enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

RO

Ianuarie 2019 – aprilie 2020

Scurgerile de informații

Raportul ENISA privind situația amenințărilor

Prezentare generală

O încălcare a securității datelor are loc atunci când datele pentru care este responsabilă o organizație fac obiectul unui incident de securitate din care a rezultat o încălcare a confidențialității, disponibilității sau integrității.[1] Încălcarea securității datelor cauzează frecvent o scurgere de informații, care este una dintre amenințările cibernetice majore, acoperind o mare varietate de informații compromise, de la informații personale identificabile (PII), date financiare stocate în infrastructuri IT la informații personale despre starea de sănătate (PHI) păstrate în registrele de date ale furnizorilor de servicii medicale.

Când apar încălcări ale securității în titlurile buletinelor, blogurilor, ziarelor și rapoartelor tehnice, accentul se pune mai ales pe adversari sau pe eșecul catastrofal al proceselor și tehnicilor de apărare cibernetică. Cu toate acestea, adevărul incontestabil este că, în pofida impactului sau a sferei unui astfel de eveniment, încălcarea securității este cauzată de obicei de acțiunea unei persoane sau de un eșec al procesului organizațional.[2]

Constatări

2 013_ dezvăluiri de date confirmate în 2019

În prima jumătate a anului 2019, organizațiile au înregistrat o creștere cu 11 % a dezvăluirilor de date comparativ cu 2018.[5,6]

14 %_ din toate incidentele din sectorul financiar au fost dezvăluiri de date

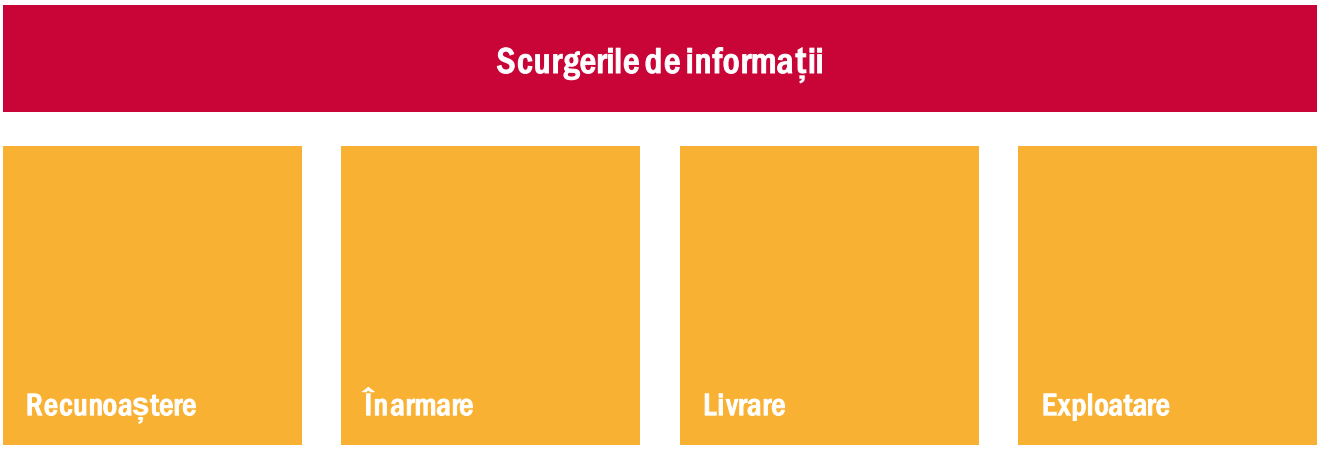
În 47 % din acestea, victima a fost o bancă.[9]

4,1_ milioane de înregistrări de date au fost expuse la nivel global în prima jumătate a anului 2019

E-mail-urile și parolele se aflau pe primele locuri pe listă.[10]

5,46_ milioane EUR este cel mai mare cost suportat de sectorul asistenței medicale[11]

Kill chain



Etapă din fluxul de activitate de atac

Amploarea scopului

Instalare

Comandă și control

Acțiuni privind obiectivele

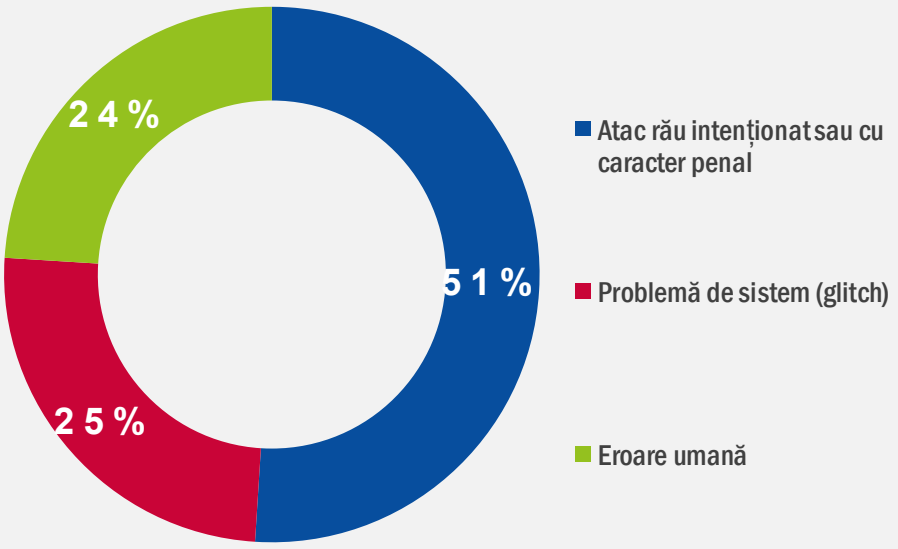
Cadrul Cyber Kill Chain® a fost dezvoltat de Lockheed Martin, fiind adaptat după un concept militar legat de structura unui atac. Pentru a studia un anumit vector de atac, utilizați această diagramă kill-chain pentru a trasa fiecare etapă a procesului și a face referire la instrumentele, tehnicile și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

MAI MULTE INFORMAȚII

_Cele mai importante incidente de scurgeri de informații

- În ianuarie 2019, cercetătorul independent Troy Hunt a identificat 773 de milioane de adrese de e-mail și parole ale utilizatorilor în **serviciul MEGA de stocare în cloud**. Hunt a numit acest set de date care a făcut obiectul unei încălcări a securității drept „Colecția nr. 1” și a anunțat serviciul „Have I been Pwned?”, astfel încât să poată notifica deținătorii conturilor să-și schimbe parolele de conectare pentru accesarea platformei MEGA.[12] În aceeași lună, indivizi necinstiți au publicat detalii personale, comunicări private și informații financiare ale câtorva sute de **politicieni germani**, ținte fiind toate partidele politice, în afară de extrema dreaptă AfD (Alternative für Deutschland).[6]
- În februarie 2019, peste 61 de milioane de conturi au fost selectate de pe 16 site-uri internet și scoase la vânzare pe dark web. Proprietarii site-urilor Whitepages, Dubsmash, Armor Games, 500px și ShareThis au constatat că datele furate ale utilizatorilor lor au fost vândute pentru mai puțin de 20 000 USD (aproximativ 17 000 EUR) în Bitcoin.[13]
- În martie 2019, sute de milioane de utilizatori **Facebook** și **Instagram** au constatat că le-au fost expuse datele de identificare prin gestionarea deficitară a stocării parolelor de către compania de platforme de comunicare socială.[14]
- În aprilie 2019, în India, au fost expuse 12,5 milioane de fișe medicale ale femeilor însărcinate, din cauza unui server guvernamental care a făcut obiectul unei scurgeri de informații, aparținând unei agenții de asistență medicală. Informațiile medicale expuse au fost legate de actul de preconcepție și de tehnici de diagnostic prenatal, o lege indiană adoptată care interzice determinarea prenatală a sexului în încercarea de a împiedica familiile indiene să avorteze fetele nenăscute și să încline raportul de gen spre băieți.[15]

- În mai 2019, **DoorDash**, un serviciu de livrare de alimente, a suferit o încălcare a securității datelor care a afectat aproape 5 milioane de utilizatori. Ancheta ulterioară a stabilit că au fost accesate informații precum nume, adrese de e-mail, adrese de livrare, istoricul comenzilor, numere de telefon și parole. Compania a declarat că au fost accesate și ultimele patru cifre ale cardurilor de credit și ale numerelor de cont bancar ale unor consumatori.[16]
- În iunie 2019, **Agenția americană de colectare a datoriilor medicale (American Medical Collection Agency – AMCA)** a început să-și anunțe clienții cu privire la o piratare a sistemului care a încălcat securitatea datelor de facturare și medicale ale unora dintre clienții săi, inclusiv 11,9 milioane de înregistrări ale **Quest Diagnostics**, care este una dintre cele mai mari companii de analize de sânge din Statele Unite. Potrivit unei declarații 8K recente a Comisiei de valori mobiliare, un hacker a obținut acces la sistemul AMCA timp de aproape opt luni, în perioada 1 august 2018 - 30 martie 2019.[17]



Cauzele principale ale divulgării informațiilor. Sursa: Ponemon, IBM Security[22]

Cele mai importante incidente de scurgeri de date

- În iulie 2019, corporația financiară **Capital One** a suferit o scurgere de informații care a afectat 100 de milioane de cereri de carduri de credit, 140 000 de numere de securitate socială și 80 000 de numere de conturi bancare. Capital One a raportat că nu au fost expuse numere de cont ale cardului de credit sau datele de identificare pentru conectare. Cu toate acestea, încălcarea securității a expus nume, adrese, coduri poștale, numere de telefon, adrese de e-mail și date de naștere.[18]
- În august 2019, 160 de milioane de înregistrări ale **MoviePass** au fost lăsate necriptate. Deoarece baza de date a companiei nu a fost protejată prin parolă, au fost lăsate expuse numerele cardurilor de credit ale clienților și alte detalii. Baza de date a rămas online câteva zile.[19] Între timp, o scurgere masivă de informații a expus 27,8 milioane de elemente biometrice ale personalului deținute de **Poliția Metropolitană Britanică, bănci și contractori din domeniul apărării**. Baza de date a fost administrată de Suprema, o companie care colaborează cu poliția britanică.[20,21]
- În septembrie 2019, au fost piratate peste 218 milioane de conturi de jucători **'Words with Friends'**. Baza de date a utilizatorilor a inclus date de la jucători de pe Android și iOS care au instalat jocul înainte de 2 septembrie. Echipa de hackeri „Gnostic players" a accesat informații precum numele jucătorilor, adresele de e-mail, identitățile de conectare și multe altele.[23]
- În octombrie 2019, Adobe a lăsat 7,5 milioane de înregistrări ale clienților Creative Cloud pe o bază de date nesecurizată. Scurgerea de informații a inclus adresele de e-mail și statutul plăților utilizatorilor.[24]
- În noiembrie 2019, Facebook a oferit acces necorespunzător la datele de profil ale celor 70 000 de clienți pentru aproximativ 100 de dezvoltatori de aplicații. Unul dintre aceștia a furat datele cu caracter personal și ulterior le-a folosit pentru a escroca clienții.[25]

- În decembrie 2019, un **politician olandez** a fost pasibil de 3 ani de închisoare pentru piratarea conturilor iCloud a 100 de femei și publicarea ilegală de fotografii nud. S-a constatat că politicianul a spart conturile personale iCloud ale femeilor cu acreditări găsite în încălcări anterioare ale bazelor de date publice.[26] În aceeași lună, detaliile a peste 10,7 milioane de oaspeți ai stațiunii **Metro-Goldwyn-Mayer (MGM)** au fost divulgate pe un forum de hacking. Informațiile divulgate includeau numele complete ale clienților, adresele de domiciliu, numerele de telefon, adresele de e-mail și datele de naștere.[27]

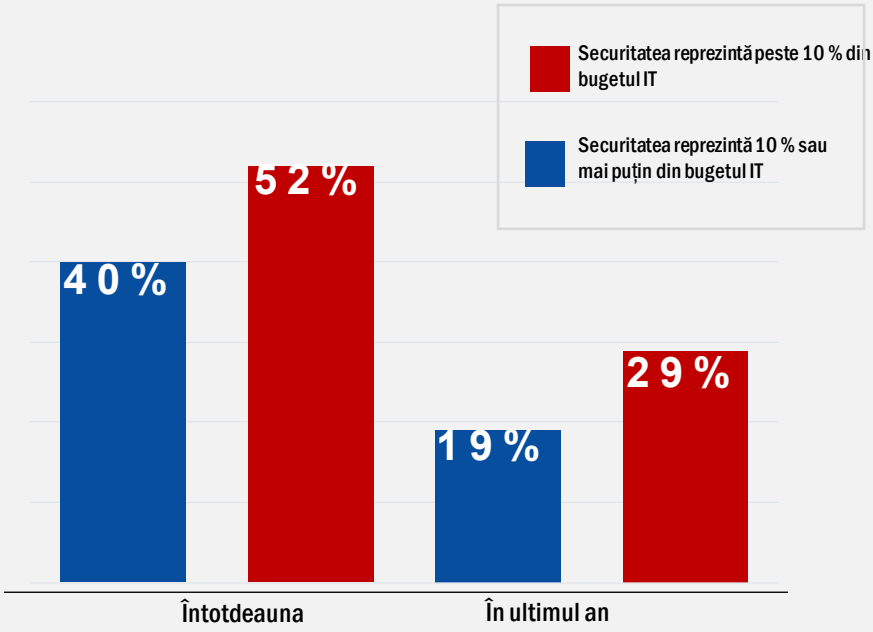


Figura 1: Ratele incidentelor de încălcare a securității în funcție de nivelul cheltuielilor pentru securitate. Sursa: CNET[14]

Vectori de atac

_Cum

Vectorul principal de atac în scurgerea de informații este reprezentat de deținătorii de informații privilegiate. Acest termen este folosit pentru a descrie o persoană cu interes în „exfiltrarea" informațiilor privilegiate importante în numele unui terț. Alți vectori de atac obișnuiți utilizați de această amenințare sunt configurațiile greșite, vulnerabilitățile și erorile umane.

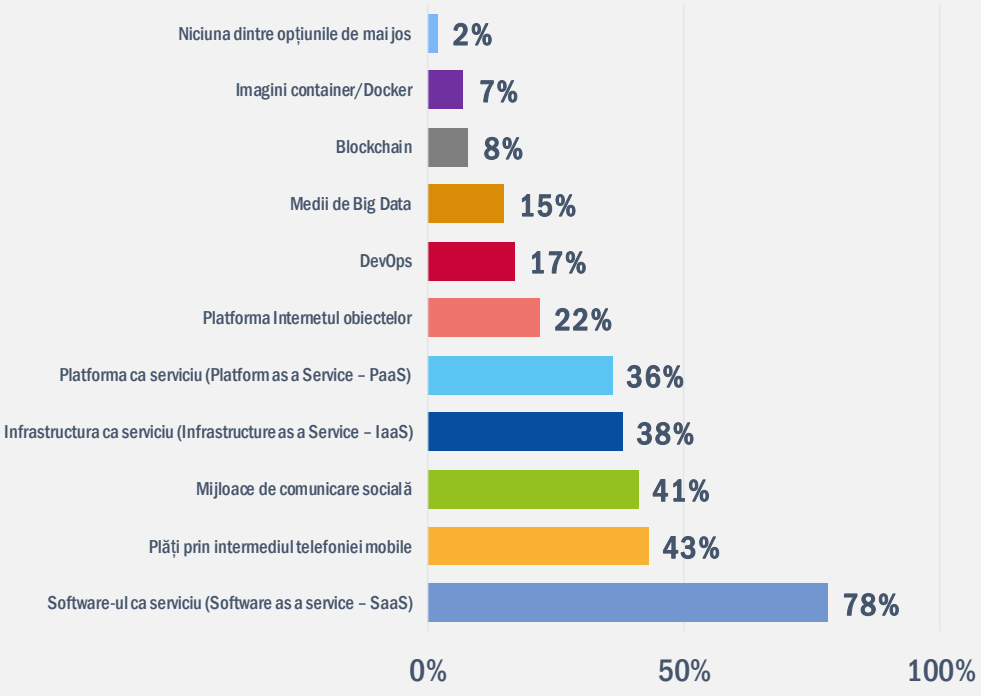


Figura 2: Tipuri de date sensibile sau reglementate stocate. Sursa: Thales[40]

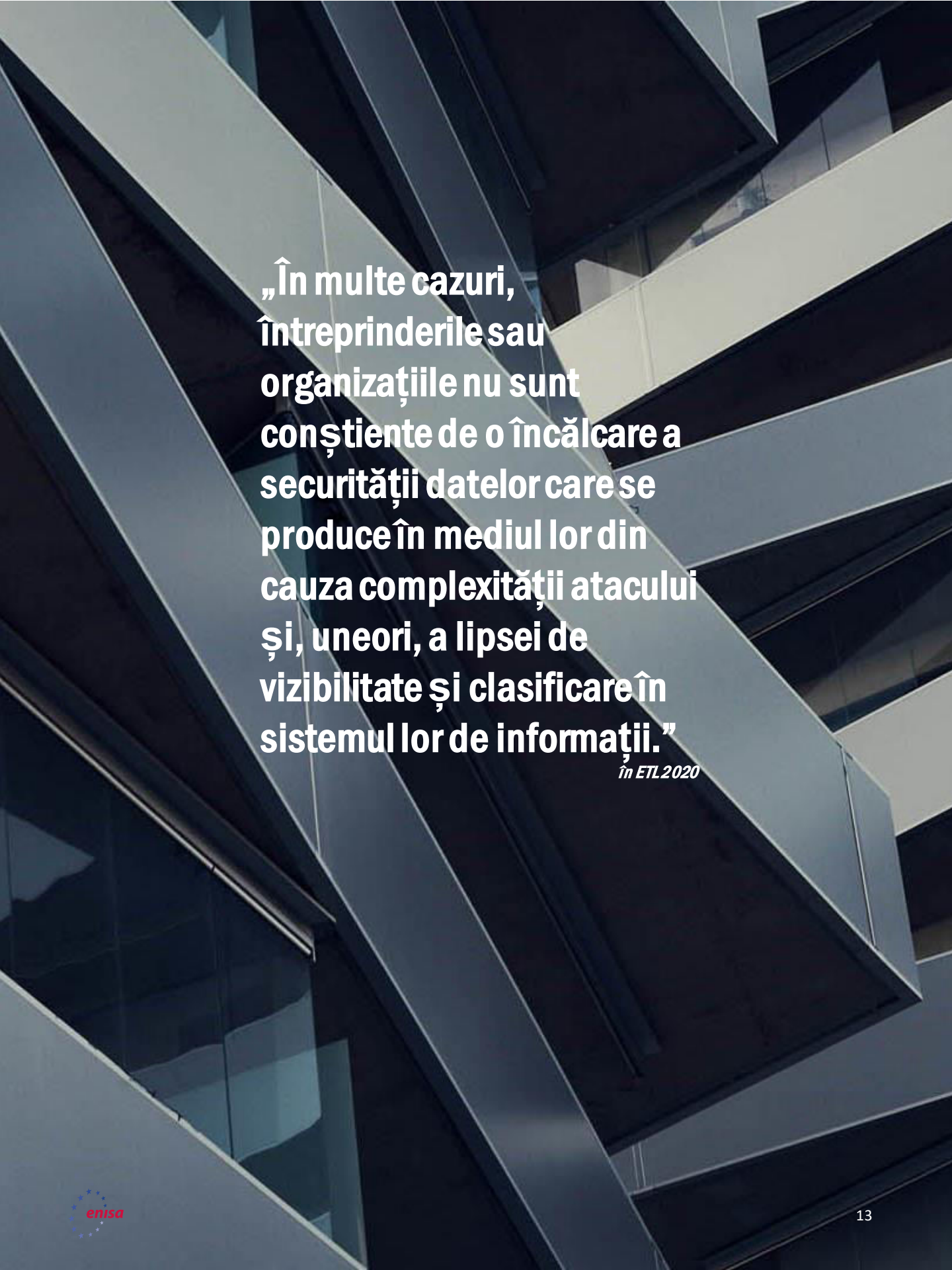
„Încălcarea securității datelor cauzează frecvent o scurgere de informații, care este una dintre amenințările cibernetice majore, acoperind o mare varietate de informații compromise”

în ETL 2020

Măsuri de atenuare:

Acțiuni propuse

- Anonimizarea, pseudonimizarea, minimizarea și cifrarea datelor în conformitate cu prevederile stabilite în RGPD al UE, în Legea privind confidențialitatea consumatorilor din California (CCPA) și în Protecția pe mai multe niveluri a securității informațiilor din China (MLPS 2.0).[28,29,30,31] Verificarea permanentă a angajamentelor de reglementare pentru entitățile omoloage care nu se încadrează în inițiative bilaterale sau multilaterale.[32,33,34]
- Stocarea datelor doar pe active IT sigure.[35]
- Limitarea privilegiilor de acces ale utilizatorilor conform principiului necesității de a cunoaște.[35,36] Revocarea privilegiilor de acces ale persoanelor care nu sunt angajate.[35]
- Educarea și instruirea periodică a personalului organizației dvs.[35,37]
- Utilizarea de instrumente tehnologice pentru a evita eventualele scurgeri de date, cum ar fi scanarea vulnerabilităților, scanarea malware-ului și instrumentele de prevenire a pierderii de date (DLP). Implementarea criptării datelor, a sistemului portabil și a dispozitivelor și interfețelor securizate.[36,38]
- Un plan de continuitate a activității (BCP) este crucial pentru a face față unei încălcări a datelor. Acest plan prezintă tipul de date stocate și locația acestora, precum și potențialele răspunderi care ar putea apărea la punerea în aplicare a acțiunilor de securitate și recuperare a datelor. Un BCP implică un răspuns eficace la incidente, care are ca scop soluționarea, gestionarea și rectificarea daunelor cauzate de un astfel de incident.[39]



„În multe cazuri, întreprinderile sau organizațiile nu sunt conștiente de o încălcare a securității datelor care se produce în mediul lor din cauza complexității atacului și, uneori, a lipsei de vizibilitate și clasificare în sistemul lor de informații.”

în ETL 2020

Referințe

1. „Ce este o încălcare a securității datelor și ce trebuie făcut în cazul unei asemenea încălcări?" Comisia Europeană. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_ro

2. „The human factor of cyber security" (Factorul uman al securității cibernetice). CSO. https://www.csoonline.com/article/3504813/the-human-factor-of-cyber-security.html

3. Howard Poston. „Common causes of large breaches (Q1 2019)" [Cauze frecvente ale marilor încălcări ale securității (T1 2019)]. 1 mai 2019. INFOSEC Institute. https://resources.infosecinstitute.com/common-causes-of-large-breaches/#gref

4. J. Clement. „Average cost of data breaches worldwide from 2014 to 2019" (Costul mediu al încălcărilor securității datelor la nivel mondial din 2014 până în 2019). 13 august 2019. Statista. https://www.statista.com/statistics/987474/global-average-cost-data-breach/

5. „2019 Data Breach Investigations Report" (Raportul investigațiilor privind încălcarea securității datelor din 2019). 2019. Verizon. https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

6. „CyberThreatscape Report" (Raport privind peisajul amenințărilor cibernetice) 2019. iDefense – Accenture. https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf

7. „Cybercrime will cost businesses over $2 trillion by 2019" (Criminalitatea informatică va costa întreprinderile peste 2 trilioane USD până în 2019). 12 mai 2015. Juniper Research https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion-by-2019

8. „How much would a data breach cost your business?" (Suma pe care întreprinderea dvs. ar trebui să o suporte pentru o încălcare a securității datelor). 2019. IBM. https://www.ibm.com/security/data-breach

9. G. Dautovic. „Top 25 Financial Data Breach Statistics for 2020" (Top 25 de statistici privind încălcarea securității datelor financiare pentru 2020). 11 martie 2020. Fortunly. https://fortunly.com/statistics/data-breach-statistics#gref

10. Davey Winder. „Data Breaches Expose 4.1 BIllion Records In First Six Months of 2019" (Încălcările securității datelor expun 4,1 miliarde de înregistrări în primele șase luni ale anului 2019). 20 august 2019. Forbes. https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/#40479be4bd54

11. „Cost of a Data Breach Report" (Costul unui raport de încălcare a securității datelor). 2019. Ponemon Institute – IBM. https://databreachcalculator.mybluemix.net/executive-summary/

12. Troy Hunt. „The 773 Million Record "Collection #1." Data Breach" (Încălcarea securității datelor din „Colecția nr. 1" de 773 de milioane de înregistrări). 17 ianuarie 2019. Troy Hunt. https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

13. Lewis Morgan. „List of data breaches and cyber attacks in February 2019 – 873,919,635 records leaked" (Lista de încălcări ale securității datelor și de atacuri cibernetice din februarie 2019 – 873 919 635 de înregistrări au făcut obiectul unei scurgeri de informații). 26 februarie 2019. IT Governance. https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-february-2019-692853046-records-leaked

14. Rae Hodge. „2019 Data Breach Hall of Shame: These were the biggest data breaches of the year" (Topul rușinii din 2019 în ceea ce privește încălcarea securității datelor: acestea au fost cele mai mari încălcări ale securității datelor din an) 27 decembrie 2019. CNET. https://www.cnet.com/news/2019-data-breach-hall-of-shame-these-were-the-biggest-data-breaches-of-the-year/

15. Catalin Cimpanu. „Indian govt agency left details of millions of pregnant women exposed online" (Agenție guvernamentală indiană a lăsat expuse online detalii despre milioane de femei gravide). 1 aprilie 2019. ZDNet. https://www.zdnet.com/article/indian-govt-agency-left-details-of-millions-of-pregnant-women-exposed-online/

16. Shelby Brown. „DoorDash data breach affected 4.9M customers, drivers, merchants" (Încălcarea securității datelor DoorDash a afectat 4,9 milioane de clienți, șoferi, comercianți). 26 septembrie 2019. CNET. https://www.cnet.com/news/doordash-data-breach-affected-4-9-million-customers-workers-and-merchants/

17. Jessica Davis. „11.9M Quest Diagnostics Patients Impacted by AMCA Data Breach" (11,9 milioane de pacienți ai Quest Diagnostics au fost afectați de încălcarea securității datelor AMCA). 3 iunie 2019. HealthITSecurity https://healthitsecurity.com/news/11.9m-quest-diagnostics-patients-impacted-by-amca-data-breach

18. Alfred Ng, Mark Serrels. „Capital One data breach involves 100 million credit card applications" (Încălcarea securității datelor la Capital One implică 100 de milioane de cereri de carduri de credit). 30 iulie 2019. CNET. https://www.cnet.com/news/capital-one-data-breach-involves-100-million-credit-card-applications/

19. Shelby Brown. „Data breaches timeline: EasyJet cyberattack exposes over 9M people, and more" (Cronologie privind încălcarea securității datelor: atacul cibernetic EasyJet expune peste 9 milioane de persoane și multe altele). 19 mai 2020. CNET. https://www.cnet.com/how-to/equifax-mgm-resorts-beyond-every-major-security-breach-and-data-hack-update/

20. Josh Taylor. „Major breach found in biometrics system used by banks, UK police and defence firms" (Încălcare majoră a securității constatată în sistemul de elemente biometrice utilizat de bănci, poliția britanică și companii din domeniul apărării). 14 august 2019. The Guardian. https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms

21. Guy Fawkes. „Report: Data Breach in Biometric Security Platform Affecting Millions of Users" (Raport: încălcarea securității datelor pe platforma de securitate biometrică care afectează milioane de utilizatori). 16 iunie 2020. vpnMentor. ttps://www.vpnmentor.com/blog/report-biostar2-leak/

22. „Cost of a Data Breach Report" (Costul unui raport de încălcare a securității datelor). 2019. Ponemon - IBM Security. https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.148238199.1762516747.1577395260-1128561362.1577395260

23. Oscar Gonzalez. „Zynga data breach exposed 200 million Words with Friends players" (Încălcarea securității datelor Zynga a expus 200 de milioane de jucători de Words with Friends). 1 octombrie 2019. CNET. https://www.cnet.com/news/people-rarely-change-their-passwords-after-a-data-breach-study-says/

24. John E Dunn. „Adobe database exposes 7.5 million Creative Cloud users" (Baza de date Adobe expune 7,5 milioane de utilizatori Creative Cloud). 28 octombrie 2019. Naked Security. https://nakedsecurity.sophos.com/2019/10/28/adobe-database-exposes-7-5-million-creative-cloud-users/

25. „Insider Sold 68K Customer Records to Scammers: Trend Micro" (Un deținător de informații privilegiate a vândut 68 000 de înregistrări ale clienților către escroci: Trend Micro). 8 noiembrie 2019. CISOMAG. https://www.cisomag.com/insider-sold-68k-customer-records-to-scammers-trend-micro/

26. Catalin Cimpanu. "Dutch politician faces three years in prison for hacking iCloud accounts and leaking nudes" (Politician olandez riscă 3 ani de închisoare pentru piratarea conturilor iCloud și publicarea ilegală de nuduri). 3 decembrie 2019. ZDNet. https://www.zdnet.com/article/dutch-politician-faces-three-years-in-prison-for-hacking-icloud-accounts-and-leaking-nudes/

27. Corinne Reichert. „MGM Resorts confirms data breach of 10.7 million guests" (Stațiunile MGM confirmă încălcarea securității datelor a 10,7 milioane de oaspeți). 19 februarie 2020 https://www.cnet.com/news/mgm-resorts-confirms-data-breach-of-10-million-guest-accounts/

28. „Regulamentul (UE) 2016/679 al Parlamentului și Consiliului European din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește procesarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor)." 27 aprilie 2016. Parlamentul European, Consiliul Uniunii Europene. https://eur-lex.europa.eu/legal-content/RO/ALL/?uri=celex%3A32016R0679

29. „AB-375 Privacy: personal information: businesses, Assembly Bill No. 375, Chapter 55" (Confidențialitate AB-375: informații cu caracter personal: întreprinderi, proiectul de lege al Adunării nr. 375, capitolul 55). 29 iunie 2018. California Legislative Information. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

30. Shrub Chandrasekaran, Justin Fishman. „China's Cybersecurity Future and its Impact on U.S. Business" (Viitorul securității cibernetice al Chinei și impactul său asupra afacerilor din SUA). 31 octombrie 2019. Jolt Digest. https://jolt.law.harvard.edu/digest/chinas-cybersecurity-future-and-its-impact-on-u-s-business

31. Reed Smith LLP. „MLPS 2.0: China's enhanced data security multi-level protection scheme and related enforcement updates" (MLPS 2.0: Schema consolidată de protecție pe mai multe niveluri a securității datelor din China și actualizările de aplicare aferente). 9 octombrie 2019. Lexology. https://www.lexology.com/library/detail.aspx?g=36c6932b-bf41-4e08-b430-e3bc839a2328

32. „Data protection if there's no Brexit deal" (Protecția datelor dacă nu există un acord Brexit). 13 septembrie 2018. GOV. UK, Departamentul pentru Digital, Cultură, Media și Sport. https://www.gov.uk/government/publications/data-protection-if-theres-no-brexit-deal/data-protection-if-theres-no-brexit-deal

33. Eduardo Ustaran, „Brexit and data protection: Laying the odds" (Brexit și protecția datelor: stabilirea cotelor). 21 septembrie 2018. Privacy Perspectives, iapp. https://iapp.org/news/a/brexit-and-data-protection-laying-the-odds/

34. Ibrahim Hasan. „Data protection and Brexit" (Protecția datelor și Brexit). 5 septembrie 2016. Gazette. https://www.lawgazette.co.uk/legal-updates/data-protection-and-brexit/5057412.article

35. Eric Dosal. „5 Tips to Prevent Data Leakage at Your Company" (5 sfaturi pentru a preveni scurgerile de date la întreprinderea dvs.). 15 martie 2018. Compuquip Cybersecurity. https://www.compuquip.com/blog/5-tips-to-prevent-data-leakage-at-your-company

36. „10 ways to protect sensitive business data" (10 moduri de a proteja datele comerciale sensibile). 28 octombrie 2019. QuoStar. https://www.quostar.com/blog/10-tips-to-help-prevent-a-data-leak/

37. „Annual Cybersecurity Report" (Raport anual privind securitatea cibernetică). 2018. Cisco https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf?dtid=odicdc000016&ccid=cc000160&oid=anrsc005679&ecid=8196&elqTrackId=686210143d34494fb27ff73da9690a5b&elqaid=9452&elqat=2

38. „Cybercrime tactics and techniques: Q2 2018" (Tactici și tehnici de criminalitate informatică: T2 2018). 2018. Malwarebytes Labs

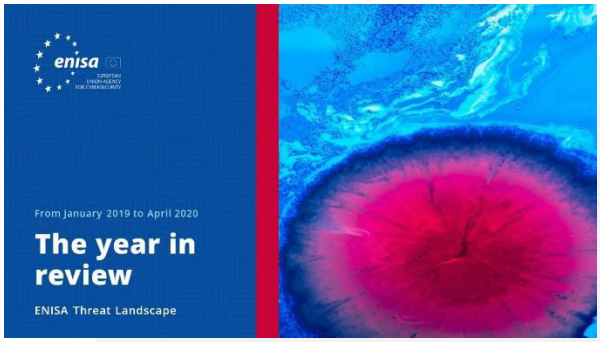
https://resources.malwarebytes.com/files/2018/07/Malwarebytes_Cybercrime-Tactics-and-Techniques-Q2-2018.pdf

39. Mona Mangat. „81 Eye-Opening Data Breach Statistics for 2020" (81 de statistici revelatoare despre încălcarea securității datelor pentru 2020). 27 ianuarie 2020. phoenixNAP. https://phoenixnap.com/blog/data-breach-statistics

40. „2020 Data Threat Report – Global Edition" (Raportul privind amenințările la adresa datelor 2020 – ediția globală). 2020. Thales Group. https://www.thalesesecurity.com/2020/data-threat-report

41. Oscar Gonzalez. „Zynga data breach exposed 200 million Words with Friends players" (Încălcarea securității datelor Zynga a expus 200 de milioane de jucători de Words with Friends). 1 octombrie 2019. C | net. https://www.cnet.com/news/words-with-friends-hack-reportedly-exposes-data-of-more-than-200m-players/

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**

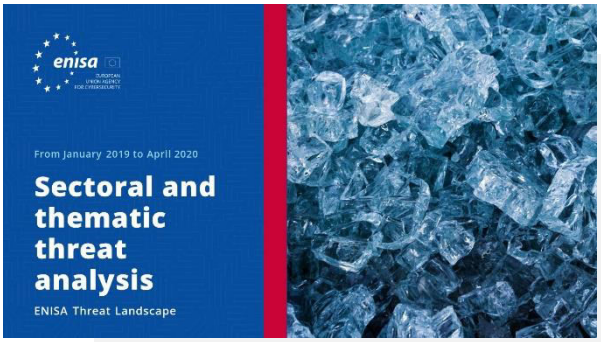
Lista ENISA a celor mai importante 15 amenințări din perioada ianuarie 2019 – aprilie 2020.

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



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.

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 trebuie 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