Club It&C
WWW.CLUBITC.RO
MAI 2025

CONSOLIDAREA
SECURITĂȚII IDENTITĂȚII

FRAUD XDR:
Protecție mai inteligentă
pentru sistemul bancar modern

Reglementarea DORA

Conformarea la directiva de
securitate cibernetică NIS2


Allied Telesis


allevo
THINKING EVOLUTION


AXIS
COMMUNICATIONS


asee
by osseco


BiT
software
ENTERSOFT


BRINEL
IQANTO


BUCHAREST
PROMOROBOTS


foundever™


HONOR


Club IT&C


hp


INFORM
Member of AUSTRIACARD HOLDINGS


KASPERSKY lab


LIFE
IS
HARD
WORK SOFT


LIFEINCLOUD


milestone


oppo


PRO SYS


Romsym Data


Schneider
Electric


SOLVIT
works naturally


SYSTEM INNOVATION ROMANIA


TCL
The Creative Life


VERTIV.


xiaomi

pag. 22

Fraud XDR: Protecție mai inteligentă pentru sistemul bancar modern

CUPRINS

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

TAG media

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

Predicții pentru 2025

Recent, Symantec a publicat un şir de predicții legate de posibilele probleme cu care se va confrunta industria securității cibernetice în 2025.

Predicțiile indică o creștere a agresiunii cibernetice a Rusiei, un ecosistem ransomware în creștere, atacatori care vizează platforme cloud de încredere cândva, și faptul că utilizarea instrumentelor Land (LOTL) și grupurile de ransomware se extind la noi zone geografice.

1. Agresorii ruși (și orice alt fel) se vor confrunta cu EDR și controlul aplicațiilor.

Atacatorii pot lovi de oriunde, dar apărările inteligente fac diferența. Cu sistemul de detectare și răspuns (EDR) nativ în cloud Carbon Black sau EDR local de la Symantec, organizațiile pot detecta conexiunile de rețea de la adresele IP rusești și pot detecta tehnicile utilizate de operațiuni criminale, cum ar fi Dragonfly, care vizează infrastructura critică. Controlul aplicațiilor, inițiat de Carbon Black și predecesorul său Bit9, permite doar aplicațiilor și fișierelor de încredere să ruleze în mediul dvs., ajutând în același timp să blocheze codurile rău intenționate și executabilele – parte a unei poziții de încredere zero. Carbon Black App Control poate fi implementat on-premise sau în cloud pentru a proteja activele pe care alte soluții nu le au, cum ar fi sistemele vechi și dispozitivele de la punctul de vânzare.

2. Atacatorii ransomware se vor baza pe dv. să aveți protecție de bază.

Indiferent dacă arma lor preferată este ransomware-ul sau o altă tehnică, atacatorii fac adesea mișcarea pe baza presupunerii că organizația dvs. folosește protecție de bază. Trebuie să le demonstrați că au greșit. Protecțiile precum Symantec EDR și Carbon Black EDR pot detecta comportamente de amenințare asociate în mod obișnuit cu ransomware – comportamente pe care alte instrumente de primă linie nu le detectează. Între timp, soluțiile de prevenire a pierderii datelor (DLP) precum Symantec DLP împiedică accesul la datele sensibile, indiferent de vectorul de atac. Și datele sunt ceea ce urmăresc atacurile ransomware.

3. Atacurile Living Off the Land (LOTL) pot avea mai puțin teren de acțiune.

Atacurile LOTL sunt în creștere, actorii amenințărilor folosind funcții și instrumente ale sistemului de operare pentru a lansa ransomware și alte atacuri. (Aproape jumătate dintre atacurile

ransomware din 2021-2023 au folosit instrumente LOTL.) Cele mai recente soluții de securitate cibernetică pot ajuta la prevenirea acestor incursiuni. Unul este Adaptive Protection, o caracteristică unică a Symantec Endpoint Security (SES) care blochează automat utilizarea anormală a instrumentelor și software-ului legitim. În plus, clienții Symantec EDR se pot abona la o listă de urmărire a driverelor vulnerabile și rău intenționate care ar putea fi ținte LOTL.

4. „Identitatea" va deveni următorul domeniu mare în detectarea bazată pe date și prevenire analitică.

Actorii amenințărilor fură acum identități și monitorizează comportamentele, astfel încât să se poată masca pe deplin drept utilizatori legitimi, chiar și cei cu privilegii ridicate. Devine din ce în ce mai greu să identifici aceste atacuri doar pe baza utilizării instrumentelor și este din ce în ce mai necesar să încorporezi identitatea și informațiile de acces în logica de detectare. Industria va revizui analiza comportamentului utilizatorilor și entităților (UEBA), ghidându-l pe căi mai integrate și mai bine direcționate.

5. Corelația va rămâne Sfântul Graal, dar centralizarea va fi nuanțată.

Toată lumea acceptă acum că securitatea cibernetică trebuie să fie bazată pe date, că trebuie colectat un nivel cu totul nou de telemetrie și că informațiile trebuie corelate între domeniile de rețea, punct final, informații, identitate și infrastructură. Furnizorii vor gândi în afara cutiei atunci când vine vorba de centralizare, aplecându-se puternic pe concepte precum filtrarea inteligentă, agregarea pe niveluri și corelarea încrucișată de tip peer-like – și vor construi arhitecturi specializate pentru securitate cibernetică.

6. Clienții se vor aștepta la automatizarea și comercializarea descoperirilor din ultimul deceniu.

Cu câțiva ani în urmă, clienții nu erau dispuși să ofere managementul impactului operațional care ar putea pune capăt carierei atacatorilor în defavoarea analizei avansate, învățării automate sau AI. Dar lucrurile înaintează rapid până acum, iar clienții se întreabă: „Dacă puteți detecta cu încredere și puteți răspunde cu ușurință, de ce nu ați automatizat toate acestea pentru noi?" Ei doresc ca ceea ce era avansat și interactiv în urmă cu câțiva ani să devină încorporat și automat. Furnizorii care au stocat ani de analiză structurată și organizată a atacurilor și informații despre amenințări de clasă mondială vor fi bine poziționați pentru a profita imediat de modelele în limbaj mare (LLM) și pentru a oferi acel viitor. Vânzătorii cărora le lipsesc acestea se vor lupta să supraviețuiască.

7. Detectarea amenințărilor și răspunsul se vor consolida în mediile hibride.

Mediile de lucru hibride intensifică provocarea securizării punctelor finale în diverse sisteme on-premise și cloud. În 2025, sistemele unificate de detectare și răspuns a amenințărilor vor deveni esențiale. Aceste platforme vor trebui să combine EDR, detectarea și răspunsul extins (XDR) și orchestrarea securității pentru a monitoriza, detecta și remedia amenințările în timp real. Schimbarea valorifică automatizarea și inteligența amenințărilor pentru a reduce punctele moarte ale forței de muncă distribuite și pentru a accelera timpii de răspuns. Soluțiile care oferă vizibilitate profundă asupra comportamentelor terminalelor și integrarea cu ecosisteme mai largi de informații despre amenințări sunt cele mai bine pregătite pentru a răspunde acestei nevoi.

8. Strategiile avansate de prevenire a pierderii datelor (DLP) se vor concentra pe fluxurile de lucru descentralizate.

Creșterea instrumentelor AI generative, a muncii de la distanță și a fluxurilor de lucru descentralizate a sporit riscul scurgerii involuntare sau rău intenționate de date. Organizațiile vor acorda prioritate strategiilor DLP avansate care încorporează protecția datelor conștientă de context și (după cum s-a menționat mai sus) analize inteligente ale comportamentului utilizatorilor. În 2025, soluțiile DLP vor evolua cu procesarea limbajului natural (NLP) și învățarea automată, permițând detectarea în timp real a partajării datelor sensibile pe platformele de colaborare și serviciile cloud. Măsurile proactive, cum ar fi redactarea automată și controalele granulare ale accesului, vor câștiga, de asemenea, proeminență.

9. Strategiile pentru canalul de vânzări de securitate cibernetică se vor schimba.

Canalele tradiționale de vânzare nu mai sunt echipate pentru a face față complexităților peisajului securității cibernetice de astăzi. Organizațiile recunosc din ce în ce mai mult că extinderea strategiilor lor de canal necesită mai mult decât parteneriate tranzacționale – necesită un ecosistem colaborativ în care partenerii să fie împuterniciți cu instrumentele, instruirea și informațiile necesare pentru a oferi soluții integrate, fără întreruperi, prin partenerii locali pe care îi cunosc și în care au încredere. Pe măsură ce trecem în 2025, un nou model de lansare pe piață a canalului, condus de programul revoluționar Catalyst Partner Program al Broadcom, este gata să stabilească o tendință pe care probabil că alte companii de tehnologie o vor urma. Acestea nu vor fi singurele tendințe care definesc 2025, dar este sigur că vor atrage atenția la un moment dat. Când o vor face, sperăm că veți dispune de **măsurile de protecție** necesare pentru a face față provocărilor din acest an.

Romsym Data este unul dintre cei mai importanți furnizori de soluții IT din România și oferă cele mai noi tehnologii Symantec pe piața din România și Republica Moldova.

AI: Noul arsenal al criminalilor cibernetici și amenințările pentru business-uri

Inteligența artificială transformă industriile din întreaga lume. Deși creează premisele pentru mai multă inovație și eficiență, oferă și noi oportunități infractorilor cibernetici.

De la automatizarea atacurilor la neutralizarea sistemelor foarte sigure, AI este, fără îndoială, o armă puternică pentru hackeri, reprezentând o creștere fără precedent a amenințărilor pentru companiile mari. Un studiu Kaspersky, realizat în rândul profesioniștilor InfoSec din companiile mijlocii și mari din întreaga lume, a arătat că 46% dintre respondenți cred că majoritatea atacurilor cibernetice suferite de organizațiile lor în ultimele 12 luni au folosit tehnologii AI într-un fel sau altul. AI dă putere infractorilor cibernetici să-și atace țintele cu o mai mare viteză și precizie. Una dintre cele mai semnificative transformări este modul în care AI a revoluționat campaniile automate de phishing și inginerie socială. Folosind instrumente de inteligență artificială, hackerii pot acum să analizeze în profunzime datele angajaților, depistându-le pozițiile în companie, analizând comportamentele lor în comunicare și identificând activitatea lor în cadrul rețelelor sociale pentru a crea tactici de inginerie socială extrem de personalizate și credibile.

În mod alarmant, AI este, de asemenea, folosită de infractorii cibernetici pentru a produce conținut audio și video de tip deepfake, reproducând vocile și chipurile directorilor executivi sau ale altor directori pentru a-i folosi în escrocherii frauduloase. În plus, AI ajută atacatorii să evite mecanismele tradiționale de securitate. Folosind algoritmi de învățare automată, un atacator poate testa toate variantele posibile ale atacului în timp real, ceea ce îi oferă o modalitate mai eficientă de a evita software-ul de securitate cibernetică și firewall-urile.

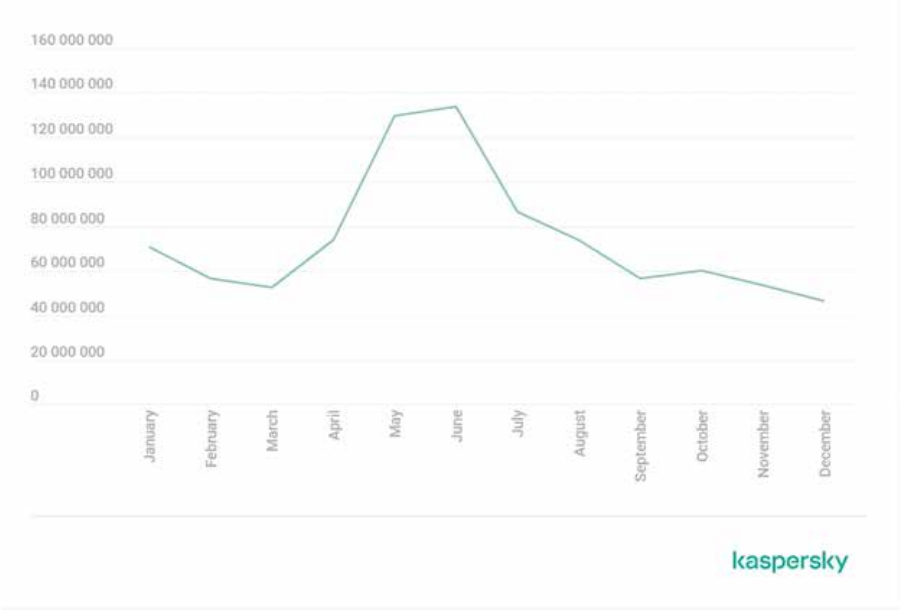
Apariția atacurilor susținute de AI înseamnă că businessurile de toate tipurile și dimensiunile sunt acum expuse unui risc crescut. Anterior, unele companii nu erau percepute ca ținte potențiale, dar acum AI dă putere atacatorilor să-și extindă operațiunile. Infractorii cibernetici pot ataca mii de companii simultan, cu un efort minim. Atacurile pot fi acum desfășurate mai eficient, ascunzând în același timp urmele care duc la sursa actului rău intenționat.

Daunele asociate cu atacurile conduse de AI, atât financiare, cât și reputaționale, pot fi majore pentru companii. În plus, pot duce la amenzi și costuri legale, precum și prejudicii pe termen lung aduse la nivelul încrederii clienților – un domeniu deosebit de sensibil pentru sectoare precum finanțele, asistența medicală și

serviciile juridice, care se bazează foarte mult pe încrederea și confidențialitatea consumatorilor.
Pentru a contracara amenințarea tot mai mare a infracțiunilor cibernetice bazate pe inteligența artificială, companiile trebuie să se concentreze pe construirea unui cadru cuprinzător de securitate cibernetică, în loc să se bazeze numai pe soluții AI. Deși instrumentele AI joacă un rol critic în monitorizarea în timp real și detectarea amenințărilor, ele nu sunt suficiente. Securitatea cibernetică eficientă necesită o abordare pe mai multe straturi, care să includă instrumente avansate de securitate, instruire regulată a angajaților și planificare proactivă a răspunsului la incident. Numai combinând tehnologia, educația și pregătirea companiilor, acestea pot construi reziliența necesară pentru a face față provocărilor generate de amenințările din ce în ce mai sofisticate, bazate pe inteligența artificială.

Aproape 900 de milioane de încercări de phishing în 2024

Soluțiile de securitate Kaspersky au blocat peste 893 de milioane de încercări de phishing în 2024 – o creștere cu 26% față de 2023, când totalul a fost de aproape 710 milioane. Creșterea tentativelor în perioada mai – iulie este în mod tradițional legată de sezonul vacanțelor, când fraudatorii încearcă frecvent să atragă călătorii cu escrocherii care implică rezervări false la companii aeriene și la hoteluri, pachete turistice înșelătoare și oferte prea bune pentru a fi adevărate.



Încercări de click pe link-uri de phishing, descoperite de soluțiile de securitate Kaspersky, 2024

Experții au observat o serie de scheme de phishing și escrocherie care vizează furtul de date sau bani și instalarea de software rău intenționat. În 2024, infractorii cibernetici au imitat adesea site-urile unor branduri cunoscute precum Booking, Airbnb, TikTok, Telegram și altele. O campanie în curs, de exemplu, a vizat utilizatorii TikTok Shop. Criminalii cibernetici au creat pagini de conectare false concepute pentru a fura acreditările vânzătorilor. În plus, escrocii au valorificat știrile în tendințe, orchestrând scheme de fraudă care implică subiecte hype, de exemplu jocul de criptomonede Hamster Kombat și portofelele TON.
Schemele frauduloase au încercat, de asemena, să valorifice imagini false ale celebrităților, promovând în mod fals giveaway-uri cu premii valoroase pentru fani, care nu au fost niciodată livrate. Tendința persistă în 2025.
Potrivit datelor Kaspersky, în 2024, atât persoanele fizice, cât și utilizatorii corporativi au primit de peste 125 de milioane de ori documente și link-uri rău intenționate pe e-mail.
Infractorii cibernetici au folosit diverse tactici în campaniile de e-mail care vizează companiile, după cum au observat experții. Acestea au inclus trimiterea de e-mailuri cu arhive protejate prin parolă care ascund conținut rău intenționat și imagini SVG deghizate în grafice inofensive, precum și multe alte scheme. Atacatorii au atras victimele să facă click pe conținut rău intenționat prin false chemări în judecată, oferte false, notificări oficiale contrafăcute și multe altele.
Aproape fiecare al doilea e-mail trimis către mesageriile corporațiilor – 47% din traficul global, marcând o creștere cu 1,27 puncte procentuale față de anul precedent – a fost spam. În timp ce spamul include diferite amenințări prin e-mail, inclusiv cele menționate mai sus, nu este întotdeauna rău intenționat și constă în mare parte din reclame nesolicitate. Experții observă că tendințele spam-ului corporativ din ultimul an prezintă în mod proeminent reclame pentru soluții AI, seminarii web aferente, servicii de promovare online, scheme de creștere a numărului de followers și multe altele.

Gardianul Silențios al Bankingului Digital: De Ce Aplicația Ta Are Nevoie de App Protector Acum

În era în care conexiunile digitale dictează ritmul industriei bancare, aplicațiile mobile au devenit principala poartă de acces către serviciile financiare.

#AppProtector

Dar aceste facilități consumate de clienții bancari atrag și interesul persoanelor rău intenționate. Iar băncile nu-și pot permite să fie luate prin surprindere.

Aici intră în scenă **App Protector** dezvoltat de ASEE – o soluție de ultimă generație, creată pentru a **proteja aplicațiile mobile bancare împotriva amenințărilor, înainte ca acestea să se materializeze,** consolidând în același timp încrederea clienților și reziliența instituției.

Protecție Inteligentă. Reacție Instantanee.

"Ce diferențiază App Protector este capacitatea sa de detecție a amenințărilor în timp real, direct pe dispozitivul pe care sunt instalate aplicatiile bancare mobile. Nu așteaptă să se producă un atac. În schimb, identifică proactiv anomalii precum root-area dispozitivului, injecții malițioase sau cititoare de ecran neautorizate – garantând că aplicația bancară mobilă rămâne permanent sub protecție", declară Alina Enache, Sales Manager, Banking Business Unit, ASEE România.

Funcționalități cheie:

- **Detecție fără întârziere:** Securitate în momentul critic.
- **Protecție offline:** Siguranță chiar și în lipsa conexiunii la internet.
- **Vizibilitate granulară:** Analiză în timp real a amenințărilor pentru aplicațiile mobile.
- **Impact minim asupra UX-ului:** nu afectează performanța aplicației și experiența utilizatorului.
- **Integrare rapidă:** Implementare fără blocaje.

Atacurile Nu Mai Sparg Uși. Se Autentifică.

În peisajul digital actual, infractorii cibernetici nu mai forțează intrarea – se conectează. De la aplicații false până la atacuri prin overlay de ecran, App Protector este construit pentru a **detecta și bloca noi vectori de amenințare**, încă din stadiul incipient.

Gata Pentru Conformitate. Proiectat Pentru Încredere.

Cu App Protector, băncile nu își protejează doar infrastructura și clienții – ci și **răspund proactiv exigențelor de conformitate** precum PSD2, GDPR și reglementărilor de securitate.
Este o soluție tehnologică adaptată cerințelor reale ale transformării digitale din sectorul bancar.

De Ce Este Esențial Acum

Se estimează că, în 2025, peste 4,2 miliarde de utilizatori la nivel global vor folosi aplicații de mobile banking. În acest context, o singură breșă de securitate poate genera pierderi financiare de peste 4 milioane de dolari în medie, alături de daune de imagine greu de reparat. Securitatea nu mai este opțională – este un avantaj competitiv esențial.

Nu Aștepta Atacul. Protejează-ți Aplicația Acum

Într-o lume în care atacurile cibernetice se produc în milisecunde, **apărarea nativă, în timp real, devine esențială.** App Protector îți oferă exact acest lucru: o barieră inteligentă între datele tale și pericolele invizibile.

Fii cu un pas înaintea amenințărilor – descoperă App Protector acum în strategia ta digitală – pentru că aplicația ta merită mai mult decât un firewall. Merită o fortăreață.

Backlink: https://cybersecurity.asee.io/downloads/app-protector-datasheet/

De ce Confluence este soluția ideală pentru gestionarea parolelor?

Lumea digitală este într-o continuă mișcare, un workflow sigur și productiv este o nevoie de bază a companiilor ce vor să rămână competitive.

Indiferent că este vorba de o echipă mică sau o companie mare, platforma Confluence din suita Atlassian este soluția ideală de a îmbunătăți productivitatea dintre echipe. Aceasta oferă nu doar un spațiu de partajare a informațiilor între membri, dar asigură și o gestionare eficientă a parolelor. Crearea unui mediu de lucru sigur este important pentru succesul pe termen lung. Securizarea informațiilor, pe lângă protejarea datelor, contribuie și la încrederea părților implicate, fie ele angajați sau clienți.

Gestionarea defectuoasă a parolelor. Cum te poate ajuta Confluence?

Un număr mare de parole de gestionat sau utilizarea unor parole slabe pot compromite securitatea datelor într-o companie. Confluence, fiind o platformă colaborativă, permite gestionarea securizată a informațiilor prin:

- crearea de pagini protejate, accesibile membrilor autorizați;
- autentificare multifactorială (MFA), asigurând un nivel suplimentar de securitate;
- permisiuni avansate, unde pot fi setate drepturi de acces pentru vizualizarea și/ sau editarea informațiilor;
- notificări automatizate în privința actualizării parolelor și a credențialelor.

În acest fel, Confluence este o soluție eficientă de gestionare parole, integrată într-o platformă care devine un hub central de partajare a resurselor și informațiilor unui business.

Avantaje ale utilizării platformei Confluence

Măsurile de securitate oferite de Confluence asigură protecția datelor și, în același timp, o colaborare eficientă pentru ca echipele să își poată atinge obiectivele. Astfel, platforma devine un instrument menit să îmbunătățească experiența utilizatorului și să optimizeze procesele de lucru:

- îmbunătățirea productivității prin metode avansate de autentificare: se reduce timpul de căutare a parolelor, se elimină stresul apărut în urma uitării parolelor și, în felul acesta, utilizatorii alocă mai mult timp concentrându-se pe sarcinile avute;
- proces de colaborare între echipe mai eficient printr-un sistem de permisiuni bine definit: datele sunt partajate în funcție de necesitate, iar echipele pot lucra fără grija de a compromite alte date care nu țin de activitatea lor;
- acces controlat prin care utilizatori autorizați pot vizualiza sau edita informații.

Confluence, un pas către un workflow sigur și eficient

În mediul de afaceri, informația circulă rapid și riscurile în ceea ce privește securitatea datelor este mult mai mare. Implementarea unui sistem de permisiuni eficient care să asigure o gestionare mult mai ușoară a parolelor poate optimiza întregul proces de lucru, de la colaborarea dintre utilizatori până la protejarea datelor. Asigurarea unui sistem de permisiuni va duce la îmbunătățirea performanței per total în cadrul unei organizații.

De asemenea, Confluence ajută la o mai mare clarificare a rolurilor și responsabilităților membrilor unei echipe, reducând astfel suprapunerea de sarcini și confluzia. În același timp, această comunicare permisă de platformă între utilizatori sporește nivelul de satisfacție al angajaților prin autonomia pe care aceștia o au în îndeplinirea obiectivelor.

Dacă vrei să afli cum poți integra Confluence în fluxul tău de lucru, programează o discuție cu echipa Life in Codes la lifeincodes.com pentru a primi răspunsuri și sfaturi personalizate.

Nu uita să te abonezi la **newsletter-ul** lor pentru a fi la curent cu ultimele noutăți!

Vizitează **https://lifeincodes.com/blog/**

Evoluția AI în atacurile de tip phishing: de ce chiar și cei mai experimentați pot deveni victime

Evoluția AI nu afectează doar diverse industrii, dar a transformat și tacticile infractorilor cibernetici. O tendință alarmantă este utilizarea inteligenței artificiale pentru a perfecționa înșelătoriile de tip phishing, rafinarea acestora, țintirea unor persoane specifice, făcând aceste atacuri aproape imposibil de detectat.

Kaspersky analizează modul în care inteligența artificială transformă industria phishing-ului și de ce chiar și cei mai bine pregătiți angajați în domeniul cibernetic cad victime acestor escrocherii. Potrivit unui studiu recent Kaspersky, numărul de atacuri cibernetice suferite de organizații în ultimele 12 luni a crescut cu aproape jumătate. Această creștere a volumului atacurilor a fost observată de 49% dintre respondenții studiului. Cea mai răspândită amenințare a venit din atacurile de tip phishing, 49% dintre cei chestionați raportând acest tip de incident. Pe măsură ce AI devine un factor favorizant mai răspândit pentru infractorii cibernetici, jumătate dintre respondenți (50%) anticipează o creștere semnificativă a numărului de atacuri de tip phishing. Experții Kaspersky au analizat modul în care inteligența artificială este utilizată în atacurile de tip phishing și de ce experiența, de una singură, nu este întotdeauna suficientă pentru a evita să devii victimă. Anterior, atacurile de tip phishing se bazau pe un mesaj generic trimis în masă către mii de persoane, în speranța că unul dintre destinatari va cădea în capcană. AI a schimbat acest lucru prin scriptarea e-mailurilor de phishing în forme extrem de atent personalizate, distribuite în număr mare. Folosind informații disponibile public, precum cele de pe rețelele sociale, platformele de joburi și site-urile

companiilor, aceste instrumente alimentate de inteligența artificială pot genera e-mailuri personalizate în funcție de rolul, interesele și stilul de comunicare al unei persoane. De exemplu, un CFO poate primi un e-mail fraudulos care reflectă tonul și formatarea mesajelor CEO-ului său, inclusiv referințe exacte la evenimentele recente ale companiei. Acest nivel de personalizare face extrem de dificil pentru angajați să distingă între comunicările legitime și cele rău intenționate.

AI a introdus, de asemenea, deepfake-uri în arsenalul de phishing. Acestea sunt din ce în ce mai mult valorificate de infractorii cibernetici pentru a crea mesaje audio și video false, dar extrem de precise, concepute pentru a reda vocea și înfățișarea directorilor pe care doresc să-i imite. De exemplu, într-un caz raportat, atacatorii au folosit un deepfake pentru a uzurpa identitatea mai multor membri ai personalului în timpul unei conferințe video, convingându-l pe angajat să transfere aproximativ 25,6 milioane de dolari. Pe măsură ce tehnologia deepfake continuă să avanseze, este de așteptat ca astfel de atacuri să devină mai frecvente și mai greu de detectat.

Infractorii cibernetici pot manipula scripturile sistemelor tradiționale de filtrare a e-mailurilor cu ajutorul inteligenței artificiale. Analizând și imitând tiparele legitime de e-mail, e-mailurile de phishing generate de AI pot ocoli detectarea software-ului de securitate. Algoritmii de învățare automată pot testa și rafina campaniile de phishing în timp real, sporindu-le ratele de succes și făcându-le din ce în ce mai sofisticate.

Chiar și angajații cu experiență pot cădea victime ale acestor atacuri avansate de phishing. Nivelul de realism și personalizare pe care AI îl poate atinge poate trece peste scepticismul care îi face precauți pe profesioniștii cu experiență. Mai mult, atacurile generate de AI exploatează adesea psihologia umană, cum ar fi sentimentul de urgență, frica sau autoritatea, presând angajații să acționeze fără a verifica de două ori autenticitatea cererii.

Pentru a se apăra împotriva atacurilor de phishing susținute de inteligență artificială, organizațiile trebuie să adopte o abordare proactivă și pe mai multe straturi care să pună accent pe securitatea cibernetică cuprinzătoare. Instruirea regulată și actualizată în ceea ce privește conștientizarea securității cibernetice axate pe inteligența artificială este esențială pentru angajați, ajutându-i să identifice semnele subtile de phishing și alte tactici rău intenționate. Pe lângă aceasta, companiile ar trebui să implementeze instrumente de securitate robuste, capabile să detecteze anomalii în e-mailuri, cum ar fi modele de scriere neobișnuite sau metadate suspecte.

Un model de securitate de tip zero-trust joacă, de asemenea, un rol esențial în minimizarea pagubelor potențiale ale unui atac reușit. Prin restricționarea accesului la date și sisteme sensibile, această abordare se asigură că, indiferent dacă atacatorii încalcă un nivel de securitate, nu pot compromite întreaga rețea. Împreună, aceste măsuri creează o strategie de apărare cuprinzătoare, combinând tehnologia avansată cu supravegherea umană vigilentă.

Costul ascuns al confortului

Compromisurile de confidențialitate sunt adesea trecute cu vederea atunci când utilizăm aplicații populare. Acestea includ aplicațiile de social media, dar și altele, cum ar fi aplicațiile de comerț electronic, de fitness și de monitorizare a sănătății. Deși aceste aplicații aduc un plus de confort, ele colectează și distribuie cantități uriașe de date personale, expunând utilizatorii la profilare invazivă și la potențiale riscuri de securitate.

Odată cu evoluția urmăririi datelor bazate pe inteligență artificială și a analizei predictive, riscurile legate de confidențialitate asociate cu aceste aplicații sunt mai importante ca niciodată.

Multe dintre aplicațiile pe care le folosim zilnic, adesea fără să ne dăm seama, colectează în liniște informații sensibile. Unele dintre cele mai îngrijorătoare categorii includ aplicații de social media precum TikTok, Instagram și Threads, care colectează în mod constant date despre locația unui utilizator, obiceiurile de navigare ale acestuia și chiar date vocale. Aplicațiile de socializare bazate pe video sau fotografii, pot folosi inteligența artificială pentru a accesa galeriile foto și a analiza imaginile și metadatele încorporate, putând determina localizarea dumneavoastră geografică.

Aplicațiile de cumpărături sunt, de asemenea, folosite pentru a colecta date referitoare la istoricul achizițiilor, locația și chiar prezența offline în apropierea magazinelor fizice. La fel ca aplicațiile de social media, retailerii pot urmări mișcările noastre atât online, cât și offline, creând un profil detaliat al obiceiurilor și comportamentului nostru de consum.

Aplicațiile de sănătate și fitness contribuie și mai mult la crearea unui profil detaliat al unui utilizator, colectând unele dintre cele mai intime date personale ale noastre, inclusiv indici de sănătate și rutine zilnice care pot fi partajate cu terți.

Nu uitați să verificați permisiunile aplicațiilor, să utilizați instrumente axate pe confidențialitate, să solicitați aplicațiilor să nu urmărească datele dispozitivului dumneavoastră, să evitați conexiunile Wi-Fi publice și să examinați setările aplicațiilor. Majoritatea utilizatorilor de smartphone-uri au zeci de aplicații instalate, dar folosesc zilnic doar un număr redus dintre acestea.

Consolidarea securității identității

Trecerea în cloud poate ajuta organizațiile să îmbunătățească colaborarea, să reducă costurile și să opereze mai eficient. Dar poate introduce și noi vulnerabilități de securitate, poate provoca departamente IT și poate întrerupe procesele care rulau folosind resurse locale.

Mai mult, organizațiile care trebuie să îndeplinească cerințele de certificare a modelului de maturitate a securității cibernetice (CMMC 2.0) sau a cerințelor Guvernanței Community Cloud (GCC) se confruntă cu obstacole suplimentare care pot face ca trecerea la cloud să fie un proces lent, costisitor și agravant.

De aceea, RSA lucrează cu Microsoft pentru a securiza și accelera migrarea în cloud. Integrarea RSA External Authentication Method (EAM) poate ajuta utilizatorii Microsoft să treacă în cloud în siguranță, să-și dezvolte maturitatea Zero Trust și să câștige mai multă valoare din resursele locale.

Ce este EAM

În 2024, Microsoft a recunoscut că clienții săi ar putea dori să folosească capacități de securitate suplimentare pentru a proteja identitățile utilizatorilor.

Integrarea EAM permite organizațiilor să facă exact asta: integrarea RSA EAM permite organizațiilor să protejeze accesul la resursele Microsoft folosind **RSA ID Plus**. Integrarea, care a fost deja implementată de sute de clienți comerciali și guvernamentali, le permite clienților să implementeze capabilități de autentificare fără parolă, rezistente la phishing, precum protocoalele FIDO2, biometria și autentificarea cu coduri QR, în medii cloud și hibride.

RSA EAM asigură că organizațiile pot aduce aproape toate capabilitățile RSA pentru procesele de autentificare și conectare.

Acest lucru este deosebit de remarcabil pentru evenimentele cu risc ridicat, cum ar fi recuperarea acreditărilor și înscrierea securizată. Folosind RSA ID Plus, utilizatorii se pot înscrie fără probleme și în siguranță în organizația lor cu **verificarea identității (IDV)**, menținând în același timp un nivel ridicat de asigurare a identității.

Acest lucru este deosebit de valoros pentru instituțiile de servicii financiare și alte industrii foarte reglementate, asigurând că fiecare utilizator începe cu o identitate puternică și verificată și protejând întregul ciclu de viață al identității, reducând riscul accesului neautorizat de la început.

Pe măsură ce tot mai multe organizații se deplasează în cloud, asigurarea unei tranziții securizate este o prioritate de top, în special pentru echipele IT care gestionează infrastructurile de autentificare la nivel local.

Această inițiativă este deosebit de provocatoare pentru organizațiile care explorează Entra ID. Soluția Microsoft nu acceptă resurse locale: organizațiile ar trebui să mute imediat toate resursele, datele și aplicațiile în cloud pentru a implementa Entra ID. Acest lucru ar presupune probabil o revizuire completă a infrastructurii lor existente, care necesită resurse substanțiale pentru a migra aplicațiile și datele. Acest proces poate consuma mult timp și poate introduce noi vulnerabilități.

Soluția RSA EAM abordează această problemă permițând organizațiilor să continue să folosească autentificatoarele existente la nivel local, în timp ce se extind în cloud, minimizând întreruperile asociate cu o astfel de tranziție majoră. Cu **70%** din organizații care operează în medii hibride, organizațiile ar trebui să fie capabile să securizeze toți utilizatorii din toate mediile – fără a avea infrastructura IT sau luarea deciziilor dictate de limitările furnizorilor.

Echipele IT pot folosi RSA EAM pentru a proteja accesul la cloud folosind autentificatoare locale securizate, oferind continuitate și securitate pe parcursul tranziției lor către cloud și flexibilitatea de a trece la cloud în propriul ritm. Cu RSA EAM, echipele IT își pot menține investițiile în metodele de autentificare existente în timp ce își extind raza de acțiune la aplicațiile cloud securizate – făcând călătoria către cloud sigură, fluidă și mai eficientă.

RSA EAM poate ajuta organizațiile să respecte cerințele Microsoft de autentificare multifactor (MFA) pentru conectarea și autentificarea Azure. Prin integrarea RSA EAM în procesele lor de conectare și autentificare, organizațiile se pot asigura că mediile lor rămân securizate și își menținutilizatorii conectați la serviciile de care au nevoie.

Pentru contractanții guvernamentali și organizațiile care manipulează informații sensibile, atingerea conformității cu standardele înalte GCC este crucială. Integrarea RSA EAM îndeplinește aceste cerințe stricte, menținând în același timp flexibilitatea pentru utilizatorii care accesează mediile Azure și Office de la punctele finale non-GCC.

Integrarea RSA EAM ajută organizațiile să îndeplinească mai multe cerințe CMMC 2.0, în special cele legate de controlul accesului și autentificarea cu mai mulți factori (MFA). Iată cum RSA se aliniază acestor nevoi de conformitate:

• **Controlul accesului (AC.L2-3.1.3):** RSA EAM permite MFA securizat pentru conturile privilegiate, cum ar fi conturile de conectare la Azure și conturile administrative. Această capacitate ajută organizațiile să protejeze sistemele sensibile și să respecte această cerință critică de control al accesului.

• **Identificare și autentificare (IA.L2-3.5.3):** EAM RSA oferă infrastructura necesară pentru a îndeplini această cerință prin integrarea cu Microsoft, asigurând acces sigur la resursele critice.

• **Controlul accesului (AC):** Acest lucru ajută organizațiile să impună MFA în mod consecvent între utilizatori, aliniindu-se la cerințele CMMC 2.0.

Aceste cerințe sunt concepute pentru a spori securitatea informațiilor sensibile prin asigurarea unor practici solide de verificare a identității. Cu capabilitățile MFA cuprinzătoare ale RSA și integrarea puternică cu Microsoft, organizațiile pot atinge conformitatea cu CMMC 2.0, avansând în același timp maturitatea Zero Trust și reducându-și suprafața de atac.

Când liderii de securitate se gândesc la „mai bine împreună", ei se gândesc la soluții care funcționează perfect pentru a elimina golurile, a reduce riscurile și a crea o experiență mai simplă.

Este exact ceea ce RSA și Microsoft au oferit cu această integrare: capacitatea de a oferi o securitate robustă a identității, care îndeplinește cerințele critice de conformitate, adăugând în același timp un nivel de încredere pentru cei care au cea mai mare nevoie. Folosind integrarea RSA EAM împreună cu ID Plus, organizațiile pot aborda cu încredere nevoile de conformitate, pot reduce riscurile și își pot accelera călătoria către o etapă optimă de maturitate Zero Trust.

Această soluție combinată nu numai că oferă securitate puternică, dar oferă și o experiență perfectă pentru administratori și utilizatorii finali, sporind în cele din urmă productivitatea și oferind liniște.

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.

Malware-ul de tip stealer ar putea fi responsabil pentru scurgerea a peste 2 milioane de carduri bancare

Experții Kaspersky estimează că aproximativ 2,3 milioane de carduri bancare au fost expuse pe dark web. Deși, la nivel global, procentul cardurilor potențial compromise este sub unu la sută, 95% dintre cazurile analizate par a fi valide din punct de vedere tehnic.
Malware-ul de tip infostealer nu este conceput doar pentru a fura informații financiare, ci și acreditări, cookie-uri și alte date valoroase ale utilizatorilor. Aceste informații sunt compilate în fișiere de tip jurnal și apoi distribuite în comunitățile subterane de pe dark web. Un infostealer poate infecta un dispozitiv dacă victima descarcă și rulează, fără să știe, un fișier malițios, de exemplu, unul deghizat în software legitim, cum ar fi un cheat pentru jocuri. Acesta se poate răspândi prin linkuri de phishing, site-uri compromise, atașamente malițioase în e-mailuri sau mesaje și diverse alte metode, vizând atât dispozitive personale, cât și corporative.

Luptele geopolitice determină creșterea activității ransomware

Volumul înregistrat de atacuri ransomware a crescut cu 19% în octombrie 2024, până la un total de 468 de incidente în întreaga lume, un număr semnificativ dintre acestea în SUA, unde controversatele alegeri prezidențiale probabil i-au încurajat pe actorii amenințărilor vorbitori de limbă rusă să lovească, potrivit ultimului raport lunar al NCC Group, „Threat". **de Bogdan Marchidanu**

Deși amploarea tentativelor de intervenție a statului rus în procesul electoral din SUA nu este încă pe deplin cunoscută, șeful NCC al departamentului de informații despre amenințări, Matt Hull, a spus că nu a fost nicio surpriză în ultimele câteva săptămâni înainte ca sondajul din 5 noiembrie să fi văzut o creștere a activității amenințărilor. .

„Motivațiile geopolitice, precum alegerile din SUA, au arătat că state naționale precum Rusia continuă să aibă o influență puternică asupra volumului global de atacuri cibernetice", a spus el. „Datele arată că asistăm la o dinamică în schimbare a peisajului amenințărilor, cu statele naționale și grupurile criminale organizate colaborând din ce în ce mai mult", a spus Hull. „Întrucât diferiți actori amenințări își valorifică reciproc resursele, este esențial pentru organizații să se asigure că sunt în fruntea practicilor fundamentale de securitate, cum ar fi gestionarea parolelor, securitatea punctelor terminale și autentificarea cu mai mulți factori."

Într-adevăr, împărțită după geografie, regiunea Americii de Nord – care include și țări precum Canada și Mexic – a reprezentat 272, sau 56%, din atacurile ransomware înregistrate. În comparație, 97 de atacuri, 20%, au victimizat organizații din Europa, așa că, în total, peste trei sferturi din toate atacurile ransomware observate luna trecută au vizat aceste două regiuni. Desigur, acest lucru nu este pentru a

exclude restul lumii și, în special, un atac a demonstrat în mod adecvat aparenta estompare a liniilor dintre statele naționale și criminalii organizați. Acesta a fost un incident în care sistemele gigantului japonez de electronice Casio au fost afectate de ransomware-ul Underground, care este legat de grupul rus de criminalitate cibernetică Storm-0978 sau RomCom.
Atacul dublu de extorcare a vizat datele angajaților, candidaților și partenerilor de afaceri și a cauzat și întreruperi ale serviciilor. Probabil a început prin CVE-2023-36884, un vuln de execuție de cod de la distanță în Microsoft Office, despre care se știe că a fost vizat de actori de stat ruși; și conform NCC, se crede că RomCom este una dintre numeroasele bande care efectuează atacuri în numele Kremlinului.
NCC a spus că tensiunea geopolitică tot mai mare dintre Rusia și Japonia a adăugat un strat „convingător" incidentului. Rusia, care deține insula Sakhalin – parte a patriei ancestrale a poporului indigen Ainu din Japonia – și insulele Kurile din apropiere, de la sfârșitul celui de-al Doilea Război Mondial, se crede că sunt preocupate de colaborarea militară din ce în ce mai mare a Japoniei cu alianța NATO, iar Moscova a protestat împotriva unui exercițiu militar comun recent, Keen Sword 2024, între SUA și Japonia.
„Aceste activități militare și postura de apărare consolidată a Japoniei ar fi putut contribui la o creștere a tacticilor agresive din partea entităților cibernetice afiliate Rusiei", au scris autorii raportului.
Atacurile asupra companiilor japoneze ar putea servi ca o formă de presiune sau de răzbunare, semnalând nemulțumirea Rusiei față de strategiile de apărare ale Japoniei. Prin țintirea unor întreprinderi cheie japoneze, Rusia, prin intermediul unor grupuri criminale cibernetice afiliate, ar putea urmări să perturbe stabilitatea economică și să proiecteze puterea fără o confruntare militară deschisă.
Situația arată complexitatea războiului cibernetic modern, în care întreprinderile criminale și actorii susținuți de stat ar putea urmări atât obiective financiare, cât și strategice… Ca atare, întreprinderile ar trebui să cuprindă o varietate de amenințări, tradiționale și susținute de stat, în strategia lor de apărare.
În ceea ce privește cei mai prolifici operatori de ransomware, RansomHub a fost cel care și-a continuat dominația ca cea mai activă bandă în octombrie, asumându-și responsabilitatea pentru 68 de atacuri, deși aceasta a scăzut puțin față de luna anterioară.
Locul al doilea a fost deținut de Play, care a reprezentat aproximativ 55 de atacuri; urmat de Killsec, cu intre 30 si 40; Sarcom, cu aproximativ 30; și Meow, cu vreo 25.
Restul celor mai active 10 operațiuni luna trecută au fost Fog, Hunters, ElDorado, Medusa și BlackSuit.
În general, sectorul industrial, care include operatorii de infrastructură națională critică (CNI), a rămas cel mai vizat, reprezentând 148, sau 30%, dintre atacurile observate. Consumar a urmat sectorul discreționar (retail), cu 100 de atacuri; iar sectorul sănătății a reprezentat 55.
„După cum s-a demonstrat prin concentrarea asupra CNI, atacurile devin mai puțin aleatorii și mai direcționate către organizațiile care vor avea un impact maxim", a spus Hull. „Cei care se bazează pe „uptime" și dețin cantități mari de proprietate intelectuală sau informații de identificare personală sunt ținte de mare valoare."

AI și securitatea cibernetică cresc cheltuielile IT

O analiză de piață Forrester a estimat că organizațiile din Europa vor crește cheltuielile IT cu 5% în 2025. Conform previziunii tehnologice globale 2024-2029 a firmei de analiză, cheltuielile vor ajunge la 4,9 miliarde de dolari în 2025, cu investiții accelerate în inteligența artificială (AI), securitatea cibernetică și infrastructura cloud. AI generativ (GenAI), securitatea cibernetică și serviciile cloud sunt gata să stimuleze creșterea cu 5,6% în 2025, față de 4,6% în 2024.
Europa urmează să cheltuiască mai puțin decât SUA și Asia Pacific ca proporție din produsul intern brut (PIB). Cercetările de la Forrester arată că SUA au reprezentat 41% din cheltuielile globale în domeniul tehnologiei și 46% din cheltuielile cu software-ul AI în 2024. Aproape 70% dintre primele 24 de companii care au înregistrat cea mai rapidă creștere din 2015 până în 2023 provin din SUA, iar mai mult de jumătate dintre acestea sunt companii media și informaționale.
Prognoza Forrester arată că cheltuielile tehnologice din Asia Pacific vor crește cu 5,6% în 2025. Analistul prezice că regiunea Asia Pacific va fi martora la o creștere a PIB-ului real care va depăși cu mult media globală, condusă de țări precum India, Filipine, Vietnam și Indonezia. Inițiativele guvernamentale din
China și India și investițiile sporite în GenAI și semiconductori în Japonia și Coreea de Sud vor contribui la creșterea cheltuielilor tehnologice. India va avea cea mai rapidă creștere, cheltuielile tehnologice fiind așteptate să crească cu 9,6% în 2025.
Potrivit Forrester, software-ul și serviciile IT combinate vor reprezenta 66% din cheltuielile globale pentru tehnologie în 2025, alimentate de investițiile sporite în serviciile de securitate cibernetică și modernizarea sistemelor vechi. Numai software-ul va crește cu o rată de 10,5% și se așteaptă să capteze 60% din creșterea cheltuielilor globale în domeniul tehnologiei până în 2029, devenind astfel sectorul tehnologic cu cea mai rapidă creștere.

LifeinCloud Security Framework

Securitate IT integrată. Infrastructură sub control. Reziliență digitală reală.

Într-o eră a atacurilor cibernetice tot mai sofisticate organizațiile nu mai pot miza pe soluții reactive. Este timpul pentru o abordare completă, proactivă, scalabilă și mai ales, adaptată la realitățile fiecărei infrastructuri.

Alexandru Trifu,
Chief Sales Officer LifeinCloud

Din această nevoie s-a născut LifeinCloud Security Framework, un model integrat de securitate IT care combină infrastructura noastră de tip cloud privat, serviciile MSP & MSSP, precum și bunele practici confirmate de experiența acumulată in cei 16 ani de activitate.

Într-un articol recent, spuneam că deciziile bune se iau pe baza cunoștințelor, nu a consecințelor. Această filozofie ghidează și structura LifeinCloud Security Framework: deciziile privind securitatea IT nu trebuie luate sub presiunea unui incident, ci dintr-o poziție de control, vizibilitate și competență tehnologică.

1. Infrastructura: Cloud Privat creat pentru securitate:

Cloud-ul privat LifeinCloud este construit pe un model de izolare completă, control granular și vizibilitate totală.

Caracteristici tehnice:

- găzduit în centrul de date propriu din București și cu puncte de prezență în Londra și Frankfurt.
- platformă orchestrată cu Apache CloudStack, sistem de stocare distribuit Ceph.
- rețele complet segmentate, VLAN dedicat, firewall perimetral și intern.
- criptare end-to-end pentru stocare și transmisie.
- politici de tip Zero Trust, autentificare multifactor (MFA), control pe bază de roluri (RBAC).
- integrare cu soluții de backup și disaster recovery, replicate geografic.

Beneficii de business:

- control total asupra infrastructurii IT, fără compromisuri de conformitate.
- costuri predictibile și scalare flexibilă în funcție de nevoi.
- suport complet pentru cerințe de audit, GDPR, ISO 27001.
- reziliență crescută în fața atacurilor ransomware și a incidentelor operaționale.

2. Servicii gestionate – MSP: infrastructură operată profesionist:

Din poziția de "Managed Services Provider", LifeinCloud oferă clienților operarea integrală a infrastructurii IT, de la nivel de server și rețea, până la backup, patching și monitorizare.

Caracteristici:

- suport tehnic și monitorizare 24/7 cu SLA garantat.
- monitorizare proactivă a performanței sistemelor.
- managementul actualizărilor și al ciclului de viață software.
- automatizare operațională și scripturi de remediere remote.

Beneficii:

- eficiență operațională fără a crește costurile interne.
- echipele IT interne pot fi concentrate pe inovare, nu pe mentenanță.
- timp de disponibilitate garantat (uptime SLA 99.99%).

3. Servicii de securitate gestionată – MSSP: protecție continuă, prevenție

LifeinCloud oferă servicii de tip "Managed Security Services Provider", care adaugă un strat activ de protecție cibernetică peste orice infrastructură IT.

Caracteristici:

- monitorizare continuă a incidentelor de securitate (SIEM/XDR).
- integrare cu Bitdefender GravityZone, firewall-uri inteligente, IDS/IPS.
- detecție comportamentală, învățare automată (machine learning) pentru anomalii.
- simulări de atac, audituri de securitate, consultanță pentru remediere.

Beneficii:

- răspuns rapid la amenințări – timp mediu de detecție și remediere, sub 10 minute.
- vizibilitate completă asupra riscurilor și a vulnerabilităților.
- aliniere cu cerințele de securitate ale industriilor reglementate (financiar, medical, public).

4. Backup și Disaster Recovery:

Orice sistem de securitate este incomplet fără o strategie de continuitate.

Caracteristici:

- backup-uri criptate, automate, replicate geografic.
- teste periodice de restaurare.
- RTO/RPO personalizate în funcție de criticitatea sistemelor.

Beneficii:

- continuitate operațională indiferent de context.
- recuperare rapidă în caz de atac ransomware.
- conformitate cu standardele internaționale.

5. Studiu de caz: Cloud Privat + MSSP pentru un client din domeniul financiar:

Un client din industria financiară, cu cerințe stricte de conformitate (GDPR, PCI-DSS), a migrat întreaga infrastructură IT într-un cloud privat LifeinCloud găzduit în centrul din Frankfurt.

Proiectul a inclus:

- izolarea completă a rețelei și segmentarea pe zone de încredere;
- integrarea cu Bitdefender GravityZone XDR pentru detecție avansată;
- monitorizare non-stop a comportamentului infrastructurii;
- plan de backup și DR replicat în București.

La două luni de la migrare, a fost detectată o tentativă de atac tip credential stuffing asupra unei aplicații interne. Sistemul XDR a blocat conexiunile suspecte, iar echipa MSSP LifeinCloud a aplicat o remediere completă în mai puțin de 10 minute, fără impact asupra serviciilor de producție. Raportul de incident a fost folosit pentru ajustarea politicilor de acces și îmbunătățirea nivelului de securitate.

Rezultat: clientul a redus riscurile de securitate cu peste 80%, și-a crescut disponibilitatea aplicațiilor critice și a obținut certificarea ISO 27001.

Prin intermediul soluției complete "LifeinCloud Security Framework", companiile nu doar se protejează, ci se pregătesc pentru viitor. Combinăm robustețea infrastructurii noastre de cloud privat cu flexibilitatea operațională a serviciilor gestionate și vigilența continuă a MSSP, pentru a crea un ecosistem IT antifragil, sigur și adaptabil.

"Securitatea nu mai este opțională. Cu LifeinCloud, devine fundamentală".

Conformarea la directiva de securitate cibernetică NIS2 a intrat în linie dreaptă

Companiile din România care activează în sectoarele esențiale și critice pentru societate și economie, respectiv energie, transport, sănătate, financiar-bancar, apă potabilă și infrastructură digitală, precum și din alte domenii considerate importante precum serviciile poștale și de curierat, gestionarea deșeurilor, industria chimică sau cea alimentară trebuie să se conformeze prevederilor directivei europene NIS2 privind securitatea cibernetică.

Entitățile care fac obiectul NIS2 trebuie să aibă în vedere îmbunătățirea atât a măsurilor lor de gestionare a riscurilor de securitate cibernetică, cât și a programelor de raportare a incidentelor, pentru a se conforma cerințelor impuse. Nerespectarea NIS2 poate conduce la amenzi semnificative din partea autorităților, dar și la costuri semnificative pentru organizații.

Pentru a se pregăti, entitățile vizate de NIS 2 trebuie să ia în considerare: stabilirea unui cadru de guvernanta privind securitate cibernetică care să acopere toate aspectele identificarea, evaluarea și gestionarea riscurilor, actualizarea periodică a politicilor de securitate IT, implementarea unor controale stricte referitoare la accesul la date, microsegmentarea, adoptarea unor tehnologii (avansate) de detecție și răspuns aliniate la obiectivele și principalele zone de risc ale business-ului, proceduri clare de raportare a incidentelor, detectare și monitorizare automatizată în timp real sau periodic, formarea continuă a personalului, înregistrarea detaliată a incidentelor de securitate cibernetică, evaluări regulate ale riscurilor și audituri. Implementarea acestor măsuri va sprijini un management integrat al riscurilor la nivelul companiei.

Măsurile luate trebuie să asigure un nivel de securitate cibernetică adecvat nivelului de risc al entității, care se evaluează conform metodologiei cuprinse în ordinul directorului DNSC. De asemenea, entitățile

esențiale și cele importante sunt obligate să se supună efectuării unui audit de securitate cibernetică în condițiile și cu periodicitatea stabilite de DNSC, în funcție de nivelul de risc.
Companiile vizate trebuie să raporteze, fără întârzieri nejustificate, orice incident care are un impact semnificativ asupra prestării serviciilor lor prin intermediul Platformei naționale pentru raportarea incidentelor de securitate cibernetică – PNRISC. Astfel, trebuie să raporteze nu mai târziu de 24 de ore de la data la care au luat cunoștință de incidentul semnificativ, o avertizare timpurie care, după caz, dacă există suspiciuni că incidentul este cauzat de acțiuni ilicite sau răuvoitoare sau că ar putea avea un impact transfrontalier sau nu mai târziu de 72 de ore din momentul în care au luat cunoștință de incidentul semnificativ dacă prezintă o evaluare inițială a acestuia, inclusiv a gravității și a impactului acestuia, precum și a indicatorilor de compromitere.
Un incident este considerat semnificativ sau impactul unui incident este considerat semnificativ dacă a provocat sau poate provoca perturbări operaționale grave ale serviciilor sau pierderi financiare pentru entitatea în cauză, a afectat sau poate afecta alte persoane fizice sau juridice, cauzând prejudicii materiale sau nonmateriale considerabile.
DNSC poate derula activități de supraveghere, verificare și control efectuate de persoane desemnate în acest sens și poate dispune efectuarea de audituri de securitate ad-hoc, realizate de un auditor de securitate cibernetică atestat.
Următoarele fapte constituie încălcări grave: neîndeplinirea obligației de notificare sau de remediere a incidentelor semnificative, neîndeplinirea obligației de remediere a deficiențelor constatate de către autoritățile competente, obstrucționarea auditurilor sau a activității de monitorizare dispuse de DNSC în urma constatărilor, furnizarea de informații false sau vădit denaturate, îngrădirea accesului personalului desemnat de către DNSC în spațiile supuse controlului, cât și asupra datelor și informațiilor necesare controlului, etc.
Vor fi aplicate contravenții pentru nerespectarea, printre altele, a obligațiilor privind luarea unor măsuri tehnice, operaționale și organizatorice, de a se supune unui audit de securitate cibernetică în condițiile stabilite, de a transmite datele solicitate, de a realiza și transmite anual autoevaluarea nivelului de maturitate, de a întocmi și transmite planul de măsuri pentru remedierea deficiențelor, în termen de 30 de zile de la realizarea autoevaluării, de a pune în aplicare măsurile de gestionare a riscurilor, de a urma cursuri de formare profesională în domeniul securității cibernetice, etc

Softlead & Blackshell pregătesc companiile din România pentru alininierea la Directiva de securitate NIS 2

Softlead, singura platformă de tip marketplace din România care ajută companiile să aleagă soluția software potrivită, pe baza ADN-ului Digital, anunță semnarea unui parteneriat strategic cu Blackshell, companie de securitate românească, ce le oferă companiilor și instituțiilor publice acces la soluții software dedicate protecției cibernetice.
Obiectivul parteneriatului: educarea și protejarea companiilor mici și mijlocii în fața vunerabilităților cibernetice
Prin acest parteneriat, cele două companii își propun să contribuie la informarea și educarea a peste 10.000 de companii din România din cele mai expuse domenii de activitate despre modul în care pot folosi soluții software avansate, prietenoase cu utilizatorii, în vederea prevenirii amenințărilor și vulnerabilităților cibernetice.
Astfel, prin platforma Softlead, Blackshell le va oferi companiilor din România acces la o serie de instrumente prin care acestea pot testa gradul de vulnerabilitate la care se expun în mediul online sau în contextul propriei infrastructuri de la birou, precum și soluții de securitate dedicate, utile indiferent de mărimea companiei sau de industria din care face parte.
Portofoliul de produse Blackshell cuprinde soluții de securitate VPN, protecţii anti-phishing și anti scurgere a datelor, scanarea continuă a vulnerabilităților, precum și instrumente de analiză și auditare extrem de utile în stabilirea unei strategii de protecție.
Aplicațiile Blackshell pot deveni populare în rândul companiilor din România inclusiv prin partenerii IT prezenți pe platforma Softlead, cele peste 740 de entități software având posibilitatea de a deveni reselleri ai soluțiilor. În acest sens, Blackshell propune un program de parteneriat dedicat furnizorilor de servicii integrate, oferind acces la o infrastructură modernă, sigură și facilă.
Tot mai multe companii sunt atrase de tehnologiile avansate la care accesul devine tot mai facil de la o zi la alta. Acesta este și motivul pentru care atacurile cibernetice nu mai sunt o prioritate doar pentru companiile mari, ci pentru orice entitate care deține echipamente și infrastructuri tehnice, ce pot reprezenta puncte de atracție pentru atacatori. De aceea, parteneriatul strategic inițiat între Softlead și Blackshell este un pas esențial în sprijinirea companiilor să ia decizii corecte și informate în contextul protecției datelor și angajaților”– **Alexandra Roată, Co-Founder Softlead**.
Implementarea Directivei este urgentată de creșterea alarmantă a incidentelor de securitate cibernetică. Astfel, conform raportărilor CIRAS (Sistemul de Raportare și Analiză a Incidentelor Cibernetice), în 2023, numărul incidentelor a atins un record de 1.271, de 16 ori mai mare decât în 2012.

5 capabilități care redefinesc managementul fraudelor bancare online

Escrocii devin din ce în ce mai vicleni, iar serviciile bancare online au devenit o țintă principală. În ultimii ani, s-a înregistrat o creștere a atacurilor sofisticate, alimentată de trecerea rapidă la digital în timpul pandemiei.

Menținerea în fața acestor scheme nu mai este opțională pentru bănci și instituții financiare. Clienții cer viteză, simplitate și, mai presus de toate, securitate. Cu mizele atât de mari, o strategie de apărare proactivă nu este doar inteligentă, ci este esențială. Iată cinci capabilități cheie care pot ajuta instituțiile financiare să combată frauda la sursă.

Transparență deplină în fiecare sesiune

Frauda prosperă în punctele moarte. Metodele tradiționale de detectare, cum ar fi scorurile de risc, simplifică realitățile complexe într-o singură măsură, lipsind adesea semnele subtile de pericol.

Obținerea unei **vizibilități complete** înseamnă să vedeți fiecare acțiune dintr-o sesiune de utilizator – fiecare atingere, glisare sau încercare de conectare. Acest nivel de claritate permite răspunsuri precise, oprind amenințările fără a perturba utilizatorii autentici.

Detectare rapidă prin analiză pe mai multe straturi

Frauda nu se anunță. Adesea, este ascuns în modele comportamentale complexe sau anomalii subtile pe dispozitive și canale.

Combinarea tehnologiilor precum biometria comportamentală, verificările integrității dispozitivului și analiza riscului tranzacțional permite identificarea rapidă a amenințărilor. Cu capacitatea **de a analiza mai multe puncte de date în timp real**, analiștii se pot concentra asupra riscurilor reale, reducând zgomotul în câteva minute.

Inteligență care urmărește amenințările

Escrocii își perfecționează în mod constant tactica, făcând din monitorizarea amenințărilor o luptă continuă. A rămâne în avans necesită o analiză continuă și o clasificare a riscurilor emergente.

Prin **valorificarea informațiilor personalizate** privind amenințările, instituțiile își pot prioritiza eforturile în mod eficient, reducând stresul asupra analiștilor și sporindu-le capacitatea de a acționa decisiv. Rezultatul este o echipă mai pregătită și mai puțin copleșită.

Reactivitate în timp real pentru servicii fără întreruperi

În lumea digitală de astăzi, întârzierile sunt costisitoare. Clienții se așteaptă la răspunsuri imediate atunci când accesează servicii, iar detectarea fraudelor nu face excepție.

Dacă sistemele de detectare nu pot ține pasul cu cerințele în timp real, riscă fie să frustreze utilizatorii legitimi, fie să permită fraudei să treacă.

Luarea deciziilor în timp real asigură că **fiecare tranzacție este evaluată instantaneu,** permițând răspunsuri rapide și precise. Aceasta înseamnă experiențe fără probleme pentru clienți și un mediu sigur pentru toată lumea.

Automatizare inteligentă care funcționează pentru dvs

Gestionarea manuală a răspunsurilor la fraudă este ca și cum a reține o inundație cu o găleată. Automatizarea nu este doar

despre eficiență, ci despre precizie.

Prin implementarea unor sisteme inteligente, adaptabile, instituțiile financiare pot stabili **reguli inteligente care să răspundă dinamic** la amenințările în evoluție. Acest lucru nu numai că asigură securitatea, ci și menține operațiunile fluide, chiar și sub presiunea atacurilor la scară largă.

Construiește o apărare pregătită pentru orice

Gestionarea fraudei nu mai înseamnă a reacționa la ceea ce s-a întâmplat deja, ci înseamnă a rămâne înaintea a ceea ce urmează. Cu **combinația potrivită de instrumente și strategii,** instituțiile financiare își pot proteja clienții, reputația și rezultatul final.

Cleafy a ținut cont de acest lucru atunci când a dezvoltat soluția. O soluție care analizează continuu activitățile online pe canalele digitale, combinând mai multe tehnologii de detectare cu date de informații despre amenințări.

Soluţiile Cleafy sunt distribuite în România de compania **SolvIT Networks.**

Controlere compacte și eficiente pentru instalații centralizate cu mai multe uși

Axis Communications lansează două controlere de rețea pentru acces, oferind control complet pentru până la opt uși. Cu alimentare integrată pentru încuietori, aceste controlere all-in-one simplifică instalarea și reduc complexitatea.

AXIS A1710-B permite controlul a până la patru uși, cu suport pentru opt cititoare OSDP și opt încuietori, în timp ce AXIS A1810-B poate gestiona până la opt uși, oferind compatibilitate cu 16 cititoare OSDP și 16 încuietori. Aceste dispozitive compacte, de tip barebone, au un design mai redus ca dimensiuni față de majoritatea controlerelor de acces de pe piață, fiind concepute pentru instalări centralizate.

Datorită sistemului integrat de gestionare a alimentării încuietorilor, aceste controlere simplifică instalările complexe. În plus, conectorii sunt colorați pentru a facilita gestionarea cablurilor.

Cu suport nativ pentru cititoare OSDP și un accesoriu opțional pentru cititoare Wiegand, aceste controlere scalabile și pregătite pentru viitor sunt ideale atât pentru instalații de mici dimensiuni, cât și pentru cele extinse.

Fiecare dispozitiv poate stoca până la 250.000 de acreditări și 250.000 de înregistrări de evenimente. De asemenea, pot fi integrate cu AXIS Camera Station

Secure Entry sau cu soluții ale partenerilor, oferind un sistem complet și scalabil de gestionare video și control al accesului.

Caracteristici principale:

- Control centralizat pentru instalare simplificată
- Control complet pentru până la 8 uși
- Suport integrat pentru până la 16 cititoare OSDP și 16 încuietori
- Certificare OSDP Verified pentru comunicație securizată cu cititoarele
- Funcționalități de securitate cibernetică integrate

Axis Edge Vault, o platformă de securitate cibernetică bazată pe hardware, protejează dispozitivul și informațiile sensibile împotriva accesului neautorizat. De asemenea, asigură stocarea în siguranță a cheilor criptografice în modulul de calcul certificat EAL6+.

Aceste produse sunt OSDP Verified, garantând o comunicație bidirecțională securizată. În plus, oferă autentificare flexibilă și sigură, permițând utilizarea diferitelor tipuri de acreditări.

Funcționalitatea de autentificare multi-factor adaugă un nivel suplimentar de securitate.

Reglementarea DORA: O schimbare a jocului pentru securitatea bancară și rezistența digitală

În ecosistemul financiar interconectat de astăzi, perturbările sunt inevitabile. Atacurile cibernetice, întreruperile sistemului și încălcările datelor provoacă instituțiile la fiecare nivel, punând în pericol continuitatea operațională și încrederea clienților.

Noua Digital Operational Resilience Act (DORA) este o reglementare transformatoare menită să întărească reziliența operațională a sectorului financiar european.

Până la 17 ianuarie 2025, instituțiile financiare din Europa trebuiau să adere la noi standarde stricte. DORA nu se referă doar la conformitatea cu reglementările; este un cadru cuprinzător pentru a se asigura că întreprinderile se pot adapta, recupera și prospera pe fondul provocărilor neprevăzute.

Ce este DORA?

DORA stabilește un cadru de reglementare robust, menit să asigure rezistența operațională a sectorului financiar. Recunoaște dependențele complexe din cadrul ecosistemului financiar și introduce măsuri de atenuare a riscurilor din surse interne și externe. Instituțiile financiare, furnizorii terți și furnizorii de servicii critice sunt toate incluși în umbrela DORA, ceea ce face ca aceasta să fie o abordare holistică pentru protejarea sectorului.

Componentele cheie ale DORA includ:

- **Raportarea incidentelor:** protocoale clare pentru raportarea în timp util a incidentelor operaționale, permițând răspunsuri rapide și îmbunătățiri sistemice.
- **Managementul riscului de la terți:** Supraveghere cuprinzătoare a furnizorilor și partenerilor pentru a se asigura că respectă aceleași standarde de rezistență ca și instituțiile pe care le sprijină.

- **Testarea rezistenței:** testarea de rutină a sistemelor pentru a se pregăti pentru diverse scenarii de perturbare, asigurând pregătirea pentru provocările din lumea reală.
- **Planuri de recuperare și răspuns:** planificare detaliată pentru a restabili operațiunile rapid și eficient după un incident.

Impactul DORA asupra securității bancare

Accentul DORA pe reziliența operațională are implicații profunde pentru securitatea bancară. Iată câteva dintre efectele transformatoare:

1. Standarde îmbunătățite de securitate cibernetică: DORA impune garanții riguroase împotriva amenințărilor cibernetice, solicitând instituțiilor să întărească apărarea împotriva phishingului, ransomware-ului și a altor activități rău intenționate. Accentul actului pe testare asigură că vulnerabilitățile sunt identificate și abordate înainte ca atacatorii să le poată exploata.

2. Reziliența holistică a ecosistemului: prin extinderea supravegherii de reglementare la furnizorii terți și furnizorii de servicii critice, DORA se asigură că întregul lanț de aprovizionare financiar este rezistent. Acest lucru reduce riscul defecțiunilor sistemice care decurg dintr-o singură verigă slabă.

3. Management îmbunătățit al incidentelor: cadrul standardizat de

raportare a incidentelor DORA asigură că întreruperile sunt gestionate eficient, minimizând timpul de nefuncționare și menținând încrederea clienților. Instituțiile financiare trebuie să stabilească canale de comunicare clare cu părțile interesate în timpul crizelor.

4. Încrederea clienților consolidată: transparența și pregătirea stimulează încrederea. Instituțiile conforme cu DORA semnalează clienților și autorităților de reglementare deopotrivă că acordă prioritate securității și fiabilității, consolidând încrederea în sistemul financiar.

Cum se aliniază Cleafy cu reglementările DORA

La Cleafy, sunt înțelese provocările adaptării la noile reglementări precum DORA, menținând în același timp eficiența operațională. Soluțiile noastre de detectare a fraudei și de gestionare a riscurilor sunt concepute pentru a vă completa strategia de rezistență fără a adăuga dependențe inutile.

Perspective îmbogățite cu riscuri

Cleafy vă îmbogățește eforturile de detectare a fraudelor prin identificarea tranzacțiilor potențial riscante, fără a vă perturba sistemele principale de procesare a plăților.

Independență operațională

Platforma noastră funcționează asincron, asigurându-ne că orice întrerupere din partea noastră nu compromite capacitatea dumneavoastră de a furniza servicii financiare neîntrerupte.

Strategii de securitate adaptive

Chiar și în cazul rar al indisponibilității temporare a lui Cleafy, băncile pot implementa măsuri adaptative, cum ar fi aplicarea Autentificării puternice a clienților (SCA), pentru a menține securitatea și stabilitatea.

Prin clasificarea adecvată a serviciilor în cadrul DORA, Cleafy vă asigură că vă puteți concentra asupra zonelor critice fără sarcini de reglementare inutile. Soluțiile noastre adaugă valoare fără a vă spori dependența de sistemele terțe, făcând conformarea mai simplă și mai eficientă.

Transformarea provocărilor DORA în oportunități

Adaptarea la DORA poate părea descurajantă, dar este și o șansă de a reevalua și a perfecționa abordarea instituției dumneavoastră cu privire la risc și fiabilitate. În loc să revizuiască sistemele existente, DORA încurajează investițiile strategice în domenii care sporesc rezistența și încrederea.

Misiunea Cleafy este să simplifice acest proces. Platforma FxDR oferă instituțiilor capacități avansate de detectare a fraudei și de gestionare a riscurilor asigurarea independenței operaționale. Cu Cleafy, nu doar îndepliniți standardele de reglementare, ci stabiliți un nou punct de referință pentru rezistență și încredere în serviciile financiare.

Soluţiile Cleafy sunt distribuite în România de compania **SolvIT Networks.**

Incidente care îți afectează planurile de continuitate operațională

Pentru a trage un semnal de alarmă, am realizat un top al celor mai frecvente incidente care afectează planurile de continuitate operațională ale companiilor:

Ransomware criptează, de obicei, fișierele victimei sau blochează sistemul, făcându-l inaccesibil. Pe lângă plata cererii de răscumpărare, pierderile pot fi cauzate și de întreruperea activității sau de posibilele amenzi pentru încălcarea reglementărilor privind protecția datelor.

La nivel de hardware, pot apărea probleme din cauza defectelor de fabricație, uzurii, supraîncălzirii sau problemelor electrice. La nivel de software, cauzele cele mai des întâlnite pentru defecțiuni sunt bug-urile, erorile de programare, problemele de compatibilitate sau vulnerabilitățile în codul software. Probleme pot apărea și la nivel de rețea, prin coruperea datelor, dar și pe baza unor erori umane. La nivel de aplicații, defecțiunile pot provoca haos operațional pentru clienți. Penele de curent sau căderile de tensiune nu produc doar întreruperea operațiunilor normale, dependente de electricitate. Impactul poate fi foarte mare, mai ales pentru organizațiile care se bazează pe infrastructura IT on-premises.

Inundațiile pot provoca daune importante clădirilor, infrastructurii IT, echipamentelor și inventarului, ceea ce înseamnă reparații sau înlocuiri costisitoare pentru întreprinderi. Inundațiile pot deteriora depozitele sau centrele de distribuție și pot împiedica circulația mărfurilor și a materiilor prime, ceea ce provoacă întârzieri în producție, distribuție și livrarea de produse și servicii.

Incendiile pot distruge dispozitive electronice, servere și sisteme de stocare a datelor, ceea ce duce la pierderea de date, documente, înregistrări și proprietate intelectuală esențiale, cu impact potențial pe termen lung asupra continuității și competitivității afacerii. Și sistemele electrice, sistemele HVAC (încălzire, ventilație și aer condiționat), instalațiile sanitare și rețelele de comunicații pot fi deteriorate sau distruse de incendii, necesitând reparații sau înlocuiri costisitoare.

M247 oferă soluții care acoperă toate palierele vulnerabile, de la conectivitate la Internet și comunicații, până la backup, cloud și servicii de colocare.

Fraud XDR: Protecție mai inteligentă pentru sistemul bancar modern

Lupta împotriva fraudei bancare online se intensifică. Atacatorii devin din ce în ce mai sofisticați, exploatând vulnerabilități cu mult înainte ca o tranzacție frauduloasă să aibă loc.

Metodele tradiționale de detectare a fraudelor, cândva piatra de temelie a securității bancare, se luptă să țină pasul. De ce? Pentru că se concentrează în primul rând pe tranzacții, detectând frauda doar atunci când aceasta are deja loc. Dar până în acel moment, fraudatorii au ocolit deja măsurile de securitate, au preluat conturile și au lăsat instituțiile financiare să se chinuie să atenueze daunele.

Pentru a rămâne cu adevărat în frunte, băncile trebuie să-și regândească abordarea. Viitorul prevenirii fraudei nu este doar despre detectarea tranzacțiilor frauduloase, ci este despre oprirea fraudei înainte ca aceasta să se întâmple. Aici intervine Fraud Extended Detection & Response (FxDR). Spre deosebire de sistemele de securitate convenționale, FxDR oferă o vizualizare holistică, în timp real, a întregii experiențe bancare digitale, permițând instituțiilor financiare să detecteze și să oprească activitatea frauduloasă înainte ca aceasta să escaladeze.

Băncile nu se mai pot baza pe modele învechite de prevenire a fraudei

Sistemele tradiționale se concentrează în primul rând pe monitorizarea tranzacțiilor pentru a identifica activitățile suspecte. Cu toate acestea, escrocii moderni au devenit adepți în a ocoli aceste măsuri prin țintirea întregii sesiuni de utilizator, câștigând adesea controlul înainte de a iniția orice tranzacție. Această schimbare necesită o abordare mai cuprinzătoare care oferă vizibilitate de la capăt la capăt, permițând băncilor să detecteze și să prevină activitățile frauduloase în fiecare etapă a călătoriei utilizatorului.

Escrocii nu se bazează pe o singură metodă de a exploata instituțiile și victimele. În schimb, ei folosesc strategii variate, cum ar fi preluări de cont (ATO), sisteme de transfer automat (ATS) și escrocherii cu plăți autorizate push (APP) pentru a ocoli măsurile de securitate. De aceea, Cleafy implementează o abordare stratificată a detectării fraudelor, integrând mai multe metode de detectare, în loc să se bazeze doar pe analiza tranzacțiilor.

Cum abordează Fraud Extended Detection & Response (FxDR) aceste provocări

FxDR schimbă jocul în prevenirea fraudei. Prin monitorizarea continuă a comportamentului utilizatorului și a interacțiunilor în timp real, FxDR poate identifica anomalii care indică o intenție frauduloasă cu mult înainte de producerea unei tranzacții. Această abordare permite instituțiilor financiare să acționeze rapid, oprind amenințările înainte ca acestea să devină fraude.

Platforma FxDR a lui Cleafy merge un pas mai departe prin asigurarea vizibilității pe canalele web, mobile și API, de la interacțiunile pre-autentificare până la și dincolo de tranzacție. Această abordare holistică permite cel mai rapid și mai eficient răspuns, protejând eficient împotriva unui spectru de amenințări și combatând frauda la sursă.

Rolul AI în prevenirea fraudelor moderne

AI este parte integrantă a eficacității FxDR. Cu toate acestea, AI folosită trebuie să fie atât explicabilă, cât și adaptabilă. Spre deosebire de modelele „cutie neagră" opace, platforma Cleafy bazată pe inteligență artificială oferă perspective transparente asupra proceselor de luare

a deciziilor, asigurându-se că echipele de securitate înțeleg rațiunea din spatele fiecărei alerte.

Capacitățile Cleafy folosesc microservicii și principii modulare de inteligență artificială, producând un set de micro-modele țintite care nu necesită o pregătire extinsă privind datele de fraudă etichetate. Aceasta înseamnă că sistemul Cleafy funcționează în câteva zile, nu în luni, oferind valoare imediată, asigurând în același timp rezistența pe termen lung împotriva amenințărilor în evoluție.

Integrarea FxDR în sistemele de detectare

Este bine să existe sisteme de detectare stabilite – lupta împotriva fraudei necesită în cele din urmă mai multe straturi. Cu toate acestea, deși sistemele existente pot oferi un grad de protecție, ele funcționează adesea în silozuri și reacționează la amenințări prea târziu în călătoria utilizatorului. FxDR îmbunătățește aceste configurații prin adăugarea unui nivel de apărare în timp real, înainte de tranzacție, care integrează toate interacțiunile pe canale și sesiuni, astfel încât narațiunea sau povestea digitală completă să fie disponibilă pentru analiză. Această integrare nu numai că întărește securitatea băncii, dar și eficientizează operațiunile, reducând atât pierderile legate de fraudă, cât și costurile operaționale asociate gestionării unor astfel de incidente.

Soluția FxDR se integrează perfect cu infrastructura de securitate existentă a unei bănci, operând la nivelul rețelei și al traficului de aplicații. Prin urmare, este discret în furnizarea de informații despre amenințări în timp real, integritatea dispozitivului și a aplicațiilor, analiză comportamentală și capabilități de răspuns automat.

În plus, abordarea Cleafy nu se bazează pe o singură metodă de detectare, ci mai degrabă utilizează o combinație de colectare granulară de date pe dispozitive, aplicații, rețele, comportament și tranzacții. Aceste date sunt analizate prin mai multe modele de detectare concepute special, producând semnale de risc deterministe, care pot fi citite de om. Aceste semnale pot fi valorificate pentru răspunsuri personalizate, în loc să fie pur și simplu alimentate într-un scor de risc global, oferind băncilor control deplin asupra atenuării amenințărilor.

Concluzie

O abordare proactivă este primordială în lupta împotriva fraudei. Prin adoptarea FxDR, băncile pot detecta și preveni activitățile frauduloase înainte ca acestea să afecteze clienții, protejându-le activele și reputația.

Actorii amenințărilor dezvoltă în mod constant tacticile, iar instituțiile financiare trebuie să rămână cu un pas înainte. Abordarea Cleafy depășește în mod constant metodele tradiționale de detectare a fraudei, deseori prezicând frauda în medie cu 15 zile înainte de producerea unei tranzacții frauduloase.

Prin valorificarea expertizei Cleafy, a tehnologiei și a cadrului global de partajare a informațiilor, băncile pot neutraliza eficient amenințările de fraudă cu o acuratețe precisă, prevenind atacurile înainte ca acestea să ducă la pierderi financiare.

Soluţiile Cleafy sunt distribuite în România de compania **SolvIT Networks.**

Riscurile generării de parole cu ajutorul AI

Majoritatea serviciilor online și aplicațiilor cer utilizatorului să creeze o parolă. Șansele sunt ca multe dintre aceste parole să nu fie folosite zilnic și, din cauza acestei abundențe, există o probabilitate mare ca unele să fie reutilizate.

Gestionarea slabă a parolelor este agravată de folosirea unor combinații comune de nume, cuvinte din dicționar și cifre. Aceste parole sunt relativ ușor de spart, iar dacă un infractor cibernetic obține acces la una dintre ele, poate obține acces și la o mulțime de alte conturi.

Acesta este motivul pentru care se recomandă utilizatorilor să creeze parole unice și aleatorii pentru a reduce vulnerabilitatea cauzată de reutilizarea acelorași parole. Totuși, crearea și gestionarea parolelor poate fi o sarcină dificilă. Pentru a ușura acest proces, mulți ar putea fi tentați să apeleze la modele lingvistice mari (LLMs) precum ChatGPT, Llama sau DeepSeek pentru a genera parole.

Atracția este evidentă: în loc să se chinuie să creeze o parolă puternică, utilizatorii pot, pur și simplu, întreba AI-ul „Generează o parolă sigură” și vor primi instant un rezultat. AI-ul generează șiruri aparent aleatorii, evitând tendința umană de a crea parole previzibile, bazate pe cuvinte cunoscute. Dar aparențele pot fi înșelătoare — parolele generate de AI nu sunt întotdeauna la fel de sigure pe cât par.

Specialiștii Kaspersky au testat acest lucru generând 1.000 de parole folosind unele dintre cele mai cunoscute și de încredere modele: ChatGPT (de la OpenAI), Llama (din grupul Meta), DeepSeek (un model recent din China). Toate modelele știu că o parolă bună trebuie să aibă cel puțin 12 caractere, să conțină litere mari și mici, cifre și simboluri. Ele menționează acest lucru și în procesul de generare a parolelor.

Astfel, DeepSeek și Llama generează uneori parole compuse din cuvinte de dicționar, în care unele litere sunt înlocuite cu cifre de formă similară: S@d0w12, M@n@tee3, B@n@n@7 (DeepSeek), K5yB0a8dS8, S1mP1eL1on (Llama). Ambele modele au tendința de a genera parola „password”: P@ssw0rd, P@ssw0rd!23 (DeepSeek), P@ssw0rd1, P@ssw0rdV (Llama). Evident, astfel de parole nu sunt sigure. Trucul cu înlocuirea literelor cu alte caractere este bine cunoscut și poate fi ușor spart prin „brute force”. ChatGPT nu are această problemă și generează parole care par într-adevăr aleatorii.

Soluțiile Milestone Systems pentru securitatea IT a infrastructurilor critice

Într-o eră marcată de digitalizare accelerată și amenințări cibernetice tot mai sofisticate, securitatea infrastructurii critice a devenit o prioritate strategică pentru organizațiile din domenii vitale, precum energie, transport, sănătate sau servicii publice.

Aceste organizații au nevoie de soluții de securitate fiabile, scalabile și aliniate la cele mai stricte reglementări. În acest articol, vom analiza modul în care tehnologia video inteligentă oferită de Milestone Systems contribuie la consolidarea securității infrastructurilor critice și vom evidenția cele mai utilizate produse Milestone în diferite domenii de activitate.

Cerințe de securitate

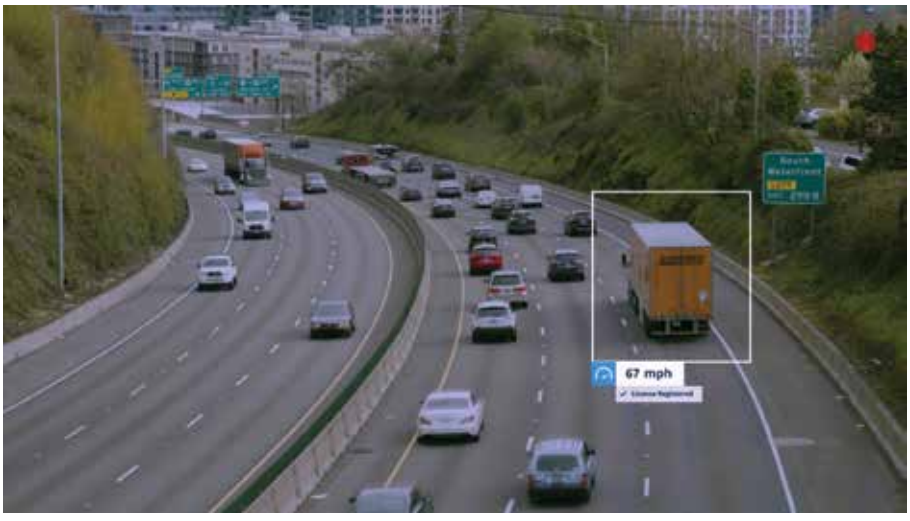
Sarcinile pe care trebuie să le îndeplinească un sistem de securitate sunt:

- Detectarea intruziunilor
- Detectarea termică și a incendiilor
- Detectarea scurgerilor
- Controlul accesului
- Recunoașterea plăcuțelor de înmatriculare
- Prevenirea fraudelor/ furturilor interne

Toate aceste activități implică monitorizarea spațiilor și a persoanelor, precum și pot contribui la atenuarea unei game largi de amenințări. Milestone se potrivește perfect clienților care caută scalabilitate, conformitate cu reglementările și asistență pe termen lung.

Software scalabil

Diferiți clienți din domeniul infrastructurii critice vin cu abordări diferite. Centralele nucleare vor include securitatea armată 24/7 la fața locului, în timp ce o companie de distribuție a apei ar putea avea sute de site-uri fără personal, unde monitorizarea de la distanță este utilizată pentru a detecta scurgerile din conductele deteriorate. Dar, indiferent dacă furnizați energie electrică, gaze naturale, telecomunicații sau servicii de gestionare a apei, probabil că aveți unele nevoi comune. Probabil că trebuie să monitorizați mai multe site-uri pentru a asigura atât securitatea fizică, cât și securitatea cibernetică. Și fiecare locație are probabil multe camere de securitate,



puncte de control al accesului și senzori diferiți. Poate aplicația Milestone să suporte sute sau chiar mii de astfel de dispozitive? Da.

Dar ceea ce este la fel de important este că Milestone suportă aproape orice tip de dispozitiv de monitorizare, indiferent de producător. Acesta este motivul pentru care numim tehnologia noastră "platformă deschisă", pentru că funcționează cu ceea ce aveți deja. Mulți dintre clienții noștri doresc să înlocuiască sistemele NVR vechi cu o soluție nouă, dar nu dispun de bugetul necesar pentru a-și actualiza simultan tot hardware-ul. Cu Milestone, puteți utiliza camerele, senzorii și altele existente și apoi să le actualizați treptat, pe măsură ce apare necesitatea. Platforma deschisă înseamnă, de asemenea, că software-ul nostru funcționează și cu o serie întreagă de aplicații PSIM (Physical

Security Identity Manager).

Asistență continuă

Milestone a fost prima companie care a furnizat o soluție software de gestionare video cu platformă deschisă. Suntem în domeniu de peste 25 de ani. Dar de ce ar trebui să vă intereseze? Ei bine, având în vedere implicațiile financiare și umane ale unui atac asupra infrastructurii critice, clienții noștri doresc să lucreze cu furnizori cu un istoric excelent. Milestone a fost și continuă să fie dedicată asigurării celui mai înalt standard de securitate și calitate. Reglementările enumerate în secțiunea anterioară ar putea să nu însemne prea mult la prima vedere, dar ar fi greu să găsiți alți furnizori de VMS care să îndeplinească aceleași cerințe, fiind în același timp o platformă deschisă.
În plus, Milestone are o rețea extinsă de parteneri în întreaga lume. Pentru clienții noștri, acest lucru înseamnă că vor exista întotdeauna în apropiere profesioniști care știu cum să sprijine oamenii din sectorul dumneavoastră de activitate cu instalațiile Milestone pentru mulți ani de acum înainte.

Securitate cibernetică

În aplicațiile și instalațiile în care materialele video, audio și metadatele joacă un rol esențial ca probe, este extrem de important ca fișierele media să fie transmisă, stocată și, în general, manipulată într-un mod securizat din momentul în care este captată de cameră, până în momentul în care este utilizată ca probă, de exemplu în instanță.
Milestone XProtect® Corporate și XProtect Expert și XProtect Smart Client oferă o serie de funcționalități de securitate care permit utilizatorilor să mențină securitatea și integritatea completă de la un capăt la altul a datelor media transmise și înregistrate, de exemplu:

- fluxuri media criptate de la camere prin intermediul serverelor VMS către clienții VMS
- baze de date media criptate pe serverele de înregistrare și pentru exporturile în format XProtect
- semnarea și verificarea digitală a bazelor de date media, autentificarea securizată a utilizatorilor și permisiuni de acces detaliate
- controlul centralizat al formatelor și caracteristicilor de export permise, de exemplu funcționalitatea de a preveni reexportarea bazelor de date media care au fost deja exportate

Combinarea unei game de metode standard de securitate IT cu un set de caracteristici VMS unice în produsele Milestone XProtect VMS permite clienților să realizeze o implementare sigură a soluțiilor de supraveghere video cu securitate completă end-to-end și criptare a datelor media VMS.
Suportul XProtect VMS pentru criptarea atât a datelor media difuzate, cât și a celor înregistrate, asigură faptul că media nu poate fi capturată sau accesată de persoane neautorizate în timpul tranzitului prin rețea sau în repaus în baza de date media. Suportul suplimentar al XProtect VMS pentru semnături digitale în baza de date media a serverului de înregistrare și în bazele de date media exportate asigură posibilitatea de a verifica dacă dovezile media nu au fost falsificate, nici în serverele de înregistrare VMS, nici ulterior, în timpul transportului sau al vizualizării media exportate.

În plus față de funcționalitatea de criptare și semnare digitală, XProtect VMS oferă proprietarului VMS un control strict asupra persoanelor care au acces la anumite dispozitive și funcționalități de export, inclusiv controlul centralizat și aplicarea formatelor și destinațiilor de export permise, utilizarea criptării și a semnării digitale, precum și opțiunea de a interzice reexportarea mediilor exportate.
Utilizarea întregii suite de funcții de securitate cibernetică din Milestone XProtect VMS permite clienților să opereze o instalație de supraveghere video sigură, chiar și în medii cu nevoi și riscuri sporite de securitate cibernetică.

Milestone Technology Day România 2025 a avut loc pe **16 aprilie** și a reunit, alături de echipa de conducere a Milestone, parteneri renumiți, lideri în domeniul tehnologiei. Evenimentul s-a desfășurat la JW Marriott Bucharest Grand Hotel, unde s-au purtat discuții despre provocările actuale din industrie și s-au explorat modalitățile prin care tehnologia video devine din ce în ce mai inteligentă, oferind soluții aplicabile în diverse domenii. În cadrul evenimentului, au fost prezentate și exemple concrete de utilizare a soluției XProtect de la Milestone, evidențiind modul în care se poate sprijini transformarea digitală.

SSE-urile sporesc securitatea aplicațiilor native în cloud

Un serviciu de securitate edge (SSE) simplifică securitatea în mediile cloud, multicloud și cloud hibrid. Mai ales în cazul întreprinderilor mai mici care nu au neapărat personal intern pentru a dezvolta, gestiona și securiza propriile aplicații în cloud.

Un SSE guvernează politica de securitate și accesul la aplicații pentru mediile cloud. Ajută la determinarea ce li se permite utilizatorilor să facă, când au voie să facă acest lucru și cum au voie să facă acest lucru.

La un nivel de bază, un SSE oferă o poartă web securizată pentru a guverna ce aplicații sunt accesibile. Acest lucru poate ajuta companiile să evite IT-ul umbră, în special în mediile hibride și la distanță. Un SSE oferă, de asemenea, un firewall pentru aplicații web pentru a monitoriza și filtra traficul HTTP. Securitatea interfeței de programare a aplicațiilor și criptarea web sunt, de asemenea, standard cu SSE. În cele mai multe cazuri, SSE-urile analizează traficul HTTP mult mai granular decât ar avea timp pentru un administrator web. Este mult mai ușor să construiți și să executați reguli predefinite cu un SSE.

Un alt beneficiu: un SSE se bazează pe arhitectura de rețea zero-trust. Spre deosebire de VPN-urile, care permit accesul la rețele întregi, ZTNA oferă acces la aplicația specifică solicitată. Combinați acest lucru cu o gestionare puternică a identității și a accesului, iar o afacere poate ajunge la un mediu cloud extrem de sigur. Echipele pot folosi, de asemenea, un SSE pentru a rula interogări împotriva unui motor de inteligență artificială pentru a se asigura că nu dezvăluie informații vulnerabile sau secrete comerciale.

Poate cel mai mare beneficiu al unei SSE este simplitatea sa. Indiferent dacă liderii IT mută aplicații în cloud sau se abonează la aplicații SaaS, echipele ar trebui să combine acele aplicații native din cloud cu un SSE.

SSE-urile și SaaS se potrivesc în cloud

Adesea, organizațiile trec la SaaS, deoarece este mai ușor de gestionat și mai previzibil. Prea des, companiile încearcă să-și construiască propriile aplicații, pentru a afla mai târziu că au suportat costuri mult mai mari decât anticipau. Această problemă este mai puțin probabil să apară cu SaaS.

Evident, fiecare aplicație nu poate fi o aplicație SaaS și va fi întotdeauna nevoie de infrastructură locală. Dar cele care pot fi mutate în SaaS ar trebui să fie și toate acestea ar trebui protejate cu un SSE. La fel ca SaaS, un SSE este gestionat prin interfețe mai simple; este un model de cheltuieli operaționale; poate fi accesat intern sau extern, ceea ce îl face ideal pentru mediile cloud hibride și poate oferi o securitate mai mare prin proiectare.

Nu vă fie teamă de cloud din motive de securitate – trebuie doar să fiți judicios cu privire la sarcinile de lucru care aparțin cloud-ului și să fiți inteligent în privința modului în care le asigurați.

Phishing-ul s-a reinventat. Ești sigur că și afacerea ta e pregătită?

Atacurile de tip phishing continuă să reprezinte o amenințare semnificativă la adresa securității cibernetice, iar e-mailul rămâne principalul vector utilizat de atacatori.

Iată trei statistici relevante care evidențiază amploarea și impactul acestor atacuri:

- Conform Directoratului Național de Securitate Cibernetică, în 2024, atacurile de tip phishing au constituit aproximativ o treime (32,95%) din totalul incidentelor de securitate cibernetică raportate în România. (DNSC)
- Se estimează că utilizarea modelului phishing-as-a-service (PhaaS) va fi responsabil pentru peste 50% din furturile de credențiale în 2025 (Barracuda).
- Costul mediu global al unei brese de date a depășit 4,9 milioane USD (IBM Cost of a Data Breach Report).

Gata cu emailurile naive, pline de greșeli și linkuri dubioase. În 2025, phishing-ul arată (și sună) ca o conversație reală cu CEO-ul tău. Criminalii cibernetici folosesc acum AI generativ, deepfake-uri video și chiar coduri QR ca să păcălească angajații — iar atacurile devin din ce în ce mai greu de detectat.
După cum spune Alexandra Duricu, CISO, ASEE (Romania): „Phishing-ul nu mai este un atac generic. Este personalizat, construit pe baza informațiilor deja disponibile online. Tocmai de aceea, companiile au nevoie de mai mult decât filtre clasice sau traininguri de conștientizare de bază."

În tot acest peisaj delicat și dificil de navigat pentru clienții noștri, apar și partenerii de tehnologie cu care pleci la drum. Alegerea soluției potrivite poate face diferența dintre un atac detectat și unul devastator.
Dintre cei mai importanți furnizori globali de tehnologie în domeniul securității cibernetice, Check Point se detașează prin abordarea proactivă, bazată pe inteligență artificială, care merge dincolo de protecția tradițională. Soluțiile lor antiphishing sunt gândite pentru peisajul actual — unde viteza, contextul și comportamentul utilizatorului contează mai mult decât simpla detectare a unui link suspect.

Check Point Harmony Email & Collaboration oferă o suită completă de protecție împotriva celor mai avansate forme de phishing:

- Detectează comportamente anormale și tentative de impersonare în timp real
- Scanează fișiere și linkuri — inclusiv cele găzduite pe platforme legitime precum OneDrive sau SharePoint.
- Oferă protecție în fața conturilor compromise sau atacurilor din interior
- Blochează inclusiv atacuri bazate pe coduri QR dificil de filtrat de soluțiile tradiționale

Atacurile vin. Întrebarea este: ești pregătit să le faci față?

Nu poți lupta cu atacuri sofisticate folosind soluții de ieri. Fiecare zi fără o strategie clară de apărare este o fereastră deschisă pentru atacatori.
Echipa noastră de specialiști nu doar că înțelege riscurile, le simulează, le anticipează și le neutralizează. De la atacuri simulate care testează vigilența echipei tale, până la implementarea unor soluții de ultimă generație precum Check Point, suntem aici să construim un scut real, nu o iluzie de protecție.

Acționează acum — înainte să fii nevoit să reacționezi în criză!

#cybersecurity #phishing #CheckPoint #securitateIT #AI #CISO #sigurantaorganizationala #Romania #emailsecurity #infosec #cyberresilience
Backlink: **https://www.checkpoint.com/harmony/email-security/**

Responsabilii cu securitatea se luptă să echilibreze securitatea și obiectivele de afaceri

În întreaga lume, liderii de securitate spun că se luptă să echilibreze nevoia de a-și securiza datele în mod corespunzător și nevoia de a maximiza utilizarea eficientă a acestor date pentru a-și atinge obiectivele de afaceri, potrivit unui studiu realizat de analiștii de la Gartner, care a constatat că doar 14% dintre liderii cibernetici țin cont de acest lucru. **de Bogdan Marchidanu**

Sondajul firmei de analiză asupra a 318 lideri seniori de securitate – realizat în vara anului 2024 – a constatat că 35% erau încrezători că pot securiza activele de date, iar 21% erau încrezători că pot folosi datele pentru a-și atinge obiectivele de afaceri. Capacitatea de a le face pe amândouă era peste șase din șapte.

Nathan Parks, specialist principal pentru cercetare la Gartner, a spus că este în mod clar un lucru care trebuia abordat. „Cu doar 14% dintre liderii SRM capabili să-și securizeze datele în timp ce susțin obiectivele de afaceri, multe organizații se pot confrunta cu o vulnerabilitate crescută la amenințări cibernetice, sancțiuni de reglementare și ineficiențe operaționale, riscând în cele din urmă avantajul lor competitiv și încrederea părților interesate", a spus el.

În lumina constatărilor, Gartner a dezvoltat o listă de verificare în cinci puncte pentru liderii de securitate – lideri de securitate și

risc, în limbajul său – pentru a-și alinia mai bine nevoile de afaceri la cerințele stricte de securitate a datelor și pentru a atinge cu succes atât protecția eficientă a datelor, cât și obiectivele de activare a afacerii:

• CISO ar trebui să încerce să ușureze fricțiunile legate de guvernanță pentru afacere prin co-crearea politicilor și standardelor de securitate a datelor cu contribuții și feedback de la utilizatorii finali din întreaga afacere;

• Aceștia ar trebui să încerce să alinieze eforturile de guvernanță legate de securitatea datelor printr-un parteneriat mai bun cu celelalte funcții interne ale afacerii pentru a identifica zonele de suprapunere și potențiala sinergie;

• Aceștia ar trebui să identifice și să delimiteze în mod clar orice cerințe de securitate cibernetică nenegociabile pe care afacerea trebuie să le îndeplinească în mod absolut atunci când gestionează riscuri de securitate a datelor necunoscute sau neașteptate anterior;

• În ceea ce privește inteligența artificială generativă (GenAI) și luarea deciziilor legate de aceasta, aceștia ar trebui să aibă grijă să definească balustrade adecvate, la nivel înalt, care să permită părților interesate să experimenteze în cadrul unor parametri stabiliți;

• Și, în cele din urmă, ar trebui să colaboreze cu echipele de date și analize ale companiei pentru a asigura acceptarea la nivel de consiliu la nivelurile de securitate a datelor.

Ultimul punct abordat de Gartner, privind construirea de relații de lucru mai eficiente cu conducerea superioară, a căror activitate principală nu este investită în securitatea cibernetică, este un ghimpe peren în coasta multor lideri de securitate, care deplâng adesea atitudini divergente.

Acest lucru a fost evidențiat într-un studiu recent publicat de firma Splunk, specializată în analiză de securitate și observabilitate, deținută de Cisco, care a chestionat ofițerii șefi de securitate a informațiilor (CISO) din 10 țări, inclusiv Marea Britanie și SUA. Splunk a constatat că CISO participau din ce în ce mai mult la sălile de consiliu, dar a evidențiat decalaje mari între prioritățile lor și alți membri ai consiliului.

De exemplu, a spus firma Splunk, când a fost vorba de inovarea cu tehnologii emergente, cum ar fi GenAI, 52% dintre CISO au vorbit despre asta ca fiind o prioritate, comparativ cu 33% din alți membri ai consiliului de administrație, despre perfecționarea sau recalificarea angajaților cibernetici, 51% dintre CISO au considerat că aceasta este o prioritate, comparativ cu 27% dintre membrii consiliului de administrație, au spus că contribuie la creșterea veniturilor și a inițiativelor CISO3 a prioritizat acest lucru, comparativ cu 24% dintre membrii consiliului de administrație.

Deși raportul complet este mai nuanțat decât ar sugera aceste statistici, studiul a arătat, de asemenea, că doar 29% dintre CISO credeau că obțin bugetul necesar pentru a funcționa eficient, în timp ce 41% dintre membrii consiliului de administrație au considerat că bugetele de securitate sunt absolut bune.

Hackerii vizează companii printr-o înșelătorie de recrutare pe LinkedIn

Specialiștii în securitate informatică de la Bitdefender au analizat o tentativă eșuată de „recrutare" pe LinkedIn. Totul începe cu un mesaj atrăgător: o oportunitate de a colabora la o platformă de schimb de criptomonede descentralizată. Detaliile sunt vagi, însă promisiunea unui job flexibil, remote și bine plătit poate atrage victime ușor de păcălit. Versiuni similare ale acestei escrocherii au fost observate și în alte domenii, precum turismul sau finanțele.

Dacă victima își arată interesul, „procesul de recrutare" continuă cu solicitarea unui CV sau a unui link către un repository GitHub personal. Deși aceste cereri par inofensive, acestea pot fi folosite pentru a colecta informații personale sau pentru a face interacțiunea să pară legitimă.

După ce obține informațiile dorite, atacatorul trimite un set de fișiere ce conține așa-numitul „Minimum Viable Product" (MVP) al proiectului, împreună cu un document cu întrebări care pot fi rezolvate doar prin rularea unui demo. La prima vedere, codul pare inofensiv. Însă, o analiză mai atentă dezvăluie un script ascuns și dificil de descifrat, care încarcă și rulează dinamic cod periculos de pe un server extern.

Cercetătorii Bitdefender au descoperit o amenințare informatică de tip info-stealer, capabilă să infecteze Windows, macOS și Linux și să colecteze datele asociate unor game largi de portofele de criptomonede și extensii de browser. Odată activată, amenințarea informatică instalată pe sistem poate să întreprindă următoarele acțiuni:

• Fură fișiere importante din extensiile vizate ale browserului

• Colectează datele de autentificare stocate în browser

• Sustrage informațiile către un server controlat de atacatori.

După compromiterea inițială, amenințarea informatică inițiază o serie de acțiuni suplimentare pentru a extinde atacul. Înregistrează apăsările de taste, monitorizează clipboard-ul și colectează informații despre sistem, inclusiv fișiere confidențiale și date de autentificare. De asemenea, menține o conexiune activă cu serverele atacatorilor, ceea ce le permite accesul neautorizat și sustragerea continuă a datelor.

În etapa finală, amenințarea informatică instalează componente suplimentare pentru a ocoli soluțiile de securitate și a comunica prin rețele anonime. Poate colecta informații despre dispozitiv, poate instala un backdoor pentru acces ulterior și, în unele cazuri, folosește resursele sistemului pentru a mina criptomonede.

Strategii pentru abordarea riscurilor de securitate în implementările IIoT

În ultimii câțiva ani, Internetul lucrurilor (IoT) a devenit din ce în ce mai omniprezent. Peste 27 de miliarde de dispozitive în rețea vor fi online în 2021 și 75 de miliarde până în 2025. Internetul Industrial al Lucrurilor (IIoT), în special, ar putea adăuga 14 trilioane de dolari la economia globală până în 2030.

Numeroase sectoare industriale se bazează deja pe dispozitive IIoT, cum ar fi contoare inteligente, alarme și senzori pentru întreținerea automată a mașinilor și sarcini critice de predicție pentru afaceri; urmărirea stocurilor; și transformarea procesului/fluxului de lucru.

Dar, în ciuda importanței sale tot mai mari, organizațiile care trec la IIoT nu își pot permite să ignore problemele de securitate. O rețea IIoT se poate extinde pe mai multe mile și poate avea sute de mii de puncte de date. O slăbiciune a unui dispozitiv poate face toate celelalte dispozitive din rețea vulnerabile la atacuri cibernetice și poate crește riscul de întrerupere a procesului, manipulări neautorizate și chiar spionaj corporativ.

Pentru a proteja dispozitivele și rețelele IIoT, companiile trebuie să înceteze să se gândească la securitate ca la un gând ulterior. Securitatea prin obscuritate nu este o soluție adecvată; necesitatea orei este securitatea prin proiectare.

Iată câteva modalități prin care companiile care trec la IIoT pot minimiza riscurile de securitate.

Selectați tehnologia Cyber-Hardened potrivită

Pe măsură ce rețelele IIoT cresc, organizațiile industriale trebuie să implementeze tehnologii de securitate puternice specifice IoT. Dar mai întâi, obțineți claritate asupra aspectelor importante precum:

- Vectori critici de amenințare
- Considerente de reglementare și de conformitate
- Tehnologia tip de mașină la mașină (M2M) și necesitatea operațiunilor fără defecțiuni
- Tipul de date care sunt colectate, mai ales dacă sunt sensibile la timp și/sau critice pentru afaceri
- Factori externi care pot afecta transmiterea și primirea fiabilă a datelor între diferite puncte
- Un compromis acceptabil între caracteristici, ușurință în utilizare și securitate

Pe baza acestor răspunsuri, o serie de tehnologii pot fi identificate și implementate pentru a oferi securitate continuă pentru implementările IIoT, inclusiv:

- **Criptare** pentru a preveni compromiterea datelor sensibile
- **Securitatea rețelei și autentificarea dispozitivelor** pentru a securiza implementările între dispozitive, echipamente de vârf și sisteme back-end
- **Identity and Access Management (IAM)** pentru a securiza și gestiona relațiile dintre dispozitive și identități
- **Analize de securitate** pentru a identifica și opri potențialele atacuri sau intruziuni care pot ocoli controalele tradiționale de securitate

Dispozitive precum **routerul VPN AR2010V** de la Allied Telesis simplifică instalarea și gestionarea unei infrastructuri IIoT conectate, chiar și în scenarii extrem de solicitante. Acest lucru îl face o soluție puternică atunci când atât securitatea, cât și performanța ridicată sunt primordiale într-o implementare IIoT.

Securitatea este o problemă strategică de afaceri, nu o problemă tehnologică

Securitatea IIoT trebuie considerată o problemă strategică de afaceri care necesită soluții robuste și pe termen lung, mai degrabă decât o problemă tehnologică care trebuie rezolvată prin soluții punctuale.

Pentru aceasta, este esențial să se stabilească indicatori cheie de performanță (KPI) și să se stabilească proceduri și practici pentru a le îndeplini. Un program formal de securitate IIoT și un model de excelență operațională pot ajuta atât la reducerea riscului de securitate, cât și la îmbunătățirea performanței. Pentru a implementa acest program în întreaga întreprindere, trebuie creată o echipă de securitate interfuncțională de securitate IT, inginerie, operațiuni și un furnizor de sisteme de control.

Angajații ar trebui să aibă o mai mare vizibilitate asupra operațiunilor de securitate IIoT și a tehnologiei operaționale (OT) pentru a îmbunătăți gradul de conștientizare a amenințărilor și cunoașterea strategiilor de atenuare. Un program personalizat de formare în domeniul apărării cibernetice, cum ar fi cel oferit în comun de Allied Telesis și NUARI, ar trebui să fie, de asemenea, un

element critic al unui cadru de securitate. Organizațiile au nevoie, de asemenea, de resurse calificate de securitate cibernetică IIoT pentru a efectua în mod regulat un inventar al echipamentelor și pentru a face față compromisurilor în materie de securitate, confidențialitate și fiabilitate, fără a afecta negativ continuitatea operațională. În cele din urmă, firma și echipele sale de securitate ar trebui să creeze și să utilizeze automatizări, precum și inginerie, livrare și integrare continuă pentru a asigura o protecție consecventă.

Încorporați IIoT în cadrul de risc la nivel de întreprindere

Pentru o rețea IIoT în creștere, companiile trebuie să intensifice jocul de gestionare a riscurilor, gestionându-l la nivel de întreprindere. Companiile trebuie să identifice și să profileze toate punctele finale IoT și să le monitorizeze în mod regulat pentru a evalua vulnerabilitatea la risc.

Pentru a identifica vulnerabilitățile și a se pregăti pentru potențiale atacuri cibernetice, ar trebui efectuate evaluări coerente ale riscurilor și ar trebui documentate planuri detaliate de diminuare a riscurilor. De asemenea, este o idee bună să efectuați simulări de încălcare și să monitorizați centrul de operațiuni de securitate. Consolidarea capacităților de inteligență în domeniul securității cibernetice poate ajuta angajații să înțeleagă vectorii de atac la care sunt cei mai vulnerabili. Riscul poate proveni și din factori externi, astfel încât definirea unui SLA clar oriunde se bazează pe integratori de sistem și alți parteneri.

Pentru atenuarea optimă a riscurilor, cu controalele de securitate și prioritizarea adecvate, distrugeți orice izolare existente între **funcțiile IT și OT** și valorificați expertiza comună pentru a consolida securitatea generală IIoT. Și prin folosirea dispozitivelor de ultimă generație, cum ar fi **seria IE340** de switch-uri gestionate Industrial Ethernet Layer 2 de la Allied Telesis, o rețea poate fi protejată cu mecanisme de securitate superioare, inclusiv SSL, SSH, 802.1X și multe altele. Simultan, performanța ridicată, fiabilitatea și **ușurința de gestionare** oferă cea mai bună valoare din infrastructura lor IIoT.

Concluzie

Implementarea tehnologiilor și dispozitivelor IIoT într-un ritm mai rapid decât sunt securizate poate lăsa organizațiile vulnerabile la multe pericole legate de cibernetică. Aceste riscuri pot afecta productivitatea și eficiența operațională, stabilitatea financiară și chiar reputația companiei.

Din păcate, majoritatea organizațiilor se află în fazele incipiente ale adoptării de practici și tehnologii de protecție pentru a minimiza aceste riscuri.

IIoT va experimenta o creștere exponențială în următorii câțiva ani, așa că este esențial ca firmele să facă din securitatea IIoT prioritatea lor principală. Numai atunci își pot folosi cu adevărat puterea în creștere pentru cazurile de utilizare critice din lumea reală.

Allied Telesis este acum capabilă să lucreze îndeaproape cu sectorul productiv, construind cele mai noi soluții pentru a fructifica tehnologia IoT la nivelul palierului de producție al fabricii.

Allied Telesis

exterro

FTK 8.1 pentru o examinare digitală unificată: investighează datele de pe dispozitive mobile, Windows și Mac într-o singură platformă

Identifică legături comune între sursele de date și crează o narațiune coerentă, în special atunci când dovezile se află pe mai multe dispozitive.

FTK 8.1 aduce funcționalități de ultimă generație care revoluționează modul în care se analizează și gestionează probele digitale. Această platformă redefinește investigațiile, oferind cea mai rapidă și colaborativă soluție pentru analiza datelor mobile, completată de o putere de procesare scalabilă și suport extins pentru extragerile native și parsarea artefactelor mobile. Prin integrarea analizei datelor mobile cu probele tradiționale obținute de pe computere, FTK creează o imagine de ansamblu completă. Această abordare permite identificarea relațiilor, tiparelor de comunicare și aliasurilor cunoscute, oferind investigatorilor un avans decisiv în derularea anchetelor.

FUNCȚIONALITĂȚI FTK 8.1

Procesarea datelor extrase de pe dispozitive mobile

După clonarea unui dispozitiv Android sau iOS, datele pot fi integrate în FTK pentru o analiză unificată, alături de alte dovezi informatice conexe.

Exterro nu înlocuiește soluțiile consacrate pentru clonarea dispozitivelor mobile, ci le completează, oferind investigatorilor posibilitatea de a folosi instrumentul preferat pentru extragerea datelor. Ulterior, aceștia pot analiza cu ușurință dovezile extrase, inclusiv datele aplicațiilor de mesagerie, în contextul probelor informatice asociate, utilizând platforma FTK, integrandu-le într-un singur caz.

Analiza aplicațiilor de mesagerie

FTK oferă investigatorilor posibilitatea de a analiza mesaje din peste 35 de platforme de chat, inclusiv iMessage, Twitter și WhatsApp. Mesajele sunt reconstruite într-un format aproape original, facilitând interpretarea conversațiilor. FTK 8.1 aduce îmbunătățiri semnificative, precum:

- filtre pentru datele din chat, care permit focalizarea pe intervale de timp cheie,
- suport pentru răspunsuri inline, mesaje șterse și editate,
- traducerea automată a limbajului din conversații,
- Google Takeouts,
- parsare pentru artefacte iOS 17, KMZ, Biome și multe altele.

Aceste funcționalități permit o analiză mai eficientă și completă a datelor din aplicațiile de mesagerie.

Analiza și identificarea tiparelor de comunicare ale entităților analizate

Modulul inovator Entity Management din FTK simplifică analiza tiparelor complexe de comunicare, oferind o înțelegere clară și rapidă a relațiilor dintre utilizatori.

Acesta permite:

- Identificarea și combinarea aliasurilor cunoscute, atât automat, cât și manual;
- Vizualizarea celor mai comunicative entități și aplicații de chat, pentru o analiză concentrată;
- Gruparea conversațiilor pe utilizatori și nu în funcție de aplicațiile de chat utilizate.

Această abordare oferă investigatorilor o perspectivă unificată asupra relațiilor și interacțiunilor dintr-un caz, înainte de analiza detaliată a artefactelor individuale.

Îmbunătățirea modalității de raportare

Noul generator de rapoarte complet personalizabil din FTK le permite investigatorilor să organizeze și să prezinte dovezile într-o narațiune clară și coerentă. Prin revizuirea datelor mobile și a celor de pe calculatoare într-un singur fișier de caz FTK, poți crea mult mai ușor un raport unificat, fără a fi necesar să folosești mai multe instrumente pentru a genera rapoarte separate.

- În rapoarte se pot încorpora conversații, documente, e-mailuri, multimedia și cronologii.
- Se pot selecta cuvinte cheie care vor fi evidențiate automat în datele raportului.
- Se poate adăuga logoul propriu, antete, subsoluri și personalizări pentru aspectul coloanelor.
- Rapoartele se salvează cu ușurință în

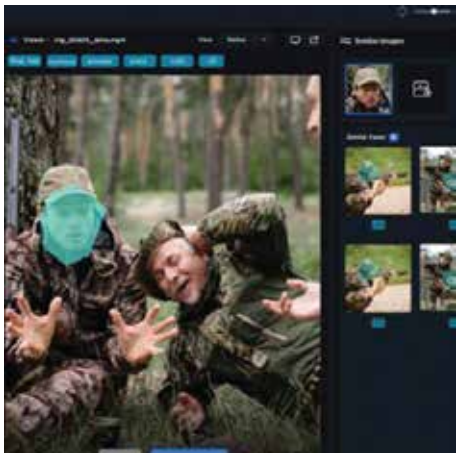
formatele Word și PDF sau se pot crea șabloane pentru un strat rapid.

Revizuire multimedia cu ajutorul AI

Utilizezi AI pentru a identifica automat elemente cheie din fotografii și videoclipuri. Realizezi recunoaștere avansată a imaginilor și facială, precum și potrivirea fețelor similare pe întregul set de date.

Identifici rapid imagini care conțin persoane, vehicule, bani și multe altele. Găsești și potrivești fețele trasând un cerc în jurul feței pe care vrei să o localizezi.

Elimină orele de revizuire manuală a



videoclipurilor, folosind AI pentru a marca automat elemente cheie, cum ar fi armele sau drogurile, în fișierele video.

În România, **soluțiile Exterro** sunt furnizate de către ProVision, unul dintre cei mai importanți distribuitori „value added" (VAD) de soluții și produse de securitate cibernetică din țară. Pe lângă distribuție, compania oferă servicii specializate de consultanță, monitorizare, detecție și răspuns la incidente de securitate a informațiilor prin intermediul echipei ProActive Hunt. Pentru mai multe detalii, vizitați **provision.ro.**

„Noul modul de management al entităților (Entity Management) din FTK reprezintă o schimbare majoră în domeniu. Odată ce confirmăm proprietarul unui dispozitiv, primul nostru pas într-o investigație este să determinăm cine este acea persoană, iar astfel petrecem ore întregi analizând cu cine și cum comunica. Cu managementul entităților, acum înțelegem imediat aceste tipare de comunicare, având o privire de ansamblu asupra tuturor conversațiilor utilizatorului dispozitivului din toate aplicațiile și nu mai suntem nevoiți să folosim metoda veche de a citi manual mii de thread-uri de chat, unul câte unul. Această funcționalitate va reprezenta o adevărată revoluție în industria noastră."

— INSPECTOR ȘEF, O importantă agenție de poliție din Europa

Broadcom introduce prima capacitate de predicție a incidentelor din industrie pentru a opri atacurile

Broadcom a recent lansat recent Incident Prediction, o capacitate de securitate de primă importanță în industrie care extinde Adaptive Protection, o caracteristică unică a Symantec Endpoint Security Complete (SES-C), prin valorificarea AI pentru a identifica și perturba atacurile terestre și alte atacuri TL-off.

Instruit pe un catalog de peste 500.000 de lanțuri de atac din lumea reală, construite de echipa Symantec Threat Hunter de clasă mondială, Incident Prediction pune din nou avantajul în mâinile apărătorilor prin: prezicerea comportamentelor atacatorilor, împiedicând următoarea lor mișcare în lanțul de atac chiar și atunci când folosesc software legitim și apoi readucerea rapidă a întreprinderii la starea normală. Cu Incident Prediction, SES-C oferă o rezistență cibernetică excepțională împotriva adversarilor motivați.

Cu Incident Prediction, analiștii SOC și alți profesioniști în securitate pot:

Automatiza atenuarea și perturba atacatorii: identificarea automată a următorilor pași pe care un anumit atacator îi va face cel mai probabil pe baza tiparelor de atac din trecut. Apoi se aplică politici de atenuare pentru a bloca acele acțiuni anticipate, perturbând progresul majorității atacatorilor înainte ca aceștia să își poată atinge obiectivul final de a cripta datele sau de a filtra informații.

Reduce sarcina pentru analiștii SOC: se elimină necesitatea ca analiștii SOC să trieze manual alertele, să analizeze secvențele de atac și să determine strategii de atenuare. Se ocupă de acest lucru automat, eliberându-i pe analiști să se concentreze asupra altor priorități de securitate.

Evite impactul asupra afacerii: Incident Prediction oferă comportamente specifice granulare ale atacatorilor pentru a bloca limitarea impactului asupra proceselor normale de afaceri. O zi obișnuită, dar măsurile brute de atenuare, care perturbă afaceri, cum ar fi carantinarea mașinilor, închiderea rețelei, eliminarea accesului utilizatorilor sau reimaginarea mașinilor sunt în mare măsură inutile.

Reduce suprafața de atac: îmbunătățirea Symantec Adaptive Protection, care identifică și recomandă blocarea aplicațiilor și comportamentelor cu prevalență scăzută pentru a micșora în mod proactiv suprafața de atac. Ajută la închiderea „ușilor" atacatorilor și a tehnicilor lor comune de atac.

SolvIT Networks este partener strategic pentru Europa Centrală și de Est al Broadcom.

Eficiență în managementul securității și conformității

Securitatea cibernetică deficitară este principalul motiv pentru care IMM-urile se numără printre victimele preferate de atacatori. În 2024, Europa a înregistrat o creștere alarmantă a extorsiunii cibernetice care vizează IMM-urile (53%), față de anul precedent.

Provocările cu care se confruntă IMM-urile în domeniul securității cibernetice sunt numeroase, fapt care subliniază nevoia de aplicații specializate pentru îmbunătățirea posturii de securitate.

Pentru a răspunde acestor provocări, **Safetech Innovations a dezvoltat platforma integrată ISAM.** Fiind dedicată automatizării procesului de management al securității informației, soluția eficientizează activități precum inventarierea proceselor de business și a sistemelor informatice, managementul vulnerabilităților, analiza și managementul riscurilor de securitate, gestiunea incidentelor și indicatorilor de securitate, agregând toate datele într-o singură aplicație.

Safetech Innovations pune la dispoziția organizațiilor o versiune nouă și optimizată a ISAM, care asigură o imagine de ansamblu completă asupra posturii de securitate a organizației, prin următoarele componente cheie:

- **Tablou de bord intuitiv**, cu vizualizări pentru analiza scorurilor de securitate, vulnerabilităților, grafice active, riscuri, neconformități, indicatori de securitate, evenimente și incidente de securitate.

- **Incident Management.** Oferă un registru electronic pentru gestionarea tuturor incidentelor pe tot parcursul ciclului lor de viață. Asigură un cadru pentru eficientizarea răspunsului la incidente și minimizarea timpilor de nefuncționare, fiind o sursă unică de informații pentru evenimente și incidente de securitate.

- **Inventory** facilitează gestiunea proceselor de business (dezvoltare produse, logistică, resurse umane, contabilitate etc.), a serviciilor și activelor IT, împreună cu riscurile și vulnerabilitățile asociate. Componenta este importantă în procesele de identificare a vulnerabilităților, atenuarea riscurilor și conformitatea cu cadrele de reglementare (ISO 27001, NIS 2, GDPR), care impun organizațiilor menținerea unui inventar detaliat al activelor deținute. ISAM asigură un depozit centralizat și constant actualizat al tuturor proceselor de business, al serviciilor și al activelor informatice.

- **Vulnerability Management.** Managementul vulnerabilităților (identificate în interiorul și în exteriorul rețelei organizației) oferă un suport centralizat pentru descoperirea evaluarea și remedierea vulnerabilităților, reducând suprafața de atac. Include o componentă de scanare, care gestionează rezultatele scanărilor din diferite instrumente de scanare a vulnerabilităților. Permite urmărirea statusului ticketelor, al eforturilor de remediere și programarea unor scanări recurente.

- **Security Indicators** permite organizațiilor să definească, să monitorizeze și să analizeze metrici de proces, indicatori de performanță (KPI) și indicatori de risc (KRI) pentru a urmări tendințele generale ale proceselor. KPI măsoară eficacitatea proceselor de securitate, pe când KRI urmăresc

expunerile potențiale la risc, oferind semnale de avertizare timpurie.

• **Risk Management** permite crearea și gestiunea fișelor de risc și efectuarea evaluărilor de risc. Ajută organizațiile să identifice, evalueze și să atenueze riscurile de securitate, asigurând confidențialitarea și integritatea activelor critice.

• **Compliance Management**. ISAM facilitează și analiza conformității, pentru a urmări dacă organizația îndeplinește standardele și reglementările de securitate aplicabile. Eficientizează și simplifică procesul de conformitate la NIS 2 sau DORA printr-o zonă centralizată pentru evaluarea, urmărirea și raportarea posturii de conformitate.

• **Reports.** Pentru a răspunde diferitelor cerințe de raportare, ISAM permite generarea a două tipuri de rapoarte: de monitorizare și de securitate. Acestea permit evidențierea metricilor și tendințelor de securitate.

• **Settings** este o componentă prin care aplicația poate fi configurată și customizată, inclusiv configurarea de nomenclatoare, contacte, utilizatori, roluri, șabloane de e-mail, subrețele etc.

ISAM poate fi rulată (1) din cloud, (2) de pe un server găzduit de Safetech Innovations sau (3) de pe infrastructura IT on-premises a clientului, fiind accesată printr-o interfață web.

Clienții au la dispoziție trei variante de licențiere, „Essential", „Advanced" și „Elevate", care diferă în funcție de funcționalitățile disponibile și integrările opționale. Prețul anual pentru utilizarea aplicației este dimensionat în funcție de variantă și de numărul de active gestionate.

De asemenea, ISAM permite adăugarea de servicii Safetech MSP sau MSSP și a scannerului de vulnerabilități Tenable Nessus as-a-Service.

Clienții existenți ai ISAM beneficiază de noua versiune a soluției și funcționalitățile asociate tipului de licențiere actual.

Cele mai bune practici în protejarea confidențialității și a datelor personale

Soluțiile de stocare de tip air-gapped – dispozitive de stocare criptate hardware care pot fi gestionate de angajați și păstrate offline – reprezintă cea mai puternică formă de securitate cibernetică pentru datele mobile. Aceste dispozitive dispun de sisteme de securitate integrate permanent, necesită autentificare adecvată și includ un mecanism de autodistrugere pentru a proteja împotriva încercărilor de ghicire a parolelor.

Unitățile criptate sunt concepute special pentru a proteja atât datele stocate, cât și dispozitivele la care sunt conec Seria Kingston IronKey™ oferă dispozitive concepute pentru a securiza datele și rețelele într-o lume interconectată, în care securitatea IT este atât un standard, cât și un avantaj competitiv. Aceste unități dispun de memorie flash de înaltă performanță, oferă backup local securizat și adaugă un strat suplimentar de protecție a datelor, sporind confidențialitatea. Unitățile USB criptate sunt robuste, având carcase rezistente la manipulare, firmware semnat digital,

tastaturi virtuale și moduri complexe de acces, alături de numeroase alte caracteristici adăugate de-a lungul anilor pentru a se adapta peisajului tehnologic în continuă evoluție.

Seria IronKey include modelele Vault Privacy 50, Keypad 200 și SSD-ul extern Vault Privacy 80. Aceste dispozitive, criptate hardware cu AES 256-bit și conforme cu standardul FIPS 140-3, oferă atât managerilor de nivel enterprise, cât și proprietarilor de afaceri mici siguranța că datele stocate vor rămâne protejate împotriva încercărilor de intruziune cibernetică, chiar și în cazul pierderii sau furtului dispozitivului fizic.

Pentru mai multe informații, vizitați **https://www.kingston.com/en/solutions/data-security/ironkey.**

Previzualizarea optimizărilor soluției fără parolă RSA Mobile FIDO

La RSA, misiunea a fost întotdeauna eliminarea verigilor slabe din securitatea digitală. Compania a anunțat recent o etapă semnificativă în această călătorie: previzualizarea soluției mobile FIDO, disponibilă în aplicația RSA Authenticator V4.4 pentru iOS și Android. RSA ID Plus este un server certificat FIDO2, iar odată cu această etapă, aplicația de autentificare pentru iOS și Android este acum un autentificator certificat FIDO2.

Acest lucru marchează angajamentul de a crea experiențe de pionierat sigure, intuitive și fără întreruperi pentru utilizatori – și încercarea de a eradica parolele odată pentru totdeauna.

Parolele au fost de multă vreme o vulnerabilitate critică în securitatea cibernetică, bazându-se pe memoria și discreția umană, ceea ce duce adesea la parole slabe, reutilizate. De mult timp, am acceptat soluții fără parolă, cum ar fi codul QR, biometria, codul de acces unic sau autentificatoare hardware certificate FIDO2, cum ar fi RSA DS100, pentru a aborda aceste vulnerabilități.

Această ultimă piatră de hotar oferă întreprinderilor siguranța fără parolă, adăugând suport de cheie de acces legat de dispozitiv (FIDO mobil) la aplicația noastră RSA Authenticator, oferind o alternativă sigură și ușor de utilizat, care elimină vulnerabilitatea preferată a infractorilor cibernetici, îmbunătățește securitatea organizațională și menține utilizatorii conectați și productivi.

Lider cu cheile de acces legate de dispozitiv

Cheile de acces au primit multă atenție, atât din cauza angajamentelor de la Facebook, Apple și Amazon pentru o soluție mai orientată spre consumatori, cât și pentru că Alianța FIDO a adoptat termenul „cheie de acces” pentru orice tip de acreditări FIDO. Acest lucru a condus la o anumită confuzie cu privire la ceea ce înseamnă exact o organizație atunci când folosește cuvântul „cheie de acces”, pe care am încercat să îl clarificăm.

Cea mai importantă distincție este diferența dintre cheile de acces legate de dispozitiv și cele sincronizate:

- **Chei de acces legate de dispozitiv:** Acest tip de cheie de acces este creat în siguranță și stocat pe un singur dispozitiv. Cheia privată nu părăsește niciodată dispozitivul, asigurând un nivel ridicat de securitate. Cheile de acces legate de dispozitiv minimizează riscul expunerii cheilor și oferă protecție robustă împotriva phishingului și a altor amenințări cibernetice. Aceasta înseamnă că cheia de acces nu poate fi utilizată pe un alt dispozitiv fără a o înregistra manual din nou, ceea ce o face opțiunea ideală pentru întreprinderi și organizațiile din sectorul public. Aceste soluții sunt rezistente la phishing și oferă un grad mai ridicat de securitate.
- **Cheile de acces sincronizate:** cheile de acces sincronizate sunt stocate și sincronizate pe mai multe dispozitive prin intermediul serviciilor cloud, oferind confortul de a accesa servicii pe diferite dispozitive fără a fi nevoie să le înregistrați pe fiecare în parte. Ele permit, de asemenea, recuperarea cheii de acces dacă dispozitivul gazdă este pierdut, furat

sau înlocuit, ceea ce este deosebit de util deoarece utilizatorii își actualizează adesea telefoanele mobile la fiecare doi ani. Deși acest lucru îmbunătățește confortul utilizatorului, necesită măsuri de securitate robuste pentru a proteja cheile de acces sincronizate în cloud. Cheile de acces sincronizate pot fi potrivite pentru utilizarea consumatorilor, dar este posibil să nu ofere același nivel de securitate necesar pentru mediile federale și de întreprindere.

Prin implementarea unei soluții cu cheie de acces legată de dispozitiv în aplicația RSA Authenticator pentru iOS și Android, contribuim la consolidarea cadrului Zero Trust al clienților noștri, asigurând o cale profund integrată și simplă către autentificarea fără parolă rezistentă la phishing. Această tehnologie elimină punctele slabe ale parolelor tradiționale, oferind o experiență de utilizator simplă și intuitivă.

Philip Corriveau, RSA, subliniază de ce este importantă această dezvoltare: „La RSA, credem că securitatea nu ar trebui să fie o barieră, ci o parte integrantă a experienței utilizatorului. Cu ajutorul cheilor de acces legate de dispozitiv în cadrul aplicației RSA Authenticator pentru iOS și Android, nu doar îmbunătățim securitatea; Transformăm modul în care utilizatorii interacționează cu identitățile lor digitale."

Cum protejează cheile de acces legate de dispozitiv împotriva atacurilor?

Cheile de acces legate de dispozitiv oferă mai multe straturi de securitate care neutralizează atacurile comune:

- **Phishing:** Deoarece cheia privată nu părăsește dispozitivul, atacatorii nu o pot intercepta sau fura prin încercări de phishing. Este imposibil din punct de vedere tehnic să phishing cheia de acces direct de pe dispozitivul unui utilizator. În timp ce actorii răi pot încerca să phishing accesul la cloud pentru a descărca o copie a cheii, cheia privată în sine rămâne securizată pe dispozitiv, împiedicând majoritatea atacurilor să reușească.
- **Inginerie socială:** cu cheile de acces legate de dispozitiv, cheia privată nu poate fi partajată sau extrasă. Utilizatorii nu trebuie să acceseze, să-și amintească sau să manipuleze cheia privată, ceea ce reduce semnificativ riscul atacurilor de inginerie socială. Atacatorii nu pot păcăli utilizatorii să dezvăluie ceva la care nu au acces.
- **Adversar în mijloc:** chiar dacă un atacator interceptează comunicarea dintre un serviciu și autentificator, nu poate folosi cheia publică singur pentru a obține acces.

Cheile de acces FIDO și mandatul prezidențial

În timp ce aproape fiecare organizație din fiecare sector poate beneficia de Mobile FIDO, soluția poate fi deosebit de valoroasă pentru agențiile guvernamentale care se străduiesc să îndeplinească mandatul prezidențial de securitate cibernetică și să respecte Ordinul executiv 14028 până la sfârșitul anului fiscal.

EO14028 cere agențiilor guvernamentale să folosească soluții fără parolă, rezistente la phishing pentru a-și autentifica utilizatorii. Este o componentă critică a modernizării și apărării infrastructurii critice, dar necesită agențiilor guvernamentale să acționeze rapid și să implementeze o soluție dovedită.

„Cheia de acces certificată FIDO2, legată de dispozitiv de la RSA este un atu important pentru agențiile federale care se străduiesc să respecte mandatul prezidențial și termenul limită pentru FY2024", a declarat **președintele federal RSA, Kevin Orr.** „Mai mult decât bifarea unei casete, RSA poate aduce zeci de ani de pedigree pe primul loc în securitate și o soluție unificată, scalabilă și ușor de utilizat, care poate îmbunătăți colaborarea pentru sectorul public."

La ce să vă așteptați de la soluția RSA mobil FIDO fără parolă

Soluția mobilă FIDO este un pas crucial către oferirea unei experiențe consecvente și fără parolă, de la început până la sfârșit. Aplicația RSA Authenticator V4.4 pentru iOS și Android acceptă FIDO mobil ca previzualizare tehnică. Capacitatea FIDO mobilă va fi disponibilă în general cu aplicația RSA Authenticator V4.5 pentru iOS și Android. Această versiune va include îmbunătățiri suplimentare și o experiență de utilizator simplificată.

Consolidarea încrederii zero cu soluția mobilă fără parolă a RSA

Soluția RSA mobil FIDO este o potrivire puternică pentru mediile Zero Trust, în care accesul sigur și fără parolă este crucial. Cheile de acces legate de dispozitiv se aliniază cu principiile Zero Trust prin verificarea fiecărei încercări de acces fără a se baza pe parole, care sunt vulnerabile la phishing și la furtul de acreditări. Cu cheile de acces legate de dispozitiv, cheia privată rămâne în siguranță pe dispozitivul original, asigurându-se că accesul este limitat doar la dispozitivele verificate – ideal pentru protejarea forței de muncă la distanță și hibridă.

Pe lângă o securitate mai bună, soluția RSA mobil FIDO îmbunătățește flexibilitatea, permițând accesul ușor în mediile de lucru, reducând întreruperile, păstrând în același timp datele sensibile în siguranță. Pe măsură ce mandatele guvernamentale impun autentificarea rezistentă la phishing, soluția RSA mobil FIDO ajută organizațiile nu numai să asigure nevoile de astăzi, ci și să se pregătească pentru standardele de mâine.

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

Vertiv™ PowerUPS 9000: Un nou standard în protecția alimentării

Cererea tot mai mare pentru infrastructuri de alimentare fiabile și performante în centrele de date și mediile industriale a condus la dezvoltarea unor soluții de ultimă generație, precum Vertiv™ PowerUPS 9000. Proiectat pentru a asigura o alimentare neîntreruptă cu eficiență maximă, acest sistem UPS se remarcă prin designul său modular, rezistența și adaptabilitatea la diverse aplicații.

Un avantaj esențial al Vertiv™ PowerUPS 9000 este eficiența sa energetică remarcabilă, care ajunge până la 97,5% în modul de conversie dublă și până la 99% în modul online dinamic. Această performanță contribuie la reducerea consumului de energie și a cerințelor de răcire, ceea ce se traduce prin costuri operaționale mai mici și un impact redus asupra mediului. Datorită tehnologiei de conversie fără transformator, cu IGBT pe trei nivele, sistemul oferă o performanță optimizată, fiind o soluție economică pentru companiile ce doresc un echilibru între fiabilitate și eficiență.

Scalabilitatea este o altă caracteristică definitorie a PowerUPS 9000. Cu o capacitate de putere cuprinsă între 250 kW și 5 MW, acesta oferă flexibilitatea necesară atât pentru implementări de mici dimensiuni, cât și pentru proiecte de amploare. Modulele de putere și bypass-ul static hot-swappable,permit întreținerea fără opriri, permitând funcționarea continuă chiar și în timpul actualizărilor de sistem. În plus, amprenta sa compactă economisește până la 32% mai mult spațiu comparativ cu modelele anterioare, făcându-l o soluție ideală pentru medii unde eficiența utilizării spațiului este esențială.

Fiabilitatea reprezintă un aspect fundamental al PowerUPS 9000. Fiecare modul de putere funcționează autonom,

cu sisteme de control separate, permițând izolarea defecțiunilor și prevenind propagarea acestora. Sistemul include, de asemenea, un comutator static solid-state cu funcționare continuă, care îmbunătățește disponibilitatea energiei printr-un mecanism de siguranță eficient în cazul variațiilor neprevăzute. Instrumente avansate de diagnostic, cum ar fi tehnologia Waveform Capture, permit o analiză detaliată a calității energiei, facilitând identificarea și soluționarea problemelor înainte ca acestea să afecteze performanța sistemului. În plus, PowerUPS 9000 este conceput pentru a face față condițiilor de mediu extreme, având certificare seismică și protecție împotriva supratensiunilor și fluctuațiilor de tensiune.

Prin integrarea capabilităților de monitorizare bazate pe inteligență artificială, PowerUPS 9000 funcționează împreună cu Vertiv™ Life™ Advanced Incident Management, permițând monitorizarea în timp real a stării sistemului și întreținerea predictivă. Este complet compatibil cu Building Management Systems (BMS) și Network Management Systems (NMS), susținând protocoale de comunicație precum Modbus, SNMP și BACnet, oferind astfel o integrare fără probleme în infrastructurile existente. Capacitățile avansate de detectare a defectelor și diagnosticare la distanță îmbunătățesc eficiența operațională, permițând companiilor să identifice și să remedieze potențialele defecțiuni înainte ca acestea să devină probleme critice.

Versatilitatea PowerUPS 9000 se extinde în multiple industrii. Este deosebit de potrivit pentru centrele de date hyperscale și întreprinderi, care necesită o densitate mare de putere și redundanță pentru a menține operațiunile neîntrerupte. De asemenea, susține aplicații critice în sănătate, producție și telecomunicații, unde chiar și o scurtă întrerupere a alimentării poate avea consecințe semnificative. Capacitățile sale avansate de răspuns la sarcină îl fac o alegere ideală pentru AI și medii de calcul de înaltă performanță, unde fluctuațiile

de putere pot fi imprevizibile. Funcția inteligentă de paralelizare a sistemului menține o eficiență optimizată chiar și la sarcini parțiale, făcându-l o soluție eficientă pentru organizațiile care doresc să reducă costurile energetice.

Dincolo de performanță, **PowerUPS 9000** contribuie la reducerea costului total de proprietate (TCO) prin consumul optimizat de energie și cerințele reduse de răcire. Susținând tehnologiile de baterii litiu-ion și nichel-zinc, acesta facilitează eficiența și fiabilitatea pe termen lung, minimizând nevoile de întreținere. În plus, arhitectura distribuită a sistemului de baterii îmbunătățește eficiența stocării energiei, oferind o toleranță crescută la fluctuațiile de putere și durate extinse de backup.

Pentru a permite fiabilitatea și performanța pe termen lung ale infrastructurii critice de alimentare, este necesară o strategie completă de servicii și suport. Vertiv oferă servicii integrate pentru proiecte și întreținerea UPS-urilor pe întreaga durată a ciclului de viață, acoperind toate etapele, de la planificarea inițială și instalare până la întreținerea continuă și optimizarea sistemului. Faza de punere în funcțiune include testări riguroase pentru a obține conformitatea cu standardele de performanță și siguranță. După punerea în funcțiune, rețeaua globală de ingineri de service Vertiv asigură suport non-stop, diagnosticare la distanță și întreținere predictivă, ajutând afacerile să prevină opririle costisitoare. Cu mai mult de 3.500 de ingineri de service globali și instrumente avansate de monitorizare, Vertiv subliniază că soluțiile sale UPS funcționează la eficiență maximă pe întreaga lor durată de viață. Testele de acceptanță în fabrică și centrele de experiență pentru clienți ale companiei permit organizațiilor să evalueze performanța sistemului în scenarii reale înainte de implementare, oferind o tranziție fără întreruperi către operațiuni critice.

Cu tehnologia sa de ultimă generație, scalabilitatea modulară și capabilitățile inteligente de monitorizare, Vertiv™ PowerUPS 9000 stabilește un nou standard în protecția alimentării. Indiferent dacă este vorba despre centre de date mari, facilități industriale sau aplicații bazate pe inteligență artificială, oferă fiabilitate, eficiență și flexibilitate neegalate. Pentru afacerile care doresc să îmbunătățească infrastructura de alimentare pentru a fi pregătite pentru viitor, PowerUPS 9000 reprezintă o soluție robustă și inovatoare care susține operațiuni neîntrerupte și economii pe termen lung.

Pentru mai multe informații despre Vertiv PowerUPS 9000, vizitați **Vertiv.com** sau contactați experții locali Vertiv la **emea.ro@Vertiv.com.**

„Continuitatea alimentării cu energie este o cerință indispensabilă pentru mediile esențiale de astăzi. Vertiv™ PowerUPS 9000 este proiectat pentru a oferi reziliență maximă, eficiență și adaptabilitate, permițând companiilor să construiască o infrastructură energetică pregătită pentru viitor. Datorită scalabilității și capacităților avansate de monitorizare, este alegerea ideală pentru organizațiile care nu își permit nici măcar un moment de întrerupere. În plus, sistemul său inteligent de gestionare a bateriilor prelungește durata de viață a acestora, reducând costurile de înlocuire și susținând o operare mai eficientă."

George Topalov,
Senior Sales Manager la Vertiv Romania

DeepSeek și riscurile securității cibernetice

Lansarea și popularitatea asistentului AI DeepSeek au atras nu doar atenția utilizatorilor, ci și pe cea a infractorilor cibernetici. Fără o supraveghere centralizată, natura open-source a platformei creează oportunități atât pentru inovație, cât și pentru exploatare rău intenționată.

Atacatorii pot folosi versiuni compromise ale software-ului, pagini de înregistrare false sau chiar token-uri cripto speculative pentru a înșela utilizatorii și a compromite securitatea datelor. Deși DeepSeek nu oferă detalii specifice despre natura atacului cu care s-a confruntat, este important să înțelegem că infractorii cibernetici vor căuta inevitabil să exploateze astfel de instrumente în scopuri rău intenționate. Kaspersky a observat tendințe similare cu alte modele populare de inteligență artificială, care au fost utilizate pentru activități precum crearea de e-mailuri de tip phishing, traducerea textului, generarea de scripturi și efectuarea de cercetări open-source pentru a produce conținut mai direcționat și mai convingător. Aceste instrumente pot fi folosite și ca momeală pentru a răspândi escrocherii și aplicații rău intenționate.

Ceea ce iese în evidență în cazul DeepSeek este natura sa open-source, care este o sabie cu două tăișuri. În timp ce cadrul open-source încurajează transparența, colaborarea și inovația, el introduce, de asemenea, riscuri etice și de securitate semnificative. Când utilizați un instrument open-source, nu puteți fi întotdeauna sigur cum sunt gestionate datele dumneavoastră, mai ales dacă altcineva le-a implementat. Exploatarea software-ului open-source a fost o tendință majoră în peisajul amenințărilor anul trecut, infractorii cibernetici derulând campanii complexe pentru a încorpora malware. În 2024, scanerul open-source Kaspersky a detectat peste 12.000 de pachete rău intenționate în depozite deschise. Fără supraveghere centralizată, infractorii pot începe să creeze versiuni compromise de software sau să introducă programe de tip backdoor deghizate drept instrumente legitime pentru utilizarea API-ului DeepSeek, generând riscuri grave pentru utilizatori și organizații.

Noul asistent DeepSeek AI a atras multă atenție în ultimele zile și au fost observate mai multe cazuri de înșelătorie legate de acesta.

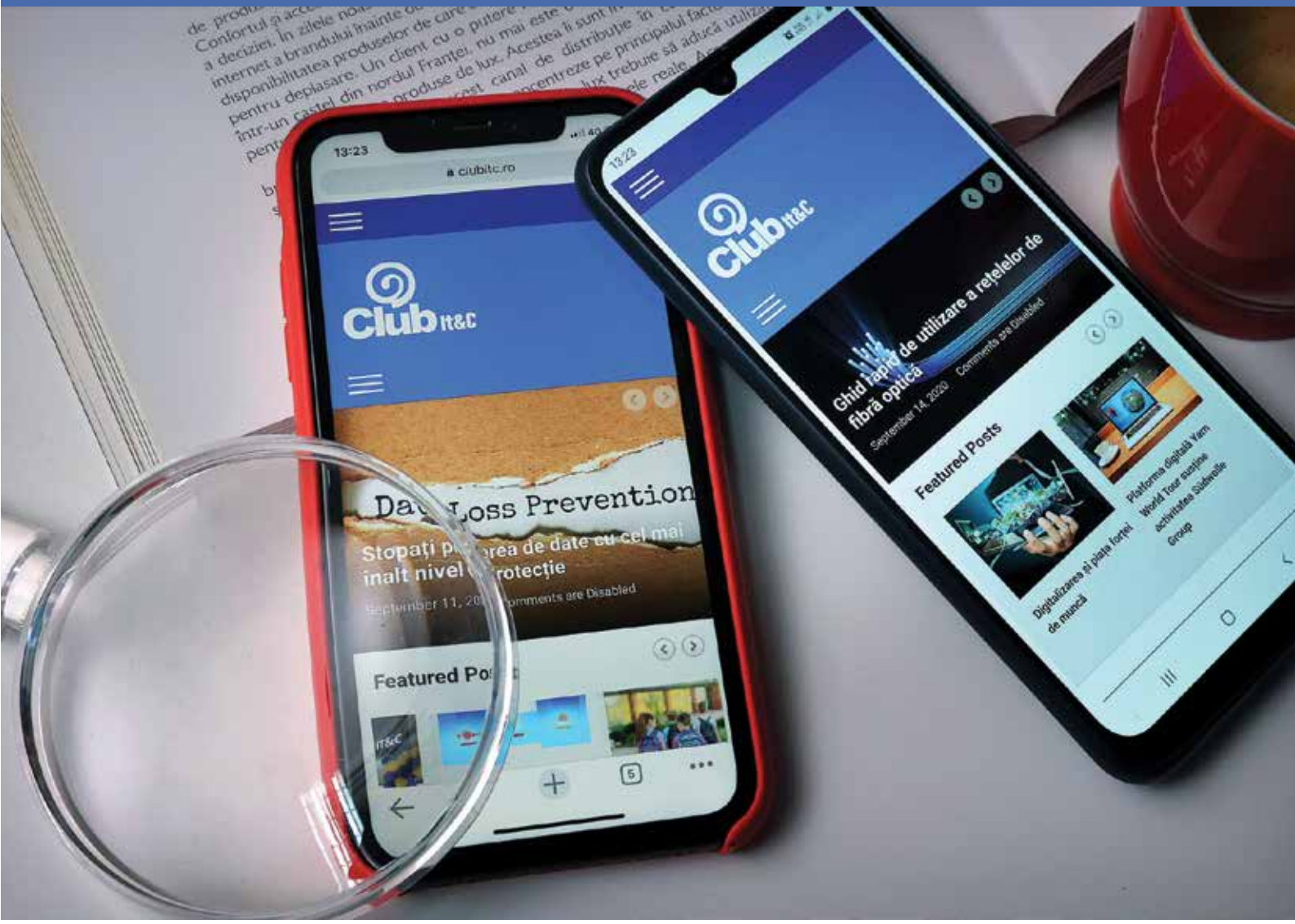
Din cauza numărului mare de utilizatori noi și a unui presupus atac cibernetic asupra DeepSeek, există erori în procesul de înregistrare pe aplicația și site-ul web DeepSeek – multe înregistrări nu pot fi finalizate. Această situație poate fi exploatată de infractorii cibernetici pentru a fura acreditările utilizatorilor prin pagini web false care imită DeepSeek.

Prin astfel de pagini de înregistrare false, atacatorii pot colecta e-mailurile și parolele utilizatorilor. Acestea pot fi exploatate pentru a accesa conturile utilizatorilor – pe DeepSeek sau în alte servicii (dacă parola este aceeași pentru mai multe conturi).

De asemenea, au apărut mai multe noi token-uri cripto bazate pe entuziasmul generat de DeepSeek, disponibile pentru vânzare. Acestea nu sunt asociate oficial cu brandul DeepSeek, astfel încât capitalizarea lor este speculativă.

Pentru a vă proteja de astfel de atacuri, verificați cu atenție adresele paginilor care solicită date de acreditare sau logare, asigurați-vă că toate parolele dvs sunt puternice și unice, utilizați întotdeauna **autentificarea cu doi factori** și folosiți **protecție fiabilă** pentru toate dispozitivele dumneavoastră.

more information, better solutions



Premium content • Analysis • Trends • Studies • Business Solutions • News

Club IT&C

www.clubitc.ro www.clubitc.eu

Data Management and Business Solutions

INFORM

Member of AUSTRIACARD HOLDINGS