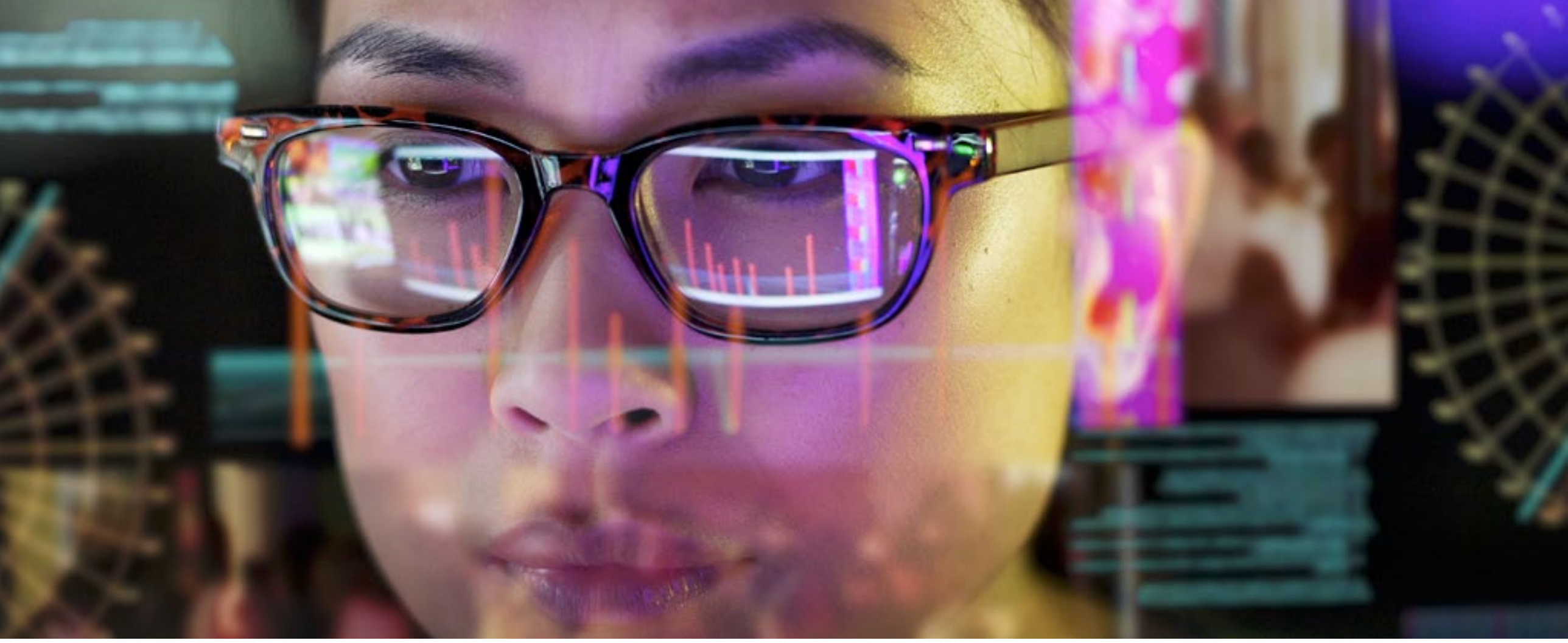


Proteggi e potenzia la tua azienda

Affronta la crescente complessità delle minacce informatiche e dei requisiti normativi in continua evoluzione

Brochure

Alcatel·Lucent
Enterprise

Introduzione

Mentre le organizzazioni attraversano trasformazioni profonde nei propri modelli di business, la sicurezza emerge come uno dei temi più critici. L'ascesa delle tecnologie basate sull'intelligenza artificiale ha messo in discussione i modelli di sicurezza tradizionali, rendendo necessaria una revisione delle pratiche consolidate.

A fronte di questi cambiamenti, il nostro team di esperti di sicurezza informatica in ambito soluzioni di rete, comunicazione e cloud ha unito le proprie competenze per condividere analisi approfondite sui nuovi rischi che le aziende devono affrontare e sulle soluzioni di protezione necessarie per restare competitive e sicure.

Il panorama in evoluzione della cybersicurezza

L'ambiente della sicurezza informatica è caratterizzato da una rapida evoluzione tecnologica, minacce sempre più sofisticate e normative in costante aggiornamento. Gli esperti del settore hanno identificato le tre tendenze principali che stanno influenzando profondamente la sicurezza informatica aziendale:

1. Il ruolo ambivalente dell'intelligenza artificiale
2. Il continuo aumento di ransomware e attacchi alla supply chain
3. La necessità di una solida gestione delle identità all'interno di architetture basate sull'approccio zero trust

Il ruolo ambivalente dell'IA nella sicurezza informatica

L'intelligenza artificiale come arma per gli attacchi

L'impiego malevolo dell'intelligenza artificiale è diventato una delle minacce più rilevanti per la sicurezza aziendale. I criminali informatici sfruttano l'intelligenza artificiale per automatizzare la raccolta di informazioni, creare campagne di phishing altamente personalizzate e sviluppare malware adattivi in grado di eludere i tradizionali sistemi di rilevamento.

Gli strumenti basati sull'IA possono analizzare dati pubblici per profilare obiettivi, generare audio e video deepfake realistici e sfruttare vulnerabilità con precisione chirurgica. Ad esempio, le e-mail di phishing generate dall'IA, che imitano gli stili di comunicazione legittimi, hanno un tasso di successo del 40% più alto rispetto ai metodi tradizionali. Questi attacchi diventano ancora più frequenti e pericolosi in quanto gli strumenti di IA sono sempre più accessibili, anche persone con competenze limitate possono sfruttarli per lanciare attacchi sofisticati.

La tecnologia deepfake è un'applicazione particolarmente insidiosa dell'IA, poiché permette agli aggressori di impersonare dirigenti o colleghi durante video chiamate in tempo reale per autorizzare transazioni fraudolente o ottenere informazioni riservate. In un caso documentato, un video deepfake di un CFO che dava istruzioni per effettuare un bonifico bancario ha causato una perdita di 25 milioni di dollari a una multinazionale. Questi episodi evidenziano l'importanza di protocolli di autenticazione avanzati e di programmi di formazione per aiutare i dipendenti a riconoscere contenuti sintetici e potenzialmente dannosi.

L'IA come strumento di difesa

Paradossalmente, l'IA rappresenta anche il pilastro delle difese in campo cybersecutity. Gli algoritmi di machine learning analizzano grandi volumi di dati per rilevare le anomalie, prevedere possibili vettori di attacco e automatizzare le risposte agli incidenti. I sistemi di sicurezza potenziati dall'IA possono, ad esempio, identificare vulnerabilità zero day (non ancora note), riconoscendo sottili pattern comportamentali nel traffico di rete, riducendo i tempi medi di rilevamento da settimane a poche ore. Gartner afferma che le organizzazioni che investono in piattaforme di threat intelligence basate sull'IA registrano il 30% in meno di violazioni riuscite rispetto a chi si affida a sistemi tradizionali[1]. I sistemi basati sull'IA sono particolarmente efficaci nell'identificare le minacce interne, monitorando il comportamento degli utenti e segnalando pattern di accesso insoliti, un aspetto sempre più critico negli attuali ambienti di lavoro remoti e ibridi.

Sfide normative ed etiche

La natura a duplice uso dell'IA ha richiesto risposte normative rigorose. La normativa europea sull'IA, promulgata nel febbraio 2025, vieta le applicazioni IA ad alto rischio in ambiti come la sorveglianza biometrica e impone trasparenza nel processo decisionale algoritmico. Oggi le imprese devono effettuare audit di terze parti sui sistemi di IA, documentare la provenienza dei dati e garantire un uso etico - un'operazione complessa data l'opacità di molti modelli di machine learning. Per affrontare questa sfida, le organizzazioni stanno istituendo comitati etici trasversali sull'IA e collaborando con gli enti regolatori per definire i quadri futuri.

Ransomware e attacchi alla supply chain in aumento

Puntare su fornitori chiave

Gli attacchi ransomware sono evoluti da campagne opportunistiche a operazioni strategiche mirate a fornitori e service provider. Gli attacchi del 2024 a CDK Global e Change Healthcare hanno dimostrato come la compromissione di un singolo fornitore possa paralizzare interi settori, causando miliardi di perdite tra interruzioni operative e sforzi di recupero. Oggi, gli aggressori si concentreranno sempre più su fornitori di software-as-a-service (SaaS) e su aziende di infrastrutture cloud, sfruttando il loro ruolo centralizzato negli ecosistemi aziendali. Ad esempio, un attacco ransomware a un importante provider di servizi di cloud storage potrebbe bloccare contemporaneamente l'accesso ai dati di migliaia di aziende, amplificando il potere di estorsione.

La proliferazione di sistemi interconnessi e l'insufficiente gestione del rischio della supply chain facilitano questi attacchi. Molte aziende non hanno visibilità sul livello di sicurezza dei loro fornitori, il che le rende vulnerabili a fallimenti a catena. Secondo Gartner, entro il 2026 il 60% delle organizzazioni subirà una violazione significativa della supply chain, alimentata da vulnerabilità di terze parti nelle pipeline DevOps e nei dispositivi IoT fleet[1].

Ecosistemi di ransomware-as-a-service (RaaS)

L'aumento delle piattaforme ransomware-as-a-service ha democratizzato l'accesso a strumenti di attacco avanzati, consentendo anche a criminali poco esperti di lanciare campagne sofisticate. Gli operatori RaaS forniscono malware personalizzabili, portali di pagamento e supporto nelle negoziazioni in cambio di una quota del riscatto - in genere dal 20 al 30%. Questo modello ha portato a un aumento del 150% degli incidenti ransomware dal 2023, con richieste medie di riscatto superiori a 5 milioni di dollari per incidente.

Il ransomware moderno utilizza tecniche di offuscamento basate sull'IA, come codice polimorfico e crittografia a tempo ritardato, per eludere il rilevamento. Gli aggressori inoltre sottraggono i dati prima di implementare la crittografia, minacciando di divulgare informazioni sensibili in caso di mancato pagamento, una tattica nota come doppia estorsione. Le aziende stanno contrastando queste minacce con backup isolati (air-gapped), soluzioni di archiviazione decentralizzate e sistemi di verifica dell'integrità basati su blockchain.

Le organizzazioni avranno bisogno di tecnologie sicure a tutto tondo per prevenire, contenere e limitare l'impatto degli attacchi ransomware alla supply chain.

1. https://www.gartner.com/en/newsroom/press-releases/2025-03-03-gartner-identifiesthe-top-cybersecurity-trends-for-2025
2. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Gestione dell'identità e l'imperativo del modello "zero trust"

La crisi d'identità delle macchine

Con l'adozione da parte delle aziende di IA generativa, dispositivi IoT e architetture cloud native, le identità delle macchine - credenziali per dispositivi, API e workload automatizzati - hanno superato le identità umane in termini di volume e rischio. Nel 2025 Gartner ha identificato le macchine non gestite come uno dei principali vettori di attacco, con chiavi API e account di servizio compromessi che contribuiscono al 45% delle violazioni cloud[1]. Per affrontare questo problema, le aziende adottano sempre più diffusamente strumenti di gestione dei certificati che automatizzano una rotazione più frequente delle credenziali, rafforzando le loro policy di minimo privilegio per il rilevamento in tempo reale di comportamenti anomali delle macchine.

Architettura zero trust in pratica

Contesti basati sull'approccio zero trust, secondo cui nessuna entità umana o macchina è intrinsecamente affidabile, sono passati da obiettivi aspirazionali a necessità operative. L'implementazione si concentra sull'autenticazione continua, sulla micro-segmentazione e su comunicazioni crittografate. Ad esempio, una rete basata sull'approccio zero trust potrebbe richiedere la verifica biometrica per l'accesso ai dati sensibili, isolare gli ambienti di sviluppo dai sistemi di produzione e criptare tutto il traffico est-ovest all'interno dei data center.

Il National Institute of Standards and Technology (NIST) ha riportato in una valutazione sull'efficacia dell'approccio zero trust dell'architettura[2] che le organizzazioni che lo adottano riducono in media del 70% l'impatto delle violazioni. Il successo dipende dall'integrazione dei principi di zero trust con l'infrastruttura esistente, una sfida per le aziende con sistemi legacy. Stanno guadagnando terreno approcci ibridi, come i perimetri software-defined per asset on premises e soluzioni zero trust cloud-native.

Fattori umani e minacce interne

Secondo il World Economic Forum, il 95% degli incidenti di sicurezza informatica è riconducibile a un errore umano. Gli attacchi di phishing che sfruttano i contenuti generati dall'intelligenza artificiale aggirano i filtri delle e-mail con un'efficacia superiore del 30% rispetto ai metodi tradizionali, mentre i dipendenti che espongono involontariamente le credenziali in strumenti di collaborazione sono responsabili del 25% delle violazioni. Le minacce interne sono aggravate da errori nella configurazione manuale degli accessi di rete e dal lavoro remoto, dove dispositivi personali e reti non sicure creano punti di ingresso per gli aggressori.

È diventato essenziale aiutare gli utenti a proteggersi meglio, riducendo al contempo il peso di policy di sicurezza sempre più restrittive. Per gli amministratori di rete e applicazioni, l'automazione delle operazioni e l'assistenza attiva tramite IA devono fornire gli strumenti necessari per proteggersi dalle conseguenze di potenziali configurazioni errate.

L'approccio di Alcatel-Lucent Enterprise alla sicurezza delle soluzioni di comunicazione e di rete

L'approccio alla sicurezza di Alcatel-Lucent Enterprise consiste nell'assicurare che le interazioni digitali siano efficaci e conformi agli standard di settore. La tecnologia digitale è ormai diffusa, con una crescente adozione crescente di IA e di dispositivi IoT che raccolgono dati per supportare avvisi in tempo reale e pianificazione futura. Proteggere e rafforzare le reti e le comunicazioni che alimentano il business odierno è fondamentale per evitare interruzioni del servizio. Le soluzioni ALE per le comunicazioni aziendali e le infrastrutture di rete implementano la cybersecurity end-to-end, poichè è l'unico modo per garantire che la sicurezza venga applicata completamente. Questo approccio alla sicurezza informatica aiuta le imprese e le istituzioni pubbliche a:

- Prevenire gli attacchi informatici introducendo la cybersecurity in ogni fase della progettazione del prodotto per ridurre la superficie oggetto di attacchi informatici
- Proteggersi dagli attacchi informatici applicando gli standard di sicurezza e le best practice più recenti in tutte le componenti della soluzione per rafforzarne la resistenza complessiva
- Reagire agli attacchi informatici con azioni rapide e appropriate per limitare l'impatto e migliorare la resilienza, qualora si debba affrontare un attacco.

In qualità di produttore di hardware e articoli basati su software, l'approccio di ALE alla sicurezza informatica si concentra sulle aree descritte di seguito, per individuare le potenziali vulnerabilità nel panorama delle minacce informatiche.

1. Sicurezza per progettazione

Storicamente, in fase di progettazione, la sicurezza delle soluzioni era un aspetto fondamentale ma secondario rispetto all'implementazione di nuove funzionalità. Con il cambiamento del panorama tecnologico, le priorità di progettazione tradizionali si sono invertite. Ora, i requisiti di sicurezza informatica devono guidare la progettazione delle soluzioni. Le soluzioni hardware e software 'secure by design' considerano la sicurezza in ogni fase: studio, sviluppo e fornitura del prodotto. Tutti i sistemi hardware e operativi sono di tipo industriale, la protezione Denial of Service (DoS) è integrata e le soluzioni implementano le migliori pratiche di cybersecurity più rilevanti per il settore.

2. Sicurezza basata sul modello Zero Trust Network Access (ZTNA)

Le strategie di sicurezza che basano l'affidabilità sulla posizione dell'utente all'interno del firewall aziendale, sulle credenziali di accesso o sull'applicazione o sul dispositivo utilizzato non sono più sufficienti, anche quando si combinano più meccanismi di sicurezza. Oggi nessun utente, dispositivo o applicazione dovrebbe godere di fiducia implicita. Il modello di sicurezza basato sullo Zero Trust Network Access (ZTNA) aiuta le organizzazioni a contrastare efficacemente le minacce in continua evoluzione. ZTNA non si fida di alcun utente, dispositivo o applicazione, indipendentemente dalla loro posizione. ALE applica lo ZTNA consentendo l'applicazione di policy basate sui ruoli, il controllo degli accessi basati sulla posizione (integrato Unified Policy Authentication Manager-UPAM) e la segmentazione dinamica tra utenti, dispositivi e applicazioni (di default con Shortest Path Bridging-SPB, User Network Profiles-UNP), sia gestiti che non gestiti.

3. Macro e micro-segmentazione

La macro e la micro-segmentazione consentono un approccio granulare e altamente controllato alla sicurezza informatica per tutti gli utenti, dispositivi e applicazioni che accedono alla rete. La macro-segmentazione separa utenti, dispositivi e applicazioni in base al loro dominio funzionale, impedendo la comunicazione con elementi appartenenti ad altri macro-segmenti. Ad esempio, le applicazioni unified communication e collaboration di un macro-segmento non possono comunicare con le tecnologie adibite alla sicurezza, come telecamere a circuito chiuso e sistemi di chiusura porte, in un secondo macro-segmento, né con sensori e controlli per l'illuminazione, riscaldamento e condizionamento in un terzo macro-segmento.

La micro-segmentazione definisce il modo in cui utenti, dispositivi e applicazioni all'interno di un macro-segmento possono interagire tra loro ed è generalemnte regolata da policy di sicurezza molto specifiche. Ad esempio, una telecamera di sorveglianza non dovrebbe essere autorizzata a interfacciarsi con una serratura elettronica, anche se entrambi appartengono allo stesso macro-segmento in termini di sicurezza.

4. Crittografia end-to-end

Dipendenti, clienti, partner e fornitori possono trovarsi ovunque. Le soluzioni che utilizzano per comunicare e collaborare possono essere installate nell'edificio in cui lavorano, dall'altra parte della città, o in un data center all'altro capo del mondo e devono garantire scambi di informazioni sicuri e riservati tramite voce, video e testo. Ogni conversazione deve essere completamente crittografata dall'origine alla destinazione, per assicurare che solo i partecipanti possano accedere alle informazioni scambiate. Ciò significa che ogni elemento hardware e software coinvolto nelle comunicazioni end-to-end deve essere dotato di meccanismi di crittografia nativamente integrati e approvati dalle autorità di sicurezza.

5. Certificazioni di sicurezza, privacy e conformità normativa

Qualche anno fa, le certificazioni e gli accreditamenti di sicurezza più rigorosi erano richiesti esclusivamente per prodotti quali i firewall, o per settori come quello della difesa. Oggi standard di sicurezza specifici devono essere applicati a tutti i prodotti tecnologici, in qualsiasi settore. È fondamentale verificare che certificazioni e accreditamenti riconosciuti supportino le dichiarazioni di sicurezza informatica.

Ecco alcuni esempi di conformità da considerare:

- Standard globali di sicurezza e privacy, come l'ISO 27001
- Standard di sicurezza e privacy specifici per settore, come l'Health Insurance Portability and Accountability Act (HIPAA) negli Stati Uniti e l'Hébergeurs de Données de Santé (HDS) per l'hosting di dati sanitari in Francia.
- Regolamentazioni regionali di sicurezza e privacy, come il Regolamento Generale sulla Protezione dei Dati (GDPR) e la Direttiva NIS 2 nell'Unione europea.

6. Test continui e specifici sulla sicurezza

Come gli standard di sicurezza, anche i processi di test di sicurezza specifici, un tempo riservati ai prodotti di sicurezza, sono ora obbligatori anche per le soluzioni di unified communication e collaboration. I test di penetrazione sono un esempio lampante. Questi test simulano attacchi informatici per rivelare vulnerabilità di sicurezza, per poterle correggere proattivamente prima che si verifichino problemi. Per restare al passo con le minacce informatiche in un panorama in continua evoluzione, i test di penetrazione basati esclusivamente su requisiti di sicurezza informatica devono essere eseguiti in modo continuativo. I fornitori di tecnologia impegnati a supportare i propri clienti nel mantenere la massima sicurezza informatica devono fornire le risorse, le competenze e gli strumenti necessari per eseguire test di penetrazione continui.

7. Sovranità dei dati

La sovranità dei dati è diventata importante per la maggior parte delle aziende che devono proteggere la loro proprietà intellettuale, preservare la fiducia dei clienti e garantire un vantaggio competitivo. Con l'adozione di nuove tecnologie come il cloud e, più recentemente, l'IA, l'apertura dei sistemi di comunicazione delle aziende al mondo esterno è più importante che mai e la sicurezza dell'accesso alla rete è altrettanto fondamentale. Alcune aziende opteranno per una soluzione di cloud pubblico che soddisfi le loro esigenze, limitando al contempo la superficie di attacco interna del loro sistema informatico. Altre strutture sceglieranno un approccio più tradizionale, con applicazioni di unified communication ospitate sulla propria rete privata, sia on premises che in un cloud privato dedicato. Qualunque sia la scelta del cliente, ALE è in grado di fornire prodotti e servizi in qualsiasi contesto di implementazione per garantire la sovranità sui dati critici.

8. Operazioni intelligenti e automazione della sicurezza

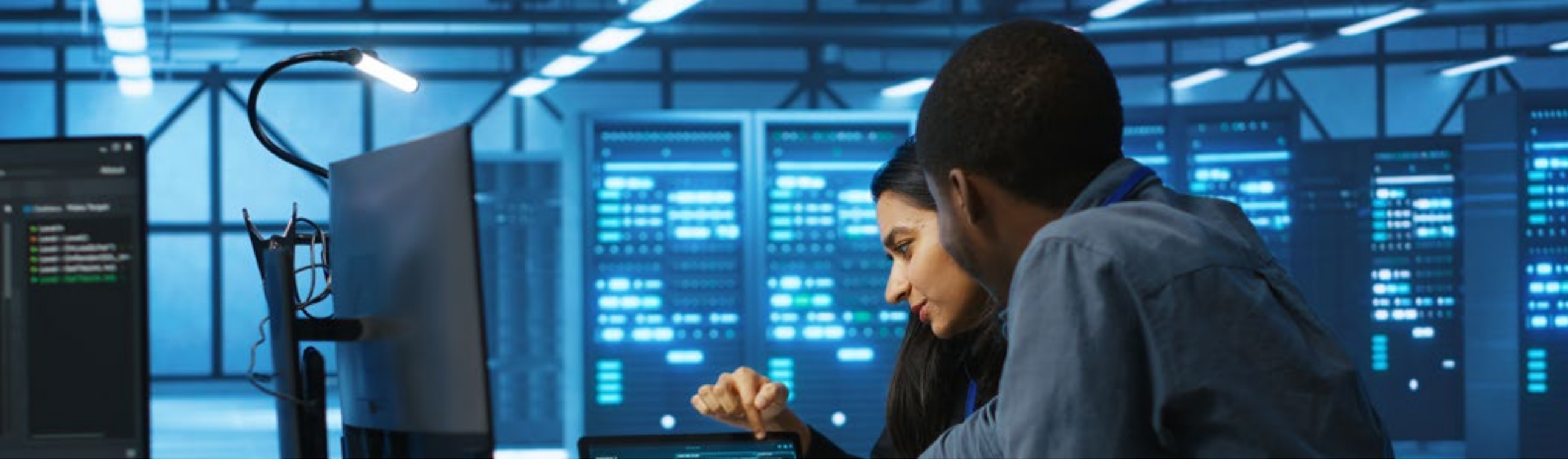
La suite OmniVista e Network Advisor di ALE introducono sicurezza operativa avanzata tramite monitoraggio in tempo reale, audit delle configurazioni e automazione della risposta alle minacce. Con l'AIOps integrato, le anomalie di rete vengono rilevate proattivamente e vengono suggerite azioni correttive guidate, spesso risorvibili con un solo clic, per affrontare problemi di QoE o di conformità. Questo riduce l'errore unamo, accelera la risposta agli incidenti e garantisce il ripsetto delle policy anche in ambienti complessi.

9. Connettività sicura ovunque

ALE supporta la SD-WAN sicura per aziende con più sedi e lavoro remoto, combinando visibilità della rete, sicurezza e ottimizzazione delle prestazioni, in linea con i moderni modelli di lavoro. Con crittografia MACsec, l'integrità e la riservatezza dei dati sono garantite in ambienti WAN multisito.

10. Software per la Supply Chain sicuro e affidabile

ALE applica misure rigorose per proteggere il software della propria supply chain, incluse immagini firmware firmate, processi di avvio sicuri, sisetmi operativi rinforzati e validazione indipendente del codice sorgente. Queste pratiche limitano l'esposizione alle minacce basate sul software e garantiscono ambienti di implementazione affidabili.



Perché scegliere ALE, come partner affidabile per proteggere l'infrastruttura di rete e la piattaforma di comunicazione della tua azienda

Mentre molti fornitori di tecnologia parlano di cybersecurity, pochi possiedono le competenze necessarie per garantire una protezione end-to-end. Alcatel-Lucent Enterprise va oltre, applicando tutte le best practice necessarie per offrire una cybersecurity pienamente integrata e sicura.

Alcatel-Lucent Enteprise si impegna a:

- Applicare le best practice e le reccomandazioni del National Institute of Science and Technology (NIST) in sede di valutazione del rischio di nuove funzionalità e in fase di implementazione delle funzionalità di sicurezza informatica, come la crittografia nativa, nei propri prodotti.
- Applicare gli standard ISO 27001 a tutte le sue soluzioni.
- Promuovere l'approccio ZTNA, la segmentazione di rete granulare nonché le policy di sicurezza concrete per ridurre il rischio di attività non autorizzate
- Eseguire test altamente specializzati e specifici per la sicurezza, come i test di penetrazione, su tutti i propri prodotti.
- Garantire che propri prodotti ottengano le principali certificazioni di settore, come HDS, HIPAA, Family Educational Rights and Privacy Act (FERPA) e FIPS 140-2 per pubblica amministrazione e difesa.
- Tenere conto delle certificazioni regionali dei prodotti, come CSPN di ANSSI in Francia, ENS in Spagna, ACN in Italia, C5 in Germania e ANATEL in Brasile
- Rispettare le normative regionali in materia di sicurezza e privacy, come il GDPR, il CRA e la direttiva NIS 2 dell'Unione Europea.

In qualità di esperti riconosciuti in cybersecurity, contribuiamo alle proposte dell'Unione Europea per le direttive di sicurezza informatica. Mettiamo inoltre a disposizione la nostra esperienza per aiutare i clienti a scegliere e implementare con il TCO più basso (30-50% di sconto) la combinazione di soluzioni di unified communication e collaboration sicure più adatta alle loro esigenze, nonché a formare i loro dipendenti sulle migliori pratiche di sicurezza informatica. Il nostro approccio all'architettura Zero-Trust consente ai nostri clienti di dimostrare ai loro assicuratori che stanno adottando una strategia proattiva e, in generale, di beneficiare di uno sconto fino al 20-30% sulla loro assicurazione contro i rischi informatici.

Conclusioni

Le tendenze relative alla sicurezza informatica del 2026 richiedono un cambiamento di paradigma nelle strategie aziendali. Le organizzazioni devono conciliare il duplice ruolo dell'IA come minaccia e difesa, investire in supply chain resilienti per resistere agli attacchi ransomware e riprogettare i sistemi di gestione delle identità per un mondo basato sull'approccio zero trust. La conformità normativa, l'uso etico dell'IA e la collaborazione tra settori saranno elementi chiave per mitigare i rischi. Con l'espansione delle superfici di attacco dovuta all'adozione dell'edge computing e dell'l'IoT, le aziende che danno priorità a difese adattive, formazione dei dipendenti e attività proattivedi threat hunting saranno meglio posizionate per crescere in questo contesto instabile.

Il percorso futuro richiede innovazione tecnologica e il supporto e la competenza di un partner affidabile come Alcatel-Lucent Enterprise.

Maggiori informazioni

Per saperne di più, visita il sito ALE Security Solutions. Per parlare con uno dei nostri esperti di sicurezza, contattaci.

www.al-enterprise.com/it-it Il nome e il logo Alcatel-Lucent sono marchi registrati di Nokia usati su licenza da ALE. Per maggiori informazioni sugli altri marchi utilizzati dalle affiliate di ALE Holding, visitare il sito web: www.al-enterprise.com/en/legal/trademarks-copyright. Tutti gli altri marchi appartengono ai rispettivi proprietari. Le informazioni presentate sono soggette a modifiche senza preavviso. ALE Holding e le sue affiliate non si assumono alcuna responsabilità per eventuali inesattezze contenute nel presente documento. © 2026 Copyright ALE International, ALE USA Inc. Tutti i diritti riservati in tutti i paesi. DID25080602IT (Gennaio 2026)

Alcatel·Lucent
Enterprise