Club IT&C
WWW.CLUBITC.RO
APRILIE 2024

DISASTER RECOVERY, prioritate reală pentru companiile românești

Remedierea vulnerabilităților software

Soluții avansate pentru securitatea în mediul industrial

Securitatea cibernetică a soluțiilor video

M247

Pe lângă atacurile cibernetice, o altă problemă în desfășurarea unei afaceri o reprezintă dezastrele naturale (cutremure, incendii, inundații, etc) și defecțiunile echipamentelor IT (calculatoare, servere, rutere, switch-uri, etc), care cauzează întreruperea producției și/sau pierderea de informații importante pentru compania respectivă.

Cu o experiență de **peste 20 ani în mediile centrelor de date** și o **rețea globală** de invidiat în industrie suntem alegerea perfectă ca **partener tehnologic pentru protejarea și securizarea activelor** tale business.

Protejează-ți și securizează-ți infrastructura, rețeaua, sistemele (aplicațiile) și datele cu soluția

M247 Disaster Recovery

Această soluție este construită cu ajutorul **tehnologiilor Dell** și **dispozitive de stocare scalabile** și **redundante** de mare capacitate, atingând **192TB într-un singur pool de date.** Pentru replicarea datelor folosim soluții consacrate de la **Veeam** și **Zerto** (Veeam a fost declarat lider în 2022, pentru al șaselea an consecutiv în Cadranul Magic Gartner pentru Soluțiile Software de Backup și Replicare Enterprise).

Prin soluția **M247 Disaster Recovery** oferim:

- Separarea geografică a datelor companiei tale
- Protecția datelor împotriva dezastrelor naturale
- Recuperarea ușoară a datelor în orice moment
- Inamovibilitatea datelor (datele salvate nu pot fi criptate, modificate sau șterse în urma unor atacuri cibernetice)
- Costuri reduse prin folosirea unei soluții "as a service"
- Suport specializat de la experții M247

Contactează-ne pentru mai multe detalii:
www.m247.com/ro-ro/
office@m247.com


Allied Telesis


AXIS
COMMUNICATIONS


asee
by asseco


BRINEL


BiT
software
ENTERSOFT


BUCHAREST
PROMOROBOTS


Crayon


LIFEINCLOUD


hp


INFORM
Member of AUSTRIACARD HOLDINGS


KASPERSKY lab


LIFE
IS
HARD
WORK SOFT


Club IT&C


METAMINDS
Tech meets trust.


M247


milestone


PRO SYS


Relevance


Romsym Data


SAFETECH
INNOVATIONS


Schneider
Electric


SOFTNET
CONSULTING


SOLVIT
works naturally


SYSTEM INNOVATION ROMANIA


TCL
The Creative Life


TOTAL
Technologies


veeAM


VERTIV.


vodafone


xiaomi

pag. 12 **Soluții avansate pentru securitatea în mediul industrial**

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

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

Cheltuielile de securitate informatică vor avea un vârf în 2024

Conform raportului Technology spending intentions elaborat de TechTarget în colaborare cu ESG, serviciile şi tehnologia de securitate informatică vor deveni în acest an principalele zone de investiţii IT în regiunea EMEA, în sectoare care nu se limitează la securitatea informatică a firmei, ci şi la reţelistică, infrastructură, aplicaţii DevSecOps şi GenAI. **de Bogdan Marchidanu**

Cu 48% din organizaţiile din EMEA plănuind să îşi crească cheltuielile IT în acest an – 22% dintre acestea cu un volum de peste 10% – şi cumpărătorii optimişti în ansamblu în privinţa bugetelor pentru tehnologie în 2024, securitatea informatică se prefigurează a fi principalul beneficiar al acestei tendinţe, circa 63% din firme intenţionând să-şi efectueze cheltuielile în acest sector în acest an, faţă de doar 4% care au declarat că intenţionează să scadă nivelul cheltuielilor. În total, 49% din respondenţi au spus că securitatea informatică a devenit "semnificativ" mai importantă pentru firma lor în ultimii doi ani. Respondenţii din EMEA au citat, de asemenea, îmbunătăţirea rezilienţei securităţii informatice ca principală justificare pentru toate cheltuielile IT, conform datelor. Această tendinţă ascendentă va fi în mod cert influenţată în viitorul imediat de o gamă largă de noi reglementări legislative la nivel european, inclusiv de diverse iniţiative UE precum Digital Services Act, Data Act, European Health Data Space, Data Governance Act şi AI Act, toate acestea vizând o mai mare transparenţă, utilizarea responsabilă a datelor şi securitatea informatică îmbunătăţită.

Între timp, noul document Cybersecurity Certification Scheme emis de Comisia Europeană ar putea ajuta la creşterea standardelor de securitate şi, prin aceasta, la bugetarea mai bună a, printre altele, cloud-ului şi reţelisticii 5G.

La nivel global, principalele trei zone de cheltuieli în 2024 par a fi managementul vulnerabilităţii, testarea pătrunderilor ilegale şi prevenirea pierderilor de date. Ele sunt urmate de autentificarea multi-factor, acces la reţea zero-trust, securitate a e-mailurilor, confidenţialitateaşi guvernanţa datelor şi accesul de tip single sign-on.

Riscurile cibernetice sunt prioritizate de numai un sfert dintre companiile din ECE

Companiile din Europa Centrală și de Est (ECE), prioritizează riscurile "tradiționale", adică instabilitatea economică, situația geopolitică și volatilitatea macroeconomică, în detrimentul celor digitale, tehnologice sau cibernetice (cum ar fi ransomware, piraterie și urmărire), conform studiului PwC 2024 Digital Trust Insights Survey.

Doar 27% dintre companiile din ECE prioritizează riscurile digitale și tehnologice, față de 51% la nivel global, iar 37% acordă o importanță ridicată riscurilor cibernetice, față de 43%. În schimb 47% dintre respondenți consideră volatilitatea macroeconomică o prioritate (vs 41% la nivel global).

În evaluarea amenințărilor cibernetice care provoacă îngrijorare în următoarele 12 luni, cele mai multe companii din ECE (44%) menționează operațiunile de hack-and-leak, comparativ cu media globală de 37%, evidențiind accentul regional pe protecția datelor.

Consecințele unui atac cibernetic care îi îngrijorează pe cei mai mulți respondenți din ECE (54%) se referă la pierderea datelor despre clienți, angajați sau tranzacții, aproape de media globală de 52%. Preocupările legate de daunele aduse brandului companiei, inclusiv pierderea încrederii clienților, sunt aproape identice, cu 49% în ECE și 50% în media globală.

Creșterea bugetului de investiții, o necesitate

La nivel de buget, companiile din Europa Centrală și de Est par să caute modalități de creștere a investițiilor în securitate cibernetică. În acest moment, există discrepanțe și investiții inegale în soluții, instrumente și formare de securitate cibernetică.

Doar 7% dintre respondenți (vs 10% la nivel global) se așteaptă la o creștere substanțială a bugetului de investiții, de peste 15%, iar 21% dintre organizații estimează o majorare de 6-10% a bugetului (vs 31% global). În același timp, 23% dintre respondenții din regiune intenționează să își mențină bugetele cibernetice neschimbate, spre deosebire de 9% la nivel global și în Europa de Vest.

Interesant este că un număr considerabil mai mare de participanți din ECE au raportat o lipsă de conștientizare cu privire la bugetul cibernetic.

În următoarele 12-18 luni, companiile din regiune vor pune un accent mai mare pe securitatea rețelelor (40%), depășind media globală de 28%, astfel indicând un angajament puternic pentru întărirea infrastructurii de bază. În plus, organizațiile acordă prioritate securității în cloud la 34% și gestionării identității și accesului (30%) într-o măsură puțin mai mare decât omologii la nivel mondial, 33% și, respectiv, 21%.

Tot la categoria bugete, majoritatea companiilor din ECE se așteaptă la creșterea costurilor de conformitate (la nivel global: 75%). În general, în Uniunea Europeană există un focus destul de mare pe acest aspect, având în vedere cerințele NIS2 / DORA / Cyber Resilience Act, care solicită un nivel ridicat de maturitate si transparență privind practicile cibernetice.

Codași la utilizarea AI în detectarea amenințărilor cibernetice

Inovația se concentrează pe detectarea mai bună a amenințărilor cibernetice

existente și îmbunătățirea funcțiilor de securitate pentru a compensa lipsa specialiștilor și a optimiza costurile. Când vorbim despre inovație, inteligența artificială joacă un rol important în lupta contra atacurilor cibernetice. Regiunea ECE rămâne în urma mediei mondiale în ceea ce privește implementarea inițiativelor de securitate cibernetică și realizarea beneficiilor acestora. Utilizarea Large Language Models (LLM) și a inteligenței artificiale generative în detectarea și reducerea riscurilor se situează la doar 9%, spre deosebire de 21% la nivel global. În plus, 20% dintre respondenții din ECE nu au planuri de implementare a acestor inițiative, spre deosebire de 7% dintre respondenții la nivel mondial.

Cleafy recurge la AI ca să ajute băncile în scop de protecție

Cleafy, companie de prevenție a fraudelor şi securitate informatică, a lansat o nouă tehnologie de clasificare, detectare şi răspuns proactiv la noile variante de malware în timp real, în scopul rezolvării unei probleme care devine tot mai amenințătoare.

Noile variante de malware rămân adesea nedectate de soluţiile tradiţionale de securitate, permiţând infractorilor să exploateze vulnerabilităţi şi să lanseze atacuri care rămân nedetectate. Aceste variante sunt distribuite pe numeroase canale, inclusiv ca ataşamente e-mail, site-uri web compromise şi tentative de phishing.

Noul update de produs vine ca rezultat al unei recente injecţii de numerar efectuate de firma United Ventures şi este primul dintr-o serie de lansări noi planificate pentru lunile următoare.

Cleafy poate detecta acum malware în timp real şi clasifica noi variante de malware în decurs de secunde, astfel accelerând dramatic procesele tradiţionale care durau săptămâni de zile.

Platforma Cleafy detectează şi combină semnale din interiorul aplicaţiilor mobile şi web sau din cadrul ecosistemului dispozitivelor şi al reţelei, oferind vizibilitate completă asupra canalelor digitale.

Platforma Cleafy a fost construită cu gândul la ecosistemul bancar.

Mecanismele AI în timp real ale platformei furnizează un răspuns rapid la noile variante de malware, permiţând băncilor să-şi protejeze automat clienţii, fără să-şi întrerupă activitatea. Mai mult, soluţia oferă analiştilor informaţiile necesare pentru înţelegerea naturii şi capabilităţilor malware-ului detectat, alături de sugestii de reguli de răspuns pentru conservarea unei poziţii optime de securitate.

Tehnologia AI Cleafy se bazează pe opt ani de culegere de date telemetrice malware. Acest fapt furnizează firmei o bună capacitate de înţelegere a comportamentelor malefice, ceea ce îi permite să o ia înaintea ameninţărilor emergente şi să furnizeze soluţii proactive de securitate robuste.

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

3 motive pentru care Disaster Recovery trebuie să fie o prioritate reală pentru companiile românești

Cu peste trei secole în urmă, Benjamin Franklin spunea că „Un gram de prevenție este mai bun decât un kilogram de medicamente". Verdictul este valabil și astăzi, doar că, în rețeta actualizată, „gramul de prevenție" a fost înlocuit cu soluțiile de Disaster Recovery.

Dependența tot mai mare de IT obligă organizațiile să adopte o nouă abordare a modului în care gestionează riscurile. Astăzi, mai mult ca oricând, soluțiile de Disaster Recovery sunt esențiale pentru companiile care nu vor să-și asume riscuri inutile și urmăresc o redresare rapidă cu reluarea activității în parametri optimi, în eventualitatea unui incident.

Este adevărat că, pentru multe companii, planificarea pentru necunoscut este dificilă, iar bugetele pentru prevenirea unor riscuri potențiale sunt greu de obținut. Pe de altă parte însă, argumentațiile de tipul „Doar nu se va întâmpla tocmai nouă!" sunt foarte costisitoare pe termen lung. Lipsa unui plan de recuperare în caz de dezastru te poate expune la costuri de recuperare ridicate, ratarea unor oportunități de business, afectarea reputației și pierderea de clienți.

Iată câteva scenarii frecvente la nivel local și care, în lipsa unor soluții eficiente de Disaster Recovery, pot avea urmări grave pentru compania ta.

Dezastrele naturale chiar se întâmplă

Atunci când apare într-o discuție sintagma „Disaster Recovery", majoritatea persoanelor se gândesc, în mod automat, la cutremure, cicloane, inundații și alte calamități de asemenea amploare. În ultimul timp, și România a avut parte de astfel de fenomene naturale. La o scară mai mică, este adevărat, dar efectele perturbatoare sunt reale.

De exemplu, cutremurele au înregistrat anul acesta o creștere a frecvenței în România, făcându-și apariția în zone considerate anterior cu risc seismic redus. În acest context, se pune întrebarea câte dintre companiile locale care au investit în servere sau echipamente de stocare dispun și de rack-uri cu sisteme de protecție la cutremur.

Aversele torențiale din ultimele luni au afectat nu doar localități din mediul rural, ci și orașe cu infrastructuri dezvoltate, dar care au fost scoase din funcțiune din cauza acumulărilor mari de apă. Iar în numeroase cazuri copacii doborâți de furtunile iscate din senin au întrerupt alimentarea cu energie electrică, fenomen care a pus la grea încercare organizațiile care nu dețin soluții de electro-backup. Pe de altă parte, puține dintre cele care au UPS-uri dedicate le și testează periodic, pentru a le verifica randamentul.

Și valurile de caniculă, respectiv recordurile de temperaturi atinse recent în România, au creat probleme critice. Mai ales în marile aglomerări urbane, unde echipamentele de răcire ale camerelor de servere au fost suprasolicitate. Din nou, puține dintre ele sunt dotate cu echipamente HVAC dedicate acestor medii, capabile să asigure temperatura recomandată de operare.

Mașinile nu sunt perfecte, dar și oamenii greșesc

Există însă și dezastre mai puțin vizibile în mass-media, dar ale căror efecte sunt la fel de mari.

De exemplu, anul trecut, conform datelor Inspectoratului General pentru Situații de Urgență, în România s-a înregistrat o creștere cu 41% a acestui tip de incendii, raportându-se peste 30.000 de cazuri la nivel național. În acest context, foarte puține companiii care operează Data Room-uri proprii dețin și instalații de stingere a incendiilor adecvate protejării echipamentelor IT, cum sunt, de exemplu, cele cu gaz inert. Marea lor majoritate sunt dotate cu extinctoare clasice și hidrant, total contraindicate circuitelor electronice.

Pe de altă parte, nici „mașinile" nu sunt perfecte. Chiar dacă tehnologia a avansat într-un ritm extrem de rapid, nimeni nu este imun la defecțiuni ale hard disk-ului, „morți subite" ale SSD-urilor, probleme cu echipamentele de rețelistică etc.

Potrivit studiului anual realizat de Uptime Institute, în 2022 echipamentele IT au generat aproximativ 36% din downtime-urile neplanificate. În astfel de situații, și mai ales în cazul echipamentelor vechi, contractele de mentenanță și suport încheiate cu furnizorii nu acoperă necesitățile reale ale multor companii. Să luăm un exemplu concret, cel al serverelor utilizate peste vârstă optimă de 5 ani. În astfel de cazurii, costurile cu administrarea mașinilor respective crește cu 148%, conform analizei IDC „Why Upgrade Your Server Infrastructure Now?". Totodată, după pragul de 5 ani, riscul de downtime

neplanificat crește cu 20% anual.
În plus, și oamenii fac greșeli. Conform sursei citate erorile umane sunt responsabile de aproape două treimi din întreruperile neplanificate. Concret, erorile de configurare ale echipamentelor de rețea au generat anul trecut 45% dintre cazurile de downtime, iar în cazul sistemelor IT și software procentul este 64%! Problema este gravă pentru că deficitul de personal calificat în acest domeniu crește constant, multe companii neavând practic de unde să angajeze oameni pe pozițiile de care au nevoie. Ceea ce duce la supraîncărcarea echipelor IT interne și așa sub-dimensionate, având în vedere ritmul accelerat de transformare digitală a proceselor de business.

Nu e complicat sau costisitor să ai Disaster Recovery

Evenimentele perturbatoare – de orice natură ar fi acestea – nu pot fi prevenite în totalitate. Dar pot fi atenuate și ținute sub control printr-un plan de recuperare în caz de dezastru, realizat în mod realist, și cu ajutorul soluțiilor de Disaster Recovery performante.
Sunt foarte puține companiile care își pot permite să investească în achiziționarea și implementarea unei infrastructuri IT complet redundante. Și mai puține cele care dețin personalul calificat care să poată asigura operarea, mentenanța și intevenția rapidă în cazul unui downtime neplanificat.
Cu toate acestea, necesitatea asigurării continuității proceselor de business este critică pentru orice organizație. De aceea, tot mai multe companii apelează la serviciile furnizorilor de Disaster Recovery, cum este și M247. Oferta noastră, bazată pe experiența acumulată în peste 20 de ani de operare a centrelor de date, la nivel global, este special concepută pentru a fi flexibilă și accesibilă oricărui tip de companie.
Soluțiile noastre sunt pentru toate bugetele și asigură de la backup și replicarea completă a sistemelor și aplicațiilor, până la restaurarea datelor și reluarea proceselor de business în timp garantat. Asigurăm totodată servicii de monitorizare, verificare și testare regulată a soluțiilor de Disaster Recovery pe care le furnizăm, precum și conectivitate rezilentă și mobilitate în cloud.
Apelând la soluțiile M247 de Disaster Recovery, ai garanția că riscurile generate de dezastre pot fi ținute sub control și că îți poți relua activitatea în cel mai scurt timp posibil.
Pentru mai multe detalii, echipa M247 vă stă la dispoziție la adresa de mail office@m247.com.

Construirea unei baze solide pentru securitatea cibernetică a soluțiilor dvs. video

În lumea digitală de astăzi, nu ne surprinde faptul că securitatea cibernetică reprezintă una dintre preocupările majore în diferite ședințe de board. 96% dintre directorii executivi afirmă că este esențială pentru creșterea și stabilitatea organizației, conform Accenture. și al timpilor nefuncționali neprogramați.

De Jos Beernink, Vicepreședinte EMEA la Milestone Systems

A această preocupare pentru securitatea cibernetică este perfect justificată, deoarece se estimează că infracțiunile cibernetice vor genera costuri majore de 9,5 trilioane de dolari americani în 2024, conform firmei de cercetare Cybersecurity Ventures. Astfel de pierderi pot duce la falimentul unei afaceri, fără a lua în considerare costul prejudiciului de imagine .

Riscurile cibernetice ale imaginilor video

A fi conștient de riscurile unui sistem de supraveghere video care nu este în siguranță - și cum să atenuezi aceste riscuri - este, prin urmare, o abilitate critică pentru toți liderii din domeniul securității. Camerele, senzorii conectați și software-ul de management video (VMS) pot reprezenta ținte atractive pentru actorii malefici, datorită datelor colectate. Datele pot fi folosite pentru șantaj sau pentru a obține informații confidențiale. Hackerii pot vinde imagini ale structurii și nivelurilor de personal ale clădirii la diferite ore ale zilei către infractori, de exemplu. Camerele IP pot fi de asemenea folosite ca dispozitive de acces pentru atacuri mai mari, inclusiv atacuri globale de respingere distribuită a serviciului (DDoS) care folosesc camere și alte dispozitive conectate pentru a trimite un flux de trafic către site-uri web țintind și alte infrastructuri.

Când vine vorba de protejarea afacerilor, nici măcar două sisteme nu vor fi similare. Protecția unei școli va fi foarte diferită de cea a unui centru de date sau a unei ferme solare. Prima etapă în protejarea organizației și a sistemelor sale de supraveghere este, prin urmare, înțelegerea a ceea ce trebuie protejat, cum și de cine, plus potențialul de daune care pot apărea atunci când (și nu dacă) se produce un atac.

Directiva NIS2

Protejarea camerelor și a sistemelor video este pe cale să devină și mai importantă datorită Directivei NIS2 iminente, o legislație la nivel european care își propune să îmbunătățească nivelul general al securității cibernetice în sistemele de rețea și informații. Orice soluție de supraveghere care intră în industriile "esențiale" va fi influențată de domeniu (ne referim la sectorul energetic, transportul, sectorul bancar, administrația publică și infrastructurile digitale).

Abordarea Milestone față de securitatea cibernetică

Puteți afla mai multe despre abordarea Milestone System în ceea ce privește subiectele de securitate cibernetică, cum ar fi: importanța securității fizice, cine este responsabil, cum să luați în considerare elementul uman, măsurile fundamentale de securitate cibernetică, cum să vă păstrați rețeaua separată și cât de importantă este abordarea multi-layered pe securitate.

Pentru a vă ajuta în călătoria către o rețea video securizată cibernetică, Milestone Systems găzduiește o serie de seminarii web de securitate cibernetică. Indiferent dacă începeți de la 0 o strategie de securitate cibernetică sau vă gândiți să vă bazați pe măsurile de securitate cibernetică existentă, aceste seminarii web și evenimente vă vor ajuta să construiți reziliența în sistemul video al organizației.

Mai multe detalii despre aceste seminarii web, inclusiv primul webinar despre elementele de bază ale unei strategii de securitate cibernetică video, pot fi găsite aici: **t.ly/nuvno.**

Măsuri pe care companiile le pot lua pentru a consolida securitatea

Asigurarea securității instrumentelor tehnologice este esențială pentru integritatea și succesul unei întreprinderi

Iată ce măsuri pot lua companiile pentru a consolida securitatea:

1. Actualizări și patch-uri regulate: Asigurați-vă că toate programele, sistemele de operare și aplicațiile sunt actualizate. Furnizorii lansează frecvent patch-uri pentru a remedia vulnerabilitățile de securitate cunoscute.

2. Firewall-uri și sisteme de detectare a intruziunilor: Implementați firewall-uri pentru a filtra traficul de intrare și de ieșire și sisteme de detectare a intruziunilor pentru a monitoriza activitățile rău intenționate.

3. Autentificarea cu mai mulți factori (MFA): Implementarea MFA pentru toate sistemele și aplicațiile critice. Acest lucru adaugă un nivel suplimentar de securitate dincolo de parole.

4. Criptare: Criptați datele sensibile, atât în repaus, cât și în tranzit. Acest lucru garantează că, chiar dacă datele sunt interceptate, acestea rămân ilizibile.

5. Copii de rezervă regulate: Mențineți copii de rezervă regulate ale datelor esențiale, asigurându-vă că copiile de rezervă sunt criptate și stocate în siguranță, fie în afara site-ului, fie în cloud.

6. Formarea angajaților: Instruiți în mod regulat angajații cu privire la cele mai bune practici de securitate, cum ar fi recunoașterea tentativelor de phishing și gestionarea în siguranță a parolelor.

7. Controlul accesului: Să puna în aplicare măsuri stricte de control al accesului. Asigurați-vă că angajații au acces numai la informațiile și sistemele necesare pentru funcțiile lor.

8. Securitate Endpoint: Utilizați soluții antivirus, anti-malware și alte soluții de securitate pentru punctele finale pe toate dispozitivele conectate la rețeaua companiei.

9. Evaluări de vulnerabilitate și teste de penetrare: Testați-vă în mod regulat sistemele pentru a identifica vulnerabilitățile. Angajarea unor experți externi pentru teste de penetrare poate oferi informații despre potențialele puncte slabe de securitate.

10. Practici de dezvoltare securizată: Dacă dezvoltați software, urmați practici de codare sigure și analizați codul pentru a detecta vulnerabilitățile. Instrumente precum analizoarele de cod static pot fi de ajutor.

11. Planul de răspuns la incidente: Să aveți un plan clar și practicat pentru situațiile în care apar incidente de securitate. Acest lucru asigură o atenuare rapidă și un impact minim.

12. Securitate fizică: Asigurați-vă că sălile de servere și centrele de date dispun de măsuri de securitate fizică, cum ar fi controale de acces, camere de supraveghere și spații de stocare sigure pentru copii de rezervă.

13. Securitatea furnizorului: Asigurați-vă că furnizorii terți respectă practici de securitate solide. Aceștia pot fi o potențială verigă slabă dacă au acces la sistemele dumneavoastră.

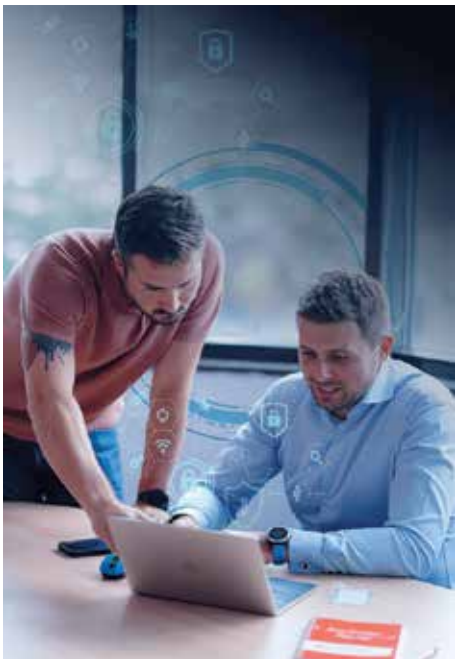
14. Segmentarea rețelei: Împărțiți rețeaua în segmente pentru a vă asigura că, dacă un segment este compromis, intrusul nu are automat acces la tot.

15. Audituri periodice: Auditați și revizuiți periodic politicile de securitate, controalele de acces și alte practici pentru a vă asigura că acestea sunt eficiente și actualizate.

16. Configurație securizată: Asigurați-vă că serverele, aplicațiile și bazele de date sunt configurate în siguranță, eliminând serviciile inutile sau porturile deschise.

17. VPN-uri: Utilizați rețelele private virtuale (VPN) pentru accesul la distanță la rețeaua companiei pentru a asigura conexiuni sigure și criptate.

Ce aduce nou în cybersecurity Fortra Terranova Security, cea mai recentă soluție din portofoliul BRINEL

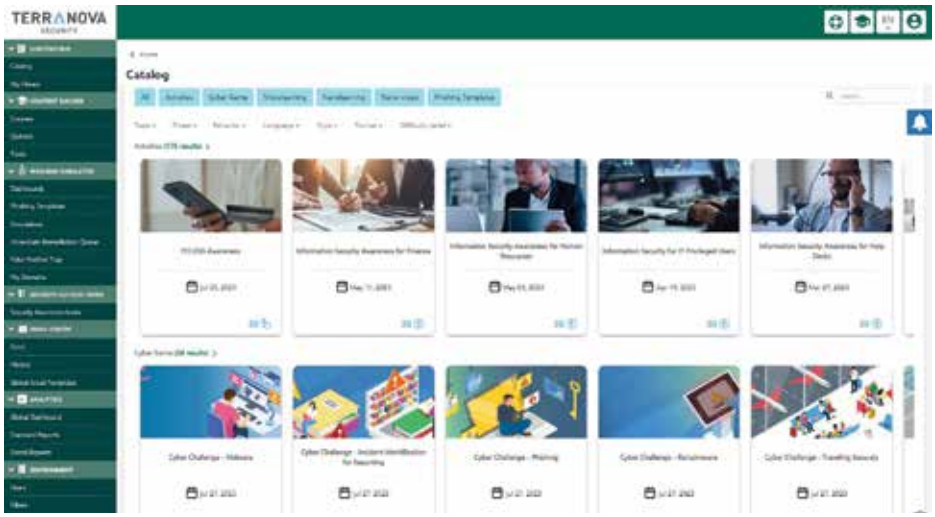


În era digitală în continuă evoluție, securitatea cibernetică este mai importantă ca niciodată pe măsură ce afacerile se confruntă cu riscuri din ce în ce mai complexe și sofisticate, generate de cele mai multe ori de erori umane. Astfel, investiția în trainingul adecvat al angajaților devine crucială și poate reprezenta o armă puternică în arsenalul unei organizații pentru protejarea datelor sensibile, a informațiilor critice și a infrastructurii sale digitale.

În acest context, platforma Fortra Terranova Security, pusă la dispoziția organizațiilor de BRINEL, se remarcă ca o soluție proactivă, inovatoare și eficientă pentru reducerea riscurilor de securitate cibernetică cauzate de personalul insuficient pregătit. Aceasta se distinge printr-o interactivitate crescută dată de posibilitatea de a participa la simulări variate, conținut actualizat, funcționalități de urmărire a progresului și feedback personalizat pentru îmbunătățirea învățării.

Ce beneficii aduce această soluție?

• Creșterea conștientizării în materie de securitate: Training-ul ajută angajații să recunoască semnele atacurilor cibernetice și să respingă amenințările de securitate cu care se confruntă organizația prin adoptarea unor practici de lucru sigure.



• Reducerea riscului de atacuri cibernetice: Angajații instruiți în materie de securitate sunt mai puțin susceptibili să cadă pradă atacurilor cibernetice cum ar fi phishing-ul sau malware-ul.

• Consolidarea culturii de securitate: O soluție de training în securitate ajută la dezvoltarea unei culturi organizaționale care prioritizează securitatea, încurajând comportamente responsabile în ceea ce privește protejarea datelor și informațiilor sensibile.

• Diminuarea considerabilă a costurilor asociate incidentelor de securitate: Prin reducerea riscului de atacuri cibernetice și a incidentelor de securitate, organizațiile economisesc resurse financiare și operaționale care altfel ar fi fost necesare pentru gestionarea și remedierea acestor incidente.

• Conformitate cu reglementările și standardele de securitate: O soluție de training în securitate poate ajuta organizația să respecte cerințele legale și reglementările specifice din domeniul securității informațiilor și să evite astfel penalizări sau amenzi.

• Personalizarea și adaptabilitatea: Fortra Terranova Security poate fi personalizată pentru a se potrivi nevoilor specifice ale organizației și poate fi actualizată în mod regulat pentru a ține pasul cu noile amenințări și tactici ale atacatorilor.
• Monitorizare și raportare: Fortra Terranova Security oferă funcționalități avansate de monitorizare a progresului angajaților în ceea ce privește training-ul și de raportare a rezultatelor, permițând organizației să evalueze eficacitatea programului și să identifice eventualele lacune în cunoștințele angajaților în materie de securitate.

BRINEL, un partener complet pentru securitatea cibernetică a afacerii tale

BRINEL este recunoscută pentru expertiza în domeniul securității cibernetice, oferind soluții și servicii adaptate nevoilor specifice ale fiecărei companii, pentru a constitui o apărare robustă împotriva atacurilor cibernetice.

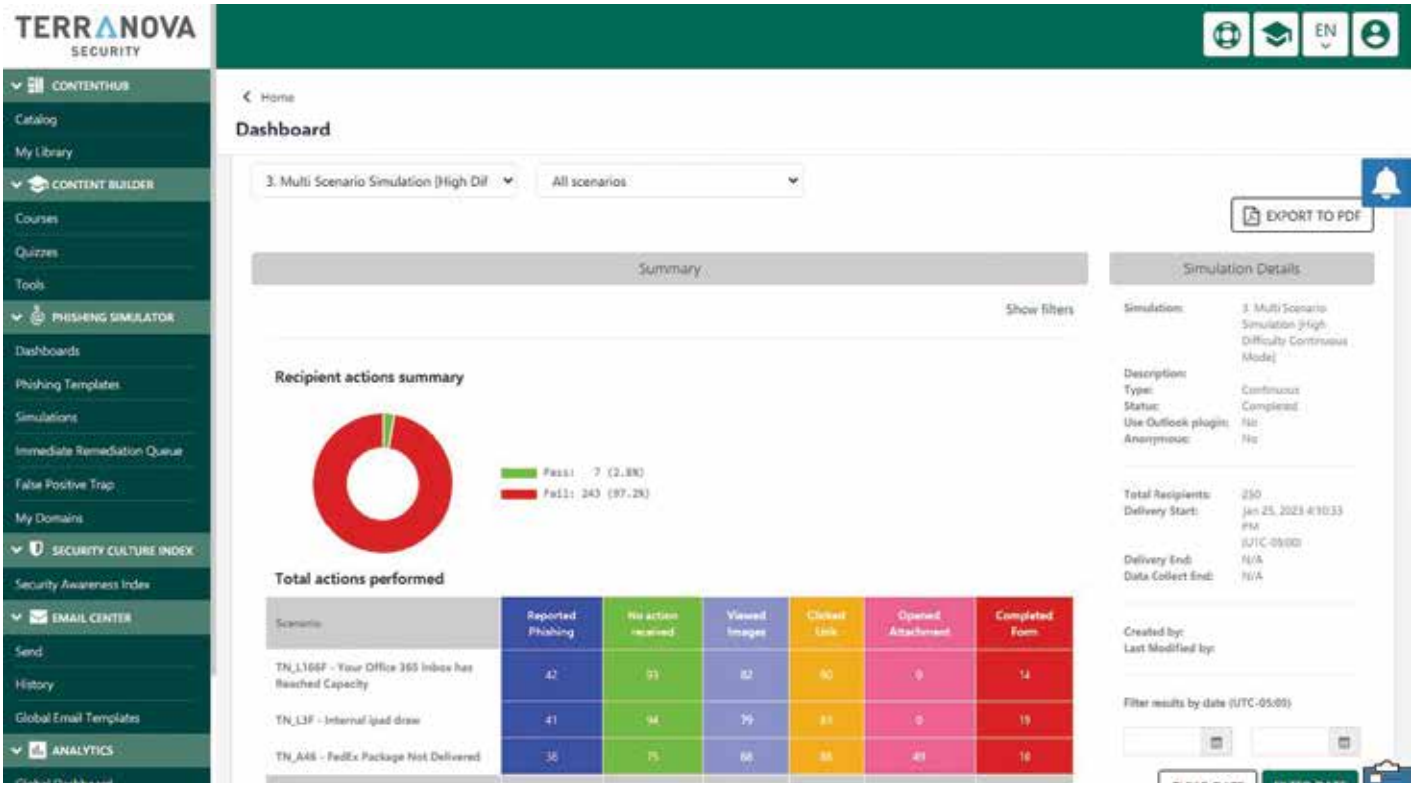
Competențele extinse includ identificarea și gestionarea amenințărilor, implementarea soluțiilor de securitate personalizate și oferirea de suport tehnic continuu pentru protejarea infrastructurii și a datelor clienților.

De peste 30 de ani pe piața de IT, BRINEL este o companie lider în tehnologie care are un portofoliu extins pentru a vă asista în procesul de transformare digitală.

Astfel, furnizează o gamă largă de soluții și servicii avansate care includ: soluții pentru Data Center modern, loc de muncă digital, servicii cloud, modernizarea aplicațiilor utilizând tehnologii open-source sau soluții low-code/no-code, AI/ML, digitalizarea afacerilor utilizând ERP, soluții de securitate cibernetică, consultanță și managed services. În plus, pentru a sprijini succesul organizațiilor, oferim clienților un set de instrumente digitale cu IP propriu (BRINEL Digital Tools).

Cu o echipă de specialiști de top și parteneriate solide cu lideri globali în domeniul IT, prin abordarea personalizată și dedicarea față de succesul clienților, BRINEL se asigură că puterea cloud-ului conduce organizațiile către o profitabilitate durabilă și o creștere scalabilă.

BRINEL rămâne o organizație agilă sub umbrela iQanto, un brand nou înființat pentru zona de IT și robotică, parte a grupului SNEF. care permite și susține crearea de strategii de creștere pe termen lung.



Soluții avansate pentru securitatea în mediul industrial

În era digitală mediul industrial nu este nicidecum imun la prezența tehnologiei informației și la pericolele ce însoțesc lumea digitală. Dată fiind miza mare din domeniile producției, energiei și altele din aceeași categorie, securitatea cibernetică este o prioritate în prezent.

În acest articol vom aduce în discuție două dintre tehnologiile moderne ce pot îmbunătăți semnificativ abordarea de securitate în rețelele din domeniile industriale, precum și o soluție avansată de protecție activă.

Microsegmentarea: Izolare și Protecție

Microsegmentarea este o abordare în administrarea rețelelor, ce constă în împărțirea lor în segmente cât mai mici fezabil, izolate, denumite zone de securitate. Aceste segmente sunt complet separate, iar comunicare dintre ele este atent controlată, chiar dacă tradițional ar fi făcut parte dintr-o singură rețea. Fiecare segment poate avea politici de securitate specifice, cu reguli de acces și permisiuni definite individual, ceea ce facilitează detectarea unui potențial atac și limitarea daunelor în cazul unei eventuale breșe de securitate.

Astfel, chiar dacă un segment este compromis, riscul de răspândire a atacului este limitat, deoarece comunicarea cu alte segmente este restricționată.

OpenFlow: Controlul Inteligent al Fluxului de Date

OpenFlow este un protocol de comunicare deschis, conceput pentru a oferi o modalitate flexibilă și programabilă de gestionare a traficului în rețele. În esență, OpenFlow permite separarea logică a planului de control al rețelei de planul de date, ceea ce oferă administratorilor rețelei un control centralizat și granular asupra modului în care pachetele de date sunt direcționate în cadrul infrastructurii.

Prin intermediul acestui tip de control, inexistent altfel în rețelele clasice, administratorii pot implementa politici de trafic personalizate, pot lua decizii de securitate pentru întreaga rețea și nu per echipament și pot reacționa rapid la amenințările de securitate redirectând sau limitând traficul în funcție de necesități.

Un exemplu de soluție specializată despre care vorbeam la începutul articolului vine din colaborarea între Allied Telesis și Nozomi Networks.

Cei de la Nozomi Networks au o experiență îndelungată în securitatea industrială, soluțiile lor fiind capabile de a detecta pericole cibernetice în medii industriale, sau chiar schimbarea de la comportamentul uzual al unei rețele.

Allied Telesis are experiență îndelungată în producerea de echipamente hardware pentru rețele industriale, și a fost unul dintre primii producători care au integrat protocolul OpenFlow în echipamentele enterprise și cele industriale.

Punând la un loc produsele celor doi vendori obținem o soluție ce este capabilă să recunoască o multitudine de potențiale pericole, care semnalează rețelei acest lucru, iar rețeaua ia decizia potrivită pentru această situatie. Decizia cea mai simplă este probabil blocarea unui nod suspect de a fi fost compromis din punct de vedere al securității, dar în mediul industrial asta nu este întotdeauna cea mai bună decizie. O întrerupere a fluxului de producție poate produce costuri extrem de mari, potențial mai mari decât costul breșei de securitate în sine.

Echipamentele cu capabilități OpenFlow de la Allied Telesis pot fi instruite să creeze o micro segmentare în timp real a rețelei, scoțând nodul respectiv din rețeaua în care se află și creându-i un microsegment cu politici de securitate atent configurate. Nodul își va putea continua activitatea legitimă în timp ce potențialul atacator va fi blocat, iar echipa de securitate are timpul necesar să rezolve incidentul fără presiunea adusă de oprirea unei linii de producție.

În concluzie, securitatea în domeniul industrial este mai mult decât o necesitate în momentul de față, este o parte integrantă a procesului de producție în sine. Presiunea pusă pe echipele ce proiectează și administrează soluțiile

de securitate din acest domeniu este mare. Acestea fiind spuse, există și soluții puțin diferite, soluții ce nu funcționează în modul clasic al rețelelor de comunicații, soluții ce pot reduce poate puțin această presiune.

Plăți în siguranță

ING a lansat serviciul de geolocalizare, o nouă funcționalitate în Home'Bank, cu scopul de a detecta tranzacțiile frauduloase și operațiunile suspecte efectuate în aplicația bancară din alte arii geografice.

Pentru oferirea unei protecții suplimentare clienților, sistemul poate semnala tranzacțiile efectuate la POS și transferurile bancare neobișnuite, dar și acțiunile inițiate în Home'Bank, precum vizualizarea datelor cardului sau autorizarea plăților securizate.

Pentru activarea serviciului de geolocalizare, clienții trebuie să permită accesul la locația dispozitivului mobil de pe care se autentifică, pentru a prelua coordonatele GPS.

Cum funcționează opțiunea de geolocalizare din Home'Bank

Din aplicația Home'Bank Android/ iOS, clienții pot accesa secțiunea 'Mai multe' -> 'Securitate și login' -> 'Geolocalizare'. Opțiunea poate fi dezactivată sau reactivată în orice moment de către clienți.

Geolocalizarea funcționează doar cu locația telefonului activă. În cazul în care utilizatorii opresc permisiunile pentru locație pe acel dispozitiv, ING nu va putea folosi informația despre localizare chiar dacă serviciul va figura activ, până la reacordarea permisiunilor.

Este important de menționat că ING nu folosește informatiile despre geolocalizare în scopuri comerciale, iar clienții pot opta oricând pentru dezactivarea serviciului.

Security Service Edge, un nou trend în sfera Network Security

Pe măsură ce adoptă transformarea digitală, firmele îşi dau rapid seama că singura cale de a securiza utilizatorii, conţinutul şi resursele în cloud este de a avea şi securitatea în cloud. Mutarea în cloud reprezintă o misiune dificilă, mai ales pentru organizaţiile mari şi complexe.

Pentru a adresa provocările de securitate ale transformării digitale, industria de profil s-a concentrat pe cadrul de funcţionare al unei arhitecturi Secure Access Service Edge (SASE). Atunci când protecţia datelor reprezintă temelia cadrului de funcţionare, o astfel de arhitectură devine un mijloc de dobândire a securităţii de tip Zero Trust în cloud. Însă, înainte ca o asemenea arhitectură să fie posibilă, trebuie implementată o temelie Security Service Edge(SSE).

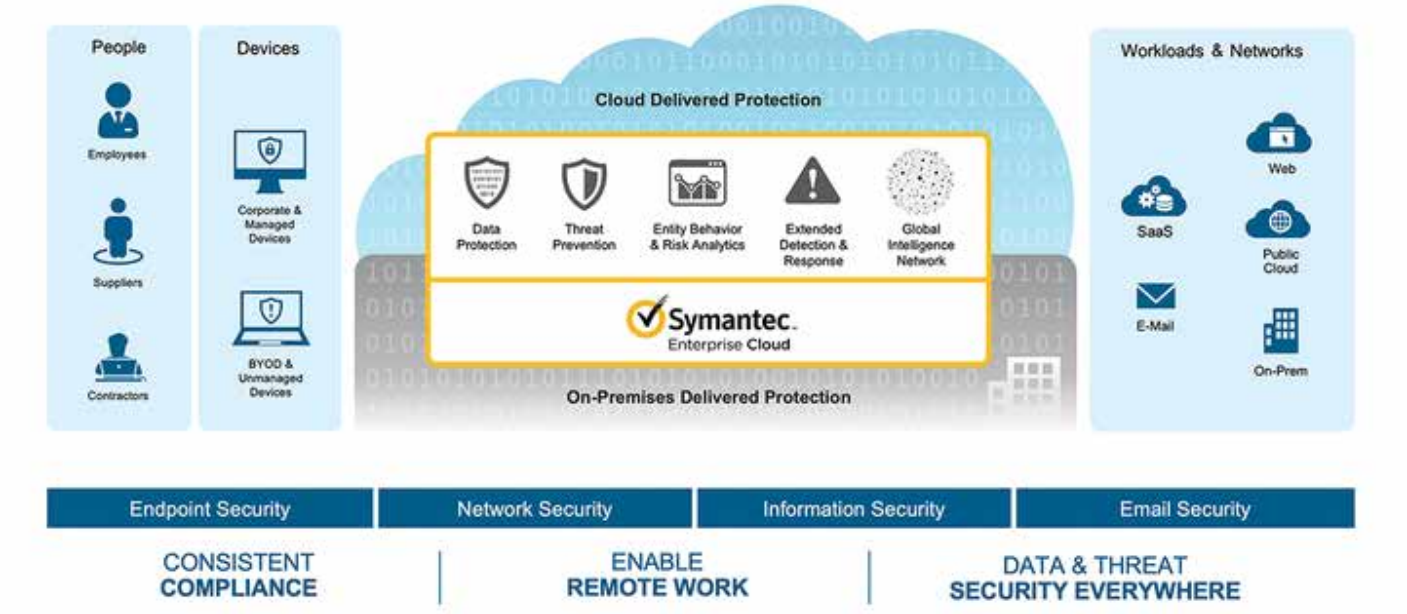
SSE este o viziune asupra stării finale şi nu un ghid clar de implementare. Nu există o singură cale corectă pentru toată lumea. Drumul pentru fiecare firmă este determinat de ceea ce are la dispoziţie, ceea ce îi lipseşte, buget, personal, obligaţii contractuale, reglementări, nevoi şi alţi factori. De aceea, acest drum este dificil, însă toate drumurile au un punct comun: determinarea începutului.

Cele de mai sus reprezintă contextul general în care Symantec propune pieţei o nou abordare din punct de vedere al soluţiei. Symantec Network Protection înlătură nesiguranţa începutului călătoriei SASE deoarece include un set cuprinzător de capabilităţi critice pe care firmele le pot implementa când şi unde socotesc că ar fi potrivit.

Network Protection este o soluţie SSE completă de securizare a reţelei, internetului şi aplicaţiilor cloud prin intermediul unui set de servicii incorporate într-o reţea edge de clasă înaltă. Construite pe o arhitectură cloud-native cu o poartă de acces web înalt securizată şi controale CASB, capabilităţile soluţiei sunt extinse la aplicaţii web şi de cloud public şi privat.

Soluţia este sprijinită de un model portabil de licenţiere care permite clienţilor să-şi menţină amprenta edge proxy fără costuri suplimentare. Acest fapt permite transformarea digitală cu orice viteză, indiferent dacă utilizatorii lucrează de la un sediu central, de acasă sau din oricare altă locaţie. Network Protection conlucrează uşor cu Symantec DLP Cloud, o soluţie de protecţie unicat de la Broadcom pentru alcătuirea celei mai complexe soluţii data-centric SASE din cadrul industriei de profil.

Soluţia Network Protection include capabilităţi SWG cheie, printre care se numără SWG avansat livrat prin cloud şi SWG on-premises – ambele operând fără sincope împreună cu o interfaţă de



management unificat, raportare şi control al politicii. În acelaşi timp, funcţionalităţile cheie CASB conferă clienţilor o privire mai bună asupra aplicaţiilor cloud.

Broadcom a dus securitatea reţelei la următorul nivel incluzând mai multe capabilităţi SSE avansate în cadrul Network Protection. Toţi utilizatorii licenţiaţi au dreptul la o tehnologie ZTNA inovatoare care permite accesul securizat la aplicaţii private de pe orice dispozitiv gestionat sau negestionat de la distanţă, astfel eliminându-se necesitatea unei VPN.

De asemenea, utilizatorii sunt protejaţi de ameninţări prin Full Browser Isolation, Advanced Cloud Sandboxing şi Deep Content Inspection – toate acestea fiind incluse în licenţa Network Protection. Capabilităţile Network Protection sunt furnizate pe o arhitectură avansată, optimizată edge care utilizează infrastructura de cloud public Google. Este o componentă de securitate cheie a Symantec Enterprise Cloud, integrând soluţiile de securitate cibernetică Broadcom livrate din cloud în implementări cloud, edge şi hibride.

Security Service Edge, precum şi alte soluţii de securitate de la Symantec,

Romsym Data

Atingerea conformității cu standardele PCI DSS

Reduceți riscul de încălcări ale datelor legate de titularii de carduri de plată prin aplicarea practicilor de securitate dovedite.

Ce este PCI DSS?

PCI DSS, Standardul de Securitate al Datelor Industriei de Plăți, este un set de procese și practici concepute pentru a asigura transferul sigur și securizat al datelor cardurilor de plată. Scopul său este de a îmbunătăți siguranța datelor consumatorilor și încrederea în ecosistemul de plăți. Standardul se aplică tuturor entităților care stochează, procesează sau transmit datele titularilor de carduri (CHD) și/sau datele de autentificare sensibile (SAD), sau ar putea afecta securitatea mediului de date al titularului de card (CDE). Acest lucru include afacerile care colectează date sensibile pentru autentificarea titularilor de carduri sau autorizarea tranzacțiilor de plată.
PCI DSS este impus de companiile emitente de carduri de plată pentru a asigura securitatea tranzacțiilor cu carduri de plată. Dacă gestionați datele deținătorilor de carduri, devine responsabilitatea dvs. să fiți conformi cu PCI DSS și să validați conformitatea în mod regulat.

Implementarea acestui standard aduce beneficii suplimentare, permițând organizațiilor să:

- Prevină încălcarea securității datelor.
- Reducă riscul pierderii de date
- Mențină încredere clienților
- Evite amenzi și penalități
- Se conformeze ușor și la alte cadre de lucru

Pentru a fi conform cu PCI DSS, organizația dvs. trebuie să îndeplinească o serie de cerințe de securitate operaționale și tehnice care se aplică unui CDE. Un CDE este alcătuit din persoane, procese și sisteme care interacționează cu sau ar putea afecta informațiile despre cardul de plată.
PCI DSS 4.0, cea mai recentă versiune a PCI DSS, constă din 12 cerințe concepute pentru a proteja datele contului de plată.

ManageEngine

Suitele de soluții de management IT de la ManageEngine vă pot ajuta să îndepliniți aceste 12 cerințe răspândite pe 6 obiective și, în consecință, să asigurați conformitatea cu PCI DSS.
Descărcați ghidul **ManageEngine** pentru a obține detalii despre modul în care și ce sub-cerințe sunt îndeplinite de soluțiile distribuite de **Romsym Data.**

Identitatea devine prima linie de securitate

La ora actuală, Uniunea Europeană şi Parlamentul European a elaborat ghidurile de implementare pentru European Digital Identity Framework. Parlamentul European lucrează, de asemenea, la directiva Network and Information Security (NIS2), care are impact direct asupra viitorului securității identității şi al cerințelor de conformitate.

Deocamdată, în ciuda rolului critic, **securitatea identităţii** pentru indivizi şi organizaţii tinde mai degrabă să lipsească. Atacurile ransomware au rămas constant o ameninţare de top în ciuda investiţiilor în soluţii de detecţie şi remediere. Ele sunt adesea precedate de furturi de credenţiale, care permit infractorilor să atace din lateral active critice pentru criptarea datelor unei organizaţii.

Altfel spus, una din cele mai mari ameninţări cibernetice de la ora actuală este cea a atacurilor asupra identităţii. Prin urmare, prin întărirea protejării identităţii prin folosirea tehnologiilor rezistente la phishing şi a autentificării multi-factor se poate combate eficient această ameninţare.

PE MĂSURĂ CE AMENINŢĂRILE CIBERNETICE CONTINUĂ SĂ EVOLUEZE, DEVINE TOT MAI IMPORTANTĂ RECUNOAŞTEREA ROULUI CRITIC AL IDENTITĂŢII.

Folosirea de tehnici avansate de protecţie prin intermediul **inteligenţei artificiale** şi a politicilor care furnizează tehnici alternative de securizare reduce riscul, după cum software de detectare a **ameninţărilor mobile** permite conformitatea cu cerinţele **NIS2**.

Vestea bună e că investiţiile în soluţii de securizare a identităţii ajută organizaţiile să menţină conformitatea, să ofere experienţe bune, să reducă costurile de tip help desk şi să automatizeze autentificarea. Identitatea deserveşte diverse roluri în organizaţie, motiv pentru care liderii ar trebui să o prioritizeze. Iar ca strategie de minimizare riscuri, ea justifică din plin investiţiile.

Produsele şi soluţiile Symantec sunt distribuite în România de compania SolvIT Networks.

Symantec
A Division of Broadcom

5 instrumente indispensabile pe zona de securitate

Toate tipurile de afaceri, fie ele mari sau mici, au nevoie de cel mai înalt nivel posibil de protecție împotriva potențialelor atacuri rău intenționate și a accesului neautorizat. Fără măsuri de securitate adecvate, puteți pierde integritatea rețelei și a datelor. De aceea, un sistem solid de securitate a rețelei este esențial pentru a securiza rețelele împotriva potențialelor amenințări, cum ar fi pierderea de date, furtul și sabotajul. Pandemia și lucrul de acasă au condus la mai multe provocări pe zona de securitate. Potrivit studiilor realizate de firmele de cercetare, în anul 2022 s-au înregistrat în medie 1600 de atacuri săptămânal pentru fiecare organizație, în creștere cu 38% față de anul precedent.

În continuare, vă prezentăm câteva instrumente indispensabile pe zona de securitate.

1. Anti-Malware

Infractorii cibernetici de astăzi se ascund nu numai în cele mai întunecate colțuri ale internetului, ci și în restaurantele sau cafenelele pe care le vizitezi și în care te conectezi.

Serviciul Anti-Malware de la Zyxel încorporează tehnologia de vârf cu terțe părți, care a atins rate de detectare deosebită, obținând constant premii de la laboratoarele independente de testare AV-Comparatives Malware Protection. Utilizând răspunsul rapid și o abordare ușoară a securității, Zyxel îmbunătățește eficiența serviciului anti-malware consumând în același timp o putere de calcul limitată, oferind protecție completă împotriva malware-ului „în sălbăticie" care se află în prezent pe o gamă largă de rețele globale.

Integrarea produselor gateway de securitate Zyxel permite scanarea malware bazată pe flux, precum și oferirea de suport pentru diferite protocoale, inclusiv HTTP, FTP, SMTP și POP3. Este oferit și suport suplimentar pentru inspecția de criptare SSL (HTTPS).

2. Anti-Spam

E-mailul este cea mai comună metodă și punctul de plecare al atacurilor care vizează organizațiile. Filtrele Anti-Spam detectează și filtrează e-mailurile spam cu protecție cuprinzătoare, cu mai multe straturi. E-mailul este o formă indispensabilă de comunicare care și-a făcut loc în fiecare aspect al vieții noastre moderne. Cu toate acestea, statisticile arată că mai mult de 70 la sută din toate e-mailurile sunt spam, iar mai mult de 90 la sută din spam poartă o anumită formă de malware.

Zyxel Anti-Spam folosește un sistem de apărare pre-perimetru bazat pe cloud pentru a vă proteja e-mailul de malware. Serviciul Zyxel Anti-Spam reduce e-mailul nesolicitat și crește productivitatea afacerii, permițându-vă să blocați spam-ul la marginea rețelei, eliberând astfel serverele de e-mail.

3. Application Patrol

Rețelele de astăzi sunt atacate de o gamă în continuă expansiune de amenințări. Întrucât viitorul muncii este flexibil și munca de la distanță este utilizată pe scară largă, gestionarea angajaților care pierd prea mult timp cu aplicații care nu sunt legate de muncă poate fi o provocare majoră pentru companii. Administratorii se confruntă cu pierderea nu numai a riscului de securitate, ci și a productivității și a lățimii de bandă a rețelei din cauza utilizării nerestricționate a Internetului.

Zyxel Application Patrol este proiectat pentru a oferi managementul aplicațiilor de nivel 7, clasificarea acoperă aplicații de rețea bine-cunoscute, cum ar fi rețele sociale, jocuri, productivitate și alte aplicații și comportamente web. Baza de date Zyxel acceptă mii de aplicații și comportamentele acestora, împreună cu aplicațiile în creștere și în continuă schimbare, operațiunile noastre funcționează cu ciclul repetat de colectare, analiză și verificare a fluxului.

4. Intrusion Prevention System

Atacatorii exploatează adesea vulnerabilitățile sistemelor sau ale aplicațiilor pentru a întrerupe și a obține controlul asupra aplicațiilor sau mașinilor.

Sistemul de prevenire a intruziunilor (IPS) Zyxel este cunoscut și sub denumirea de Detectare și prevenire a intruziunilor (IDP), care este o tehnologie de securitate a rețelei și de prevenire a amenințărilor care ajută companiile să stabilească măsuri de securitate în timp util împotriva atacurilor cunoscute de tip zero-day. Serviciul IPS vă protejează pe deplin mediul de rețea de afaceri cu detectarea anomaliilor de trafic dintr-o gamă largă de activități suspecte – cum ar fi injecția SQL, DoS și aplicațiile rău intenționate.

5. Filtrare Web

Există multe site-uri rău intenționate existente care pot capta utilizatorii, pot infecta sistemele cu viruși sau instalează programe spyware atunci când sunt accesate neglijent. O soluție eficientă este necesară pentru ca administratorii să gestioneze accesul la web și să controleze traficul atunci când angajații accesează site-uri web.

Zyxel Web Filtering este un serviciu de abonament de securitate complet integrat care protejează rețelele împotriva atacurilor rău intenționate de la site-uri web necinstite, ajutând în același timp administratorii să gestioneze și să controleze accesul utilizatorilor. Zyxel Web Filtering utilizează abordări hibride, inclusiv o bază de date stocată în cache local și o bază de date URL optimizată pentru cloud, îmbunătățind performanța și acuratețea.

Cea mai sigură alegere pentru eliminarea vulnerabilităților și diminuarea riscurilor: servicii de testare de securitate cibernetică

Securitatea cibernetică reprezintă în prezent una din principalele provocări cu care se confruntă organizațiile din întreaga lume. Conform Cyber Magazine, la finalul anului trecut erau detectate zilnic peste 46 de milioane de potențiale atacuri cibernetice la nivel global.

Un atac cibernetic reușit poate aduce prejudicii grave asupra competitivității, rentabilității, reputației, loialității clienților și a încrederii partenerilor oricărei organizații. Din acest motiv, tot mai multe companii apelează la furnizori specializați în servicii de testare securitate cibernetică.

Testarea periodică a sistemelor de securitate este una din cele mai eficiente și rapide metode prin care organizațiile pot detecta vulnerabilitățile infrastructurii lor informatice. Prin intermediul serviciilor furnizate de specialiștii în domeniu, companiile obțin nu doar o listă a problemelor cu care se confruntă, ci și recomandări și informații acționabile asupra zonelor critice în care trebuie să intervină.

4 motive să contractați servicii de testare de securitate cibernetică

Pe măsură ce sistemele IT sunt înlocuite sau suferă modificări, în infrastructura informatică a oricărei organizații pot apărea noi vulnerabilități. Prin testarea sistematică a securității cibernetice, acestea pot fi detectate și remediate înainte ca un atacator sau o amenințare să le poată exploata. Colaborarea cu un furnizor specializat, precum Safetech Innovations, aduce câteva beneficii importante:

1. Managementul și diminuarea riscurilor – Vulnerabilitățile și punctele slabe ignorate și/sau necontrolate din infrastructura unei companii au potențialul de a o expune la amenințări reale. Totodată, folosirea aplicațiilor de la parteneri și/sau a serviciilor externalizate induce riscuri suplimentare. Prin utilizarea serviciilor de testare, riscurile de acest tip pot fi detectate, ierarhizate și remediate în mod proactiv. Astfel, organizațiile obțin o protecție îmbunătățită în fața amenințărilor avansate.

2. Reducerea costurilor – În securitatea cibernetică, prevenirea unui atac este preferabilă remedierii în urma efectelor acestuia. Utilizarea serviciilor de testare poate reduce cheltuielile și efortul de recuperare și remediere după o pierdere datorată unui astfel de atac. Pe de altă parte însă, nu multe companii dețin intern competențele, experiența și instrumentele necesare detecției și tratării potențialelor riscuri. Prin apelarea la serviciile unui furnizor specializat în servicii de testare securitate cibernetică, aceste limitări pot fi depășite rapid și în condiții de predictibilitate a costurilor.

3. Limitarea timpului de nefuncționare – Orice întrerupere a funcționării rețelei, aplicațiilor sau serviciilor unei companii duce la scăderi de productivitate. Testarea periodică permite detectarea și remedierea erorilor de configurare și a vulnerabilităților care pot produce întreruperi neplanificate ale fluxurilor de lucru.

4. Conformitatea cu reglementările legale – În prezent, tot mai multe standarde și cerințe legale și de reglementare impun companiilor să facă teste și audituri ale sistemelor de securitate. În prezent, astfel de cerințe sunt prevăzute în PCI DSS, ISO 27001, **Directiva NIS**, norme BNR, ASF etc. Prin testarea periodică, companiile obțin o verificare și o validare a nivelului de conformitate. În plus, furnizorii de servicii de acest tip oferă și recomandări de măsuri pentru îndeplinirea cerințelor de conformitate cu normele legale aplicabile și cu standardele asumate de companie.

Ofertă completă de testare a infrastructurii și aplicațiilor

Safetech Innovations este unul din principalii furnizori de servicii de testare a sistemelor de securitate cibernetică în România. Compania a realizat de-a lungul celor 14 ani de activitate, peste 2.000 de teste, în urma cărora au fost identificate mai mult de 10.000 de vulnerabilități.

Printre clienții Safetech se numără companii din industria financiar-bancară, producția de energie, utilități, farmaceutice și sănătate, asigurări etc., care activează în România, dar și în străinătate.

De-a lungul anilor, compania a perfecționat și aplicat consecvent o anumită metodologie de testare. Totodată, a investit constant în dezvoltarea competențelor și are un nivel ridicat de expertiză în acest domeniu. În cadrul testelor realizate, echipa Safetech pornește de la stabilirea activelor critice care trebuie protejate pentru fiecare companie client. Faza de testare permite identificarea defectelor din infrastructura și aplicațiile organizațiilor,

care pot merge de la configurări greșite, până la erori de proiectare a aplicațiilor. Totodată, testele detectează și amenințările malware care au reușit să treacă de sistemele de protecție. Fiecare test realizat de specialiștii Safetech analizează impactul amenințărilor sau al breșelor de securitate asupra confidențialității, integrității și disponibilității datelor. Testarea se realizează atât în mod automat, pentru detectarea vulnerabilităților și aplicațiilor malware, cât și manual, pentru a verifica testele automate și identifica posibilele erori existente.

Compania românească furnizează o gamă completă de servicii de testare securitate cibernetică care includ:

• **Servicii de scanare a vulnerabilităților** – Acestea verifică atât infrastructurile on-premises, cât și mediile cloud și facilitează identificarea vulnerabilităților exploatabile și remedierea lor rapidă.

• **Teste de penetrare** – Echipa noastră are o experiență vastă în domeniul testelor de penetrare și utilizează echipamente și aplicații specializate. Oferta acoperă de la teste de penetrare a rețelei, până la aplicații mobile sau web.

• **Verificarea codului aplicațiilor** – Specialiștii Safetech asigură servicii de inspectare a codului aplicațiilor pentru identificarea potențialelor vulnerabilități datorate programării.

Pentru mai multe informații despre serviciile Safetech Innovations, demonstrații practice și oferte comerciale, vă invităm să îi contactați prin email la **sales@safetech.ro** sau prin telefon la **+40 21 3160565.**

Atacurile de smishing în creștere

Numărul atac urilor de tip smishing în România a crescut de peste șase ori în 2023 în comparație cu anul anterior, potrivit unei analize interne realizate de sendSMS. În 75% din cazurile de smishing, s-a încercat furtul de identitate prin utilizarea unei etichete personalizate (numele expeditorului) pentru a induce în eroare utilizatorii că mesajele sunt trimise de diferite companii. Atacurile de tip smishing sunt asemănătoare cu cele de phishing, dar folosesc mesaje SMS pentru a înșela potențialele victime. În majoritatea cazurilor, utilizatorii trebuie să acceseze un link și ajung pe un site web fals, creat special pentru a sustrage detalii confidențiale (cum ar fi datele cardului sau de autentificare în aplicația bancară). În alte cazuri, utilizatorilor li se cere să instaleze programe malware pe dispozitivele lor mobile.

Potrivit analizelor sendSMS din ultimii trei ani, cele mai multe fraude de tip smishing din România vizează domeniul bancar (56%), industria de curierat (25%) și serviciile de telecomunicații (15%).

Securitatea fizică, o cerință de actualitate pentru centrele de date

Una dintre cele mai frecvente probleme de securitate, cu care se confruntă centrele de date o reprezintă amenințările interne reprezentate de angajații sau vizitatorii care acționează cu scopuri răuvoitoare.

Este un risc dificil de controlat pentru că nu există măsuri de depistare timpurie a persoanelor autorizate, dar cu rele intenții. În scenariile extreme, acestea pot provoca însă pagube importante – de exemplu, pot accesa neautorizat un server și pot sustrage date sau șterge suporturile de stocare, pot produce defecțiuni electro-mecanice dificil de depistat sau întrerupe conexiunile de date etc.

Există însă și alte situații, în care amenințările vin din exterior. Cum ar fi cazurile în care persoane neautorizate pot trece de sistemele de securitate perimetrale folosind ecusoanele ale vizitatorilor autorizați. Sau situațiile în care foști angajați pot pătrunde nestingheriți în incinta centrelor utilizându-și drepturile de acces care nu au fost șterse din sistemul de autorizare. Sunt situații reale și perfect posibile pentru că „băieții răi" există nu doar în lumea virtuală. Riscul este real, iar specialiștii consideră că operatorii Centrelor de Date își concentrează atenția preponderent pe asigurarea securității informatice. Potrivit datelor Uptime Institute, cheltuielile centrelor de date cu securitatea fizică reprezintă aproximativ 5% din bugetele operaționale și doar în cazuri extreme ajung la 30%.

Securitatea fizică este cerută de standarde

Cu toate acestea, asigurarea securității fizice este o condiție clar stipulată în standardele folosite pentru certificarea centrelor de date. De exemplu, standardul de infrastructură ANSI/TIA-942 furnizează recomandări concrete privind protecția activelor din Data Centere, fie prin măsuri de securitate fizică, fie prin sisteme de prevenire a incendiilor. Și standardul ISO27001 are prevederi clare pe zona securității fizice, deși titlul oficial este „Tehnologia Informației – Tehnici de securitate – Sisteme de management al securității informației". De exemplu, secțiunea „A.9 Controlul accesului" include măsuri – fizice și informatice – de limitare a accesului la informații și la echipamentele pe care sunt stocate acestea. Iar secțiunea „A.11 – Securitate fizică și de mediu" prevede măsuri de control pentru împiedicarea accesului fizic neautorizat și protejare a echipamentelor și instalațiilor împotriva riscurilor de a fi compromise de intervențiile umane sau naturale.

Arhitectură pe patru niveluri

Datele Uptime Institute arată că 20% dintre centrele de date s-au confruntat cu o formă de tentativă de acces neautorizat în ultimii cinci ani. Potrivit studiului „Data center security: Reassessing physical, human and digital risks", rata scăzută a incidentelor de acest tip demonstrează succesul strategiilor de securitate fizică adoptate. Însă aceasta nu înseamnă reducerea vigilenței și reducerea investițiilor în măsurile de prevenire și blocare a accesului neautorizat, distrugere a echipamentelor sau întrerupere a serviciilor.

Arhitectura de securitate fizică adoptată de majoritatea centrelor de date este dezvoltată pe modelul „Box inside a box", care prevede asigurarea protecție pe patru niveluri:

- Securitate perimetrală și a facilităților;
- Securizarea clădirii propriu-zise a centrului de date;
- Asigurarea securității camerei de control („Computer room");
- Protejarea rack-urilor și/sau a spațiilor rezervate pentru clienți.

Soluții pentru toate nevoile

Soluțiile de securitate fizică recomandate sunt numeroase și nu există o „rețetă" universal valabilă pentru toate centrele de date, fiecare organizație adoptând măsurile care se potrivesc cel mai bine nevoilor și cerințelor specifice. Există însă soluții care au început devină standard în industria Data Center. Cum sunt, de exemplu, sistemele CCTV și senzori folosite atât în exteriorul centrului, cât și în interiorul acestora. Sau sistemele de autentificare multifactor, prin care clasicele ecusoane de acces – care pot fi împrumutate – sunt dublate prin metode de autentificare biometrică. La acestea se adaugă bariere, sisteme de tip ecluză, porți de acces cu închidere electrică, turnicheți, scanere de bagaje etc., totul corelat cu sistemul central de control și monitorizare a accesului în timp real. La polul opus se situează „excepțiile" de tipul placarea pereților exteriori ai centrului de date cu panouri kevlar, pentru îmbunătățirea protecției fizice, sau cu aliaje metalice pentru asigurarea protecției împotriva atacurilor EMP.

Evoluția continuă

Tehnologiile de securitate fizică evoluează

continuu, de aceea experții Uptime recomandă centrelor să nu se „relaxeze", ci să continute sa investească în noi tehnologii. Cum sunt, de exemplu, noile generații de sisteme de supraveghere video perimetrală care sunt dotate cu funcționalități avansate, precum recunoașterea automată a numerelor de înmatriculare (Automatic Number-Plate Recognition – ANPR) pentru a ține evidența vehiculelor care intră și ies. Acestea pot fi dublate, dacă nevoile o cer, cu soluții de tip radar care ajută la localizarea rapidă a persoanelor neautorizate, cu rețele de senzori audio și detecție a mișcării pentru validare dual a intruziunilor etc. La rândul lor, și noile sisteme de monitorizare video folosite în interiorul centrelor de date integrează funcționalități de recunoaștere inteligentă a comportamentelor anormale sau a cazurilor când sunt încălcate regulile prestabilite de securitate (precum accesul în zone interzise publicului, acces neautorizat etc.) Uneori, adoptia unor astfel de sisteme nu este optionale ci o necesitate directă. Cum este de exemplu cazul sistemelor de detectare a temperaturii prin intermediul camerelor cu termoviziune, impuse de evoluția pandemie și necesitatea depistării rapide a persoanele care prezintă un risc crescut de infectare.

Nevoia de specialiști

Toate aceste soluții nu își ating potențialul maxim dacă nu sunt integrate și dacă nu ajută la aplicarea unor reguli și strategii coerente de securitate. De exemplu, sistemele de monitorizare video și soluțiile de autentificare biometrică sunt inutile dacă unui fost angajat nu i-au fost retrase drepturile de acces.

Pentru implementarea și configurarea unei arhitecturi de securitate fizică e nevoie însă de experiență și competențe specifice, total diferite de cele necesare operării unui centru de date. Specialiștii Tema Energy întrunesc aceste condiții și vă pot ajuta să alegeți soluțiile capabile să vă asigure nivelul de securitate dorit.

Dacă doriți să eliminați riscul investițiilor inutile sau prea costisiloare, precum și pe cel al subutilizarii soluțiilor alese, contactați specialiștii Tema Energy!

Vicarius vuln_GPT permite echipelor de securitate să găsească și să repare vulnerabilitățile software

Vicarius a lansat în ultimul trimestru din 2023, vuln_GPT, un model LLM care generează scripturi de remediere a vulnerabilităților software mai rapid decât hackerii.

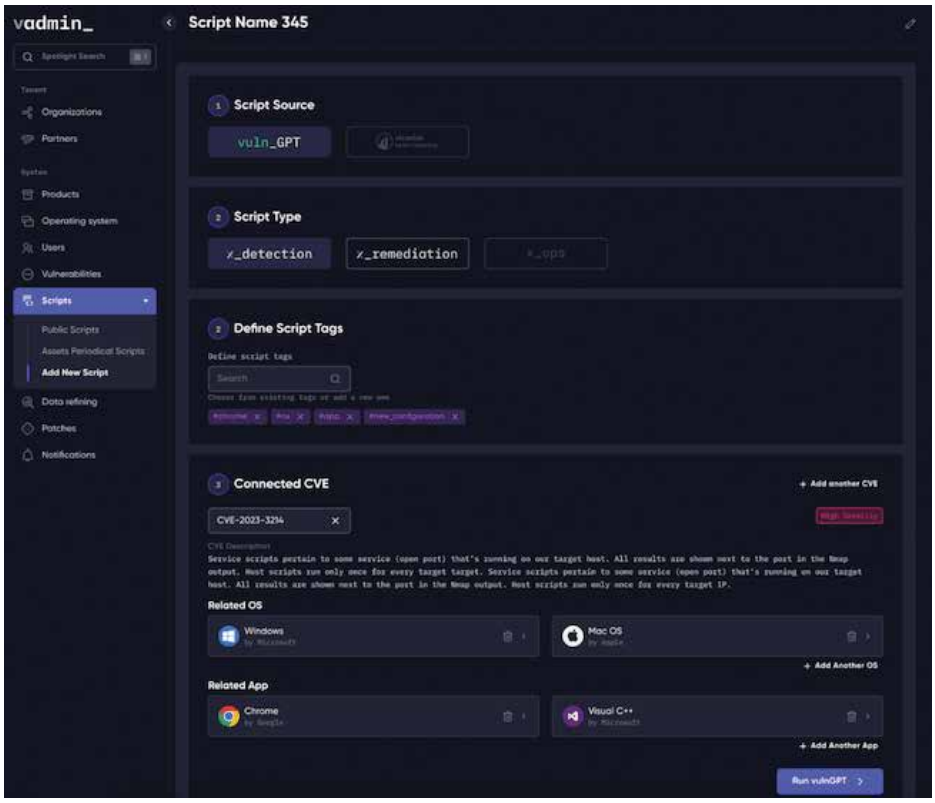
Motorul vuln_GPT va fi oferit gratuit în cadrul vsociety, comunitatea socială Vicarius pentru cercetătorii din securitate. Scripturile vuln_GPT pot fi apoi implementate cu ușurință ca parte a soluției vRx, care permite remedierea instantanee a vulnerabilităților.

În peisajul digital în continuă evoluție, au fost detectate 200.000 de vulnerabilități, 10% doar în ultimul an, iar ritmul de creștere este exponențial. Identificarea și gestionarea manuală a „zero-day" este o povară grea, necesitând multă muncă zilnic. La aproape 60 de zile de la identificarea vulnerabilității MOVEit, un sfert dintre organizațiile afectate erau vulnerabile. Apariția celor mai recente amenințări cibernetice bazate pe inteligență artificială, cum ar fi WormGPT, face și mai dificilă detectarea și blocarea lor.

Când vine vorba de soluții de gestionare a vulnerabilităților, furnizorii vechi se sprijină foarte mult pe partea de evaluare și detecție, dar nu au acordat atenția adecvată remedierii. Remedierea este deja un proces complex, iar echipele de securitate rămân precaute atunci când aplică patch-urile furnizorilor, de teamă să nu provoace întreruperi sau timpi de nefuncționare a sistemelor. Chiar dacă este disponibil un patch, adesea intervine o perioadă de așteptare pentru a minimiza orice risc potențial.

vuln_GPT este un motor de remediere AI, care poate genera automat un script de remediere pentru a executa o serie de acțiuni. De exemplu, scripturile pot elimina un fișier, pot închide un port, pot dezactiva un protocol sau pot iniția un control compensator. Toate acestea sunt strategii care pot oferi o soluție solidă și fiabilă în timp ce furnizorii lucrează la lansarea unui patch sau în timp ce echipele de securitate testează unul într-un mediu de laborator.

Mai mult, deoarece vuln_GPT funcționează fără intervenția umană, face și detectarea și remedierea vulnerabilităților mai rapide și mai rentabile, fără a fi nevoie de echipe mari de cercetare sau de ingineri de securitate foarte calificați, economisind timp și bani. Recent, au fost descoperite vulnerabilități critice de tip zero-day în Terrestrial Trunked Radio (TETRA), un protocol de comunicații radio utilizat pe scară largă de guverne, forțe de ordine și organizații militare. În timp ce unele dintre vulnerabilități pot fi remediate prin actualizări de firmware, altele, nu, fiind mai dificil de remediat, cum ar fi un backdoor în CVE-2022-24402 care poate expune informații sensibile. Folosind vuln_GPT, Vicarius elimină munca manuală de identificare și aplicare a celor mai eficiente controale de compensare.



Cu vuln_GPT, Vicarius deschide era scripturilor generate de AI pentru a atenua CVE și ajută la reducerea semnificativă a decalajului dintre detectare și remediere. MTTD (timp mediu de detectare) rămâne o problemă proeminentă pentru echipele IT, dar MTTR prezintă o provocare și mai mare, deoarece majoritatea echipelor nu sunt bine echipate pentru a remedia rapid vulnerabilitățile.

vuln_GPT permite echipelor de securitate să rezolve rapid problemele critice, să reducă semnificativ timpul de reacție, să reducă consecințele costisitoare ale unui incident și să reducă MTTD și MTTR. Vicarius consideră că momentul este potrivit pentru a ajuta la rezolvarea decalajului de competențe, în special atunci când echipele interne de cercetare au personal redus și au resurse insuficiente.

Soluțiile Vicarius care identifică vulnerabilitățile software-ului sunt distribuie în România de compania SolvIT Networks.

Combaterea fraudelor financiare cu ajutorul GenAI

Un studiu global adresat profesioniștilor anti-fraudă, realizat de către SAS cu ACFE (Asociația Examinatorilor de Fraudă Certificați), dezvăluie un entuziasm foarte ridicat în privința AI-ului generativ, însă este prezentată și o realitate plină de provocări în domeniu.

AI-ul generativ a captivat imaginația publicului, pe fondul capacităților și promisiunilor de a se putea integra în fiecare dintre aspectele societății. Devine astfel, de înțeles, faptul că 83% dintre profesioniștii domeniului anti-fraudă anticipează că vor adăuga această tehnologie în arsenalul lor, în următorii doi ani.

Interesul pentru inteligență artificială (AI) și învățare automatizată (ML) este mai crescut ca niciodată.

ÎN PREZENT, APROXIMATIV 1 DIN 5 PROFESIONIȘTI ANTI-FRAUDĂ (18%) MENȚIONEAZĂ CELE DOUĂ UNELTE ÎNTRE CELE PE CARE LE FOLOSESC PENTRU A DETECTA FRAUDA.

Alți 32% anticipează că vor implementa astfel de tehnologii în următorii doi ani. În acest ritm, utilizarea AI și ML în programele anti-fraudă se va tripla până la finele lui 2025.

Cu toate acestea, rata de adoptare a inteligenței artificiale și a învățării automatizate este sub așteptări. Cu toate că interesul este foarte crescut, adoptarea efectivă a AI și ML a crescut cu doar 5% începând cu 2019. Estimările din 2019 și 2022 preconizau rate de 25%, respectiv 26%.

În vreme ce utilizarea unui număr ridicat de tehnici de analiză a datelor a ajuns la un platou, folosirea datelor biometrice și a roboticii în programele anti-fraudă a fost într-o continuă creștere și dezvoltare. Folosirea datelor biometrice fizice a crescut cu 14% începând cu 2019, fiind acum o resursă în cazul a 40% din respondenți. Unul din cinci (20%) intervievați folosește robotica, inclusiv automatizări robotice de procese, în creștere de la 9% în 2019. Aceste tehnologii sunt cel mai des întâlnite în cazul serviciilor bancare și financiare. 51% dintre respondenți folosesc date biometrice fizice, iar 33% folosesc robotica.

DefCamp – rol crucial în creșterea nivelului de conștientizare și înțelegere a securității cibernetice

Atacurile cibernetice au devenit tot mai numeroase în ultimii ani, dar în același timp și protecția societății românești s-a îmbunătățit, cu o conștientizare în creștere și investiții tot mai mari în securitate cibernetică. Tudor Damian, coordonator al ediției DefCamp Cluj-Napoca, ne-a vorbit într-un interviu despre principalele amenințări cibernetice, despre cum poate contribui societatea la promovarea unei culturi a securității, dar și despre principalele greșeli ale companiilor.

Tudor Damian,
Coordonator DefCamp Cluj-Napoca

Club IT&C: Care sunt cele mai mari amenințări și vulnerabilități în ceea ce privește securitatea cibernetică în ziua de astăzi?

Tudor Damian: Cele mai mari amenințări și vulnerabilități în securitatea cibernetică din momentul de față includ ransomware, phishing, atacurile asupra lanțului de aprovizionare (supply chain attacks), vulnerabilitățile software nesecurizate și amenințările interne. Cu o clară tendință de creștere în ultimii ani, ransomware-ul continuă să fie o problemă majoră, cu atacuri care criptează datele victimelor și cer recompense pentru decriptare. Phishing-ul exploatează ingineria socială pentru a obține acces la informații confidențiale, de obicei ocolind majoritatea măsurilor tehnice de protecție și făcând apel la neatenția sau naivitatea utilizatorilor. Atacurile asupra lanțului de aprovizionare țintesc furnizorii de software sau hardware, afectând multe organizații printr-un singur punct de vulnerabilitate cu mult timp înainte ca produsele lor să ajungă în posesia clienților.

Club IT&C: Cât de protejată este astăzi societatea românească în fața atacurilor cibernetice?

Tudor Damian: Protecția societății românești în fața atacurilor cibernetice s-a îmbunătățit în ultimii ani, cu o conștientizare în creștere și investiții în securitate cibernetică. Totuși, ca în orice altă țară, există un spectru larg de maturitate în securitatea cibernetică între diferite organizații, unele fiind foarte bine protejate, în timp ce altele sunt mai vulnerabile.
O tendință pozitivă, însă, este legată de creșterea gradului de conștientizare al pericolului acestor amenințări atât în cadrul organizațiilor de toate dimensiunile, precum și în rândul publicului larg.

Club IT&C: Cum poate un eveniment precum Defcamp să contribuie la creșterea nivelului de conștientizare și înțelegere a securității cibernetice în rândul companiilor și indivizilor?

Tudor Damian: Evenimentele precum DefCamp joacă un rol crucial în creșterea nivelului de conștientizare și înțelegere a securității cibernetice. Acestea oferă platforme pentru schimbul de cunoștințe și de bune practici între experți în securitate, companii și publicul larg. Discuțiile, prezentările, demonstrațiile și competițiile de hacking contribuie la educația și formarea participanților, sensibilizându-i cu privire la riscurile cibernetice și modalitățile de a se proteja.

Club IT&C: Au înțeles companiile din România importanța securității cibernetice? Se află acest domeniu printre principalele investiții?

Tudor Damian: Deși companiile din România încep să înțeleagă importanța securității cibernetice, mai ales în contextul ultimelor atacuri și riscuri făcute publice, gradul de investiție și atenție acordată acestui domeniu încă variază destul de mult de la o companie la alta. Multe organizații au început să aloce bugete semnificative pentru securitatea informației și conformitate, recunoscând că securitatea cibernetică este fundamentală pentru protecția datelor, a activelor și a reputației. Din păcate, în multe cazuri acești pași sunt încă într-o fază incipientă, sau ajung să facă acest pas doar în urma unui incident de securitate.

Club IT&C: Ce tehnologii emergente sau tendințe în securitatea cibernetică ar trebui să urmărim în viitorul apropiat?

Tudor Damian: Pe termen scurt și mediu, noile tendințe în domeniul securității cibernetice cu siguranță vor include inteligența artificială și învățarea automată pentru detectarea amenințărilor și răspuns automatizat, securitatea bazată pe identitate pentru a gestiona accesul la resurse, securitatea Cloud și strategiile "Zero Trust". De asemenea, pașii repezi cu care domeniul criptografiei post-quantum avansează reprezintă o nouă amenințare și necesită noi abordări pentru asigurarea integrității și confidențialității datelor.

Club IT&C: Care sunt cele mai frecvente greșeli sau neglijențe pe care le fac companiile în ceea ce privește securitatea cibernetică și cum pot fi evitate?

Tudor Damian: Din experiența de până acum, cele mai frecvente greșeli sau neglijențe includ de cele mai multe ori lipsa unei strategii de securitate cibernetică cuprinzătoare, slaba gestionare a patch-urilor de securitate, lipsa instruirii angajaților pe zona de securitate cibernetică și insuficiența (sau inexistența) planurilor de răspuns la incidente. Companiile pot evita aceste greșeli prin adoptarea unui cadru de securitate robust, prin educarea continuă a angajaților și testarea periodică a capacității lor de răspuns la incidente.

Club IT&C: Care este rolul educației și al conștientizării publicului în promovarea securității cibernetice și cum poate societatea în ansamblu să contribuie la crearea unui mediu online mai sigur?

Tudor Damian: Educația și conștientizarea publicului sunt esențiale pentru promovarea securității cibernetice. Inițiativele de educație publică, campaniile de conștientizare și programele de formare pot ajuta indivizii să recunoască și să evite comportamentele riscante online. Societatea în ansamblu poate contribui prin promovarea unei culturi a securității, încurajând practici de securitate bune la nivel individual și organizațional, și susținând politicile și reglementările care protejează spațiul cibernetic. Cu siguranță, creșterea vizibilă a numărului de evenimente de profil precum DefCamp pe piața autohtonă constituie la rândul ei un catalizator.

Crește numărul de campanii care folosesc documente PDF cu cod malițios sau care exploatează vulnerabilități în aplicațiile Office

Raportul trimestrial HP Wolf Security Threat Insights arată că atacatorii cibernetici continuă să găsească modalități ingenioase de a-i păcăli pe utilizatori și de a infecta punctele terminale.

Echipa de cercetare a descoperit mai multe campanii notabile, printre care:

• Campania DarkGate, care folosește instrumente publicitare pentru a perfecționa atacurile - Atașamentele PDF malițioase, care apar ca mesaje de eroare OneDrive, direcționează utilizatorii către conținut sponsorizat găzduit de o platformă publicitară populară și de acolo către malware-ul DarkGate.

o Prin utilizarea serviciilor de anunțuri publicitare, hackerii pot analiza ce momeli generează click-uri și infectează cei mai mulți utilizatori, iar acest lucru îi ajută să rafineze campaniile pentru un impact sporit.

o Hackerii pot utiliza instrumente CAPTCHA pentru a împiedica sandbox-urile să scaneze programele malware și să oprească atacurile.

o DarkGate le oferă atacatorilor cibernetici acces backdoor în rețele, expunând victimele la riscuri precum furtul de date și ransomware.

• Exploit-uri Office - În trimestrul al patrulea (T4) din 2023, cel puțin 84% dintre tentativele de intruziune care au folosit foi de calcul și 73% dintre cele cu documente Word au încercat să exploateze vulnerabilități în aplicațiile Office.

• Malware-ul PDF e tot mai folosit - 11% din malware-ul analizat în T4 a folosit PDF-uri, comparativ cu doar 4% în T1 și T2 din 2023. Un exemplu notabil a fost o campanie WikiLoader care a folosit un PDF fals de livrare a coletelor pentru a-i păcăli pe utilizatori să instaleze malware-ul Ursnif.

• Discord și TextBin sunt folosite pentru a găzdui fișiere malițioase - Hackerii folosesc site-uri legitime pentru a găzdui fișiere infectate și, astfel, evită scanerele anti-malware.

Prin izolarea amenințărilor care au evitat instrumentele de detectare de pe PC-uri – dar, în același timp, permițând ca programele malware să ruleze în siguranță - HP Wolf Security are o perspectivă specifică asupra celor mai recente tehnici folosite de hackeri în peisajul în continuă schimbare al criminalității cibernetice. Până în prezent, clienții HP Wolf Security au deschis peste 40 de miliarde de atașamente de e-mail, pagini web și fișiere descărcate, fără să fie raportate breșe de securitate.

Raportul detaliază modul în care atacatorii cibernetici continuă să-și diversifice metodele de atac pentru a ocoli politicile de securitate și instrumentele de detectare. Alte constatări includ:

• Arhivele au fost cel mai popular tip de livrare de malware pentru al șaptelea trimestru consecutiv, fiind folosite în 30% dintre programele malware analizate de HP.

• Cel puțin 14% dintre amenințările prin e-mail identificate de HP Sure Click au ocolit unul sau mai multe instrumente de securitate.

• Principalii vectori de amenințare în trimestrul al patrulea au fost e-mailurile (75%), descărcările din browser (13%) și alte mijloace, cum ar fi USB-urile (12%).

Secure By Design, un pariu sigur în securitatea cibernetică

De cele mai multe ori, reacția imediată la incidentele de securitate, cum ar fi atacurile ransomware, este căutarea cauzei. Impactul atacurilor demonstrează costurile ridicate ale problemelor de securitate. Nimeni nu vrea să fie următoarea victimă a unui „data breach".

Dar în securitatea cibernetică, de obicei, nu există o singură cauză. În majoritatea incidentelor, atacatorii profită de un lanț de vulnerabilități. Nu este productiv să cauți cauza și efectul când. Echipele de securitate ar trebui să analizeze mediul general, arhitectura și modul în care funcționează tehnologia, precum și procesele și cultura lor de afaceri și să le apropie de arhitectura zero-trust. Probabil că povestea despre ALPHV / BlackCat și-au lansat atacurile nu va fi cunoscută complet, dar sunt cunoscute unele dintre condițiile care au ajutat să înșele victimele și cum au creat riscuri care i-au favorizat pe atacatori.

Securizat prin design, Securizat implicit

Atacurile BlackCat / ALPHV subliniază cât de dificilă este securizarea serverelor. Actualizările multiple, parolele de administrator și reluarea parolei se adaugă la o suprafață de atac mare, complexă și fragilă. Acest tip de configurație favorizează de obicei atacatorii.

Alternativa se bazează principiile Secure by Design și Secure by Default, care acordă prioritate securității în toate caracteristicile produsului, operațiunile și procesele. Secure by Design și Secure by Default se bazează pe detalii. Este ușor să spui că un produs acordă prioritate securității, dar este dificil să îndeplinească acel criteriu.

RSA dezvoltă soluții de securitate care se bazează pe aceste principii. Nu se sincronizează parolele Active Directory sau LDAP — nu sunt acele acreditări. În schimb, se solicită implementarea un dispozitiv virtual care se conectează la arhivele locale de utilizatori și validează parolele în timp real, în loc să le detecteze și să le sincronizeze cu cloud.

Aici sunt unele compromisuri: este nevoie mai mult timp și efort pentru implementarea unui dispozitiv virtual consolidat și routerul de identitate virtuală. Dar acesta cost se merită, pentru că se minimizează suprafața de atac.

RSA Mobile Lock, care stabilește încredere în dispozitivele neadministrate și ajută la securizarea BYOD, subliniază principiile Secure by Design și Secure by Default. Mobile Lock caută amenințări doar când utilizatorii încearcă să se autentifice folosind RSA Authenticator pentru iOS și Android și restricționează autentificarea numai atunci când detectează o amenințare. De asemenea, interoghează doar minimumul absolut de date pentru a-și îndeplini funcțiile.

La fel este și cu agentul de autentificare cu mai mulți factori (MFA). În cazul unei întreruperi a internetului, agentul MFA este în siguranță la o implementare locală. Aceasta înseamnă că atacatorii nu pot evita MFA doar deconectându-se de la internet sau făcând ca serviciul de backend MFA să pară offline.

Securitatea adevărată nu este niciodată supraproiectată: se bazează pe un amestec sensibil de soluții simple ori de câte ori este posibil și una mai complexă atunci când este necesar. Fiecare componentă a unui serviciu trebuie să fie proiectată pentru a limita suprafața de atac ori de câte ori este posibil. Asta înseamnă să colectezi doar minimumul de informații de care un sistem are absolut nevoie și să folosești acele informații numai atunci când este nevoie. Înseamnă, de asemenea, luarea unor decizii arhitecturale care să minimizeze suprafața de atac, mai degrabă decât să o extindă inutil.

Soluţiile RSA pot fi achiziţionate în România prin distribuitorul SolvIT Networks.

Companiile investesc anual pentru a-și perfecționa echipele de securitate cibernetică

Peste 70% dintre companii plătesc mai mult de 100.000 USD pentru formare suplimentară, anual, pentru a actualiza abilitățile angajaților lor din departamentele de securitate cibernetică, a arătat un studiu recent Kaspersky.

Cu toate acestea, există o lipsă de cursuri relevante care să acopere noi sfere problematice de pe piața educațională și formările nu le aduc întotdeauna rezultatul așteptat. Potrivit cercetării, companiile investesc sume semnificative în îmbunătățirea competențelor echipelor lor de securitate cibernetică: 43% dintre organizații spun că de obicei cheltuiesc între 100.000 și 200.000 USD pe an pe cursuri de securitate a informațiilor, în timp ce 31% investesc chiar peste 200.000 USD pentru programe de formare. Restul de 26% declară că plătesc de obicei mai puțin de 100.000 USD pentru inițiative educaționale.

Mulți profesioniști în securitate cibernetică (39%) consideră că instruirea acordată de companii nu este suficientă. Pentru a rămâne competitivi pe piață și pentru a-și menține cunoștințele și abilitățile la zi, aceștia sunt dispuși să plătească pentru cursuri de formare suplimentare din banii lor.

Piața educațională se luptă să țină pasul cu industria în schimbare rapidă și nu reușește să livreze la timp programele de formare necesare. Deficitul de cursuri care acoperă noi sfere provocatoare (49%) e principala problemă pentru cei care caută formare în domeniul securității cibernetice.

Majoritatea cursanților tind să uite ceea ce au învățat pentru că nu au ocazia să aplice cunoștințele nou dobândite, prin urmare cursurile le sunt inutile.

Nevoia de pre-condiții speciale de pregătire, cum ar fi codarea și matematica superioară, care nu sunt specificate în etapa de preînregistrare, e de asemenea, problematică pentru 45% dintre practicieni.

Pentru a pregăti în mod eficient echipele de securitate cibernetică, experții Kaspersky recomandă următoarele:

- Investiți în cursuri de securitate cibernetică de calitate pentru specialiști, pentru a-i ține la curent cu cele mai recente cunoștințe.
- Folosiți simulatoare interactive pentru a testa expertiza angajaților și pentru a evalua modul în care aceștia gândesc în situații critice.
- Oferiți profesioniștilor dumneavoastră InfoSec o vizibilitate mai bună asupra amenințărilor cibernetice care vizează organizația.

Soluții de securitate anti-efracție și automatizare rezidențială

Johnson Controls oferă soluții holistice pentru toată gama de sisteme de siguranță și securitate, în special pentru sistemele de detecție și avertizare la efracție, de la detectori și senzori până la sisteme de semnalizare dotate cu inovații de ultimă oră – cum ar fi tehnologia wireless PowerG.

Soluțiile inteligente de detectare a efracției de la Johnson Controls oferă o protecție cuprinzătoare multi-stratificată împotriva potențialelor amenințări și ajută la crearea unui mediu sigur de lucru și de viață. De asemenea, aceste soluții oferă o integrare flexibilă cu sistemele existente, inclusiv cele video,cele pentru control acces și alte sisteme. Tehnologia wireless PowerG oferă toate beneficiile securității tradiționale prin cablu, fără problemele și vulnerabilitățile cablurilor, integrând și consolidând întregul ecosistem de dispozitive de securitate aflate la sediul clienților, oferind utilizatorilor control fără probleme asupra propriei securități. Dispozitivele wireless PowerG funcționează cu tehnologie de ultimă oră, oferind fiabilitate și performanță optime. Integrarea wireless bidirecțională PowerG sporește siguranța clădirilor și prin opțiunile de scalabilitate și extindere la nivel înalt ale rețelei de securitate.

Ca element central al unei soluții de detecție a efracției, centrala integrată de securitate și home automation **Qolsys** IQ Panel 4, certificată Grad 2 conform normativului european EN50131, oferă conectivitate și fiabilitate de cea mai înaltă clasă, integrând multiple canale de comunicație a datelor: LTE, Wi-Fi, Z Wave, Zigbee, Bluetooth, PowerG, etc., și este compatibilă cu unele protocoale de comunicație wireless de generație mai veche. Ecranul tactil elegant cu rezoluție HD de 7" are o cameră de 8 megapixeli

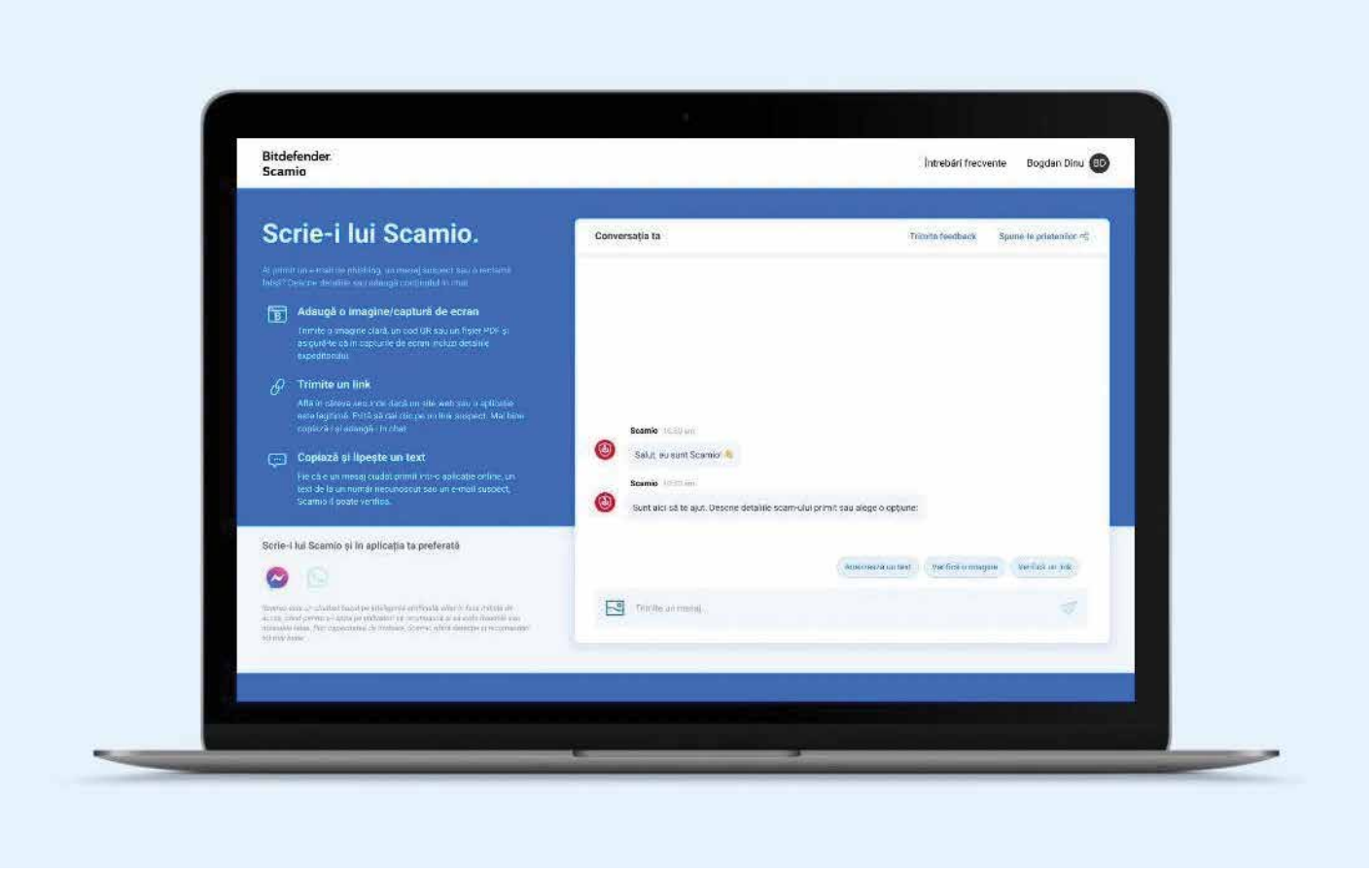
îmbunătățită cu un dispozitiv Flex-Tilt pentru a regla unghiul camerei pentru obținerea fotografiilor transmise la dezarmarea sistemului sau vizualizarea înregistrărilor video din timpul alarmelor. Qolsys IQ Panel 4 răspunde adecvat diferitelor cerințe ale clienților, dar toate cu aceleași caracteristici de bază: capacitatea de a înrola peste 120 de dispozitive de siguranță / securitate (detectori de mișcare, de incendiu, de inundație, de șocuri, etc.) și peste 150 de dispozitive de automatizare (termostate, becuri, comutatoare electrice, electrovane, relee de comandă diverse etc.), dar și videointerfoane și camere video de supraveghere într-o singură locație, putând fi separate în mai multe partiții pentru gestionarea securizată a acestora, oferind astfel control total utilizatorului asupra propriei locuințe. Performanțele deosebite ale tuturor centralelor sunt asigurate cu ajutorul unui procesor integrat IoT Snapdragon 8 core de la Qualcomm. Comunicația wireless PowerG criptată AES 128 biți, ultra-fiabilă, bidirecțională, cu optimizarea automată a puterii de emisie, cu salt de frecvență în banda de comunicație 868MHz, asigură o comunicație sigură între centrale și detectori, ignorând toate interferențele electromagnetice punctuale și oferind astfel o protecție cibernetică de neegalat, asigurând performanță fiabilă cu minimalizarea incidentelor datorate unor potențiale alarme false.

De asemenea, centralele Qolsys IQ se bucură de o integrare completă cu serviciile de securitate interactive Alarm.com care oferă suport extins pentru clienții din mediul rezidențial, IMM/Comercial, Wellness, dezvoltatori sau clădiri multi-familiale, toate într-o singură aplicație mobilă intuitivă. Platforma robustă, gestionată în cloud Alarm.com oferă control deplin asupra sistemelor

smart de securitate, folosind tehnologii inovatoare care cresc interacțiunea dintre oameni și lucrurile la care țin cel mai mult – familiile, căminele și afacerile lor.
În familia de produse ELKO au fost incluse și echipamentele de detecție Visonic. Acesta este un dezvoltator și producător internațional de sisteme și componente electronice specializate de securitate. Visonic oferă senzori și alte tipuri de periferice, 100% compatibile cu centralele de efracție Qolsys, încorporând cele mai avansate soluții de detectare a efracțiilor pentru o protecție de înaltă securitate (Grad 2 și 3) pentru interior, exterior și de perimetru, pentru orice locație comercială, industrială sau rezidențială. Datorită acestei compatibilități, familia de periferice de securitate Visonic se bucură de instalare rapidă și simplă, iar preocuparea constantă a producătorului pentru soluțiile ecologice are ca punct central minimizarea consumului de energie al acestora, ceea ce duce la o durată de viață mai lungă a bateriilor.
Echipa ELKO Romania, cu experiența câștigată de-a lungul anilor în domeniul securității fizice, vă poate ajuta cu informații, demo de produs sau Proof of Concept, în vederea evaluării aplicabilității în diverse scenarii de utilizare (solutii@elko.ro).

Bitdefender Scamio – Detectorul tău de fraude bazat pe AI

Acest chatbot gratuit, te ajută 24/7 să verifici rapid orice mesaj, folosește soluțiile Bitdefender de detecție a atacurilor cibernetice.
Trimite orice text, e-mail, mesaj primit într-o aplicație online, link sau cod QR suspect pentru a fi analizat în câteva secunde. Scamio descoperă cu ușurință chiar și cele mai bine deghizate fraude.
Este ușor să folosești Scamio și e gratuit. Iată cum:
1. Începe o conversație cu Scamio și conectează-te la contul tău Bitdefender.
2. Copiază textul unui mesaj pe care l-ai primit, încarcă o captură de ecran a unui e-mail sau doar pune o întrebare.
3. Obții un răspuns rapid de la Scamio și scapi de dubii.
Indiferent că este vorba despre tentative de phishing, site-uri frauduloase, e-mailuri înșelătoare sau tactici de inginerie socială, Scamio le dă de urmă.
Cu Scamio alături, ești protejat de fraudele de azi și de mâine.



NIS 2: Antifragile în securitatea cibernetică

Directiva NIS 2 (Directiva (UE) 2022/2555) are ca scop îmbunătățirea securității cibernetice în diferite sectoare, impunând cerințe stricte de securitate cibernetică și obligații de gestionare a incidentelor. Aceasta impune entităților să implementeze analize de risc, politici de securitate IT, și proceduri de gestionare a incidentelor pentru a reduce eficient amenințările cibernetice. Mai mult, directiva pune accentul pe obligațiile de raportare pentru incidentele potențiale și permite divulgarea coordonată a vulnerabilităților.

de Alexandru Trifu, Chief Sales Officer la LifeinCloud

Pentru companiile care folosesc soluții de cloud computing și servicii de tip management IT, respectarea NIS 2 este crucială pentru a asigura măsuri solide de securitate cibernetică și capacități de răspuns la incidente. Prin respectarea NIS 2, organizațiile își pot îmbunătăți postura de securitate, pot întări securitatea lanțului de aprovizionare, pot îmbunătăți securitatea rețelelor și pot întări măsurile de control al accesului.

În plus, alinierea cu cerințele NIS 2 poate duce la o creștere a conștientizării, pregătirii și rezilienței cibernetice împotriva amenințărilor cibernetice, protejând în cele din urmă infrastructura și serviciile critice.

Măsurile-cheie de securitate cibernetică necesare conform Directivei NIS 2 includ:

• Analiza riscului și politici de securitate a sistemului informațional: Organizațiile trebuie să efectueze analize de risc și să stabilească politici robuste de securitate a sistemului informațional pentru a identifica și a reduce riscurile cibernetice

• Evaluarea eficacității gestionării riscurilor cibernetice: Entitățile sunt obligate să evalueze eficacitatea practicilor lor de gestionare a riscurilor cibernetice pentru a se asigura că se protejează adecvat împotriva amenințărilor cibernetice

• Planificarea continuității afacerilor: NIS 2 subliniază importanța de a avea planuri cuprinzătoare de continuitate a afacerilor pentru a asigura reziliența operațională în fața incidentelor cibernetice

• Cerințe de securitate și arhitectură de rețea de referință: Implementarea unor cerințe specifice de securitate și stabilirea unei arhitecturi de rețea de referință sunt componente cruciale ale respectării măsurilor de securitate cibernetică NIS 2

• Supravegherea conducerii și formarea în domeniul securității cibernetice: Directiva impune consiliilor de administrație să supravegheze abordările de gestionare a riscurilor cibernetice și să impună formarea în securitatea cibernetică pentru angajați pentru a îmbunătăți în mod general conștientizarea în domeniul securității

• Securitatea lanțului de aprovizionare: Organizațiile trebuie să abordeze vulnerabilitățile din lanțul lor de aprovizionare și să asigure practici sigure de dezvoltare pentru a reduce riscurile asociate dependențelor de terți.

Soluțiile de cloud computing oferă beneficii de securitate cibernetică prin posibilitatea de a fi antifragile, un concept din cartea lui Nassim Taleb "Antifragil: Lucrurile care câștigă din dezordine". Antifragilitatea în securitatea cibernetică implică îmbunătățirea sistemelor în urma stresorilor, șocurilor și atacurilor, spre deosebire de reziliență, care menține starea actuală. Infrastructurile de cloud computing pot fi proiectate să fie antifragile, câștigând din dezordine și devenind mai robuste cu fiecare provocare.

Organizațiile pot deveni antifragile în măsurile lor de securitate cibernetică adoptând următoarele strategii:

• Lecții învățate: Implementarea unui proces robust de lecții învățate este crucială pentru ca organizațiile să devină antifragile. Acest lucru implică analizarea incidentelor de securitate cibernetică anterioare, înțelegerea modului în care au avut loc și încorporarea acestor insight-uri în apărarea viitoare

• Strategia barbell: Strategia barbell a lui Nassim Taleb poate fi aplicată și în securitatea cibernetică. Această abordare combină măsuri hyper-conservative (fragile) și hyper-agresive (antifragile) în timp ce minimizează orice lucru în mijloc (rezilient). De exemplu, utilizarea modelelor de criptare asimetrice cu chei private fragile și chei publice antifragile poate ajuta la protejarea informațiilor sensibile

• Testare echipa purple: Desfășurarea exercițiilor de echipa purple poate ajuta organizațiile să devină antifragile. Acest exercițiu de colaborare între apărători și atacatori permite o mai bună înțelegere a mecanismelor atacului și apărării, ducând la îmbunătățirea măsurilor de securitate cibernetică

• Operații autonome de securitate: Implementarea operațiilor autonome de securitate poate ajuta organizațiile să

devină antifragile. Prin analizarea automată a datelor de activitate și învățarea din ele, aceste sisteme pot identifica și mitiga rapid amenințările fără intervenție umană.

Prin adoptarea acestor strategii, organizațiile pot depăși doar reziliența și pot deveni antifragile, învățând și devenind mai puternice în fața provocărilor de securitate cibernetică.

Unele măsuri de protecție de bază pentru reziliența cibernetică includ:

• Implementarea autentificării în doi pași: Utilizarea autentificării în doi pași pentru a adăuga un nivel suplimentar de securitate conturilor utilizatorilor, făcând mai dificil accesul persoanelor neautorizate la informații sensibile

• Testarea și evaluarea regulată a sistemelor: Realizarea regulată a evaluărilor de vulnerabilități, a testelor de penetrare și a auditurilor de securitate pentru a identifica punctele slabe și lacunele din sisteme. Această abordare proactivă ajută la abordarea vulnerabilităților înainte ca atacatorii să le poată exploata

• Stabilirea criptării și protecției datelor: Implementarea unor măsuri robuste de criptare pentru a proteja datele în repaus și în tranzit. Implementarea unor controale de acces stricte, protocoale de autentificare și categorii de clasificare a datelor pentru a asigura confidențialitatea, integritatea și disponibilitatea informațiilor critice

• Dezvoltarea unei strategii robuste de backup și recuperare: Pregătirea pentru scenarii de coșmar prin crearea unei strategii cuprinzătoare pentru backup și recuperarea datelor. Realizarea regulată a backup-urilor pentru datele critice, efectuarea testelor pentru a asigura procesele eficiente de restaurare și luarea în considerare a utilizării backup-urilor în afara locului sau a soluțiilor bazate pe cloud pentru redundanță sporită

• Monitorizarea continuă a amenințărilor: Utilizarea sistemelor de monitorizare în timp real care oferă vizibilitate în rețele, sisteme și aplicații. Utilizarea sistemelor de detectare a intruziunilor, a informațiilor de securitate și a managementului

evenimentelor (SIEM) și a analizei jurnalelor pentru a detecta și răspunde prompt la amenințările cibernetice.

Unele amenințări cibernetice comune de care ar trebui să fie conștiente organizațiile includ:

• Malware: Malware este o amenințare comună și persistentă care implică instalarea de software nedorit pe un sistem pentru a cauza daune, cum ar fi blocarea accesului, ștergerea fișierelor, furtul de informații sau răspândirea la alte sisteme

• Furtul de parole: Furtul de parole apare atunci când persoane neautorizate fură sau ghicesc parole pentru a obține acces la informații sensibile. Atacatorii pot folosi diverse metode, cum ar fi atacurile brute force sau ingineria socială, pentru a obține parole

• Interceptarea traficului: Cunoscută și sub numele de spionaj, interceptarea traficului implică interceptarea informațiilor trimise între un utilizator și o gazdă. Aceste informații furate pot include autentificări sau date valoroase, care pot fi folosite în mod rău intenționat

• Atacuri de phishing: Escrocheriile de phishing se bazează pe inginerie socială pentru a păcăli persoanele în a dezvălui informații sensibile, cum ar fi parolele. Atacatorii trimit adesea mesaje sau e-mailuri înșelătoare care par legitime pentru a obține date personale

• Atacuri DDoS: Atacurile Distribuite de Serviciu Denial (DDoS) supraîncarcă serverele cu solicitări de utilizator, ceea ce determină încetinirea sau inaccesibilitatea site-urilor web. Aceste atacuri perturbă operațiile normale prin inundarea serverelor cu trafic

• Amenințările interne: Amenințările interne apar atunci când persoanele cu acces autorizat compromit intenționat sau neintenționat securitatea unei organizații. Acest lucru poate include angajați care împărtășesc date sensibile, devin victime ale atacurilor de phishing sau trec cu intenție peste măsurile de securitate

• Amenințări persistente avansate (APT-uri): APT-urile sunt atacuri cibernetice sofisticate și țintite care își propun să fure date pe o perioadă extinsă fără a fi detectate. Detectarea anomalilor în datele de ieșire și monitorizarea activităților neobișnuite sunt cruciale în combaterea APT-urilor

• Malvertising: Malvertising implică injectarea de cod malițios în rețelele legitime de publicitate online pentru a redirecționa utilizatorii către site-uri malițioase sau pentru a instala malware pe dispozitivele lor. Rețelele de publicitate ar trebui să implementeze procese de validare pentru a reduce riscul de atacuri de malvertising.

Prin aplicarea principiilor de antifragilitate în securitatea cibernetică, organizațiile își pot îmbunătăți capacitatea de a prospăta în fața amenințărilor cibernetice, trecând dincolo de simpla reziliență, pentru a se îmbunătăți și a evolua activ în fața adversității.

Companiile au nevoie de peste 6 luni pentru a ocupa posturile de securitate cibernetică

Pe măsură ce piața globală ale muncii continuă să solicite profesioniști InfoSec, cea mai recentă cercetare Kaspersky a arătat că 41% dintre companii recunosc că echipele lor de securitate cibernetică au personal insuficient.

Studiul identifică abilitățile și caracteristicile cerute de șefi atunci când angajează personal.

Respondenții spun că este nevoie de peste șase luni pentru a ocupa o poziție medie de InfoSec. Așa cum era de așteptat, recrutarea pentru funcții de nivel superior durează cel mai mult, 36% dintre companii spunând că necesită aproape un an sau mai mult, în timp ce locurile de muncă pentru juniori pot fi ocupate în cel mai scurt timp - una până la trei luni, potrivit a 42% dintre respondenți. Aceste cifre sunt alarmante, deoarece companiile care își desfășoară activitatea pentru perioade lungi de timp fără personalul necesar sunt expuse unui risc uriaș. Absența personalului de securitate cibernetică oferă infractorilor oportunități ample de a pătrunde în infrastructura companiei și de a afecta procesele de business.

Întrebați despre cele mai mari provocări în găsirea și angajarea profesionistului InfoSec „potrivit", majoritatea respondenților au menționat o discrepanță între certificare și competențele practice reale (52%) și lipsa de experiență (49%), subliniind că expertiza profesională dovedită este una dintre cele mai importante caracteristici pe care companiile le caută la un practician în securitate cibernetică.

Costul mare în angajarea acestor specialiști este un obstacol pentru 48% dintre șefi, iar concurența globală, exprimată prin practici de angajare agresive și competitive de către mai multe organizații, deranjează peste 41% dintre respondenți. Cifre ca acestea arată că, indiferent dacă o companie găsește în sfârșit candidați care îndeplinesc toate cerințele, nu înseamnă că aceștia vor și lucra pentru compania respectivă, deoarece într-un mediu atât de competitiv, alte organizații îi pot urmări, astfel încât procesul de angajare ar putea continua pe termen foarte lung.

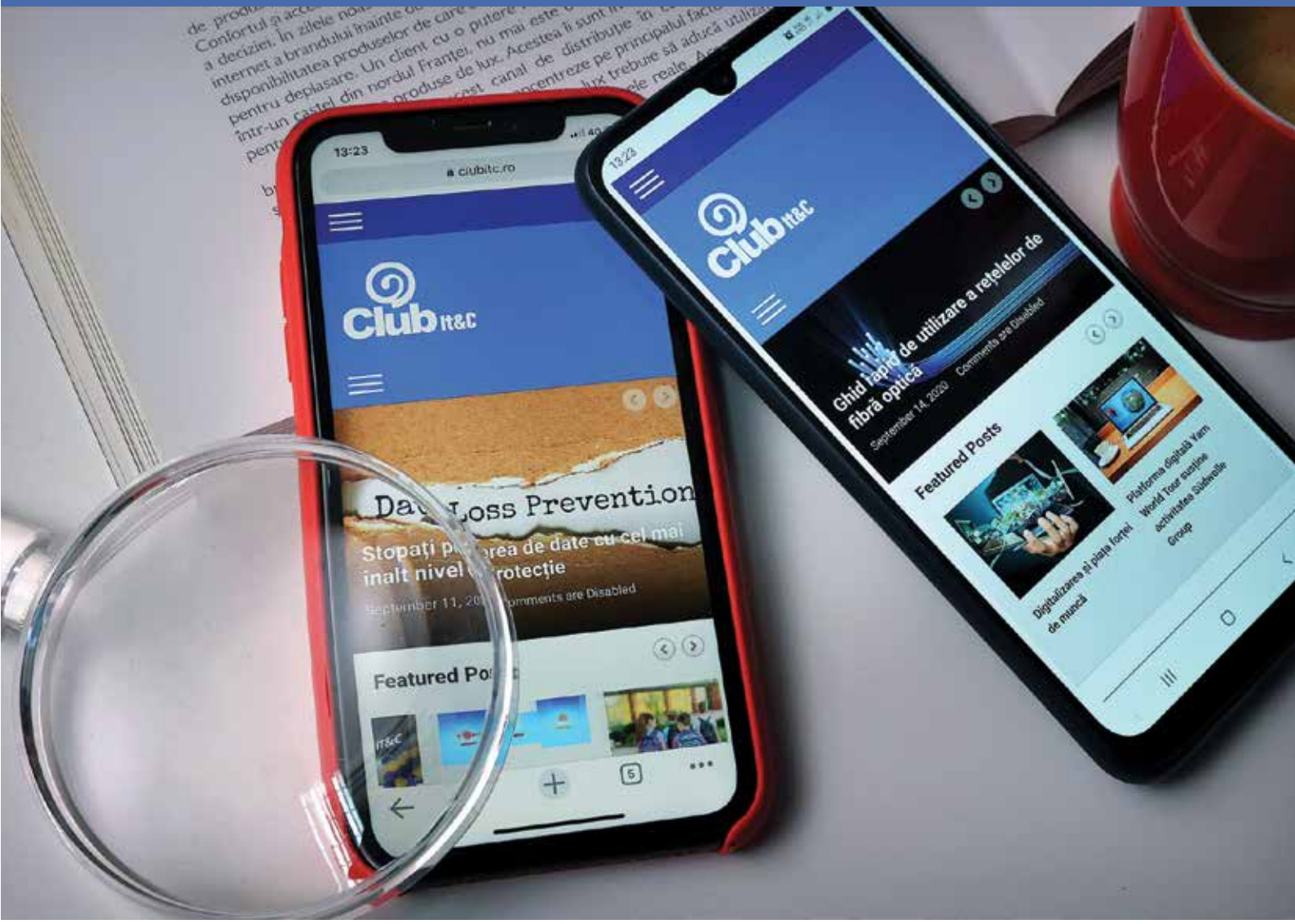
Pentru a minimiza consecințele negative ale deficitului global de personal de securitate cibernetică, experții Kaspersky recomandă următoarele:

• Adoptați servicii de securitate gestionate, cum ar fi Kaspersky Managed Detection and Response (MDR) și/sau Incident Response, dobândind astfel expertiză suplimentară fără a angaja personal suplimentar. Acest lucru ajută la protejarea împotriva atacurilor cibernetice și la investigarea incidentelor în cazul în care compania nu are personal de securitate cibernetică.

• Educați în mod regulat personalul IT și InfoSec despre riscurile cibernetice reale și investiți în formarea lor pentru a-și dezvolta abilitățile în detectarea și răspunsul la amenințările cibernetice chiar și sofisticate.

• Utilizați soluții centralizate și automatizate, cum e Kaspersky Extended Detection and Response (XDR) ca să reduceți sarcinile echipei de securitate IT și să minimizați riscurile. Prin agregarea și corelarea datelor din mai multe surse într-un singur loc și folosind tehnologii de învățare automată, astfel de soluții reduc timpul mediu de detectare a amenințărilor (MTTD) și oferă răspuns automat rapid.

more information, better solutions



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

Club IT&C

www.clubitc.ro www.clubitc.eu

Pregătit pentru provocări cu noile tehnologii

Descoperă soluțiile potrivite pentru afacerea ta.

www.vodafone.ro/business

Together we can
vodafone business