Raportul Business Internet Security 2025

Ediția a VII-a

Noiembrie, 2024

orange™ Business

Cuprins

Am investit în soluții avansate de detecție, gestionare și prevenție, pentru a ne asigura că partenerii noștri beneficiază de cele mai moderne tehnologii.

Julien Ducarroz
Chief Executive Officer
Orange România

2024 a fost și continuă să fie un an plin de provocări majore în domeniul securității cibernetice, marcat de o creștere semnificativă atât în numărul, cât și în complexitatea atacurilor cibernetice. Într-un context global în care amenințările cibernetice devin tot mai sofisticate, observăm tot mai des atacuri direcționate inclusiv către infrastructuri critice, ceea ce subliniază vulnerabilitățile sistemelor esențiale. Datele colectate de noi arată că sectorul energetic a fost cel mai vizat (31% dintre atacuri), urmat de administrația locală și centrală (27%) și industria IT&C (25%).

În plus, am asistat la o intensificare a atacurilor asupra infrastructurilor de telecomunicații, un segment esențial pentru funcționarea societății moderne. La acest context s-a adăugat intrarea în vigoare a directivei EU NIS2 pe 17 octombrie, care extinde cerințele de securitate pentru furnizorii de servicii digitale și impune noi standarde pentru gestionarea riscurilor asociate entităților și rețelelor critice.

La Orange, am răspuns acestor provocări printr-o creștere continuă a portofoliului nostru de servicii de securitate cibernetică. Am investit în soluții avansate de detecție și gestionare a vulnerabilităților, precum Threats Exposures Management (TEM), în servicii de monitorizare și răspuns la incidente prin SOC-ul Orange Business, precum și în soluții de prevenție, precum BIS – Business Internet Security, dar și de consultanță în securitate cibernetică, totul pentru a ne asigura că partenerii noștri beneficiază de cele mai moderne tehnologii și de expertiza necesară pentru protejarea infrastructurilor lor.

Un alt aspect esențial al eforturilor noastre este implicarea activă în educația și formarea viitorilor experți în securitate cibernetică. În cadrul parteneriatelor noastre strategice, sprijinim organizarea celor mai importante competiții și evenimente naționale din acest domeniu, precum RoCSC, UNbreakable România, DefCamp și Olimpiada Națională de Securitate Cibernetică (OSC). Anul trecut, peste 3.300 de tineri talentați au participat la aceste competiții, demonstrând interesul și potențialul ridicat în acest sector. Prin aceste inițiative, continuăm să susținem dezvoltarea unei noi generații de profesioniști care să ajute la consolidarea securității digitale atât la nivel național, cât și internațional.

1. Securitatea cibernetică în 2024 Provocări, incidente importante și schimbări

Într-o lume din ce în ce mai digitalizată, securitatea cibernetică devine o prioritate esențială pentru organizații, guverne și indivizi. Anul 2024 a adus o serie de provocări fără precedent în acest domeniu, pe fondul avansului tehnologic rapid și a amenințărilor cibernetice tot mai sofisticate.

Deschidem prima ediție în limba română a raportului BIS trecând în revistă principalele provocări cu care se confruntă securitatea cibernetică în 2024, incidentele de securitate notabile care au avut loc și schimbările semnificative în reglementări și practici.

Unul dintre cele mai mari obstacole în calea securității cibernetice este complexitatea crescândă a amenințărilor. Atacurile ransomware continuă să fie printre cele mai frecvente forme de atac, iar în 2024, grupările de hackeri au devenit mai organizate și mai sofisticate. Nu mai este vorba doar despre criptarea fișierelor și cererea de răscumpărare; acum, atacatorii amenință să publice date sensibile, aplicând presiune suplimentară asupra victimelor.

Inteligența artificială (I.A.) este folosită din ce în ce mai des de către atacatori

Pe măsură ce tehnologiile de inteligență artificială avansează, acestea sunt utilizate atât de către atacatorii cibernetici, cât și de specialiștii în securitate. De exemplu, atacatorii pot utiliza I.A. pentru a automatiza atacurile de phishing, făcându-le și mai convingătoare. Într-un fel similar celui în care Large Language Models (LLMs) sunt folosite pentru a genera conținut, acestea pot fi utilizate de către atacatori pentru a crea textele vectorilor phishing, în diferite limbi.

În același timp, specialiștii în securitate folosesc I.A. pentru a îmbunătăți detecția anomaliilor și anticiparea atacurilor, dar această cursă tehnologică antrenează o dinamică complexă între bine și rău în sfera cibernetică.

Lipsa resurselor în rândul companiilor mici

Multe organizații, în special IMM-urile, se confruntă cu o lipsă de resurse financiare pentru a investi în soluții de securitate adecvate. Crizele economice și schimbările de pe piețele globale au pus presiune asupra bugetelor de securitate cibernetică, ceea ce a dus adesea la o abordare reactivă în loc de una proactivă. Aceasta amplifică vulnerabilitățile și riscurile, iar consecințele pot fi devastatoare.

Anul 2024 a fost marcat de câteva incidente remarcabile de securitate cibernetică care au captat atenția mediilor internaționale și au ridicat semne de întrebare asupra capacităților de apărare existente. Cele mai importante dintre aceste incidente sunt prezentate în continuarea raportului BIS, în secțiunea „Incidentele notabile ale anului 2024”.

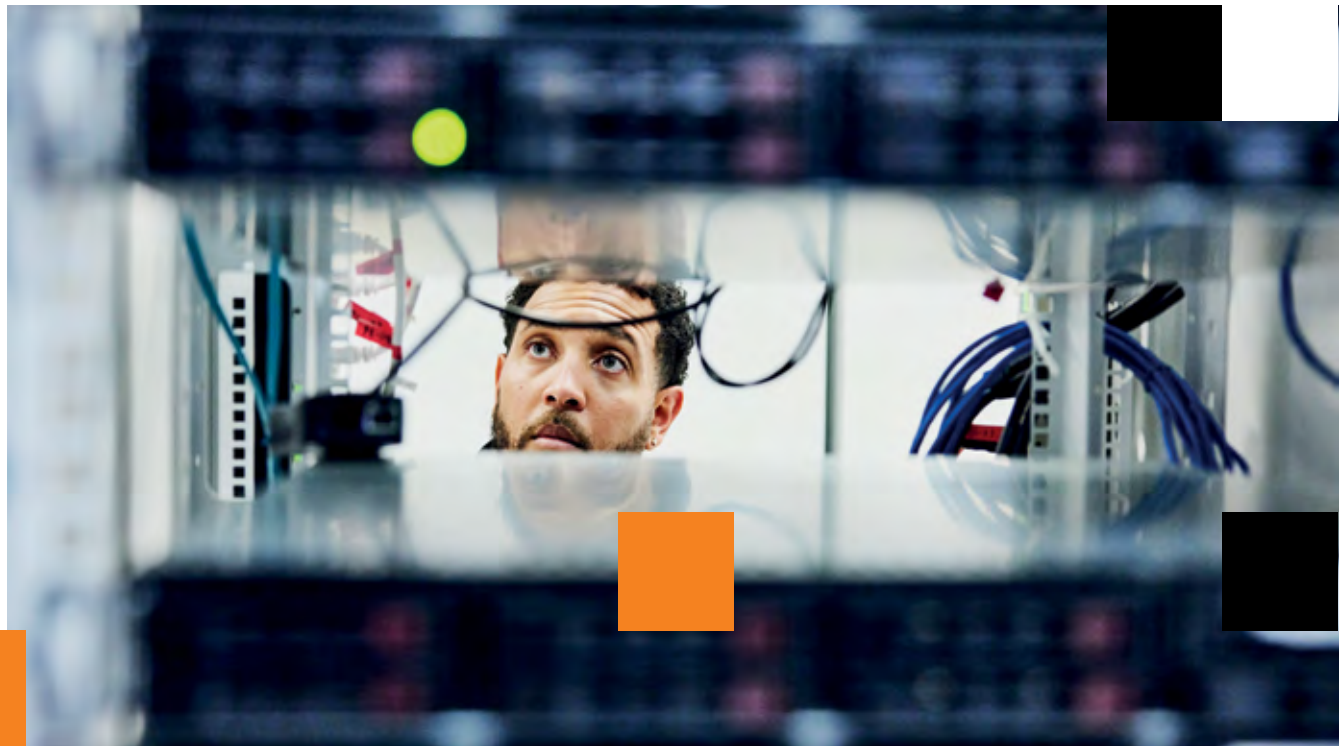
Iar dacă anul 2024 a fost, până la momentul publicării raportului nostru, unul foarte bogat în astfel de incidente, 3 tipologii importante și îngrijorătoare, în același timp, au ținut capetele afișelor:

Atacurile asupra infrastructurilor critice

În anul 2024, lumea s-a confruntat cu o creștere alarmantă a atacurilor cibernetice îndreptate împotriva infrastructurilor critice. Aceste atacuri, orchestrate în principal de grupări de hackeri din Rusia, au pus în pericol nu doar funcționarea normală a serviciilor esențiale, ci și securitatea națională și bunăstarea cetățenilor în întreaga lume. Infrastructurile critice, cum ar fi rețelele electrice, sistemele de apă, comunicațiile și transportul, au devenit ținte prioritare în războiul cibernetic, iar amploarea și sofisticarea acestor atacuri au crescut dramatic.

După invazia din Ucraina din 2022, tensiunile internaționale au crescut, iar Rusia a fost acuzată de utilizarea atacurilor cibernetice ca arme hibride. În 2024, hackeri susținuți de Kremlin au intensificat activitățile lor, atacând statele occidentale ca parte a unei strategii mai ample de destabilizare. Aceste grupări, precum APT29 (Cozy / Fancy Bear), au fost implicate în multiple atacuri care au vizat atât infrastructuri critice, cât și instituții guvernamentale și companii private.

Motivele din spatele acestor atacuri sunt variate. Pe de o parte, se urmărește slăbirea adversarilor politici prin crearea haosului și a instabilității. Pe de altă parte, există și un interes economic, deoarece atacurile pot conduce la furtul de date sensibile și informații comerciale importante. Nu în ultimul rând, aceste acțiuni pot servi ca mijloc de intimidare, demonstrând puterea și abilitățile cibernetice ale Rusiei pe scena internațională.



În 2024, atacurile au variat de la malware și ransomware, la atacuri de tip denial-of-service (DDoS) și phishing avansat. Un incident semnificativ a fost raportat[1] în aprilie, când o rețea de hackeri din Rusia, autointitulată „Sandworm" și ulterior numită de către Mandiant – Google, cu indicativul APT44, a reușit să compromită sistemele informatice ale unor facilități energetice și de tratare a apelor din Ucraina. Prin infiltrarea rețelelor IT și SCADA ale centralei, acești hackeri au provocat întreruperi temporare ale alimentării cu energie electrică, iar efectele s-au resimțit imediat în rândul populației și al industriilor afectate. Hackerii au folosit un backdoor mai puțin cunoscut, numit Kapeka, pentru a instala malware pe dispozitivele de control industrial din aceste facilități.

De asemenea, atacurile ransomware au crescut, cu grupuri care au cerut sume uriașe pentru decriptarea datelor compromise. Un alt incident major a avut loc în timpul verii[2], când un sistem de gestionare a apelor din Arkansas a fost atacat, rezultând oprirea unor automatizări în cadrul facilității. Acest atac a generat panică și a subliniat vulnerabilitatea infrastructurilor critice la atacuri cibernetice.

Consecințele acestor atacuri sunt resimțite la nivelul întregii societăți. Pe lângă disfuncționalitățile și costurile economice imense, atacurile asupra infrastructurilor critice afectează și încrederea cetățenilor în guverne și în capacitatea acestora de a proteja bunăstarea publică. De asemenea, sporește percepția precarității securității cibernetice, subliniind necesitatea urgentă de a investi în tehnologii de apărare cibernetică și în formarea personalului specializat.

În plus, atacurile cibernetice pun presiune asupra relațiilor internaționale. Țările afectate pot răspunde prin sancțiuni economice sau prin măsuri de contracarare, ceea ce ar putea escalada și mai mult tensiunile globale. Colaborarea internațională devine esențială pentru a contracara această amenințare, iar organizațiile internaționale ar trebui să joace un rol activ în promovarea normelor și standardelor de securitate cibernetică.

Atacurile cibernetice din 2024, orchestrate de grupări de hackeri susținute de instituții statale, au demonstrat cât de vulnerabile sunt infrastructurile critice în fața amenințărilor cibernetice. Ca răspuns, este crucial ca statele să colaboreze și să dezvolte strategii de apărare cibernetică care să protejeze bunurile esențiale ale societății. Conștientizarea și educația în domeniul securității cibernetice sunt esențiale pentru prevenirea și mitigarea riscurilor, iar răspunsurile internaționale la aceste provocări vor determina, în cele din urmă, stabilitatea și securitatea globală pe termen lung.

1. https://therecord.media/russian-hackers-target-energy-facilities-ukraine
2 https://industrialcyber.co/utilities-energy-power-water-waste/hackers-target-arkansas-city-water-treatment-plant-prompting-federal-investigation/

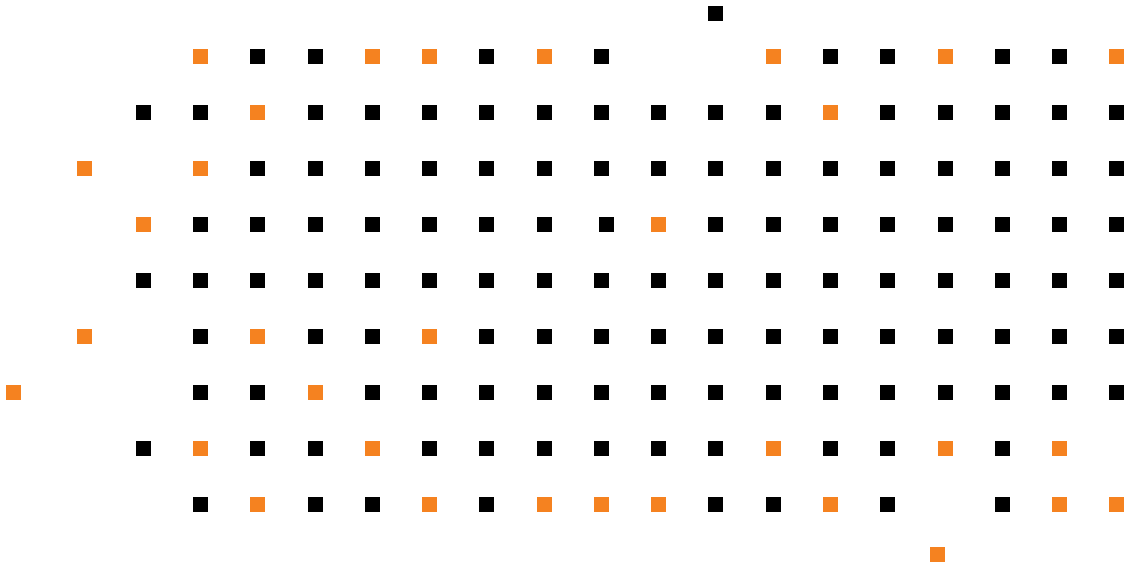
Breșele de date

Ca în anii anteriori, 2024 a adus în prim plan numeroase breșe de date care au fost raportate de către beneficiari. Vedem în 2024 imaginea ultimilor 3-4 ani, cu sisteme de date expuse în internet și insuficient de bine protejate. Leak-urile Elastic au generat breșe[3] de sute de milioane de seturi de date, iar unelte specializate în descoperirea instanțelor Elastic neprotejate, precum ZoomEye, sunt folosite zilnic pentru a raporta astfel de incidente. Migrarea masivă către sisteme cloud, aduce vulnerabilități majore în configurarea acestor platforme pentru procesarea și stocarea datelor, iar breșele majore din anii recenți sunt dovadă a faptului că securitatea mediilor cloud reprezintă un domeniu de îmbunătățire.

Campanii de dezinformare și fake news

În era informațională, campaniile de dezinformare au devenit o formă comună de atac cibernetic. În 2024, au fost lansate diverse campanii care au avut scopul de a influența alegeri politice și de a crea instabilitate socială. Aceste acțiuni au demonstrat că securitatea cibernetică nu se limitează doar la protejarea datelor, ci include și gestionarea informațiilor și a percepțiilor publicului.

Campanii importante de dezinformare au fost create și distribuite prin rețelele de socializare iar specificul anului 2024 este utilizarea I.A. generative pentru a contribui la „credibilitatea” mesajelor. Astfel, fenomenul fake news a căpătat și o dimensiune nouă, aceea a deep fakes, o metodă relativ recentă de manipulare a imaginilor și a înregistrărilor audio-video, folosind mecanisme I.A., pentru a schimba conținutul sau sensul înregistrării inițiale.



3 https://medium.com/@zoomeye_team/urgent-warning-elasticsearch-configuration-vulnerability-leads-to-global-data-leakage-governments-fb44bce18f0f

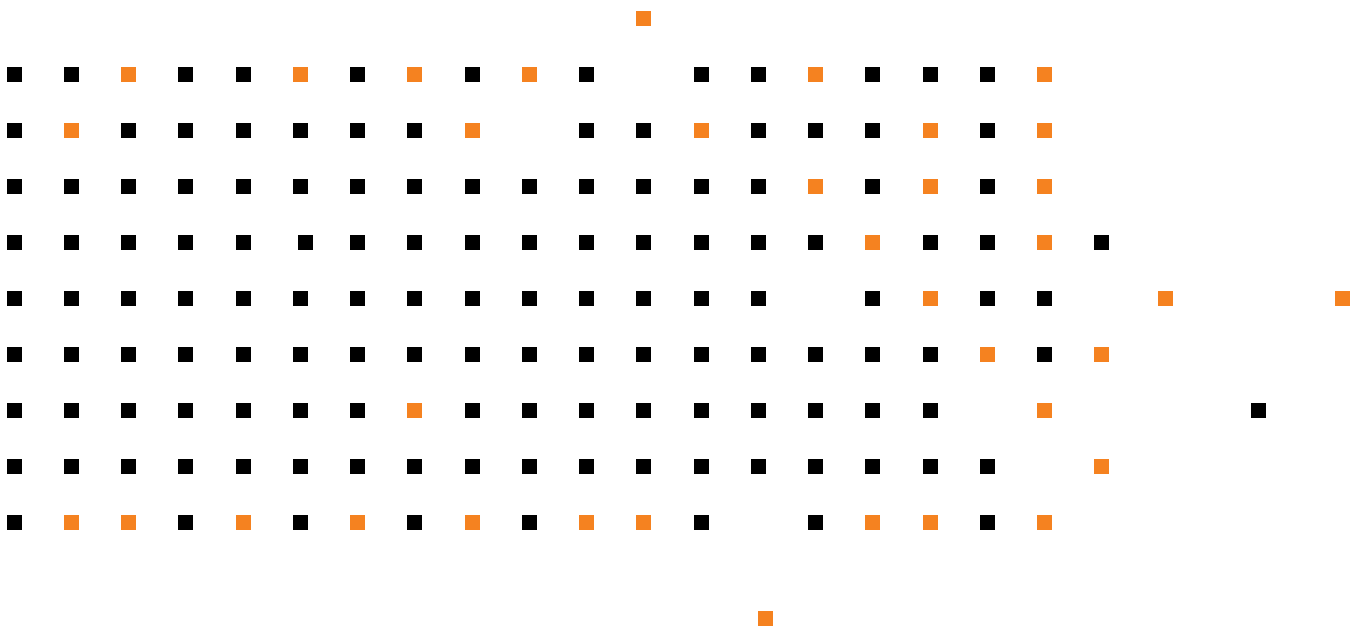
Răspunsul la incidente

În urma acestor incidente, guvernele din întreaga lume au început să implementeze reglementări mai stricte în domeniul securității cibernetice. Uniunea Europeană a adoptat noi directive care impun companiilor să își îmbunătățească protocoalele de securitate și să raporteze rapid incidentele de securitate. Aceste reglementări sunt menite să protejeze datele personale ale cetățenilor și să asigure integritatea infrastructurilor critice.

Investiții în educație și conștientizare

O schimbare semnificativă în 2024 a fost creșterea investițiilor în educația și conștientizarea securității cibernetice. Organizațiile au început să implementeze programe de formare pentru angajați, pentru a atrage atenția asupra riscurilor cibernetice și a modului în care pot contribui la securizarea informațiilor. Această abordare proactivă poate reduce semnificativ numărul incidentelor cauzate de greșelile umane.

Colaborarea internațională
Provocările de securitate cibernetică sunt, prin natura lor, transnaționale, ceea ce a dus la o creștere a colaborării internaționale. Statele au început să împărtășească informații și resurse pentru a combate atacurile cibernetice într-un mod coordonat. Aceste inițiative demonstrează importanța unei reacții unite în fața amenințărilor cibernetice globale.

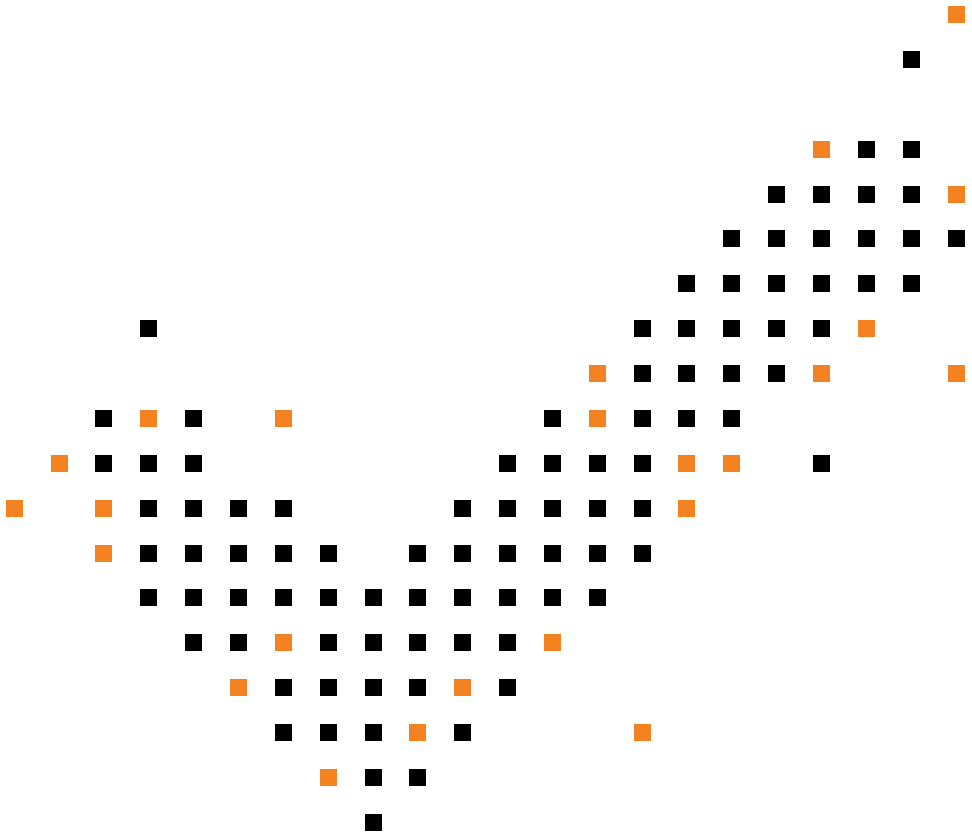


Importanța implementării Directivei NIS2 în Uniunea Europeană

În era digitalizării accelerate, securitatea cibernetică devine o prioritate globală. Uniunea Europeană (UE) a recunoscut această necesitate, iar implementarea Directivei NIS2 reprezintă un pas semnificativ în consolidarea securității cibernetice la nivel european. Directiva NIS2 (Network and Information Systems Directive) este o revizuire a primei directive NIS, adoptată în 2016, și reflectă necesitatea de a răspunde amenințărilor în continuă evoluție din spațiul cibernetic.

Directiva NIS a fost prima reglementare la nivel european care abordează securitatea rețelelor și a sistemelor informaționale. Cu toate că NIS a adus progrese semnificative, a devenit evident că aceasta nu era suficientă pentru a face față amenințărilor contemporane, cum ar fi atacurile cibernetice din partea actorilor statali sau non-statali, ransomware-ul și alte tipuri de amenințări cibernetice. Directiva NIS2, adoptată[4] în decembrie 2020, vizează îmbunătățirea și extinderea cadrului existent de securitate cibernetică, oferind unul mai robust și mai coordonat pentru combaterea amenințărilor cibernetice.

4 https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union



Beneficiile implementării Directivei NIS2

Îmbunătățirea securității cibernetice. Prin definirea unor cerințe mai stricte pentru operatorii de servicii esențiale și furnizorii de servicii digitale, NIS2 contribuie la creșterea nivelului de securitate cibernetică în întreaga Uniune Europeană. De asemenea, include măsuri specifice de prevenire, reacție și raportare a incidentelor cibernetice.

Cooperarea între statele membre. NIS2 încurajează cooperarea mai strânsă între statele membre prin crearea unei rețele de centre de competență în domeniul securității cibernetice. Aceasta facilitează schimbul de informații și colaborarea internațională în combaterea amenințărilor cibernetice.

Responsabilizarea sectorului privat. Directivele NIS2 extind responsabilitatea în domeniul securității cibernetice la o gamă mai largă de entități, inclusiv furnizori de servicii cloud și platforme online. Aceasta înseamnă că nu doar agențiile guvernamentale, ci și sectorul privat trebuie să se alinieze la standarde ridicate de securitate.

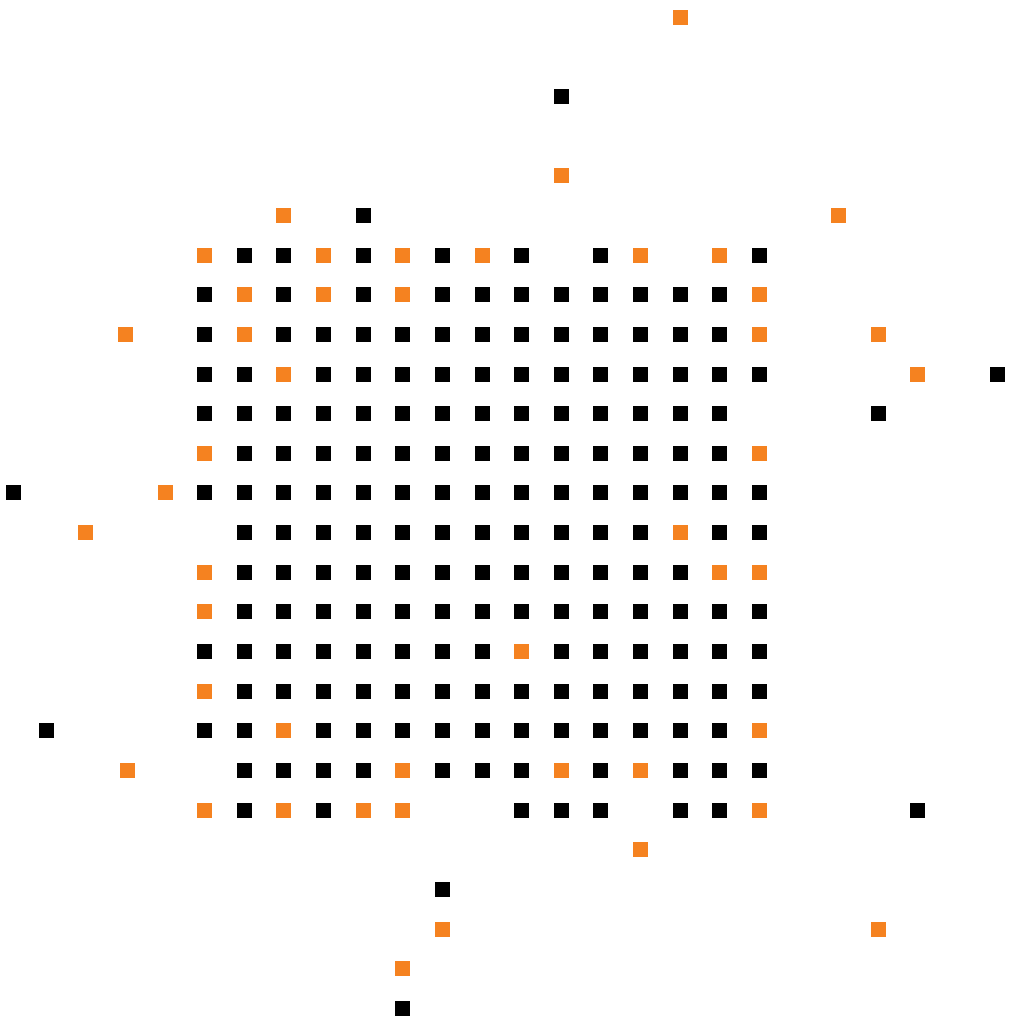
Alinierea la standardele internaționale. Implementarea NIS2 ajută UE să se alinieze la normele internaționale de securitate cibernetică, consolidând astfel poziția sa în arena globală. Aceasta include standarde de protecție a datelor și măsuri împotriva atacurilor cibernetice care sunt din ce în ce mai acceptate la nivel internațional.

Provocările implementării Directivei NIS2

Costurile de conformitate. Multe organizații, în special IMM-urile, ar putea întâmpina dificultăți financiare în implementarea măsurilor de conformitate cu NIS2. Aceasta poate duce la o discrepanță între capacitățile companiilor mari și cele mici, ceea ce ar putea afecta competitivitatea.

Complexitatea reglementărilor. Directiva NIS2 vine cu un set extins de cerințe care pot fi percepute ca fiind complexe. Aceasta poate genera confuzie atât în sectorul public, cât și în cel privat, dificultăți în interpretarea regulamentelor și provocări în formarea personalului în ceea ce privește noile standarde.

Rezistența culturii organizaționale. Implementarea noilor măsuri poate întâlni opoziție din partea angajaților care pot fi reticenți în a adopta noi politici sau tehnologii. Este esențial să se dezvolte o cultură organizațională care să încurajeze securitatea cibernetică ca o responsabilitate comună.



Impactul asupra statelor membre și întreprinderilor

Implementarea Directivei NIS2 va avea un impact semnificativ asupra statelor membre și întreprinderilor din UE. În primul rând, statele vor trebui să investească în capacități mai bune de răspuns la incidentele cibernetice, inclusiv formarea personalului și dezvoltarea infrastructurii tehnologice. În al doilea rând, companiile vor trebui să-și reevalueze strategiile de securitate cibernetică, ceea ce poate duce la crearea unor noi locuri de muncă în sectorul IT și la inovare în dezvoltarea tehnologiilor de securitate.

Pe termen lung, implementarea NIS2 ar putea conduce la creșterea încrederii consumatorilor în serviciile digitale, ceea ce ar putea stimula economia digitală europeană. De asemenea, un mediu cibernetic mai sigur ar putea atrage investiții străine și ar putea îmbunătăți competitivitatea pe plan global a companiilor europene.

Implementarea Directivei NIS2 este esențială pentru securitatea cibernetică în Uniunea Europeană, reprezentând un pas important spre consolidarea rezilienței cibernetice. Deși există provocări semnificative în ceea ce privește conformitatea şi interpretarea reglementărilor, beneficiile posibile sunt enorme. Crearea unui cadru mai robust de securitate cibernetică nu doar că protejează infrastructurile critice și datele cetățenilor, dar contribuie, de asemenea, la construirea unei economii digitale mai sigure și mai competitive. Prin urmare, statele membre și organizațiile din UE trebuie să colaboreze eficient pentru a asigura o implementare de succes a acestei directive cruciale.

Mai multe detalii despre impactul NIS2, precum și perspectiva profesionistă a colegului nostru, Vasile Voicu, despre provocările și oportunitățile aduse odată cu NIS2, în secțiunea „Protejează-ți afacerea. Ce este important să știi despre Directiva NIS2?”

2. Va transforma inteligența artificială securitatea cibernetică a viitorului?

Într-o lume din ce în ce mai digitalizată, securitatea cibernetică a devenit o preocupare fundamentală atât pentru organizații, cât și pentru indivizi. Atacurile cibernetice sunt în continuă creștere, iar metodele prin care infractorii cibernetici își desfășoară activitatea devin din ce în ce mai sofisticate. Inteligența artificială (IA) promite să revoluționeze acest domeniu, oferind soluții inovatoare pentru prevenirea, detectarea și răspunsul la aceste amenințări.

Dar este I.A. un panaceu pentru aceste riscuri și amenințări complexe? În continuare, explorăm modul în care I.A. va transforma securitatea cibernetică în următorii ani, abordând atât avantajele, cât și provocările pe care le aduce această tehnologie.

Evoluția I.A. în atacurile cibernetice

Atacurile cibernetice au evoluat considerabil în ultimele decenii. De la virusuri simple și programe malware, infractorii cibernetici utilizează acum metode mai complexe, cum ar fi phishingul avansat, atacurile de tip ransomware și exploatarea vulnerabilităților zero-day. Acest context face ca organizațiile să fie nevoite să-și întărească măsurile de securitate și să investească în unelte și procese ce oferă capacitatea de a ține pasul cu această evoluție.

Automatizarea culegerii de informații despre vulnerabilități

Un aspect îngrijorător al evoluției atacurilor cibernetice este automatizarea acestora. Infractorii cibernetici folosesc deja I.A. pentru a îmbunătăți eficiența atacurilor, ceea ce face ca organizațiile să fie mai vulnerabile. Un exemplu îl reprezintă automatizarea proceselor de auditare – scanare - în scopul de a descoperi vulnerabilități. Folosirea Machine Learning și a unor loop-uri automatizate, cresc substanțial capacitatea atacatorilor de a descoperi rapid și cu precizie, sisteme expuse și vulnerabile ce pot fi folosite pentru a iniția atacuri cibernetice sau pentru a pivota în infrastructurile compromise.

Crearea de malware

I.A. poate fi utilizată în scop ofensiv pentru a automatiza crearea a noi variante de malware, ce ridică complexitatea și dificultatea detecției. Prin folosirea mecanismelor Machine Learning pentru a analiza comportamentul diferitelor variante existente de malware, precum și a metodelor de detecție și blocare disponibile în uneltele de securitate, atacatorii pot genera variante noi ce pot „păcăli” uneltele de detecție din soluțiile anti-malware curente.

Phishing 2.0

Atacatorii pot folosi I.A. pentru a crea mesaje convingătoare, menite să pară legitime. Unelte Machine Learning pot fi folosite pe seturi de date mari, ce conțin mesaje e-mail, pentru a genera text personalizat, în aparență legitim, menit să convingă utilizatorii că acel e-mail provine de la o sursă de încredere.

Rolul I.A. în securitatea cibernetică

Am aflat cum inteligența artificială poate să creeze un avantaj pentru atacatori, putem trece de partea cealaltă a baricadelor pentru a discuta cum I.A. poate îmbunătăți semnificativ securitatea cibernetică. Tehnologii precum analiza comportamentală, detectarea anomaliilor, automatizarea răspunsului sau optimizarea proceselor de securitate sunt printre cele mai răspândite implementări ale Machine Learning în securitatea operațională.

Analiza comportamentală

I.A. poate analiza comportamentele utilizatorilor și ale sistemelor pentru a identifica activități suspecte. Folosind Machine Learning, algoritmii pot detecta comportamente neobișnuite, alertând administratorii despre posibilele atacuri cibernetice. Această abordare proactivă permite o reacție rapidă și eficientă la amenințări.

Detectarea anomaliilor

Tehnologiile bazate pe I.A. pot fi folosite pentru a analiza volume mari de date, identificând anomalii care ar putea indica o breșă de securitate. Aceste sisteme sunt capabile să învețe comportamente normale și să remarce devierile, ceea ce le facilitează detectarea unor atacuri noi și neașteptate. Un exemplu bun este cel al parcurgerii de către I.A. a unui volum mare de log-uri ale platformelor de rețea, pentru a depista conexiuni VPN inițiate în afara orelor de program sau conexiuni către internet de pe stații de lucru care, altfel, nu ar fi comunicat cu acele destinații.

Automatizarea răspunsului

Răspunsul rapid la incidentele de securitate cibernetică este esențial. I.A. poate automatiza procesele de răspuns, precum izolarea sistemelor compromise sau blocarea accesului utilizatorilor suspecți. Această automatizare nu doar că reduce timpul necesar pentru a răspunde, ci și minimizează impactul incidentului.

Web Application Firewall (WAF)

Sistem de protecție a aplicațiilor web împotriva atacurilor cibernetice

orange.ro/business

orange™ Business

3. Singularizarea,

o nouă filozofie de securitate

Noi abordări în combaterea amenințărilor cibernetice

Mihail Pleșa,
Security Researcher, Orange Services

Moving Target Defense (MTD) reprezintă o strategie inovatoare în domeniul securității cibernetice, care presupune modificarea continuă a suprafeței de atac. Această abordare are ca obiectiv prevenirea atacurilor cibernetice prin crearea unui mediu dinamic și imprevizibil.

Te-ai întrebat vreodată cum reușesc hackerii să pătrundă în sistemele noastre?

În spatele oricărui atac cibernetic se află un plan bine pus la punct, care parcurge mai multe etape. Hai să descoperim împreună aceste etape și să vedem cum putem preveni astfel de amenințări.

1 Etapa de recunoaștere

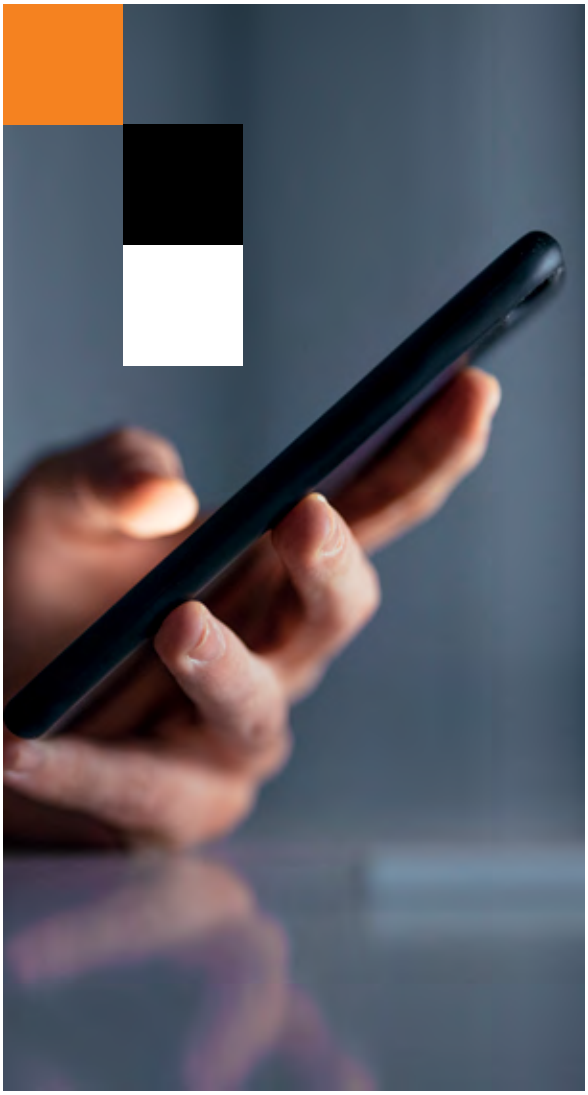
În primul rând, atacatorul trebuie să parcurgă o etapă de recunoaștere, în care colectează informații despre țintă, utilizând tehnici precum scanarea rețelei, căutarea de informații publice și analiza traficului.
Pe baza acestor informații, atacatorul poate identifica vulnerabilitățile și punctele slabe ale sistemului vizat.

2 Exploatarea vulnerabilităților

După ce a obținut informațiile necesare, atacatorul poate încerca să obțină acces la sistem. Un aspect crucial este legătura dintre etapa de recunoaștere și identificarea vulnerabilităților. Atacatorul nu poate identifica vulnerabilități fără informațiile obținute în prima etapă. Cu alte cuvinte, dacă sistemul ar fi într-o schimbare continuă, informațiile colectate în etapa de recunoaștere ar deveni rapid inutile, iar vulnerabilitățile descoperite nu ar mai putea fi exploatate.

Aceasta constituie **esența strategiei Moving Target Defense (MTD)**, care își propune să neutralizeze eficiența atacurilor cibernetice prin menținerea unui **mediu de securitate dinamic și imprevizibil.**

Să luăm ca exemplu aplicația de mesagerie WhatsApp



Mulți dintre noi suntem familiarizați cu faptul că WhatsApp utilizează criptarea integrală (end-to-end encryption). Aceasta înseamnă că, deși mesajul transmis de pe dispozitivul expeditorului trece prin serverul WhatsApp, acesta nu poate fi decriptat decât de către destinatar.

Un aspect mai puțin cunoscut este că WhatsApp beneficiază și de proprietatea de perfect forward secrecy (PFS). PFS garantează că mesajele criptate în trecut nu pot fi decriptate, chiar dacă cheia de criptare curentă este compromisă și cunoscută de către un atacator. Să ne gândim la PFS ca la un seif cu combinație schimbătoare. Chiar dacă cineva află combinația curentă a seifului (cheia de criptare), nu poate deschide seifurile mai vechi, pentru că fiecare mesaj folosește o combinație diferită. Astfel, mesajele anterioare rămân în continuare protejate, chiar dacă cheia curentă este compromisă.

Acest nivel de securitate este posibil datorită unei strategii de tip Moving Target Defense (**MTD**). WhatsApp implementează protocolul Signal, care se bazează pe algoritmul numit double ratchet (DR). Utilizând protocoale criptografice avansate, DR asigură faptul că fiecare mesaj este criptat cu o cheie diferită. Cu alte cuvinte, DR garantează schimbarea continuă a suprafeței de atac cu fiecare mesaj transmis, consolidând astfel securitatea comunicațiilor.

Singularizarea, o nouă filozofie de securitate
În cadrul echipei Orange, cercetăm o nouă filozofie de securitate, numită singularizare. Esența acestei metode este de a face fiecare instanță a unui sistem unică. Această abordare poate avea un impact semnificativ atât asupra securității, cât și asupra eficienței sistemului.

De exemplu, algoritmul de criptare DES. Majoritatea algoritmilor de criptare simetrici au o structură ciclică bazată pe runde: intrarea unei runde este ieșirea rundei precedente (pentru prima rundă, se consideră că intrarea este chiar informația care trebuie criptată). La fiecare rundă, informația este alta.

În acest context, "informația" se consideră un șir de biți. De exemplu, dacă dorim să criptăm textul "Hello", acesta este transformat în șirul de biți 01001000 01100101 01101100 01101100 01101111, prin intermediul unui tabel de coduri numit ASCII.

Procesul de criptare constă în trei mari operații:

1 **Substituția:** are rolul de a adăuga confuzie procesului de criptare. La fiecare rundă a cifrului, șirul de biți de intrare este divizat în grupuri de câte 6 biți. Cu ajutorul unor tabele numite S-boxes, fiecare grup de 6 biți este înlocuit cu un altul de 4 biți.
Există 8 tabele S-boxes: primul tabel transformă primul grup de 6 biți, al doilea tabel transformă următorul grup de 6 biți și așa mai departe. De exemplu, primul tabel S-box mapează grupul de 6 biți 010001 către grupul de 4 biți 1010.

2 **Permutarea:** ajută la amestecarea informației în timpul criptării. Practic, chiar și o mică schimbare în datele de intrare va duce la o schimbare mare în rezultatul final.
Cum funcționează? După ce datele au fost transformate, biții (0 și 1) sunt rearanjați.
De exemplu, bitul de pe poziția 1 este mutat pe poziția 16, iar bitul de pe poziția 16 este mutat pe poziția 10, și așa mai departe, până când toți cei 32 de biți sunt amestecați.
De asemenea, folosim 8 tabele numite S-boxes, iar fiecare tabel generează 4 biți. Așa că, în urma acestei etape de amestecare, obținem un total de 32 de biți.

3 **Adăugarea cheii de rundă:** cu toate că prin substituție și permutare biții de intrare ai unei runde au fost modificați și rearanjați, nu putem considera cele două operații suficiente pentru a spune că informația este protejată (confidențială). Acest lucru se întâmplă deoarece atât tabelele S-box, cât și permutarea sunt publice: oricine le poate găsi în specificațiile algoritmului.

Pentru a ne asigura că datele rămân secrete, avem nevoie de o cheie specială pentru criptare. La fiecare etapă de criptare, algoritmul DES folosește o cheie secretă diferită, formată din 48 de biți.

Cum funcționează? Biții de la intrarea în rundă se combină cu biții din cheia secretă printr-o operație simplă numită „adunare modulo 2” (sau XOR). De exemplu, dacă avem 0111 ca biți de intrare și cheia este 1100, rezultatul va fi 1011. Această combinare ajută la protejarea informației.

În algoritmul DES, procesul de criptare se repetă de 16 ori. Stabilirea numărului exact de repetiții este adesea complicată, deoarece nu există o regulă matematică clară pentru acest lucru.

Decizia privind câte runde să fie folosite depinde de tipurile de atacuri pe care algoritmul le poate întâlni, unul dintre ele fiind atacul de criptanaliză diferențială. Nu vom intra în detalii, **însă am cercetat dacă un concept numit singularizare poate ajuta la protejarea împotriva acestui tip de atac.**

Ideea din spatele singularizării este că fiecare instanță a algoritmului de criptare ar trebui să fie diferită. Aici, provocarea este să găsim ce poate face fiecare versiune a algoritmului DES unică.
De exemplu, tabelele S-box, permutația și structura criptării au fost stabilite cu mare atenție de cei care au creat algoritmul. Orice schimbare în aceste elemente necesită o nouă analiză de securitate, lucru care poate dura mult timp.

Analizând cum funcționează algoritmul, am propus o modificare în modul în care adăugăm cheia.
În loc să folosim aceeași metodă simplă de adunare pentru fiecare rundă, am decis să folosim diferite metode de adunare (modulo 2, 4, 8 sau 16), în funcție de cheia pe care o folosim.
De exemplu, dacă avem biții 0111 și cheia 1100, folosind adunarea modulo 16, rezultatul ar fi 0011.
Această abordare nu afectează securitatea criptării.

În urma cercetărilor noastre, am descoperit că această metodă poate ajuta la protejarea împotriva atacurilor de criptanaliză diferențială, fără a slăbi algoritmul. Acest lucru ar putea însemna că putem folosi un număr mai mic de runde, ceea ce face algoritmul mai eficient.

Deși DES nu mai este folosit în prezent din cauza simplității sale, a fost un punct de plecare important pentru cercetările noastre. Suntem la începutul căutărilor și există multe întrebări despre cum poate funcționa singularizarea. Rezultatele pozitive pe care le-am obținut ne motivează să continuăm.

O direcție viitoare de cercetare este cum singularizarea poate îmbunătăți algoritmii de criptare moderni, cum ar fi AES. În cazul aplicațiilor web, AES funcționează bine, dar în ceea ce privește dispozitivele IoT, eficiența criptării devine crucială pentru consumul de energie și performanța generală.

O altă direcție de cercetare este dacă singularizarea poate ajuta la prevenirea atacurilor de tip side-channel, care sunt importante, în special pentru dispozitivele IoT. De asemenea, ne întrebăm dacă singularizarea poate fi folosită ca bază pentru protocoale criptografice mai complexe, cum ar fi cele care permit analiza datelor criptate.

Există încă multe întrebări fără răspuns despre singularizare și despre cum această nouă filozofie poate influența securitatea cibernetică. Acum este un moment favorabil pentru cercetare, oferind oportunități unice de a explora și de a contribui într-un domeniu care evoluează constant.

4.
Cum evoluează atacurile DDoS?

Top tendințe și măsuri de prevenție

Sorin Nicolae,
Senior OSS & Automation Engineer, Orange Services

Imaginează-ți că deții un magazin foarte popular, iar în fiecare zi, mii de clienți vin să îți cumpere produsele. Totul merge bine până într-o zi când, dintr-odată, magazinul este blocat. Nu mai poate fi accesat de către noi clienți, site-ul de comenzi nu mai funcționează și telefoanele sună fără oprire.

Motivul? Un grup de indivizi trimit un val uriaș de vizitatori falși care inundă magazinul, ocupând toate locurile disponibile și blocând accesul clienților reali.

Acesta este un atac de tip DDoS sau Distributed Denial of Service.

În lumea virtuală, un atac DDoS funcționează la fel. Un număr masiv de cereri false sunt trimise către site-ul unei companii, serverul acesteia sau chiar aplicațiile sale online. În loc să fie accesat de clienții reali, sistemul este suprasolicitat de aceste cereri malițioase și devine incapabil să funcționeze corect, provocând blocaje sau chiar căderi complete. Aceasta poate afecta orice companie, de la micile afaceri până la marile corporații, provocând pierderi de venituri și deteriorând reputația.

De ce este important să înțelegi și să monitorizezi aceste atacuri?

Identificarea tiparelor de atac

Pentru a îți proteja magazinul (fie el real sau virtual), trebuie să fii mereu cu ochii pe ușă. Monitorizarea activităților neobișnuite te ajută să identifici din timp, potențialii intruși. În termeni tehnici, asta înseamnă că firmele monitorizează constant atacurile DDoS pentru a recunoaște care sunt tipurile cele mai frecvente. Fie că este vorba de atacuri care inundă rețelele cu trafic sau care țintesc aplicațiile web.

Îmbunătățirea pregătirii și a rezilienței

Într-un magazin, dacă știi că e o perioadă aglomerată, vei aduce mai mult personal și vei pregăti măsuri de urgență. La fel și în spațiul digital, companiile care sunt conștiente de amenințările DDoS își actualizează continuu protecțiile. Acestea folosesc tehnologii avansate precum firewall-urile pentru aplicații web (WAF) și soluțiile de protecție DDoS. Asta le permite să detecteze rapid atacurile și să reacționeze prompt.

Reducerea riscurilor și limitarea impactului

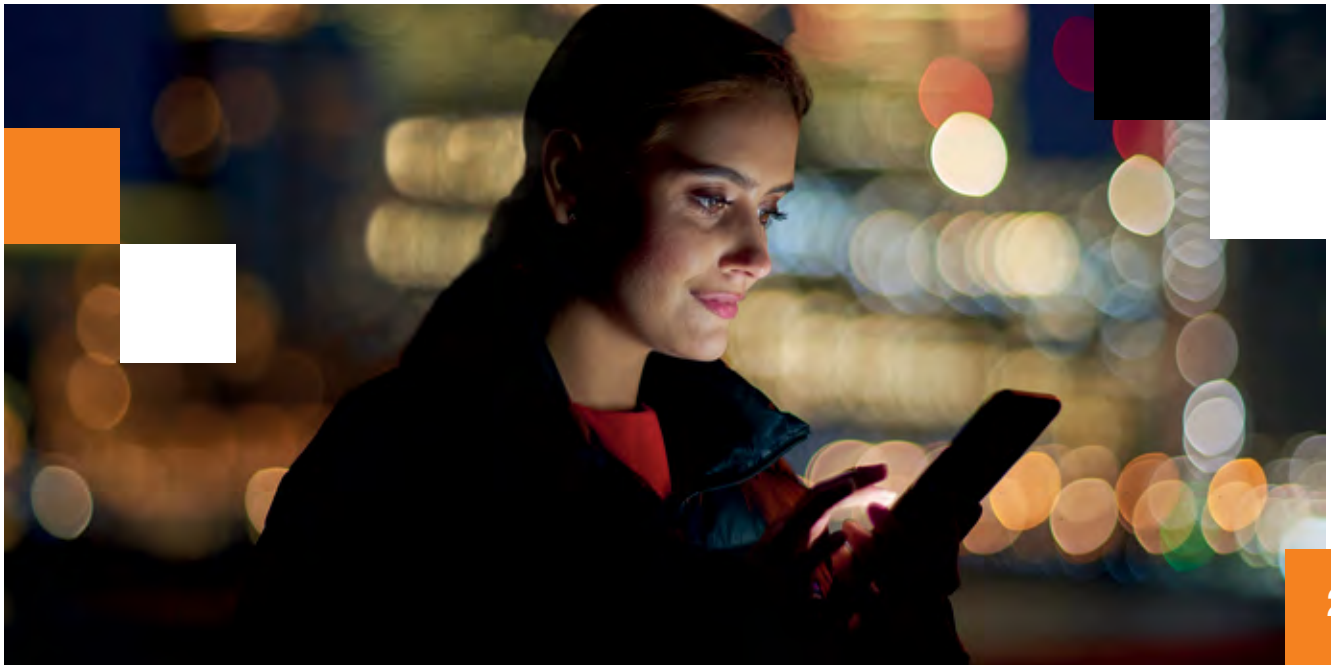
Dacă te pregătești din timp pentru astfel de atacuri, poți minimiza pagubele. În cazul unui magazin fizic, poate vei separa fluxul clienților în mai multe zone pentru a evita aglomerația. În lumea digitală, asta înseamnă segmentarea rețelei sau utilizarea caching-ului pentru a diminua efectele unui atac DDoS. În acest fel, infrastructura esențială rămâne protejată, iar afacerea poate continua fără întreruperi majore.

Reacția rapidă în caz de incident

Dacă atacul totuși reușește, cu un plan de urgență bine pus la punct, poți salva situația. E ca și cum ai avea un al doilea magazin pregătit să preia clienții sau un sistem de redirecționare care să rezolve rapid blocajele. Pentru companiile digitale, asta înseamnă să aibă soluții de backup și redirecționare a traficului pentru a limita cât mai mult daunele.

Numărul atacurilor DDoS în prima jumătate a anului 2024 a crescut cu 46% comparativ cu aceeași perioadă a anului trecut, ajungând la 445.000 în a doua jumătate a anului 2024. Pe baza datelor actuale colectate, se preconizează o tendință similară și pentru 2025.

Această creștere alarmantă a atacurilor de tip **Distributed Denial of Service (DDoS)** indică nu doar o intensificare a frecvenței atacurilor, ci și o evoluție a tacticilor utilizate de infractorii cibernetici. Creșterea cu 46% în doar un an sugerează o schimbare semnificativă în peisajul amenințărilor cibernetice globale, pe care atât companiile, cât și organizațiile guvernamentale trebuie să o abordeze cu maximă seriozitate.



Care sunt factorii care au dus la creșterea numărului de atacuri?

Accesul facil la instrumente de atac DDoS

Imaginează-ți că cineva vrea să perturbe activitatea unui magazin online, dar nu are cunoștințele tehnice necesare. Ei bine, pe dark web, există acum servicii și kit-uri de atac „DDoS for hire”, care fac totul mai simplu. La fel cum ai putea închiria un serviciu online pentru alt tip de sarcină, acești infractori cibernetici pot lansa atacuri fără prea mult efort și la costuri reduse, fără să fie nevoie să fie experți în tehnologie.

Extinderea dispozitivelor IoT nesecurizate

Tot mai multe case și afaceri folosesc dispozitive inteligente conectate la internet: de la frigidere și camere de supraveghere, până la termostate și becuri. Problema este că multe dintre aceste dispozitive nu sunt bine securizate, ceea ce le face ținte ușoare pentru hackeri. Odată compromise, aceste dispozitive devin parte dintr-o „armată” de dispozitive (numită botnet) folosite pentru a lansa atacuri DDoS masive.

Complexitatea crescută a atacurilor

În trecut, un atac DDoS se rezuma adesea la suprasolicitarea unei rețele prin trimiterea unui volum mare de trafic. Astăzi, atacatorii folosesc metode mult mai sofisticate. Așa numitele atacuri **multivectoriale** combină diferite tehnici – atacuri volumetrice, la nivel de protocol sau la nivel de aplicație – ceea ce le face mult mai greu de detectat și de blocat.

Instabilitatea geopolitică și războaiele cibernetice

Într-un context global tot mai tensionat, atacurile DDoS au devenit o armă în războaiele moderne. Guverne și grupuri non-statale folosesc aceste atacuri pentru a viza infrastructuri critice cum ar fi bănci, guverne sau platforme media, cu scopul de a destabiliza țări sau de a afecta operațiunile economice ale unor concurenți.

Impactul atacurilor DDoS asupra diferitelor industrii. Nivele rețea vs. aplicație

Atacurile la nivel de rețea (L3–4) au afectat în principal industriile de gaming, tehnologie și telecomunicații din cauza importanței serviciilor lor de date în timp real. Aceste sectoare, în special gamingul și pariurile online, sunt ținte majore datorită cerințelor ridicate de interacțiune și angajament al utilizatorilor.

În schimb, atacurile la nivel de aplicație (L7) au influențat puternic sectoare precum serviciile financiare, e-commerce-ul și media, perturbând procesele de tranzacționare și livrarea de conținut. În cazul furnizorilor de tehnologie, atacurile pot afecta simultan mai mulți clienți, iar companiile telecom riscă întreruperi majore, afectând utilizatorii și afacerile.

Top 3 industrii vizate de atacuri la nivel de rețea

Gaming	47%
Tehnologie	33%
Telecomunicații	20%

Top 3 industrii vizate de atacuri la nivel de aplicație

Finanțe	41%
Media & Entertainment	31%
E-Commerce	28%

În vederea anticipării unei **creșteri continue a numărului de atacuri DDoS în 2025**, este important să iei măsuri proactive pentru a proteja infrastructura afacerii tale:

Monitorizarea continuă și în timp real a traficului
Gândește-te la monitorizarea traficului de date ca la un sistem de alarmă de securitate. Soluțiile avansate de monitorizare a rețelei permit detectarea rapidă a anomaliilor, semnale timpurii ale unui posibil atac DDoS. Cu o supraveghere continuă, companiile pot reacționa imediat la orice activitate suspectă, intervenind înainte ca atacul să producă daune semnificative. Astfel, **prevenirea** devine primul pas crucial în apărarea împotriva atacurilor cibernetice.

Investiția în soluții de protecție volumetrică
Pentru a face față atacurilor de mare amploare, multe companii mari aleg soluții de mitigare DDoS bazate pe „curățarea" traficului la nivelul furnizorului de internet. Aceasta este o soluție eficientă, deoarece furnizorii de servicii internet pot gestiona volume mari de trafic, protejând astfel infrastructura internă a companiei de suprasolicitare. Este ca și cum ai muta traficul într-o mare uriașă, unde valurile sunt disipate înainte de a ajunge la tine.

Planuri de continuitate a afacerii și recuperare în caz de dezastru
Fiecare organizație ar trebui să fie pregătită pentru cel mai rău scenariu. Asta înseamnă să aibă un plan bine definit de recuperare după un atac DDoS. Aceste planuri includ **backup-uri redundante**, astfel încât datele esențiale să fie salvate și restaurate rapid. De asemenea, procedurile de redirecționare a traficului către servere alternative sunt esențiale pentru a menține funcționarea serviciilor, chiar și în timpul unui atac masiv.

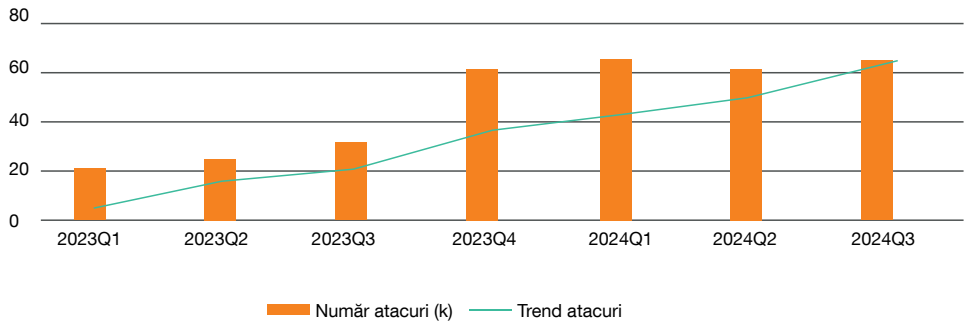
Educația și formarea angajaților
Angajații sunt adesea punctul cel mai vulnerabil în securitatea unei companii. De aceea, instruirea acestora este esențială. Educația despre bunele practici de securitate, precum recunoașterea semnalelor timpurii ale unui atac sau identificarea activităților suspecte, poate preveni infiltrările neintenționate. Un personal bine pregătit poate răspunde mai rapid și mai eficient la un posibil atac, limitând astfel pagubele.

Tendințele atacurilor DDoS în România

Atacurile DDoS din România au înregistrat o creștere constantă în perioada Q3 2023 – Q2 2024, conform datelor disponibile. Deși magnitudinea acestora a variat de la un trimestru la altul, numărul total de atacuri a continuat să crească, reflectând o intensificare a activităților cibernetice rău intenționate. Sectoarele cele mai vizate au fost cel financiar, telecomunicațiile și serviciile online.

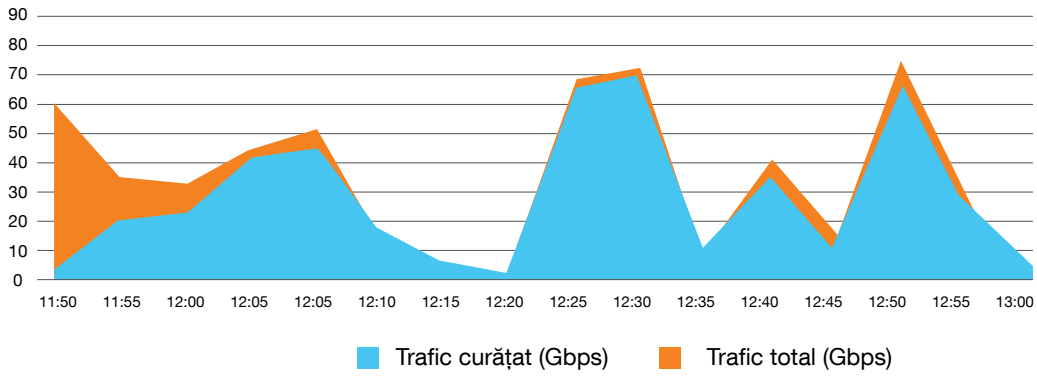
Trimestru	Număr atacuri (mii)	Volum maxim atacuri (Gbps)	Viteză maximă atacuri (Mpps)	Durată maximă atacuri (zile)
Q3 2023	30.5	129	26.5	6
Q4 2023	67.2	196	60.8	7
Q1 2024	63.3	177	63.1	6
Q2 2024	63.3	251	49.3	7

Creșterea numărului de atacuri DDos în România



Un exemplu notabil a avut loc în 2024, când Orange a atenuat cu succes cel mai mare atac DDoS observat până acum asupra sectorului bancar din România. Acest atac a avut o magnitudine de 73.6 Gbps și a durat aproximativ 1 oră. Incidentul a demonstrat importanța investițiilor în soluții avansate de protecție și atenuare a atacurilor DDoS pentru a asigura continuitatea activităților critice în mediul digital.

Alertă client din sectorul bancar



Creșterea constantă a atacurilor DDoS, atât la nivel global, cât și în România, evidențiază **necesitatea urgentă de îmbunătățire a strategiilor de apărare cibernetică la nivelul fiecărei afaceri.** Atacurile la nivel de rețea și la nivel de aplicație continuă să afecteze diverse industrii, de la gaming și telecomunicații până la sectorul financiar și e-commerce.

Totodată, monitorizarea atentă a tendințelor DDoS este esențială pentru a anticipa amenințările și a implementa măsuri proactive care să asigure stabilitatea operațională și protecția infrastructurilor critice.

Așadar, în această epocă modernă a tehnologiei, să fii pregătit pentru un atac DDoS, e ca și cum ai avea mereu o umbrelă la tine. Poate nu plouă chiar acum, dar când o va face, vei fi tare bucuros că ești protejat!

5.

Protejează-ți afacerea. Ce este important să știi despre Directiva NIS2?

Vasile Voicu,
Delivery Services Manager, Orange România

Totul este bazat pe **trei piloni esențiali**, construiți inițial în cadrul NIS1:

1. Extinderea implementării măsurilor de securitate cibernetică de la nivelul Operatorilor de Servicii Esențiale (OSE) la:

   - Sectoare cu o **importanță critică ridicată:** energie; transport; bancar; infrastructuri ale pieței financiare; sănătate; apă; infrastructură digitală (furnizori de servicii DNS; TLD; furnizori de rețele publice de comunicații electronice; managementul serviciilor ICT).

   - **Alte sectoare cu importanță critică:** servicii poștale și de curierat; managementul deșeurilor; chimicale; alimente; fabricarea de dispozitive medicale, calculatoare și electronice, mașini și echipamente, autovehicule și alte echipamente de transport; furnizori digitali (motoare de căutare online și platforme de servicii de rețele sociale) și institute de cercetare.

2. Nivelul ridicat de pregătire pentru statele membre prin realizarea strategiei naționale pentru securitate cibernetică și înființarea CSIRT (Company Security Incident Response Team). Directiva NIS2 conține prevederi referitoare la supravegherea strictă din partea UE.

3. Cooperarea strategică între statele membre UE în domeniul securității cibernetice. NIS2 introduce noi mecanisme de raportare și partajare a informațiilor.

Directiva NIS2 stabilește câteva cerințe esențiale care ajută organizațiile să devină mai sigure și mai pregătite pentru a face față provocărilor cibernetice.

Iată cum arată aceste cerințe, împărțite în cinci arii importante:

1. **Guvernanță:** este necesar ca fiecare organizație să creeze și să implementeze politici clare de securitate. Managementul trebuie să fie implicat activ, luând măsuri pentru identificarea și gestionarea riscurilor și vulnerabilităților, pentru a asigura o protecție adecvată a informațiilor.

2. **Protecție:** organizațiile trebuie să protejeze securitatea rețelelor și a sistemelor informatice, dar și siguranța fizică a personalului. Totul include și întreținerea sistemelor și controlul accesului la resursele digitale.

3. **Apărare cibernetică:** securitatea digitală presupune detectarea și gestionarea incidentelor care pot afecta siguranța rețelelor și a sistemelor informatice. Este important ca organizațiile să aibă procese clare pentru a identifica rapid aceste incidente și a răspunde prompt.

4. **Reziliență:** continuitatea serviciilor esențiale trebuie să fie prioritară. Directiva subliniază importanța unei bune gestionări a situațiilor de criză, în special a incidentelor majore care pot afecta funcționarea serviciilor critice.

5. **Raportare:** pentru a proteja organizația și clienții săi, orice incident semnificativ trebuie raportat rapid către CSIRT sau autoritatea competentă.

Pe lângă aceste cerințe, NIS2 solicită utilizarea soluțiilor de securitate cibernetică certificate, conforme cu standardele europene. Pentru a îndeplini aceste cerințe, este important ca organizațiile să fie proactive, să identifice și să adreseze vulnerabilitățile din sistemele lor IT/OT și să se asigure că echipele lor au cunoștințele necesare pentru a menține o infrastructură IT sigură.

Dacă organizația din care faci parte intră sub incidența NIS2, află că trebuie luate aceste măsuri esențiale:

- **Planuri și politici de securitate** - este important ca fiecare organizație să aibă un plan clar de securitate cibernetică care să asigure furnizarea sigură a serviciilor. Acest plan ar trebui să includă obiectivele strategice de securitate, guvernanța și politicile necesare, cum ar fi securitatea prin criptare, auditul, întreținerea și gestionarea incidentelor de securitate.

- **Instruirea angajaților** - oamenii sunt cheia unei securități eficiente, așa că organizațiile trebuie să ofere instruire constantă pentru toți utilizatorii de rețele și sisteme informatice. În acest fel, toți angajații sunt la curent cu amenințările cibernetice și știu cum să reacționeze în fața riscurilor.

- **Gestionarea activelor** - stabilește un cadru adecvat pentru identificarea, clasificarea și implementarea unui inventar al proceselor IT, sistemelor și elementelor componente ale rețelelor și sistemelor informatice. În baza gestionării activelor, se lansează actualizări și patch-uri, iar organizația stabilește ce elemente din componența rețelelor și sistemelor informatice sunt afectate de noi probleme de securitate.

Organizația elaborează o procedură pentru etichetarea și clasificarea datelor și informațiilor pentru a reflecta sensibilitatea acestora și se asigură că aceasta este respectată, iar datele/informațiile sunt gestionate corespunzător.

- **Cartografierea ecosistemului** - identifică părțile interesate, inclusiv furnizorii care au acces la activele critice ale operatorului. Acest proces este materializat printr-o situație cartografică a ecosistemului, având ca scop identificarea și evaluarea riscurilor potențiale reprezentate de relațiile cu părțile interesate ale ecosistemului. Se realizează prin identificarea unei liste a riscurilor potențiale și evaluarea efectului acestora asupra furnizării serviciilor esențiale.

- **Managementul arhitecturii** - organizația trebuie să dezvolte și să actualizeze constant schema arhitecturii rețelelor și sistemelor informatice, asigurând că instalarea echipamentelor și serviciilor este esențială pentru funcționarea și securitatea acestora.

Pentru managementul suporturilor de memorie externă, organizația trebuie să adopte o procedură privind utilizarea acestora, inclusiv principii și măsuri de securitate. Suporturile de scris detașabile conectate la rețelele și sistemele informatice, trebuie utilizate exclusiv pentru operațiuni legate de furnizarea serviciului esențial și/sau funcționarea rețelelor și sistemelor informatice.

- În vederea limitării propagării incidentelor de securitate cibernetică, organizația aplică o procedură privind **segregarea și segmentarea** rețelei informatice. Acest lucru înseamnă că separă fizic sau logic rețelele și sistemele informatice de alte sisteme informatice proprii sau de la terți. Interconectările dintre rețele și sisteme trebuie să aibă măsuri de securitate adecvate.

- **Filtrarea traficului** - este necesară pentru a proteja rețelele și sistemele informatice împotriva atacurilor cibernetice. Organizația definește, implementează și actualizează permanent procedurile de filtrare a traficului, stabilind reguli pentru restricționarea fluxurilor de trafic, care nu sunt necesare pentru funcționarea rețelelor și sistemelor informatice și care ar putea facilita un atac cibernetic.

- Organizația va stabili **măsuri de protecție** împotriva **atacurilor malware** și va implementa mijloace de control pentru detecția, prevenirea și recuperarea informației în scopul protecției împotriva atacurilor malware. Echipamentele hardware, sistemele de operare, aplicațiile software și subsistemele rețelelor și sistemelor informatice trebuie configurate și protejate corespunzător atât împotriva atacurilor fizice, cât și logice.

- **Administrarea conturilor** - organizația stabilește conturi de administrare destinate exclusiv persoanelor responsabile pentru administrarea și întreținerea sistemelor și rețelelor informatice. Aceste conturi de administrator sunt individualizate și restricționate la perimetrul funcțional și tehnic al fiecărui administrator, astfel încât fiecare administrator să aibă permisiuni individualizate.

- **Administrarea rețelelor și sistemelor informatice** - se realizează în conformitate cu o procedură pentru utilizarea sistemelor de administrare, care trebuie să respecte anumite reguli. Aceste reguli includ utilizarea exclusivă a resurselor hardware și software ale sistemelor informatice pentru operațiuni de administrare a rețelelor și sistemelor informatice.

- **Managementul identificării și autentificării utilizatorilor** - organizația stabilește și menține evidența conturilor unice pentru utilizatorii și procesele automate care accesează resursele rețelelor și sistemelor informatice, dezactivează conturile neutilizate și revizuiește periodic evidența acestora. Pentru procesele critice, organizația va stabili un mecanism de autentificare în cel puțin doi pași și va schimba datele de autentificare implicite, înainte ca o resursă să intre în funcțiune.

- **Managementul drepturilor de acces** - organizația acordă drepturi doar atunci când sunt strict necesare pentru utilizator sau procesul automatizat, pentru îndeplinirea atribuțiilor acestora. În procesul de acordare a drepturilor de acces, se aplică principiul necesității de a cunoaște și principiul celui mai mic privilegiu.

- **Mentenanța rețelelor și sistemelor informatice** - organizația trebuie să elaboreze și să implementeze o procedură pentru menținerea securității rețelelor și sistemelor informatice, care descrie politica de instalare a oricărei noi versiuni sau măsuri corective pentru o resursă desemnată. Totodată obligă informarea cu privire la vulnerabilități și măsuri corective de securitate, care privesc resursele rețelelor informatice.

- **Managementul securității fizice** - organizația previne accesul fizic neautorizat, deteriorarea și interferența informațiilor organizației și locațiile în care se procesează informațiile. În acest sens, organizația elaborează și aplică o procedură privind accesul și securitatea resurselor și informațiilor.

- **Managementul vulnerabilităților și alertelor de securitate** - are la bază elaborarea, actualizarea și implementarea unei proceduri pentru detectarea alertelor și incidentelor de securitate, care afectează rețelele și sistemele informatice. De asemenea, organizația dezvoltă un proces de identificare, clasificare, remediere și eliminare a vulnerabilităților, în special în software și firmware. Pentru limitarea riscurilor de securitate se va implementa un program pentru managementul vulnerabilităților, care poate include instalarea unui patch, reconfigurarea unui software și educarea utilizatorilor.

- **Înregistrarea evenimentelor** - se implementează un sistem de înregistrare a evenimentelor la nivelul rețelelor și sistemelor informatice, inclusiv evenimente legate de autentificare utilizatorilor, gestionarea drepturilor de acces, accesul la resurse, modificările regulilor NIS și funcționarea rețelelor și sistemelor informatice.

Se realizează detectarea incidentelor de securitate prin colectarea datelor de înregistrare, marcarea evenimentelor înregistrate cu ajutorul surselor de timp sincronizate, centralizate și arhivarea acestora pentru o perioadă de cel puțin șase luni. Formatul de arhivare a evenimentelor permite cercetarea automată a acestora.

- Pentru apărarea cibernetică a securității rețelelor și sistemelor informatice, organizația dezvoltă și implementează un SIEM (Security Information and Event Management), care oferă **jurnalizarea și asigurarea trasabilității** activităților în cadrul rețelelor și sistemelor informatice.

- **Răspuns la incidente de securitate** - fluxul incidentelor constă în crearea, actualizarea și implementarea unei proceduri pentru gestionarea, răspunsul și analiza incidentelor care afectează funcționarea sau securitatea rețelelor și sistemelor informatice.

- Organizația trebuie să implementeze un **sistem de monitorizare și management al evenimentelor și incidentelor de securitate,** bazat cel puțin pe un senzor de detectare a intruziunilor la nivel de rețea. Acesta beneficiază de o sursă constantă de indicatori de compromitere și analizează logurile echipamentelor critice pentru a identifica abaterile de la politicile de securitate și intruziunile.

- **Comunicarea incidentelor** - organizația se interconectează la serviciul de alertare și cooperare al DNSC care îi permite să ia notă, fără întârziere, de informațiile transmise de DNSC, ca CSIRT Național, cu privire la incidente, vulnerabilități, amenințări și informări relevante.

Următoarele etape ale acestui proces sunt:

- Elaborarea și implementarea unei proceduri de interconectare la serviciul de alertare și cooperare al DNSC.

- Monitorizarea permanentă a alertelor și solicitărilor primite, prin acest serviciu sau prin celelalte modalități de contact.

NIS2 va impune penalități financiare pentru organizațiile care nu vor fi conforme cu cerințele în intervalul de timp specificat în legea de aplicare. Controalele vor fi strict tehnice, în scopul validării securității informatice a operațiunilor organizațiilor.

Vor fi pasibili de sancțiuni managerii executivi ai organizațiilor care nu se vor conforma cerințelor directivei NIS2. Implementarea politicilor, procedurilor și soluțiilor menționate în acest articol va facilita managementul riscului IT și OT și va conduce la respectarea reglementărilor directivei NIS2.

6. Ransomware în 2024 Reușim să ținem pasul?

Ransomware-ul a devenit una dintre cele mai acute probleme de securitate cibernetică în ultimii ani, iar în 2024, situația nu este decât o continuare a acestei tendințe alarmante. Această formă de malware criptează datele utilizatorilor sau organizațiilor, solicitând o recompensă, de cele mai multe ori în criptomonede, pentru a le debloca. Prevalența ransomware-ului în 2024, tacticile evoluate folosite de atacatori, impactul asupra organizațiilor și măsurile de prevenire și răspuns pe care acestea le pot implementa sunt subiecte de interes pentru majoritatea organizațiilor, iar conștientizarea riscurilor ransomware, în rândul angajaților reprezintă, în continuare, una dintre cele mai eficiente metode de limitare a impactului acestor atacuri.

Evoluția ransomware-ului

Creșterea numărului de atacuri

În 2024, atacurile de tip ransomware au crescut exponențial, având în vedere că din ce în ce mai multe organizații au ales să își desfășoare activitățile într-un mediu digital. În special, companiile mici și mijlocii sunt vizate, întrucât multe dintre acestea nu dispun de resursele necesare pentru a implementa măsuri de securitate eficiente. Contextul politic și social încărcat, în special în Europa și SUA, au contribuit din plin la avalanșa de atacuri ransomware, unele notabile, precum și la tipurile de malware folosit.

Ransomware-as-a-Service (RaaS). O tendință notabilă în infracționalitatea cibernetică este emergența modelului Ransomware-as-a-Service, care permite chiar și infractorilor cu abilități tehnice limitate să declanșeze atacuri. Aceasta a dus la o democratizare a ransomware-ului, facilitând accesul la instrumente avansate pentru o gamă largă de atacatori.

Ransomware as a Service (RaaS) a devenit un model de afaceri din ce în ce mai popular printre criminalii cibernetici, transformând ransomware-ul dintr-o amenințare singulară într-o industrie bine organizată. Ransomware as a Service este un model în care atacatorii cibernetici oferă software-ul de ransomware și infrastructura necesară pentru a efectua atacuri în schimbul unei părți din răscumpărarea obținută. Acest model permite chiar și celor fără cunoștințe tehnice avansate să devină atacatori. RaaS include, de obicei, un panou de control, suport tehnic și actualizări pentru a îmbunătăți eficiența atacurilor.

Cum funcționează RaaS?

Crearea software-ului. Atacatorii dezvoltă un software de ransomware sofisticat, care poate cripta fișierele utilizatorilor și să ceară o răscumpărare în schimbul deblocării acestora.

Platforma de vânzare. Acest software este apoi disponibil pe diverse forumuri clandestine, unde atacatorii pot să-l "închirieze" pentru a lansa propriile atacuri.

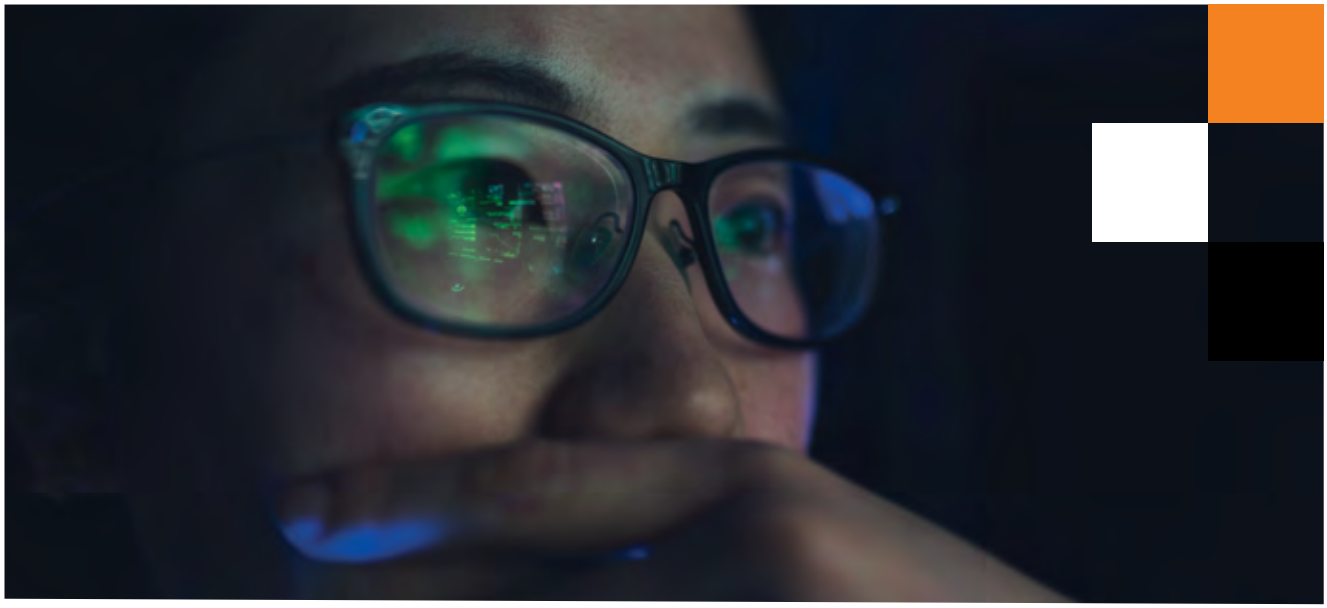
Suport tehnic. Ofertele RaaS includ de obicei suport tehnic pentru persoanele care nu au competențe tehnice. Acestea primesc ajutor în configurarea atacului și în gestionarea campaniilor.

Împărțirea profitului. Ransomware-ul este proiectat pentru a împărți rapid profiturile. De obicei, creatorii de RaaS primesc un procent din răscumpărarea plătită de victime, în timp ce atacatorul păstrează restul.

REvil, cunoscut și sub numele de Sodinokibi, a fost una dintre cele mai notorii platforme RaaS. A fost implicat în atacuri asupra unor organizații mari, inclusiv Kaseya, care a afectat peste 1.500 de companii[5] în întreaga lume în 2021. Atacatorii au solicitat o răscumpărare de 70 de milioane de dolari, demonstrând impactul devastator pe care un atac RaaS îl poate avea asupra unei organizații. REvil se remarcă prin trimiterea de e-mailuri de amenințare și prin tacticile de extorcare.

- Sodinokibi poate fi distribuit prin diverse metode, cum ar fi campaniile de phishing, exploatarea vulnerabilităților software, și mesaje de e-mail compromise.
- Uneori, atacatorii utilizează accesul la rețelele interne obținut prin intermediul unor metode de inginerie socială sau prin exploatarea unor vulnerabilități cunoscute.
- Odată ce ransomware-ul a infiltrat sistemul, acesta se va implanta, în mod obișnuit, pe un sistem de operare Windows, dar poate afecta și alte platforme precum MacOS sau Debian/GNU
- Ransomware-ul criptează fișierele victimei, vizând extensiile cele mai comune (documente, imagini, baze de date etc.), și lasă un fișier text (de obicei numit "README.txt") cu instrucțiuni despre cum poate fi plătită răscumpărarea.
- Atacatorii cer de obicei o sumă de bani în criptomonedă, de cele mai multe ori Bitcoin, pentru a oferi cheia de decriptare. Sumele cerute pot varia, dar acestea pot fi destul de mari, în funcție de severitatea atacului și de organizația vizată.
- Sodinokibi utilizează tehnici de evaziune avansate pentru a evita detecția de către unelte anti-malware. Acestea pot include criptarea codului său sau utilizarea unor tehnici de „fileless malware" care afectează memoria sistemului fără a scrie fișiere pe disc.
- În multe cazuri, Sodinokibi nu criptează doar fișierele, ci și exfiltrează date sensibile înainte de a le cripta. Atacatorii amenință că vor publica aceste date pe dark web dacă nu li se plătește răscumpărarea.

5 https://www.wired.com/story/revil-ransomware-supply-chain-technique/



DarkSide este o altă entitate RaaS notabilă care a câștigat o notorietate semnificativă prin atacul[6] asupra Colonial Pipeline în mai 2021. Acest atac a dus la blocarea unei mari părți a infrastructurii de combustibil din Statele Unite, provocând penurie și creșteri semnificative ale prețului combustibilului. Atacatorii au cerut o răscumpărare de 4,4 milioane de dolari, pe care au și primit-o. DarkSide utilizează un business model în care se angajează să nu atace organizații din sectorul medical sau infrastructura critică.

DarkSide a apărut pentru prima dată pe scena RaaS în august 2020. Această grupare de ransomware a surprins prin abordarea sa bine gândită și sofisticată, axându-se pe atacuri bine planificate și pe vizarea companiilor cu venituri mari. Primul atac notabil asociat cu DarkSide a avut loc în martie 2021, când grupul a vizat o serie de organizații din diverse sectoare. Cel mai cunoscut atac a fost cel asupra Colonial Pipeline în mai 2021, care a dus la blocarea unei mari părți a livrărilor de carburant pe Coasta de Est a Statelor Unite. Atacul a avut un impact semnificativ asupra economiei, provocând panică și deficit de combustibil.

DarkSide utilizează o abordare sofisticată pentru a infecta sistemele țintă:

- **Recunoaștere.** Atacatorii își aleg țintele, adesea companii mari sau organizații cu resurse semnificative. Acest lucru se face prin intermediul tehnicilor de recunoaștere, care pot include scanning-ul rețelelor, analiza infrastructurii IT și identificarea punctelor slabe.

- **Infiltrare.** Odată ce o țintă este aleasă, atacatorii folosesc diverse metode pentru a obține acces la rețea, inclusiv phishing, exploituri de software sau accesul direct prin parole compromise.

- **Extinderea accesului.** După ce obțin accesul inițial, atacatorii își consolidează controlul prin instalarea de instrumente de acces la distanță și prin escaladarea privilegiilor. Acest pas le permite să navigheze și să controleze rețeaua mai eficient.

- **Criptarea datelor.** Odată ce au obținut accesul necesar, atacatorii criptează datele organizației, lăsând ținta fără posibilitatea de a accesa informațiile critice. În mod obișnuit, ransomware-ul DarkSide include mesaje care informează victimele despre atac și oferă instrucțiuni pentru plata răscumpărării.

6 https://www.cybereason.com/blog/inside-the-darkside-ransomware-attack-on-colonial-pipeline

- **Cererea de răscumpărare.** După criptarea datelor, atacatorii solicită o sumă de bani, de obicei în criptomonedă (Bitcoin sau altă monedă digitală), în schimbul cheii de decriptare.

RaaS are un impact profund asupra peisajului securității cibernetice, transformând modul în care se desfășoară atacurile de ransomware. Modelul RaaS a democratizat accesul la instrumentele de atac, permițând chiar și infractorilor cu cunoștințe tehnice limitate să comită atacuri devastatoare. Aceasta a dus la o creștere exponențială a numărului de atacuri ransomware.

Criminalii cibernetici adoptă din ce în ce mai des tehnici avansate, cum ar fi atacurile de tip „double extortion", în care, pe lângă criptarea fișierelor, datele sensibile sunt furate și amenințările de publicare sunt direcționate către victime. Conceptul „double extortion" a apărut în 2019, odată cu atacul grupului Maze[7]. Această strategie a marcat o schimbare semnificativă în peisajul ransomware-ului, atacatorii nu doar criptând fișierele victimelor, ci și amenințând cu publicarea sau vânzarea informațiilor sensibile pe dark web. Acest tip de extorcare a fost atractiv, deoarece oferea un dublu stimulent pentru victime de a plăti: riscul pierderii datelor și amenințarea expunerii informațiilor confidențiale, care ar putea afecta reputația și stabilitatea financiară a organizației.

Antivirusurile tradiționale și soluțiile de securitate slab integrate nu pot detecta întotdeauna ransomware-ul RaaS din cauza complexității acestuia și a variantelor sale în continuă schimbare.

Pentru combaterea RaaS, organizațiile trebuie să adopte o abordare multifațetată, orientată spre prevenire. Câteva măsuri de bază includ:

- **Educația angajaților.** Organizarea de sesiuni de formare pentru angajați pentru a-i ajuta să identifice și să evite e-mailurile suspecte sau atacurile de phishing.
- **Backup-uri regulate.** Realizarea de backup-uri periodice și stocarea acestora în locații diferite pentru a limita pierderile în cazul unui atac.
- **Actualizări de securitate.** Practica de a menține toate sistemele și software-urile la zi, pentru a preveni exploatarea vulnerabilităților.
- **Soluții avansate de securitate.** Implementarea de soluții de securitate avansate, cum ar fi sistemele de detectare a intruziunilor și protecția bazată pe comportament.

Ransomware as a Service reprezintă o amenințare semnificativă pentru organizațiile din întreaga lume. Cu un business model eficient și în continuă evoluție, RaaS a permis atacatorilor să devină din ce în ce mai îndrăzneți în metodele lor. În fața acestor amenințări emergente, este crucial ca organizațiile și indivizii să fie conștienți și pregătiți să se apere împotriva acestor atacuri devastatoare. Educația, conștientizarea și tehnologia sunt esențiale în conceperea unei strategii eficiente de apărare împotriva ransomware-ului.

Transformarea tacticilor

Atacatorii din 2024 au început să folosească metode sofisticate, cum ar fi ingineria socială avansată și atacurile de tip supply chain, care complică detecția și prevenția prin metode „tradiționale", precum măsuri de securitate perimetrală sau pe end-point. De asemenea, în ciuda plăților efectuate, victimele nu primesc de fiecare dată accesul la uneltele și cheile de decriptare, ceea ce le determină

7 https://www.hhs.gov/sites/default/files/maze-ransomware.pdf

pe multe să recurgă la soluții de backup pentru a-și restaura datele.

Costurile financiare

Ransomware-ul nu doar că afectează reputația organizațiilor, dar și bugetele acestora. În 2024, costurile[8] globale legate de ransomware, inclusiv plățile și cheltuielile pentru recuperare, au atins miliarde de dolari. Companiile care aleg să plătească recompensa nu au garanția că vor obține accesul la datele criptate, ceea ce face ca suma totală pierdută să fie și mai mare.

Ransomware-ul a evoluat considerabil în ultimele decenii, devenind una dintre cele mai îngrijorătoare amenințări la adresa securității cibernetice la nivel global. Anii 2023 și 2024 au fost martorii unei proliferări a atacurilor de acest tip, cu un impact financiar devastator asupra companiilor și organizațiilor din diverse industrii.

Atacurile ransomware implică, în general, criptarea fișierelor victimei, iar hackerii cer o răscumpărare pentru decriptarea acestora. Conform unui raport[9] realizat de Cybersecurity Ventures, costurile globale asociate atacurilor ransomware în 2024 au fost estimate la 20 de miliarde de dolari, o creștere semnificativă față de 2023, când costurile erau de aproximativ 16 miliarde de dolari. Această creștere poate fi atribuită unei varietăți de factori, inclusiv dezvoltarea de tehnici noi și mai sofisticate de atac, precum și expansiunea pe piețe emergente.

În 2024, multe organizații au ales să plătească răscumpărarea cerută de atacatori în încercarea de a-și recupera rapid datele critice. Un studiu[10] realizat de Sophos a arătat că 43% dintre organizații au plătit răscumpărarea în 2023, iar această tendință a continuat în 2024. Sumele cerute de atacatori variază considerabil, dar în medie, acestea se ridică la aproximativ 200.000 de dolari. Această sumă poate fi devastatoare pentru IMM-uri, dar și pentru companiile mari, care au de obicei proceduri complexe de recuperare a datelor.

8 https://www.esentire.com/web-native-pages/cybercrime-to-cost-the-world-9-5-trillion-usd-annually-in-2024#:~:text=Ransomware%20will%20cost%20its%20victims,refine%20their%20malware%20payloads%20and
9 https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/
10 https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2024-wp.pdf

Pe lângă suma plătită ca răscumpărare, organizațiile afectate suportă costuri semnificative pentru recuperarea datelor, restaurarea infrastructurii IT și consolidarea securității. Conform estimărilor Kaspersky, aceste costuri pot depăși de 3 ori suma plătită pentru răscumpărare. De exemplu, dacă o companie a plătit 100.000 de dolari, este posibil ca ea să cheltuie încă 300.000 de dolari pentru a-și restabili sistemele și a preveni atacurile viitoare.

Costurile directe reprezintă doar o parte din impactul financiar al ransomware-ului. Există și costuri indirecte care pot afecta grav operațiunile și profitabilitatea unei companii.

Atacurile ransomware pot duce la întreruperea operațiunilor și la pierderi semnificative de venituri. Un raport[11] Forbes a arătat că, în medie, organizațiile afectate își pierd 25% din veniturile anuale în urma unui atac ransomware. Aceasta se datorează nu doar întreruperii serviciilor, ci și impactului asupra reputației și încrederii clienților.

Impactul financiar al ransomware-ului în 2024 este profund, atingând atât costurile directe, cât și cele indirecte. Organizațiile trebuie să fie conștiente de aceste amenințări și să investească în soluții de securitate cibernetică pentru a se proteja. În plus, conștientizarea și educarea angajaților reprezintă un aspect esențial al strategiei de apărare împotriva ransomware-ului. Având în vedere tendințele emergente, este esențial ca liderii din industrie să reevalueze și să ajusteze regimul de securitate cibernetică al organizațiilor lor pentru a face față provocărilor viitoare.

11 https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/

7.

Îmbunătățim securitatea datelor afacerii tale prin centre de date securizate

Cristian Turcin,
Lead Cloud, Collocation & Professional Services,
Orange România

Într-un peisaj digital în continuă evoluție, securitatea datelor companiei tale ori a celei în care îți desfășori activitatea este esențială. Pe măsură ce organizațiile îmbrățișează transformarea digitală, necesitatea unor soluții robuste și sigure pentru găzduirea datelor devine tot mai importantă.

Astăzi, serviciile de colocare sunt fundația sigură pentru infrastructura afacerii tale.

Și probabil te întrebi, **de ce să alegi serviciile noastre de colocare?**

Pentru că îți oferim un mediu sigur pentru echipamentele tale. Când îți plasezi serverele în centrele noastre de date avansate, beneficiezi de:

1. **Securitate 24/7**, avem supraveghere constantă, acces controlat și protocoale de securitate de ultimă generație pentru a-ți proteja datele.
2. **Fiabilitate** cu surse de alimentare redundante și sisteme de răcire eficiente. Ne asigurăm că operațiunile tale nu se opresc niciodată.
3. **Conformitate,** centrele noastre respectă toate reglementările de securitate, ajutându-te să rămâi în conformitate cu legea.

Majoritatea serviciilor furnizate de noi - de la cloud computing și soluții de securitate, la IoT și alte servicii IT și telecomunicații - sunt deținute și gestionate prin centrele noastre de date securizate. Această abordare integrată asigură un nivel ridicat de securitate și fiabilitate pentru fiecare aspect al infrastructurii tale digitale.

Astfel, alegi **Orange Business** și beneficiezi de:

- **Securitate end-to-end.** Deținând atât centrele de date cât și serviciile, implementăm măsuri de securitate consistente la toate nivelurile mediului IT al afacerii tale.

- **Integrare perfectă.** Serviciile noastre sunt proiectate să funcționeze eficient împreună în cadrul infrastructurii noastre securizate, oferind performanțe optime și ușurință în administrare.

- **Suport și expertiză unificate.** Cu un singur furnizor pentru toate nevoile tale, primești suport complet din partea echipei noastre de experți.

- **Protecție sporită a datelor.** Controlul nostru asupra întregului lanț de livrare a serviciilor ne permite să aplicăm politici stricte de protecție a datelor, protejând informațiile împotriva amenințărilor.

- **Conformitate cu reglementările.** Asigurăm conformitatea serviciilor noastre și a centrelor de date cu standardele internaționale de securitate, simplificând eforturile tale de conformitate.

Prin încrederea acordată serviciilor și infrastructurii securizate furnizate de noi, investești într-o strategie de securitate integrată și durabilă. Această sinergie nu doar că protejează datele tale critice, dar îmbunătățește și eficiența și fiabilitatea operațiunilor IT și telecom.

Cu o prezență îndelungată pe piața locală, suntem un **partener de încredere** pentru diverse domenii de afaceri din România. Înțelegerea profundă a pieței locale și a mediului de reglementare ne permite să adaptăm serviciile noastre pentru a răspunde nevoilor specifice ale întreprinderilor românești.

Expertiza noastră acoperă:

- **Cunoștințe de conformitate locală:** suntem bine familiarizați cu legislația privind protecția datelor din România și reglementările specifice industriei, asigurându-ne că serviciile noastre te ajută să respecți toate cerințele legale.

- **Perspectivă culturală și de afaceri:** experiența noastră în colaborarea cu diverse companii din România ne permite să oferim soluții care se aliniază practicilor operaționale și culturii organizaționale.

- **Parteneriate solide în industrie:** colaborările cu furnizori de tehnologie locali și internaționali ne îmbunătățesc ofertele de servicii, aducând cele mai bune soluții în inovație și fiabilitate.

Centrele de date securizate sunt fundația transformării digitale.

În contextul digital actual cu o piață într-o continuă schimbare, companiile sunt nevoite să adopte transformarea digitală pentru a rămâne relevante și competitive. Această transformare implică integrarea tehnologiei digitale în toate ariile afacerii, schimbând fundamental modul în care îți desfășori activitatea și oferi valoare clienților. Totuși, acest proces introduce și noi provocări, în special în menținerea unor măsuri solide de securitate în fața amenințărilor cibernetice tot mai sofisticate.

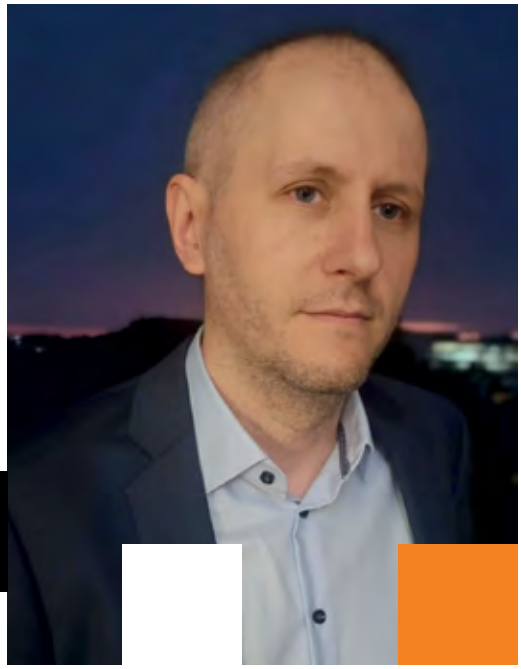
Soluțiile securizate pentru centrele de date sunt esențiale pentru succesul inițiativelor de transformare digitală.

Cu **Orange Business** ai acces la soluții inovatoare care îți protejează datele și îți asigură un mediu sigur și scalabil pentru creșterea afacerii tale. Contactează-ne și descoperă cum putem transforma împreună viziunea ta digitală în realitate. Fă primul pas spre un viitor mai sigur al afacerii tale!

8.

Cybersecurity

sau cum am învățat să nu mă tem de schimbare



Mădălin Vasi
Managing Security Solutions Architect, Orange România

Este ora 6:30 dimineața, telefonul sună insistent. O voce îngrijorată:

"Sistemele nu funcționează! Nu putem factura, iar camioanele sunt blocate la poartă. Până și backup-ul a fost criptat. Ne puteți ajuta?"

Acesta este momentul de care atât companiile, cât și furnizorii, se tem cel mai mult: un dezastru neașteptat care aduce organizația în pragul unei crize. Întrebarea care apare în acest context este: cum am ajuns aici?

O altă situație: "Ne-au sunat de la DNSC. Avem 6 luni să prezentăm auditul NIS. Suntem doar noi doi în departamentul IT. Ce trebuie să facem?"

Aceste două scenarii reflectă provocări critice cu care se confruntă multe organizații. Într-o lume plină de amenințări, de la încălzirea globală, conflicte armate până la sabotaje și atacuri cibernetice, atunci când afacerea ta depinde de sisteme IT, soluțiile nu sunt simple și implică mulți factori.

În acest context, **existența unui cadru legislativ precum legea NIS este un aspect pozitiv,** oferind direcții clare și standarde de urmat.

Un lucru este cert: pentru a realiza o transformare profundă a organizației, va fi necesară o abordare sistematică a politicilor de securitate și IT. Stabilirea primului pas, însă, poate fi cel mai mare obstacol, mai ales când opțiunile sunt copleșitoare și resursele sunt limitate.

În plus, fiecare producător își promovează soluțiile ca fiind ideale pentru conformitatea NIS. Însă orice soluție trebuie asimilată, implementată și operată corect pentru a fi eficientă.

Așadar, cum procedăm?

1 Primul pas: evaluarea inițială

Imaginează-ți că ești la începutul unei călătorii, realizezi că lumea se schimbă rapid, iar măsurile existente nu sunt suficiente. Așadar, trebuie să decizi să faci primul pas spre transformare: **evaluarea inițială.**

O putem denumi analiza gap sau pre-audit. Este ca o inspecție a casei, înainte de renovare. Identificând punctele slabe și zone ce necesită îmbunătățiri, tot în acest pas este importantă și analiza infrastructurii IT.

La finalul acestei etape vei pregăti un **masterplan**, un plan de acțiune detaliat pentru următoarele 6 luni până la 2 ani (indiferent că obiectivul este conformarea cu NIS sau protejarea activelor critice, a oamenilor sau a infrastructurii).

2 Alocarea bugetului

Acum că există un plan, trebuie să obții bugetul.

Nu te îngrijora dacă nu poți aloca imediat un buget complet. Important este să începi transformarea, să pui în mișcare strategia și să planifici bugetele pentru viitor. Gândește pe termen lung – o perioadă de cel puțin 2 ani. Acest lucru îți permite să vizualizezi rezultatele și să ajustezi planul pe parcurs.

Sfat important: Implică top managementul în discuția despre importanța acestei investiții. Securitatea cibernetică nu este doar o cheltuială, ci o **asigurare pentru continuitatea și succesul afacerii.**

3 Implementarea soluțiilor

Cu planul și bugetul pregătite, ești gata să treci la acțiune. Implementarea soluțiilor este momentul în care planurile prind viață.

Începe cu un plan de acțiune etapizat, care îți permite să introduci măsurile de securitate treptat, fără a perturba operațiunile zilnice.

Următoarele sunt exemple de soluții eficiente și cu impact maxim:

- **Conștientizarea importanței securității cibernetice**

  Unul dintre cei mai rapizi pași este să investești în oameni. Asigură-te că echipa este instruită și conștientă de bunele practici de igienă în cybersecurity.

De ce este important? Pentru că factorul uman este adesea cea mai slabă verigă în securitate. Printr-un program de training și campanii anti-phishing, poți reduce semnificativ riscurile.

- **Soluții "as-a-service"**

  Tehnologia evoluează rapid, iar soluțiile livrate ca servicii pot fi o modalitate eficientă de a îmbunătăți securitatea, fără investiții masive în infrastructură.

Ce ar trebui să ai în vedere? Alege soluții de la producători recunoscuți, pentru care există expertiză în piață și în afacerea ta. Evită soluțiile fără un istoric solid.

Soluțiile centralizate livrate din cloud ca servicii permit, de exemplu, să implementezi și să operezi o soluție de firewall avansat fără complicații.

Un exemplu accesibil este cel oferit chiar de **Orange Business:** serviciul **Business Internet Security** ce a deservit sute de clienți din România, oferind protecție avansată într-un mod accesibil și eficient.

- **Persoana responsabilă**

Cine este responsabil de securitatea datelor în cadrul afacerii tale? Evident că toată lumea. Dar este esențial să existe un lider dedicat care să coordoneze eforturile.

Numirea unui Chief Information Security Officer (CISO) poate face diferența. Acest lider va coordona strategia de securitate, asigurând colaborarea între departamente și integrarea în ecosistemul de parteneri.

- **Colaborarea și sprijinul extern**

Este recomandat să ceri ajutorul experților și organizațiilor specializate pentru a simplifica procesul.

La **Orange Business,** ne-am poziționat ca un partener de încredere, oferind suport continuu și expertiză actualizată alături de colaboratori cu experiență, pentru a te îndruma către cele mai bune alternative.

Folosește-te de resursele oferite de autorități recunoscute: organizații precum DNSC și ENISA furnizează ghiduri, bune practici și suport pentru conformare, alături de organizații internaționale de standardizare precum NIST sau CIS. Aceste resurse te pot ajuta să înțelegi mai ușor complexitatea reglementărilor și standardelor.

În final, nu ești doar tu în această călătorie.

Noi, la **Orange Business**, suntem alături de tine, gata să te ajutăm să construiești încredere și să îți protejezi afacerea. Fie că ești la început de drum sau ai făcut deja primii pași, colaborarea și comunicarea sunt cheile succesului.

Te încurajăm să începi transformarea chiar de astăzi!

9. Amenințări la adresa identității digitale

Pentru fiecare dintre noi, identitatea digitală reprezintă o realitate a timpurilor de-acum. Suma tuturor informațiilor pe care cu bună știință le-am publicat pe internet, pe platformele de socializare sau pe cele profesionale, interacțiunile și mesajele din aplicațiile preferate, datele personale stocate în clouduri publice ori private, toate acestea converg în această identitate digitală, un abstract al artefactelor folosirii internetului.

Într-o lume din ce în ce mai digitalizată, unde interacțiunile sociale, economice și profesionale se desfășoară în principal online, protejarea identității digitale este esențială. În acest context, amenințările la adresa identității digitale se diversifică și devin tot mai sofisticate, având potențialul de a produce daune semnificative.

Probabil că ai citit cele ce urmează și cu altă ocazie, în publicații și articole de specialitate. Din fericire, unele dintre aceste informații apar din ce în ce mai des și în campaniile de conștientizare ale autorităților și ale celor din privat, în rețelele sociale și în publicațiile cu caracter generalist, confirmând nevoia de a cunoaște riscurile și amenințările din această lume digitală.

Phishingul

Phishingul este o tehnică folosită de atacatori pentru a obține informații sensibile, cum ar fi parolele sau detaliile cardurilor de credit, prin determinarea utilizatorilor să ofere aceste informații prin intermediul unor platforme sau e-mailuri false. Aceste atacuri au devenit din ce în ce mai sofisticate și folosesc texte și imagini de calitate, menite să convingă utilizatorii de pretinsa legitimitate. Un procent semnificativ din toate atacurile cibernetice ce sunt monitorizate și blocate în infrastructura Orange Business sunt rezultatul unor campanii de phishing.

Cum afectează phishingul identitatea digitală.

1. **Furtul de informații personale.** Odată ce hoții de identitate obțin acces la informațiile personale, cum ar fi numele, adresele, numerele de telefon, datele de naștere sau CNP-ul țintelor, ei pot folosi aceste date pentru a se prezenta ca victimele lor. Aceasta poate duce la fraudă și la crearea unor conturi online în numele victimei.

2. **Acces neautorizat la conturi.** Prin obținerea credențialelor de autentificare, atacatorii pot accesa conturi de e-mail, rețele sociale sau conturi bancare. Aceasta le permite să efectueze tranzacții financiare frauduloase sau să răspândească informații false sub identitatea victimei.

3. **Reputație afectată.** Atunci când informațiile personale sunt compromise, victimele se pot confrunta cu probleme de reputație. De exemplu, dacă cineva folosește contul de e-mail al unei persoane pentru a trimite mesaje spam sau pentru a angaja activități ilegale, acest lucru poate afecta reputația victimei pe termen lung.

4. **Stres emoțional și psihologic.** Pe lângă impactul financiar și legal, victimele phishingului pot resimți un stres emoțional semnificativ. Îngrijorarea cu privire la utilizarea abuzivă a informațiilor personale poate duce la anxietate și la o stare de nesiguranță.

Anul 2024 a adus cu sine o creștere semnificativă a numărului de atacuri de phishing, iar analiza statisticilor în acest domeniu ne oferă o imagine clară asupra evoluției amenințărilor și a modalităților de protecție.

Din datele colectate și procesate în platformele Orange Business observăm că numărul atacurilor de phishing a crescut cu aproximativ 28% în 2024 comparativ cu anul anterior. Această creștere a fost în mare parte determinată de evoluția tehnologiilor de comunicare, cum ar fi utilizarea tot mai frecventă a aplicațiilor de mesagerie și a rețelelor sociale pentru transmiterea link-urilor înșelătoare. De asemenea, atacurile de phishing s-au diversificat, având acum la bază metode mai sofisticate, ce includ phishingul vocal (vishing) și phishingul prin SMS (smishing).

În 2024, tacticile de phishing au evoluat pentru a deveni mai greu de identificat. Una dintre cele mai utilizate tehnici a fost utilizarea atacurilor de tip „spoofing”, în care atacatorii își maschează adresele de email astfel încât acestea să pară că provin din surse de încredere. Statisticile noastre arată că

peste 90% dintre atacurile de phishing au fost efectuate prin emailuri care păreau legitime și sunt asociate cu instituții financiare sau servicii populare.

Studii publicate și citate în articole recente[12] arată că aproximativ 3 miliarde de mesaje phishing sunt trimise în fiecare zi, la nivel global. Adică aproximativ 2% dintre toate emailurile trimise, în fiecare zi, pe întreaga planetă.

Organizațiile mari, în special cele din domeniul bancar și al sănătății, sunt ținte frecvente. Aceleași studii arată că peste 73% dintre instituțiile financiare raportează că au fost supuse cel puțin unui atac de phishing în 2024, iar acest procent este în creștere.

Ce este de făcut? Educația utilizatorilor, conștientizarea riscurilor și tehnologii avansate de detecție și protecție

Pentru a contracara amenințările de phishing, organizațiile investesc tot mai mult în educația utilizatorilor și în soluții tehnologice avansate. Aceste programe includ simulări de atacuri de phishing și sesiuni de formare pentru a ajuta angajații să recunoască semnele unui atac.

Pe lângă educație, tehnologiile de securitate joacă un rol crucial în prevenirea atacurilor. Soluțiile de filtrare a emailurilor, autentificarea cu doi factori și utilizarea inteligenței artificiale pentru detectarea comportamentului anormal sunt doar câteva dintre măsurile implementate de organizații pentru a-și proteja datele sensibile.

Malware

Malware-ul este un alt tip de amenințare care poate afecta identitatea digitală. Acesta include software-uri malițioase concepute să compromită sistemele de securitate ale utilizatorilor. Prin infectarea unui dispozitiv precum telefonul inteligent sau laptopul personal, malware-ul poate fura date personale, poate înregistra activitatea utilizatorului sau poate cripta informațiile, solicitând ulterior o răscumpărare. Din ce în ce mai multe aplicații și extensii de browser sunt compromise, expunând utilizatorii la riscuri.

Atacurile prin inginerie socială

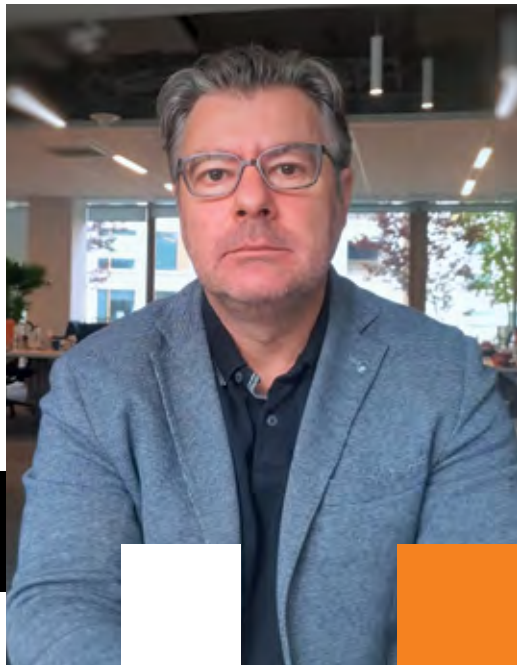
Atacurile prin inginerie socială se bazează pe manipularea psihologică a utilizatorilor pentru a-i determina să divulge informații sensibile. Aceste tactici pot include apeluri telefonice, mesaje directe sau contact prin rețele sociale, unde atacatorii pretind că sunt persoane de încredere. De cele mai multe ori, atacurile de acest tip se bazează pe crearea unei urgențe, ceea ce face ca utilizatorii să acționeze fără a analiza situația în detaliu.

Breșele de date

Breșele de date reprezintă o amenințare majoră pentru identitatea digitală. Acestea se produc atunci când datele personale ale utilizatorilor sunt furate din sistemele unei organizații, ceea ce poate include nume, adrese, date de naștere, parole și, uneori, informații financiare. Breșele de date au devenit frecvente, iar consecințele pot fi devastatoare – utilizatorii își pot găsi identitatea furată și pot fi expuși la fraude financiare.

12 https://www.zdnet.com/article/three-billion-phishing-emails-are-sent-every-day-but-one-change-could-make-life-much-harder-for-scammers/

10. Inteligența artificială în securitatea cibernetică: o sabie cu două tăișuri



Laurențiu Popescu,
Lead Cybersecurity, Orange România

Bine ai venit în era digitală, unde inteligența artificială (I.A.) devine din ce în ce mai importantă în combaterea atacurilor cibernetice. Dar, ca orice superputere, are și o latură întunecată. Pe de o parte, I.A. ajută la protejarea datelor, însă pe de altă parte, infractorii cibernetici își perfecționează metodele de atac.

Să ne aruncăm împreună o privire asupra modului în care aceste tehnologii sunt folosite, atât pentru siguranța noastră, cât și împotriva noastră.

Cum folosesc atacatorii cibernetici inteligența artificială?

Phishingul și I.A.

Te-ai gândit vreodată cât de ușor poate un hacker să îți fure informațiile personale? Cu ajutorul I.A., mesajele de phishing devin extrem de credibile și personalizate. Atacatorii cibernetici analizează date despre tine, de la conturile de social media până la e-mailurile pe care le trimiți, și creează mesaje care par că vin din partea unor persoane sau organizații de încredere. Greu de detectat, nu-i așa?

Malware îmbunătățit prin I.A.

Ești pregătit pentru un atac mai sofisticat? Malware-ul, alimentat de I.A., învață și se adaptează. Acesta poate analiza o rețea și poate alege momentul optim pentru a acționa sau poate decide să rămână inactiv pentru o perioadă lungă de timp pentru a evita detectarea.

Atacurile de tip "zero-day"

Vulnerabilitățile de tip "zero-day" sunt acele puncte slabe ale unui sistem sau aplicații necunoscute dezvoltatorilor, dar exploatate de atacatori. Cu ajutorul I.A., infractorii pot analiza codul software pentru a descoperi vulnerabilități noi mai rapid decât echipele de securitate, iar atacurile asupra acestora pot fi lansate automat. I.A. accelerează procesul de identificare și exploatare a acestor vulnerabilități, făcând răspunsul rapid mult mai dificil.

Atacurile DDoS automatizate

Atacurile DDoS (Distributed Denial of Service) implică supraîncărcarea unui server sau a unei rețele cu trafic fals, astfel încât resursele acestuia să devină indisponibile pentru utilizatorii legitimi. Inteligența artificială poate fi utilizată pentru a coordona rețele uriașe de dispozitive infectate (botnets), pentru a lansa atacuri mai eficiente și mai greu de oprit. Algoritmii I.A. pot ajusta dinamica atacurilor în timp real, maximizând impactul și dificultatea de a opri atacul.

Deepfake-urile și falsificarea datelor

Tehnologiile de tip deepfake folosesc rețele neuronale pentru a crea imagini și videoclipuri false extrem de convingătoare. În atacurile cibernetice, acestea pot fi utilizate pentru a înșela angajații sau factorii de decizie dintr-o organizație, făcându-i să creadă că interacționează cu o persoană de încredere. Un exemplu poate fi un videoclip fals cu un CEO care cere transferuri financiare urgente sau divulgarea de informații sensibile.

Ce avantaje au atacatorii?

- **Adaptabilitate și automatizare.** Utilizarea I.A. permite atacatorilor să automatizeze o mare parte din procesele necesare pentru a iniția și întreține atacuri. Ceea ce înseamnă că pot lansa simultan atacuri complexe asupra mai multor ținte, fără a fi nevoie de o implicare manuală extinsă.

- **Învățare continuă.** Algoritmii I.A. pot învăța din greșeli și se pot adapta pentru a deveni mai eficienți. Astfel, oferă un avantaj major în fața soluțiilor tradiționale de securitate cibernetică, care tind să fie reactive și mai puțin flexibile.

- **Detecție dificilă.** Atacurile bazate pe I.A. sunt deseori mult mai subtile și greu de detectat. Malware-ul, de exemplu, poate utiliza tehnici de machine learning pentru a evita soluțiile de securitate, care folosesc semnături cunoscute pentru a detecta amenințările.

- **Eficiență sporită în compromiterea sistemelor.** Un atacator care utilizează I.A. poate analiza volume mari de date mult mai rapid decât un atacator uman, descoperind mai ușor vulnerabilitățile și exploatându-le cu o precizie mai mare.

Cum răspundem în fața acestor amenințări?

- **Prin utilizarea I.A. în apărarea cibernetică** - organizațiile încep să integreze soluții de securitate bazate pe I.A. pentru a combate aceste noi tipuri de atacuri. Algoritmii de machine learning pot fi antrenați să detecteze comportamente anormale în rețele și să prevină atacurile înainte ca acestea să cauzeze daune.

- **Prin educarea și conștientizarea angajaților -** este crucială pentru a recunoaște tactici de phishing avansate și falsificări de tip deepfake. Pe măsură ce atacurile devin din ce în ce mai sofisticate, educația continuă rămâne o componentă esențială a apărării cibernetice.

- **Prin colaborarea internațională** - pentru a face față acestei amenințări în creștere, guvernele și organizațiile de securitate cibernetică din întreaga lume încep să colaboreze mai strâns, schimbând informații despre vulnerabilități și amenințări emergente bazate pe I.A.

Deși I.A. aduce beneficii semnificative în numeroase domenii, inclusiv în securitatea cibernetică, atacatorii cibernetici o folosesc tot mai mult pentru a-și perfecționa metodele. Această tendință creează o provocare continuă pentru profesioniștii din securitatea informațională, care trebuie să adopte tehnologii la fel de avansate pentru a preveni și a combate atacurile bazate pe I.A.

În acest context, **securitatea cibernetică bazată pe I.A. nu este doar o necesitate,** ci o cursă continuă pentru a rămâne înaintea celor care exploatează aceste tehnologii cu alte scopuri.

Threats Exposures Management

Soluție de scanare continuă a vulnerabilităților de securitate

orange.ro/business

orange™ Business

11. Retrospectiva anului 2024 în incidente de securitate cibernetică

De-a lungul fiecărei ediții a raportului nostru, am adunat o cronologie a evenimentelor de importanță majoră pentru contextul global al securității cibernetice. Continuăm și în această primă ediție în limba română cu trecerea în revistă a unora dintre cele mai importante atacuri cibernetice sau pierderi și furturi de date, care au afectat infrastructurile și datele companiilor, în ultimele 12 luni.

Atacurile ransomware – în special cele ale grupării LockBit, dublate de DDoS, au fost printre cele mai prolifice amenințări ale anului 2024, iar pierderile de date din infrastructuri cloud nesecurizate au continuat și în acest an. Printre țintele vizate de aceste atacuri, cele mai importante rămân autoritățile publice, spitalele și universitățile, dar și companiile ce sunt parte din lanțuri de aprovizionare complexe, dedicate soluțiilor pentru operatorii de infrastructuri critice sau infrastructuri esențiale.

Noiembrie 2023

- Un atac ransomware a afectat disponibilitatea serviciilor on-line ale administrațiilor publice din 70 de municipalități ale Germaniei
- o breșă în securitatea sistemelor Samsung a dus la expunerea unor date personale ale clienților din UK
- Boeing au fost victimele unor atacuri ransomware ale grupării LockBit, în urma cărora au fost expuse 46 GB de date ale companiei

Decembrie 2023

- 3 spitale aparținând grupului german Katholische Hospitalvereinigung Ostwestfalen (KHO) au confirmat că au fost victimele unor atacuri ransomware, ale grupării LockBit, ce au dus la sistarea unor servicii
- KyivStar, cel mai mare operator de telecomunicații din Ucraina, a fost victima unor atacuri cibernetice în urma cărora au fost afectate serviciile oferite către baza de 25 de milioane de clienți
- Clienții furnizorului de servicii de conectivitate XFinity au fost victimele unei breșe de date ce a expus informațiile a 36 milioane de beneficiari

Ianuarie 2024

- Gigantul industrial Schneider a fost victima a unui atac ransomware în urma căruia au fost expuse date sensibile
- Monobank, un serviciu e-banking popular în Ucraina, este victima unor atacuri DDoS la scară largă
- VF Corporation, una dintre cele mai mari companii în industria textilă, și-a anunțat cei peste 35 milioane de clienți că datele lor au fost expuse

Februarie 2024

- Gigantul în servicii cloud, CloudFlare, a confirmat că a fost victima unui atac în urma căruia atacatorii au avut acces la sistemele interne de ticketing
- Gruparea ransomware Cactus pretinde că a compromis 1.5 TB de date în urma atacului asupra Schneider Electric, raportat în luna Ianuarie 2024
- Municipalitatea Fulton din statul Georgia confirmă că a fost victima unui atac ransomware orchestrat de gruparea LockBit

Martie 2024

- Gigantul telecom AT&T confirmă că date aparținând de 73 de milioane dintre clienții săi, au fost compromise și expuse în forumuri dark web
- Compania financiară Paysign, furnizor de servicii de plăți electronice, a anunțat că desfășoară o investigație pentru a confirma furtul a peste 1.2 milioane de înregistrări de date ale clienților săi
- Agenția națională franceză pentru ocuparea forței de muncă confirmă că o breșă în securitatea sistemelor proprii a dus la compromiterea informațiilor despre 43 de milioane de persoane

Aprilie 2024

- Vulnerabilitate în echipamentele TP-Link: compania este activ exploatată de 6 rețele bot-net
- Municipalitatea Jackson, din statul Missouri, declară stare de urgență din cauza unor atacuri ransomware ce au afectat disponibilitatea unor sisteme publice
- Home Depot, unul dintre cei mai importanți retaileri din Statele Unite ale Americii, confirmă o breșă de securitate ce a dus la expunerea datelor personale a peste 10.000 de angajați ai companiei

Iunie 2024

- Gigantul telecom Frontier, victimă a unor atacuri ransomware
- TeamViewer – victimele unui atac al grupării APT29 „Cozy Bear”
- Datele personale ale unor contributori ai New York Times, publicate într-un GitHub

August 2024

- 1TB de date personale aparținând angajaților din instituții publice ale orașului Columbus, din statul Ohio, compromise și publicate în DarkWeb
- 240GB de date aparținând angajaților și clienților Toyota, compromise într-un atac al grupării ZeroSevenGroup
- Gigantul petrolier Halliburton a dezactivat majoritatea sistemelor OT pentru a mitiga efectele unui atac ransomware

Octombrie 2024

- Celebrul portal „Internet Archive” – victimă a unui atac ce a compromis website-ul și a dus la pierderea a 31 de milioane de înregistrări ale vizitatorilor site-ului
- Rackspace, victimă a unui atac zero-day în platformele de monitorizare a infrastructurilor
- American Water, principalul furnizor de servicii de utilități și apă potabilă din Statele Unite ale Americii, victimă a unui atac ransomware

Mai 2024

- Ticketmaster, cel mai mare site de vânzări de bilete, a fost victima unui atac cibernetic ce a rezultat în compromiterea datelor a peste 500 de milioane de utilizatori
- Dell anunță că datele a peste 49 de milioane de clienți au fost compromise în cadrul unui atac cibernetic
- Date confidențiale aparținând pacienților spitalului Simone Veil din Cannes, Franța, au fost publicate în urma unui atac al grupării ransomware LockBit

Iulie 2024

- Jurnalele apelurilor efectuate în primele 6 luni ale anului 2022, în rețelele AT&T, sustrase de atacatori
- Peste 1TB de date interne ale companiilor din grupul Disney, sustrase în urma unui atac ransomware
- Datele a mai mult de 2,5 milioane de clienți ai Prudential Financial, expuse într-o breșă de securitate

Septembrie 2024

- Deutsche Flugsicherung (DFS), agenția națională pentru controlul și monitorizarea spațiului aerian al Germaniei, victimă a unui atac cibernetic
- Informații personale ale angajaților companei Microchip, sustrase în cadrul unui atac ransomware
- Date ale clienților gigantului în securitate cibernetică, Fortinet, compromise în urma unei breșe de securitate

12. Business Internet Security – Statistici importante din 2024

Business Internet Security (BIS) este un serviciu de securitate oferit de Orange Business, disponibil întreprinderilor mijlocii și mari, care analizează lunar peste 14 milioane de amenințări de securitate în infrastructurile clienților noștri. Colectăm date relevante anonimizate de la companii din diverse industrii, cum ar fi serviciile publice, comerțul cu amănuntul, transportul și energia. Datele obținute sunt apoi prelucrate prin InfraAI, platforma noastră Big Data Security Analytics dezvoltată la nivel intern, pentru a corela și îmbogăți informațiile comerciale pe care le furnizăm clienților noștri, pentru a obține perspective și informații utile. Datele pentru întocmirea acestui raport sunt generate prin corelarea informațiilor anonimizate din mai multe sisteme de securitate utilizate în unitățile noastre de servicii, cum ar fi firewall-uri NG, gateway-uri de securitate web și e-mail, sisteme de protecție împotriva atacurilor DDoS, sisteme de detectare a intruziunilor sau firewall-uri pentru aplicații web și datele statistice colectate în urma efectuării testelor de penetrare sau a auditurilor de securitate efectuate pentru clienții noștri.

Informațiile colectate de la senzorii noștri de securitate cibernetică sunt îmbogățite în InfraAI, prin corelarea cu multiple surse de investigare a amenințărilor. Informațiile prezentate în acest raport acoperă perioada începând din trimestrul al 4-lea din 2023 și până la finalul trimestrului al 3-lea din 2024.

Distribuția amenințărilor pe verticalele din industrie

Analiza noastră din ultimele 4 trimestre dezvăluie că sectorul energetic a fost cel mai vizat, în baza noastră de clienți B2B cu peste 31% din totalul atacurilor detectate și blocate în BIS, iar anul acesta, la fel ca în ultimele două perioade de raportare, ransomware-ul este principalul vinovat. Administrația publică (locală și centrală) urmează pe locul al doilea, cu 27% dintre toate detecțiile blocate în BIS, amenințând infrastructurile din sectorul public.

În final, companiile din industria IT au fost a treia cea mai vizată industrie, în statistica noastră, cu 25% dintre toate atacurile având ca țintă companiile respective.

Deși motivațiile, tehnicile și procedurile atacatorilor sunt, de obicei, dificil de observat și analizat, există o serie de motive posibile pentru orientarea acestora, cu precădere către industria energetică a României - o evoluție consecventă către dezvoltarea și lansarea de instrumente digitale orientate către utilizator, pentru consumatori și prosumatori din sectorul energetic, a permis clienților să fie abordați rapid de către furnizorii lor de energie. În plus, progresele înregistrate în ceea ce privește integrarea de noi instrumente IT în sistemele operaționale a multor companii din sectorul energetic au dus la creșterea suprafeței de atac și au făcut din actorii principali din acest sector o țintă foarte interesantă pentru atacatori.

Top 5 al industriilor cu amenințări cibernetice blocate în BIS

Industrie	Procent al atacurilor
Energie	31,88%
Administrație publică	27,09%
Servicii IT	25,22%
Sănătate	9,82%
Comerț	5,99%

Distribuția amenințărilor în regiunile României

Din baza noastră de clienți la nivel național, am adunat informații legate de atacurile din toate industriile, iar regiunea București a fost cea mai vizată, cu 34,12% din toate amenințările detectate care au vizat activele situate geografic în regiunea capitalei noastre. Pe locul al doilea se află regiunea de sud-est, ca și în anul precedent, cu 25,23% din totalul amenințărilor distribuite pe sectoare de activitate, iar pe locul al treilea se află regiunea Banat cu 14,91% din totalul amenințărilor.

Distribuția amenințărilor blocate în BIS, în regiunile din România

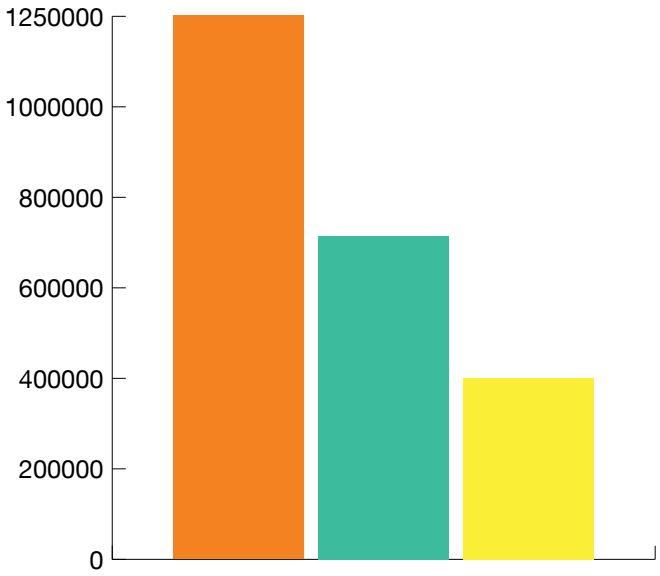
Industrie	Procent al atacurilor
București	34,12%
Sud-Est	25,23%
Banat	14,91%
Alte regiuni	25,74%

În ceea ce privește cele mai afectate orașe în ultimele 12 luni, Bucureștiul se află pe primul loc, cu o medie de 1.250.000 de atacuri prevenite în fiecare lună, la nivelul bazei noastre de clienți localizați acolo, Constanța fiind pe locul al doilea, cu o medie de 715.000 de atacuri blocate în fiecare lună, iar Timișoara pe locul al treilea, cu aproape 400.000 de amenințări detectate și blocate în fiecare lună.

Am dezvoltat și automatizat o metodă îmbunătățită pentru a permite localizarea precisă a diferitelor infrastructuri aflate sub protecția BIS la sediile clienților noștri. Procesul se bazează pe consolidarea datelor din CRM-urile noastre, legate de asocierea adreselor IP a ASN-urilor, și pe integrarea datelor specifice clienților, pentru a îmbunătăți poziționarea activelor într-o anumită zonă geografică. Acest lucru permite platformei noastre InfraAI să extragă date fiabile și să furnizeze analize despre amenințările, actorii și țintele din România, precum și informații precise cu privire la asocierea cu diferitele sucursale și puncte de prezență ale clienților noștri BIS.

Distribuţia ameninţărilor în oraşele din România

Oraş	Media ameninţărilor blocate, în fiecare lună, în BIS
Bucureşti	1.250.000
Constanţa	715.000
Timişoara	400.000



Distribuția amenințărilor după tip

2024 a fost încă o dată un an al atacurilor de tip ransomware. Mai multe campanii au afectat sute de milioane de endpoints, cu pierderi totalizând zeci de miliarde USD. Un raport al Sophos confirmă că peste 59% dintre toate organizațiile monitorizate au fost ținte ale unor atacuri ransomware[13]. În cadrul BIS, acest procent este mai redus – 32% dintre toate entitățile monitorizate au fost vizate de cryptomalware.

Am văzut atacuri de tip ransomware răspândite prin vectori obișnuiți - e-mailuri, rețele sociale, descărcări nesigure, dar și distribuție prin vulnerabilități zero-day sau day-1.

În România au avut loc numeroase incidente de ransomware care au vizat întregul spectru de industrii, atacatorii utilizând instrumente de inteligență artificială generativă pentru a crea amestecarea codurilor lor și pentru a genera „zgomot digital”.

La fel ca în anii precedenți, atacurile DDoS au fost numeroase și au vizat întreaga bază de clienți ai BIS, cu precădere în sectorul financiar și bancar. Atacatorii au folosit uneltele și procedeele cu care suntem familiarizați – Botnets IT / IoT, iar volumele de trafic au crescut și în acest an, odată cu răspândirea la scară largă a conexiunilor la internet multi-gigabit.

Raportul BIS prezintă perspectivele specialiștilor Orange Business în privința acestor două tipuri de amenințări, dar și bune practici și unelte pentru mitigarea acestora.

13 https://www.sophos.com/en-us/content/state-of-ransomware

Distribuţia ameninţărilor după tip

Tip de ameninţare	Procent al atacurilor
Ransomware	36,12%
DDoS	31,94%
Altele	31,94%

Distribuția amenințărilor după țările de origine a atacurilor

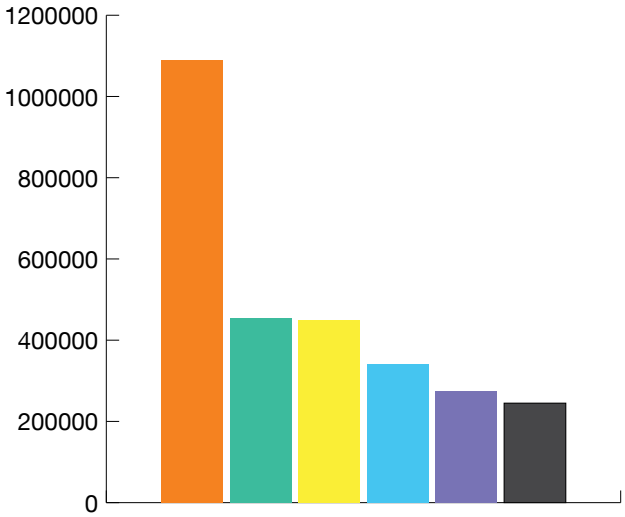
Majoritatea surselor atacurilor detectate de soluția noastră de securitate folosesc adrese IP falsificate sau raportate imprecis, astfel, este dificil să identificăm cu exactitate „adevărata” sursă geografică a unui atac.

Pentru a evita această limitare, folosim mai multe metode de îmbunătățire pentru a determina o localizare mai precisă a unora dintre principalele amenințări pe care le observăm și care atacă baza noastră de clienți și integrăm în platforma noastră, InfraAI, servicii de geo-localizare externe pentru a crește precizia datelor raportate.

În ultimele 12 luni s-a înregistrat o creștere a traficului rău intenționat care provine de la IP-uri din Rusia și China, precum și în perioada anterioară. Majoritatea atacurilor DDoS detectate și blocate în BIS provin din rețele Botnet ce sunt distribuite pe întreaga planetă, dar în aceste cazuri vom considera țara de origine a atacului ca fiind aceea în care putem localiza unul sau mai multe platforme de tip C2C – Command and Control, pentru acele Botnets.

Distribuţia ameninţărilor după ţara de origine

Ţara	IP unice ale atacatorilor (medie lunară, ultimele 12 luni)
Statele Unite ale Americii	1.090.000
China	455.000
România	450.000
Rusia	340.000
Franţa	275.000
Regatul Unit	245.000



13. Educația, inovarea și cercetarea la Orange

UNbreakable România

UNbreakable România este cel mai complex program de securitate cibernetică pentru liceeni și studenți din țară. Prin activitățile propuse, UNbreakable oferă o privire de ansamblu asupra nivelului de performanță în domeniul securității cibernetice la nivel național. Misiunea UNbreakable este de a oferi tinerilor pasionați de securitate cibernetică cele mai variate resurse, teoretice și practice, atât de utile dezvoltării competențelor necesare pentru a deveni buni specialiști în domeniu. Pe lângă un mediu de învățare intensivă, inițiativa oferă și un cadru competitiv, de testare, care încurajează colaborarea și schimbul de experiență.

Astfel, UNbreakable joacă un rol important în scăderea decalajului forței de muncă în securitate cibernetică pe plan local și internațional.

UNbreakable România 2024 pe scurt

- UNbreakable este cel mai complex program de securitate cibernetică pentru liceenii și studenții din România;
- A început ca un simplu concurs de tip Capture the Flag; primele ediții pilot au avut loc în 2020, cu 500 de participanți;
- S-a dezvoltat treptat într-un program care, înaintea celor două faze de competiție – un concurs individual și unul pe echipe, ambele în format online –, a introdus și o etapă de pregătire, un bootcamp în care tinerii să poată accesa resurse teoretice, exerciții și webinarii pentru a se pregăti atât pentru concursurile amintite, cât și pentru cariera lor în securitate cibernetică;
- Prin formatul programului și prin resursele pe care le oferă, a devenit o experiență valoroasă de învățare, apreciată de către toți participanții;
- Prin rezultatele obținute de către tineri, este un program care ne motivează să ne uităm cu încredere spre viitorul industriei de securitate cibernetică;
- Vestea și mai bună care completează lista de mai sus este că ediția din 2024 a UNbreakable România a dus programul la următorul nivel.

Cum se desfășoară UNbreakable România?

1

Etapa de pregătire (online)

Participanții au acces la module teoretice și practice pentru a se familiariza atât cu formatul și metodologia concursului, cât și cu domeniul securității cibernetice. Ei pot interacționa cu mentori (experți din industrie și alumni din comunitate), pot participa la webinarii susținute de aceștia și pot rezolva exerciții pe platforma tehnică educațională CyberEDU.

2

Concursul individual (online)

Participanții vor concura 48 de ore. Obiectivul este de a rezolva cât mai multe exerciții de securitate cibernetică și de a trimite cât mai multe „steaguri" (soluții corecte) pentru a se situa in topul clasamentului. În această etapă, se evaluează performanța la nivel individual, competențele și abilitățile tehnice, ca mai apoi fiecare participant să știe ce cunoștințe trebuie aprofundate.

3

Finala concursului

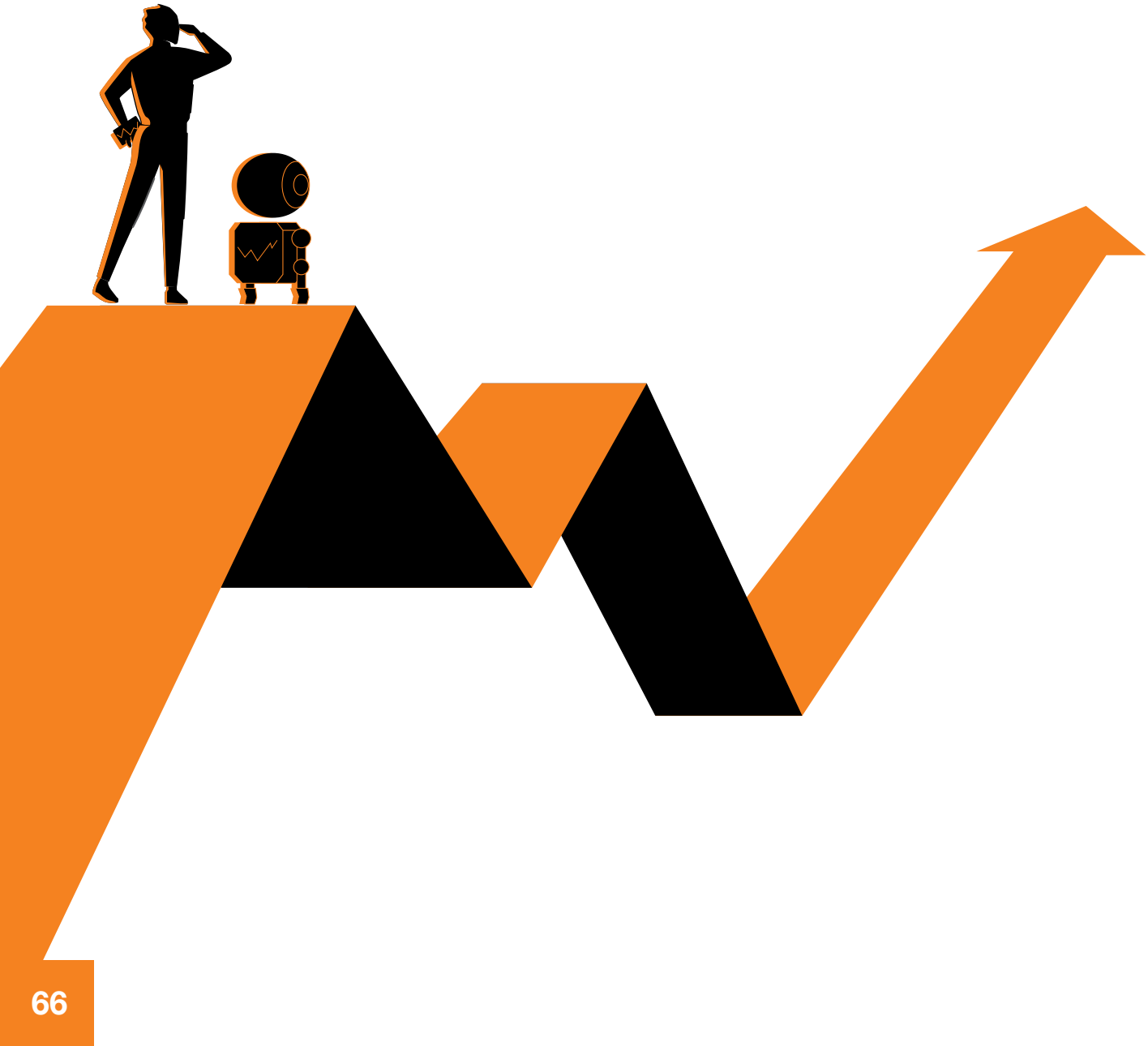
Pentru ca participanții din primele trei faze ale acestui program să aibă parte de o experiență competițională autentică și pentru a avea ocazia de a cunoaște și relaționa direct cu tineri care împărtășesc pasiunea pentru securitate cibernetică, ediția din 2024 a UNbreakable România a introdus și o etapă de tip FINALĂ, sub forma unei competiții pe echipe în format fizic. În cadrul finalei se califică doar primele 15 echipe (LICEU + UNIVERSITATE) clasate în top la competiția online pe echipe.

Rezultatele ediției 2024:

- 1,400 tineri înscriși
- 150 de exerciții
- 20 de mentori
- 17 webinarii
- 192 de licee
- 31 de universități
- 41 de județe
- 20 de exerciții
- 839 de participanți

Orange Fab – accelerează inovația în securitate cibernetică

Programul Orange Fab susține start-upurile inovatoare din domeniul securității cibernetice pentru a dezvolta soluții ce protejează spațiul digital. Într-un peisaj online în continuă schimbare, securitatea este esențială. Cu Orange Fab, ajutăm start-upurile să dezvolte tehnologii capabile să contracareze amenințările cibernetice moderne.



De ce să alegi Orange Fab?

Orange Fab oferă mai mult decât resurse – pune la dispoziție o rețea globală, expertiză de industrie și sprijin personalizat pentru a asigura succesul start-upurile în domeniul securității.

Prin programul nostru, start-upurile beneficiază de:

- **Mentorat specializat.** Acces direct la experți în securitate cibernetică și mentori din ecosistemul Orange.
- **Rețea globală.** Conexiuni cu baza de clienți și partenerii Orange din întreaga lume.
- **Proiecte proof of concept pentru clienții Orange.** Sprijin pentru a dezvolta soluții și a genera impact real.
- **Vizibilitate în industrie.** Creșterea notorietății prin asocierea cu un brand de încredere, cu o prezență globală.

Pentru cine este Orange Fab?

Căutăm start-upurile vizionare care dezvoltă soluții inovatoare de securitate – de la inteligență cibernetică și criptare, la protecția identității și gestionarea riscurilor. Dacă lucrezi la soluții care abordează provocările cibernetice actuale, Orange Fab te poate sprijini să crești.

Construim împreună viitorul securității digitale

Lumea digitală are nevoie de lideri în securitate cibernetică acum mai mult ca niciodată. Dacă start-upul tău este pregătit să facă un pas înainte și să creeze un impact real, aplică la Orange Fab. Împreună vom construi un viitor digital mai sigur.

Contactează-ne chiar azi!

Ești pregătit să contribui la securizarea lumii digitale? Alătură-te Orange Fab și începe-ți călătoria spre inovație în securitatea cibernetică.

Aplică acum:

Proiectele Orange în cercetare și inovare

Orange România este unul dintre cei mai activi participanți la Acțiunile de Cercetare și Inovare finanțate de Uniunea Europeană, cu un istoric impresionant în furnizarea de capabilități avansate de experimentare și validare a scenariilor de utilizare pentru tehnologiile inovatoare. Infrastructura noastră din 5G Lab din București și Iași oferă servicii de ultimă generație pentru dezvoltarea, testarea și validarea tehnică și comercială a noilor tehnologii în domeniile complexe ale rețelelor viitorului, ale rețelelor multi-domain, ale tehnologiilor IoT, dar și ale securității cibernetice.

Orange România, alături de partenerii săi din mediile academice și antreprenoriale, livrează cercetare în tehnologii avansate, în 16 proiecte în desfășurare în cadrul Horizon Europe, Digital Europe Programme și Connecting Europe Facility.

RIGOUROUS

Proiectul RIGOUROUS propune crearea unei platforme menite să identifice și să abordeze riscurile majore de securitate cibernetică, încredere și confidențialitate care amenință rețelele, dispozitivele și infrastructura de calcul ce vor susține următoarele generații de servicii de telecomunicații. RIGOUROUS va aborda aceste provocări prin introducerea unui nou cadru de servicii holistice și inteligente care utilizează noi mecanisme de învățare automată (ML) și inteligență artificială, care pot reacționa în mod dinamic la suprafața de amenințare în continuă schimbare la toate nivelurile de orchestrare și în toate funcțiile de rețea.

Pe scurt, RIGOUROUS vizează următoarele obiective principale:

- Cadrul holistic de servicii inteligente pentru securizarea managementului ciclului de viață al continuumului IoT-Edge-Cloud
- Integrarea principiilor DevSecOps în ciclul de operare al platformei RIGOUROUS
- Orchestrarea automată a securității, managementul încrederii și implementarea sunt bazate pe modele și pe inteligență artificială
- Strategii avansate de detectare, decizie și atenuare a anomaliilor bazate pe inteligență artificială
- Demonstrarea unui set de cazuri de utilizare relevante din punct de vedere industrial în medii operaționale

RIGOUROUS este finanțat prin Programul UE pentru Cercetare și Inovare Orizont 2020 în baza Acordului de finanțare nr. 856709.

https://rigourous.eu/

DYNABIC

Obiectivul strategic al DYNABIC este de a crește reziliența și capabilitățile de continuitate a activității ale serviciilor esențiale europene în fața amenințărilor cibernetice și fizice avansate. Acest obiectiv va fi urmărit prin furnizarea de noi metode, modele și instrumente socio-tehnice pentru a sprijini reziliența prin gestionarea și controlul holistic al riscurilor de continuitate a activității în timpul funcționării și prin adaptarea dinamică a răspunsurilor la nivel de sistem, uman și organizațional.

DYNABIC stabilește un set de obiective specifice, menite să ofere cadrul DYNABIC pentru asigurarea unei rezilienţe sporite a sistemelor critice, asigurând în același timp continuitatea activității și a operațiunilor prin adaptarea dinamică și inteligentă a răspunsurilor sistemului, ale oamenilor și ale organizațiilor.

Acest lucru va permite operatorilor de servicii esențiale să prezică, să evalueze cantitativ și să

atenueze în timp real riscurile de continuitate a activității și potențialele lor efecte în cascadă, folosind o nouă serie de metode și instrumente care permit pregătirea pentru intervenție în caz de dezastre în infrastructurile critice și îmbunătățind prevenirea riscurilor de continuitate a activității în incidente și atacuri între organizații și domenii.

Acest proiect a primit finanțare prin Programul UE pentru Cercetare și Inovare Orizont Europa în baza acordului de finanțare nr. 101070455.

https://dynabic.eu/

ADROIT-6G

Scopul ADROIT6G este de a demonstra aplicațiile cu nivel scăzut de maturitate tehnologică pentru viitoarea rețea 6G, folosind o nouă abordare cognitivă bazată pe inteligența artificială distribuită. Proiectul își propune să îmbunătățească performanța și controlul în interacțiunile cu serviciile digitale și să susțină aplicațiile de viitor.

Obiectivele proiectului vor fi atinse prin implementarea a trei cazuri de utilizare:

- PoC 1 Realitate extinsă imersivă (XR)
- PoC 2 IoT industrial (IIoT)
- PoC 3 Roboți colaborativi (coboți) în construcții

Proiectul ADROIT6G a primit finanțare de la Întreprinderea comună pentru rețele și servicii inteligente (SNS JU) în cadrul Programului UE pentru Cercetare și Inovare Orizont Europa în temeiul acordului de finanțare nr. 101095363.

https://adroit6g.eu/

TrialsNet

Viziunea proiectului TrialsNet este de a permite realizarea unor valori societale convingătoare prin punerea în aplicare a aplicațiilor 5G și ulterioare, care vor fi demonstrative pentru tranziția către următoarea generație de rețele mobile. Prin testele sale la scară largă cu industrii verticale în cele trei domenii: i) Infrastructură, Transport, Securitate și Siguranță, ii) E-sănătate și Situații de urgență și iii) Cultură, Turism și Divertisment, TrialsNet va fi mijlocul de conectare a lumii digitale cu lumile fizice și naturale.

Vor exista 13 cazuri de utilizare care vor acoperi trei domenii menționate anterior și care vor fi dezvoltate în patru țări. În România, la Iași, vom găzdui 2 dintre cele 13 cazuri de utilizare, unul privind monitorizarea inteligentă a mulțimilor și celălalt legat de dezvoltarea unei soluții de management inteligent al traficului.

Proiectul TrialsNet a primit finanțare prin Programul UE pentru Cercetare și Inovare Horizon-JU-SNS-2022 în baza acordului de finanțare nr. 101095871.

https://trialsnet.eu/

6Green

În cadrul proiectului 6Green, ne-am asumat obiectivul de a reduce amprenta de carbon calculată, în comparație cu 5G, de 10 ori mai mult.

Eficiența provine din utilizarea extinsă a soluțiilor de tip „cloud-native”, care plasează aplicațiile de afaceri și de consum la marginea rețelei, mai aproape de utilizatorii finali, și sunt capabile să decidă în mod autonom și proactiv cum să direcționeze traficul utilizatorilor într-un mod eficient și cum să reducă resursele care nu sunt utilizate.

Viitoarele rețele 6G vor fi, de asemenea, conștiente de emisiile de carbon legate de deciziile automate de calcul pe care le pot lua, astfel încât să utilizeze energia în cel mai eficient mod.

Toate aceste acțiuni vor fi posibile prin utilizarea extinsă a algoritmilor ML, care vor învăța în mod activ din funcționarea rețelei și vor lua decizii pe baza informațiilor primite de la toate părțile interesate (operatori de rețele mobile, întreprinderi și proprietari de aplicații comerciale).

Acest proiect a primit finanțare prin Programul UE pentru Cercetare și Inovare Orizont Europa în baza acordului de finanțare nr. 101096925.

https://www.6green.eu/

SOCCER

Proiectul „Consolidarea capacităților centrelor operaționale de securitate pentru reziliența europeană - SOCCER”, creat pentru a răspunde la propunerea europeană DIGITAL- ECCC-2022-CYBER-03-SOC - Consolidarea capacității centrelor operaționale de securitate (SOC) - reunește un consorțiu de experți în securitate cibernetică și în tehnologie din Germania, Franța, Ungaria și România.

Pe parcursul a 36 de luni, propunerea noastră urmărește:

- Să dezvolte și să implementeze tehnologii de ultimă oră pentru accesul securizat la date (Centrul de securitate) și partajarea semnalelor de investigare a amenințărilor (TIS) între entitățile europene, permițând monitorizarea și detectarea amenințărilor cibernetice de către capacitățile consolidate.

- Să interconecteze și să consolideze ecosistemele avansate ale Centrelor de operațiuni de securitate (SOC) din Germania, Ungaria și România, cu scopul de a spori reziliența securității cibernetice atât la nivel național, cât și la nivelul UE.

Acest proiect a primit finanțare prin Programul UE Europa Digitală în baza acordului de finanțare nr. 101127847.

https://soccer.sztaki.hun-ren.hu/

CYRESRANGE

Proiectul răspunde preocupărilor și directivelor europene în domeniul securității cibernetice, ca urmare a îndeplinirii unor cerințe sinoptice la nivelul UE, exprimate prin Strategia Cibernetică a UE prezentată de Comisia Europeană și de Înaltul Reprezentant al Uniunii pentru afaceri externe și politică de securitate pentru „a construi reziliența la amenințările cibernetice și a se asigura că cetățenii și întreprinderile beneficiază de tehnologii digitale de încredere”, unde „suveranitatea tehnologică a UE trebuie să se bazeze pe reziliența tuturor serviciilor și produselor conectate”.

Arhitectura consorțiului de proiect și participarea unui grup de excelență în domeniul securității cibernetice, cu o largă reprezentare la nivel național și european, asigură îndeplinirea unei premise a strategiei UE în domeniul securității cibernetice: „Toate cele patru comunități cibernetice - cele care se ocupă de piața internă, de aplicarea legii, de diplomație și de apărare - trebuie să colaboreze mai strâns în vederea unei conștientizări comune a amenințărilor. Acestea ar trebui să fie pregătite să răspundă în mod colectiv atunci când se materializează un atac, astfel încât UE să fie mai mare decât suma părților sale.”

Propunerea noastră de proiect abordează primul obiectiv de consolidare a capacității actorilor din domeniul securității cibernetice de a reacționa în mod coordonat la incidente de securitate cibernetică la scară largă, promovând în același timp rolul CSIRT-urilor, al rețelei CyCLONe și luând în considerare Planul de acțiune. Proiectul nostru va pune la dispoziția părților interesate un set de metodologii structurate, baze de date de vulnerabilități și instrumente criminalistice, precum și obiective și instrumente de furnizare automată de conținut.

Proiectul se concentrează pe crearea de noi paradigme privind crearea, interconectarea și consolidarea unor game de securitate cibernetică la nivel național și regional cu mari capacități în domeniul european, inclusiv în ceea ce privește infrastructurile critice, fără a se limita doar la sectoarele reglementate de Directiva NIS.

Acest proiect a primit finanțare prin Programul UE Europa Digitală în baza acordului de finanțare nr. 101128088.

https://cyresrange.net/

iSEE-6G

iSEE-6G se extinde dincolo de JCS (comunicare și detecție în comun) și propune o platformă radio unificată JCCSP (comunicare, calcul, detecție și transfer de energie în comun), care include toate elementele de suport ale soluțiilor propuse în viitoarele rețele 6G. Prin integrarea, exploatarea și susținerea tehnologiilor de bază 6G, iSEE-6G oferă:

- Noi soluții de suprafețe inteligente reconfigurabile (RIS) și sisteme agile de filtrare spațială orientate spre JCCSP
- Designul nivelului fizic optimizat prin JCCSP, inclusiv designul formei de undă, designul structurii cadrului, modelarea canalelor, precodificarea/filtrarea spațială în ceea ce privește paradigma arhitecturală a rețelei de acces radio deschise (O-RAN)
- Proiectarea schemelor încrucișate activate de JCCSP cu noi capabilități în ceea ce privește arhitectura de rețea orientată spre servicii
- Soluții la nivel de sistem implementate prin JCCSP pentru furnizarea de noi funcționalități către o rețea 6G fără celule

Validarea conceptului (PoC) iSEE-6G se axează pe cazurile de utilizare JCCSP de pe coridoarele aeriene, unde vehiculele aeriene fără echipaj cu diferite roluri care oferă diferite servicii coexistă și se coordonează între ele. În cadrul bancului de testare al Orange România, JCCSP bazată pe forme de undă 5G exploatează capacitățile de colectare ale indicatorilor cheie de performanță ai acesteia. Utilizarea bancului de testare va fi extinsă într-un loc în aer liber, unde vor fi utilizate vehicule aeriene fără echipaj și dispozitive IoT pentru a testa capabilitățile de transfer de energie fără fir (WPT). Se utilizează puterea de calcul Edge pentru monitorizarea serviciilor de Protecție Publică și Asistență în caz de Dezastre (PPDR) și implementarea JCCSP ca serviciu.

Acest proiect a primit finanțare prin Programul UE pentru Cercetare și Inovare Orizont Europa în baza acordului de finanțare nr. 101139291.

https://isee6g.eu/

6G-PATH

Drumul spre 6G începe acum, când 5G s-a maturizat și este implementat la nivel mondial, atât în sectorul public, cât și în cel privat. Cu toate că 5G a făcut un pas înainte în multe domenii, cum ar fi performanța și eficiența, comunitatea în general se așteaptă întotdeauna la mai mult din punct de vedere al eficienței și din punct de vedere al performanței din partea industriei și a furnizorilor de tehnologie care doresc să își îmbunătățească în continuare ofertele și produsele. Cererile continue pentru o rată de transfer mai mare, o latență mai mică și comunicații mai eficiente din punct de vedere energetic trebuie să fie susținute de cazuri de utilizare relevante care să poată susține și să demonstreze necesitatea acestor cereri.

Obiectivul 6G-PATH este de a contribui la promovarea dezvoltării și integrării în continuare a unor instrumente și produse noi și îmbunătățite ale companiilor din UE cu 5G/6G, măsurând în același timp indicatorii cheie de performanță și elementele de valoare cheie relevante. Pentru a realiza acest lucru, unele bancuri de testare vor face parte din consorțiul de proiect, care va fi utilizat în cazurile de utilizare corespunzătoare, răspândite în patru industrii verticale importante: sănătate, educație, orașe inteligente și agricultură.

6G-PATH intenționează să colaboreze îndeaproape cu alte proiecte Stream-B și Stream-C în curs de desfășurare/în curs de demarare, într-o buclă de feedback, în cadrul căreia inovațiile pe care partenerii le realizează în alte proiecte pot fi implementate și testate în continuare prin grupul nostru de cazuri de utilizare și propuneri deschise, împărtășind în același timp rezultatele noastre pentru a consolida și mai mult inovația în curs de realizare.

Acest proiect a primit finanțare prin Programul UE pentru Cercetare și Inovare Orizont Europa în baza acordului de finanțare nr. 101139172.

https://6gpath.eu/

6G-INTENSE

Rețelele inteligente 6G ale viitorului vor oferi o infrastructură de înaltă performanță și eficientă din punct de vedere energetic pe care vor putea fi dezvoltate și implementate serviciile de internet de generație următoare și alte servicii. 6G va promova o revoluție industrială și o transformare digitală și va accelera construirea de societăți inteligente care vor duce la îmbunătățirea calității vieții, facilitând sistemele autonome, comunicarea haptică și asistența medicală inteligentă.

Pentru a atinge obiectivele într-un mod sustenabil, este bine înțeles că sunt necesare noi abordări în ceea ce privește modul în care infrastructurile de telecomunicații sunt arhitecturate, federalizate și orchestrate.

Aceste noi abordări necesită ecosisteme cu mai multe părți interesate care să promoveze sinergii între operatorii de rețele mobile și proprietarii de toate tipurile de resurse de calcul și de rețea, care vor împărți costurile extraordinare ale unei noi generații de upgrade de la 5G la 6G, facilitând în același timp noi modele de afaceri. Este clar că noile paradigme de arhitectură aduc o complexitate fără precedent din cauza dimensiunii și eterogenității domeniilor de orchestrare implicate, care ar trebui să fie însoțite de capacități de automatizare la fel de performante. Astfel, 6G vizează „Sfântul Graal” al inteligenței omniprezente bazate pe inteligență artificială, denumită inteligență artificială nativă. Cu toate acestea, infrastructurile cu mai multe părți interesate prevăzute în 6G, conform conceptului de „rețea de rețele”, vor adăuga un nivel de complexitate fără precedent în materie de gestionare, din cauza dimensiunii și eterogenității domeniilor de orchestrare implicate.

Acest proiect a primit finanțare prin Programul UE pentru Cercetare și Inovare Orizont Europa în baza acordului de finanțare nr. 101139266.

https://6g-intense.eu/

6G-MUSICAL

6G-MUSICAL este un proiect revoluționar care îmbină tehnologiile de radiodetecție și de comunicare pentru a crea noi paradigme în domeniul comunicațiilor radio. Acesta urmărește să echipeze nodurile periferice de infrastructură ale 6G cu elemente integrate de radiodetecție bazate pe radiofrecvență/radar care colaborează cu componentele de comunicații. Acest lucru permite localizarea, urmărirea obiectelor și crearea de imagini 3D, cu o precizie și o rezoluție de nivel CM. Ca atare, proiectul va investiga noi arhitecturi de sistem și semnale eficiente din punct de vedere spectral și energetic, pentru a facilita comunicațiile de mare viteză în benzi de frecvențe multiple, integrate cu detectare și localizare precisă.

În domeniul comunicațiilor wireless, proiectul va defini noi forme de undă adecvate pentru radiodetecție și comunicații, va exploata tehnici de detecție compresivă și va defini algoritmi de detecție și localizare multimodală cooperativă. În domeniul rețelelor, se va pune accentul pe procedurile de sincronizare/calibrare între nodurile periferice și pe tehnicile de compresie pentru a permite transportul cu costuri reduse al informațiilor colectate către un centru de fuzionare a datelor.

Acest proiect a primit finanțare prin Programul UE pentru Cercetare și Inovare Orizont Europa în baza acordului de finanțare nr. 101139176.

https://6gmusical.eu/

HEAT

Proiectul propune crearea unor platforme OSS pentru a permite dezvoltarea unor tehnologii imersive, de tip XR și VR pentru captura, procesarea și transmiterea experiențelor vizuale, auditive și senzoriale inedite.

Alături de partenerii din România – Universitatea Transilvania din Brașov, la Orange urmărim dezvoltarea și pilotarea unor scenarii de utilizare care ne vor permite să transmitem conținut avansat, de tip XR – extended reality, prin rețelele noastre 5G, de la evenimente artistice precum Transilvania Blues Festival Brașov.

Acest proiect a primit finanțare prin Programul UE pentru Cercetare și Inovare Orizont Europa în baza acordului de finanțare nr. 101135637.

https://www.immersion.fr/en/heat-hybrid-extended-reality/

5G Connect Danube Delta

Comunitățile din Delta Dunării vor avea acces la tehnologia 5G Orange prin intermediul unui proiect cu finanțare europeană. Beneficiile proiectului 5G Connect Danube Delta* (5G-CDD) se vor reflecta în patru arii majore: educație digitală, telemedicină, turism lent și monitorizarea mediului înconjurător.

Proiectul este unic în România și se va derula pe o perioadă de trei ani, din octombrie 2024 până în septembrie 2027, cu o valoare totală de aprox. 3,5 milioane de euro.

Consorțiul de parteneri coordonați de Orange România include Fundația Orange, Asociația Ivan Patzaichin Mila23, Universitatea Națională de Științe și Tehnologie Politehnica București, Virtual Board, alături de partenerii asociați Consiliul Județean Tulcea și Telios Care.

Proiectul presupune instalarea unei infrastructuri comerciale bazate pe 5G Stand Alone și Edge Cloud în 19 localități din județul Tulcea. Implementarea unei rețele 5G Stand Alone reprezintă o provocare tehnică datorită dificultăților geografice, fiind totodată o premieră pentru industria telecomunicațiilor din România. Aceasta implică utilizarea unor componente noi de rețea core ce îmbunătățesc considerabil performanțele față de rețelele 5G Non-Standalone existente. Totodată, tehnologia Edge Cloud reduce distanța dintre utilizatori și servicii, asigurând latențele și viteza necesare pentru aplicațiile proiectului 5G Connect Danube Delta.

Proiectul 5G-CDD reprezintă o inițiativă crucială pentru regiunea Deltei, o zonă caracterizată de multiple provocări socio-economice datorate izolării, depopulării și lipsei oportunităților de angajare. Prin implementarea tehnologiei 5G și integrarea aplicațiilor de educație digitală, telemedicină, turism și monitorizare ambientală, obiectivul proiectului este de a contribui la transformarea arealului, oferind soluții inovative pentru o parte din problemele cu care se confruntă acum comunitățile locale. Numărul beneficiarilor direcți și indirecți se ridică la aproximativ 20.000 de persoane.

5G-CDD are drept obiectiv construirea unei infrastructuri de conectivitate 5G (5G Stand Alone și Edge Cloud), în mai multe localități preponderent greu accesibile și plasate în zona umedă a Deltei, sporind calitatea vieții locuitorilor, ajutând în același timp la îmbunătățirea oportunităților de business și angajare din regiune.

Telemedicină

Tehnologia de internet de mare viteză va permite conectarea dispozitivelor medicale existente prin laptopuri / tablete compatibile 5G, implementarea unei aplicații mobile de control medical la distanță, folosirea soluțiilor de telemedicină Telios Care și implementarea conceptului de Point of Care (punct de ajutor medical). Această intervenție se va implementa în 10 unități medicale.

Educație digitală

Prin amplificarea activităților în cadrul hubului educațional Orange Digital Center în Mila 23, la Centrul de Inovare Comunitară, Fundația Orange va valorifica conținutul educațional gratuit disponibil pe Platforma Digitaliada și va facilita colaborarea în timp real între elevi și profesori prin predare hibridă, inclusiv prin integrarea platformei de predare online VBoard. În plus, aici va fi pilotată aplicația de educație VR, dezvoltată în cadrul proiectului 6G-PATH**, într-o școală din județul Tulcea. Grupul țintă îl reprezintă peste 2000 de beneficiari din 17 școli și cursanți din Orange Digital Center.

Turism lent

Asociația Ivan Patzaichin Mila 23 va dezvolta aplicația de mobil MILA23 care va îmbunătăți experiența turiștilor din Delta Dunării prin furnizarea de conținut educațional, rute și puncte de interes, cu funcții de geo-fencing și de raportare a evenimentelor periculoase. De asemenea, vor fi monitorizate punctele de interes turistic cu ajutorul camerelor de supraveghere inteligente compatibile 5G.

Monitorizare de mediu

Principalele zone protejate vor fi dotate cu senzori de monitorizare a mediului conectați la routere 5G. Tehnologia modernă va permite și îmbunătățirea condițiilor hidrologice locale, a curățeniei suprafeței apei și a culturilor naturale de stuf. Această componentă are la bază proiectul DaWetRest, în care UNSTPB este partener.

Prin implicarea și sprijinul autorităților locale, proiectul 5G-CDD va reprezenta un pas important în adresarea specificităților regiunii și în exploatarea potențialului său unic prin tehnologie avansată.

*Proiectul 5G Connect Danube este finanțat prin programul Connecting Europe Facility al Comisiei Europene, cadrul 5G and Edge Cloud for Smart Communities, Grant Agreement 101181137.

14. European Cyber Security Challenge 2024

European Cyber Security Challenge (ECSC) este o competiție anuală care reunește tineri talentați din întreaga Europă, pasionați de securitatea cibernetică. Ediția din 2024 a avut loc în Torino, Italia, și a oferit participanților o platformă excelentă pentru a-și testa cunoștințele și abilitățile într-un mediu competitiv și colaborativ. ECSC a fost inițiată cu scopul de a crea o comunitate europeană puternică în domeniul securității cibernetice. Competiția a cunoscut o creștere semnificativă în popularitate de-a lungul anilor, atrăgând un număr din ce în ce mai mare de participanți din întreaga Europă. România participă la ECSC de la ediția din 2015 și suntem una dintre echipele cu un parcurs bun și constant. Deși am scris în multe rânduri despre prezența **#teamromania** în această competiție, pentru această primă ediție în limba română a raportului BIS, am decis să vă povestim, în detaliu, despre multe dintre lucrurile ce fac ECSC o competiție atât de importantă pentru performanța în securitate cibernetică, în România.

Ce este ECSC?

ECSC este mai mult decât o simplă competiție. Este un eveniment care:

- **Promovează talentul.** Atrage tineri cu vârste cuprinse între 14 și 24 de ani, oferindu-le oportunitatea de a-și demonstra abilitățile în domeniul securității cibernetice.
- **Stimulează colaborarea.** Echipele formate din 10 membri (5 juniori și 5 seniori) lucrează împreună pentru a rezolva provocări complexe.
- **Oferă experiență practică.** Participanții se confruntă cu sarcini realiste din domenii precum securitatea web, securitatea mobilă, criptografie, reverse engineering și forensics.
- **Creează o comunitate.** Evenimentul facilitează networking-ul între tineri pasionați de cybersecurity, creând o comunitate puternică.

Cum decurge competiția?

Competiția se desfășoara pe parcursul a câteva zile și implică:

- **Rezolvarea de provocări.** Echipele trebuie să rezolve o serie de sarcini tehnice într-un timp limitat.
- **Colectarea de puncte.** Fiecare sarcină rezolvată corect aduce echipei un anumit număr de puncte.
- **Clasament.** Echipele sunt clasate în funcție de numărul total de puncte obținute.

De ce este importantă această competiție?

ECSC joacă un rol crucial în:

- **Identificarea viitorilor experți în cybersecurity.** Competiția ajută la descoperirea și dezvoltarea tinerelor talente în acest domeniu.
- **Îmbunătățirea nivelului de securitate cibernetică.** Prin promovarea educației și a competiției în domeniul cybersecurity, ECSC contribuie la creșterea nivelului de securitate cibernetică în Europa.
- **Crearea unei forțe de muncă calificată.** Evenimentul ajută la pregătirea unei noi generații de specialiști în cybersecurity, care sunt atât de necesari în lumea digitală de astăzi.

Ce este o competiție CTF?

Capture the Flag (CTF) este un tip de competiție în securitatea cibernetică în care participanții, individual sau în echipă, încearcă să rezolve o serie de provocări tehnice. Scopul este de a „captura steaguri” – fragmente de cod sau informații ascunse – care demonstrează rezolvarea cu succes a unei sarcini. Aceste sarcini pot varia de la exploatarea vulnerabilităților în aplicații web până la analiza de trafic de rețea sau decriptarea mesajelor.

De ce sunt importante competițiile CTF?

- **Dezvoltarea abilităților.** CTF-urile oferă o platformă excelentă pentru a-ți îmbunătăți abilitățile tehnice în domeniul securității cibernetice, precum programare, rețele, criptografie și forensics.
- **Gândire critică.** Rezolvarea provocărilor CTF necesită gândire logică, creativitate și abilitatea de a te adapta la situații noi.
- **Lucru în echipă.** Multe competiții CTF se desfășoară în echipă, ceea ce încurajează colaborarea și comunicarea eficientă.
- **Networking.** CTF-urile sunt o modalitate excelentă de a cunoaște alți pasionați de securitate cibernetică și de a-ți extinde rețeaua de contacte.

Tipuri de provocări într-un CTF

- **Web.** Exploatarea vulnerabilităților în aplicații web, cum ar fi injecțiile SQL, XSS sau CSRF. Provocările de tip web reprezintă o parte esențială a competițiilor CTF (Capture the Flag). Ele simulează scenarii reale de hacking, unde participanții trebuie să identifice și să exploateze vulnerabilități în aplicații web pentru a obține acces neautorizat și a „captura steagul” – un fragment de cod care confirmă rezolvarea cu succes a provocării.

  Tipuri comune de provocări web în CTF

  - **Injecții SQL.** Exploatarea vulnerabilităților în interogările SQL pentru a obține acces neautorizat la baza de date.
  - **XSS (Cross-Site Scripting).** Injectarea de cod client-side (de obicei JavaScript) într-o pagină web vulnerabilă, pentru a fura cookie-uri, a redirecționa utilizatori sau a executa alte acțiuni malițioase.
  - **CSRF (Cross-Site Request Forgery).** Induce un utilizator autentificat să execute acțiuni nedorite pe un site web, cum ar fi transferul de fonduri sau schimbarea parolei.
  - **Includere de fișiere locale.** Exploatarea unei aplicații web pentru a include și executa fișiere arbitrare de pe server.
  - **Bypass de autentificare.** Ocolirea mecanismelor de autentificare pentru a obține acces la zone restricționate ale aplicației.
  - **Vulnerabilități în framework-uri.** Exploatarea vulnerabilităților specifice framework-urilor web populare, precum WordPress, Drupal sau Laravel.
  - **Logic flaws.** Identificarea și exploatarea erorilor logice în codul aplicației, cum ar fi condiții de cursă sau divizarea prin zero.
  - **Reversing.** Analiza codului binar pentru a descoperi funcționalități ascunse sau vulnerabilități. **Reverse engineering,** sau **inginerie inversă**, este procesul de a analiza un program sau un sistem pentru a înțelege cum funcționează, fără a avea acces la codul sursă original. În cadrul competițiilor CTF, aceste provocări implică dezasamblarea de programe binare pentru a descoperi funcționalități ascunse, algoritmi, chei de criptare sau vulnerabilități exploatabile.
  - **Analiza de malware.** Participanții trebuie să analizeze un fișier malware pentru a înțelege comportamentul său, a identifica funcționalitățile malițioase și, eventual, a dezvolta un antidot.
  - **Cracking de programe.** Participanții trebuie să găsească o modalitate de a ocoli protecțiile unui program (cum ar fi seriale, keygenuri) pentru a obține funcționalitatea completă.
  - **Reversarea de firmware.** Analiza firmware-ului dispozitivelor embedded (cum ar fi routere, IoT devices) pentru a descoperi vulnerabilități sau a modifica comportamentul dispozitivului.
  - **Analiza de protocoale.** Dezasamblarea și analiza traficului de rețea pentru a înțelege protocoalele utilizate și a identifica potențiale vulnerabilități.

- **Pwning** în contextul competițiilor CTF se referă la exploatarea unor vulnerabilități la nivel de sistem de operare pentru a obține controlul total asupra unui sistem. Este una dintre cele mai complexe și prestigioase categorii de provocări, necesitând o înțelegere profundă a arhitecturii sistemelor de operare, a exploiturilor și a tehnicilor de exploatare.

Ce înseamnă să "pwnezi" un sistem?

Când spui că ai "pwnat" un sistem, înseamnă că ai reușit să:

- **Execuți cod arbitrar.** Ai introdus și executat propriul cod pe sistemul țintă, oferindu-ți astfel control deplin asupra acestuia.
- **Obții acces root.** Ai obținut cele mai înalte privilegii de acces pe sistem, care îți permit să faci orice operațiune.
- **Citești sau scrii în memorie restricționată.** Ai accesat zone ale memoriei care nu sunt accesibile în mod normal și astfel poți manipula datele și modifica comportamentul programului.

Tipuri comune de vulnerabilități exploatate în provocările de pwning:

- **Buffer overflows.** O eroare de programare care permite scrierea de date dincolo de o zonă alocată în memorie, ceea ce poate duce la suprascrierea informațiilor din memorie, pointeri sau alte date critice.
- **Use-after-free.** Exploatarea unei zone de memorie care a fost eliberată, dar la care se face în continuare referire.
- **Integer overflows.** Exploatarea erorilor în operațiile aritmetice cu numere întregi, care pot duce la comportament neașteptat.
- **Format string vulnerabilities.** Exploatarea funcțiilor de formatare a șirurilor de caractere pentru a executa cod arbitrar.
- **Heap overflows.** Similar cu buffer overflows, dar se referă la zone de memorie alocate din heap.

- **Provocările de criptografie în cadrul competițiilor CTF** implică descifrarea de mesaje criptate, analiza de algoritmi și protocoale criptografice, precum și descoperirea de vulnerabilități în sistemele criptografice.

Tipuri de provocări de criptografie în CTF:

- **Cifruri clasice.** Cifruri simple, precum Cezar, Vigenère, substituție, care necesită aplicarea unor tehnici de criptanaliză manuale sau cu ajutorul unor scripturi simple.
- **Cifruri moderne.** Algoritmi criptografici mai complecși, cum ar fi AES, RSA, folosind diferite moduri de operare și parametri.
- **Hash-uri.** Analiza funcțiilor de hash (MD5, SHA-1, SHA-256) pentru a identifica coliziuni sau a recupera date din hash-uri.
- **Steganografie.** Extragerea de informații ascunse în imagini, audio sau alte fișiere.
- **Protocoale criptografice.** Analiza și exploatarea vulnerabilităților în protocoale precum SSL/TLS, SSH.

- **Forensics.** Analiza de imagini disk, pachete de rețea sau alte artefacte digitale pentru a extrage informații relevante.

Tipuri de provocări de forensics în CTF:

- **Analiza imaginilor de disc.** Investigarea unei imagini a unui hard disk pentru a găsi fișiere șterse, activități suspecte, sau pentru a reconstrui un sistem de fișiere.
- **Analiza pachetelor de rețea.** Studierea unei capturi de pachete de rețea pentru a identifica tipurile de trafic, protocoalele utilizate, și pentru a descoperi atacuri în curs.
- **Analiza memoriei.** Investigarea unor dumpuri de memorie pentru a găsi procese suspecte, injecții de cod sau alte indicii despre un atac.
- **Analiza de log-uri.** Studierea fișierelor log pentru a identifica activități neobișnuite, erori sau atacuri.
- **Steganografie.** Extragerea de informații ascunse în imagini, audio sau alte fișiere.

- **Misc.** Categoria Miscellaneous în cadrul competițiilor CTF reprezintă o categorie variată, care poate include orice tip de provocare care nu se încadrează în celelalte categorii tradiționale, cum ar fi Web, Crypto, Reverse, Pwning sau Forensics. Această categorie poate fi considerată o "cutie neagră" de provocări, adesea necesitând gândire laterală, creativitate și cunoștințe diverse.

Tipuri comune de provocări Misc într-un CTF:

- **Puzzle-uri logice.** Provocări care necesită rezolvarea de enigme, rebusuri sau jocuri de logică.
- **Trivia.** Întrebări de cultură generală sau legate de subiecte specifice.
- **Jocuri.** Provocări care implică jocuri simple, cum ar fi tic-tac-toe, Sudoku sau jocuri de cărți.
- **Steganografie.** Ascunderea de informații în imagini, audio sau alte fișiere.
- **Provocări legate de hardware.** Sarcini care implică interacțiunea cu dispozitive hardware sau circuite electronice.
- **Provocări legate de limbaje de programare.** Sarcini care necesită cunoștințe de programare în limbaje neobișnuite sau utilizarea de tehnici de programare avansate.
- **Provocări legate de cultura populară.** Referințe la filme, muzică, cărți sau alte forme de media.

Competițiile de tip **Attack - Defense** reprezintă o formă de testare a abilităților de securitate cibernetică, atât din perspectiva atacatorului, cât și a apărătorului. Aceste evenimente simulează un mediu real în care echipele se confruntă într-o luptă continuă pentru a compromite sau a apăra sisteme informatice complexe.

Formatul competițiilor

Formatul general al unei competiții Attack - Defense poate varia, dar de obicei implică următoarele etape:

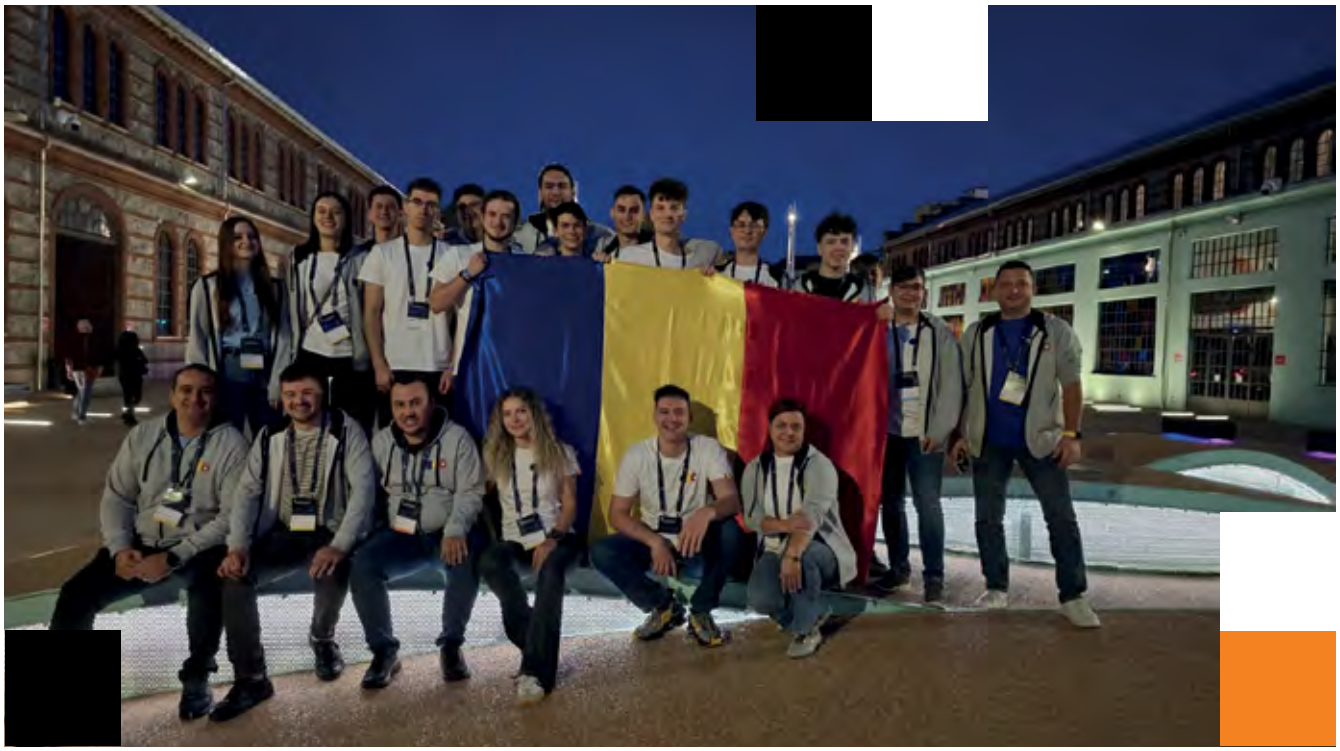
1. **Configurarea mediului.** Organizatorii pregătesc o infrastructură virtuală sau fizică care simulează o rețea corporativă, cu diverse sisteme și aplicații vulnerabile.
2. **Faza de pregătire.** Echipele participante au la dispoziție o perioadă de timp pentru a analiza sistemele și a identifica potențiale vulnerabilități.
3. **Faza de competiție.** Echipele de atac încearcă să exploateze vulnerabilitățile pentru a obține acces neautorizat la sisteme și a îndeplini obiectivele stabilite de organizatori (de exemplu, obținerea accesului root, furtul de date). În același timp, echipele de apărare trebuie să monitorizeze constant sistemele, să detecteze atacurile și să le remedieze.
4. **Evaluare.** La finalul competiției, se evaluează performanța fiecărei echipe în funcție de obiectivele îndeplinite, timpul necesar pentru a compromite sau a apăra sistemele și alte criterii specifice

România la ECSC 2024

Echipa României a obținut rezultate remarcabile la ediția din 2024 a ECSC, clasându-se pe locul 8 din 37 de echipe participante. Acest rezultat este o dovadă a talentului și a pregătirii tinerilor români în domeniul securității cibernetice. Iar această pregătire reprezintă, în sine, un drum lung și presărat cu provocări.

#teamromania își încep pregătirea, an de an, în etapele de selecție din primăvară – UNBreakable România, Romanian Cyber Security Challenge (ROCSC) și – începând din 2024 – Olimpiada Națională de Securitate Cibernetică. Da, 3 competiții, fiecare dintre ele menite să pună la încercare capacitatea lor, a celor mai talentați tineri și tinere din România, de a lucra individual, dar și în echipă pentru a obține unul dintre locurile ce-i trimit în etapele finale ale acestor 3 competiții.

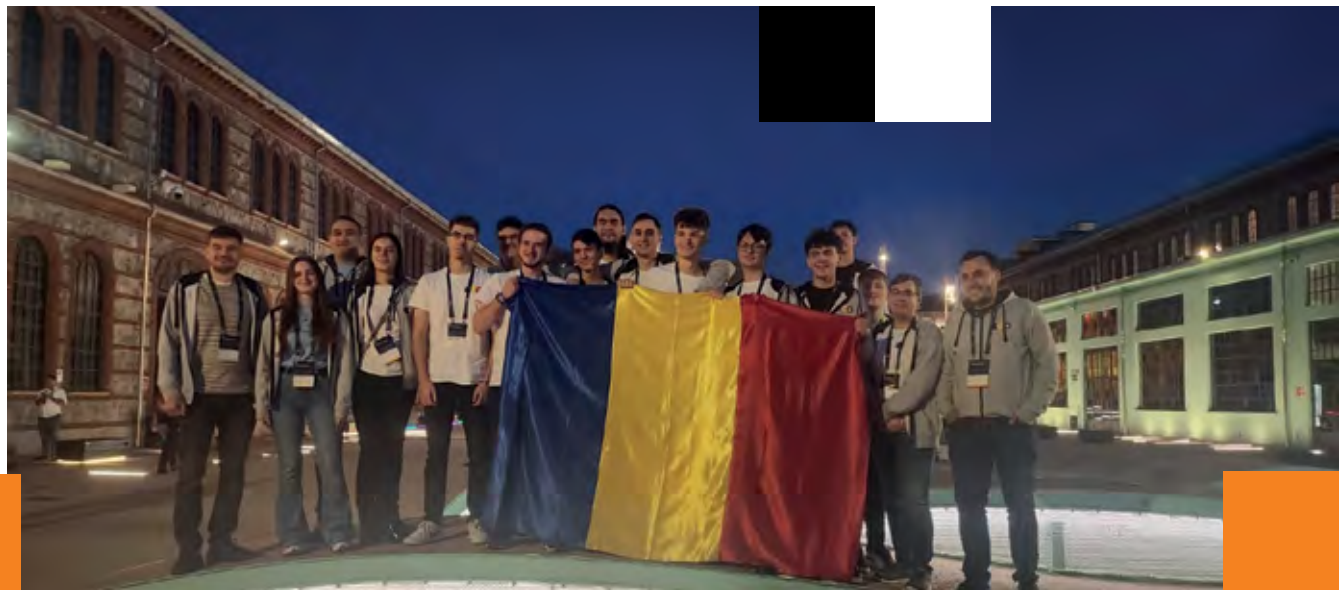
Dar de ce trei competiții? Selecția componenței **#teamromania** a fost, de la prima participare, susținută de organizarea unor competiții CTF de către partenerii și organizatorii din România. În timp, această competiție a căpătat format și formă și a devenit Romanian Cyber Security Challenge – un eveniment CTF adresat celor cu vârsta cuprinsă între 14 și 25 de ani ce doresc să concureze pentru un loc în #teamromania.



Ulterior, în 2020, Orange, alături de partenerii noștri și ai competiției – Bit Sentinel și CyberEDU, a creat UNbreakable România, o competiție de securitate cibernetică la nivel național, accesibilă oricărui elev ori student din școlile și universitățile din România. UNbreakable a adresat un număr mult mai mare de participanți și a contribuit semnificativ la includerea CTF-urilor în limbajul și practica profesorilor de TIC din liceele din România.

În 2024, cu sprijinul partenerilor noștri din rândul instituțiilor publice – Ministerul Educației, Directoratul Național de Securitate Cibernetică și Centrul Național Cyberint - și a prietenilor noștri – Bit Sentinel și CyberEDU, am contribuit la organizarea primei ediții a Olimpiadei Naționale de Securitate Cibernetică.

Astfel, la mijlocul anului acesta, trecuserăm, deja, prin 3 competiții importante, menite să ducă securitatea cibernetică și competițiile CTF cât mai aproape de fiecare elev și student din România, iar în fiecare dintre aceste competiții, tinerii și tinerele care au participat au obținut rezultate foarte bune.



Așa că am mers mai departe, printr-un proces de selecție transparent, și am format o echipă de 20 de persoane, cei mai buni jucători și jucătoare din cele 3 CTF-uri, pe care i-am invitat într-un bootcamp, timp de o săptămână, la Bran. În cele 5 zile petrecute în bootcamp, participanții au avut acces la training și cursuri oferite de experții în securitate cibernetică din cadrele partenerilor **#teamromania**, au concurat în CTF-uri dificile, cu challenge-uri similare celor pe care le-au întâlnit la ECSC, și – cel mai important! – au reușit să construiască o echipă.

Timpul a trecut repede, de la mijlocul verii până la începutul lunii octombrie, când **#teamromania**, adică cei mai buni 10 jucători din bootcamp, însoțiți de 2 jucători în rolul de rezerve și reprezentanți ai instituțiilor și companiilor private, parteneri ai echipei, au plecat spre Torino, locul în care a fost organizată ediția 2024 a European Cyber Security Challenge.

2 zile de competiție – Jeopardy în prima zi și Attack - Defense în cea de-a doua – au trecut și acestea foarte repede, iar **#teamromania** au arătat încă odată că sunt printre cei mai buni. Locul 8 din 37 de echipe ce au concurat, la câteva zeci de puncte distanță de Top 5, au demonstrat ceea ce știam deja – suntem buni!

Ediția 2025 va fi găzduită de Polonia și noi sperăm că atunci vom urca mai sus de locul 8! Cert este că vom scrie despre aventura #teamromania la ECSC 2025 în ediția următoare a raportului nostru.

15. 10 Predicții despre evoluția securității cibernetice în 2025

Anul 2025 se conturează ca fiind unul marcat de o creștere exponențială a amenințărilor cibernetice, dar și de o evoluție semnificativă a măsurilor de securitate menite să ne protejeze de aceste amenințări. Încheiem prima ediție în limba română a raportului Business Internet Security cu 10 predicții despre evoluția securității cibernetice în anul următor, ce sunt bazate pe rezultatele activităților noastre de cercetare și dezvoltare.

1. Inteligența artificială va fi atât armă, cât și scut

- I.A. va fi folosită pentru a crea atacuri de phishing extrem de personalizate, capabile să imite perfect comunicarea umană, pentru a genera cod malware mai sofisticat și pentru a identifica vulnerabilități în sisteme complexe într-un timp record.
- I.A. va fi utilizată pentru a analiza în timp real cantități uriașe de date, detectând anomalii și potențiale amenințări, pentru a automatiza răspunsul la incidente și pentru a crea soluții de securitate personalizate.
- **Implicații:** Organizațiile vor trebui să investească în soluții de securitate bazate pe I.A. pentru a rămâne competitive și pentru a proteja datele sensibile.

2. Ransomware-ul va continua să fie o problemă majoră

- Vom asista la o creștere a disponibilității modelului Ransomware ca serviciu (RaaS), unde atacatorii vor oferi acces la instrumente și cunoștințe specializate pentru a facilita atacurile.
- Infrastructurile critice, cum ar fi rețelele electrice, sistemele de apă și spitalele, vor fi ținte preferate.
- **Implicații:** Organizațiile trebuie să implementeze planuri solide de recuperare în caz de dezastru și să realizeze backupuri regulate ale datelor.

3. Securitatea datelor personale va fi sub lupa autorităților

- **GDPR și alte reglementări.** Regulamentul General privind Protecția Datelor (GDPR) și alte reglementări similare vor fi aplicate cu mai multă strictețe, iar amenzile pentru încălcările de securitate vor fi semnificativ mai mari.
- **Privacy by design.** Companiile vor fi obligate să integreze securitatea datelor în toate etapele de dezvoltare a produselor și serviciilor.
- **Implicații:** Organizațiile vor trebui să implementeze programe de conformitate GDPR și să investească în tehnologii de criptare și anonimizare a datelor.

4. Creșterea atacurilor asupra lanțurilor de aprovizionare

- **Atacuri asupra furnizorilor.** Atacatorii vor viza în mod special furnizorii de software și hardware pentru a compromite sistemele clienților acestora.
- **Software-ul cu sursă deschisă.** Vulnerabilitățile din software-ul cu sursă deschisă vor fi exploatate pe scară largă.
- **Implicații:** Organizațiile trebuie să își verifice cu atenție lanțurile de aprovizionare și să utilizeze doar software de la furnizori de încredere.

5. Securitatea IoT va fi o prioritate

- **Dispozitive medicale.** Dispozitivele medicale conectate vor fi o țintă atractivă pentru atacatori.
- **Smart homes.** Atacurile asupra sistemelor de acasă inteligente vor deveni mai frecvente.
- **Implicații:** Producătorii de dispozitive IoT trebuie să acorde o atenție deosebită securității, iar utilizatorii trebuie să își protejeze rețelele Wi-Fi și să își actualizeze dispozitivele în mod regulat.

6. Securitatea cloudului va fi testată la limită

- **Configurări greșite.** Configurările greșite ale serviciilor cloud vor fi exploatate pentru a obține acces neautorizat la date.
- **Atacuri asupra containerelor.** Atacurile asupra containerelor vor deveni mai sofisticate.
- **Implicații:** Organizațiile trebuie să implementeze măsuri de securitate solide pentru cloud, cum ar fi segmentarea rețelei, criptarea datelor și monitorizarea continuă.

7. Atacurile de tip phishing vor deveni și mai sofisticate

- **Deepfakes.** Tehnologia deepfake va fi utilizată pentru a crea atacuri de phishing extrem de convingătoare.
- **Atacuri personalizate.** Atacurile de phishing vor fi personalizate pentru fiecare victimă în parte.
- **Implicații:** Angajații trebuie să fie instruiți să recunoască atacurile de phishing și să țină pasul cu schimbările din acest domeniu.

8. Deficitul de specialiști în securitate cibernetică se va acutiza

- **Cerere mare, ofertă mică.** Cererea de specialiști în securitate cibernetică va continua să depășească oferta, ceea ce va duce la o creștere a costurilor pentru aceste servicii.
- **Automatizarea.** Automatizarea unor sarcini va fi necesară pentru a compensa lipsa de personal.
- **Implicații:** Organizațiile vor trebui să investească în programe de formare și dezvoltare a competențelor în domeniul securității cibernetice.

9. Securitatea cibernetică va deveni o parte integrantă a culturii organizaționale

- **Conștientizarea angajaților.** Angajații vor fi responsabilizați pentru securitatea cibernetică și vor primi traininguri regulate.
- **Politici de securitate clare.** Organizațiile vor implementa politici de securitate clare și ușor de înțeles.
- **Implicații:** Cultura organizațională va fi orientată către securitate, iar angajații vor fi motivați să raporteze orice incident suspect.

10. Colaborarea public-privat va fi esențială

- **Parteneriate strategice.** Guvernele și sectorul privat vor colabora pentru a împărtăși informații despre amenințări și pentru a dezvolta soluții comune.
- **Standarde comune.** Se vor stabili standarde comune pentru securitatea cibernetică la nivel global.
- **Implicații:** Organizațiile vor beneficia de o mai bună protecție și de acces la informații de intelligence.

Glosar de termeni

Securitate cibernetică - Securitatea informatică este o ramură a informaticii care se ocupă cu identificarea riscurilor implicate de folosirea dispozitivelor informatice, cum sunt calculatoarele, smartphone-urile, dar și rețelele de calculatoare, atât publice, cât și private, și cu oferirea de soluții pentru înlăturarea lor.

Amenințări cibernetice (amenințări) - Posibilitatea unei încercări rău intenționate de a deteriora sau perturba o rețea sau un sistem de calculatoare.

Servicii de securitate gestionate - În domeniul informaticii, serviciile de securitate gestionate (MSS) sunt servicii de securitate a rețelei care au fost externalizate către un furnizor de servicii. O companie care furnizează un astfel de serviciu este un furnizor de servicii de securitate gestionată (MSSP).

IDS - Un sistem de detecție a intruziunilor (IDS) este un dispozitiv sau o aplicație software care monitorizează o rețea sau sisteme pentru a detecta activități rău intenționate sau încălcări ale politicii. Orice activitate rău intenționată sau încălcare este de obicei raportată fie unui administrator, fie colectată la nivel central, folosind un sistem de management al evenimentelor și informațiilor de securitate (SIEM).

IPS - Sistemele de prevenire a intruziunilor (IPS) sunt dispozitive de securitate a rețelei sau dispozitive virtuale care monitorizează activitățile de rețea sau de sistem pentru a detecta activități rău intenționate, înregistrează informații despre aceste activități, le raportează și încearcă să le blocheze sau să le oprească.

WAF - Un firewall pentru aplicații web (sau WAF) filtrează, monitorizează și blochează traficul HTTP către și de la o aplicație web. Un WAF se diferențiază de un firewall obișnuit prin aceea că poate filtra conținutul unor aplicații web specifice, în timp ce firewall-urile obișnuite servesc ca o poartă de siguranță între servere. Prin inspectarea traficului HTTP, acesta poate preveni atacurile care provin din defecte de securitate ale aplicațiilor web, cum ar fi injecția SQL, scriptingul încrucișat (XSS), includerea de fișiere și configurările eronate de securitate.

SIEM - Produsele și serviciile software de management al evenimentelor și informațiilor de securitate (SIEM) combină managementul informațiilor de securitate (SIM) cu managementul evenimentelor de securitate (SEM). Acestea oferă o analiză în timp real a alertelor de securitate generate de aplicații și hardware de rețea.

Ransomware - Este un tip de malware (vezi termenul) din domeniul criptovirologiei care amenință să publice datele victimei sau să blocheze permanent accesul la acestea, dacă nu se plătește o răscumpărare.

Malware - (prescurtare de la program rău intenționat) Este orice program conceput în mod intenționat pentru a provoca daune unui computer, unui server sau unei rețele de computere. Acesta poate lua forma unui cod executabil, unor scripturi, unui conținut activ și altor programe. Codul este descris ca viruși de calculatori, viermi informatici, troieni, ransomware, spyware, adware, scareware, pe lângă alți termeni.

Botnet - Un botnet reprezintă mai multe dispozitive conectate la internet, fiecare dintre acestea rulând unul sau mai mulți roboți. Botnet-urile pot fi folosite pentru a efectua atacuri distribuite de tip refuz-serviciu (atacuri DDoS), pentru a fura date, pentru a trimite spamuri și pentru a permite atacatorului să acceseze dispozitivul și conexiunea acestuia. Un botnet este controlat de un centru de comandă și control, operat de către proprietar.

DDoS - Un atac de tip refuz-serviciu (atac DoS) este un atac cibernetic în care făptuitorul încearcă să facă o mașină sau o resursă de rețea indisponibilă pentru utilizatorii destinați, prin întreruperea temporară sau nedeterminată a serviciilor unei gazde conectate la internet. Refuzul serviciului se realizează de obicei prin inundarea mașinii sau a resursei vizate cu solicitări inutile pentru a supraîncărca sistemele și a împiedica îndeplinirea unora sau a tuturor solicitărilor legitime. Într-un atac distribuit de tip refuz-serviciu (atac DDoS), traficul de intrare care inundă victima provine din multe surse diferite. Acest lucru face efectiv imposibilă oprirea atacului prin simpla blocare a unei singure surse.

Router - Un dispozitiv care permite unei rețele locale (LAN) să se conecteze la o rețea de arie largă (WAN) printr-un modem (DSL sau cablu), o rețea de telefonie mobilă în bandă largă, o rețea optică de uz general sau altă conexiune.

Java Script - Alături de HTML și CSS, JavaScript este una dintre cele trei tehnologii de bază ale World Wide Web. JavaScript permite realizarea de pagini web interactive și, prin urmare, este o parte esențială a aplicațiilor web. Majoritatea site-urilor web îl folosesc și toate browserele web importante au un motor JavaScript dedicat pentru a-l executa.

Payload (malware) - Payloadul este partea de date transmise care reprezintă mesajul efectiv sau, în contextul unui virus sau vierme informatic, payloadul este partea de malware care efectuează acțiuni rău intenționate.

Phishing - Încercarea de a obține informații sensibile, cum ar fi nume de utilizator, parole și detalii ale cărților de credit (și bani), adesea din motive rău intenționate, deghizându-se într-un site web de încredere, comunicare care se realizează de obicei prin falsificarea e-mailurilor sau prin mesagerie instantanee, și care adesea îndrumă utilizatorii să introducă date personale pe un site web fals, al cărui aspect este identic cu cel legitim, singura diferență fiind URL-ul site-ului în cauză.

Exploit - Un program, o cantitate de date sau o secvență de comenzi care profită de o eroare de programare sau de o vulnerabilitate pentru a face ca un comportament neintenționat sau neprevăzut să apară în software-ul sau hardware-ul calculatorului pentru a obține controlul asupra unui sistem informatic, a permite escaladarea privilegiilor sau a executa un atac de tip refuz-serviciu (DoS sau DDoS asociat).

Criptografie cu cheie publică - Criptografia cu cheie publică, sau criptografia asimetrică, este orice sistem criptografic care utilizează perechi de chei: chei publice care pot fi diseminate pe scară largă și chei private care sunt cunoscute numai de proprietar. Aceasta îndeplinește două funcții: autentificare, în care cheia publică verifică dacă un deținător al cheii private asociate a trimis mesajul, și criptarea, în care doar deținătorul cheii private asociate poate decripta mesajul criptat cu cheia publică.

CVE - Sistemul de vulnerabilități și expuneri comune (CVE) oferă o metodă de referință pentru vulnerabilitățile și expunerile cunoscute public în materie de securitate a informațiilor.

Politica Bring Your Own Device (BYOD) - Bring your own device (BYOD) - numită și bring your own technology (BYOT), bring your own phone (BYOP) și bring your own personal computer (BYOPC) - se referă la politica prin care li se permite angajaților să aducă dispozitive personale (laptopuri, tablete și smartphone-uri) la locul de muncă și să utilizeze acele dispozitive pentru a accesa informațiile și aplicațiile privilegiate ale companiei.

Echipa:

Ioan Constantin, Cyber Security Expert

Cristian Pațachia, Development & Innovation Manager

Mădălina Pavel, Business Services Marketing Manager

Cristina Ilisei, Brand & Communication

Cosmin Grancea, Business Services Marketing Manager

Ana Ciobanu, Startup Programs Manager

Cuprins

Mai eficient

mai creativ

Descoperă puterea inteligenței artificiale cu Microsoft Copilot.

Detalii pe oran.ge/CopilotMicrosoft

Microsoft
Solutions Partner

orange™