enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

RO

ianuarie 2019 – aprilie 2020

Amenințările din interior

Raportul ENISA privind situația amenințărilor

Prezentare generală

O amenințare din interior este o acțiune care poate conduce la un incident, desfășurată de o persoană sau de un grup de persoane afiliate sau care lucrează pentru potențiala victimă. Există mai multe tipare asociate cu amenințările din interior. Un model bine cunoscut de amenințare din interior (cunoscut și sub denumirea de „abuz de privilegii") apare atunci când persoanele din afară colaborează cu actori interni pentru a obține acces neaprobat la active. Deținătorii de informații privilegiate pot provoca daune în mod neintenționat, prin neglijență sau din cauza lipsei de cunoștințe. Întrucât acești deținători de informații privilegiate se bucură adesea de încredere și privilegii, precum și de cunoștințe despre politicile organizaționale, procesele și procedurile organizației, este dificil să se facă distincția între accesul legitim, cel rău intenționat și cel eronat la aplicații, date și sisteme.[1]

Cele cinci tipuri de amenințări din interior pot fi definite în funcție de motivațiile și obiectivele lor:

a) lucrătorii neatenți care utilizează necorespunzător datele, încalcă politicile de utilizare și instalează aplicații neautorizate;

b) agenții din interior care fură informații în numele unor persoane din exterior;

c) angajații nemulțumiți care încearcă să-și prejudicieze propria organizație;

d) deținătorii de informații privilegiate rău intenționați care folosesc privilegiile existente pentru a fura informații pentru beneficiul personal;

e) terții incapabili care compromit securitatea prin utilizarea abuzivă a informațiilor sau accesul rău intenționat la un activ sau utilizarea rău intenționată a acestuia.

Toate cele cinci tipuri de amenințări din interior trebuie studiate în mod continuu deoarece recunoașterea existenței lor și a modului lor de operare trebuie să definească strategia organizației în materie de securitate și protecție a datelor.

Constatări

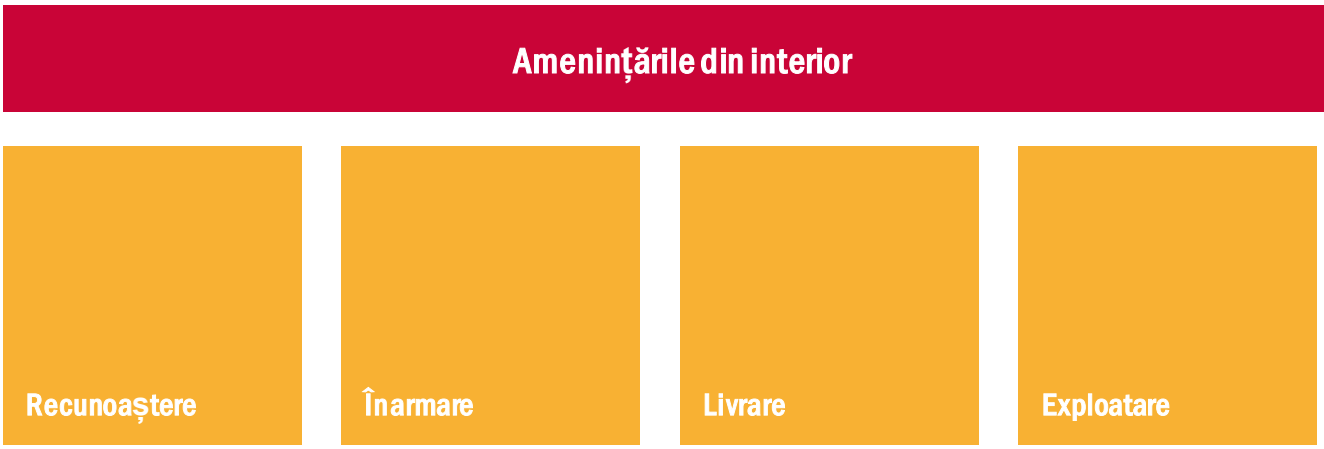
65 %_ **din impactul amenințărilor din interior include daune aduse reputației și finanțelor organizației[12]**

88 %_ **din organizațiile examinate recunosc că amenințările din interior constituie un motiv de alarmă[10]**

11,45_ **milioane EUR este costul mediu anual al incidentelor de securitate cibernetică cauzate organizației de un deținător de informații privilegiate[8]**

40 %_ **din organizațiile examinate se simt vulnerabile la expunerea informațiilor comerciale confidențiale[11]**

Kill chain



Etapă din fluxul de activitate de atac

Amploarea scopului

Instalare

Comandă și control

Acțiuni privind obiectivele

Cadrul Cyber Kill Chain® a fost dezvoltat de Lockheed Martin, fiind adaptat după un concept militar legat de structura unui atac. Pentru a studia un anumit vector de atac, utilizați această diagramă kill-chain pentru a trasa fiecare etapă a procesului și a face referire la instrumentele, tehnicile și procedurile utilizate de atacator.

MAI MULTE INFORMAȚII

Descriere

_Banii vorbesc

Datorită costului în creștere al altor vectori de atac, atacatorii sunt dispuși să ofere sume mari de bani deținătorilor de informații privilegiate. Prețul deținătorilor de informații privilegiate variază, în funcție de poziția deținătorului de informații privilegiate în companie, de compania însăși, de tipul și complexitatea serviciului solicitat, de tipul de date sustrase și de nivelul de securitate al companiei. Unele dintre modurile în care atacatorii recrutează deținători de informații privilegiate includ: (1) simpla postare a unei oferte pe forumuri și oferirea unei recompense pentru anumite informații; (2) deghizarea acțiunilor lor, astfel încât angajații nu își dau seama că acționează ilegal, dezvăluie informații cu caracter personal sau se angajează în activități de utilizare abuzivă a informațiilor privilegiate; și (3) șantajul.[4]

_Acțiuni necinstite Urbi et Orbi

Un fost inginer software de la un furnizor de servicii cloud a profitat de un firewall pentru aplicații web configurat greșit și a accesat peste 100 de milioane de conturi ale clienților și înregistrări ale cardurilor de credit. De atunci, compania a remediat vulnerabilitatea și a declarat că „nu au fost compromise numerele de cont ale cardurilor de credit sau datele de autentificare". Acest caz de amenințare din interior este deosebit de interesant deoarece fostul angajat transformat în hacker nu era preocupat de ascunderea identității. Hackerul a împărtășit metoda de piratare colegilor de la Capital One pe un serviciu de chat. De asemenea, hackerul a postat informațiile pe GitHub (folosind numele complet) și s-a și lăudat pe rețelele de socializare cu faptele respective. Acest tip de comportament este un fenomen pe care psihologii îl numesc „scurgere de informații" în care deținătorii de informații privilegiate ce plănuiesc să aducă pagube își dezvăluie planurile. Capital One se așteaptă ca această încălcare a securității să coste până la 150 de milioane USD (aproximativ 127 de milioane EUR).[5]

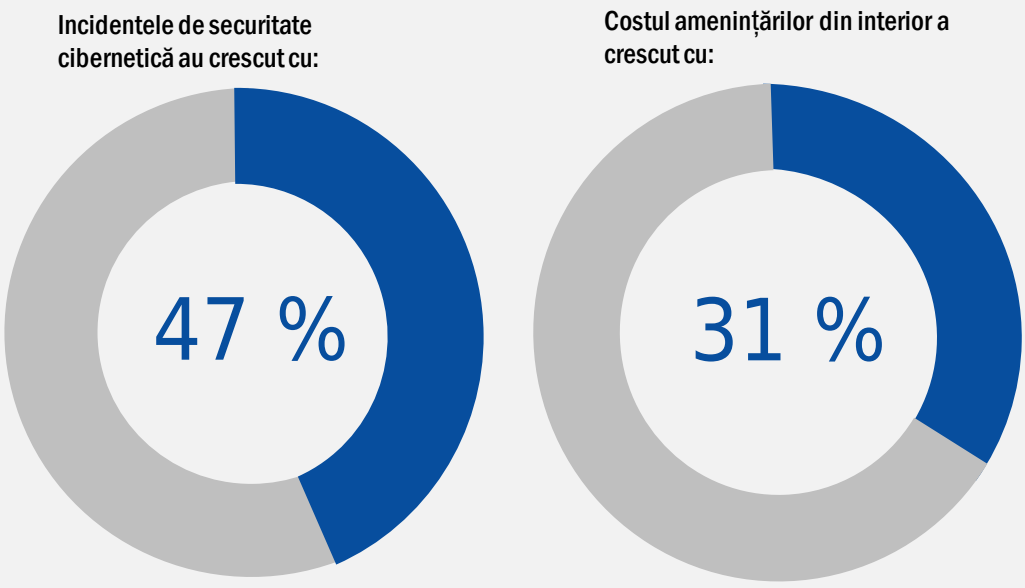


Figura 2: Incidente și tendințe de cost. Sursa: ObservelT[8]

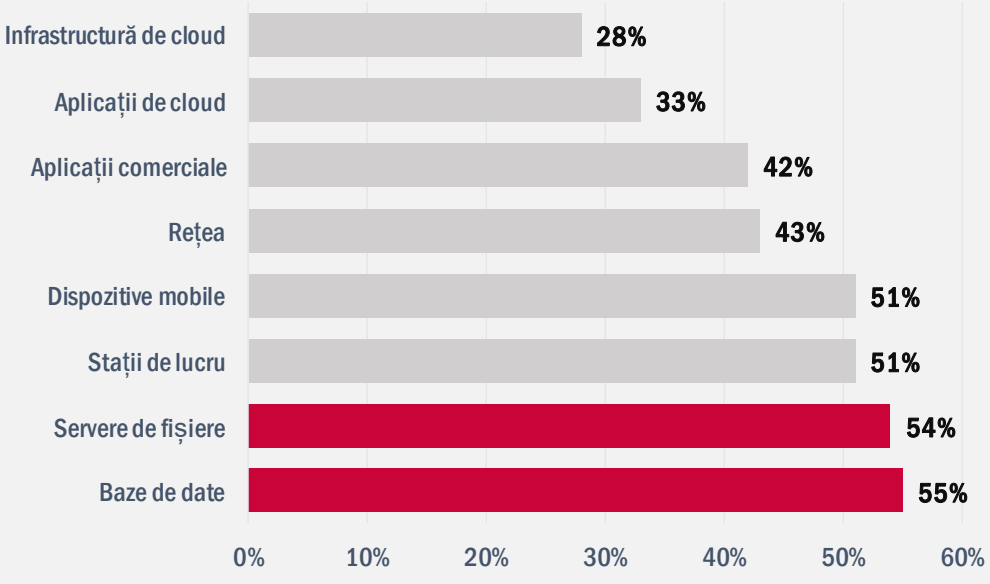


Figura 2: Active IT vulnerabile la amenințări din interior. Sursa: Help Systems[9]

Vectori de atac

_Cum

Un sondaj recent[14] a arătat că grupurile sunt cele mai periculoase amenințări din interiorul companiilor și al altor organizații.

Potrivit experților în materie de securitate cibernetică[15], phishingul (38 %) este cea mai mare vulnerabilitate în cazul amenințărilor neintenționate din interior. Pe ultimele locuri de pe listă sunt spear phishing (21 %), parolele slabe sau reutilizate (16 %), conturile orfane (10 %) și navigarea pe site-uri suspecte (7 %).

_Zona de impact a incidentelor de amenințări din interior

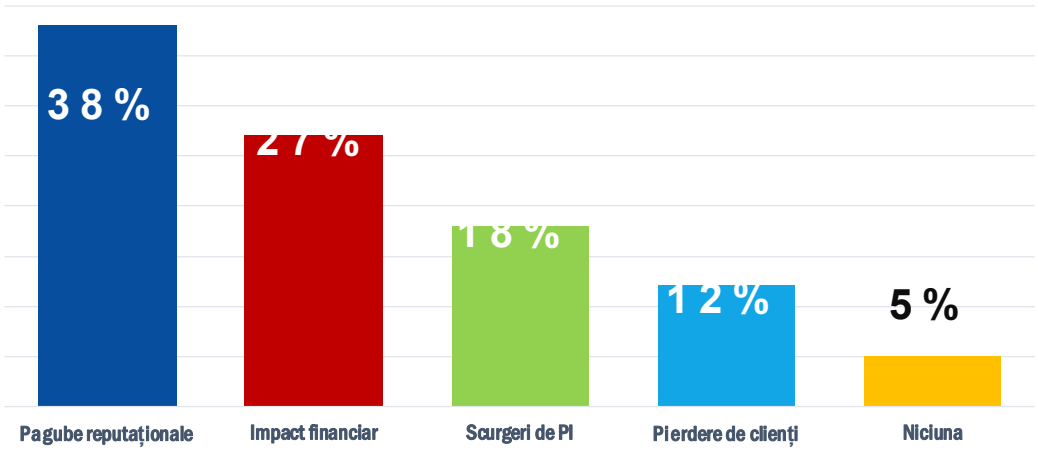


Figura 3 - Sursa: Egress[12]


„Deținătorii de informații privilegiate pot provoca daune neintenționate din neglijență sau din cauza lipsei de cunoștințe.”
în ETL 2020

Măsuri de atenuare

Acțiuni propuse

- Implementarea unei tehnologii de inspecție profundă a pachetelor (DPI) pentru detectarea anomaliilor, care oferă utilizatorilor industriali o platformă de încredere pentru monitorizarea fluxului procesului de comandă și control și a datelor de telemetrie și protejarea împotriva amenințărilor externe. În același timp, aceasta diminuează riscul de interferență „avansată" din partea inginerilor, operatorilor SCADA sau a altor angajați interni cu acces direct la sisteme.[16]
- Introducerea unui plan de contramăsuri pentru amenințările din interior în strategia și politicile generale în materie de securitate. Acest plan include de regulă un cadru de gestionare a riscurilor, un plan de continuitate a activității (BCP), un program de recuperare în caz de dezastru (DRP), o politică de management financiar și contabil și o gestionare legală și de reglementare.[1]
- Dezvoltarea unui program de securitate care constă în: desfășurarea de activități de vânare a amenințărilor, efectuarea scanării vulnerabilităților și a testelor de penetrare, utilizarea de măsuri de securitate a personalului, utilizarea de măsuri de securitate fizică, utilizarea de soluții de securitate a rețelei, utilizarea de soluții de securitate a stațiilor de lucru, utilizarea de măsuri de securitate a datelor, utilizarea de măsuri de gestionare a identității și accesului, stabilirea de capacități de gestionare a incidentelor, menținerea de servicii de criminalistică digitală și utilizarea metodelor de inteligență artificială (IA) pentru a preveni atacurile din interior.
- Elaborarea unei politici de securitate privind amenințările din interior, bazată pe conștientizarea utilizatorilor, care este unul dintre cele mai eficace controale pentru acest tip de amenințare cibernetică.
- Aplicarea de controale tehnice robuste. Măsurile de securitate tradiționale tind să se concentreze asupra amenințărilor externe, dar acestea nu sunt de regulă eficiente în identificarea riscurilor interne care provin din interiorul organizației. Pentru a proteja activele, se recomandă aplicarea de instrumente precum prevenirea pierderilor de date (DLP) pentru a preveni sustragerea datelor.[1]

- Reducerea numărului de utilizatori cu privilegii și acces la informații sensibile. Dacă un angajat nu are nevoie de acces la unele informații pentru a-și face treaba, este mai bine să se restricționeze ceea ce poate vedea, evitând astfel accesul neautorizat.[17]
- Consolidarea mediului digital, care include o mai bună securitate a rețelei, sistemelor, aplicațiilor, datelor și conturilor.[1]

Referințe

1. „Insider Threat Report" (Raportul privind amenințările din interior), 2019. Verizon. https://enterprise.verizon.com/resources/reports/insider-threat-report.pdf

2. „Insider Threat Statistics Facts and Figures" (Date și cifre din statisticile privind amenințările din interior). Ekran System. https://www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures

3. „CyberEdge 2019 CDR Report" (Raportul CyberEdge CDR 2019), 2019. CyberEdge. https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf

4. „Corporate Security Predictions 2020" (Predicții de securitate corporativă 2020). 2019. 3 decembrie 2019. Kaspersky.

https://securelist.com/corporate-security-predictions-2020/95387/

5. „Famous Insider Threat Cases" (Cazuri celebre de amenințări din interior), septembrie 2019. Security Boulevard. https://securityboulevard.com/2019/09/famous-insider-threat-cases-insider-threat-awareness-month/

6. „The rise of insider threats: Key trends to watch" (Creșterea amenințărilor din interior: tendințe cheie de urmărit), 2019. Tech Beacon.

https://techbeacon.com/security/rise-insider-threats-key-trends-watch

7. „Cost of Cybercrime study" (Costul studiului privind criminalitatea informatică), 2019. Accenture. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

8. „Cost of Insider Threats" (Costul amenințărilor din interior), 2020. Observer IT. https://www.observeit.com/cost-of-insider-threats/

9. „Cybersecurity Insiders 2019 Insider Threat Report" (Deținătorii de informații privilegiate în materie de securitate cibernetică – Raportul privind amenințările din interior 2019), 2019. Help Systems. https://www.helpsystems.com/cta/2019-cybersecurity-insiders-insider-threat-report

10. „Forcepoint Insider threat Data Protection" (Forcepoint – Protejarea datelor de amenințările din interior), 2017. Force Point.

https://www.forcepoint.com/sites/default/files/resources/files/brochure_insider_threat_data_protection_en.pdf

11. „State of Insider Threats in the Digital Workplace" (Situația amenințărilor din interior la locul de muncă digital), 2019. Better Cloud. https://www.bettercloud.com/monitor/wp-content/uploads/sites/3/2019/03/BetterCloud-State-of-Insider-Threats-2019-FINAL.pdf

12. „Insider Data Breach Survey 2019" (Sondaj privind încălcarea securității datelor din interior). 2019. Egress. https://scoop-cms.s3.amazonaws.com/566e8c75ca2f3a5d5d8b45ae/documents/egress-opinionmatters-insider-threat-research-report-a4-uk-digital.pdf

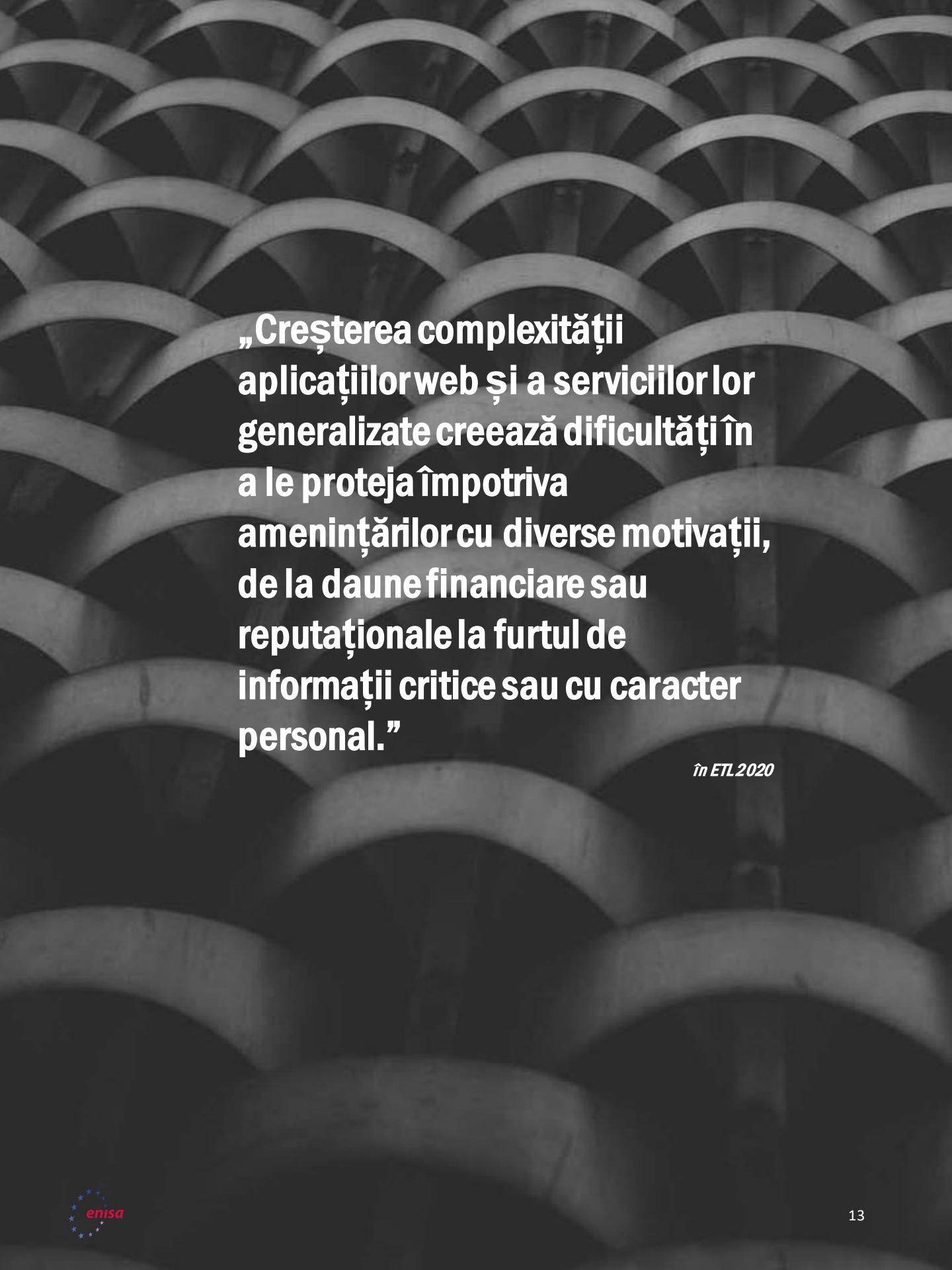
13. „Insider Threat Report" (Raport privind amenințările din interior). 2019. Nucleos Cyber. https://nucleuscyber.com/wp-content/uploads/2019/07/2019_Insider-Threat-Report_Nucleus_Final.pdf

14. „Insider Threat Report" (Raport privind amenințările din interior). 2019. Haystax. https://haystax.com/wp-content/uploads/2019/07/Haystax-Insider-Threat-Report-2019.pdf

15. „Insider Threat Report" (Raport privind amenințările din interior). 2019. Fortinet. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/insider-threat-report.pdf

16. „Kaspersky Industrial CyberSecurity: solution overview 2019" (Securitate cibernetică industrială Kaspersky: prezentare generală a soluției 2019). 2019. Kaspersky. https://ics.kaspersky.com/media/KICS-Solution-overview-2019-EN.pdf

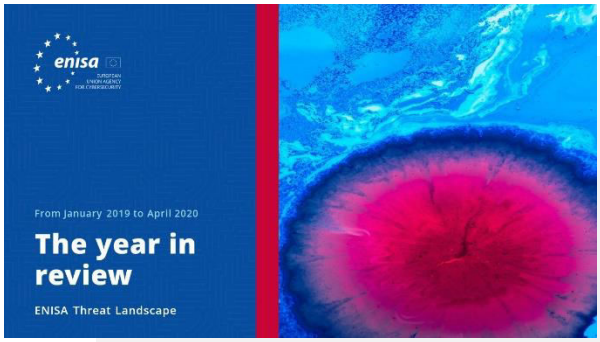
17. „Post-vacation cybersecurity tuneup: Get your company ready!" (Îmbunătățirea securității cibernetice după vacanță: pregătește-ți compania!). 1 septembrie 2017. Panda. https://www.pandasecurity.com/mediacenter/adaptive-defense/cyber-security-get-company-ready/



„Creșterea complexității aplicațiilor web și a serviciilor lor generalizate creează dificultăți în a le proteja împotriva amenințărilor cu diverse motivații, de la daune financiare sau reputaționale la furtul de informații critice sau cu caracter personal.”

în ETL 2020

Documente conexe



Raportul ENISA privind situația amenințărilor **Trecerea în revistă a anului**

Rezumat al tendințelor de securitate cibernetică pentru perioada ianuarie 2019 – aprilie 2020.

CITIȚI RAPORTUL

Raportul ENISA privind situația amenințărilor
Lista celor mai importante 15 amenințări

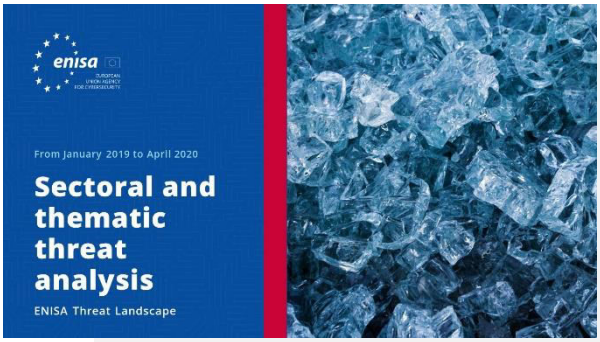
Lista ENISA a celor mai importante 15 amenințări din perioada ianuarie 2019 – aprilie 2020.

CITIȚI RAPORTUL

Raportul ENISA privind situația amenințărilor
Teme de cercetare

Recomandări privind teme de cercetare în diferite sectoare din securitatea cibernetică și informațiile privind amenințările cibernetice.

CITIȚI RAPORTUL



Raportul ENISA privind situația amenințărilor **Analiza sectorială și tematică a amenințărilor**

Analiza contextualizată a amenințărilor în perioada ianuarie 2019 - aprilie 2020.

CITIȚI RAPORTUL

Raportul ENISA privind situația amenințărilor **Tendințe emergente**

Principalele tendințe în securitatea cibernetică observate în perioada ianuarie 2019 - aprilie 2020.

CITIȚI RAPORTUL

Raportul ENISA privind situația amenințărilor
Prezentare generală a informațiilor privind amenințările cibernetice

Situația actuală a informațiilor privind amenințările cibernetice în UE.

CITIȚI RAPORTUL

Despre

_Agenție

Agenția Uniunii Europene pentru Securitate Cibernetică, ENISA, este agenția Uniunii dedicată realizării unui nivel comun ridicat de securitate cibernetică în întreaga Europă. Înființată în 2004 și consolidată prin Regulamentul UE privind securitatea cibernetică, Agenția Uniunii Europene pentru Securitate Cibernetică
contribuie la politica cibernetică a UE, sporește credibilitatea produselor, serviciilor și proceselor TIC cu ajutorul sistemelor de certificare a securității cibernetice, cooperează cu statele membre și organismele UE și ajută Europa să se pregătească pentru provocările cibernetice viitoare. Prin schimbul de cunoștințe, consolidarea capacităților și campanii de sensibilizare, agenția colaborează cu părțile interesate cheie pentru a consolida încrederea în economia conectată, pentru a spori reziliența infrastructurii Uniunii și, în cele din urmă, pentru a menține securitatea digitală a societății europene și a cetățenilor. Mai multe informații cu privire la ENISA și activitatea sa sunt disponibile la adresa www.enisa.europa.eu.

Contribuitori

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) și *toți membrii Grupului părților interesate al ENISA CTI:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) și Thomas Hemker.

Editori

Marco Barros Lourenço (ENISA) și Louis Marinos (ENISA).

Date de contact

Pentru întrebări despre această lucrare, vă rugăm să utilizați adresa enisa.threat.information@enisa.europa.eu.

Pentru întrebări din partea mass-media despre această lucrare, vă rugăm să utilizați adresa press@enisa.europa.eu.

Dorim să aflăm părerea dumneavoastră despre acest raport!
Vă rugăm să acordați câteva momente completării chestionarului. Pentru a accesa formularul, faceți clic aici.

Aviz juridic

Trebuie luat în considerare faptul că această publicație reprezintă punctele de vedere și interpretările ENISA, cu excepția cazului în care se prevede altfel. Această publicație nu ar trebui interpretată ca o acțiune juridică a ENISA sau a organismelor ENISA, cu excepția cazului în care aceasta a fost adoptată în conformitate cu Regulamentul (UE) nr. 526/2013. Această publicație nu reprezintă neapărat stadiul actual al tehnologiei și ENISA o poate actualiza periodic.

Sursele terțe sunt citate corespunzător. ENISA nu este responsabilă pentru conținutul surselor externe, inclusiv al site-urilor externe menționate în această publicație.

Această publicație are doar scop informativ și trebuie să fie accesibilă în mod gratuit. Nici ENISA și nici persoanele care acționează în numele său nu sunt responsabile pentru modul în care ar putea fi utilizate informațiile conținute în această publicație.

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Grecia
Telefon: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu