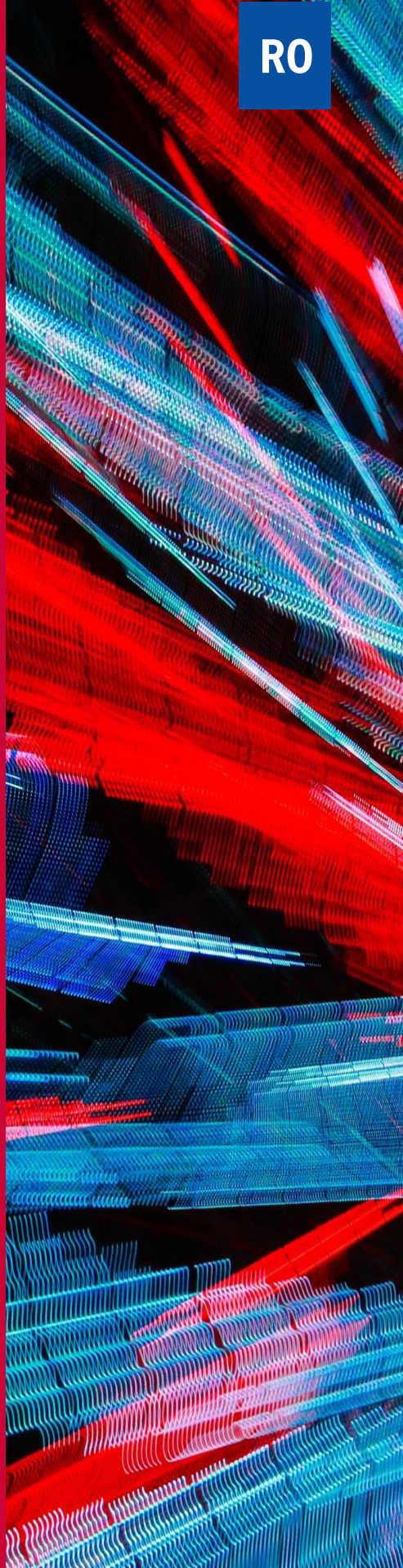
enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

RO



Ianuarie 2019 – aprilie 2020

Tendințe emergente

Raportul ENISA privind situația amenințărilor

Prezentare generală

La ce să vă așteptați

Odată cu începutul unui nou deceniu, ne putem aștepta la schimbări semnificative în ceea ce privește modul în care percepem și înțelegem securitatea cibernetică sau securitatea spațiului cibernetic. Spațiul cibernetic astfel cum este definit în **ISO/IEC 27032:2012**[1] este un ***„mediu complex rezultat din interacțiunea dintre oameni, programe software și/sau servicii pe internet prin intermediul dispozitivelor tehnologice și a rețelelor conectate la internet, care nu există sub nicio formă fizică”***. Protecția acestui mediu complex va deveni și mai dificilă pe măsură ce conectăm mai mulți oameni, dispozitive, sisteme și rulăm mai multe procese și servicii în rețea. De asemenea, suntem mai dependenți de fiabilitatea, integritatea, disponibilitatea și încrederea în acesta pentru a lucra, a relaționa și a face multe dintre activitățile noastre de zi cu zi. Odată cu creșterea acestei dependențe, vor apărea mai multe oportunități pentru factorii rău intenționați de a utiliza spațiul cibernetic pentru a manipula, intimida, înșela, hărțui și înșela persoane și organizații. Protecția persoanelor, a întreprinderilor și a organizațiilor în timpul utilizării spațiului cibernetic va tinde să se schimbe în următorul deceniu, de la securitatea tradițională a rețelelor și informațiilor (NIS) la un concept mai amplu care include conținut și servicii.

În ultimul deceniu, „a patra revoluție industrială” a accelerat semnificativ ritmul schimbării, transformând ceea ce fac oamenii, cum o fac, ce abilități sunt necesare, unde se desfășoară munca, cum sunt structurate relațiile de muncă și cum este organizată, distribuită și recompensată munca.

Din cauza pandemiei actuale de COVID-19, începem deceniul cu o nouă normă și cu schimbări profunde în lumea fizică și în spațiul cibernetic. Odată cu distanțarea socială sau izolarea, oamenii vor tinde să folosească spațiul virtual pentru a comunica, a relaționa și a socializa. Această nouă normă va introduce noi provocări în lanțul valoric digital și, în special, în industria securității cibernetice.

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.

Există prea multe variabile care trebuie luate în considerare în eforturile de eficientizare a gestionării riscului cibernetic. Un factor important este diversitatea tehnologică cu care se confruntă în prezent majoritatea organizațiilor. Un alt aspect este complexitatea instrumentelor, tacticilor, tehnicilor și procedurilor (TTP) utilizate de adversari pentru a desfășura atacuri. Actorii rău intenționați adaptează și ajustează TTP-urile la mediul victimei în funcție de necesități și colaborează cu alții pentru a-și atinge obiectivele.

Definirea unei poziții de risc, gestionarea datelor, aplicarea valorilor relevante și răspunsul la schimbare sunt obstacole în calea creării unei strategii eficace de guvernanță a riscurilor cibernetice. **În următorul deceniu vor fi necesare noi abordări pentru a ne feri de analiza de tip siloz și pentru a ne apropia de un model de tip matrice de factori, variabile și condiții interconectate**. Aceasta constituie o provocare semnificativă pentru multe organizații care încearcă să-și protejeze infrastructura, operațiunile și datele împotriva unor adversari mai puternici, cu resurse mai bune și mai bine echipați.

Tendințe emergente

Zece provocări de securitate cibernetică

01_Gestionarea riscurilor sistemice și complexe.

Riscul cibernetic se caracterizează prin viteza și amploarea propagării sale, precum și prin intenția potențială a factorilor de amenințare. Interconectarea diferitelor sisteme și rețele permite incidentelor cibernetice să se răspândească rapid și pe scară largă, ceea ce face ca riscurile cibernetice să fie mai greu de evaluat și de combătut.

02_Detectarea de inteligență artificială adversară pe scară largă.

Detectarea amenințărilor care exploatează inteligența artificială pentru a lansa un atac sau pentru a evita detectarea va constitui o provocare majoră pentru viitorul sistemelor de apărare cibernetică.[14]

03_Reducerea erorilor neintenționate.

Odată cu creșterea numărului de sisteme și dispozitive conectate la rețea, erorile neintenționate continuă să fie una dintre cele mai exploatate vulnerabilități în incidentele de securitate cibernetică. Soluțiile noi care vizează reducerea acestor erori vor oferi o contribuție importantă la reducerea numărului de incidente.

04_Lanțul de aprovizionare și amenințările față de terți.

Lanțul de aprovizionare diversificat care caracterizează astăzi industria tehnologică oferă noi oportunități pentru ca factorii de amenințare să profite de aceste sisteme complexe și să exploateze vulnerabilitățile multiple introduse de un ecosistem eterogen de furnizori terți.[16]

05_Instrumentarea și automatizarea securității.

Informațiile privind amenințările cibernetice și analiza comportamentală vor dobândi importanță odată cu automatizarea proceselor și a analizelor. Investițiile în automatizare și instrumentare vor permite profesioniștilor în securitate cibernetică să investească în elaborarea unor strategii
robuste de securitate cibernetică.

06_Reducerea rezultatelor fals pozitive. Această promisiune mult așteptată este esențială pentru viitorul industriei de securitate cibernetică și în lupta împotriva oboselii cauzate de starea de alarmă.

07_Strategii de securitate zero-încredere. Cu o presiune tot mai mare asupra sistemelor IT pusă de noile cerințe comerciale, cum ar fi munca la distanță, digitalizarea modelului de afaceri și extinderea datelor, mulți factori de decizie consideră că încrederea zero este soluția de facto pentru securizarea activelor corporative.

08_Erori în migrația în cloud a întreprinderilor. În contextul în care multe întreprinderi își migrează datele către soluții bazate pe cloud, numărul de erori de configurare va crește, expunând datele la o posibilă încălcare a securității. Furnizorii de servicii cloud vor aborda problema utilizând sisteme care identifică automat acest tip de erori.

09_Amenințări hibride. Noul mod de operare adoptă amenințări la adresa lumii virtuale și fizice. Răspândirea dezinformării sau a știrilor false, de exemplu, este un element cheie în peisajul amenințărilor hibrid. EUvsDisinfo[15] este un proiect emblematic al Grupului de lucru East StratCom al Serviciului European de Acțiune Externă, creat pentru a aborda amenințarea reprezentată de dezinformare.

10_Atractivitatea infrastructurii cloud ca țintă va crește. Dependența din ce în ce mai mare de infrastructura publică de cloud va crește riscul întreruperilor de producție. Configurarea greșită a resurselor cloud este în continuare cauza principală a atacurilor cloud, dar atacurile care vizează direct furnizorii de servicii cloud câștigă popularitate în rândul hackerilor.

Tendințe emergente

_ Cheltuieli în materie de securitate cibernetică

Potrivit lui Gartner[17], multe consilii de administrație vor cere îmbunătățirea datelor și înțelegerea rezultatelor după ani de investiții intensive în securitate cibernetică. Aceasta se datorează în principal unei creșteri a cheltuielilor în materie de securitate cibernetică proporțional cu investițiile făcute în noi tehnologii. Potrivit unui raport al IDC[22], cheltuielile pentru securitatea cibernetică au atins 103 miliarde USD (aproximativ 87,5 miliarde EUR) în 2019, sumă care este cu 9,4 % mai mare decât în anul precedent. Managerii de securitate vor fi evaluați în curând pentru rezultatele obținute după ani de investiții și sunt esențiali pentru a menține date îmbunătățite despre rezultatele obținute.

_ Informațiile privind amenințările cibernetice vor contribui la definirea strategiilor de securitate cibernetică

Informațiile privind amenințările cibernetice (CTI)[23] urmăresc să ajute organizațiile să se pregătească mai bine, îmbunătățindu-și cunoștințele despre situația amenințărilor. În loc să se bazeze exclusiv pe informațiile generate de sistemele sau fluxurile interne (ceea ce se știe despre ceea ce este cunoscut), eficacitatea CTI va fi determinată de cunoașterea *motivului*, a *modului* și a *ceea ce* este necunoscut echipei de securitate cibernetică. Propunerea de valoare a oricărei capacități sau a oricărui program CTI este de a îmbunătăți pregătirea organizației pentru a-și proteja activele critice de amenințări necunoscute.

Cunoașterea situației amenințărilor

Cu o mai mare automatizare și instrumentare a securității cibernetice văzută ca o tendință în creștere, **echipele de securitate cibernetică vor petrece mai puțin timp desfășurând activități de monitorizare și mai mult timp dedicat sarcinilor privind gradul de pregătire**. O capacitate CTI bine concepută poate oferi cunoștințe contextualizate și care să poată conduce la măsuri concrete despre amenințări pentru a informa părțile interesate strategice, operaționale și tactice din întreaga organizație. În termeni practici, o capacitate CTI ar trebui să vizeze răspunsul la următoarele întrebări, având în vedere cerințele părților interesate, contextul și mediul organizației:

- Care este suprafața de atac?
- Care sunt cele mai valoroase active și terenul cibernetic?
- Care sunt cele mai critice vulnerabilități?
- Care sunt cei mai utilizați vectori de atac?
- Cum se comportă și operează adversarii de obicei?
- Cum arată situația amenințărilor în ceea ce privește:
    - sectorul și tipul de activitate pe care o desfășoară organizația?
    - mediul tehnologic adoptat de organizație?
- Cine trebuie să ia măsuri și ce trebuie făcut pentru a diminua riscurile generate de aceste amenințări?

Lipsa abilităților de securitate cibernetică

Lipsa profesioniștilor în tehnologie cu înaltă calificare este deja o problemă pentru ambiția de digitalizare a Europei. Conform unui studiu[23], peste 70 % din întreprinderile europene declară că lipsa competențelor reprezintă o barieră în calea strategiilor de investiții, în timp ce 46 % din întreprinderi raportează dificultăți în ocuparea posturilor vacante din cauza lipsei de competențe în domenii cheie, precum securitatea cibernetică.

Tendințe emergente

Cinci tendințe în materie de amenințări cibernetice

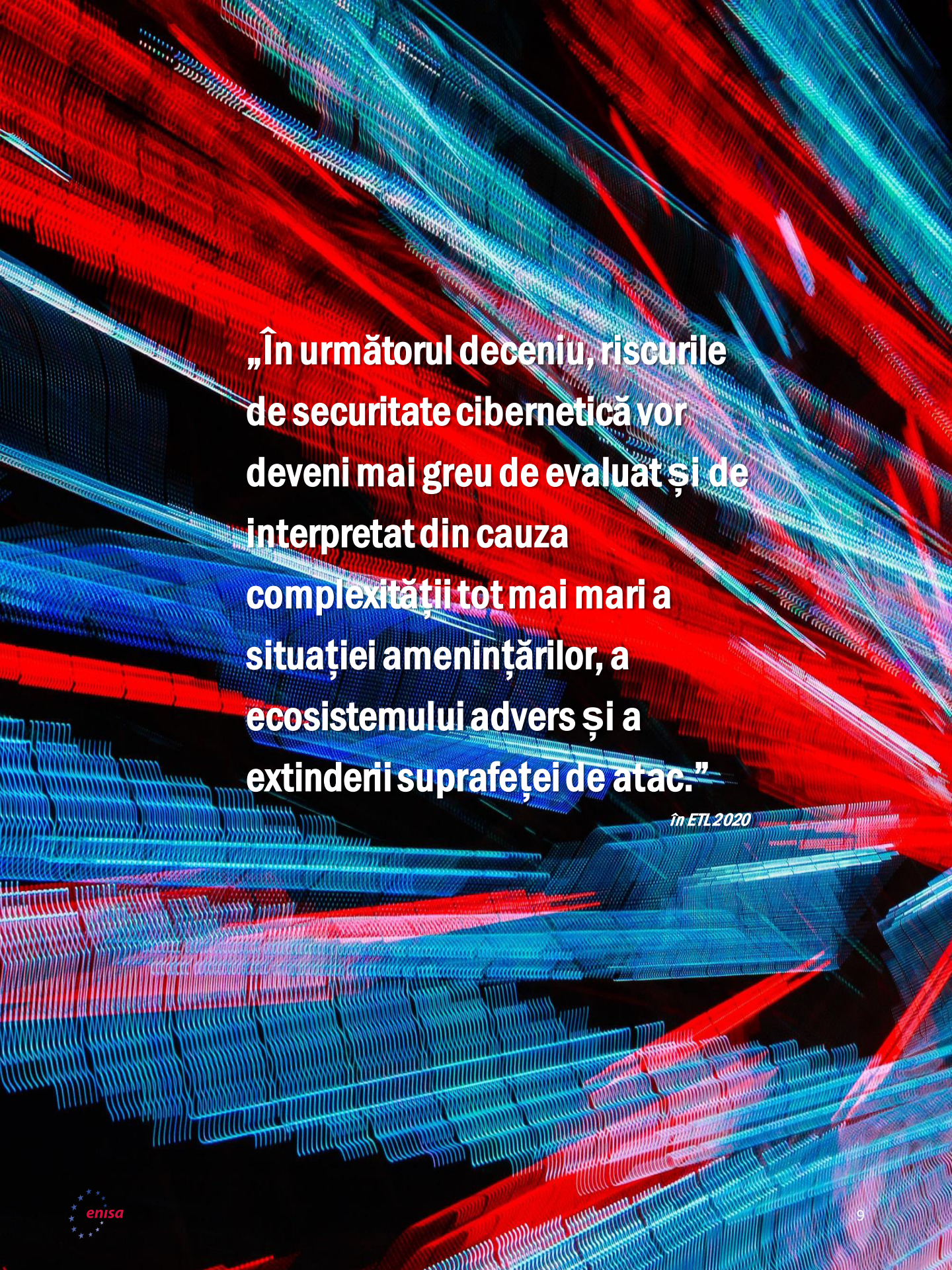
01_Programul malware este actualizat. Varietățile din familia de malware sunt actualizate la versiuni noi cu caracteristici, mecanisme de distribuție și propagare suplimentare. Emotet, de exemplu, un malware conceput inițial ca troian bancar în 2014, a devenit unul dintre cei mai eficace distribuitori de malware din 2019.[2]

02_Amenințările vor deveni complet mobile. Utilizatorii sunt din ce în ce mai dependenți de dispozitivele mobile pentru a-și securiza cele mai sensibile conturi. Utilizarea 2fa legată de un autentificator de aplicație sau printr-un SMS este unul dintre exemple. Având în vedere că tot mai multe programe malware devin complet mobile, aplicațiile frauduloase, SIMJacking și exploatarea sistemelor de operare fac din aceste dispozitive veriga cea mai slabă, prin urmare, sunt extrem de vulnerabile la atacuri.

03_Atacatorii folosesc noi tipuri de fișiere, cum ar fi fișiere de imagine de disc (ISO și IMG) pentru răspândirea programelor malware. Fișierele DOC, PDF, ZIP și XLS sunt în continuare tipul de atașament cel mai frecvent utilizat pentru răspândirea programelor malware, dar alte tipuri devin populare. Au fost identificate câteva campanii de distribuire a AgentTesla InfoStealer și NanoCore RAT folosind tipul de fișier de imagine în 2019.

04_Creșterea atacurilor ransomware țintite și coordonate. În 2019 s-a observat o escaladare a exploit-urilor sofisticate și țintite de ransomware în sectorul public, organizațiile de asistență medicală și industriile specifice din capul listei. Atacatorii petrec mai mult timp strângând informații despre victime, știind exact ce să cripteze, obținând astfel perturbări maxime și răscumpărări mai mari.

05_Atacurile de umplutură de date de încredere (credential stuffing) vor cunoaște o largă răspândire. Umplutura de date de identificare (credential stuffing) – injecția automată a combinațiilor de nume de utilizator și parole furate prin cereri de conectare automată pe scară largă îndreptate împotriva unei aplicații web – va prolifera ca urmare a unui deceniu cu un număr anormal de încălcări ale securității datelor și trilioane de înregistrări de date personale furate.


„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

Tendințe emergente

Zece tendințe emergente în materie de vectori de atac

01_ Atacurile vor fi distribuite masiv, cu o durată scurtă și un impact mai larg

Aceste atacuri sunt menite să afecteze cel mai mare număr de dispozitive posibil pentru a fura informații cu caracter personal sau pentru a bloca accesul la date prin criptarea fișierelor.

02_ Atacuri țintite exact și persistente vor fi planificate cu meticulozitate, cu obiective bine definite și pe termen lung

Actorii rău intenționați planifică acest tip de atacuri pentru a ajunge la date de mare valoare, cum ar fi informații financiare, proprietate intelectuală și industrială, secrete comerciale, informații clasificate etc.

03_ Actori rău intenționați vor folosi platforme digitale în atacuri țintite

Actorii rău intenționați vor explora potențialul platformelor digitale de a sprijini atacurile țintite (de exemplu, rețelele sociale, jocurile, mesageria, streaming etc.). De la furtul de date cu caracter personal pentru atacuri de tip spear-phishing până la distribuția extinsă a malware-ului, platformele digitale cu un număr mare de abonați sunt vectori de atac eficienți, din ce în ce mai populari în rândul actorilor rău intenționați.

04_ Exploatarea proceselor operaționale va crește

Cu mai multă automatizare și mai puțină intervenție umană, procesele operaționale pot fi modificate cu rea intenție pentru a genera profit pentru un atacator. Cunoscută în mod obișnuit sub denumirea de compromiterea procesului de afaceri (BPC), această tehnică este adesea subevaluată de specialiștii în ingineria proceselor din cauza lipsei unei evaluări adecvate a riscurilor.

05_ Suprafața de atac va continua să se extindă

E-mailul nu mai este instrumentul principal și cel mai important vector de atac pentru phishing. Actorii rău intenționați folosesc acum alte platforme pentru a comunica și a atrage victimele să deschidă pagini web compromise. Apare o nouă tendință, cu utilizarea mesajelor SMS, WhatsApp, SnapChat și social media.

06_Munca la distanță (teleworking) se va desfășura prin intermediul dispozitivelor de acasă

În contextul în care mai multe persoane lucrează de la distanță și își conectează dispozitivele la rețelele corporative, riscul de a deschide noi puncte de intrare pentru atacatori va crește. Odată cu pandemia de COVID-19, această tendință îi va îndemna pe managerii IT să înăsprească politicile de securitate și să facă modificări urgente în infrastructura IT.

07_Atacatorii vor veni mai bine pregătiți

Atacatorii își aleg cu atenție țintele, desfășoară acțiuni de recunoaștere împotriva anumitor angajați și îi vizează cu atacuri de tip phishing pentru a obține date de identificare utilizabile pentru a viza organizația. Odată ce atacatorii au acces la un singur dispozitiv, pot folosi instrumente de testare a penetrării, cum ar fi Mimikatz, pentru a colecta și a exploata date de identificare cu privilegii ridicate.

08_Tehnicile de deghizare vor deveni mai sofisticate

Factorii de amenințare inovează continuu pentru a face amenințările mai eficace și mai puțin susceptibile de a fi detectate. Anubis, un troian și un bot bancar pentru Android, a fost distribuit deghizat ca o aplicație inofensivă, în principal prin Google Play Store.[1]

09_Va crește exploatarea automată a sistemelor neperfectate și a aplicațiilor întrerupte

Creșterea anormală a traficului Telnet către portul 445 observată în 2019 a dezvăluit extinderea viermilor și exploit-urilor precum Eternal Blue. Telnet, care nu mai este utilizat decât în domeniul dispozitivelor IoT, a înregistrat în această perioadă cele mai mari volume.

10_Amenințările cibernetice se îndreaptă către periferia rețelei

Dispozitivele Edge sunt utilizate la limitele dintre rețelele interconectate.
S-a observat o tendință în creștere a atacurilor care vizează aceste dispozitive – cum ar fi routere, switch-uri și firewall – având un impact semnificativ asupra unei întreprinderi și asupra ecosistemului digital conectat.

Referințe

1. "ISO/IEC 27032:2012". ISO. https://www.iso.org/standard/44375.html

2. „Triple Threat: Emotet Deploys TrickBot to Steal Data & Spread Ryuk" (Amenințare triplă: Emotet lansează TrickBot pentru a fura date și a răspândi Ryuk). 2 aprilie 2019. Cybereason. https://www.cybereason.com/blog/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware

3. „Understanding the relationship between Emotet, Ryuk and TrickBot" (Înțelegerea relației dintre Emotet, Ryuk și TrickBot). 14 aprilie 2019. Intel471. https://blog.intel471.com/2020/04/14/understanding-the-relationship-between-emotet-ryuk-and-trickbot/

4. „Investigating WMI Attacks" (Investigarea atacurilor WMI), 9 februarie 2019. SANS. https://www.sans.org/blog/investigating-wmi-attacks/

5. „RDP Abuse and Swiss Army Knife Tool Used to Pillage, Encrypt and Manipulate Data" (Instrumentul pentru abuzul PDR și multi-instrumentul folosit pentru a jefui, cripta și manipula date), 18 decembrie 2019. Bitdefender. https://labs.bitdefender.com/2019/12/rdp-abuse-and-swiss-army-knife-tool-used-to-pillage-encrypt-and-manipulate-data/

6. „Europe's huge privacy fines against Marriott and British Airways are a warning for Google and Facebook" (Amenzile uriașe pentru încălcarea confidențialității aplicate de autoritățile europene împotriva Marriott și British Airways constituie un avertisment pentru Google și Facebook), 10 iulie 2019. CNBC. https://www.cnbc.com/2019/07/10/gdpr-fines-vs-marriott-british-air-are-a-warning-for-google-facebook.html

7. „This is how we might finally replace passwords" (Așa am putea înlocui în cele din urmă parolele), 27 mai 2019. C|Net. https://www.cnet.com/news/this-is-how-we-might-finally-replace-passwords/

9. „Authentication standards to help reduce the world's over-reliance on passwords" (Standarde de autentificare pentru a ajuta la reducerea încrederii excesive acordate de întreaga lume parolelor) FIDO. https://fidoalliance.org/overview/

10. „How Much Cyber Sovereignty is Too Much Cyber Sovereignty?" (Cât din suveranitatea cibernetică este prea mult?) 3 octombrie 2019. Council on Foreign Relations. https://www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty

11. „Conceptualising Cyber Arms Races" (Conceptualizarea curselor de înarmare cibernetică). 2016. NATO. https://ccdcoe.org/uploads/2018/10/Art-10-Conceptualising-Cyber-Arms-Races.pdf

12. „Journalism, 'Fake News' and Disinformation: A Handbook for Journalism Education and Training" (Jurnalism, „știri false" și dezinformare: manual pentru educație și formare în jurnalism), 2018. UNESCO. https://en.unesco.org/fightfakenews

13. „The Big Connect: How Data Science is Helping Cybersecurity" (Marea conectare: modul în care știința datelor contribuie la securitatea cibernetică). 12 iunie 2019. Info Security Group. https://www.infosecurity-magazine.com/blogs/data-science-helping-cybersecurity-1/

14. „Are You Ready For The Age Of Adversarial AI? Attackers Can Leverage Artificial Intelligence Too" (Sunteți pregătit pentru epoca IA adversară? Atacatorii pot profita și de inteligența artificială). 9 ianuarie 2020. Forbes. https://www.forbes.com/sites/forbestechcouncil/2020/01/09/are-you-ready-for-the-age-of-adversarial-ai-attackers-can-leverage-artificial-intelligence-too/#2a76dee14703

15. https://euvsdisinfo.eu/

16. „FBI Alerts Companies of Cyber Attacks Aimed at Supply Chains" (FBI atenționează întreprinderile cu privire la atacuri cibernetice care vizează lanțurile de aprovizionare). 21 februarie 2020. Bitsight. https://www.bitsight.com/blog/fbi-alerts-companies-of-cyber-attacks-supply-chains

17. „Gartner Identifies the Top Seven Security and Risk Management Trends for 2019" (Gartner identifică primele șapte tendințe de securitate și de gestionare a riscurilor pentru 2019). 5 martie 2019. Gartner. https://www.gartner.com/en/newsroom/press-releases/2019-03-05-gartner-identifies-the-top-seven-security-and-risk-ma

18. „Android banking trojan" (Troianul bancar Android). 3 octombrie 2019. Cyare. https://cyware.com/news/exploring-the-nature-and-capabilities-of-anubis-android-banking-trojan-6ea7dec4

19. „5 Top Trends for Mobile Cyber Security in 2020" (5 tendințe importante pentru securitatea cibernetică mobilă în 2020). 9 ianuarie 2020. Corrata. https://corrata.com/5-top-trends-for-mobile-cyber-security-in-2020/

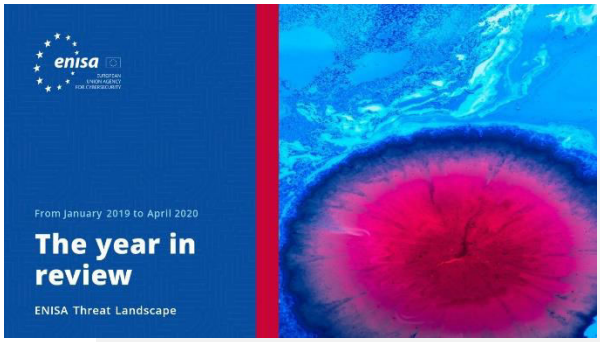
20. „Malicious Attachments Remain a Cybercriminal Threat Vector Favorite" (Atașamentele rău intenționate rămân un vector favorit de amenințare al infractorilor informatici). 27 august 2020. Threat Post. https://threatpost.com/malicious-attachments-remain-a-cybercriminal-threat-vector-favorite/158631/

21. „10 trends shaping the future of work" (10 tendințe care modelează viitorul muncii). Octombrie 2019. EPSC. https://op.europa.eu/en/publication-detail/-/publication/e77a1580-0cf5-11ea-8c1f-01aa75ed71a1/language-en/format-PDF/source-121729338

22. „Global security spending to top $103 billion in 2019, says IDC" (Cheltuielile globale de securitate vor depăși 103 miliarde USD în 2019, declară IDC), 20 martie 2019. ZDNet. https://www.zdnet.com/article/global-security-spending-to-top-103-billion-in-2019-says-idc/

23. „Insights into skills shortages and skills mismatch. learning from Cedefop's European skills and jobs survey" (Perspectivă asupra lipsei de personal calificat și neconcordanțelor de competențe. Învățăminte desprinse din sondajul Cedefop privind competențele și locurile de muncă europene). 2018. CEDEFOP. https://www.cedefop.europa.eu/files/3075_en.pdf

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

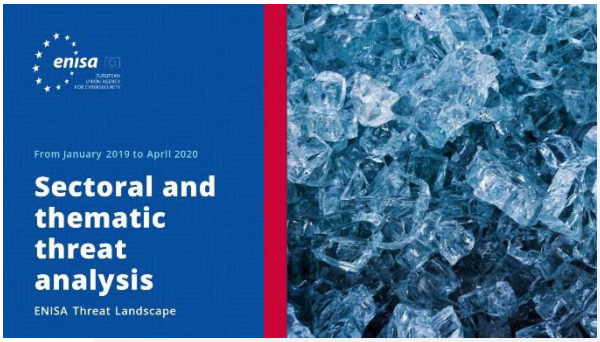
Lista ENISA a celor mai importante 15 amenințări din perioada ianuarie 2019 – aprilie 2020.

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**

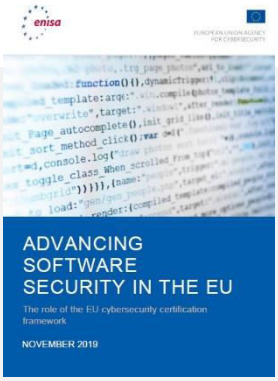
Principalele tendințe în securitatea cibernetică observate în perioada ianuarie 2019 - aprilie 2020.

CITIȚI RAPORTUL

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

Situația actuală a informațiilor privind amenințările cibernetice în UE.

Alte publicații



Promovarea securității software-ului în UE

Prezintă elemente cheie ale securității software-ului și oferă o imagine de ansamblu concisă asupra celor mai relevante abordări și standarde existente în peisajul de dezvoltare de software securizat.

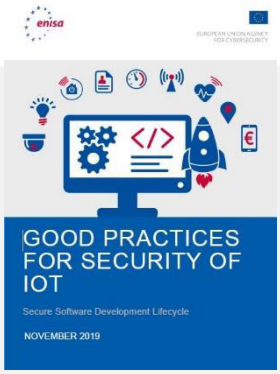
CITIȚI RAPORTUL

Bunele practici ENISA pentru securitatea mașinilor inteligente

Bune practici pentru securitatea mașinilor inteligente, și anume vehiculele conectate și (semi)autonome, pentru a intensifica experiența utilizatorilor de mașini și pentru a îmbunătăți siguranța mașinii

.

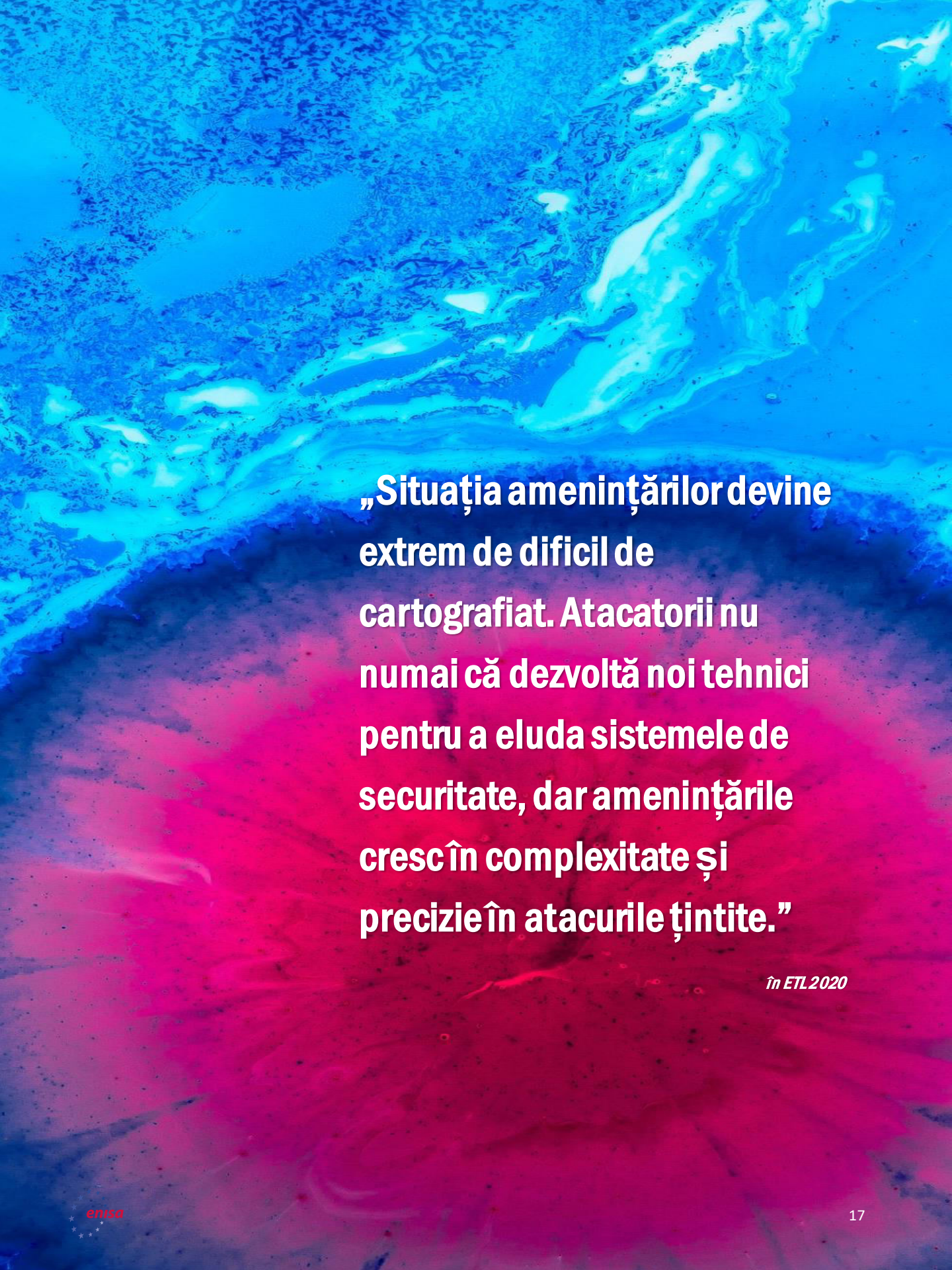
CITIȚI RAPORTUL



Bune practici pentru securitatea IoT – Ciclul de viață al dezvoltării de software securizat

Securitate ioT, cu accent special pe orientări pentru dezvoltarea de software.

CITIȚI RAPORTUL


„Situația amenințărilor devine extrem de dificil de cartografiat. Atacatorii nu numai că dezvoltă noi tehnici pentru a eluda sistemele de securitate, dar amenințările cresc în complexitate și precizie în atacurile țintite.”
în ETL 2020

Despr
e

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

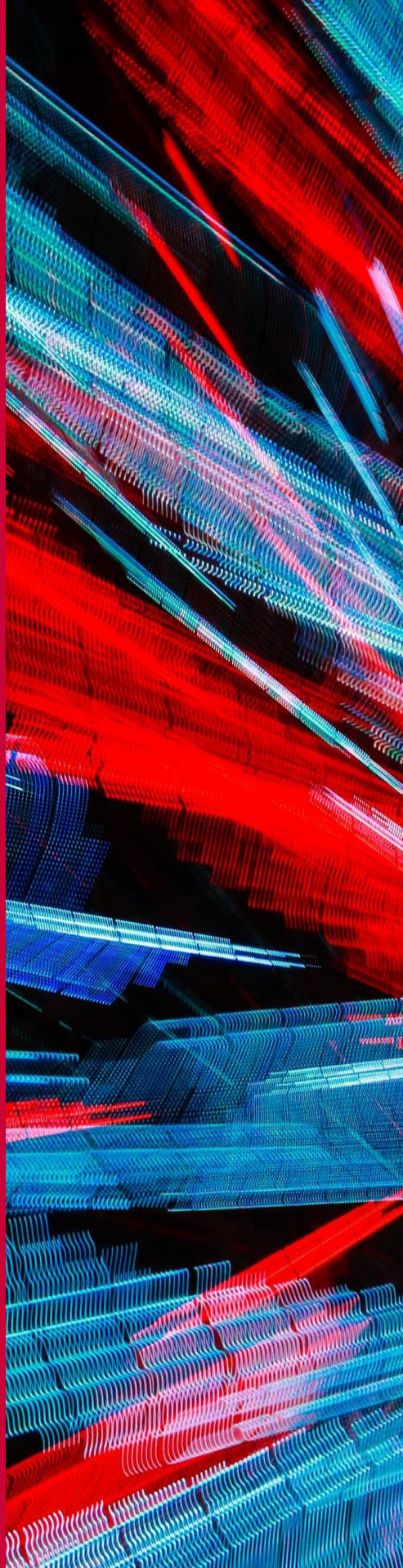
Trebuie luat în considerare faptul că această publicație reprezintă punctele de vedere și interpretările ENISA, cu excepția cazului în care se prevede altfel. Această publicație nu trebuie interpretată ca o acțiune juridică a ENISA sau a organismelor ENISA, cu excepția cazului în care aceasta a fost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