enisa

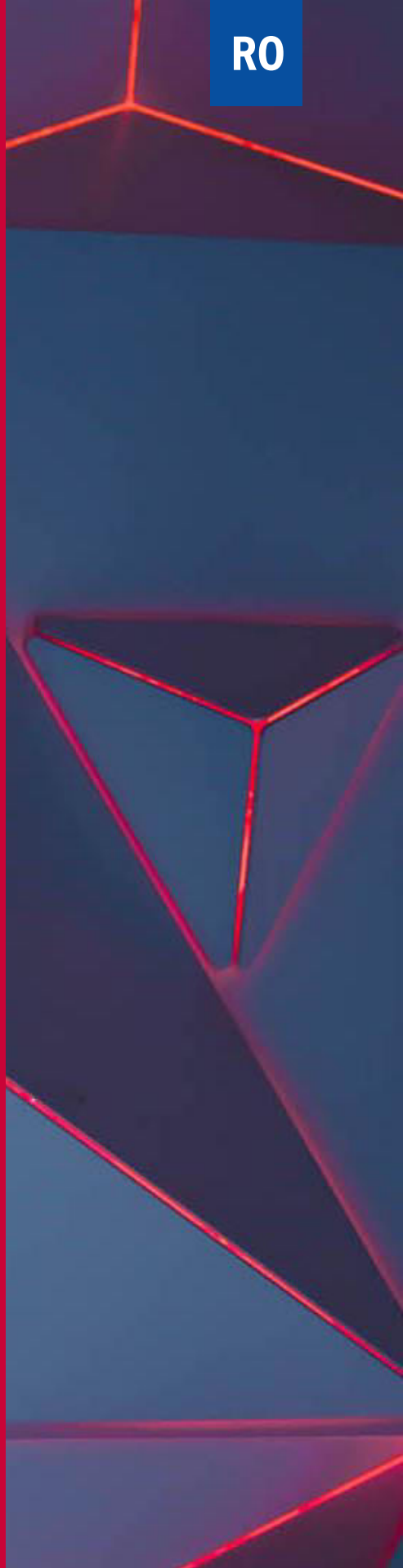
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

RO

ianuarie 2019 – aprilie 2020

Manipularea fizică/ deteriorarea/ furtul/pierderea

Raportul ENISA privind situația amenințărilor



Prezentare generală

Manipularea fizică, deteriorarea, furtul și pierderea s-au schimbat drastic în ultimii ani. Integritatea dispozitivelor este vitală pentru ca tehnologia să devină mobilă și pentru majoritatea implementărilor Internetului obiectelor (IoT). IoT poate spori securitatea fizică cu soluții mai avansate și mai complexe.[1] În acest mod, sistemele bazate pe securitatea IP cu senzori inteligenți, camerele Wi-Fi, iluminatul inteligent de securitate, dronele și încuietorile electronice pot furniza date de supraveghere care sunt evaluate de inteligența artificială (IA) și mecanismele de învățare automatizată (machine learning – ML) pentru a identifica amenințările și a răspunde cu întârziere minimă și precizie maximă.[2] Cu toate acestea, clădirile inteligente, dispozitivele mobile și dispozitivele portabile inteligente pot fi exploatate pentru a evita măsurile de securitate fizică.[3]

În 2019, atacurile fizice legate de bancomate și POS-uri au continuat în Europa și în întreaga lume, dar pierderile rezultate au fost mai mici decât media din ultimul deceniu. Vestea bună este că întreprinderile, managerii IT și factorii de decizie se orientează către planuri hibride de securitate cibernetică și fizică, deși în trecut securitatea fizică nu era o prioritate.

_Practici de securitate noi și învechite

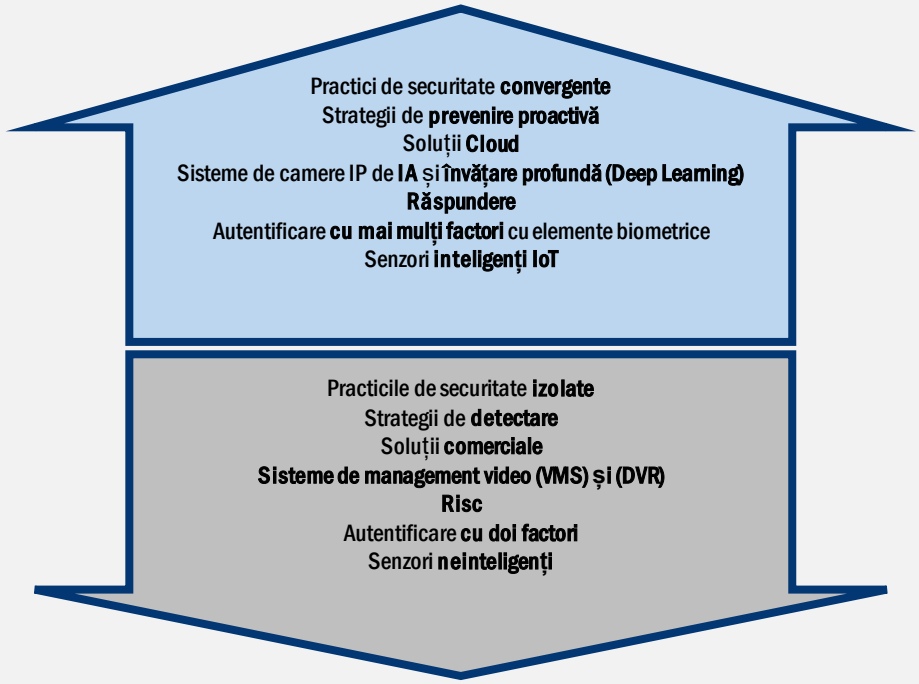
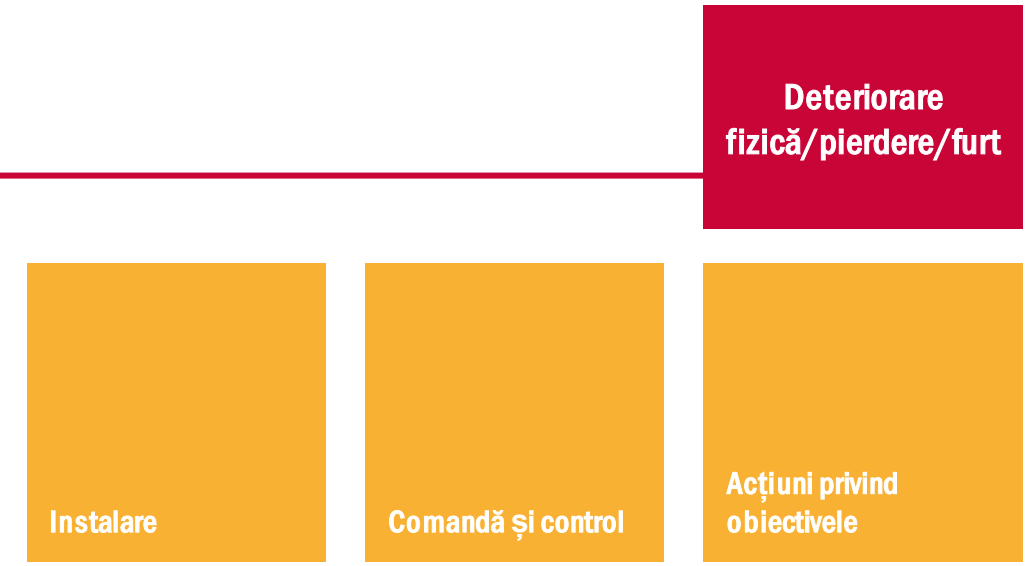


Figura 1 - Sursă: Boonedam blog[4]

Kill chain

Etapă din fluxul de activitate de atac

Amploarea scopului



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

Tendințe

_Accesul fizic este cea mai mare vulnerabilitate tip backdoor

În aprilie 2019, Vishwanath Akuthota a pledat vinovat la acuzația de vandalism, după ce a distrus echipamente cu încărcare electrică folosind un dispozitiv USB rău intenționat. Dispozitivele distruse aparțineau Colegiului Saint Rose din Albany, New York, facultatea pe care o absolvise Akuthota. În scopul atacului, acesta a accesat 66 de stații de lucru și numeroase monitoare și podiumuri digitale. Cheia „USB killer" pe care a folosit-o a fost achiziționată online. Colegiul a cheltuit peste 50 000 USD (aproximativ 42 452 EUR) pentru a înlocui echipamentul și peste 7 000 USD (aproximativ 5 943 EUR) pentru a plăti angajatul care s-a ocupat de acest incident. Akuthota a fost pasibil de 10 ani de închisoare și o amendă maximă de 250 000 USD (aproximativ 212 257 EUR).[5]

_Întreprinderile nu acordă atenție securității fizice

În cursul anului 2019 au fost efectuate diferite sondaje privind securitatea fizică. Unele dintre aceste sondaje s-au concentrat asupra directorilor executivi, managerilor IT și factorilor de decizie din mai multe industrii, iar rezultatele oferă o imagine corespunzătoare despre modul în care este gestionată securitatea fizică în cadrul companiilor. Directorii executivi din sectoarele industriale păreau să se orienteze către un plan combinat de securitate cibernetică și fizică pentru a-și proteja activele împotriva amenințărilor, luând în considerare factori precum amenințările din interior, importanța infrastructurii și integritatea rețelelor companiei. În aceste planuri combinate de securitate, cel mai mare accent, cel mai mare buget și cei mai mulți angajați erau alocați investițiilor în securitatea cibernetică (și anume 83-86 % din resursele respective), în timp ce 14-17 % din resursele companiei erau cheltuite pentru securitate fizică. În Europa, majoritatea managerilor IT (77 %) au declarat că securitatea fizică a activelor companiei lor era depășită.[7]

_Securitatea fizică ca serviciu

O tendință în 2019 a fost îmbunătățirea securității fizice prin activarea soluțiilor de securitate găzduite. Majoritatea planurilor de securitate ale managerilor IT s-au reorientat către schemele cloud și IoT sau intenționau să facă această schimbare într-o perioadă de 12 luni. Factorii de decizie au raportat că evaluau deja soluțiile de supraveghere video ca serviciu (video surveillance-as-a-service – VSaaS) și de control al accesului ca serviciu (access control as-a-service – ACaaS) pentru a îmbunătăți depistarea incidentelor și timpii minimi de răspuns și pentru a reduce ratele de rezultate fals pozitive. VSaaS și ACaaS au îmbunătățit atât securitatea fizică, cât și securitatea cibernetică, deși doar câțiva dintre managerii IT au identificat securitatea fizică ca prioritare.[8]

_Securitatea fizică a bancomatelor nu a trecut testul timpului

Astfel cum s-a observat în 2018, în această perioadă de raportare, bancomatele au fost vulnerabile la manipulări și daune fizice, cu scopul final de a fura banii din interior. În Irlanda, au fost raportate nouă incidente doar în primul trimestru al anului 2019.[9] Unii dintre atacatori au fost foarte dramatici, folosind excavatoare furate, spărgând ziduri și punând bancomatele în dube sau mașini. În alte cazuri, atacurile au fost finalizate în câteva minute, folosind explozibili, lanțuri și spargerea cu berbecul.[10] În Țările de Jos, într-un singur weekend din noiembrie au avut loc 71 de atacuri cu bombă la bancomate (Plofkraken în neerlandeză), comparativ cu 43 de atacuri similare în cursul anului 2018. Banca ABN AMRO a fost nevoită să elimine 470 de bancomate vulnerabile, iar Asociația Bancară Olandeză (NVB) a decis să închidă toate bancomatele la nivel național în fiecare seară între orele 23.00 și 7.00 în decembrie.[11] În 2019, pentru al patrulea an consecutiv, a crescut numărul de atacuri fizice asupra bancomatelor.

Tendințe

_ Interferența cu bancomatul

În cursul anului 2019, principalele expresii ale interferenței cu bancomatul au fost blocarea cardurilor, blocarea numerarului și fraudarea inversării tranzacțiilor. Imaginea de ansamblu a anului este că interferența cu bancomatele și pompele de benzină a scăzut datorită creșterii numărului de plăți EMV. Standardul EMV, numit după cele trei companii care l-au introdus (și anume, Europay, Mastercard și Visa), descrie specificațiile pentru carduri inteligente, terminale de plată și bancomate. Cardurile EMV (aka Chip și PIN sau carduri chip) au integrate cipuri cu circuite. Adoptarea cardurilor EMV a întrerupt frauda cu prezentarea cardului, cel puțin parțial.[12] Din păcate, cardurile EMV nu sunt încă utilizate pe scară largă în afara Europei și, chiar în Europa, doar câteva țări au adoptat controlul geografic, un element antifraudă al cardului EMV.[13]

_ Incidente

- Încălcarea securității de tip Killer USB evidențiază nevoia de securitate fizică. Vishwanath Akuthota, un absolvent al Colegiului Saint Rose din Albany, New York, a pledat vinovat la acuzația de vandalism asupra unor echipamente folosind un dispozitiv USB rău intenționat.[5]
- Escrocii folosesc un excavator pentru a fura bancomate din Irlanda de Nord. Numărul atacurilor fizice asupra bancomatelor este în creștere în întreaga UE.[9]
- Plofkraken în neerlandeză. Atacuri cu explozibili (cunoscute sub numele de „Plofkraken") asupra unor bancomate din Țările de Jos. Concentrate în principal asupra automatelor băncii ABN AMRO din cauza unei vulnerabilități. Acestea au determinat banca să elimine aproximativ 470 dintre bancomatele sale din Țările de Jos.[11]

Constatări

4 %_ din încălcări au fost cauzate de acțiuni fizice[12]

20 %_ din incidentele de securitate cibernetică au început sau s-au încheiat cu o acțiune fizică[12]

A cincea_ cea mai frecventă acțiune rău intenționată asupra bunurilor a fost reprezentată de atacurile fizice asupra bancomatelor[12]

54 %_ din încălcările securității datelor din toate sectoarele au inclus un atac fizic ca metodă principală

48 %_ din managerii IT utilizează supravegherea video bazată pe cloud sau controlul accesului[8]

72 %_ din angajați consideră că lăsarea informațiilor sensibile în zone accesibile publicului este cea mai gravă amenințare la adresa securității datelor[14]

65 %_ din peste 1 000 de angajați chestionați au raportat că se comportă în moduri riscante și adoptă practici identificate ca fiind riscante pentru securitatea fizică[15]

Măsuri de atenuare

_Acțiuni propuse

- Utilizarea criptării în toate stocările și fluxurile de informații care se află în afara perimetrului de securitate (dispozitive, rețele, servicii cloud etc.).
- Utilizarea inventarelor de active pentru a urmări dispozitivele utilizatorilor și se reamintește proprietarilor să verifice disponibilitatea.
- Asigurarea unui acces limitat la zonele care conțin informații sau echipamente sensibile.
- Implementarea de politici de securitate fizică bine documentate și integrarea măsurilor de securitate fizică cu cele digitale pentru a realiza o abordare holistică.
- Utilizarea de polițe de asigurare pentru a acoperi pierderile atât pentru riscurile fizice, cât și pentru riscurile cibernetice conexe.
- Elaborarea de ghiduri de utilizare pentru dispozitive mobile (smartphone-uri, tablete, laptopuri etc.) și urmarea celor mai bune practici.
- Stabilirea de proceduri bine comunicate pentru protecția fizică a activelor, inclusiv pierderea, deteriorarea și furtul.
- Asigurarea faptului că dispozitivele sunt eliminate după ce informațiile cu caracter personal sau sensibile au fost șterse în siguranță.[6]
- Reducerea timpului de răspuns pentru incidente de furt, deteriorare și pierdere.
- Implementarea autentificării multifactor, combinând datele de identificare ale utilizatorului cu elemente biometrice, carduri inteligente sau alte token-uri fizice.[16]
- Inspectarea periodică a dispozitivelor pentru modificări sau înlocuiri.[6]
- Implementarea unor procese pentru detectarea vizitatorilor autorizați sau a angajaților și atribuirea de drepturi de acces adecvate.[6]
- Implementarea de sisteme de monitorizare a accesului, sisteme de control al accesului, date de identificare de acces puternice și dispozitive de acces inteligente (de exemplu, încuietori inteligente, chei inteligente) pentru zone în care se află echipamente sensibile.[6]

_Cele mai preferabile alternative pentru datele de identificare ale utilizatorului în MFA

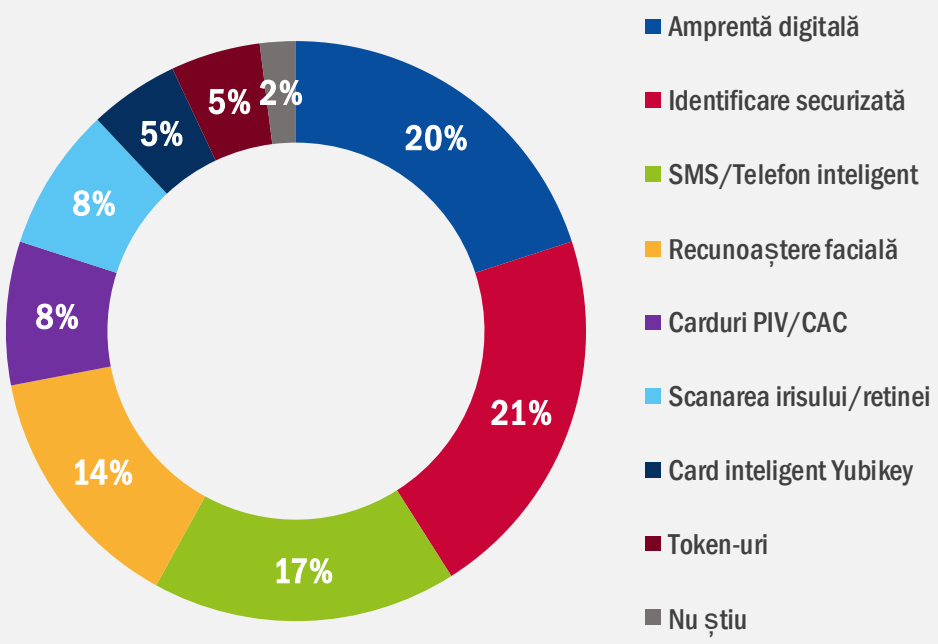


Figura 2 - Sursa: ORACLE & KPMG[16]

Referințe

1. „Physical Security Guide" (Ghid de securitate fizică). Kisi. https://pages.getkisi.com/physical-security-guide

2. Jonathan Wackrow. „Security Convergence: Addressing Evolving Cyber and Physical Security Threats" (Convergența securității: abordarea amenințărilor la adresa securității cibernetice și fizice aflate în evoluție). 2019. Teneo. https://www.teneo.com/vision-book/2019/security-convergence-addressing-evolving-cyber-and-physical-security-threats/

3. Pierluigi Paganini. „Modern Physical Security Awareness Is More Than Dumpster Diving [Updated 2019]" [Conștientizarea securității fizice moderne este mai mult decât căutarea prin coșurile de gunoi (actualizat în 2019)]. 27 august 2019. Infosec Institute. https://resources.infosecinstitute.com/modern-physical-security-awareness-is-more-than-dumpster-diving/#gref

4. Pierre Bourgeix. „2019: What's In & Out in Physical Security" (2019: Ce este inclus și ce este exclus din securitatea fizică). 2019. Boon Edam. https://blog.boonedam.us/2019-whats-in-out-in-physical-security

5. Danny Bradbury. „Killer USB Breach Highlights Need For Physical Security" (Încălcarea securității Killer USB evidențiază necesitatea securității fizice). 23 aprilie 2019. Infosec Magazine. https://www.infosecurity-magazine.com/infosec/usb-breach-physical-security-1-1-1/

6. „PCI DSS Quick Reference" (Referință rapidă PCI DSS). Iulie 2018. Consiliul pentru Standarde de Securitate PCI. https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

7. „76% Security Professionals Face Cybersecurity Skills Shortage: Report" (76 % din profesioniștii din domeniul securității se confruntă cu un deficit de competențe în domeniul securității cibernetice: raport). 7 mai 2020. CISOMAG. https://cisomag.eccouncil.org/security-leaders-lack-cybersecurity-skills/

8. „2019 Landscape Report: Hosted Security Adoption In Europe" (Raport privind situația din 2019:

adoptarea securității găzduite în Europa). 2019. Morphean. https://morphean.com/whitepaper/

9. Catalin Cimpanu. „Crooks use digger to steal ATMs in Northern Ireland as ATM physical attacks rise across the EU" (Escroci folosesc un excavator pentru a fura bancomate din Irlanda de Nord, în contextul în care numărul de atacuri fizice asupra bancomatelor crește în întreaga UE). 16 aprilie 2019. ZDNet. https://www.zdnet.com/article/crooks-use-digger-to-steal-atms-in-northern-ireland-as-atm-physical-attacks-rise-across-the-eu/

10. Jovi Umawing. „Everything you need to know about ATM attacks and fraud: Part 1" (Tot ce trebuie să știți despre atacuri asupra bancomatelor și fraude asociate cu bancomatele: partea 1) 29 mai 2019. Malwarebytes Labs. https://blog.malwarebytes.com/101/2019/05/everything-you-need-to-know-about-atm-attacks-and-fraud-part-1/

11. „ATM Explosive Attacks - Dutch ATMs to be shut down overnight to counter ATM explosive attacks" (Atacuri cu explozibili asupra bancomatelor – bancomatele din Țările de Jos vor fi închise peste noapte pentru a contracara atacurile cu explozibili asupra bancomatelor). 19 decembrie 2019. Asociația Europeană pentru Tranzacții Sigure (EAST). https://www.association-secure-transactions.eu/dutch-atms-to-be-shut-down-ovemight-to-counter-atm-explosive-attacks/

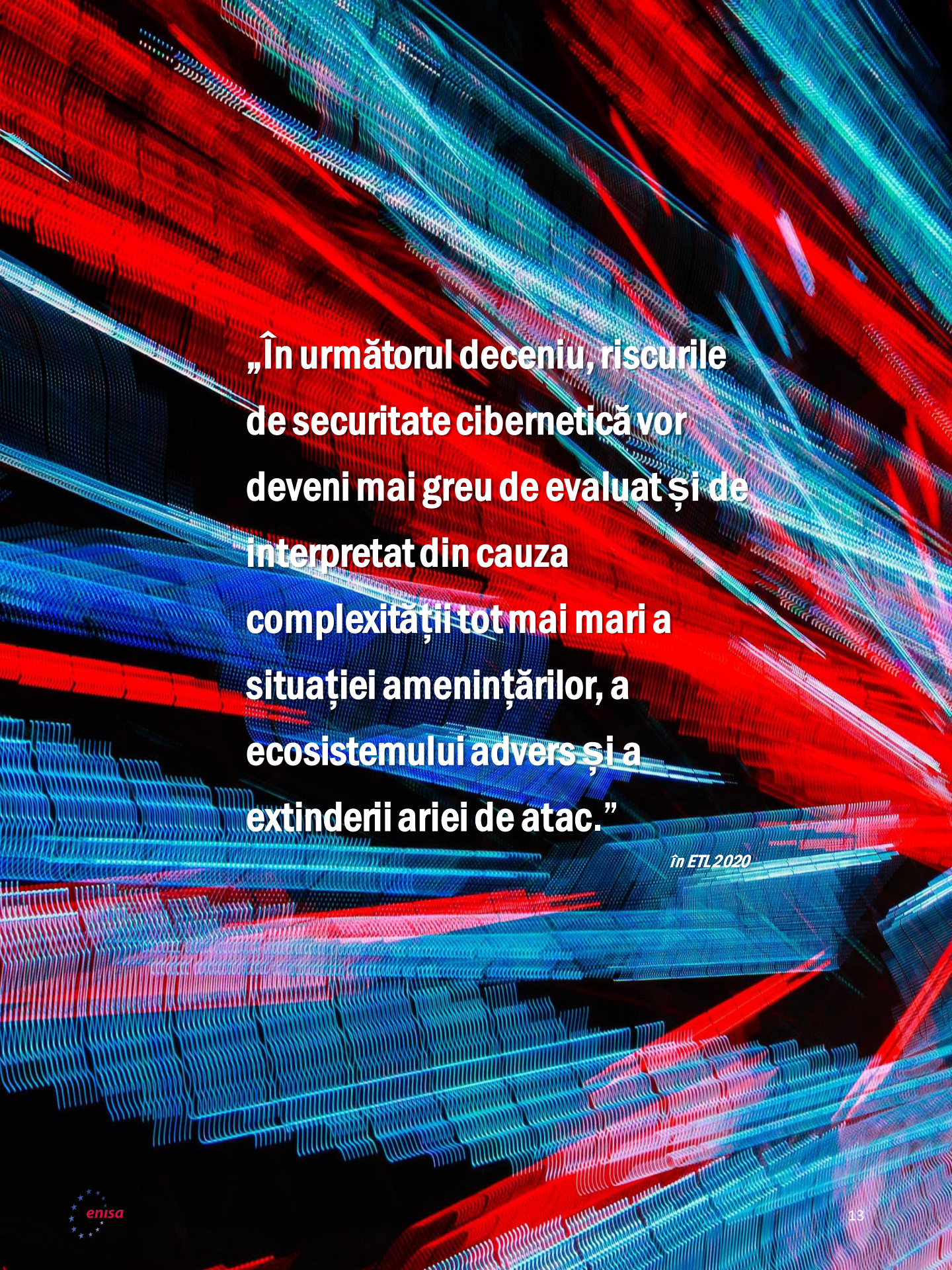
12. „2019 Payment Security Report", 2019 Data Breach Investigations Report (Raport privind securitatea plăților în 2019 – Raportul investigațiilor privind încălcarea securității datelor din 2019). Verizon. https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

13. „2019 Payment Threats and Fraud Trends Report" (Raport privind amenințările la adresa plăților și tendințele în materie de fraudă din 2019). 9 decembrie 2019. Consiliul European al Plăților. https://www.europeanpaymentscouncil.eu/document-library/other/2019-payment-threats-and-fraud-trends-report

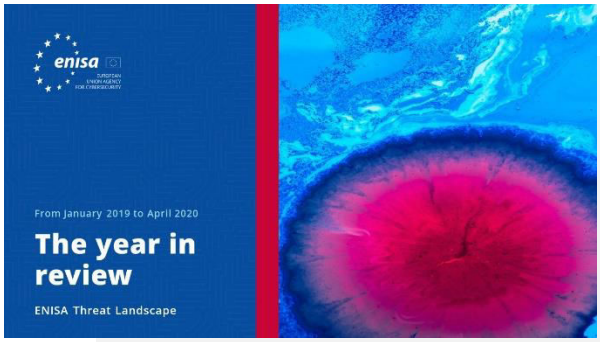
14. „2019 Eye on Privacy Report" (Raport privind analiza confidențialității din 2019). 2019. MediaPRO. https://pages.mediapro.com/Eye-on-Privacy-Report-2019-LP.html

15. „Report: 2020 State of Privacy and Security Awareness" (Raport: Situația confidențialității și a conștientizării securității în 2020). 2020. MediaPRO. https://www.mediapro.com/report-2020-state-of-privacy-security-awareness/

16. „Oracle and KPMG Cloud Threat Report" (Raportul Oracle și KPMG privind amenințările la adresa cloud-ului). 2019. ORACLE & KPMG. https://www.oracle.com/fr/a/ocom/docs/dc/final-oracle-and-kpmg-cloud-threat-report-2019.pdf


„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 ariei de atac.”
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

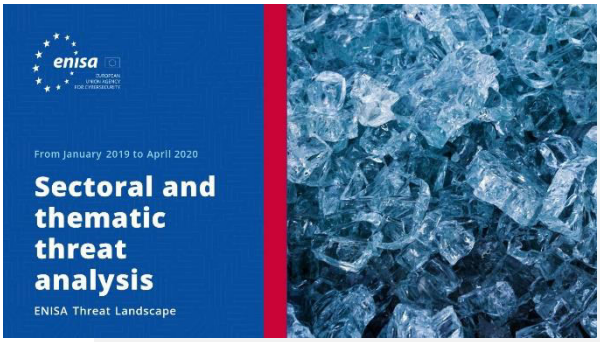
Lista ENISA a celor mai importante 15 amenințări din perioada ianuarie 2019 – aprilie 2020.

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

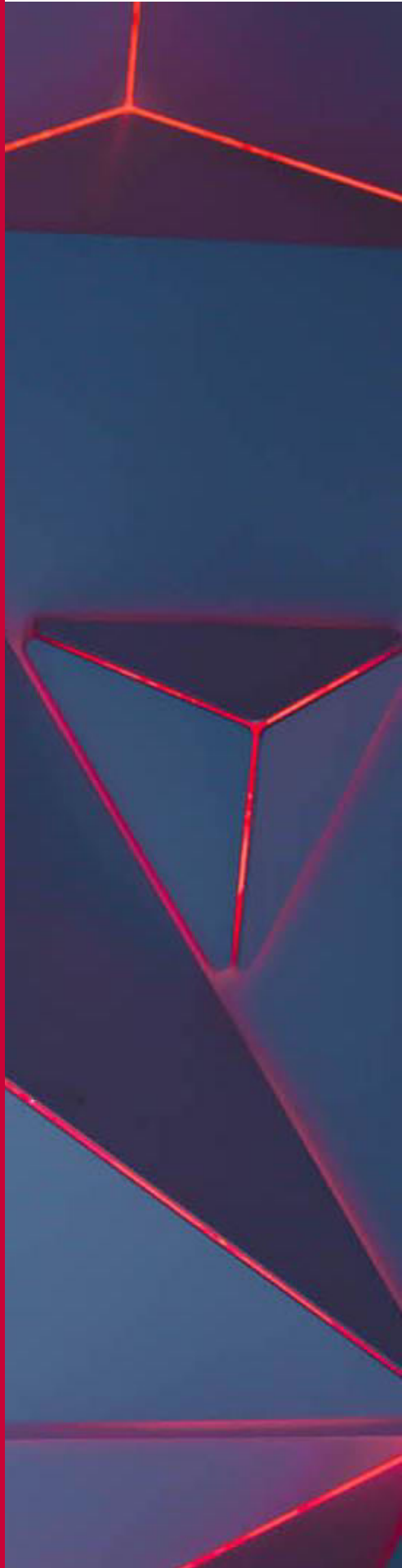
Pentru întrebări despre această lucrare, vă rugăm să utilizați adresa enisa.threat.information@enisa.europa.eu.

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.

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