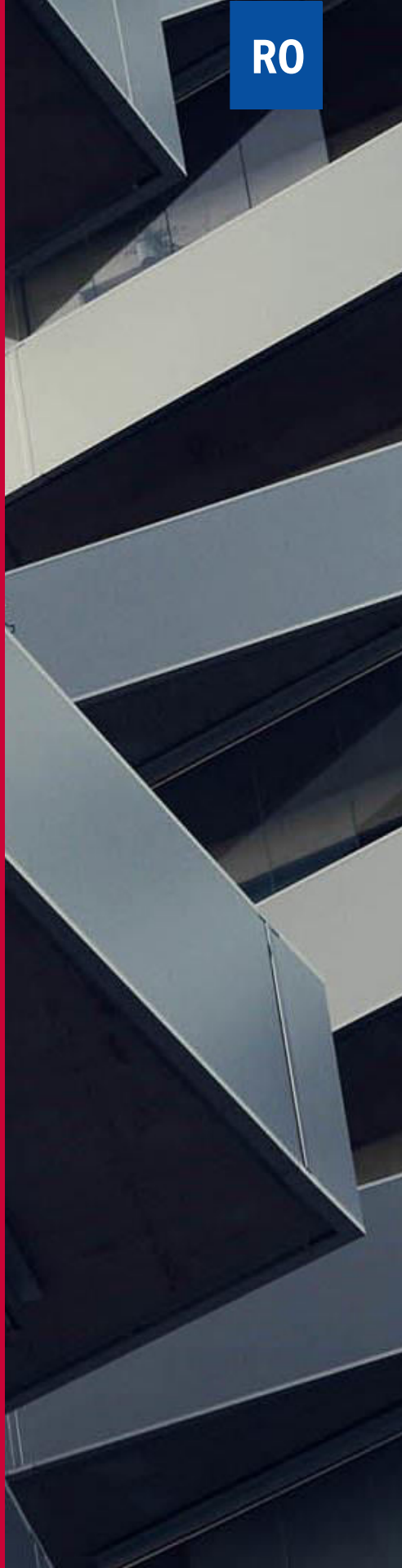
enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

RO



Ianuarie 2019 – aprilie 2020

Încălcarea securității datelor

Raportul ENISA privind situația amenințărilor

Prezentare generală

O încălcare a securității datelor este un tip de incident de securitate cibernetică în care informațiile (sau o parte a unui sistem de informații) sunt accesate fără autorizația corectă, de obicei cu rea intenție, ceea ce duce la potențiala pierdere sau utilizare abuzivă a informațiilor respective. Aceasta include, de asemenea, „eroarea umană" care se întâmplă adesea în timpul configurării și implementării anumitor servicii și sisteme și poate duce la expunerea neintenționată a datelor.[1]

În multe cazuri, companiile 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.[2] Pe baza cercetărilor, durează aproximativ 206 zile pentru a identifica o încălcare a securității datelor într-o organizație.[3] Astfel, ținând cont de timpul necesar pentru a izola, a remedia și a recupera datele, înseamnă că este nevoie de mai mult timp pentru a reveni la normal.

În pofida tuturor riscurilor implicate, organizațiile păstrează și mai multe date[4] folosind infrastructuri de stocare în cloud și medii complexe la sediu. Aceste medii sunt expuse treptat la riscuri noi și diferite, proporționale cu sensibilitatea informațiilor stocate. Nu este o surpriză faptul că numărul de încălcări a securității datelor a crescut în 2019 și 2020. Noile constatări sugerează, de asemenea, că impactul nu este resimțit exclusiv atunci când este descoperită o încălcare a securității datelor – impactul financiar poate persista mai mult de 2 ani după incidentul inițial.

Constatări

54 %_creștere a numărului total de încălcări până la jumătatea anului 2019 comparativ cu 2018.

71 %_ din încălcările securității datelor au fost motivate financiar. Aproape 25 % au avut obiective strategice pe termen lung (stat-națiune/spionaj).[5]

32 %_din încălcările securității datelor implică activitate de phishing în conformitate cu IOCTA 2019.[6] Un raport sugerează că phishing-ul se află în capul listei de contribuitori majori la încălcările securității datelor. Raportul menționează, de asemenea, că e-mailul este principala metodă de livrare a malware-ului (94 %) într-un lanț de evenimente care conduc la o încălcare a securității datelor.[3]

52%_din încălcările securității datelor au implicat hacking (piratare).[5] Alte tactici utilizate sunt atacurile sociale (33 %), malware (28 %) și greșelile sau erorile (21 %). Din 2016, hacking-ul a fost principala cauză a încălcării securității datelor în domeniul sănătății. În 2019, aproape 59 % din încălcările securității datelor raportate au fost cauzate de hacking.[7]

70 %_din încălcările securității datelor expun e-mailuri. Deși numele de utilizator/e-mailul și parolele (și anume datele de identificare) sunt ușor schimbate în comparație cu detaliile personale (și anume, data nașterii), accentul se pune mai ales pe acestea în cazurile de încălcare a securității datelor.[8]

55 %_din participanții la un sondaj Eurobarometru au răspuns că sunt îngrijorați că le-ar putea fi accesate datele de infractori și persoane care comit fraude.

Cronologie

2019

_ Ianuarie

MEGA cloud (NZ) a fost vizat de o încălcare a securității datelor, expunând 770 de milioane de e-mailuri și 21 de milioane de parole.[9]

_ Februarie

620 de milioane de conturi furate de pe 16 site-uri piratate se află în prezent la vânzare pe dark web, se laudă vânzătorul.[10]

_ Martie

12,5 milioane de fișe medicale ale femeilor însărcinate din centrul de asistență medicală al guvernului indian (IN), începând cu 2014, au fost făcute publice.[11]

_ Octombrie

Informațiile privind conturile a peste 7,5 milioane de utilizatori Adobe (SUA) au fost expuse din cauza unei baze de date online neprotejate.[18]

_ Septembrie

Mastercard (BE) a fost vizat de o încălcare a securității datelor care a afectat aproximativ 90 000 de clienți în Europa.[17]

_ August

În sistemul de elemente biometrice utilizat de bănci, poliție (Regatul Unit) și companii din domeniul apărării a fost constatată o încălcare majoră a securității.[16]

2020

_ Noiembrie

UniCredit (IT) a fost victima unei încălcări a securității datelor, care a dus la expunerea a 3 milioane de înregistrări.[19]

_ Decembrie

Furnizorul de camere inteligente Wyze (SUA) a fost vizat de două încălcări ale securității datelor la sfârșitul lunii decembrie, când bazele de date au fost lăsate expuse timp de peste două săptămâni.[20]

_ Ianuarie

250 de milioane de înregistrări de servicii și asistență pentru clienți de la Microsoft (SUA), care datează încă din 2005, au fost vizate de o încălcare a securității datelor.[21]

_ Aprilie

Facebook (SUA) a raportat o încălcare a securității datelor, expunând 540 de milioane de înregistrări ale utilizatorilor de pe serverele expuse.[12]

_ Mai

La First American Financial Corp. (SUA) s-a produs o scurgere de informații expunând sute de milioane de înregistrări ale asigurărilor de titlu.[13]

_ Iulie

S-a produs o încălcare a securității informațiilor cu caracter personal ale clienților cu carduri de credit Capital One (SUA).[15]

_ Iunie

100 de milioane de înregistrări au fost expuse prin accesul neautorizat la mediile de stocare a datelor clienților Evite.[14]

_ Februarie

Un server cloud Google (SUA) neprotejat care conține datele personale ale 200 de milioane de rezidenți din SUA.[22]

_ Martie

La compania de soluții biometrice Antheus Tecnologia (BR) s-a produs o scurgere de date.[23]

_ Aprilie

Hackerii au obținut detaliile de logare de la doi angajați Marriott (SUA) și au pătruns în sistem în ianuarie 2020.[24]

Tendințe

_Costul unei încălcări a securității datelor pentru organizații se întinde de-a lungul mai multor ani

Cercetătorii în domeniul securității au descoperit că o treime din costurile legate de încălcarea securității datelor sunt suportate la mai mult de un an de la incident. Mai precis, aproximativ 22 % din aceste costuri sunt suportate în al doilea an, în timp ce 11 % din costuri apar la mai mult de 2 ani după incidentul inițial. Aceste procente erau mai mari pentru organizațiile foarte reglementate, precum cele din serviciile financiare și sănătate, în comparație cu alte sectoare.[3]

Adoptarea de medii cloud sau multi-cloud crește rapid, similar cu cantitatea de date stocate și procesate în aceste medii.

_Micile greșeli ar putea duce la mari încălcări ale securității

Securizarea mediului cloud fără a pierde toată flexibilitatea pe care acesta o aduce infrastructurii și resurselor poate fi problematică. O singură configurare greșită poate conduce la expunerea întregii baze de date sensibile. Un cercetător în domeniul securității consideră că majoritatea încălcărilor securității datelor din cloud sunt rezultatul unei configurări greșite și sunt în mare parte neintenționate. Netflix, Ford și TD Bank sunt doar câteva exemple, printre multe altele. Dintr-o perspectivă diferită, deși încălcările securității datelor cauzate de tentative rău intenționate costă în continuare mai mult, încălcările cauzate de erorile sistemului sau erorile umane reprezintă în continuare un cost considerabil, în medie 3,24 milioane USD (aproximativ 2,74 milioane EUR).[3]

Încălcările securității datelor costă mai mult pentru întreprinderile mici

Costul încălcărilor securității datelor pentru întreprinderi sau organizații mari cu mai mult de 25 000 de angajați este de 204 USD (aproximativ 173 EUR) per angajat. Suma totală estimată la aproximativ 5,11 milioane USD (aproximativ 4,33 milioane EUR). În schimb, pentru întreprinderile mici (500-1 000 de angajați) costul mediu este de aproximativ 3 533 USD (aproximativ 3 000 EUR) pe angajat. Acesta reprezintă un cost total de 2,65 milioane USD (aproximativ 2,24 milioane EUR) pentru întreprinderile mici.[3]

Câștigul financiar este principala motivație

Se știe că entitățile rău intenționate/factorii de amenințare sunt responsabili de încălcările securității datelor (ținând cont că uneori acestea pot fi cauzate de o greșeală). În acest sens, factorii de amenințare externi reprezintă principala cauză a încălcării securității datelor, iar acest lucru ar putea include activități precum rețelele botnet. În acest sens, câștigul financiar a fost identificat în mod repetat drept principala motivație din spatele încălcărilor securității datelor facilitate de aceste grupuri de factori. Spionajul a fost, de asemenea, unul dintre motivele cheie din spatele încălcării securității datelor, dar nu la fel de important precum câștigurile personale sau financiare. Această tendință a fost aproape în concordanță cu rezultatele observate în 2010-2011.[5]

Tendințe

Preocupări legate de calculul cuantic și securitatea datelor

Cerințele de criptografie joacă un rol vital în era calculului cuantic și evidențiază probleme critice de securitate. 72 % din organizații consideră că metoda calculului cuantic le va afecta în mod strategic operațiunile legate de criptare (în următorii 5 ani). Conform rezultatelor sondajului, 92 % din respondenți sunt îngrijorați de expunerea datelor sensibile prin utilizarea acestei tehnologii în industria calculatoarelor. Principalele strategii sugerate de respondenți pentru a aborda astfel de preocupări au fost schimbarea arhitecturii de securitate și implementarea de infrastructuri-cheie de gestionare.[26]

Asistența medicală – o țintă constantă pentru actorii rău intenționați

Asistența medicală a continuat să fie una dintre cele mai atractive ținte pentru infractorii cibernetici care utilizează tehnici de ransomware[7] și phishing[7], care costă astfel de organizații milioane de euro pentru a le izola și pentru a se redresa în urma impactului. În 2019, 400 de companii din domeniul sănătății au raportat o încălcare a securității datelor din fișele medicale ale pacienților. Acesta a fost un record pentru organizațiile din domeniul sănătății.[7]

Multi-cloud – noua provocare pentru securitatea datelor

Un sondaj realizat de un cercetător în domeniul securității a raportat că 9 din 10 companii se gândesc să utilizeze sau utilizează deja medii cloud. Aproximativ 44 % din respondenții la sondaj consideră, de asemenea, că aceste medii constituie provocări pentru punerea în aplicare a măsurilor adecvate de securitate a datelor.[25]

Tipuri de date expuse (%)

Tipul de date	2019	2018	2017
E-mail	70	44	32
Parolă	64	39	27
Nume	23	37	41
Diverse	18	19	15
Număr de asigurare socială	11	22	27
Card de credit	11	16	19
Adresă	11	22	30
Cont	10	7	4
Necunoscute	8	13	18
Data nașterii	8	13	12
Date medicale	5	9	7
Date financiare	5	13	19

Tabelul 1 - Sursa: Cyber Risk Analytics[8]

Tendințe

_Scăderea continuă a încălcărilor securității tranzacțiilor realizate în cazurile în care este prezentat cardul (Card Present)

Potrivit unui raport de securitate, în 2019 s-a identificat o scădere a numărului de încălcări ale securității la punctele de vânzare (POS) și de furt de date de pe cardurile bancare (card skimming) (unde este prezentat cardul). Aceasta reprezintă o trecere de la metode tradiționale de skimming la bancomate[7] și plăți cu cardul la aplicații web în sectorul comerțului cu amănuntul. Deși numărul de incidente a scăzut în acest domeniu, nu este corect să se concluzioneze că numărul de încălcări ale securității datelor a scăzut, ci mai degrabă că se înregistrează o schimbare a vectorului. Deși scăderea ar putea fi legată de o aplicare mai largă a cardurilor/terminalelor cu cip și pin (cunoscute, de asemenea, ca EMV).[6]

_La ce să ne așteptăm în viitorul apropiat?

Potrivit unui cercetător în domeniul securității, organizațiile medicale trebuie să fie pregătite pentru o creștere cu 10 % -15 % a numărului de încălcări ale securității datelor, în care furnizorii lor de servicii vor reprezenta ținta principală.[7] În termeni generali, pe baza rezultatelor din primele 6 luni ale anului 2019, este de așteptat ca numărul de încălcări ale securității datelor să crească într-un ritm alarmant, în pofida conștientizării în rândul liderilor majori și a efortului depus de multe organizații pentru a-și securiza datele.[8]

Încălcări ale securității datelor în funcție de sector și dimensiunea organizației

Incidente	Încălcări ale securității	Mici	Mari	Necunoscute
Cazare	61	34	7	20
Administrativ	17	6	6	5
Agricultură	2	2	0	0
Construcții	11	7	3	1
Educație	99	14	8	77
Divertisment	10	2	3	5
Finanțe	207	26	19	162
Asistență medicală	304	29	25	250
Informații	155	20	18	117
Activitatea de conducere	2	1	1	0
Sectorul de producție	87	10	22	55
Minerit	15	2	5	8
Alte servicii	54	6	5	43
Sectorul profesional	157	34	10	113
Sectorul public	**330**	**17**	**83**	**230**
Sectorul imobiliar	14	6	3	5
Sectorul comerțului cu amănuntul	139	46	19	74
Comerț	16	4	8	4
Transporturi	36	3	9	24
Sectorul utilităților publice	8	2	0	6
Necunoscute	289	0	109	180
Total	2 013	271	363	1 379

Tabelul 2 - Sursa: Verizon DBIR, 2019[5]

Vectori de atac

- **E-MAIL/PHISHING**. Uzurparea identității unui furnizor terț sau a unui partener folosind e-mailul este o victorie ușoară pentru actorii rău intenționați. Se știe că acesta este vectorul cel mai des folosit de infractorii cibernetici pentru a-și viza victimele și pentru a cauza majoritatea încălcărilor securității datelor (aproape 40 % din încălcările securității în domeniul sănătății).[7,]
- **APLICAȚII CLOUD/WEB.** Aceasta reflectă utilizarea aplicațiilor web ca vector pentru tentativele actorilor rău intenționați de a încălca securitatea datelor sau operațiunile critice. Furtul de date de identificare pentru a accesa portalurile de e-mail bazate pe web este un prim exemplu. Exploatarea punctelor slabe din serverele de aplicații pentru a injecta/livra malware care fură informații sau atacuri de formjacking sunt alte exemple privind acest vector.[↗]
- **AMENINȚĂRILE DIN INTERIOR.** Aceasta se referă în principal la tentativele neautorizate sau rău intenționate de a utiliza resurse. Trebuie remarcat faptul că, în general în analiză și raportare, configurările greșite sau greșelile (erori umane) din partea echipelor interne pot fi denumite, de asemenea, „amenințări din interior". Deși majoritatea încălcărilor securității datelor sunt facilitate de actori rău intenționați externi, este în continuare valabil că deținătorii de informații privilegiate cu sau fără acces privilegiat joacă un rol cheie în încălcările securității datelor.[5]

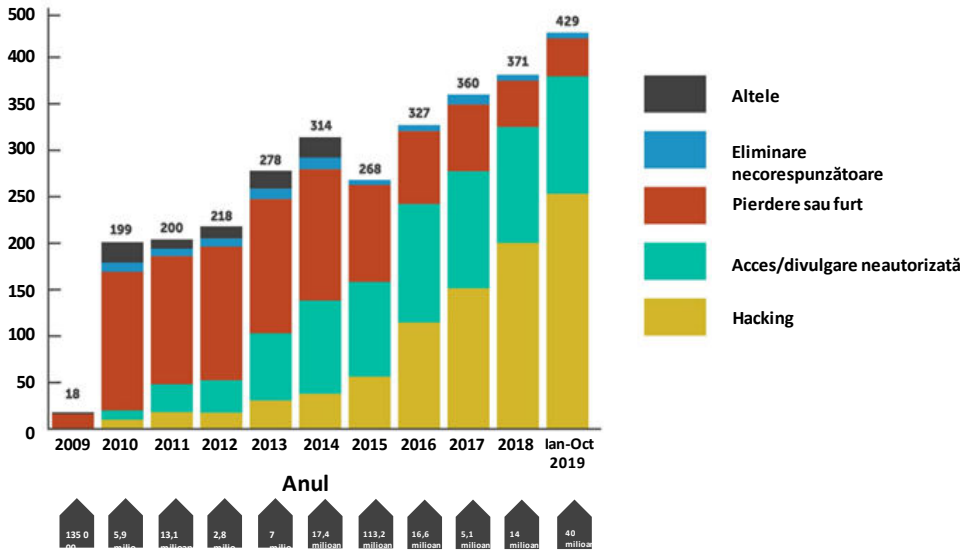
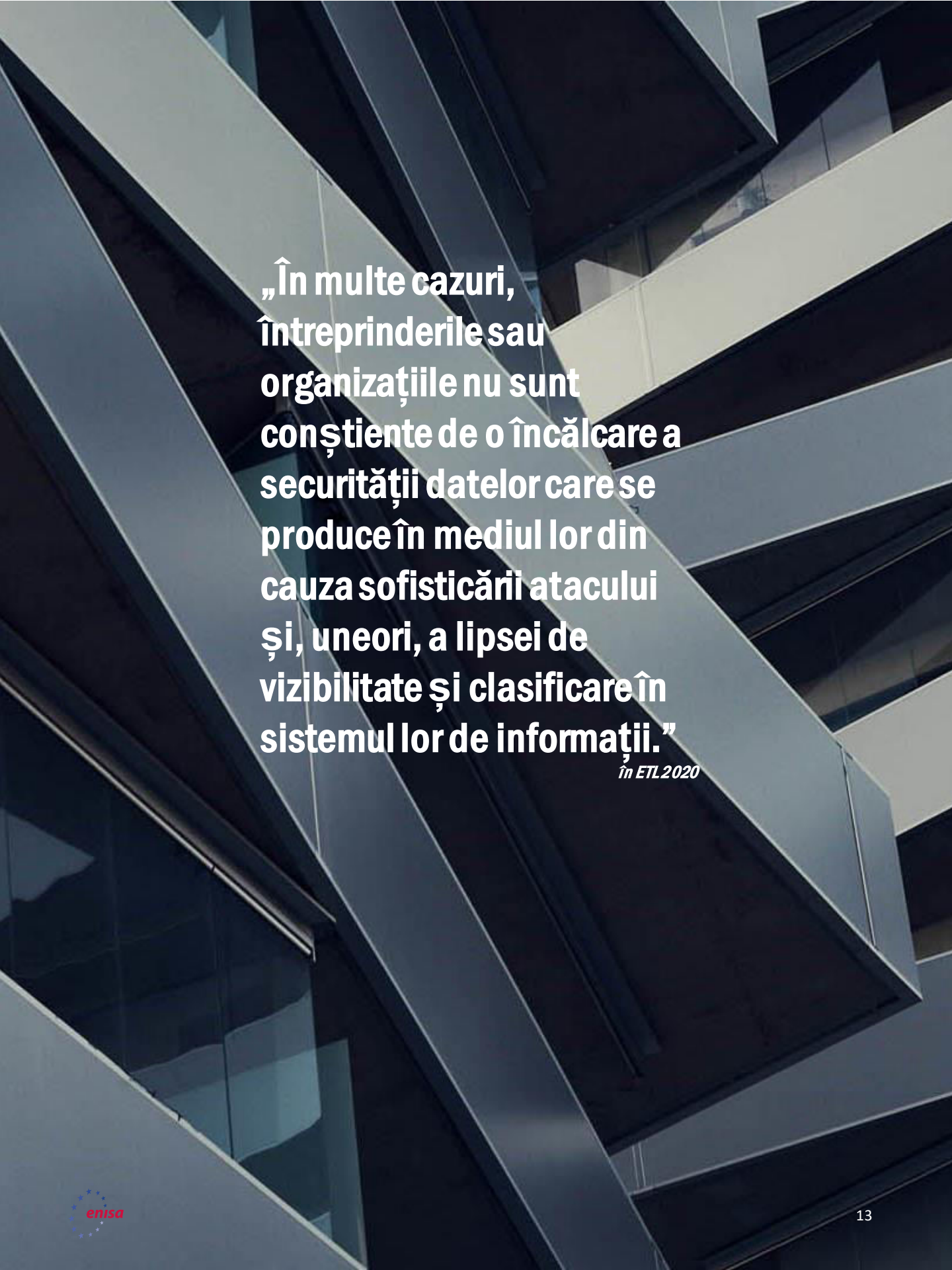


Figura 1: Entități implicate într-o încălcare a securității. Sursa: Horizon[7]



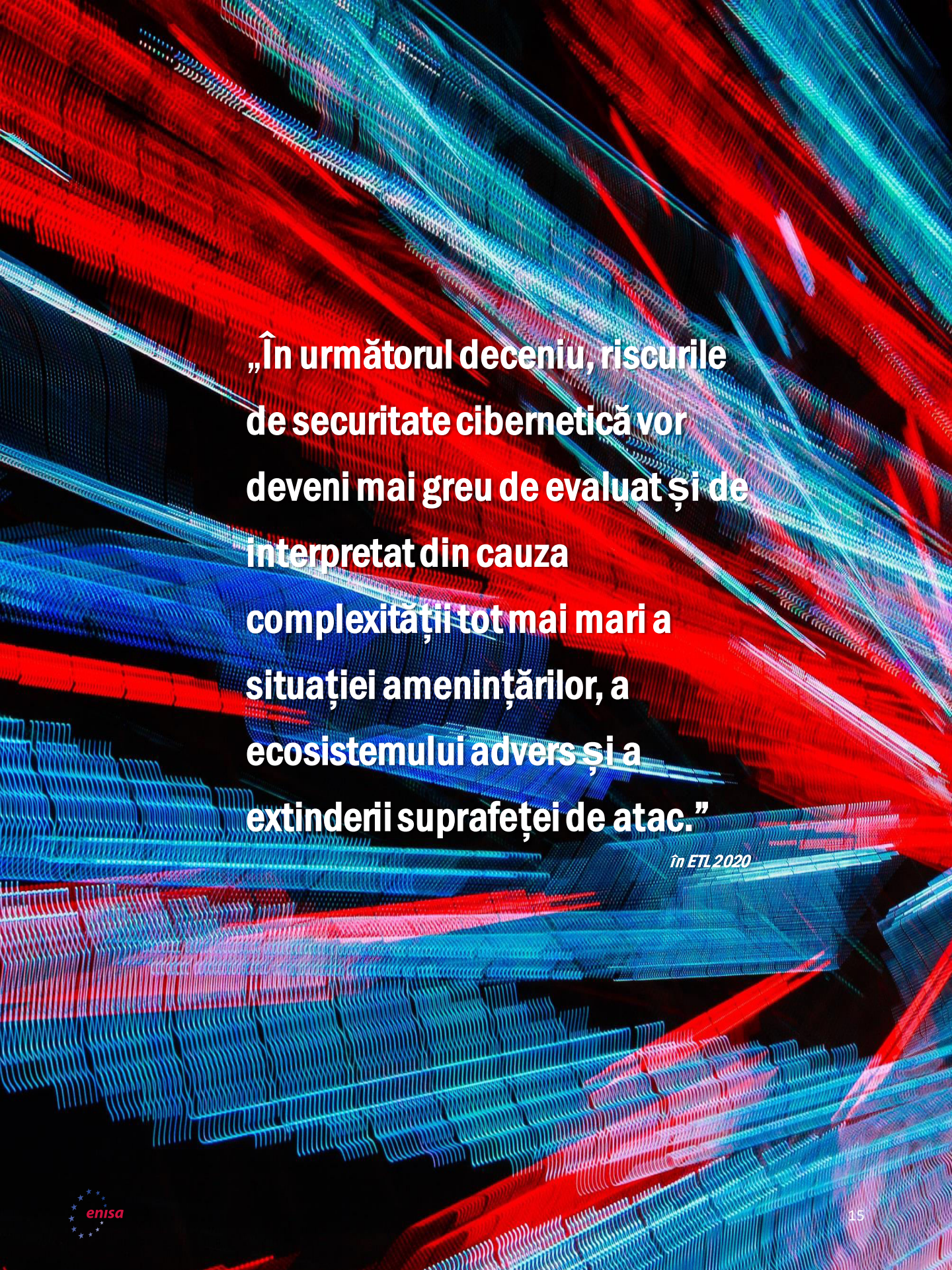
„În multe cazuri, întreprinderile sau organizațiile nu sunt conștiente de o încălcare a securității datelor care se produce în mediul lor din cauza sofisticării atacului și, uneori, a lipsei de vizibilitate și clasificare în sistemul lor de informații.”

în ETL 2020

Măsuri de atenuare

Acțiuni propuse

- Încălcarea securității datelor este, în general, rezultatul altor amenințări, iar atenuarea se suprapune cu altele discutate în acest raport.
- Luarea în considerare a investițiilor în instrumente hibride de securitate a datelor care se concentrează pe operarea într-un model de responsabilitate partajată pentru medii bazate pe cloud.[26]
- Elaborarea și menținerea unui plan de conștientizare a securității cibernetice. Furnizarea de scenarii de instruire și simulare pentru identificarea campaniilor de inginerie socială și phishing pentru personal.[7]
- Înființarea și menținerea unei echipe de răspuns la incident și evaluarea frecventă a planurilor de răspuns la incidente.[3]
- Identificarea și clasificarea datelor sensibile/cu caracter personal și aplicarea de măsuri pentru criptarea acestor date în tranzit și în repaus.[3] Cu alte cuvinte, implementarea de capacități de prevenire a pierderii de date.
- Intensificarea investițiilor în instrumente de detectare și alertare și în capacitatea de a izola și de a răspunde la o încălcare a securității datelor.
- Elaborarea și menținerea de politici puternice care impun parole puternice (gestionarea parolelor) și utilizarea autentificării cu mai mulți factori.
- Luarea în considerare a utilizării modelelor care adoptă abordarea „privilegiilor minime” pentru a asigura securitatea atât pentru resursele din spațiile comerciale, cât și pentru cele din afara acestora (și anume, modelele bazate pe principiul „încredere zero”).
- Investirea în politici și planuri și crearea de politici și planuri pentru implicarea în echipe de guvernanță, de gestionare a riscurilor și de conformitate.[26]


„În următorul deceniu, riscurile de securitate cibernetică vor deveni mai greu de evaluat și de interpretat din cauza complexității tot mai mari a situației amenințărilor, a ecosistemului advers și a extinderii suprafeței de atac.”
în ETL 2020

Referințe

1. „What is data breach?" (Ce este încălcarea securității datelor?) Norton. https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html

2. „What is data breach?" (Ce este încălcarea securității datelor?) Malwarebytes. https://www.malwarebytes.com/data-breach/

3. „Cost of Data Breach Report" (Raport privind costul încălcării securității datelor) 2019. IBM Security, Ponemon Institute. https://www.ibm.com/security/data-breach

4 Dhritimaan Shukla, Kush Wadhwa. „Data breach – threat landscape. Unauthorised exposure of an organisation's critical data" (Încălcarea securității datelor – situația amenințărilor. Expunerea neautorizată a datelor critice ale unei organizații). PWC India. https://www.pwc.in/consulting/forensic-services/data-breach-threat-landscape.html

5. „Verizon Data Breach Investigations Report" (Raportul Verizon privind investigațiile legate de încălcarea securității datelor). 2020. Verizon. https://enterprise.verizon.com/resources/reports/dbir/

6. Catherine De Bolle. „Internet Organised Crime Threat Assessment (IOCTA)" (Evaluarea amenințării pe care o reprezintă criminalitatea organizată online) 2019. Centrul european de combatere a criminalității informatice (European Cybercrime Centre, EC3), Europol. https://www.europol.europa.eu/iocta-report

7. „2020 Healthcare Cybersecurity Horizon Report" (Raport 2020 privind orizontul securității cibernetice în domeniul sănătății). 2020. Fortified Health Security. https://fortifiedhealthsecurity.com/wp-content/uploads/2019/12/Fortified-Health-Security-2020-Horizon-Report.pdf

8. Inga Goddijn. „2019 Midyear QuickView Data Breach Report – Cyber Risk Analytics" (Raport privind încălcarea securității datelor QuickView la jumătatea anului 2019 – Analiza riscurilor cibernetice). August 2019. https://pages.riskbasedsecurity.com/hubfs/Reports/2019/2019%20MidYear%20Data%20Breach%20QuickView%20Report.pdf

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

10. Chris Williams. „620 million accounts stolen from 16 hacked websites now for sale on dark web, seller boasts" (620 de milioane de conturi furate de pe 16 site-uri web piratate acum pentru vânzare pe dark web, se laudă vânzătorul), 11 februarie 2019. The Register. https://www.theregister.com/2019/02/11/620_million_hacked_accounts_dark_web/

11. 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/

12. „Losing Face: Two More Cases of Third-Party Facebook App Data Exposure" (Pierderea credibilității: încă două cazuri de expunere de date de aplicații Facebook terțe). 3 aprilie 2019. UpGuard. https://www.upguard.com/breaches/facebook-user-data-leak

13. „First American Financial Corp. Leaked Hundreds of Millions of Title Insurance Records" (First American Financial Corp a înregistrat o scurgere de informații, expunând sute de milioane de înregistrări ale asigurărilor de titlu). 24 mai 2019. KrebsonSecurity. https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records/

14. „Data Incident, Evite" (Incident de date, Evite). 14 mai 2019. Evite. https://www.evite.com/security/update

15. „Information on the Capital One Cyber Incident" (Informații despre incidentul cibernetic Capital One). 23 septembrie 2019. CapitalOne. https://www.capitalone.com/facts2019/

16. 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

17. Neil Hodge. „Mastercard reveals data breaches in third-party loyalty program" (Mastercard dezvăluie încălcări ale securității datelor în cadrul unui program de fidelitate terț). 27 august 2019. Compliance Week.

https://www.complianceweek.com/data-privacy/mastercard-reveals-data-breaches-in-third-party-loyalty-program/27614.article

18. Catalin Cimpanu. „Adobe left 7.5 million Creative Cloud user records exposed online" (Adobe a lăsat 7,5 milioane de înregistrări ale utilizatorilor Creative Cloud expuse online). 26 octombrie 2019. ZDNet. https://www.zdnet.com/article/adobe-left-7-5-million-creative-cloud-user-records-exposed-online/

19. Charlie Osborne. „UniCredit reveals data breach exposing 3 million customer records" (UniCredit dezvăluie o încălcare a securității datelor, care a cauzat expunerea a 3 milioane de date despre clienți). 28 octombrie 2019. ZDNet. https://www.zdnet.com/article/unicredit-reveals-data-breach-exposing-3-million-customer-records/

20. Chris Isidore. „Smart camera maker Wyze hit with customer data breach" (Furnizorul de camere inteligente Wyze a fost vizat de o încălcare a securității datelor clienților). 30 decembrie 2019. CNN. https://edition.cnn.com/2019/12/30/tech/wyze-data-breach/index.html

21. Davey Winder. „Microsoft Security Shocker As 250 Million Customer Records Exposed Online" (Dezvăluire șocantă de securitate la Microsoft, cu 250 de milioane de înregistrări ale clienților expuse online) 22 ianuarie 2020. Forbes. https://www.forbes.com/sites/daveywinder/2020/01/22/microsoft-security-shocker-as-250-million-customer-records-exposed-online/#2d3f9dca4d1b

22. Paul Bischoff. „US property and demographic database of 200 million records leaked on the web" (200 de milioane de înregistrări din baza de date demografice și funciare din SUA, a făcut obiectul unei scurgeri de informații pe internet). 5 martie 2020. comparitech. https://www.comparitech.com/blog/vpn-privacy/200-million-us-database-leaked/

23. Jim Wilson. „Brazil: Millions of Records Leaked, Including Biometric Data" (Brazilia: milioane de înregistrări au făcut obiectul unei scurgeri de informații, inclusiv date biometrice). 11 martie 2020. Safety Detectives. https://www.safetydetectives.com/blog/antheus-leak-report/

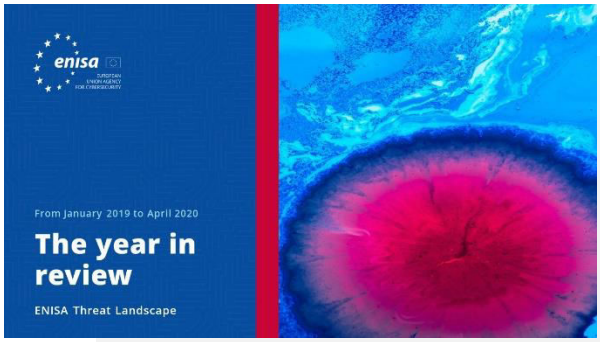
24. Zack Whittaker. „Marriot says 5.2 million guest records were stolen in another data breach" (Marriott afirmă că 5,2 milioane de înregistrări ale oaspeților au fost furate într-o altă încălcare a securității datelor) 1 aprilie 2020. Techrunch. https://techcrunch.com/2020/03/31/marriott-hotels-breached-again/?renderMode=ie11

25. "2019 Thales Data Threat Report – Global Edition" (Raportul Thales 2019 privind amenințările la adresa datelor – Ediție globală), Thales Security, 2019. https://cpl.thalesgroup.com/data-threat-report

26. "2020 Thales Data Threat Report – Global Edition" (Raportul Thales 2020 privind amenințările la adresa datelor – Ediție globală), Thales Security, 2020. https://cpl.thalesgroup.com/data-threat-report

27. Laura Paine. „2019 Verizon DBIR Shows Web Applications and Human Error as Top Sources of Breach" (Verizon DBIR 2019 arată aplicațiile web și eroarea umană ca fiind surse importante de încălcare a securității datelor) 8 mai 2019. Veracode. https://www.veracode.com/blog/security-news/2019-verizon-dbir-shows-web-applications-and-human-error-top-sources-breach

Documente conexe



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

Un 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

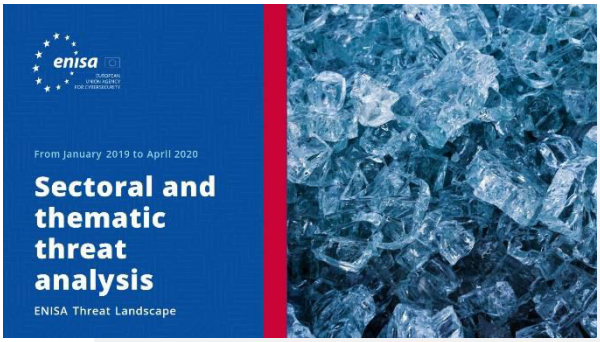
Lista ENISA a celor mai importante 15 amenințări din perioada ianuarie 2019 – aprilie 2020.

CITIȚI RAPORTUL

Raportul ENISA privind situația amenințărilor
Teme de cercetare

Recomandări privind teme de cercetare din 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

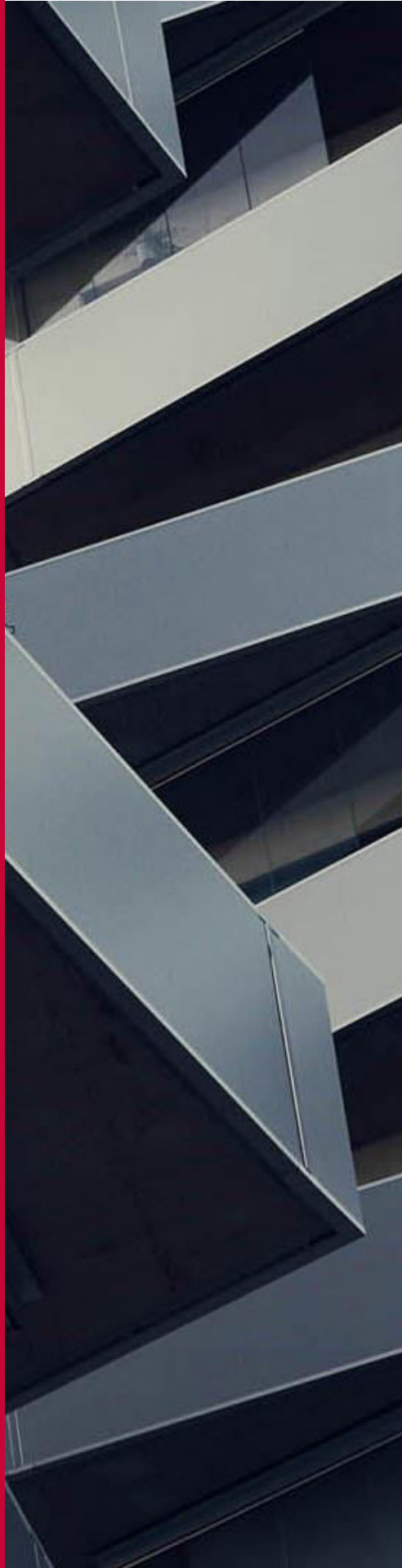
Trebuie luat în considerare faptul că această publicație reprezintă punctele de vedere și interpretările ENISA, cu excepția cazului în care se prevede altfel. Această publicație nu ar trebui interpretată ca o acțiune juridică a ENISA sau a organismelor ENISA, cu excepția cazului în care aceasta a fost 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