

VareseNews

Elmec porta la sicurezza digitale a un livello superiore con un approccio end-to-end

Pubblicato: Venerdì 3 Ottobre 2025



La sicurezza informatica, per essere realmente efficace, deve integrare **tecnologie, processi e persone in un unico ecosistema**. Con questo principio, Elmec Informatica ha sviluppato un **approccio end-to-end** che unisce protezione dei dati, gestione delle vulnerabilità, continuità operativa e cultura della consapevolezza digitale. Un modello che si traduce in procedure concrete di **remediation**, servizi avanzati di **cyber recovery** e programmi di **formazione** diffusi a tutti i livelli aziendali per sviluppare una concreta **cultura della sicurezza digitale**.

La prima edizione di **Elmec Security Summit 2025**, che si è svolta presso il **Campus Tecnologico** di Brunello, ha rappresentato l'occasione per condividere questa strategia e confrontarsi con aziende e professionisti sulle più attuali sfide del settore. L'evento ha proposto oltre 24 workshop, 20 tech experience e 7 corner tematici, offrendo un percorso immersivo che ha mostrato come l'approccio end-to-end possa diventare un fattore abilitante per il business.

Nel corso del Summit, **Filadelfio Emanuele, CISO di Elmec e Responsabile di CybergON**, ha presentato un quadro complesso e in continua evoluzione, utilizzando i dati raccolti dai propri sistemi di monitoraggio su un parco clienti eterogeneo e coadiuvato dal lavoro degli analisti. Dallo studio emerge un quadro chiaro: anche aziende con una buona maturità in ambito cyber security faticano a superare il **45% di vulnerabilità risolte**, a fronte di oltre **43.000 rilevate** dall'inizio dell'anno. È emerso, inoltre,

che il numero di attacchi di phishing cresce costantemente, anche grazie all'AI, aumentando in modo sostanziale l'efficacia degli stessi e raggiungendo il 300% di successo rispetto al 2024; c'è stato un aumento del 180% degli attacchi che utilizzano lo sfruttamento di buchi di sicurezza nell'accesso all'infrastruttura aziendale; e gli attacchi ransomware hanno avuto un incremento del 200%.

Sono dati che evidenziano come il **processo di vulnerability management** che si completa con le attività di remediation, debba scontrarsi con vincoli di business e complessità tecnologiche. Elmec, grazie al lavoro della propria business unit **CybergON** in stretta collaborazione con i Team di infrastruttura e workplace management, riesce a portare questo **tasso di remediation al 75%**, dimostrando come l'approccio end-to-end nei fatti, faccia la differenza, rispetto ad altri processi che spesso le aziende si trovano a dover coordinare quando il ventaglio di fornitori è variegato e destrutturato.

I **trend** emersi sono sostanzialmente **tre**: la **crecente attenzione alla protezione degli asset industriali**, intesi non solo come postazioni lavoro (laptop, smartphone o tablet), ma anche banche dati, applicativi o macchinari produttivi; una **spinta normativa** che sta forzatamente accelerando gli investimenti in sicurezza; un **aumento sempre più sensibile degli attacchi informatici** potenziati dall'intelligenza artificiale.

In un quadro in cui gli incidenti sono in costante aumento anno su anno, i primi 9 mesi del 2025 non hanno cambiato questo preoccupante trend. In Elmec, oltre alla protezione dei dati, è stato strutturato un **Team di Incident Response** dedicato alla gestione di incidenti estesi che arrivano a bloccare l'intera operatività del business. Questo gruppo risponde principalmente a richieste di supporto di aziende che non hanno servizi di Security Operation Center (SOC) e che si trovano a fronteggiare un fermo completo dei sistemi.

“Il vero punto di svolta per le imprese – afferma **Filadelfio Emanuele** – è comprendere che la sicurezza non è un elemento accessorio, ma un vero e proprio fattore abilitante del business. Non si tratta soltanto di tecnologie, ma di un approccio culturale che deve permeare ogni livello aziendale. Per questo la formazione delle persone gioca un ruolo decisivo: dipendenti consapevoli e preparati sono il primo baluardo contro i rischi informatici, perché sanno riconoscere potenziali minacce e adottare comportamenti corretti nelle attività quotidiane.”

L'importanza della protezione dei dati per tutelare l'utente e l'azienda

Proteggere i dati significa difendere non solo gli asset digitali, ma soprattutto la fiducia dei clienti.

Per questo, al centro della strategia di sicurezza di Elmec, c'è la gestione delle identità, garantendo che la persona giusta, con il livello corretto di autorizzazioni, acceda soltanto alle risorse necessarie allo svolgimento delle proprie mansioni. La protezione dei dati non è più quindi un tema esclusivamente IT, ma di governance: vuol dire classificare gli asset, stabilire regole chiare sugli accessi e prevenire abusi o incidenti. La gestione degli accessi e delle identità diventa quindi, un fattore determinante per ridurre i rischi di perdita delle informazioni.

Infrastrutture sicure e nuove sfide di continuità

Un altro aspetto da considerare è come la sicurezza IT vada considerata su più livelli, combinando tecnologie avanzate, processi organizzativi e controllo fisico degli accessi. È necessario prevedere per esempio una protezione H24 che passa attraverso le modalità d'ingresso negli edifici, i sistemi di Intrusion Prevention, le soluzioni anti-DDoS che monitorano la rete in tempo reale, un costante patching delle infrastrutture e il lavoro dell'ISM Team dedicato alla gestione delle vulnerabilità. A questi si aggiungono anche le soluzioni di Disaster Recovery e dei servizi innovativi come il Backup Security o il Cyber Recovery, pensati per salvaguardare l'integrità e la continuità dei dati dei clienti, trasformando la sicurezza in un vero elemento abilitante del business.

DevSecOps e intelligenza artificiale: sicurezza integrata nello sviluppo software

Tra i tanti temi emersi durante l'evento non è mancato un approfondimento sull'approccio **DevSecOps**,

che pone al centro dell'attenzione un principio chiave, ovvero che la sicurezza deve essere parte integrante del ciclo di vita del software fin dall'inizio. Ciò significa progettare applicazioni ponendosi subito domande su permessi, ambienti e punti di esposizione critici; monitorare attentamente librerie e componenti di terze parti, come quelle open source; infine, prevedere processi di rilascio controllati e validati da figure indipendenti. Solo così lo sviluppo non diventa un varco inconsapevole per nuove vulnerabilità, ma un pilastro di protezione continua.

In questo scenario, l'**intelligenza artificiale** emerge come un alleato strategico. Non sostituisce le competenze degli sviluppatori, ma le potenzia e migliora: dal supporto nel coding, alle attività di testing, fino alla generazione di documentazione più accurata. Compiti che spesso vengono percepiti come accessori, ma che in realtà incidono direttamente sia sulla sicurezza sia sulle performance di sviluppo. Il risultato è duplice: applicazioni più robuste e tempi di rilascio ridotti, senza compromettere la qualità e l'affidabilità del software.

Ospite speciale della giornata è stato **Pablo Trincia**, che, con il suo intervento dal titolo "*La verità nascosta: tra tecnologia, indagini e storie umane*" ha raccontato come la tecnologia stia cambiando il modo di raccontare e indagare il **True Crime**. Dall'utilizzo delle informazioni che spesso troviamo online, fino al ruolo dei podcast come piattaforma digitale capace di dare nuova forza a storie complesse, l'incontro ha mostrato come le innovazioni tecnologiche possano affiancare la responsabilità giornalistica e il lavoro di squadra nella costruzione di indagini e narrazioni.

Con il **Security Summit**, Elmec ha chiuso un anno ricco di appuntamenti dedicati alla **divulgazione tecnologica**, dai format Innovation, Workplace e Technicus, fino alla sicurezza. "Quattro Summit in meno di un anno, questo è il bilancio tutto in positivo del nuovo formato che abbiamo sviluppato per il pubblico di Elmec, in risposta alla crescente complessità del mondo IT", dichiara **Elisa Bisceglia, Direttrice Fiducia e Sostenibilità di Elmec**. "È stata un'occasione che ci ha visti tutti coinvolti, dalla condivisione delle competenze, all'organizzazione, fino al coinvolgimento delle aziende. Con oltre 90 workshop, 60 tecnici specializzati e più di 1.200 partecipanti, abbiamo portato contenuti concreti, roadmap operative e spunti di riflessione utili a noi per primi, ma anche a tutti i nostri ospiti, per affrontare le sfide del nostro settore. Con i nuovi Summit abbiamo raggiunto un obiettivo per noi fondamentale: rafforzare il nostro impegno nei confronti dei clienti e delle loro migliori risorse."

Redazione VareseNews
redazione@varesenews.it