SICUREZZA INFORMATICA, IL BOOM DEGLI ATTACCHI HACKER SPINGE LA RICHIESTA DI "CYBERSECURITY ANALYSTS": +29% ENTRO IL PROSSIMO DECENNIO

Basta un clic sbagliato per mettere a rischio dati, sistemi e continuità operativa aziendale e, nei casi più gravi, un'intera reputazione. Alle imprese non basta infatti più solo difendersi dagli attacchi informatici che, nel 60% dei casi, sono causati dal fattore umano ma dovranno essere sempre più resilienti, investendo in nuove figure professionali, sempre più centrali, come gli analisti di cybersecurity. Dal ruolo dell'intelligenza artificiale alla sicurezza della supply chain, fino alle sfide del futuro quantistico, Richmond Cyber resilience forum 2025 Autumn ha svelato, davanti ad una platea composta da CISO, manager e professionisti della sicurezza, quelli che saranno i principali trend del 2026. "Oggi parlare di cyber resilience significa accettare che le violazioni della cybersicurezza non siano più un'eventualità remota, ma uno scenario concreto con cui le organizzazioni devono fare i conti", afferma Marina Carnevale, events conference director di Richmond Italia

Nel mondo digitale odierno, la criminalità informatica non è più un fenomeno sporadico, ma una minaccia operativa costante: a livello globale si registra in media **un attacco cyber ogni 39 secondi**, per un totale di circa **2.200 incidenti al giorno**. Un dato stabile dal 2023 che, tuttavia, si accompagna a un impatto sempre più rilevante: secondo il ***Cybersecurity Statistics 2025***, **nel primo trimestre del 2025 il numero di record violati è aumentato del 186%**. A rendere il quadro ancora più complesso contribuisce l'evoluzione delle tecniche di attacco: il ***Verizon Data Breach Investigations Report 2025*** evidenzia che il **44% delle violazioni coinvolge ransomware**, in crescita rispetto al **32% dell'anno precedente**, mentre il **30% degli incidenti** è riconducibile a compromissioni attraverso **terze parti**, un dato raddoppiato in un solo anno. Centrale resta infine il **fattore umano**, responsabile del **60% delle violazioni**, confermandosi al tempo stesso la vulnerabilità più sfruttata e la prima linea di difesa per le organizzazioni. In questo contesto aumenta la domanda di competenze specializzate: secondo la ***University of Phoenix***, la richiesta di **analisti di cybersecurity crescerà del +29% nei prossimi dieci anni**, con un tasso di crescita superiore alla media delle altre professioni. Si tratta di figure fondamentali per affrontare qualsiasi imprevisto con preparazione, assicurando la continuità dei sistemi informatici anche nelle situazioni più critiche.

La conoscenza è potere, dunque, anche in ambito cybersecurity: la prima linea di difesa contro un attacco informatico passa dalla padronanza dei sistemi utilizzati e dall'individuazione delle loro vulnerabilità, in un contesto reso sempre più complesso dall'espansione di cloud e dell'Internet of Things (IoT). A questo scenario si affiancano normative sempre più stringenti e modalità sempre diverse di protezione dei dati e di gestione del rischio, rendendo indispensabile una rapida capacità di adattamento. Temi affrontati anche da **Jelena Zelenovic Matone** in apertura di ***Richmond Cyber resilience forum 2025 Autumn***, recentemente svoltosi a Rimini e promosso da ***Richmond Italia***, realtà specializzata nell'organizzazione di forum e iniziative B2B. Rivolgendosi a una platea di CISO e professionisti del settore, l'esperta di cybersecurity e tecnologie digitali ha utilizzato un'immagine semplice eppure straordinariamente efficace: "La tecnologia è come la dinamite alla fine dell'Ottocento: uno strumento incredibilmente potente. Se usata bene, permette di costruire gallerie, strade e addirittura collegare i continenti; se usata male, può invece distruggere interi

mondi. Il futuro dipenderà dalle decisioni che prendiamo oggi e da come scegliamo di governare questa potenza. Non è quindi la tecnologia in sé a determinare la sicurezza, ma la rapidità con cui chi la usa con intenti malevoli impara a sfruttarla e di converso la rapidità con cui dobbiamo imparare a reagire".

L'evento ha rappresentato un momento di riflessione sul significato più ampio della **resilienza** in ambito cyber, intesa come **capacità delle organizzazioni di affrontare scenari di rischio** sempre più complessi e in continua evoluzione. Dal confronto è emersa l'importanza di **adottare un approccio strutturato e condiviso**, che consenta non solo di **rafforzare le difese tecnologiche**, ma anche di **sviluppare modelli organizzativi e culturali** in grado di garantire continuità, adattamento e solidità nel tempo. In questa prospettiva, **la resilienza diventa un fattore strategico per la sostenibilità e la competitività delle imprese**, come evidenziato nel corso della plenaria di apertura da **Marina Carnevale**, events conference director di ***Richmond Italia***: "Oggi parlare di cyber resilience significa accettare che le violazioni della cybersicurezza non siano più un'eventualità remota, ma uno scenario concreto con cui le organizzazioni devono fare i conti. La resilienza non è solo prevenzione: è la capacità di anticipare il rischio, assorbire l'impatto di un attacco, reagire in modo rapido e ripristinare operatività, dati e fiducia. Richmond Cyber resilience forum nasce proprio per supportare CISO, CIO e decision maker in questo cambio di paradigma, offrendo un luogo di confronto qualificato su strategie, tecnologie e governance necessarie a garantire continuità e solidità al business anche in contesti di crisi digitale".

Il contesto a cui si riferisce il forum dà segnali di forte vitalità. Incrociando i pareri di esperti e partecipanti, è stato possibile evidenziare **5 fattori** destinati a fare tendenza nei prossimi mesi:

1. **Intelligenza artificiale nella cybersecurity**: l'IA sarà sempre più centrale sia nelle strategie di attacco, attraverso automazione e tecniche adattive, sia nelle difese aziendali, dove verrà impiegata per migliorare prevenzione, rilevamento e capacità di risposta agli incidenti.
2. **Zero Trust e identità digitale**: proseguirà l'adozione di architetture basate su verifiche continue dell'identità e dei privilegi di accesso, con l'obiettivo di ridurre la superficie di attacco e aumentare il controllo sugli ambienti IT distribuiti.
3. **Crittografia e minacce quantistiche**: le organizzazioni inizieranno a prepararsi agli effetti del calcolo quantistico, valutando l'evoluzione degli attuali sistemi di cifratura e rafforzando la propria capacità di adattamento tecnologico.
4. **Sicurezza della supply chain e governance**: la protezione dell'ecosistema di fornitori diventerà sempre più strategica, attraverso una maggiore visibilità sulle dipendenze software, l'adozione di Software Bill of Materials (SBOM) e controlli più strutturati lungo la catena di approvvigionamento.
5. **Normative e compliance**: l'evoluzione del quadro regolatorio renderà la cybersecurity un elemento strutturale dei modelli di governance, spingendo le imprese a integrare la gestione del rischio cyber nelle strategie di business e continuità operativa.

Con cortese preghiera di diffusione
Gennaio 2026

Noemi Gentilezza
ESPRESSO COMMUNICATION
n.gentilezza@espressocommunication.it
cell. 3312285111

Eugenio Alberti
RICHMOND ITALIA
ealberti@richmonditalia.it
cell. 3478734672