecamente più esposto a minacce e vulnerabilità.** La sicurezza da implementare deve agire in modo esaustivo, coinvolgendo tutte le componenti: architetturali, infrastrutturali e applicative. Prendiamo ad esempio un applicativo web erogato attraverso il cloud. Dovremmo iniziare ad **adottare almeno le seguenti precauzioni pratiche: 1) Architetturali** - si consiglia di separare la componente applicativa da quella dei dati, garantendo che il database server non sia accessibile a tutto il web, ma solo al server dell'applicazione e su porte specifiche, attentamente monitorate; **2) Infrastrutturali** – la norma di base dovrebbe includere l'implementazione di un WAF (Web Application Firewall) per proteggere le applicazioni web da attacchi dannosi e traffico internet indesiderato. Questo strumento è efficace contro varie minacce, compresi attacchi di tipo bot, injection e denial of service (DoS); 3) **Applicativi** - l'utilizzo di un singolo metodo di autenticazione, come username e password, anche se con password complesse, non è più sufficiente per difendersi da accessi indesiderati e frodi. Pertanto, è essenziale che le applicazioni siano dotate di MFA (Multi-Factor Authentication), che prevede almeno un secondo fattore di autenticazione, come ad esempio un "token" virtuale inviato al dispositivo mobile dell'utente".

## Samuele Zaniboni

**Senior Manager of Presales and Tech Engineer ESET Italia - www.eset.com/it**

"Il cloud è una risorsa ormai fondamentale per le aziende, sia dal punto di vista della sicurezza fisica che cyber: facilita lo storage e la gestione di enormi quantità di dati (si pensi, ad esempio, alla mole di dati raccolti attraverso il TVCC), consente la condivisione delle risorse (ad es. la gestione degli accessi ai sistemi aziendali) aumentando l'efficienza e riducendo gli investimenti economici richiesti. Purtroppo questi vantaggi possono trasformarsi in possibili minacce se si considera il punto di vista della sicurezza cyber delle aziende. La condivisione dei dati e delle risorse in ambiente cloud, infatti, può dar luogo a problematiche relative alla responsabilità di gestione e protezione degli stessi. **Spesso i provider di servizi cloud implementano tutte le misure** necessarie, come l'autenticazione a più fattori e sistemi di crittografia e di gestione sicura, affinché i dati gestiti negli ambienti cloud di loro competenza rimangano protetti. **Le aziende,** dal canto loro, non possono affidarsi solo alle misure di sicurezza gestite dal provider ma **devono** ugualmente **porre in essere tutte le politiche di cybersicurezza** necessarie per garantire il giusto livello di protezione di tutti i dati aziendali. L'obiettivo è perseguibile attraverso l'adozione di tecnologie di **protezione multi-livello,** in grado di mantenere monitorato ogni elemento della rete aziendale e di intervenire attraverso attività di detection e response qualora si verifichi un possibile incidente di sicurezza".

## Pierguido Iezzi

**Cyber Security Director e Ceo Swascan - www.swascan.com**

"Per affrontare le sfide attuali della cyber security, diventa sempre più imprescindibile adottare una strategia di difesa informatica basata su approcci predittivi, preventivi e proattivi. Il Cloud è uno degli ingranaggi fondamentali di questi meccanismi, che uniscono perfettamente tecnologie e competenze. Ogni azienda, indipendentemente dalle sue dimensioni, rappresenta un bersaglio accessibile e, per migliorare le difese, è cruciale focalizzarsi sulla superficie di attacco e sui vettori di attacco. Per mitigare le minacce e potenziare la resilienza e il ripristino, è fondamentale concentrarsi su una **strategia di difesa informatica – anche con l'ausilio del cloud - che possa anticipare le potenziali minacce, prevenire gli attacchi prima che si verifichino e adottare misure proattive.** Lo stesso Ministro della Difesa Guido Crosetto ha recentemente evidenziato, in un'intervista rilasciata al Cyber Magazine di Assintel, l'importanza di esprimere capacità operative all'avanguardia, dal ricorso all'Intelligenza Artificiale ai servizi cloud avanzati, considerando anche gli effetti derivanti dallo sviluppo del Quantum Computing. Questi settori strategici non riguardano solo la Difesa, ma hanno un impatto cruciale per l'intero Paese".

# Dite la vostra

## Paolo Cecchi

**Sales Director Mediterranean Region SentinelOne - https://it.sentinelone.com**

**"Le aziende oggi sono sempre più attente al tema della sicurezza informatica, in primis per assicurare la protezione di endpoint, identità e dati e, a seguire, per migliorare la sicurezza in cloud, vista la progressiva migrazione delle imprese verso i servizi nella nuvola. Per cambiare il paradigma della sicurezza dei workload e dei dati in cloud oggi non è più possibile affidarsi a soluzioni specifiche o a una piattaforma stand-alone per il cloud: le imprese necessitano di una piattaforma di security integrata, dotata di funzionalità di sicurezza avanzate, in tempo reale e basate sull'AI, per proteggere l'intera azienda a livello di endpoint, identità e cloud. Una piattaforma completamente integrata è in grado di migliorare la protezione dei dati, la sicurezza e l'automazione dell'intero ambiente cloud perché oggi è indispensabile disporre di una dashboard unificata e di un collettore capace di acquisire log, notifiche, alert e ogni ulteriore metrica che possa essere analizzata dal responsabile della security, in modo chiaro, preciso e veloce. Inoltre, l'uso di una piattaforma cloud-based integrata consente di evitare il download dei continui aggiornamenti, evitando lunghe scansioni periodiche".**

## Alessio Mercuri

**Senior Security Engineer di Vectra AI - https://it.vectra.ai**

**"La natura degli ambienti cloud richiede ai team tecnici e di sicurezza di adottare un mindset diverso per gestire la nuova superficie di attacco. Sebbene le tattiche siano simili e gli obiettivi gli stessi - ridurre il rischio, proteggere i dati riservati, soddisfare i requisiti di compliance - il cloud aggiunge infatti una complessità che cambia completamente le dinamiche. L'architettura del cloud, la mancanza di controlli sulle modifiche e le differenze nella progettazione e nelle operazioni di base delle varie piattaforme rendono questo tipo di sicurezza più complessa. Anche se gli strumenti di prevenzione fanno un ottimo lavoro nel fornire visibilità, sono insufficienti quando si tratta di rilevare nuovi vettori di attacco. Ecco perché occorre adottare gli strumenti giusti per fornire una copertura completa: è indispensabile che i team SOC si concentrino sull'identificazione degli incidenti di sicurezza grazie a una soluzione di Cloud Detection and Response (CDR). Se potenziata dall'AI, questa è in grado di monitorare tutte le azioni nell'ambiente cloud e di far emergere i comportamenti sospetti in tempo reale, consentendo ai team SecOps di stabilire le priorità, indagare e rispondere alle minacce più urgenti".**