Club It&C
WWW.CLUBITC.RO
APRILIE 2026

Gestionarea identității și a accesului este esențială pentru infrastructură

Regândirea securității pentru Agentic AI

CARDURILE BIOMETRICE: noul standard în plăți

pag. 12 De ce viitorul securității este scris în ADN-ul datelor

CUPRINS

ANALIZA

4 - Cinci predicții cibernetice pentru 2026
12 De ce viitorul securității este scris în ADN-ul datelor
30 Inteligenta Artificială: între accelerarea inovației și responsabilitatea securității
36 - Riscurile pentru infrastructura de transport în 2026

BRIEF

13 ELKO Romania adaugă i-PRO Co. în portofoliul său
21 Exclusive Networks obține statutul de Engage Preferred Services Partner Fortinet pentru țările din regiunea CEE și Orientul Mijlociu
35 RSA anunță o nouă integrare cu Microsoft Edge for Business pentru a îmbunătăți securitatea Zero Trust

AI

14 Regândirea securității pentru Agentic AI

CLOUD

10 M247, partenerul tău „de încredere digitală”
37 Întreprinderile aleg cloud-ul hibrid pentru reziliență, nu pentru simplitate

EVENIMENTE

8 ProVision Security Day

FINANCIAR

9 Identitate și acces în domeniul bancar, al serviciilor financiare și al asigurărilor
20 Criza costurilor operaționale legate de fraudă: de ce modelul actual nu poate fi scalat
22 Cardurile biometrice: noul standard în plăți

NEW TECHNOLOGY

40 Ce sunt, ce fac și de ce e nevoie de polițiști cripto în Web3?

NETWORKING

3 Rolul infrastructurii de rețea în securitatea colaborării
32 Cât de sigure sunt platformele moderne de colaborare?
33 Soluții de AI devoltate de Milestone pentru operațiuni de securitate

SERVICII

26 Ce presupune cu adevărat construirea unui Security Operations Center (SOC)
28 Capabilități enterprise în Security Center SaaS pentru investigații mai rapide și mai eficiente
38 VBSOC - Securitatea cibernetică de nivel enterprise mai aproape de IMM-uri

SOLUTII

6 Securitate pentru medii enterprise
16 Funcționalități avansate de Identity and Autentication Management în SAP Business One
18 De ce gestionarea identității și a accesului este esențială pentru infrastructură
19 Sunt cheile de acces pregătite pentru utilizare în cadrul întreprinderilor?
24 Operațiuni de securitate bazate pe analiză unificată și control operațional integrat
25 Piața smart home din România accelerează, în timp ce rămâne în faza de early adoption
27 Platformele integrate cresc nivelul de securitate
31 Securitatea imprimantelor este adesea neglijată
34 Amprenta “Life in Codes” în industria securității cibernetice

STUDII

29 Aproape 90% dintre organizații preferă modele SOC externalizate sau hibride
39 Amenințările din telecom din 2025 se vor extinde în 2026, pe măsură ce noile tehnologii aduc riscuri suplimntare

Club IT&C

Cristian Darie
cristian.darie@clubitc.ro
Director general

REDACȚIE
Andrei Marian
Cristina Manea
revista@clubitc.ro

ANALIȘTI
Bogdan Marchidanu

DTP
Georgiana Iosef
Art Director

ADVERTISING
revista@clubitc.ro

FOTO
Iustinian Scărlătescu

Club IT&C este marcă înregistrată

Str. Răchitașului nr. 6, sector 5, București; C.P. 51 - 43
Tel.: (021) 420.02.04
E-mail: revista@clubitc.ro
Web: www.clubitc.ro
ISSN 1583 - 5111

Rolul infrastructurii de rețea în securitatea colaborării

În contextul digitalizării accelerate, numărul și diversitatea echipamentelor interconectate au explodat pe măsură ce ele au devenit esențiale pentru funcționarea organizațiilor moderne.

Odată cu extinderea acestora, crește și implicit suprafața de atac, mai ales atunci când vorbim de echipamente IoT, unele cu capabilități și resurse limitate. În viziunea specialiștilor Allied Telesis, securitatea este o problemă ce trebuie abordată integrat, pornind de la aplicațiile utilizate până la infrastructura de rețea ce reprezintă fundamentul pe care rulează toate aplicațiile de business ale oricărei întreprinderi.

Soluțiile oferite includ autentificare avansată a dispozitivelor folosing metode standardizate (ex. 802.1x), liste de control al accesului, protocoale securizate și protecție împotriva atacurilor de tip DoS. Aceste mecanisme permit controlul strict al accesului utilizatorilor și dispozitivelor la resursele de colaborare, reducând riscul accesului neautorizat.

Management centralizat și vizibilitate extinsă

În viziunea Allied Telesis, un element esențial al securității cibernetice este vizibilitatea totală asupra rețelei și echipamentelor conectate la ea. Prin soluții avansate dezvoltate intern sau prin integrarea platformelor 3rd-party sub formă de plugin, organizațiile pot autentifica, autoriza și monitoriza în timp real dispozitivele și fluxurile de date asociate. Avantajele acestei abordări constau în detectarea rapidă a incidentelor de securitate, identificarea comportamentelor anormale și administrare unificată a politicilor de securitate. Această integrare este crucială pentru organizațiile moderne care partajează aplicații ce rulează centralizat, în centre de date proprii sau în cloud.

Integrarea securității fizice și cibernetice

Allied Telesis promovează conceptul de securitate convergentă, unde securitatea IT și cea fizică sunt integrate într-un ecosistem unitar. Colaborările cu furnizori de sisteme de gestiune video, precum Genetec și Milestone, demonstrează această direcție. Prin integrarea vizibilității și controlului echipamentelor de acces la rețea în platformele și sistemele de management a camerelor video se obține nu doar o protecție extinsă a infrastructurii, dar se simplifică semnificativ administrarea și operarea sistemelor mari, mărind gradul de scalabilitate și capacitatea acestora de operare. Pentru întreprinderi, acest lucru înseamnă o protecție mai bună nu doar a perimetrului fizic, dar și a tuturor datelor digitale prin limitarea accesului la rețea a dispozitivelor care nu se află într-o locație autorizată pentru această operație.

Automatizare și reacție la incidente

Un alt pilon important este automatizarea securității. Echipamentele Allied Telesis pot detecta activități suspecte și pot declanșa automat acțiuni de protecție a rețelei prin blocarea automată a accesului sau izolarea dispozitivului compromis. Această capacitate este esențială pentru reducerea timpului de reacție, limitarea impactului atacurilor și menținerea continuității serviciilor.

Scalabilitate și flexibilitate pentru mediile moderne

Aplicațiile companiilor moderne sunt utilizate în medii distribuite (remote work, cloud, IoT) ceea ce modifică abordarea tradițională a securității. Allied Telesis pune accent pe soluții unitare, scalabile, și interoperabile între sisteme de securitate cibernetică și securitate fizică. Astfel, organizațiile pot extinde fără compromisuri infrastructura de acces la date, în locații multiple și pentru actori diverși, deopotrivă oameni și mașini.

Concluze

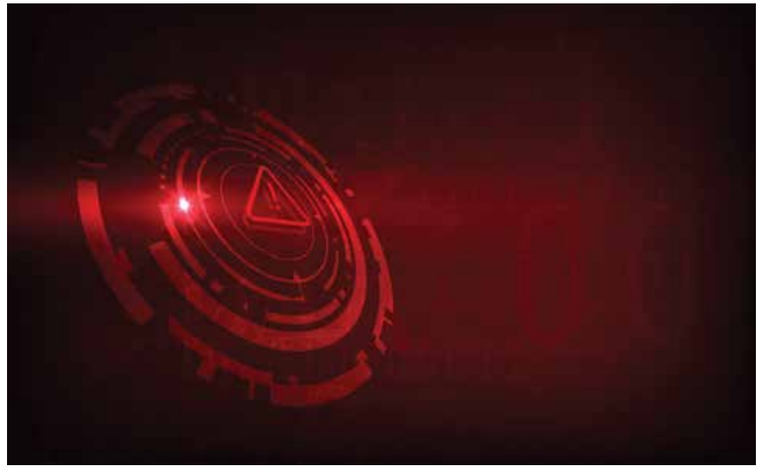
În viziunea Allied Telesis, securitatea infrastructurii operaționale nu este un element ce trebuie tratat izolat, ci un proces complex, bazat pe:

- securizarea infrastructurii de rețea
- vizibilitate și management centralizat
- integrarea securității fizice cu cea cibernetică
- automatizarea răspunsului la incidente
- scalabilitate și interoperabilitate.

Această abordare integrată permite organizațiilor să creeze medii de operare sigure, eficiente și adaptate cerințelor actuale ale transformării digitale.

Cinci predicții cibernetice pentru 2026

Pe măsură ce granițele dintre eroarea umană și inteligența artificială se estompează, apărarea nu a fost niciodată mai personală.



Ce-ar fi dacă ți-am spune că cea mai mare vulnerabilitate cunoscută a anului 2026 nu este tehnologia ta, ci încrederea ta?

Oamenii rămân cea mai ușoară cale de acces pentru atacatorii rău intenționați, iar inteligența artificială tocmai a făcut ca ingineria socială să fie aproape imposibil de oprit.

Amenințările cuantice și cele din cloud vin mult mai repede decât ne putem pregăti, iar vechile strategii pur și simplu nu vor fi suficiente.

În 2026, reziliența nu va depinde de a avea cele mai multe instrumente sau protecții, ci mai degrabă de a ști cu încredere în ce (și în cine) poți avea încredere.

Ceea ce diferențiază aceste tendințe este că sunt menite să convergă pe parcursul anului următor. Și într-un viitor care cu siguranță va testa fiecare strat de apărare pe care îl credeai sigur, amenințările de anul viitor au devenit personale.

1. Oamenii sunt cheia pentru a debloca secretele unei companii

O tendință pe care am observat-o în mai multe atacuri din acest an este cea a atacurilor care obțin acces la rețelele victimelor nu prin valorificarea vulnerabilităților zero-day sau prin utilizarea unor atacuri sofisticate asupra lanțului de aprovizionare software, ci mai degrabă prin profitarea de cea mai mare slăbiciune a organizațiilor - oamenii care lucrează acolo.

Un val de atacuri au fost efectuate de grupul de extorcare Shiny Hunters, care a vizat clienții Salesforce cu atacuri de vishing (phishing vocal) pentru a compromite acreditările sau pentru a păcăli angajații să autorizeze o aplicație OAuth rău intenționată pentru a obține acces la portalurile Salesforce ale companiilor - fără a fi nevoie de malware sau tactici sofisticate. Atacatorii furau apoi date și încercau să extragă o răscumpărare de la compania afectată.

Aceste atacuri reflectă atacuri similare pe care le-am văzut efectuate de grupul de atac Scattered Spider, despre care se știe, de asemenea, că obține acces în principal la rețelele victimelor prin efectuarea de atacuri sofisticate de inginerie socială. Aceștia au compromis numeroase cazinouri din Las Vegas în 2023, iar în 2025 au implementat ransomware-ul DragonForce în rețelele mai multor comercianți cu amănuntul cunoscuți din Marea Britanie.

Succesul acestor grupuri care utilizează astfel de tactici înseamnă că este foarte probabil să vedem și alte atacuri de natură similară în 2026. Inteligența artificială - care poate fi utilizată pentru a falsifica voci și a face ca e-mailurile frauduloase să pară mai autentice - oferă, de asemenea, atacatorilor oportunitatea de a face ca atacurile de inginerie socială să pară și mai credibile și le face un pericol și mai mare pentru organizații.

2. Rusia și Iranul ar putea oferi un răspuns cibernetic presiunilor din lumea reală

Presiunile geopolitice continue asupra Rusiei și Iranului ar putea determina actorii amenințători din aceste țări să inițieze atacuri cibernetice perturbatoare sau agravante asupra adversarilor lor, cum ar fi Ucraina, Israel, UE. și SUA. Dacă nu reușesc să își stabilească dominația militară asupra rivalilor lor, atunci pot folosi spațiul cibernetic pentru a-și susține punctul de vedere. Atacatorii din aceste țări pot, în unele cazuri, să nu aibă abilitățile și resursele necesare pentru a comite atacuri cu adevărat distructive împotriva inamicilor lor, dar atacurile de tip „distributed-denial-of-service" (DDoS), răspândirea dezinformărilor și alte activități perturbatoare ar putea fi desfășurate împotriva entităților pe care atacatorii cibernetici din aceste țări le percep ca acționând în opoziție cu regimul țării.

Recent, incursiunile dronelor în spațiul aerian al UE au cauzat probleme pentru mai multe aeroporturi, dronele care operau în spațiul aerian polonez fiind doborâte, în timp ce alte aeroporturi europene, inclusiv cele din Copenhaga, au fost, de asemenea, perturbate de activitatea dronelor în spațiul lor aerian. Vina pentru aceste incidente a fost atribuită Rusiei, deși aceasta a negat orice implicare în această activitate.

Un atac ransomware împotriva Collins Aerospace a perturbat grav operațiunile pe mai multe aeroporturi europene în septembrie 2025. Ransomware-ul a afectat software-ul Muse utilizat de Collins Aerospace, descris ca o „soluție de sistem de procesare a pasagerilor de generație următoare, de uz comun, care permite mai multor companii aeriene să partajeze ghișeele de check-in și pozițiile la poarta de îmbarcare de pe un aeroport, în loc să aibă propria infrastructură dedicată". Incidentul a însemnat că mai multe companii aeriene au fost afectate și că doar check-in-ul manual a fost disponibil pentru pasagerii care urmau să zboare, ceea ce a cauzat întârzieri majore. Deși se crede că acest incident nu este legat de activitatea statului național, acesta subliniază tipul de haos pe care actorii statului național l-ar putea provoca cu un atac similar de o astfel de natură.

Având în vedere că situația geopolitică globală este probabil să rămână instabilă pentru o perioadă de timp, perturbările și agravarea ar putea fi numele problemei. pentru atacatorii cibernetici în 2026.

3. AI Agentic va schimba peisajul amenințărilor (dar nu în modul în care credeți)

Nu există absolut nicio îndoială că AI Agentic va deveni un instrument puternic în mâinile atacatorilor și acest lucru s-ar putea întâmpla încă din 2026.

Când oamenii se gândesc la AI în mâinile unor actori rău intenționați, acest lucru ridică în mod natural temeri că aceasta va fi utilizată pentru a crea amenințări noi cu niveluri de sofisticare fără precedent. Ceea ce este mult mai probabil este că AI Agentic va afecta cantitatea atacurilor mai mult decât calitatea. Pe scurt, are potențialul de a reduce radical bariera de intrare pentru atacatori.

În prezent, un atac reușit necesită o investiție de timp și un nivel minim de expertiză tehnică. AI Agentic ar putea elimina aceste cerințe preliminare. În timp ce atacatorii anterior trebuiau să poată scrie sau achiziționa cod, să identifice vectori de infecție, să construiască seturi de instrumente de atac, să creeze infrastructură și, în multe cazuri, să includă un anumit nivel de phishing sau inginerie socială, agenții autonomi ar putea gestiona aceste complexități, cu o interacțiune sau instrucțiuni minime din partea atacatorului.

Rezultatul ar putea fi o creștere semnificativă a atacurilor automate lansate de oportuniști cu abilități limitate.

4. Spargerea indestructibilului: Provocarea iminentă a calculului cuantic

Calculul cuantic este pe cale să apară și, deși va fi o tehnologie transformatoare, reprezintă și o provocare serioasă pentru infrastructura de securitate actuală. Simplu spus, computerele cuantice reprezintă un risc existențial pentru standardele actuale de criptare care protejează totul, de la tranzacțiile financiare la comunicațiile securizate.

Metodele actuale de criptare se bazează pe probleme matematice care sunt imposibil de rezolvat din punct de vedere computațional pentru computerele din generația actuală. Cu toate acestea, computerele cuantice ar putea sparge aceste sisteme în câteva minute.

Adversarii implementează deja atacuri de tip „recoltare acum, decriptare mai târziu" (HNDL), colectând sistematic date criptate cu intenția de a le decripta odată ce calculul cuantic devine viabil. Această strategie reprezintă o amenințare clară, deoarece atacatorii nu au nevoie de capacitățile actuale de decriptare - ei pur și simplu stochează comunicații criptate, înregistrări financiare și date sensibile până când computerele cuantice pot sparge criptarea.

Acest proces de tranziție la criptarea post-cuantică nu este lipsit de provocări. Decenii de muncă au fost dedicate rafinării și protejării implementării metodelor de criptare existente, iar acum ne confruntăm cu sarcina de a revizui și rescrie codul folosind standarde noi, post-cuantice. Acest lucru va introduce inevitabil o nouă generație de erori, dar vom avea beneficiul inteligenței artificiale pentru a le atenua.

5. Nori la orizont

Există unele semne că 2026 ar putea fi anul în care o masă critică de atacatori își vor îndrepta atenția către atacuri împotriva mediilor cloud ale întreprinderilor.

Până în prezent, atacurile împotriva cloud-ului au reprezentat un mic subset de activitate rău intenționată. Deși majoritatea serviciilor cloud sunt, fără îndoială, robuste, alți doi factori au limitat numărul de atacuri: Actorii rău intenționați încă profitau generos de atacurile asupra rețelelor convenționale și nu existau cunoștințe aprofundate despre modul în care serviciile cloud puteau fi încălcate.

Există dovezi că un număr tot mai mare de atacatori își aprofundează acum înțelegerea platformelor cloud și încep să identifice strategii de atac viabile. Este doar o chestiune de timp până când aceste cunoștințe se vor răspândi.

Exploatarea managementului identității și accesului (IAM) dă deja roade. Atacatorii examinează acum depozitele de cod pentru a găsi chei de acces uitate. Folosind acestea, pot crea noi utilizatori IAM și pot atașa politici cu privilegii ridicate, stabilind acces persistent la mediile cloud.

Infrastructure-as-Code (IaC) a facilitat crearea rapidă și automată de către organizații a noii infrastructuri, după cum este necesar. Cu toate acestea, atacatorii încep deja să caute puncte slabe, cum ar fi secretele codificate hardcoded în șabloanele IaC sau configurațiile greșite care duc la resurse expuse publicului.

Pe măsură ce atacatorii își extind cunoștințele despre suprafața de atac în cloud, organizațiile trebuie să țină pasul, identificând potențialele vulnerabilități și implementând arhitecturi zero-trust.

Cea mai bună strategie nu va cădea pur și simplu în mâinile tale

Dacă 2025 ne-a învățat ceva, este că complexitatea generează oportunități atât pentru atacatori, cât și pentru apărători. Dar protejate sub straturi de securitate încercate, de încredere și adevărate, mașinile (și oamenii) noastre pot deveni o sursă de putere și rezistență de durată.

SolvIT Networks vă ajută să vă protejați datele de pierdere și furt, să fiți în conformitate cu legile privind confidențialitatea, și să vă protejați reputația

Securitate pentru medii enterprise

Aplicațiile enterprise sunt expuse constant unor riscuri precum injecții (SQL, OS, LDAP), autentificare și autorizare defectuoasă, expunerea datelor sensibile, configurări greșite ale infrastructurii sau vulnerabiliăți în API-uri.

Soluțiile Tenable permit identificarea continuă a acestor vulnerabilități prin scanare și management unificat al expunerilor, în timp ce Gigamon oferă vizibilitate profundă asupra traficului aplicațiilor, facilitând detectarea comportamentelor anormale. Din perspectiva Thales, cele mai frecvente probleme sunt autentificarea slabă sau incompletă, lipsa MFA pentru conturi sensibile, drepturile prea largi, ciclul de viață prost gestionat al identităților și păstrarea cheilor/certificatelor în software sau pe servere obișnuite.
Faptul că Thales pune accent pe MFA, SSO, identity lifecycle management, risk-based authentication și pe stocarea cheilor în HSM arată exact unde apar cele mai des breșele în aplicațiile enterprise moderne. În plus, Thales subliniază explicit că cheile private păstrate pe servere sunt mult mai expuse la compromitere decât cele din HSMuri.

De la o abordare reactivă la una proactivă

Modelul tradițional, bazat pe reacție post-incident, este depășit. Organizațiile moderne adoptă testare continuă (DevSecOps), integrarea securității în SDLC și monitorizarea în timp real.

Extreme Networks contribuie prin soluții de rețea inteligente care oferă control și segmentare avansată, reducând suprafața de atac, iar Infoblox securizează infrastructura DNS — un vector frecvent exploatat.
Trecerea reală la proactiv înseamnă să nu mai aștepți incidentul ca să întărești controalele, ci să construiești aplicația pe o fundație de identitate și criptografie: acces centralizat, MFA implicit, politici adaptive, verificare contextuală și chei critice izolate în HSM din primul moment. În modelul Thales, asta se traduce prin SSO și politici bazate pe scenarii în SafeNet Trusted Access, onboarding și lifecycle control în OneWelcome și hardware root of trust în Luna HSM, astfel încât compromiterea unui cont sau a unui server să nu însemne automat compromiterea identității ori a materialului criptografic.

Rolul automatizarii in detectarea si prevenirea vulnerabilitatilor

Red Hat Ansible Automation Platform oferă numeroase tool-uri de automatizare a securității, precum: enforce security și compliance, automate security enrollments, gather and audit inventories, răspuns automat la probleme de securitate, automate penetration testing and hardening, enforce cloud hygiene.

Automatizarea contează cel mai mult în provisioning/deprovisioning, aplicarea politicilor de acces, autentificarea la risc crescut și administrarea la scară a autentificatorilor și cheilor. Thales evidențiază lifecycle management pentru identități, politici de acces aplicate în timp real și administrarea ciclului de viață al cheilor FIDO, iar pe partea HSM rolul automatizării este să permită semnare, PKI și alte operații criptografice fără ca dezvoltatorii sau pipeline-urile să poată extrage cheile. Cu alte cuvinte, automatizarea bună reduce atât eroarea umană, cât și „secret sprawl".

În acest context, inteligența artificială (AI) și machine Learning (ML) detectează anomalii in comportamentul aplicațiilor, reduc rezultatele fals-pozitive și anticipează atacuri.

Extreme Networks integrează analize bazate pe AI pentru monitorizarea rețelei, iar Infoblox utilizează threat intelligence automatizat pentru a bloca domenii malițioase în timp real. Da, dar mai ales ca strat de detecție și decizie, nu ca substitut pentru controalele de bază.

În zona Thales, AI/ML ajută în special prin risk-based authentication, fraud/risk management și identity verification, unde semnalele de comportament și context sunt folosite pentru a identifica tentative de abuz înainte ca ele să producă impact. Totuși, chiar și cu AI, fundația rămâne aceeași: identități bine guvernate, autentificare puternică și chei protejate în HSM. AI îmbunătățește răspunsul, dar nu înlocuiește aceste controale.

Prioritizarea trebuie să țină cont de severitate (CVSS), expunere reală și impact asupra business-ului. Tenable oferă scoruri de risc bazate pe context, iar datele de trafic furnizate de Gigamon ajută la înțelegerea exploatabilității reale. Așadar, mai întâi orice vulnerabilitate care duce la compromiterea unei identități privilegiate, apoi cele care permit acces excesiv sau conturi rămase active, iar imediat după aceea orice expunere de chei private, certificate sau fluxuri de semnare.

Din perspectiva Thales, lipsa MFA pentru privileged users este deja asociată cu breșe reale, iar compromiterea unei chei private poate transforma un incident punctual într-o problemă de încredere la scară largă.

Evaluarea impactului unui atac asupra aplicatiilor critice

Impactul trebuie evaluat în funcție de downtime, pierderi financiare, afectarea reputației și compromiterea datelor.

Vizibilitatea oferită de Gigamon și controlul infrastructurii DNS prin Infoblox sunt esențiale pentru limitarea impactului.

Impactul ar trebui evaluat pe patru axe: ce identitate a fost compromisă, ce nivel de privilegii avea, dacă au fost afectate chei/certificate și care este efectul operațional asupra utilizatorilor sau proceselor critice.

Într-o arhitectură Thales, dacă identitatea este compromisă, adaptive access și politicile de acces pot limita abuzul; dacă însă este compromisă o cheie privată în afara HSM-ului, consecințele pot fi mult mai greu de controlat, fiindcă afectează însăși încrederea criptografică a aplicației, a sesiunilor TLS sau a semnăturilor software. De aceea, compromiterea identității și compromiterea cheii nu trebuie tratate ca incidente echivalente.

Important de spus aici este faptul că cultura organizațională joacă un rol critic.

De ce? Există câțiva factori esențiali. Securitatea trebuie sa fie responsabilitatea tuturor. Trebuie să existe colaborare între echipele IT, Dev si Sec. Nu în ultimul rând, este necesară asigurarea unui antrenament continuu. În context, Extreme Networks susține acest model prin vizibilitate și control asupra utilizatorilor și dispozitivelor. Cultura organizațională decide dacă securitatea devine standard de engineering sau doar o excepție impusă de audit.

În companiile unde există disciplină pe identitate și chei, echipele adoptă mai ușor SSO, MFA, passwordless, lifecycle automatizat și hardware root of trust. În celelalte apar inevitabil conturi locale, excepții permanente, chei în fișiere și politici neuniforme. Thales leagă în mod direct încrederea digitală de experiențele de sign-up, login și de modul în care identitatea și datele sunt gestionate pe tot parcursul ciclului lor de viață, ceea ce arată că problema nu este doar tehnică, ci și culturală.

Rolul Zero Trust în protejarea aplicațiilor moderne

Modelul Zero Trust presupune verificare continuă. Segmentarea strictă Extreme Networks permite implementarea segmentării dinamice, iar Infoblox contribuie la controlul accesului prin securizarea DNS și a serviciilor de rețea. În modelul Thales, Zero Trust înseamnă foarte clar: „verify everywhere, trust no one", acces decis la punctul de intrare în aplicație, reevaluare continuă și default deny. SafeNet Trusted Access este prezentat de Thales ca punct de pornire pentru implementări Zero Trust, iar adaptive access poate ridica nivelul de autentificare sau revoca accesul în funcție de context și risc. Luna HSM completează acest model prin furnizarea unui hardware root of trust pentru cheile aplicației, astfel încât chiar dacă accesul logic este presat de atacatori, materialul criptografic rămâne separat și mult mai greu de compromis.

ProVision Security Day 2026

Împreună construim securitatea digitală de mâine

„Nicio organizație nu poate combate singură criminalitatea informatică" – aceasta a fost una dintre concluziile dezbaterilor din cadrul World Economic Forum. Deși există numeroase surse din care puteți afla noutățile din domeniul securității cibernetice, puține sunt acele contexte în care vă puteți simți cu adevărat parte dintr-o comunitate, alături de sute de colegi, experți și specialiști în tehnologie.

Într-un context în care colaborarea nu mai este opțională, ci esențială, ProVision Security Day 2026 vă invită să construim împreună securitatea digitală de mâine.

Conferința anuală ProVision Security Day va avea loc pe 28 mai, la Face Convention Center, și este organizată de ProVision, distribuitor cu valoare adăugată, cu peste 29 de ani de experiență în domeniul securității informației. Evenimentul reunește reprezentanți ai unor companii lider la nivel internațional, precum CrowdStrike, OPSWAT, Trellix, Thales, Stellar Cyber, Cynet, Forcepoint, Invicti, Intel 471, Qualys, OpenText, Radware, Sycope, și BeyondTrust alături de alți parteneri importanți din ecosistemul global de securitate cibernetică.

Conferința reunește profesioniști, lideri din industrie și specialiști IT pentru o zi dedicată dialogului, inovației și experiențelor practice.

Tematică și agendă

Tema ediției din acest an – „From past lessons to AI-Driven Defense: Building Cyber Resilience together" – invită participanții într-o incursiune de la optimizarea și adaptarea tehnologiilor tradiționale la noii vectori de atac, până la colaborările care pot construi o industrie și o comunitate mai puternică. Totodată, sunt abordate provocările și oportunitățile generate de inteligența artificială.

Conferința aduce în prim-plan teme precum gestionarea riscului uman, securizarea mediului online, noile suprafețe de atac, operarea securizată a AI, protecția identității digitale, criptografia post-cuantică și consolidarea SOC. Aceste subiecte vor fi explorate prin sesiuni de prezentări, dezbateri, demonstrații tehnice și simulări, oferind participanților o perspectivă practică asupra modului în care pot anticipa și gestiona riscurile actuale.

ProVision Security Day nu este doar un spațiu de prezentare, ci oferă și o platformă de interacțiune și învățare. Participanții vor putea explora tehnologii moderne, vor asista la demonstrații tehnice și vor lua parte la exerciții care simulează scenarii reale de atac, obținând o înțelegere concretă a provocărilor din teren.

Nevoia de colaborare în comunitate

În fața unor amenințări cibernetice tot mai sofisticate, acțiunea colectivă devine esențială. Colaborarea facilitează dezvoltarea unor strategii de securitate eficiente și aplicarea celor mai bune practici din industrie. Astfel, organizațiile își pot consolida apărarea și pot crește nivelul de protecție și reziliență al infrastructurilor critice, datelor, aplicațiilor și rețelelor de comunicații.

Conferința susține formarea unei comunități puternice, în care experiența, ideile și bunele practici se transformă în soluții concrete pentru un mediu digital mai sigur.

De ce este colaborarea esențială

Un studiu publicat de National Institute of Standards and Technology evidențiază faptul că:

- nivelul de complexitate al atacurilor moderne depășește capacitatea unei singure organizații;
- colaborarea între companii, experți și instituții este esențială pentru schimbul de cunoștințe, decizii strategice și inovație;
- „secure collaboration" este considerată una dintre cele mai dificile provocări din domeniul securității cibernetice.

În același timp, analizele ISACA arată că lipsa colaborării între echipe generează vulnerabilități majore, prin reducerea vizibilității asupra amenințărilor. În schimb, colaborarea contribuie direct la creșterea acoperirii securității, îmbunătățirea detectării riscurilor și reducerea erorilor umane.

Concluzia este clară: securitatea cibernetică nu mai este doar o funcție IT, ci o responsabilitate organizațională.

Pentru comunitatea IT și pentru organizațiile care tratează securitatea ca pe un element strategic, ProVision Security Day reprezintă o oportunitate de a descoperi perspective noi, de a înțelege direcțiile în care evoluează industria și de a contribui activ la construirea unui viitor digital mai sigur. Pentru că, în securitatea cibernetică, viitorul se construiește împreună.

Participarea la conferință este gratuită și necesită înregistrare pe site-ul oficial ProVision Security Day (https://provisionsecuritydays.ro/)..

Despre ProVision Security Day

ProVision Security Day (https://provisionsecuritydays.ro/) este un eveniment dedicat profesioniștilor din domeniul securității cibernetice, organizat de către ProVision încă din 2006. Evenimentul pune în evidență principalele tendințe și inovații tehnologice din acest sector și aduce pe scenă experți de renume din companii globale de prestigiu. Fondată în 1997, ProVision este cel mai important distribuitor „value added" (VAD) de soluții și produse de securitate cibernetică din România. Suplimentar, compania oferă servicii de consultanță, monitorizare, detecție și răspuns la incidente de securitate a informațiilor, prin intermediul echipelor specializate ale centrului **ProActive Hunt.**

Pentru mai multe detalii, vizitați **https://www.provision.ro/.**

Identitate și acces în domeniul bancar, al serviciilor financiare și al asigurărilor

Pe măsură ce transformarea digitală continuă să redefinească peisajul financiar, securitatea și integritatea managementului identității capătă o importanță din ce în ce mai mare. La Thales, asigurarea încrederii la fiecare punct de contact cu clienții, partenerii și forța de muncă este prioritatea noastră principală.

Raportul Thales din 2025, „Identitate și acces în domeniul bancar, al serviciilor financiare și al asigurărilor: imperativul schimbării", oferă informații colectate de la 475 de factori de decizie de top în domeniul IT și al securității din domeniul bancar, al asigurărilor, al investițiilor și al fintech-urilor din SUA, Marea Britanie și Singapore.

Perspectivele lor prezintă o imagine convingătoare a unei industrii aflate la o răscruce de drumuri – confruntându-se cu o creștere fără precedent a identității digitale, o vigilență de reglementare și amenințări din ce în ce mai sofisticate. Constatările evidențiază nu numai ce trebuie să se schimbe, ci și modul în care organizațiile cu viziune de viitor pot transforma aceste provocări într-un avantaj competitiv.

Ce trebuie să știe orice lider din industria financiară

1. Creșterea rapidă a identităților

- **Se preconizează că identitățile clienților vor crește cu aproape 74% în următoarele 12 luni.**
- Una din cinci organizații se așteaptă ca numărul de identități ale clienților să se dubleze, ceea ce indică o creștere a adoptării serviciilor digitale și așteptări sporite.

2. ROI, complexitate și dilema mai multor furnizori

- Organizațiile se bazează în prezent pe aproximativ patru furnizori pentru fiecare stivă de identități: soluții de identitate a forței de muncă și a clienților.
- **89% raportează o dorință urgentă sau moderată de a consolida aceste medii pentru a reduce complexitatea operațională, costurile și riscurile.**
- Migrarea de la o soluție DIY de identitate a clienților la o platformă CIAM modernă, comercială, a avut ca rezultat un impact pozitiv asupra ROI pentru 99% dintre respondenți.

3. Riscul partenerilor și contractorilor este în creștere

- **Identitățile terților vor crește cu 37% în următorul an. Partenerii, contractorii și furnizorii necesită acum un acces mai larg, gestionat prin riscuri, la date și aplicații critice.**
- Directorii executivi estimează o creștere chiar mai rapidă a identității terților decât a personalului operațional – evidențiind o lacună în comunicare care trebuie eliminată pentru o gestionare eficientă a riscurilor.

4. O schimbare de paradigmă: Identitatea ca centru de profit

- **% dintre organizații își văd stiva de identități a clienților ca pe un centru de profit, față de doar 32% care o consideră un cost pur – reflectând rolul strategic tot mai mare al identității.**

5. Angajament bugetar în vremuri incerte

- Majoritatea se așteaptă ca bugetele pentru securitatea identității să crească cu peste 10% în anul următor, chiar și în contextul unei precauții economice mai largi.
- Securitatea identității este acum esențială pentru inovare, conformitate și continuitatea afacerii.

6. Apelul la modernizare

- **93% au prioritizat modernizarea identității forței de muncă, iar 89% au mandate similare pentru soluții de acces terți.**

Sondajul scoate la iveală deconectările din lumea reală – dintre lideri și echipele din prima linie, dintre complexitate și dorința urgentă de consolidare, dintre a vedea identitatea ca pe un cost și a o vedea ca pe un factor de valoare al afacerii. Pe măsură ce intrăm în următoarea eră, firmele care vor prospera vor fi cele care investesc în modernizare, automatizare și parteneriate cu furnizori de securitate de încredere.

M247 Global, partenerul tău de „încredere digitală”

Aveți încredere în digitalizare sau o considerați un risc? Conform definiției oferite de World Economic Forum, „digital trust reprezintă așteptarea fiecărei organizații ca tehnologiile și serviciile digitale – și partenerii care le furnizează – să protejeze interesele tuturor părților implicate și să susțină valorile și așteptările societale”.

Această definiție, aparent simplă, ascunde o realitate complexă: organizațiile percep lipsa încrederii digitale ca pe o sursă de risc major, de la atacuri cibernetice la întreruperi ale serviciilor și neconformitatea cu reglementările în vigoare, cum ar fi GDPR sau NIS 2.

Digital trust: o prioritate strategică

Date recente confirmă această tendință. Conform studiului PwC 2026 Global Digital Trust Insights, realizat pe un eșantion de 3.887 de directori de business și tehnologie din 72 de țări, 60% dintre liderii organizațiilor plasează investițiile în securitatea cibernetică în top trei priorități strategice. Totuși, studiul arată și un paradox: doar 24% dintre organizații investesc semnificativ mai mult în măsuri proactive (monitorizare, evaluări, teste, controale) decât în măsuri reactive (răspuns la incidente, recuperare, amenzi). Această discrepanță evidențiază faptul că, deși digital trust-ul este perceput ca prioritate, implementarea lui completă rămâne un obiectiv în lucru.
În termeni practici, încrederea digitală se construiește pe mai mulți piloni tehnologici:

- Disponibilitatea infrastructurii IT – sistemele trebuie să fie accesibile și funcționale constant; downtime-ul afectează nu doar productivitatea, ci și reputația organizației.
- Conectivitatea și latența minimă – pentru companiile care operează global, accesul rapid și fiabil la resursele digitale este esențial.
- **Securitatea cibernetică** – protecția împotriva atacurilor, DDoS și accesului neautorizat este fundamentală.
- **Conformitatea cu reglementările** – respectarea standardelor legale, precum GDPR, PCI-DSS sau NIS 2, este obligatorie.
- **Backup și recuperare în caz de dezastru** – redundanța și planurile de continuitate

garantează protecția datelor critice.
Pentru rezultate optime acești piloni trebuie să fie integrați și monitorizați constant, iar pentru aceasta, organizațiile au nevoie de un partener tehnologic de încredere.

M247 Global: furnizorul de încredere digitală în România

În România, M247 Global s-a afirmat ca partener strategic pentru companiile care doresc să-și construiască și să mențină reziliența digitală. Experiența de peste 20 de ani în infrastructură IT, rețele globale și servicii de securitate poziționează compania ca un furnizor relevant pentru nevoile digitale ale unei organizații.

Infrastructură și conectivitate

Baza relației de încredere pe care M247 Global o construiește cu clienții din România se sprijină pe infrastructura sa de top. Centrul de Date M247 Global, situat în Pipera, București, este proiectat conform standardelor Tier III și este conceput să susțină sarcini critice de business, asigurând performanță și continuitate maximă.
M247 Global oferă servicii complete de colocare a infrastructurii IT în centrul din București, cu un al doilea centru în Brașov pentru redundanță și disponibilitate sporită. Această arhitectură asigură 99,99% uptime, protecție împotriva întreruperilor și continuitate operațională indiferent de scenariu.
Infrastructura este complet redundantă, cu alimentare și răcire dual, și este monitorizată 24/7/365 de o echipă dedicată de specialiști.

Caracteristici cheie ale centrelor M247 Global:

- Infrastructură de ultimă generație, cu sisteme eficiente din punct de vedere energetic (PUE competitiv, reflectat în costuri avantajoase)
- Alimentare redundantă cu UPS și generatoare diesel (N+1)
- Sisteme de răcire profesionale, configurate N+1
- Conectivitate avansată la rețea, cu opțiuni de peering și transit
- Securitate fizică de nivel înalt: CCTV, control acces, personal de securitate la fața locului
- Acces facil pentru upgrade-uri, înlocuiri și mentenanță
- Suport tehnic disponibil 24/7/365
- Acces la energie 100% verde
- Suport profesionist pentru migrarea infrastructurii

La nivel de rețea, M247 oferă un backbone global, cu conexiuni directe către principalele Internet Exchange Points (IXPs) și marii provideri de cloud, asigurând viteză ridicată și latență minimă, esențială pentru afacerile cu operațiuni internaționale. Această conectivitate robustă permite clienților extinderea rapidă a capacităților digitale, fără limite geografice.

Securitate și continuitate

Un alt pilon al încrederii digitale este protecția datelor și securitatea cibernetică.

M247Global oferă:

- DDoS Protection – detectare și contracarare automată în timp real a atacurilor distribuite.
- Backup și Disaster Recovery (BaaS/DRaaS) – folosind tehnologiile Veeam și Zerto, datele critice sunt replicate geografic, cu posibilitatea de recuperare rapidă în caz de incident.
- Managed Security Services – firewall-uri de generație nouă (bazate pe Fortinet), monitorizare continuă și securizarea infrastructurii IT.

În plus, infrastructura M247 respectă cerințele GDPR și PCI-DSS, oferind medii izolate, private, care permit control complet asupra localizării datelor. Astfel, companiile din România se pot baza pe conformitate și protecție maximă a informațiilor sensibile.

Expertiză și suport

Încrederea digitală nu se construiește doar prin tehnologie, ci și prin echipe specializate care pot ghida companiile în implementarea și menținerea acestuia. M247 pune la dispoziție experți care asistă clienții în migrări, optimizări de infrastructură și managementul securității, asigurându-se că fiecare decizie tehnologică contribuie la reducerea riscurilor și creșterea încrederii digitale.
Pe lângă suportul tehnic, compania ajută organizațiile să implementeze măsuri proactive de protecție, nu doar reacții la incidente, conform celor identificate în studiul PwC. Aceasta include monitorizare 24/7 , teste de vulnerabilitate și evaluări continue ale infrastructurii.

Tehnologii avansate pentru AI

M247 Global nu se limitează la infrastructură și securitate clasică. Compania oferă servere dedicate pentru AI și machine learning, găzduite în medii sigure și conforme, adaptate pentru cerințele companiilor moderne. Această combinație între performanță, securitate și conformitate face din M247 un partener complet pentru companiile care doresc să construiască un avantaj competitiv bazat pe date.

Încredere în viitorul digital

Astăzi, orice organizație și orice utilizator se așteaptă ca tehnologiile digitale pe care le folosesc să funcționeze impecabil. De la jocuri online și platforme de streaming multimedia până la aplicații critice de business, precum sistemele ERP sau CRM, dependența de infrastructura digitală este tot mai mare.
M247 Global și-a asumat misiunea de a oferi pieței din România această fundație de încredere pentru utilizarea tehnologiilor digitale. Printr-o abordare integrată a infrastructurii, conectivității și securității, compania sprijină organizațiile nu doar să facă față provocărilor erei digitale, ci să își accelereze dezvoltarea și să își consolideze încrederea în fiecare componentă a operațiunilor lor digitale.

De ce viitorul securității este scris în ADN-ul datelor

Securitatea trece dincolo de perimetru, către stratul criptografic central care definește încrederea în fiecare tranzacție, dispozitiv și flux de date. Pe măsură ce informatica cuantică remodelează mediul de amenințare, durabilitatea acestui „ADN” de date devine o adevărată măsură a rezilienței. **de Bogdan Marchidanu**

Companiile au petrecut ani de zile fortificând perimetrul rețelei lor de date cu firewall-uri, framework-uri SASE și controale zero trust. Însă conectivitatea se întinde acum în cloud, site-uri edge, echipe la distanță și ecosisteme partenere, creând o suprafață de atac care se mișcă mai repede decât pot acoperi instrumentele perimetrale.

Încălcările recente evidențiază această schimbare.

Peste un milion de înregistrări au fost expuse într-un incident universitar, atribuit acreditărilor furate, arătând cum apărările tradiționale perimetrale nu pot compensa asigurarea slabă a identității sau straturile criptografice fragile.
Doar 13% dintre consumatori se simt pe deplin în siguranță atunci când deschid conturi noi, iar aproape 40% spun că puterea asigurării identității modelează cât de mult au încredere într-un brand.
Companiile simt presiunea.
72% se așteaptă ca frauda generată de inteligența artificială să devină una dintre cele mai mari provocări ale lor, chiar dacă se bazează pe inteligența artificială pentru a-și consolida apărarea.
Acest lucru îi împinge pe liderii din domeniul securității să regândească fundația pe care funcționează întreaga lor stivă.

Înțelegerea „ADN-ului” datelor

Fiecare activ protejat de instrumentele perimetrale se bazează pe ceva mai fundamental: cheile criptografice care securizează datele în repaus, în mișcare și în utilizare. Aceste chei formează ADN-ul datelor. Ele stabilesc încredere între aplicații, dispozitive și tranzacții și determină dacă informațiile rămân protejate pe măsură ce se deplasează în cadrul companiei.
Fundamentul devine mai important pe măsură ce organizațiile reechilibrează sarcinile de lucru între mediile cloud și cele locale din motive de cost, latență sau securitate. Datele traversează în mod curent platforme, arhitecturi și furnizori, iar fiecare transfer se bazează pe puterea cheilor subiacente.

Când datele dvs. întâlnesc o nouă eră de calcul

Algoritmii utilizați pe scară largă astăzi – RSA și criptografia cu curbe eliptice (ECC) – au fost construiți în jurul unor probleme matematice extrem de dificil de rezolvat pentru computerele clasice. Trecerea către calculul cuantic schimbă ecuația. Algoritmii cuantici pot rezolva problemele matematice care stau la baza RSA și ECC. Sistemele actuale încă funcționează, dar fiabilitatea lor pe termen lung nu poate fi presupusă. Pe măsură ce datele devin mai mobile și distribuite, durabilitatea „ADN-ului” lor criptografic devine o prioritate, mai degrabă decât o idee ulterioară.

Pregătirea pentru Ziua Q

Discuțiile din jurul Zilei Q reflectă trecerea industriei de la standardele criptografice concepute pentru calculul clasic la standarde concepute pentru o lume cu capabilități cuantice. Adversarii cu capabilități cuantice se vor concentra pe cel mai profund strat al stivei de securitate: cheile care ancorează încrederea între aplicații, rețele și dispozitive.

Ce semnalează NIST

Proiectul de îndrumare al NIST explică tranziția. Organizațiile ar trebui să înceapă eliminarea treptată a metodelor de criptare existente acum și să continue până în 2030. Până în 2035, RSA și ECC nu vor mai fi permise, marcând trecerea completă la criptografia post-cuantică.
NIST notează, de asemenea, că activitatea de recoltare-acum-decriptare-ulterior are deja loc, ceea ce înseamnă că datele criptate capturate astăzi pot fi expuse odată ce capacitățile cuantice se maturizează.

Trecerea la securizarea stratului de date de bază

Instrumentele perimetrale rămân esențiale, dar nu pot compensa cheile criptografice slabe sau învechite. Acest lucru creează o vulnerabilitate la nivel de bază în stiva de securitate, unde stratul fundamental de sub aplicații, rețele și controale de acces devine ținta principală pentru adversarii cu capabilități cuantice. Puterea la acest nivel determină dacă datele rămân protejate, indiferent de cât de puternic devine calculul unui atacator.
Acesta este motivul pentru care strategiile de securitate se îndreaptă către nivelul central de date. Atunci când cheile sunt sigure din punct de vedere cuantic, protecția călătorește odată cu datele în fiecare mediu.
Agențiile federale au fost deja instruite să înceapă migrarea către criptografia post-cuantică, deoarece datele criptate capturate astăzi pot fi decriptate în viitor prin metode de tip „recoltare acum-decriptare-ulterioară”. Trecerea este continuă, nu o singură actualizare, necesitând criptografii recurente, modele de costuri actualizate și prioritizarea sistemelor expuse.
Sectorul privat se mișcă în paralel. Marile corporații investesc masiv în tehnologii cuantice pentru a securiza straturile criptografice fundamentale.
Se preconizează că piața de calcul cuantic va ajunge la 1 trilion de dolari până în 2035, iar primii utilizatori se așteaptă să capteze până la 90% din valoarea creată.
Securizarea stratului de date de bază devine o cerință centrală pentru organizațiile care se pregătesc pentru riscurile erei cuantice.

Cum permite Singtel QSN o fundație mai solidă

Rețeaua hibridă Quantum-Safe (QSN) de la Singtel modernizează stratul criptografic de bază al întreprinderii prin combinarea Distribuției Cheilor Cuantice (QKD) cu Criptografia Post-Cuantică (PQC) pentru a oferi protecție cuantică la nivel de infrastructură în toate mediile.
QKD securizează legături critice pentru misiune, cu lățime de bandă mare, prin schimb de chei bazat pe fizică, în timp ce PQC extinde protecția la sucursalele, locațiile la distanță, mediile cloud și operațiunile din străinătate unde hardware-ul QKD este impracticabil.
Această arhitectură hibridă depășește limitele de distanță ale QKD bazat pe fibră și permite distribuția de chei sigure cuantice în rețelele convenționale, susținută de platforma QKD a ID Quantique și de capacitățile PQC ale Palo Alto Networks.
Livrată ca modele de implementare flexibile sau servicii de securitate gestionate, QSN hibrid permite organizațiilor din domeniul sănătății, serviciilor financiare, infrastructurii critice și multinaționalelor să securizeze atât locații centrale, cât și locații distribuite, pregătindu-și stratul de date pentru viitor, fără a aștepta apariția disrupțiilor cuantice.

ELKO Romania adaugă i-PRO Co. în portofoliul său și extinde oferta de soluții avansate de securitate video

ELKO Romania a început distribuția locală a soluțiilor i-PRO Co., companie globală specializată în tehnologii profesionale de securitate și siguranță publică, cunoscută anterior sub numele de Panasonic Security. Compania își consolidează astfel poziția pe segmentul soluțiilor de securitate enterprise și pune la dispoziția integratorilor din România un portofoliu construit în jurul inteligenței artificiale la nivel edge, interoperabilității deschise și celor mai ridicate standarde de securitate cibernetică. i-PRO este recunoscută pentru abordarea sa orientată către inovație și pentru integrarea AI în întreaga gamă de produse, de la soluții pentru infrastructură critică până la sisteme entry-level optimizate pentru implementări cloud.

Printre cele mai recente dezvoltări i-PRO se numără Security Radar, o nouă categorie de soluții pentru monitorizare perimetrală outdoor, destinată mediilor cu cerințe ridicate de securitate, precum centrale energetice, centre de date, aeroporturi sau infrastructuri izolate.

Regândirea securității pentru Agentic AI

Atunci când software-ul poate gândi și acționa singur, strategiile de securitate trebuie să treacă de la aplicarea statică a politicilor la guvernanța comportamentală în timp real.

Inteligența artificială a transformat deja modul în care operează întreprinderile, dar următorul val de inovație, Agentic AI, funcționează ca agenți autonomi sau semi-autonomi care pot rula cod, pot interacționa cu API-uri, pot accesa baze de date și pot lua decizii din mers. Organizațiile trebuie să ia măsuri imediate împotriva amenințărilor de securitate care pot apărea atunci când sistemele software trec de la producerea de text pasiv la efectuarea de sarcini operaționale active.

De la AI bazată pe prompturi la agenți bazați pe acțiune

Organizațiile au început adoptarea AI la nivel de întreprindere concentrându-se pe creșterea productivității. Au încorporat LLM-uri în fluxurile de lucru pentru a scrie documente, a rezuma date și a răspunde la întrebări. Problemele de securitate s-au concentrat pe utilizarea necorespunzătoare a prompturilor, scurgerile de date și încălcările confidențialității. Deși serioase, organizațiile ar putea gestiona aceste riscuri prin protocoale de securitate standard care monitorizează datele de intrare și ieșire și efectuează gestionarea politicilor și supravegherea sistemului.
Agentic AI schimbă paradigma. Mai mult decât să răspundă la interogări, agenții acționează în numele utilizatorilor sau pentru ei înșiși. Aceștia pot declanșa fluxuri de lucru, pot interacționa cu sisteme sensibile și chiar pot lua decizii independent. Pe măsură ce autonomia crește, crește și riscul de vătămare.
Acest lucru face importantă regândirea securității de la elementele de bază.

Noul peisaj al riscurilor

Agentic AI introduce mai multe noi amenințări la adresa securității:

- **Exploatare la nivel de acțiune:** Actorii răi pot înșela agenții să efectueze operațiuni periculoase care modifică bazele de date de producție sau dezvăluie date neautorizate.
- **Atacuri de injecție de context:** Atacatorii furnizează informații false sistemelor RAG (generare augmentată de recuperare), ceea ce declanșează acțiuni periculoase ale agenților.
- **Operațiuni invizibile:** Agenții operează adesea în liniște în culise, ceea ce face dificilă observarea a ceea ce fac fără o monitorizare strictă.
- **Vulnerabilități ale protocolului:** Standarde precum Model Context Protocol (MCP) ajută agenții să se conecteze și să lucreze împreună mai ușor, dar pentru că adesea încep cu setări excesiv de deschise, pot lăsa accidental sistemele vulnerabile.

Atacuri recente evidențiază nevoia stringentă de acțiune. De exemplu, hackerii au compromis asistentul de cod Q Amazon cu o injecție de prompturi de tip wiper. În același timp, cercetătorii au dezvăluit vulnerabilități precum EchoLeak și CurXecute care exploatează ceea ce ei numesc „tripleta letală”: accesul la date interne, capacitatea de a comunica extern și expunerea la intrări nesigure. Majoritatea agenților necesită aceste trei atribute pentru a funcționa eficient, ceea ce îi face extrem de exploatabili. Aceste cazuri demonstrează modul în care sistemele de inteligență artificială agentială pot fi manipulate în moduri pe care cadrele tradiționale de securitate LLM nu au fost niciodată concepute să le gestioneze.

Construirea de bariere pentru autonomie

Provocarea constă în găsirea echilibrului potrivit între utilitatea unui agent și siguranța sa. Pentru a minimiza riscul, întreprinderile trebuie să implementeze bariere care să urmărească întregul lanț de gândire și acțiuni executate de agenți. Aceasta înseamnă monitorizarea apelurilor instrumentelor, verificarea intenției și aplicarea controalelor contextuale. Este important de menționat că strategiile de prevenție trebuie să funcționeze pe toate platformele. În loc să se concentreze pe un anumit LLM, accentul ar trebui pus pe modul în care agenții interacționează cu sistemele și gestionează datele.

Dezvoltarea unei taxonomii a agenților

Un pas important în securizarea Agentic AI este crearea unei taxonomii a agenților. Nu toți agenții sunt la fel. Clasificarea lor va ajuta la prioritizarea controalelor. Ceea ce contează cu adevărat aici este:

- **Inițierea:** Agenți inițiați de om vs. agenți autonomi;
- **Implementarea:** Mașini locale, pe platforme SaaS sau în configurații auto-găzduite;
- **Conectivitatea:** API-uri interne, endpoint-uri terțe sau servere MCP;
- **Autonomia și încrederea:** Ce nivel de acces au agenții și dacă ar trebui să îl aibă. De exemplu, un asistent de codare local într-un mediu de dezvoltare este mult mai puțin riscant decât un agent de fundal care rulează inferențe în sistemele de producție. Prin listarea agenților și a endpoint-urilor, echipele de securitate pot monitoriza activitatea, pot evalua postura și pot aplica controale precise.

Abordări deterministe vs. dinamice ale securității

Guvernanța tradițională a LLM se bazează pe controale deterministe: politicile predefinite restricționează ceea ce modelul poate și nu poate face. În schimb, AI agentică necesită o abordare dinamică. Deoarece agenții valorifică raționamentul, inferența și luarea deciziilor probabilistice, aceștia se pot comporta în moduri neașteptate. Din acest motiv, cadrele de securitate trebuie să combine bariere deterministe cu observabilitatea în timp real și controalele adaptive.
În loc să blocheze pur și simplu interogările dăunătoare, companiile trebuie să mapeze proactiv comportamentul agenților, să valideze intenția și să controleze execuția.
Acest proces proactiv… Guvernanța este fundamentală pentru gestionarea imprevizibilității sistemelor autonome.

Către un cadru de securitate bazat pe Agentic AI

Pentru a aborda aceste provocări, organizațiile au nevoie de o abordare a securității cu patru componente principale:

- **Descoperire și profilare:** Construiți un inventar al agenților, originea lor și modul în care se conectează la sisteme.
- **Gestionarea posturii agentice:** Evaluați riscurile analizând instrumentele pe care le utilizează agenții, datele pe care le pot accesa și identitățile pe care le preiau.
- **Observabilitate:** Configurați jurnale și urme detaliate ale acțiunilor agenților, astfel încât echipele de guvernanță să aibă o vizibilitate clară.
- **Controale în timpul execuției:** Implementați monitorizarea contextuală a riscurilor, prevenirea exploatărilor și controale ale acțiunilor specifice rolului.

Acest cadru recunoaște că fiecare agent trebuie evaluat în context, cu controale ajustate la autonomia, mediul și raza de explozie a acestuia.

Redefinirea riscului bazat pe AI în cadrul întreprinderilor

Ascensiunea Agentic AI reprezintă o schimbare majoră. Întreprinderile nu mai protejează doar datele. Ele gestionează fluxuri de software autonom care pot acționa singure. Acest lucru schimbă însăși noțiunea de modele de amenințare, suprafețe de atac și strategii de securitate în contextuale, adaptive și în timp real.
Spre deosebire de sistemele de învățare în cunoștință de cauză (LLM) convenționale care generează pur și simplu text ca răspuns la solicitări, natura independentă a Agentic AI redefinește atât oportunitatea, cât și riscul.
Organizațiile care acceptă această nouă responsabilitate trebuie să își regândească măsurile de securitate. Trebuie să depășească protecțiile tradiționale și să dezvolte cadre care să anticipeze, să monitorizeze și să controleze acțiunile autonome.

Funcționalități avansate de Identity and Authentication Management în SAP Business One

Pentru că atacurile cibernetice devin tot mai frecvente, iar riscurile pentru companii cresc pe măsură, SAP Business One include acum și o serie de funcționalități pentru gestiunea accesului și identității utilizatorilor (Identity and Authentication Management).

Este un aspect neglijat de multe companii, care ignoră că sistemele ERP păstrează cele mai importante și confidențiale informații– de la date financiare la datele personale ale clienților.

Pentru SAP, protecția accesului este un aspect important, iar aici intră în scenă funcționalitățile de Identity and Authentication Management (IAM) din SAP Business One. Ele fac viața utilizatorilor mai ușoară, reducând numărul de autentificări și parole pe care trebuie să le țină minte, și în același timp cresc nivelul de securitate prin mecanisme moderne care limitează riscurile de atac.

Folosești un sistem ERP? Iată care sunt cele mai mari riscuri de securitate pentru organizația ta

Potrivit datelor SAP, companie este vizată de ransomware la fiecare 11 secunde, iar 43% dintre victime sunt din categoria SMB. Printre principalele vulnerabilități și probleme de securitate cu care se confruntă utilizatorii de sisteme ERP sunt:

- **Reguli superficiale la autentificarea în sistemul ERP**: parole simple, conturi partajate sau lipsa autentificării multifactor – MFA, toate cresc riscul accesului neautorizat și al downtime-ului.
- **Lipsa actualizărilor pentru ERP** și pentru sistemele suport creează vulnerabilități critice, de la ransomware și atacuri DoS, până la acces neautorizat.
- **Standardele de securitate și de guvernanță nu sunt respectate.** Pe măsură ce ERP-ul se extinde către diverse departamente, datele sensibile devin mai variate (financiare, medicale, proprietate intelectuală), iar nerespectarea protocoalelor specifice de securitate poate duce la breșe de date și sancțiuni legale.

- Chiar dacă ERP-ul are protocoale de securitate, **exportul de date** în fișiere externe (Excel, CSV etc.) rămâne o problemă, pentru că informațiile sensibile pot fi partajate necontrolat sau stocate pe dispozitive nesecurizate.
- Presiunea de a activa rapid noi utilizatori poate duce la **gestionarea necorespunzătoare a autorizațiilor ERP** și la întârzierea dezactivării conturilor angajaților care au părăsit compania. Lipsa autentificării moderne și a fluxurilor de lucru automatizate crește riscul de acces neautorizat și expunerea datelor sensibile.

Identity and Authentication Management în SAP Business One

ERP-ul SAP Business One oferă încă din 2022 funcționalități Identity and Authentication Management (IAM), care permit utilizatorilor să se autentifice folosindu-și contul deja existent de la un identity provider (IdP). Asta înseamnă că poți folosi Single Sign-On (SSO), adică un singur cont pentru mai multe aplicații, portaluri și servicii, ceea ce îți face viața mai ușoară și reduce „password fatigue” – stresul provocat de utilizarea a prea multe parole. În plus, SSO crește securitatea, pentru că scade riscul ca parolele multiple să fie compromise, reducând astfel suprafața de atac potențială a organizațiilor care folosesc SAP Business One.

O altă veste bună e că SAP Business One se integrează deja cu mai mulți identity provideri cunoscuți:

- Active Directory Federation Services (AD FS)
- Azure Active Directory (Azure AD)
- Okta
- SAP Identity Authentication Service (IAS).

Poți conecta acești identity provideri externi folosind protocolul OpenID Connect (OIDC), care permite confirmarea identității prin autentificarea printr-un server de autorizare. Astfel, te poți loga în SAP Business One cu un singur cont (de exemplu Microsoft) și poți activa funcții suplimentare de securitate oferite de identity provider, precum autentificarea în doi pași (2FA), fără să mai creezi un alt username sau o altă parolă.

Din SLD Control Center în SAP Business One gestionezi centralizat toate conturile: „legi” utilizatorii de identity provideri, resetezi parolele, activezi sau dezactivezi conturi – toate modificările se aplică automat pentru toți utilizatorii conectați, în toate companiile din SAP Business One. Funcția „multiple company user binding” permite legarea aceluiași utilizator din IdP la mai multe companii din SAP Business One într-un singur pas, astfel încât acesta să se poată autentifica peste tot cu același cont.

Care sunt principalele beneficii de securitate

SAP Business One consolidează protecția datelor printr-o suită completă de controale de securitate – de la gestionarea strictă a accesului și criptarea datelor, până la audit trails, backup și conformitate cu standarde globale precum GDPR și ISO/IEC 27001. În plus, serviciul IAM oferă următoarele beneficii:

- **Experiență SSO (single sign-on) și eliminarea fenomenului de „password fatigue”**: o singură autentificare, acces la toate modulele/aplicațiile integrate. În loc să aibă zeci de parole de memorat pentru aplicații diferite, angajații au nevoie doar de un singur cont. Pe lângă că e mai simplu și mai comod, elimină și riscul reutilizării parolelor slabe.
- **Autentificare Multifactor (MFA) și reducerea suprafeței de atac:** datorită IdP-ului, poți folosi autentificare în doi pași (și alți factori suplimentari). Dacă parola e compromisă, fără al doilea factor atacul este blocat. Astfel probabilitatea și costul unui atac scad considerabil. În plus, utilizarea a mai puține parole înseamnă mai puține oportunități pentru atacatori.
- **Securitate sporită la log-in:** prin conectarea la un identity provider extern, autentificarea nu se mai bazează exclusiv pe conturi și parole stocate local, vulnerabile la phishing sau furt de credențiale – ci este realizată de un serviciu dedicat și securizat.
- **Protecție consolidată, oferită de IdPs:** servicii precum Azure AD, Okta sau SAP IAS aplică măsuri avansate și moderne de securitate, precum detectarea autentificărilor suspecte, blocarea automată a accesului, politici de acces condiționat, cerințe stricte pentru parole și rotația periodică a acestora, precum și MFA. Toate sunt impuse centralizat, asigurând politici de acces stricte și coerente pentru toți utilizatorii.
- **Integrare solidă cu extensii și cu ecosistemul IT existent:** compatibilitatea cu protocolul standard OpenID Connect (OIDC) înseamnă că organizațiile pot implementa autentificarea modernă fără modificări majore ale infrastructurii, păstrând intacte aplicațiile, extensiile și fluxurile IT existente. Sistemul se integrează natural în setup-ul actual al companiei, reducând costurile, timpul de implementare și riscurile tehnice.
- **Management centralizat al utilizatorilor:** prin SLD Control Center, administratorii pot gestiona toate conturile de utilizator dintr-un singur punct: activare, dezactivare, resetare de credențiale sau modificarea parametrilor de acces. Nu mai este nevoie de configurări separate pentru fiecare companie din SAP Business One, ceea ce reduce semnificativ complexitatea operațională și riscul de erori umane.

Pentru mai multe informații despre funcționalitățile de Identity and Authentication Management precum și celelalte funcții de securitate din SAP Business One, programați o discuție cu un consultant System Innovation România, la **office@sysinconsult.ro.**

De ce gestionarea identității și a accesului este esențială pentru infrastructură

Infrastructura critică din întreaga lume a fost ținta unui val continuu de atacuri cibernetice. Incidente de mare anvergură precum Colonial Pipeline, JBS Foods, sistemele de gestionare a energiei, apei și deșeurilor au determinat guvernele la nivel global să răspundă cu noi legislații și cu linii directoare consolidate privind securitatea cibernetică, menite să protejeze aceste sectoare vitale.

Amenințarea la adresa infrastructurii critice nu a fost niciodată mai urgentă. Atacurile cibernetice care odinioară vizau datele se transformă acum agresiv pentru a perturba operațiunile infrastructurii critice (IC), deoarece acestea încearcă să profite de transformarea digitală și de modernizarea activelor IC. De asemenea, accidentele și întreruperile tehnologice reale – cum ar fi cazul în care zeci de milioane de oameni din Spania și Portugalia au rămas fără curent în 2025 sau când întreruperile tehnologice au costat băncile din Marea Britanie echivalentul a 33 de zile de funcționare și milioane de dolari în potențiale plăți compensatorii – subliniază nevoia unei infrastructuri rezistente. Miza s-a schimbat. La fel și standardul de apărare.

Protejarea infrastructurii critice se bazează pe o singură întrebare simplă: Cine are acces – și de ce?

Aici intervine Managementul Identității și Accesului (IAM). IAM-ul modern nu se rezumă doar la parole și date de autentificare. Este vorba despre vizibilitate, control și responsabilitate. Este vorba despre a ne asigura că doar persoanele potrivite, cu rolurile potrivite, pot accesa sistemele potrivite – la momentul potrivit.

În mediul de reglementare actual, organizațiile de IC și serviciile esențiale sunt obligate să aibă implementate sisteme robuste de apărare IAM. Legislația din ce în ce mai nouă impune IC să demonstreze o gestionare proactivă a riscurilor, inclusiv modul în care este guvernat accesul la sisteme, să asigure modul în care sunt verificate identitățile și modul în care sunt detectate și controlate incidentele.

Cea mai mare schimbare pentru IC este convergența sistemelor de Tehnologie a Informației (IT) și Tehnologie Operațională (OT). În mod tradițional, aceste sisteme aveau o separare intenționată și distinctă a mediilor – ceea ce înseamnă că orice s-ar întâmpla în mediul IT nu putea afecta mediul OT și invers.

Menținerea acestor sisteme separate este o strategie cheie de apărare pentru protejarea activelor IC, însă odată cu modernizarea IC și noile progrese în tehnologie, cum ar fi AI, la un moment dat IT și OT converg și aici este cel mai mare risc.

Un exemplu al acestei convergențe este evidențiat în sectorul energetic. Înainte de rețelele inteligente, operatorii de energie foloseau modele simple de prezicere (de exemplu, nevoile de vară vs. nevoile de iarnă) pentru a determina prognoza sarcinii. Odată cu transformarea în rețele inteligente, operatorii de energie utilizează senzori inteligenți cuplați cu AI pentru a calcula prognoza sarcinii.

Pentru a agrava provocarea, rețelele electrice care au fost inițial proiectate pentru a distribui electricitatea din rețea către o locuință trebuie acum să primească energie de la panourile solare casnice. Aceste resurse de energie solară captează adesea energia și o reintroduc în rețea. Operatorii de astăzi trebuie să preia aceste date de la senzorii aflați în rețelele IT și, la un moment dat, să le conveargă în mediul OT de comandă și control.

Pentru a proteja aceste medii, IAM este prima linie de apărare. Acesta impune principiul privilegiilor minime, reducând riscul unei încălcări a identității. Permite monitorizarea continuă, astfel încât anomaliile pot fi detectate înainte ca acestea să devină incidente majore. Soluțiile IAM robuste și moderne acceptă, de asemenea, un răspuns rapid, oferind operatorilor posibilitatea de a bloca sistemele sau de a revoca accesul instantaneu.

Timp de decenii, RSA a asigurat cea mai mare securitate. Am ascultat și am oferit operatorilor IC autentificarea multi-factor (MFA), guvernanța și administrarea identității (IGA), autentificarea unică (SSO) și alte capabilități de securitate a identității de care au nevoie pentru a minimiza riscurile, a identifica amenințările și a menține conformitatea cu mandatele de securitate cibernetică.

În acest timp, am identificat întrebări cheie și cele mai bune practici pentru operatorii IC, inclusiv:

Știm exact cine are acces la sistemele noastre critice – și de ce? Nu poți proteja ceea ce nu poți vedea. Pentru securitatea cibernetică a IC, vizibilitatea asupra tuturor identităților utilizatorilor, a rolurilor și a nivelurilor lor de acces este esențială și adesea o cerință de reglementare.

Aplicăm principiul privilegiilor minime pentru toți utilizatorii și mediile? Conturile supraalimentate sunt o cauză principală a încălcărilor.

Putem detecta și răspunde la comportamente suspecte legate de identitate în timp real? Controalele statice sau raportarea întârziată nu sunt suficiente. IC are nevoie de monitorizare continuă și analize ale comportamentului care să identifice normalități pentru a reduce riscul.

Cum gestionăm procesele „joiner-mover-leaver" și cât de repede putem revoca accesul? Întârzierile în aprovizionarea accesului reprezintă un vector major de amenințare. Viteza și automatizarea contează.

Pentru infrastructura IC, IAM nu este opțional – este esențial din punct de vedere operațional. Atunci când organizațiile IC integrează IAM ca parte strategică a apărării lor, își consolidează pozițiile de securitate cibernetică și pot determina dacă fiecare identitate reprezintă fie un risc potențial, fie un activ securizat.

Soluțiile de securitate IT, risc si conformitate **RSA**, sunt distribuite în România de compania **SolvIT Networks**, ajutând la reușita celor mai importante organizații din lume prin rezolvarea celor mai complexe și mai sensibile provocări privind securitatea.

Sunt cheile de acces pregătite pentru utilizare în cadrul companiilor?

Utilizarea cheilor de acces crește semnificativ securitatea în comparație cu autentificările tradiționale bazate pe parolă.

Este normal ca unele soluții pentru consumatori să se extindă și în utilizarea profesională – gândiți-vă la posibilitatea de a trimite reacții emoji la e-mailuri. Dar doar pentru că Instagram îmi permite să mă conectez folosind o cheie de acces, înseamnă că și companiile ar trebui?

Chei de acces vs. parole tradiționale

Parolele tradiționale se bazează pe secrete partajate care pot fi ghicite, furate sau phishingate, ceea ce le face un punct de intrare comun pentru atacatori. Sunt adesea… reutilizate în mai multe conturi, stocate nesigur și vulnerabile la atacuri de tip „brute force" sau „credential stuffing".

Cheile de acces elimină aceste riscuri prin înlocuirea parolelor cu criptografie cu cheie public-privată. Cheia privată nu părăsește niciodată dispozitivul utilizatorului, iar autentificarea se realizează prin demonstrarea posesiei acelei chei – fără a o transmite. Această abordare face ca majoritatea vectorilor de atac comuni să fie învechiți, inclusiv phishing-ul, furtul de credențiale și reutilizarea parolelor. Pentru organizații, cheile de acces oferă un salt înainte în autentificarea securizată, reducând în același timp povara resetărilor parolelor și a tichetelor de asistență.

Printre beneficiile cheilor de acces se numără rezistența la phishing, autentificarea la fel de simplă ca utilizarea biometricelor, sutentificări asemănătoare cu modelele comune de autentificare mobilă, securitate prin potrivirea domeniilor și autentificare fără parolă pentru a proteja infrastructura critică.

Mobilitatea este un alt aspect al creării unei experiențe fluide cu chei de acces în toate mediile. O experiență mobilă fără probleme ajută la eliminarea rezistenței utilizatorilor, minimizând curba de învățare și făcând tranziția de la parole mult mai ușoară.

Soluțiile de securitate IT, risc si conformitate RSA sunt distribuite în România de compania SolvIT Networks.

Criza costurilor operaționale legate de fraudă: de ce modelul actual nu poate fi scalat

Volumul cazurilor continuă să crească. Angajările nu pot ține pasul. Timpii de investigare se întind de la zile la săptămâni. Băncile cheltuiesc mai mult, dar rezultatele nu se îmbunătățesc.

Operațiunile antifraudă au intrat în liniște într-o criză de costuri, determinată de un model operațional care se bazează prea mult pe intervenția manuală pentru a conecta semnale pe care sistemele ar trebui deja să le înțeleagă.
În acest articol, explicăm de ce următoarea generație de apărare va depinde de o automatizare explicabilă, trasabilă și construită pe adevăr verificat.

Unde se defectează modelul actual

Detectarea fraudelor a devenit prea fragmentată pentru a fi gestionată manual. Fiecare canal, produs și furnizor nou adaugă mai multe alerte, tablouri de bord și transferuri. Analiștii își petrec cea mai mare parte a timpului reconciliind dovezile, mai degrabă decât luând decizii.

Fisurile apar în trei locuri:

- **Volum:** alertele cresc mai repede decât capacitatea analiștilor. Chiar și cele mai bune echipe nu pot ține pasul atunci când fiecare nou tip de plată sau campanie adaugă mai multe semnale de revizuit.
- **Variabilitate:** modelele de atac evoluează constant, dar cunoștințele instituționale se află în mintea analiștilor experimentați. Când aceștia trec la altă versiune, la fel se întâmplă și cu acele cunoștințe.
- **Vizibilitate:** sistemele încă evaluează câte un eveniment pe rând; un utilizator, un dispozitiv, un canal. Scorurile de risc trec între sisteme ca o prescurtare, detașate de dovezile care le-au creat.

Rezultatul este un cost mai mare, un răspuns mai lent și o oboseală crescândă. Echipele muncesc mai mult, dar văd mai puțin.

De ce automatizarea trebuie să meargă mai departe

Automatizarea a sunat întotdeauna atrăgătoare în teorie, dar dificilă în practică. Multe echipe au încercat-o și s-au retras. Modelele de tip „cutie neagră” iau decizii pe care nimeni nu le poate justifica, iar motoarele de reguli prea încrezătoare pot bloca clienții reali. Așadar, „automatizarea” a devenit sinonimă cu „scurtături pentru fluxul de lucru”, nu o schimbare reală a capacității.
Acest lucru se schimbă. Atunci când deciziile sunt construite pe date deterministe, explicabile – cum ar fi semnalele produse prin intermediul Recunoașterii Modelelor de Atacare (APR) a Cleafy – automatizarea devine sigură. Fiecare acțiune și decizie poartă dovezi în spate. Automatizarea nu scoate oamenii din proces; îi pune la conducerea acestuia.

De la om în buclă la om în buclă

Analiștii de fraude nu ar trebui să șteargă cozile; ar trebui să supravegheze sisteme care pot acționa pe baza unor semnale clare și de încredere.
Noul model de operare menține controlul asupra oamenilor, eliberându-i în același timp de sarcini repetitive. Sistemele gestionează ceea ce este previzibil:

- **Colectarea dovezilor** privind dispozitivele, rețeaua, comportamentul și tranzacțiile într-o singură vizualizare a cazului.
- **Executarea acțiunilor pre-aprobate** atunci când sunt îndeplinite condiții de încredere ridicată, cum ar fi blocarea unei plăți sau forțarea autentificării intensificate.
- **Transmiterea feedback-ului analiștilor** direct înapoi în liniile de bază pentru a îmbunătăți acuratețea detectării.

Oamenii rămân la curent; revizuirea excepțiilor, validarea cazurilor limită și menținerea guvernanței.

Recunoașterea tiparelor de atac: Fundamentul unei automatizări sigure

Recunoașterea tiparelor de atac (RPA) oferă automatizării ceva ce i-a lipsit întotdeauna: adevăr verificat. Reconstruiește modul în care se desfășoară un atac, legând semnale între dispozitive, sesiuni și canale pentru a dezvălui ce s-a întâmplat de fapt.
Deoarece fiecare detectare este cauzală, nu probabilistică, răspunsurile automate pot acționa cu încredere.
Cu această fundație stabilită, băncile pot progresa natural prin etapele de maturitate:

- **Îmbogățire automată:** datele sunt colectate și corelate automat.
- **Acțiuni bazate pe încredere:** semnalele de încredere declanșează răspunsuri sigure, predefinite.
- **Feedback în buclă închisă:** rezultatele analiștilor rafinează continuu detectarea.

Fiecare pas reduce munca manuală și îmbunătățește precizia, fără a pierde supravegherea.

Guvernanța ca principiu de proiectare

Automatizarea responsabilă depinde de transparență. Fiecare decizie automată ar trebui să poată fi urmărită până la dovezile, pragurile și politicile sale. Analiștii trebuie să vadă de ce s-a întâmplat ceva, auditorii trebuie să verifice acel lucru, iar clienții merită să știe că s-a întâmplat dintr-un motiv legitim.

Redefinirea succesului operațional

Pe măsură ce automatizarea preia o parte mai mare din volumul de muncă, modul în care este măsurată performanța se va schimba. Succesul va fi judecat în funcție de timpul de izolare, precizie și fiabilitatea automatizării, nu de numărul de cazuri închise.
Și munca se va schimba. Analiștii vor petrece mai mult timp validând deciziile decât colectând date. Vor apărea noi roluri în ceea ce privește ingineria automatizării, calitatea semnalului și guvernanța.
Centrul de operațiuni frauduloase devine un strat de orchestrare, nu o linie de procesare.

Scalarea încrederii, nu a numărului de angajați

Operațiunile de fraudă de astăzi seamănă cu operațiunile de securitate cibernetică de acum un deceniu: Se concentrează pe triajul manual și pe integrarea redusă. Aceeași transformare care a remodelat Centrul de Operațiuni de Securitate (SOC) se extinde acum și la fraudă: o trecere treptată de la operațiuni manuale la semi-automatizate, apoi către operațiuni autonome.
Recunoașterea tiparelor de atac se află în centrul acestei schimbări. Aceasta oferă date verificate, explicabile, singurul tip care poate susține automatizarea sigură și auditabilă.
Întrebarea nu este câți analiști să angajăm, ci cât de mult din procesul decizional poate fi automatizat în mod responsabil. Instituțiile care pot răspunde la această întrebare cu încredere se vor scala mai rapid și vor funcționa mai eficient, nu pentru că au eliminat oameni din buclă, ci pentru că le-au oferit sisteme în care merită să aibă încredere.
Soluțiile Cleafy sunt distribuite în România de compania SolvIT Networks.

Exclusive Networks obține statutul de Engage Preferred Services Partner Fortinet pentru țările din regiunea CEE și Orientul Mijlociu

Exclusive Networks, specialist global de încredere în soluții de cybersecurity, a fost desemnat Engage Preferred Services Partner (EPSP) în cadrul Fortinet Engage Partner Program pentru țările din Europa Centrala și de Est (CEE) și Orientul Mijlociu.

În calitate de Engage Preferred Services Partner, Exclusive Networks primește acces la training specializat și asistență directă din partea experților Fortinet, pentru a dezvolta noi competențe în furnizarea de servicii și suport avansat de securitate pentru clienți, inclusiv pentru infrastructuri hibride în continuă schimbare și extindere.

De asemenea, Exclusive Networks poate colabora direct cu experții Fortinet Professional Support în cadrul implementărilor, pentru a aplica cele mai bune practici Fortinet, crescând astfel expertiza echipei și vizibilitatea proiectelor, în timp ce dezvoltă un portofoliu de servicii mai robust și competitiv.

Cardurile biometrice: noul standard în plăți – securitate redefinită, experiență premium și avantaj competitiv

Industria serviciilor financiare traversează una dintre cele mai accelerate transformări din istoria sa. Digitalizarea, presiunea concurențială și creșterea așteptărilor clienților determină băncile să regândească nu doar produsele, ci și experiențele pe care le oferă.

În acest context, cardurile biometrice nu mai sunt doar o inovație tehnologică, ci devin un nou standard — o combinație între securitate avansată, simplitate în utilizare și valoare comercială demonstrată.
Un exemplu relevant în această direcție este N-BioCard, o soluție de plată **AUSTRIACARD HOLDINGS** de nouă generație care redefinește modul în care securitatea și confortul coexistă în tranzacțiile financiare.

N-BioCard: următoarea generație de plăți

N-BioCard (unde „N" vine de la Next Generation) simbolizează evoluția naturală a cardurilor de plată, **AUSTRIACARD HOLDINGS** integrând tehnologia biometrică direct în experiența utilizatorului.
Este un card cu interfață dual (contact și contactless) care adaugă un nivel suplimentar de securitate prin autentificare biometrică. În locul codului PIN, utilizatorul aprobă tranzacțiile prin simpla atingere a senzorului de amprentă integrat în card.
Această abordare stabilește un nou standard în industrie, demonstrând cum tehnologia poate elimina fricțiunile fără a compromite securitatea — dimpotrivă, întărind-o.

Piața confirmă: cerere reală și disponibilitate de plată

Interesul pentru astfel de soluții este susținut de date clare din piață:

- 50% dintre utilizatorii din Franța sunt dispuși să plătească suplimentar pentru un card biometric
- 46% în Germania, 42% în UK și Australia, 37% în Canada
- Prima acceptată variază între 8,7$ și 10,7$ per card

Mai mult, până la 62% dintre utilizatori ar lua în considerare schimbarea băncii pentru a beneficia de această tehnologie din oferta de servicii **AUSTRIACARD HOLDINGS**. Aceste cifre confirmă că biometria nu este doar o inovație, ci un catalizator real de creștere comercială.

Cum funcționează: simplu pentru utilizator, sofisticat în realitate

Experiența de plată rămâne familiară: cardul este apropiat de terminalul POS, la fel ca un card contactless obișnuit.
Diferența esențială constă în autentificare:

- utilizatorul plasează degetul pe senzorul de amprentă
- tranzacția este aprobată instant
- toate tranzacțiile, indiferent de valoare, sunt securizate biometric

În situații excepționale, codul PIN poate fi utilizat ca alternativă.

Rezultatul este o experiență:

- mai rapidă (< 1 secundă per tranzacție)
- mai simplă
- mai sigură

Performanță și standarde: pregătit pentru scalare globală

Cardurile biometrice respectă standarde stricte de performanță:

- < 1 secundă – durată medie tranzacție
- < 0,01% FAR – rată maximă de acceptare eronată
- < 3% FRR – rată maximă de respingere eronată

Sunt conforme cu standardele globale (EMV, ISO7816, ISO14443), ceea ce le face complet interoperabile și pregătite pentru adopție la scară largă.

Securitate redefinită: datele nu părăsesc cardul

Unul dintre cele mai puternice avantaje ale N-BioCard este arhitectura de securitate oferită de **AUSTRIACARD HOLDINGS**.
Datele biometrice sunt capturate, procesate și stocate exclusiv pe card, nu sunt transmise în afara acestuia și sunt protejate în Secure Element. Această abordare elimină riscurile de interceptare sau furt de date, respectă cele mai stricte cerințe de protecție (GDPR) și reduce drastic fraudele.
În plus, chiar și în caz de pierdere sau furt cardul nu poate fi utilizat fără amprentă, inclusiv plățile contactless de valoare mică devin imposibile.

Beneficii directe pentru utilizator

N-BioCard oferă o experiență superioară prin:

- Convenință – fără PIN, fără limite pentru contactless
- Rapiditate – plăți în mai puțin de o secundă
- Siguranță – autentificare biometrică obligatorie
- Igienă – eliminarea necesității de a atinge tastatura POS
- Control – doar utilizatorul poate autoriza tranzacțiile

Această combinație transformă cardul dintr-un simplu instrument de plată într-un element de încredere și confort zilnic.

Înrolarea: rapidă, flexibilă, sigură

Pentru a utiliza cardul, utilizatorul trebuie să își înregistreze amprenta — un proces simplu și rapid.
Opțiuni disponibile prin aplicația mobilă (NFC) sau prin dispozitiv dedicat (sleeve), utilizabil acasă sau în sucursală.

Procesul durează doar câteva secunde, iar:

- se pot înrola 1–2 degete
- datele sunt stocate exclusiv pe card
- nu există expunere externă a informațiilor

Această flexibilitate facilitează adopția și reduce barierele de utilizare.

Tehnologie avansată: eficiență și fiabilitate

În spatele experienței simple se află tehnologia Biometric Coil on Module (BCoM), care:

- integrează senzorul biometric și elementul securizat
- reduce complexitatea producției
- elimină conexiunile hardware suplimentare
- crește durabilitatea cardului

Rezultatul este o soluție scalabilă, robustă și optimizată pentru implementare industrială.

Valoare strategică pentru bănci
- Adoptarea cardurilor biometrice generează valoare pe mai multe planuri:

Diferențiere competitive - Poziționarea AUSTRIACARD HOLDINGS ca lider în inovație într-o piață saturată.

Creștere de venituri - Disponibilitatea clienților de a plăti între 8,7$ și 10,7$ deschide oportunități premium.

Reducerea fraudelor - Autentificarea biometrică limitează utilizarea neautorizată.

Experiență îmbunătățită - Plăți rapide și fără fricțiuni cresc satisfacția și loialitatea.

Valori extinse: impact operațional și strategic.

Pe lângă beneficiile evidente, cardurile biometrice aduc și avantaje suplimentare:

- eficiență operațională – mai puține interacțiuni legate de PIN
- engagement digital crescut – integrare cu aplicațiile mobile
- calitate superioară a datelor – identificare precisă a utilizatorului
- platformă pentru viitor – bază pentru identitate digitală și servicii extinse

De la inovație la standard

Cardurile biometrice, și în special soluțiile de plată **AUSTRIACARD HOLDINGS** precum N-BioCard, marchează trecerea de la securitatea bazată pe cunoaștere (PIN) la securitatea bazată pe identitate reală.

Cifrele sunt concludente:

- până la 62% dintre clienți ar schimba banca
- aproximativ 50% sunt dispuși să plătească în plus
- tranzacțiile se realizează în sub 1 secundă

Pentru bănci, aceasta nu mai este doar o oportunitate de inovare, ci o decizie strategică.
Cei care vor adopta devreme nu doar că vor răspunde unei cereri existente, ci vor defini așteptările viitoare ale pieței.

Operațiuni de securitate bazate pe analiză unificată și control operațional integrat

Pe măsură ce infrastructurile IT devin tot mai distribuite și complexe, organizațiile se confruntă cu provocări majore în administrarea securității, a identităților digitale și a operațiunilor IT. Pentru IT Manageri și CISO, vizibilitatea completă asupra infrastructurii și capacitatea de a răspunde rapid la incidente sunt esențiale pentru menținerea continuității operaționale și pentru protejarea datelor critice.

Platforma ManageEngine oferă un ecosistem integrat de soluții care acoperă principalele domenii ale managementului IT și securității cibernetice: administrarea identităților și accesului, managementul endpoint-urilor, monitorizarea infrastructurii și analiza evenimentelor de securitate. Prin consolidarea acestor funcționalități într-o arhitectură unificată, organizațiile pot obține control operațional, trasabilitate și eficiență în procesele IT.

Managementul identităților și controlul accesului privilegiat

Administrarea identităților reprezintă una dintre componentele critice ale securității IT moderne. Soluțiile ManageEngine permit controlul granular al accesului utilizatorilor, monitorizarea sesiunilor privilegiate și implementarea unor mecanisme avansate de audit și conformitate. Platforme precum ADManager Plus, ADSelfService Plus și PAM360 oferă capabilități extinse pentru gestionarea ciclului de viață al identităților digitale, implementarea autentificării multifactor și controlul accesului privilegiat la resurse critice.

Management unificat al endpoint-urilor

Endpoint Central consolidează administrarea dispozitivelor prin patch management automatizat, evaluarea și remedierea vulnerabilităților, control al configurațiilor și inventariere hardware/software în timp real. Platforma include capabilități integrate de protecție împotriva ransomware-ului și funcționalități de Data Loss Prevention (DLP), contribuind la prevenirea accesului neautorizat la date sensibile și la limitarea riscurilor asociate atacurilor cibernetice. Integrarea cu mecanisme de analiză de securitate permite identificarea și remedierea vulnerabilităților înainte de exploatare, contribuind la reducerea timpului mediu de remediere (MTTR).

Analiza evenimentelor de securitate și detecția amenințărilor

Pentru a face față amenințărilor cibernetice din ce în ce mai sofisticate, organizațiile au nevoie de mecanisme avansate de colectare și analiză a jurnalelor de securitate. ManageEngine Log360 oferă funcționalități de tip SIEM (Security Information and Event Management), permițând corelarea evenimentelor provenite din multiple sisteme, detectarea comportamentelor anormale și investigarea incidentelor de securitate. Prin analiza comportamentală a utilizatorilor și monitorizarea activităților critice, platforma sprijină echipele de securitate în identificarea rapidă a potențialelor amenințări.

Soluție unificată de monitorizare și configurare a infrastructurii IT

Platforma oferă o soluție unificată de monitorizare și configurare a tuturor elementelor din infrastructura IT. Prin intermediul unei singure console pot fi administrate și supravegheate echipamentele de rețea și sistemele critice, precum switch-uri, routere, servere fizice, mașini virtuale, aplicații, sisteme de stocare și firewall-uri. Platforma permite monitorizarea continuă a performanței, detectarea rapidă a incidentelor, gestionarea configurațiilor și menținerea unei vizibilități complete asupra întregii infrastructuri IT.
Adoptarea unei platforme integrate de management IT și securitate permite organizațiilor să își consolideze postura de securitate și să optimizeze procesele operaționale. Prin automatizare, corelarea datelor și vizibilitate centralizată, echipele IT pot identifica mai rapid incidentele, pot reduce complexitatea operațională și

pot îmbunătăți capacitatea de răspuns la amenințările cibernetice.
Romsym Data, distribuitor ManageEngine în România, oferă suport tehnic specializat, sesiuni demonstrative și asistență în implementarea soluțiilor. Echipa tehnică poate sprijini organizațiile în evaluarea arhitecturii IT existente și în integrarea soluțiilor ManageEngine într-o strategie coerentă de management operațional și securitate.

Piața smart home din România accelerează, în timp ce rămâne în faza de early adoption

Parte din ecosistemul de securitate inteligentă Yale, Linus® L2 Lite este o încuietoare inteligentă retrofit, proiectată pentru instalare DIY, fără modificări asupra ușii existente — o caracteristică importantă atât pentru proprietari, cât și pentru chiriași. Spre deosebire de Linus® L2, modelul Lite nu include Wi-Fi integrat, acesta putând fi adăugat opțional ulterior printr-un bridge Yale separat, în funcție de nevoile utilizatorului. Astfel, fiecare utilizator își poate configura soluția de securitate în funcție de funcționalitățile dorite. În același timp, securitatea rămâne o prioritate, datele fiind protejate prin criptare avansată, iar accesul în aplicație este securizat prin autentificare în doi pași (2FA).
Linus® L2 Lite integrează funcții smart esențiale pentru utilizarea de zi cu zi, precum KeySense™, care permite închiderea sau deschiderea facilă și rapidă a ușii din interior doar prin apăsarea unui buton, cât și programarea închiderii sau deschiderii ușii, fără a fi nevoie de chei sau de telefon.
De asemenea, funcția de deblocare automată permite utilizatorilor acces hands-free (cu ajutorul tehnologiei ConnectX Wi-Fi Bridge). Cu ajutorul aplicației mobile, utilizatorii pot gestiona accesul în locuință de la distanță, pot acorda chei digitale membrilor familiei sau a vizitatorilor de încredere și pot primi notificări în timp real despre activitatea de acasă. Compatibilitatea Matter over Thread oferă integrare extinsă în ecosisteme precum Apple Home, Google Home, Alexa și Samsung SmartThings, fără limitarea la un singur sistem.
Modelul Lite se adresează segmentului urban 25–45 de ani, familiilor active, utilizatorilor care partajează frecvent accesul cu terțe persoane (rude, babysitter, personal auxiliar), dar și antreprenorilor din zona închirierilor pe termen scurt sau aparthotelurilor, unde gestionarea digitală a accesului reduce costurile și eficientizează operarea.
Prin poziționarea sa accesibilă, Linus® L2 Lite contribuie la democratizarea accesului la tehnologia smart în România, într-un context economic caracterizat de creștere prudentă și decizii de achiziție atent analizate.

Ce presupune cu adevărat construirea unui Security Operations Center (SOC)

Pentru majoritatea organizațiilor care intenționează să construiască un (SOC), întrebarea nu mai este dacă merită investiția, ci ce este necesar pentru a-l face operațional.

Deși multe companii estimează că pot lansa un SOC în decurs de un an și că își pot menține bugetele sub control, experiențele din practică diferă semnificativ, fiind influențate de variații în ceea ce privește dimensiunea, nivelul de maturitate și prioritățile strategice.

Numeroase organizații intenționează să construiască un Security Operations Center (SOC) pentru a-și consolida postura generală de securitate. Aceste concluzii arată că, dincolo de planuri aparent similare, companiile se confruntă cu realități foarte diferite atunci când transformă conceptele de SOC în capabilități operaționale.

Potrivit unui studiu Kaspersky, bugetul mediu planificat la nivel global pentru înființarea unui SOC este de aproximativ 2 milioane USD. Totuși, această cifră ascunde variații semnificative la nivelul așteptărilor. Peste jumătate dintre organizații (55%) planifică bugete sub 1 milion USD, în timp ce aproximativ un sfert (24%) sunt pregătite să investească peste 2,5 milioane USD. Nivelul cheltuielilor planificate este strâns corelat cu dimensiunea companiei și cu gradul de externalizare a SOC-ului: companiile mai mici tind să se concentreze pe investiții mai modeste, în timp ce organizațiile mari sunt mult mai predispuse să planifice proiecte SOC costisitoare, reflectând o acoperire mai amplă a infrastructurii și cerințe operaționale mai ridicate.

Diferențe notabile la nivel de stat au ieșit la iveală, organizații din țări precum Vietnam și China fiind dispuse să investească peste media globală în dezvoltarea SOC-urilor, în timp ce multe alte națiuni nu intenționează să depășească pragul de 1 milion USD. Creșterea bugetelor alocate SOC-urilor poate fi explicată prin accentul strategic pus de aceste țări pe suveranitatea digitală și pe dezvoltarea de soluții de securitate interne în cadrul infrastructurilor naționale.

În ceea ce privește termenele, așteptările sunt relativ concentrate, însă există și excepții notabile. Două treimi dintre companii (66%) estimează că își vor construi un SOC în 6–12 luni, în timp ce peste un sfert (26%) anticipează termene mai îndelungate, de până la doi ani.

Deși operează în medii mai complexe, companiile mari sunt mai predispuse decât cele de dimensiune medie să prioritizeze implementarea rapidă a SOC-ului. În practică, acest lucru înseamnă adesea lansarea inițială a SOC-ului pentru segmentele critice, urmată de extinderea treptată a acoperirii la nivelul întregii infrastructuri.

Cercetarea evidențiază, de asemenea, faptul că dezvoltarea unui SOC implică o gamă largă de provocări, nu doar un singur obstacol dominant. Costurile inițiale ridicate au fost menționate cel mai frecvent, fiind indicate de o treime dintre respondenți (33%). În același timp, multe organizații întâmpină dificultăți în evaluarea eficienței (28%), proces care presupune analizarea unei game variate de indicatori de performanță (KPI), de la metrici financiare precum Return on Investment (ROI) și indicatori operaționali precum Mean Time to Detect (MTTD) și Mean Time to Response (MTTR), până la obiective strategice, cum ar fi asigurarea conformității cu standardele din industrie.

În plus, companiile se confruntă cu gestionarea unor soluții de securitate complexe (27%) și cu integrarea mai multor sisteme și tehnologii (26%).

Un sfert dintre organizații indică, de asemenea, lipsa expertizei, atât în rândul angajaților existenți (25%), cât și pe piața externă a muncii (25%), subliniind faptul că resursele umane rămân o constrângere critică, alături de tehnologie și bugete.

Pentru a construi și opera cu succes un SOC fiabil este recomandat:

- Implicați servicii complete de consultanță în etapa inițială de implementare sau pentru optimizarea operațiunilor existente de securitate.
- Îmbunătățiți performanța securității cu o soluție care analizează și stochează datele de log din întreaga infrastructură IT, oferind contextualizare și informații relevante de tip threat intelligence.
- Protejați-vă compania împotriva unei game largi de amenințări cu soluții care oferă protecție în timp real, vizibilitate asupra amenințărilor și capabilități de investigare și răspuns bazate pe AI, prin tehnologii EDR și XDR, pentru organizații de orice dimensiune și din orice industrie.
- Oferiți echipei de securitate cibernetică o vizibilitate aprofundată asupra amenințărilor care vizează organizația dumneavoastră.
- Dacă nu dispuneți de personal dedicat pentru îndeplinirea funcțiilor esențiale ale unui SOC, utilizați servicii care acoperă întregul ciclu de gestionare a incidentelor — de la identificarea amenințărilor până la protecție continuă și remediere — ajutând la prevenirea atacurilor sofisticate, investigarea incidentelor și suplimentarea expertizei interne.

Platformele integrate cresc nivelul de securitate

Utilizarea unei platforme unitare, în locul mai multor soluții individuale oferă protecție împotriva unei game largi de amenințări cibernetice, de la malware și ransomware la phishing, atacuri DDoS sau APT, dar și o binevenită simplificare operațională. Aceasta asigură un sistem de apărare eficient pentru datele sensibile și proprietatea intelectuală, permițând conformitatea cu standarde precum NIS2 sau DORA. În plus, prin centralizarea și integrarea instrumentelor de securitate, platformele oferă vizibilitate completă asupra posturii de securitate, simplifică gestionarea și permit identificarea rapidă a vulnerabilităților.

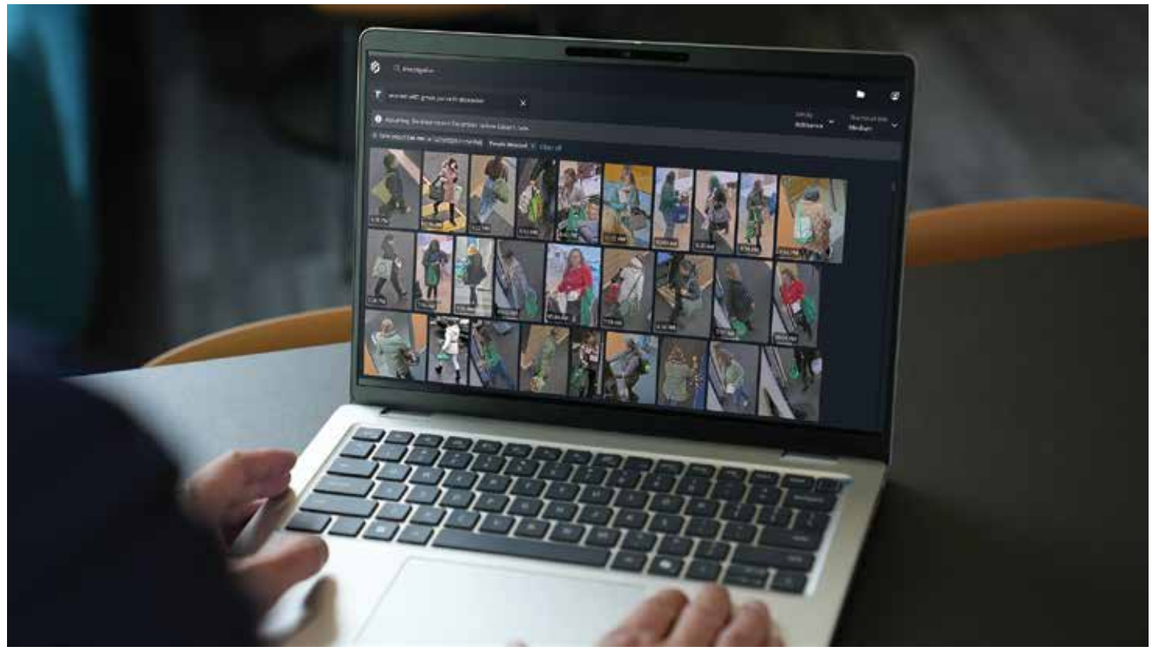
Cynet oferă o protecție completă prin detectarea și blocarea automată a amenințărilor avansate, eliminând complexitatea și suprapunerea instrumentelor de securitate, și asigurând răspuns rapid în doar câteva secunde. Platforma protejează întregul mediu IT al organizației, de la dispozitive terminale la cloud prin funcții și componente precum:

- Integrări și flexibilitate. Cynet se conectează cu instrumentele IT și de securitate existente anterior în organizații (ex. SIEM sau SOAR), folosind sute de API-uri și peste 80 de integrări built-in pentru a colecta date (50+ surse de date) și a coordona răspunsul în întregul ecosistem IT și de securitate, oferind vizibilitate completă și control centralizat.
- CyAI este motorul AI al platformei Cynet, care învață din milioane de exemple reale și se adaptează constant, previne, detectează, investighează și răspunde la amenințări în timp real. CyAI include capabilități User and Entity Behavior Analytics (UEBA) pentru monitorizarea comportamentului dispozitivelor terminale, analiza comportamentală SIEM (Security Information and Event Management), și un motor de corelare AI pentru triere rapidă a semnalelor. Platforma detectează autonom 97% dintre amenințări, remediază automat 90% dintre acestea, reduce alertele fals pozitive sub 0,9% și izolează și blochează amenințările în mai puțin de o secundă, potrivit datelor Cynet. Totodată, detectează și blochează malware-ul înainte de execuție, în timp real.

- Cynet SOAR (Security Orchestration, Automation, and Response). Cynet reduce timpul de răspuns de la câteva ore la secunde. Folosind playbook-uri predefinite, platforma izolează automat sistemele compromise, poate opri traficul periculos, eliminând amenințările, unificând complet detectarea, investigarea și răspunsul în întreg mediul IT. Integrată nativ în platformă, soluția SOAR elimină nevoia de instrumente terțe costisitoare și asigură un răspuns de până la 50 de ori mai rapid decât în fluxurile manuale.
- Cynet XDR (Extended Detection & Response) centralizează datele de securitate din toate mediile și reduce complexitatea managementului prin automatizarea sarcinilor repetitive. Platforma colectează și analizează în timp real date critice de la dispozitive terminale, sisteme de management al identității și accesului (IAM), dispozitive de rețea și medii cloud, detectând modele complexe de atac și amenințări potențiale. Prin monitorizare continuă și alerte în timp real, Cynet XDR elimină punctele oarbe și permite echipelor SOC să reacționeze rapid. Cynet reprezintă o componentă importantă în cadrul serviciilor de externalizare de SOC furnizate prin centrul Computer Emergency Response Team al Safetech Innovations.

Capabilități enterprise în Security Center SaaS pentru investigații mai rapide și mai eficiente

Noile capabilități de investigație în Genetec Security Center SaaS reduc timpul necesar analizelor de la ore la minute, inclusiv în medii complexe, multi-site și multi-vendor.



Incidentele de securitate se desfășoară adesea la nivelul mai multor clădiri, campusuri sau regiuni geografice și se bazează pe imagini și date provenite de la zeci sau chiar mii de camere și dispozitive aparținând unor furnizori diferiți. În același timp, operatorii de securitate pornesc de regulă cu informații limitate sau incomplete. Sistemele închise, concepute pentru medii cu un singur furnizor, alături de natura fragmentată a instrumentelor tradiționale de investigație, îngreunează acțiunea rapidă a echipelor pe măsură ce investigațiile se extind între locații, sisteme și branduri de camere. Pe baza capabilităților de căutare inteligentă introduse anul trecut, Genetec oferă acum o experiență de investigație care permite echipelor să lucreze mai eficient în medii complexe. Prin menținerea conexiunii dintre probe, decizii și informații contextuale, de la primul raport de incident până la închiderea cazului, investigatorii evită reluarea căutărilor sau duplicarea activităților pe măsură ce investigațiile evoluează.

Identificarea rapidă a probelor și construirea mai eficientă a cazurilor conectate

Investigațiile din Security Center SaaS sunt concepute în funcție de modul real de lucru al operatorilor și investigatorilor. Un caz poate începe cu un raport succint de incident și informații limitate, precum o oră aproximativă sau o descriere parțială a vestimentației suspectului.
Prin utilizarea căutării avansate în limbaj natural, bazată pe inteligență artificială, persoanele avizate pot transforma descrieri uzuale în interogări aplicabile asupra fluxurilor video din multiple locații și de la camere aparținând unor furnizori diferiți.
Ulterior, rezultatele pot fi restrânse pe baza unor indicii contextuale, precum locația, activitatea din proximitate sau evenimentele petrecute înainte și după incident.
Pe măsură ce sunt identificate înregistrările relevante, investigatorii își pot valida și rafina concluziile prin intermediul unei previzualizări pe timeline. Aceasta le permite să parcurgă rapid materialul video, să confirme momentele-cheie și să restrângă intervalele de timp, fără a fi nevoie să încarce sau să revizuiască integral înregistrările.
Ulterior, agentii pot urmări persoane, vehicule și obiecte în diferite scene, pot vizualiza deplasarea acestora prin analiza traiectoriei și pot înțelege modul în care s-au desfășurat evenimentele în timp, fără a analiza ore întregi de material video.
Pe măsură ce investigația avansează, probele pot fi consolidate într-un dosar, permițând construirea unei imagini complete a incidentului. Secvențele video, capturile de ecran și materialele asociate pot fi organizate automat în ordine cronologică, îmbogățite cu informații contextuale și etichete și prezentate sub forma unui storyboard coerent, care evidențiază conexiunile dintre evenimente.
Ca parte a experienței de investigație în continuă evoluție din Security Center SaaS, capabilitățile asistate de AI — inclusiv generarea automată de rezumate ale clipurilor video — îi ajută pe investigatori să documenteze rapid conținutul înregistrat, facilitând finalizarea concluziilor, partajarea rezultatelor cu părțile interesate și închiderea eficientă a cazurilor.

O experiență unificată de investigație, concepută pentru implementări de securitate la scară largă

Noile capabilități de investigație reunesc instrumente precum căutarea în limbaj natural, detecția de similaritate, identificarea intrărilor și ieșirilor, analiza contextuală, căutarea vizuală a traiectoriilor, precum și gestionarea cazurilor și a probelor, într-o experiență unificată de investigație.
Profesioniștii din domeniul securității pot trece fără întreruperi de la monitorizarea live la o investigație activă, pot colecta și analiza probe și pot partaja în mod securizat concluzii validate cu părțile interesate interne și externe, toate dintr-o singură interfață.
Începând cu luna februarie 2026, noile capabilități de investigație vor fi disponibile pentru utilizatorii Security Center SaaS, urmând ca funcționalități suplimentare să fie introduse progresiv. Acestea vor ajuta organizațiile să reducă timpul de investigație de la ore la minute și să revină mai rapid la operațiunile zilnice după soluționarea incidentelor, menținând în același timp transparența și controlul operatorilor asupra modului în care sunt formulate concluziile.
Pentru a afla mai multe despre capabilitățile de investigație din Security Center SaaS, vizitați:
https://resources.genetec.com/beyond-the-lens/find-evidence-faster-with-our-ai-based-investigation-experience.

Aproape 90% dintre organizații preferă modele SOC externalizate sau hibride

Pe măsură ce amenințările cibernetice devin tot mai sofisticate, organizațiile își regândesc modul în care își construiesc și operează Centrele de Operațiuni de Securitate. Rezultatele unei cercetării Kaspersky arată că 64% dintre companii intenționează să externalizeze o parte din SOC, combinând capabilitățile interne cu expertiza externă.
Între timp, peste un sfert dintre respondenți (26%) sunt pregătiți să implementeze complet un model SOC-as-a-Service (SOCaaS). În contrast, doar 9% plănuiesc să construiască SOC-ul integral intern, ceea ce evidențiază dificultățile tot mai mari de a menține monitorizarea permanentă și de a atrage specialiști calificați.
Externalizarea SOC permite organizațiilor să delege anumite funcții ale SOC sau chiar întregul ciclu operațional unui furnizor extern de încredere. Această abordare poate include o varietate de servicii:
• Proiectarea și arhitectura SOC
• Implementarea și mentenanța tehnologiilor SOC
• Monitorizare și analiză realizate de analiști de securitate externi
• Servicii de consultanță și training
• Furnizarea completă de SOCaaS, în care furnizorul gestionează detecția, investigarea și răspunsul la incidente 24/7.
Majoritatea companiilor preferă să păstreze intern sarcinile strategice, valorificând în același timp echipe externe și tehnologii avansate pentru activități operaționale și tehnice complexe. Printre organizațiile care planifică externalizarea funcțiilor SOC, cele mai frecvent delegate sarcini către terți au inclus instalarea și implementarea soluțiilor (55%), dezvoltarea și furnizarea soluțiilor (53%) și proiectarea SOC (47%).
Atunci când colaborează cu specialiști SOC externi, companiile au arătat, de asemenea, o preferință clară pentru suplimentarea unor roluri specifice, analiștii de prim nivel (61%) și de nivel secund (52%) fiind cei mai solicitați dintre specialiștii externi.
Aceste cifre ilustrează faptul că organizațiile se concentrează mai mult pe sarcini de securitate de primă linie și intermediare, precum monitorizarea și răspunsul la amenințări.
Principalul motiv pentru externalizarea SOC este necesitatea protecției 24/7 (55%) – o cerință operațională pe care multe echipe interne nu o pot susține singure.
Un alt beneficiu important menționat este reducerea volumului de muncă al specialiștilor interni în securitate IT (47%), permițând echipelor să se concentreze pe sarcini strategice.
În plus, accesul la soluții și tehnologii avansate (42%) și suportul extern pentru asigurarea conformității cu cerințele și standardele de reglementare (41%) stimulează, de asemenea, decizia de externalizare, subliniind valoarea expertizei specializate și a instrumentelor de ultimă generație, precum XDR, MDR, MXDR și altele
Optimizarea bugetului este importantă pentru doar 37% dintre companii – ceea ce indică faptul că, în principal, valoarea externalizării vine din îmbunătățirea protecției, nu doar din reducerea costurilor.

Inteligența Artificială: între accelerarea inovației și responsabilitatea securității


Mugur Pantaia,
Managing Director HP Inc. România

În ultimii ani, inteligența artificială a ajuns să redefinească modul în care inovăm, lucrăm, comunicăm și, de ce nu, ne petrecem timpul liber.

Pentru industria IT, aceasta este probabil cea mai rapidă transformare tehnologică de la apariția internetului sau a smartphone-ului. Dar, pentru companii precum HP Inc., această revoluție vine cu o dublă responsabilitate: aceea de a accelera inovația și, în egală măsură, de a asigura securitatea într-o lume digitală din ce în ce mai complexă.

Productivitatea intră într-o nouă eră

Inteligența artificială promite un salt major de productivitate. Vedem deja cum AI devine integrată în dispozitivele pe care le folosim zilnic – de la laptopuri și stații de lucru, până la infrastructuri cloud și instrumente de colaborare. Capacitatea acestor tehnologii de a automatiza sarcini repetitive, de a analiza volume uriașe de date și de a oferi suport decizional în timp real schimbă radical modul în care organizațiile funcționează. Pentru companii, beneficiile sunt evidente. Angajații pot lucra mai eficient, pot avea acces rapid la informații și pot dedica mai mult timp activităților strategice sau creative. Pentru liderii de business, AI devine un instrument puternic de optimizare a proceselor și de accelerare a inovării.

În același timp, democratizarea accesului la tehnologie este un element esențial. AI nu trebuie să fie un avantaj rezervat doar marilor corporații globale. Integrarea capabilităților de inteligență artificială direct în dispozitivele de lucru - în special în noua generație de PC-uri optimizate pentru AI - permite companiilor de toate dimensiunile să beneficieze de aceste progrese. Pentru economii emergente sau pentru piețe dinamice precum România, vorbim de o oportunitate reală de accelerare a transformării digitale.

AI PC de la HP nu sunt doar laptopuri mai rapide; sunt platforme pregătite pentru întreprinderi, construite cu inteligență artificială integrată local, care oferă viteză, securitate și rentabilitate. AI redefinește deja PC-ul; nu este doar o promisiune pentru viitor. Aproape 30% dintre PC-urile HP vândute în 2025 includeau capacități AI.

Fața mai puțin văzută a revoluției AI

Totuși, orice revoluție tehnologică vine și cu riscuri. În același mod în care inteligența artificială poate ajuta companiile să devină mai eficiente, ea poate fi folosită și pentru a amplifica amenințările cibernetice. Atacurile de tip phishing generate cu ajutorul AI sunt deja mult mai dificil de detectat. Automatizarea poate permite atacatorilor să lanseze campanii sofisticate la scară globală, într-un timp foarte scurt.

Cel mai recent studiu HP Threat Insights arată că infractorii cibernetici se bazează pe inteligența artificială pentru a obține viteză, modularitate și automatizare în desfășurarea campaniilor. În pofida caracterului lor standardizat și a nivelului redus de complexitate, aceste atacuri asistate de AI, construite cu efort și resurse minime, reușesc să eludeze mecanismele tradiționale de apărare din mediul enterprise.

Această realitate schimbă fundamental modul în care trebuie să privim securitatea digitală. Dacă în trecut era percepută ca un strat suplimentar, adăugat după dezvoltarea unei tehnologii, astăzi ea trebuie să fie integrată încă din faza de proiectare. Conceptul de security by design nu mai este o opțiune, ci o necesitate. În era muncii hibride, dispozitivele utilizatorilor - laptopuri, PC-uri, stații de lucru sau chiar imprimante - devin prima linie de apărare. Angajații lucrează din diverse locuri, folosesc rețele diferite și accesează date critice și în afara biroului. Fiecare dispozitiv conectat la rețea reprezintă un instrument de productivitate, dar și un potențial punct de intrare pentru o breșă de securitate. De aceea, securitatea trebuie gândită pe mai multe niveluri: hardware, firmware, sistem de operare și aplicații. Protecția datelor, autentificarea avansată și mecanismele de detecție a amenințărilor trebuie să funcționeze împreună, într-un ecosistem coerent.

Inovația are nevoie de încredere

Cred că este esențial să înțelegem că un ecosistem digital sigur presupune colaborare între companii, autorități și mediul academic. Reglementările, standardele și bunele practici trebuie să evolueze în același ritm cu tehnologia. Din această perspectivă, România are o oportunitate importantă. Ecosistemul local de IT este recunoscut pentru talentul și competențele sale tehnice, iar tot mai multe companii internaționale investesc în centre de dezvoltare și inovare aici. Integrarea inteligență a inteligenței artificiale în mediul de business și în sectorul public poate accelera semnificativ digitalizarea economiei.

Inteligența artificială va continua să transforme industria tehnologică într-un ritm accelerat. Însă succesul acestei transformări nu va depinde doar de performanța tehnologiei, ci și de încrederea pe care utilizatorii o au în ea.

Securitatea imprimantelor este adesea neglijată, ceea ce creează breșe de securitate îngrijorătoare

Bazat pe un studiu global realizat pe un eșantion de peste 800 de manageri din domeniul IT și al securității (din SUA, Canada, UK, Japonia, Germania și Franța), un raport HP Wolf Security arată că securitatea la nivel de platformă este adesea neglijată, ceea ce creează breșe de securitate îngrijorătoare.

În faza de gestionare, doar 36% dintre echipele IT fac la timp actualizările de firmware. Iar acest lucru se întâmplă în pofida faptului că petrec în medie 3,5 ore pe lună la fiecare imprimantă, pentru a gestiona probleme legate de securitatea hardware-ului și firmware-ului. Fără actualizări prompte de firmware, companiile sunt expuse la amenințări care pot avea consecințe grave, cum ar fi furtul de date sensibile sau preluarea controlului asupra dispozitivelor de către infractori cibernetici.

Raportul semnalează și alte breșe de securitate, apărute în diverse etape:

Etapa de selectare a furnizorului

- **Lipsa colaborării în procesul de achiziție:** Doar 38% dintre respondenți au declarat că departamentele de achiziții, IT și securitate colaborează pentru a defini standardele de securitate ale imprimantelor. 60% avertizează că lipsa de colaborare expune compania la riscuri.
- **Cereri de ofertă fără verificare:** 42% nu implică echipele IT/de securitate în prezentările furnizorilor; 54% nu solicită documentație tehnică pentru a valida afirmațiile privind securitatea; 55% nu trimit răspunsurile trimise de furnizori pentru a fi analizate de echipele de securitate.
- **Incapacitatea de a verifica integritatea imprimantei:** Odată livrată, peste jumătate (51%) dintre echipele IT nu pot confirma dacă imprimanta a fost compromisă în fabrică sau pe durata transportului.

Etapa de Remediere

- **Incapacitatea de a detecta și remedia amenințările:** Multe companii au dificultăți în a gestiona actualizările critice. Doar 34% pot urmări modificările neautorizate ale hardware-ului efectuate de utilizatori sau de echipele de suport și doar 32% pot detecta evenimente de securitate asociate atacurilor la nivel hardware.

Etapa de Dezafectare

- Riscuri la sfârșitul ciclului de viață: 86% dintre respondenți spun că securitatea datelor reprezintă un obstacol în reutilizarea, revânzarea sau reciclarea imprimantelor.
- Lipsa încrederii: Echipele IT nu au încredere în soluțiile actuale de ștergere securizată, 35% declarând că nu sunt siguri dacă imprimantele pot fi șterse complet și în siguranță. Între timp, 1 din 4 consideră necesară distrugerea fizică a unităților de stocare ale imprimantelor, iar 1 din 10 susține distrugerea atât a dispozitivului, cât și a unității de stocare, pentru a asigura securitatea datelor.

Raportul oferă recomandări privind abordarea acestor provocări de securitate pe parcursul ciclului de viață al imprimantei:

- Asigurarea unei colaborări eficiente între echipele IT, de securitate și de achiziții pentru definirea cerințelor de securitate și reziliență pentru imprimantele noi;
- Solicitarea și utilizarea certificatelor de securitate emise de producător, atât pentru produse, cât și pentru procesele din lanțul de aprovizionare;
- Aplicarea la timp a actualizărilor de firmware pentru a limita expunerea la amenințări cibernetice;
- Implementarea de imprimante care pot monitoriza continuu amenințările zero-day și malware-ul, cu capacități de prevenire, detecție, izolare și recuperare în fața atacurilor de nivel scăzut;
- Alegerea imprimantelor cu funcții integrate de ștergere securizată a hardware-ului, firmware-ului și datelor stocate, pentru a permite o reutilizare sau reciclare în siguranță.

Cât de sigure sunt platformele moderne de colaborare?

Companiile ar trebui să acorde prioritate protejării informațiilor sensibile prin criptare end-to-end și autentificare cu doi factori.

Tehnologia a devenit esențială pentru **colaborare,** dar platformele moderne pot introduce și noi provocări de **securitate**. Pe măsură ce partajarea fișierelor, mesageria și instrumentele de colaborare devin mai răspândite, cresc și preocupările legate de accesul la date și păstrarea conținutului.

Organizațiile au acum nevoie de soluții care pot detecta datele sensibile, le pot proteja prin token-uri sau mascare și pot oferi vizibilitate în timp real asupra modului în care acestea sunt partajate.

Pentru a face acest lucru posibil, liderii IT apelează la **autentificarea multifactor** (MFA), controlul accesului bazat pe roluri (RBAC) și integrarea cu instrumente de securitate a datelor, cum ar fi prevenirea pierderii de date (DLP) și gestionarea riscurilor pentru persoanele din interior.

Companiile ar trebui să caute tablouri de bord cu riscuri care oferă o vizibilitate largă, împreună cu instrumente simplificate și automatizate pentru crearea de reguli, monitorizare și alerte.

Ar trebui să ia în considerare instrumente care evaluează dacă conținutul partajat este încă necesar și care identifică riscurile severe care necesită atenție urgentă.

Aceste capabilități pot ajuta organizațiile să rămână în siguranță în timp ce colaborează fără a fi copleșite.

Protecție prin parolă și criptare end-to-end

Companiile ar trebui să fie preocupate de accesul neautorizat și de confidențialitatea datelor partajate în cadrul întâlnirilor.

Funcții precum criptarea end-to-end, sălile de așteptare pentru a controla cine se alătură unei întâlniri, întâlnirile protejate prin parolă și MFA adaugă straturi suplimentare de securitate.

Deși instrumente populare precum **Microsoft Teams, Webex și Zoom** sunt destinate utilizării generale, nivelul de securitate necesar depinde în mare măsură de modul în care este utilizată platforma.

Din perspectiva ei, este esențial să se asigure configurarea corectă a funcțiilor de securitate, cum ar fi MFA sau criptarea datelor în repaus.

Gestionarea riscurilor de securitate

Platformele de colaborare prezintă o serie de riscuri de securitate pe care întreprinderile nu își pot permite să le treacă cu vederea. Pe măsură ce volumul de date crește, crește și suprafața de atac.

Un alt strat de complexitate provine din cerințele de reglementare. Majoritatea companiilor, indiferent de dimensiune, operează transfrontaliere sau în industrii cu reguli de conformitate diferite, de exemplu, conformitatea cu SOC 2 sau HIPAA. Acest lucru complică serios modul în care datele trebuie gestionate și securizate, neconformitatea putând deveni rapid un risc atât juridic, cât și reputațional.

Riscurile interne – atât accidentale, cât și rău intenționate – rămân o problemă tot mai mare, agravată de potențialul de compromitere a conturilor și de amenințări externe, cum ar fi ransomware-ul. Platformele de colaborare trebuie să se adapteze la fluiditatea organizațională. În caz contrar, datele sensibile pot ajunge în fața ochilor greșiți. Dacă controalele de acces sunt slabe sau configurate greșit, avertizează ea, platformele de colaborare pot deveni porți pentru pierderea datelor. De aceea, acestea trebuie să se adapteze la fluiditatea organizațională. În caz contrar, datele sensibile pot ajunge în fața ochilor greșiți.

Peisajul amenințărilor la adresa colaborării devine, de asemenea, mai complex. Companiile ar trebui să fie conștiente de riscurile în evoluție care vin odată cu aceasta.

De exemplu, „supraîncărcarea cu instrumente”, care se luptă sub greutatea prea multor soluții disparate, afectează multe companii. Acest lucru poate duce la configurații incorecte, politici inconsistente și confuzie generală. Deschide ușa către vulnerabilități care pot fi prevenite.

Tehnologiile emergente aduc, de asemenea, noi riscuri, una dintre preocupările majore fiind strategia „recoltează acum, decriptează mai târziu”, în care atacatorii exfiltrează date criptate astăzi cu intenția de a utiliza tehnologia viitoare de calcul cuantic pentru a sparge acea criptare. Inteligența artificială generativă remodelează și peisajul amenințărilor: deși promite eficiență, aduce provocări reale de securitate.

În cele din urmă, inteligența artificială va îmbunătăți calitatea atacurilor de tip phishing și de **inginerie socială**, crescând riscul de compromitere a conturilor. Cu toate acestea, în unele cazuri, datele pot să nu fie criptate corespunzător pe măsură ce trec prin canalul de inteligență artificială, creând noi puncte de expunere.

Soluții AI dezvoltate de Milestone pentru operațiuni de securitate

În timp ce inteligența artificială generativă transformă alte industrii, mulți operatori din domeniul securității se bazează încă pe procese manuale pentru revizuirea înregistrărilor video, documentarea incidentelor și anonimizarea materialelor video.

Miza în securitate este ridicată. Alarmele ratate sau alertele fals pozitive pot avea consecințe serioase, ceea ce face ca organizațiile să fie prudente în privința erorilor provocate de halucinațiile AI, a rezultatelor inconsecvente și a încrederii în sisteme automatizate în contexte în care o judecată corectă este esențială.

Concepute pentru a reduce efortul manual în punctele-cheie ale fluxului de lucru din securitate, soluțiile de AI generativă ale Milestone permit o analiză video mai rapidă, o documentare consecventă a incidentelor și conformitate cu cerințele de reglementare — aliniate la EU AI Act și GDPR — în cadrul ecosistemului Milestone:

- AI Search le permite investigatorilor să identifice rapid elementele relevante folosind limbaj natural — fără filtre complexe sau parcurgere manuală a materialului video.
- XProtect Video Summarization utilizează AI generativă pentru a produce automat descrieri text ale înregistrărilor video, standardizând documentarea incidentelor pentru operatori și reducând dramatic timpul de analiză.
- Video Anonymization sprijină conformitatea cu GDPR și cu alte reglementări privind protecția vieții private.

Toate soluțiile sunt dezvoltate astfel încât echipele de securitate să poată avea încredere pentru implementări în scenarii reale. Modelele de limbaj vizual (VLMs) ale Milestone sunt ajustate fin pe date video specifice anumitor verticale și cazuri de utilizare, oferind rezultate consecvente și fiabile, construite special pentru inteligența video — nu AI generalistă, multi-scope, reutilizată din alte domenii.

Milestone aplică aceeași rigoare în colectarea și administrarea datelor video — având în vedere conformitatea încă de la început. Biblioteca de date video de antrenare a Milestone este formată din date obținute în mod responsabil, complet anonimizate și trasabile. Milestone utilizează tehnologia de anonimizare a brighter AI în propriul său flux de date și o pune acum la dispoziția clienților în mod direct.

Amprenta “Life in Codes” în industria securității cibernetice

Exclusive Networks, un lider global în soluții de securitate cibernetică și cloud, a stabilit un obiectiv foarte sănătos pentru echipele sale, ceva ce, de fapt, multe alte companii ar trebui să ia în considerare – optimizarea platformei Jira pentru o mai bună aliniere la fluxurile lor de lucru unice.

Deși aveau membri ai echipei interne cu experiență în utilizarea Jira, au realizat rapid că utilizarea instrumentului și configurarea acestuia pentru succesul pe termen lung sunt două lucruri foarte diferite.
În încercarea lor de a profita la maximum de Jira, Exclusive Networks a învățat lecții valoroase despre diferența dintre utilizatorii “experți” (care, de fapt, sunt utilizatori experimentați) și specialiștii în configurare. Iată o privire asupra călătoriei lor.

Provocarea expertizei interne

Exclusive Networks avea mai mulți membri ai echipei care foloseau Jira de ani de zile. Mulți chiar luaseră inițiativa de a se poziționa ca “experți Jira” interni. Cu toate acestea, compania s-a lovit rapid de un zid atunci când a încercat să adapteze Jira la noi fluxuri de lucru.

După cum afirmă Amelie Donnally, Global Program Delivery & Business Governance Director,

„O mulțime de oameni din interior pretind expertiză pentru că au mai folosit Jira. Realitatea este că au lucrat în cadrul unor structuri preexistente și nu știu cum să o configureze de la zero pentru a răspunde nevoilor noastre.”

Această provocare a evidențiat o problemă cheie: diferența dintre a ști cum să navighezi în Jira și a ști cum să o personalizezi în mod corespunzător. Această constatare a determinat Exclusive Networks să solicite ajutor extern pentru a configura platforma mai eficient.

Consultanți externi generici: Un început accidentat

Ca multe alte companii, Exclusive Networks a apelat la consultanți externi pentru a umple golul de cunoștințe. Cu toate acestea, primele câteva runde de consultanți nu au dat rezultatele la care se așteptau. Deși promiteau o soluție personalizată, consultanții nu au răspuns de multe ori așteptărilor.

„Mulți consultanți susțineau că au mai făcut asta”, a spus Amelie. „Dar ceea ce au oferit a fost generic și nu a abordat provocările noastre specifice. A devenit clar că ei nu înțelegeau pe deplin modul în care funcționează compania noastră.”
În cele din urmă, Exclusive Networks a decis să facă o pauză și să își reevalueze abordarea, recunoscând că aveau nevoie de mai mult decât un simplu ajutor extern – aveau nevoie de expertiză autentică, specializată, care să se alinieze nevoilor lor de afaceri.

Apelarea la adevărații experți Atlassian

În acest moment, Exclusive Networks a început să lucreze cu echipa Life in Codes. Cel mai potrivit pentru nevoile lor a fost Sultan, unul dintre cei 15 consultanți care fac parte din echipă, dar care are o expertiză extinsă pe Jira. Sultan a adus o abordare nouă, concentrându-se pe înțelegerea structurii și nevoilor unice ale companiei înainte de a sări la soluții. Această schimbare de abordare a fost exact ceea ce avea nevoie compania.

„Sultan nu a fost doar un expert în Jira”, a remarcat Andy De Peter, Chief Information Security & Technology Officer la Exclusive Networks.

„A înțeles cum să configureze Jira într-un mod care să se alinieze cu fluxurile noastre de lucru. În loc să aplice o soluție unică, și-a făcut cu adevărat timp pentru a proiecta un sistem care să funcționeze pentru noi.”

Rezultatul? Proiectul pilot condus de Sultan a fost o descoperire pentru companie. Expertiza sa a permis companiei să configureze Jira într-un mod flexibil, scalabil și complet integrat cu operațiunile lor zilnice.

Puterea unei soluții personalizate

Una dintre cele mai semnificative diferențe aduse de consultantul Life in Codes a fost concentrarea sa pe adaptarea sistemului la nevoile specifice ale Exclusive Networks. El nu a venit cu o abordare de tip cookie-cutter. În schimb, a ascultat provocările cu care se confruntau echipele și a conceput o configurare Jira care să funcționeze perfect cu instrumentele și procesele existente.

„Soluția creată de Sultan a fost o schimbare pentru noi”, a declarat Andy. „Nu a mai trebuit să ne forțăm fluxurile de lucru să se încadreze într-un șablon Jira existent. În schimb, sistemul a fost construit în funcție de modul în care lucrăm de fapt.”
Această abordare nu numai că a îmbunătățit eficiența echipei, dar a și pregătit terenul pentru creșterea viitoare, deoarece sistemul a fost proiectat să evolueze odată cu compania.

Drumul înainte

Cu Jira configurat în mod corespunzător pentru a răspunde nevoilor lor, Exclusive Networks este gata să profite pe deplin de capacitățile platformei. Sistemul nu este doar un instrument – ei îl văd ca pe un activ strategic care va continua să le sprijine creșterea și evoluția nevoilor de afaceri.
Privind în urmă, Exclusive Networks își dă seama că cheia succesului a fost găsirea unui partener care să poată oferi o soluție personalizată, mai degrabă decât să se bazeze pe expertiza generală: aceasta este o reamintire a valorii expertizei reale.
Pentru alte companii care se confruntă cu provocări similare, experiența Exclusive Networks oferă un mesaj clar: atunci când vine vorba de sisteme critice precum Jira, nu vă mulțumiți cu nimic mai puțin decât expertiza adevărată. Partenerul potrivit poate face toată diferența, asigurându-se că platforma funcționează pentru dumneavoastră, nu invers.
Și nu uitați: nu există substitut pentru specialiștii care înțeleg atât tehnologia, cât și afacerea pe care o deservește.

Sunteți dornic de mai mult?

Nu ezitați să contactați și să discutați cu echipa **Life in Codes** situația companiei dvs., indiferent de industrie – studiile lor de caz demonstrează că au o expertiză puternică, indiferent de profilul companiei.

RSA anunță o nouă integrare cu Microsoft Edge for Business pentru a îmbunătăți securitatea Zero Trust

RSA a anunțat disponibilitatea noului conector Device Trust pentru Microsoft Edge for Business, extinzând colaborarea cu Microsoft pentru a ajuta clienții să își consolideze strategia de securitate Zero Trust.
Pe măsură ce organizațiile continuă să opereze într-un peisaj digital din ce în ce mai complex, securizarea fiecărui punct de acces, în special a browserului, a devenit o parte critică a protejării resurselor întreprinderii. Prin aducerea soluțiilor de gestionare a accesului de încredere RSA direct în Microsoft Edge for Business, clienții pot beneficia acum de o autentificare perfectă, contextuală, prin intermediul atributului de acces condiționat al browserului gestionat, care îmbunătățește zero-trust fără a compromite experiența utilizatorului.
Având în vedere că actorii amenințători vizează fiecare componentă a suprafeței de atac și că organizațiile lucrează în mai multe medii și acceptă o gamă largă de dispozitive gestionate și negestionate, securitatea trebuie să fie fundamentală pentru fiecare utilizator, dispozitiv și aplicație – nu o idee ulterioară.
Clienții pot implementa conectorul RSA direct prin serviciul de administrare Edge din centrul de administrare Microsoft 365, simplificând integrarea și scalarea în cadrul organizației.
Soluțiile de securitate IT, risc si conformitate RSA sunt distribuite în România de compania SolvIT Networks.

Riscurile pentru infrastructura de transport în 2026

Mașinile moderne au devenit dispozitive digitale tot mai complexe, cu capacități extinse de comunicare la distanță, iar atacurile malware pot viza nu doar vehiculele în sine, ci și sistemele la care acestea sunt conectate.

În 2026, atacurile realizate de actori malware motivați financiar vor continua, utilizând în principal ransomware. Scopul unor astfel de atacuri este criptarea fișierelor, sistemelor sau a întregilor rețele ale victimelor, făcându-le inaccesibile, pentru ca ulterior atacatorii să solicite o răscumpărare (de obicei în criptomonede) în schimbul furnizării cheii de decriptare sau restabilirii accesului. De asemenea, pot fi dezvăluite noi scurgeri de date (inclusiv date confidențiale ale utilizatorilor și informații despre deplasările vehiculelor) din infrastructurile producătorilor auto.

Un alt vector important îl reprezintă atacurile asupra lanțului de aprovizionare, prin compromiterea sistemelor contractorilor, cu scopul de a perturba sistemele critice și de a provoca pierderi financiare. Auditurile de securitate efectuate periodic de Kaspersky identifică vulnerabilități care pot fi exploatate pentru astfel de atacuri.

Atacuri asupra infrastructurii de taxi și a flotelor, serviciilor de car sharing, companiilor de transport și logistică

Furtul de date personale și perturbarea sistemelor critice. Atacatorii motivați financiar sunt interesați în principal de datele personale ale utilizatorilor și de accesul la conturile acestora. Sunt posibile și atacuri ransomware menite să perturbe sistemele critice și să provoace pierderi financiare companiilor.

Blocarea de la distanță a mașinilor.

Acesta este un risc major, deoarece companiile de car sharing și taxi instalează module în vehiculele lor care permit, printre altele, blocarea de la distanță în orice moment. Dacă atacatorii obțin acces la sistemul de control al acestor module, pot bloca în masă mașinile, de exemplu, pentru răscumpărare sau sabotaj.

Hackingul sistemelor companiilor de transport și logistică și interceptarea mărfurilor.

Un alt vector potențial de risc îl reprezintă atacurile asupra companiilor de transport și logistică, pentru a intercepta ulterior comenzile și a fura fizic mărfurile. În contextul digitalizării proceselor din lanțul de aprovizionare, atacatorii pot fura fizic bunuri fără a părăsi spațiul cibernetic. Aceștia pot compromite de la distanță sistemele și manipula datele de livrare pentru a redirecționa marfa către o anumită adresă, în vederea revânzării ulterioare.

Atacuri asupra infrastructurii stațiilor de alimentare și de încărcare pentru vehicule electrice

Trendul digitalizării nu ocolește infrastructura de alimentare. Stațiile moderne de alimentare și de încărcare pentru vehicule electrice sunt proiectate pentru a fi conectate la infrastructuri cloud. Acest lucru deschide numeroase oportunități pentru atacatori. Până în 2026, sunt posibile atacuri asupra acestor infrastructuri cloud, având ca scop furtul direct de combustibil sau energie electrică, precum și al datelor clienților, cum ar fi informațiile personale sau detaliile cardurilor de combustibil.

Exploatarea vulnerabilităților arhitecturii auto pentru furtul vehiculelor

La nivel global, sunt produse tot mai multe vehicule moderne, computerizate, dotate cu numeroase unități electronice de control (ECU), iar atacatorii vor continua să exploateze erori de implementare și vulnerabilități pentru a fura vehicule. Un exemplu recent este cazul în care atacatorii au reușit să se conecteze la magistrala CAN a vehiculelor unui producător major prin intermediul unui far, obținând ulterior acces la sistemul de pornire a motorului. Experții se așteaptă ca noi vulnerabilități utilizate pentru furtul mașinilor să fie descoperite în 2026. Punctele de intrare pot fi orice interfață accesibilă: magistrala CAN, portul OBD, portul Ethernet, modulul NFC, cipurile Wi-Fi și Bluetooth și modemul LTE. Sistemele moderne de calcul integrate în vehicule sunt conectate direct sau indirect la internet, ceea ce face ca atacurile împotriva lor să fie doar o chestiune de timp. Pentru a crea sisteme rezistente la atacuri, principiile de securitate ar trebui integrate încă din etapele de proiectare și dezvoltare. Acest lucru va reduce o parte dintre riscuri și va diminua probabilitatea exploatării vulnerabilităților. Kaspersky a dezvoltat propria soluție pentru asigurarea securității informaționale a vehiculelor – Kaspersky Automotive Secure Gateway, bazată pe sistemul de operare KasperskyOS. În plus, riscurile pot fi reduse prin efectuarea periodică a auditurilor de securitate pentru identificarea și remedierea rapidă a vulnerabilităților, precum și prin instalarea unor soluții specializate cu protecție împotriva ransomware-ului și a altor tipuri de malware pe endpoint-urile din rețelele office și industriale.

Întreprinderile aleg cloud-ul hibrid pentru reziliență, nu pentru simplitate

Concluziile recentei ediții a studiului Genetec 2026 State of Physical Security Survey, la care au contribuit peste 7.300 de respondenți, arată că adoptarea cloud-ului hibrid este o alegere strategică de arhitectură determinată de nevoi operaționale pe termen lung:

- 39% dintre organizații indică scalabilitatea drept un motiv-cheie pentru adoptarea mediilor de tip cloud hibrid
- 38% indică redundanța drept un motiv-cheie pentru adoptarea mediilor cloud hibrid, ceea ce întărește accentul pus pe reziliența și continuitatea pe termen lung

Pentru a sprijini o adoptare sigură și reziliență a cloud-ului, Genetec recomandă patru priorități:

1. Plasați guvernanța în centrul deciziilor privind cloud-ul

La nivel de organizație, adoptarea cloud-ului ar trebui să fie modelată de responsabilitate, nu de comoditate. Cerințele privind securitatea cibernetică, conformitatea și supravegherea trebuie abordate de la început, nu adăugate ulterior.

2. Proiectați pentru medii hibride

Adoptarea cloud-ului la nivel de organizație rareori are loc într-o singură etapă. Majoritatea organizațiilor operează în paralel sisteme cloud, on-premise și edge, adesea pentru perioade îndelungate. Operarea în

mediile hibride le permite organizațiilor să se modernizeze în propriul ritm, menținând totodată controlul asupra infrastructurii critice și a datelor sensibile.

3. Tratați cloud-ul ca pe un model operațional, nu ca pe o destinație

Dezvoltările în cloud ar trebui să consolideze vizibilitatea și controlul asupra sistemelor de securitate fizică, nu să înlocuiască direct infrastructura existentă. Accentul ar trebui să fie pus pe integrarea funcționalităților specifice cloud în medii mai largi, nu pe impunerea unor modele uniforme de implementare.

4. Construiți pentru reziliență pe termen lung

Se așteaptă ca infrastructura de securitate fizică să rămână operațională ani de zile, chiar și în timpul întreruperilor de rețea, al întreruperilor în furnizarea serviciilor sau al schimbării condițiilor economice. Arhitecturile care susțin operarea autonomă și degradarea graduală în mediile cloud, on-premises și edge ajută organizațiile să mențină continuitatea, să respecte cerințele de reglementare și să gestioneze riscurile în evoluție fără întreruperi.

Pentru mai multe informații din partea Genetec despre securizarea sistemelor de securitate fizică enterprise în cloud, accesați: https://resources.genetec.com/ebooks-reports/enterprise-physical-security-in-the-cloud-era.

VBSOC - Securitatea cibernetică de nivel enterprise mai aproape de IMM-uri

Piața de securitate cibernetică trece printr-o transformare accelerată: companiile nu mai caută soluții izolate, ci servicii gestionate capabile să ofere protecție continuă, integrate într-o arhitectură modernă. În centrul acestei schimbări se află Security Operations Center (SOC), o echipă care monitorizează, analizează și răspunde la incidente în timp real, 24/7.

Pentru majoritatea companiilor mici și mijlocii, construirea propriului SOC este imposibilă din punct de vedere bugetar și operațional. De aceea, Vodafone Business a creat Vodafone Business Security Operations Center (VBSOC) – un serviciu gândit special pentru IMM-uri, care oferă același nivel de protecție utilizat de marile corporații.

Soluții de securitate adaptate fiecărei companii

VBSOC integrează două tipuri de personalizare esențiale:

1. Personalizare tehnică

Folosim tehnologii moderne de tip XDR/SIEM + SOAR, capabile să:

- coreleze automat volume mari de evenimente,
- înțeleagă profilul de risc al fiecărei organizații,
- genereze alerte relevante,
- activeze playbook-uri de răspuns adaptate clientului.

2. Personalizare de business

Pe lângă tehnologia avansată, punem accent pe comunicarea transparentă:

- asistență în activarea și operarea serviciului,
- suport dedicat în caz de incident,
- consultanță în implementarea regulilor de securitate în funcție de nevoile fiecărei companii.

AI-ul este motorul din spatele serviciilor VBSOC

Inteligența artificială este integrată în nucleul VBSOC pentru a crește eficiența și viteza de reacție. AI-ul ne ajută să:

- filtrăm și prioritizăm alertele, reducând drastic alarmele false;
- investigăm și răspundem automat la incidente cu complexitate redusă;
- corelăm log-uri din surse multiple și oferim recomandări clare și ușor de implementat.

Astfel, experții noștri își pot concentra timpul pe dezvoltarea de noi metode de detecție pentru atacurile avansate.

Parteneriatul strategic cu Google: protecție construită pe SecOps și Gemini

La nivel de Group, Vodafone dezvoltă servicii de securitate folosind platforma Google Security Operations (SecOps) – o soluție unificată SIEM + SOAR – și capabilitățile modelelor AI Gemini.

Această combinație permite:

Cu Google SecOps:

- colectarea și analiza telemetriei de securitate la scară mare;
- automatizarea răspunsului prin playbook-uri inteligente.

Cu Gemini integrat în SecOps:

- generarea automată de interogări și reguli de detecție,
- rezumarea incidentelor complexe,
- prioritizarea alertelor relevante,
- recomandări concrete de remediere.

Beneficii pentru IMM-uri: securitate de top, ca serviciu

Prin expertiza echipei Vodafone Business și tehnologiile Google SecOps + Gemini, clienții IMM primesc:

- protecție de nivel enterprise, fără investiții în infrastructură internă;
- soluții ușor de utilizat, fără necesitatea unui departament de securitate dedicat;
- timp excelent de detecție și răspuns, datorită automatizării și monitorizării continue.

Cu alte cuvinte, aducem capabilități avansate de monitorizare și detecție într-o zonă unde, până acum, astfel de servicii erau greu accesibile. Cum transpunerea recentă a Directivei NIS2 în legislațiile europene, inclusiv în România, schimbă fundamental modul în care companiile – nu doar cele mari, ci și IMM-urile – trebuie să își gestioneze securitatea cibernetică. NIS2 ridică standardele obligatorii de protecție, introduce cerințe clare privind monitorizarea continuă, raportarea incidentelor majore, auditarea regulilor de securitate și responsabilizarea managementului.

Pentru foarte multe IMM-uri, aceste cerințe reprezintă o provocare semnificativă. Ele nu dispun de echipe interne specializate, iar costurile unei infrastructuri proprii sunt greu de susținut. În același timp, companiile vizate de NIS2 trebuie să demonstreze un nivel ridicat de maturitate în procese, tehnologie și răspuns la incidente – exact acele componente care necesită expertiză profesionistă și monitorizare 24/7.

Într-un context în care lipsa de experți este acută, iar reglementările devin tot mai exigente, soluțiile gestionate precum VBSOC devin nu doar un serviciu util, ci o necesitate. Ele oferă IMM-urilor acces la tehnologii enterprise, capacități AI integrate și suport operațional permanent, toate livrate ca serviciu, cu costuri predictibile.

Astfel, VBSOC nu doar că îți protejează afacerea, ci îți oferă și cadrul necesar pentru a continua să inovezi în siguranță, pe o piață tot mai competitivă.

Amenințările din telecom din 2025 se vor extinde în 2026, pe măsură ce noile tehnologii aduc riscuri suplimentare

Activitatea APT, compromiterea lanțului de aprovizionare, atacurile DDoS și frauda facilitată de SIM au continuat să exercite presiune asupra operatorilor în 2025, în timp ce implementarea noilor tehnologii introduce riscuri operaționale suplimentare.

În 2025, operatorii telecom s-au confruntat cu patru mari categorii de amenințări. Atacurile țintite (APT) au continuat să vizeze obținerea unui acces discret în mediile operatorilor, în scopul spionajului pe termen lung și al exploatării poziționării privilegiate în rețea. Vulnerabilitățile din lanțul de aprovizionare au rămas o poartă de intrare importantă: ecosistemele telecom se bazează pe numeroși furnizori, contractori și platforme strâns integrate, astfel încât vulnerabilitățile din software-ul și serviciile utilizate pe scară largă pot oferi acces la rețelele operatorilor. Nu în ultimul rând, atacurile DDoS au continuat să reprezinte o problemă practică de disponibilitate și capacitate.

În perioada noiembrie 2024 – octombrie 2025, Kaspersky Security Network arată că 12,79% dintre utilizatorii din sectorul telecomunicațiilor s-au confruntat cu amenințări web, iar 20,76% au întâlnit amenințări la nivelul dispozitivelor. În același interval, 9,86% dintre organizațiile telecom la nivel global au fost afectate de ransomware.

În același timp, sectorul telecomunicațiilor trece de la o etapă de dezvoltare tehnologică rapidă la una de implementare pe scară largă — iar raportul susține că această tranziție creează noi oportunități, dar și noi riscuri operaționale pentru 2026. Kaspersky evidențiază trei domenii în care tranzițiile tehnologice pot genera perturbări dacă sunt implementate neuniform sau fără controale solide:

- gestionarea rețelelor asistată de AI, unde automatizarea poate amplifica erori de configurare sau poate acționa pe baza unor date înșelătoare;
- tranzițiile către criptografia post-cuantică, unde implementarea grăbită a abordărilor hibride și post-quantum poate genera probleme de interoperabilitate și performanță în mediile IT, de management și de interconectare;
- și integrarea 5G–satelit (NTN), unde extinderea ariei de servicii și dependența de parteneri introduc noi puncte de integrare și potențiale moduri de eșec.

Pentru a reduce riscurile și a consolida reziliența, experții Kaspersky recomandă:

- Monitorizarea continuă a peisajului APT și a infrastructurii relevante pentru telecom.
- Abordarea automatizării rețelelor bazate pe AI ca pe un program de management al schimbării.
- Creșterea nivelului de pregătire împotriva atacurilor DDoS ca problemă de management al capacității.
- Implementarea unei capabilități EDR.

Ce sunt, ce fac și de ce e nevoie de polițiști cripto în Web3?

În lupta împotriva criminalității cibernetice, două lumi diferite trebuie să colaboreze.

Prima este lumea tradițională a forțelor de ordine, bazată pe jurisdicții, proceduri legale și dovezi fizice, în cea mai mare proporție fiind vorba de infracțiuni offline. A doua este lumea nativ online a Web3, descentralizată, pseudonimă, rapidă și tehnică, care operează dincolo de granițe și adesea în afara metodelor tradiționale de investigație.

Împreună, cele două reprezintă o provocare pentru instituțiile publice, precum poliția și autoritățile de reglementare, și platformele private care gestionează infrastructura economiei digitale.

Pe măsură ce activitatea infracțională se mută în ecosisteme digitale, agențiile de aplicare a legii trebuie să se adapteze rapid. Unele au făcut progrese mari (precum cele din Coreea și Thailanda), în timp ce altele întâmpină dificultăți în a ține pasul cu tehnologiile descentralizate.

Ce este și cum arată un „polițist cripto”?

Apare un nou tip de agent al forțelor de ordine, ca răspuns la criminalitatea cibernetică din ce în ce mai sofisticată. El are o înțelegere profundă a tehnologiei blockchain și a complexității investigațiilor cripto, obținute prin instruire, experiență practică și experimentarea cu noi tehnologii. Coincidență sau nu, cei mai buni polițiști sunt, de cele mai multe ori, utilizatori pasionați de criptomonede.

Natura descentralizată și rapidă a infracțiunilor legate de criptomonede cere agilitate și adaptare constantă. Companiile private joacă un rol important în acest ecosistem, deoarece oferă expertiză tehnică forțelor de ordine, acces la instrumente de investigație și, cel mai important, date operaționale fără de care multe investigații nu ar putea fi încheiate cu succes.

Colaborând, sectoarele public și privat pot reduce lacunele critice de capacitate și resurse, ceea ce duce la răspunsuri mai rapide la amenințările emergente, făcând lupta împotriva infracțiunilor cripto mai eficientă.

În România, **prin Binance Academy**, s-au derulat în ultimii ani variate workshop-uri ori cursuri prin care se “antrenează” inclusiv reprezentanți ai Poliției pentru a fi pregătiți cât mai bine în investigarea criminalității informatice în mediile cripto și blockchain.

Blockchain-ul urmărește mersul baniilor

Spre deosebire de numerar, **criptomonedele nu dispar pe măsură ce trec, de mai multe ori, de la un utilizator la altul.** Fiecare tranzacție pe blockchain este marcată temporal, trasabilă și verificabilă public. Acest lucru a permis autorităților indiene să înceapă urmărirea USDT-ului furat în ambele cazuri prezentate mai sus.

Adică, **criptomonedele nu sunt anonime.** Dar asta nu înseamnă că ele sunt nesigure, ci exact opusul: **activele digitale pot fi mai sigure atunci când platformele, autoritățile de reglementare și forțele de ordine colaborează.**

Concluzie

Pe măsură ce criminalitatea cibernetică evoluează dincolo de granițe și modelele tradiționale, este nevoie de un nou tip de agent al forțelor de ordine, un „polițist cripto”, care să înțeleagă atât complexitățile investigațiilor blockchain, cât și metodele tradiționale de combatere a criminalității și să fie pasionat de noile dezvoltări tehnologice și de colaborarea strânsă cu sectorul privat.

Conectarea lumilor tehnologiei și forțelor de ordine nu mai este opțională, este esențială. **Scopul: să construim un viitor digital mai puternic, mai inteligent și mai sigur pentru toți.**

PROVISION
SECURITY DAY

28 MAI | FACE CONVENTION CENTER

From past lessons to AI-Driven Defense

Building Cyber Resilience Together

ProvisionSecurityDays.ro