enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

RO

ianuarie 2019 – aprilie 2020

Analiza sectorială/ tematică a amenințărilor

Raportul ENISA privind situația amenințărilor

Prezentare generală

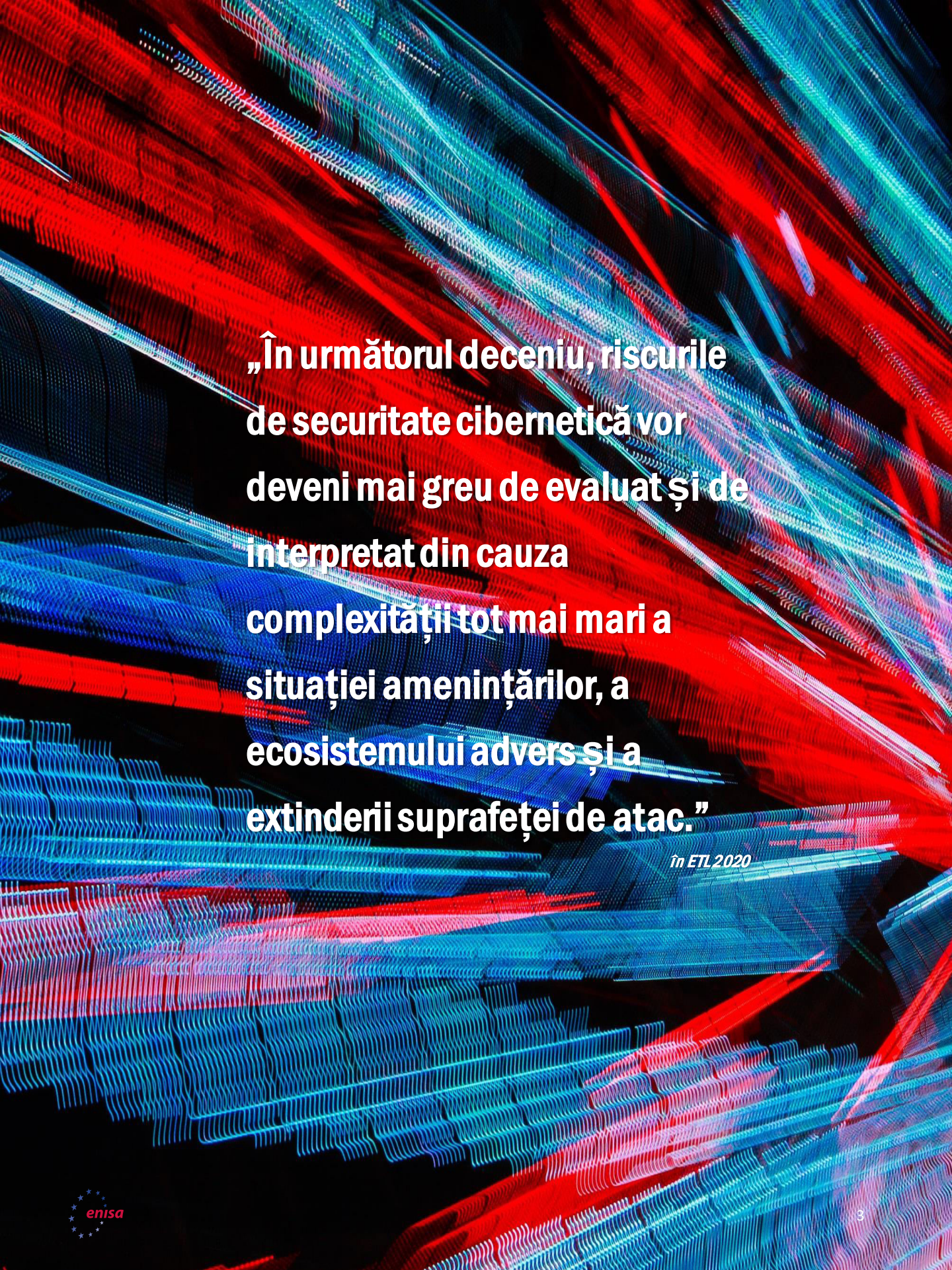
Pe lângă indicarea motivațiilor adversarilor, aceasta oferă dovezi despre cele mai comune tehnici de atac și expunerea la amenințări care se aplică unui anumit sector, semnalând astfel cerințele și prioritățile de protecție. În ceea ce privește temele, analiza amenințărilor și provocărilor asociate cu tehnologii emergente specifice contribuie la procesul de estimare, evaluare și atenuare a riscurilor viitoare.

Informațiile privind amenințările cibernetice (CTI) contextualizate pentru sectoare reprezintă un instrument important de pregătire pentru a formula concluzii cu privire la atacurile cibernetice preconizate într-un sector specific.

Statistici privind incidentele sectoriale vs. expunerea evaluată a sectoarelor emergente

Contextualizarea CTI sectoriale se bazează în principal pe incidente de securitate cibernetică întâlnite într-un sector. Deși aceasta reprezintă o metodă standard pentru componentele IT și serviciile digitale existente și stabilite, ea nu acoperă tehnologiile emergente. Acest fapt se datorează în principal lipsei de informații despre incidente pentru tehnologiile care sunt doar într-o fază pilot sau experimentală. CTI pentru tehnologiile emergente sunt contextualizate prin evaluări ale amenințărilor asupra categoriilor de active relevante pentru un anumit sector. ENISA efectuează astfel de evaluări pentru sectoare emergente precum 5G, IoT[5] și mașini inteligente[6]. ENISA utilizează situațiile amenințărilor sectoriale și tematice și evaluările protecției de bază ca metode pentru contextualizarea CTI.

În acest raport, pe lângă CTI sectoriale care se întemeiază pe statistici bazate pe incidente, prezentăm un rezumat al CTI evaluate pentru sectoarele tehnologice emergente pe baza activității ENISA.


„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

Prezentare generală

Nevoia urgentă de statistici sectoriale exacte și actualizate privind incidentele

Statisticile sectoriale privind incidentele reprezintă un instrument esențial pentru a înțelege dinamica evoluției amenințărilor, motivele adversarilor, expunerea activelor și acțiunile asupra obiectivelor. Datorită complexității atacurilor, dependențelor dintre activele vizate și naturii intersectoriale a vulnerabilităților abuzate exploatate, statisticile incidentelor prezintă unele incertitudini inerente care provin din următoarele date.

- În diferite statistici sectoriale, observăm o serie de **incidente clasificate ca „necunoscute”**[1,2]. Acest procent variază de la 1,5 % la 5 %. Dacă aceste incidente ar putea fi asociate cu unele dintre sectoarele cunoscute, procentul respectiv ar putea influența ordinea țintelor. Mai mult, cantitatea semnificativă de tehnici de atac necunoscute (aproximativ 15 %) adaugă o oarecare incertitudine evaluării motivelor agenților de amenințare.
- Majoritatea **atacurilor necesită mai mult de o etapă** (în medie trei) pentru a-și atinge obiectivele țintei finale. În multe cazuri, ținte multiple din diverse sectoare sunt implicate într-un singur atac. Prin urmare, un incident înregistrat într-un sector poate rezulta din mai multe incidente din alte sectoare care constituie etape intermediare în cadrul atacului. Astfel de dependențe între incidente pot afecta acuratețea statisticilor incidentelor.
- În afară de numărul de incidente pe sector, un element important pentru analiza statistică este **natura tehnicilor de atac utilizate**. Aceste informații pot oferi dovezi utile despre vectorul de atac cel mai frecvent utilizat și pot contribui la prioritizarea măsurilor de protecție necesare pentru un anumit sector.

- Materializarea amenințărilor depinde în mare măsură de **oportunitățile existente care sunt explorate de adversari**. De exemplu, din cauza pandemiei de COVID-19, mediile IT au devenit descentralizate. Acest lucru slăbește controalele de securitate corporative aplicate în rețeaua unei companii, ceea ce explică reorientarea atacurilor de la ținte corporative la ținte individuale[1]. Acest exemplu indică necesitatea de a „traduce" modificările observate în statistici, ținând cont de oportunitățile emergente.
- Statisticile actuale sunt elaborate având în vedere diverse criterii. **Variațiile criteriilor** statisticilor împiedică comparațiile între statisticile incidentelor. De exemplu:
    - În funcție de părțile interesate/contribuitorii colectorului de informații, baza de date cu informații despre statistici ar putea să nu acopere toate sectoarele în mod egal;
    - Clasificarea incidentelor se poate baza pe frecvența apariției acestora, indiferent de amploarea daunei (de exemplu, dimensiunea informațiilor încălcate) sau de impactul acesteia.
- Un element esențial al statisticilor sectoriale este **frecvența apariției** amenințărilor cibernetice individuale. Aceasta oferă o idee despre cea mai comună metodă de atac utilizată într-un sector. Astfel de statistici pot oferi orientări cu privire la nivelul necesar de pregătire sau maturitate a controalelor individuale de securitate care reduc expunerea la amenințările cibernetice relevante.
- Având în vedere datele de mai sus, relevante pentru statisticile incidentelor, acest raport oferă o clasificare aproximativă a sectoarelor în ceea ce privește incidentele observate, împreună cu o tendință rezultată din dinamica emergentă a expunerii potențiale a fiecărui sector. De asemenea, sunt furnizate o serie de informații despre cei mai populari vectori de atac pe sector. În acest scop, informațiile din diferite publicații au fost consolidate[1,2,3,4].

Tendințele incidentelor

SECTOR	CELE MAI POPULARE AMENINȚĂRI / ATACURI	TENDINȚELE INCIDENTELOR
Persoană fizică	• Phishing • Malware • Scurgerile de informații • Furtul de date	Stabile
Industrii multiple	• Atacuri asupra aplicațiilor web • Phishing • Malware	În creștere
Administrație publică, apărare, servicii sociale	• Malware • Phishing • Atac online	Stabile ușor descrescătoare
Financiar/Bancar/Asigurări	• Atacuri asupra aplicațiilor web • Amenințări din interior (abuz neintenționat) • Malware • Furtul de date	Stabile
Sănătate/Medical	• Malware • Amenințări din interior (abuz/eroare neintenționat/ă) • Atacuri asupra aplicațiilor web	În creștere
Educație	• Malware • Ransomware • Atacuri online	Stabile ușor descrescătoare
Informare și comunicare	• Atacuri asupra aplicațiilor web • Amenințări din interior (abuz/eroare neintenționat/ă) • Malware	Stabile
Servicii profesionale/ digitale	• Atac asupra aplicațiilor web • Amenințări din interior (abuz/eroare neintenționat/ă) • Malware	Stabile
Arte, divertisment și jocuri[8]	• Atacuri asupra aplicațiilor web • Malware • Phishing	Stabile
Sectorul manufacturier	• Malware • Atacuri asupra aplicațiilor web • Amenințări din interior (abuz/eroare neintenționat/ă)	Stabile

SECTOR	FACTORI DE INFLUENȚĂ
Persoană fizică	Autoizolarea în urma măsurilor de izolare din cauza pandemiei de COVID-19 a dus la medii IT dispersate/descentralizate și la izolarea utilizatorilor care sunt mai ușor de păcălit și au mai puține controale de securitate decât era cazul în mediile centralizate.
Industrii multiple	Utilizatorii la distanță în urma măsurilor de izolare din cauza pandemiei de COVID-19 au facilitat atacurile prin phishing și scurgerea de informații sensibile (și anume, date de identificare).
Administrație publică, apărare, servicii sociale	Este posibil ca utilizarea serviciilor cloud să fi influențat securitatea ofertelor publice. Cu toate acestea, serviciile sociale au fost afectate de un număr semnificativ de atacuri din cauza ajutoarelor financiare oferite cetățenilor în timpul pandemiei de COVID-19.
Financiar/ Bancar/Asigurări	Complexitatea sectorului financiar face dificilă interpretarea situației amenințărilor, întrucât domeniile diferite din cadrul serviciilor financiare și bancare se pot confrunta cu riscuri și amenințări cibernetice complet diferite.
Sănătate/Medical	Atenția acordată de infractorii cibernetici obiectivelor din domeniul sănătății a crescut considerabil din cauza motivelor financiare și a importanței sectorului în timpul pandemiei de COVID-19.
Educație	Deși stabil, acest sector a fost vizat în 2020 de campanii de spionaj cibernetic din cauza interesului pentru rezultatele cercetării privind COVID-19.
Informare și comunicare	Acest sector este în mod constant sub presiune din cauza dificultăților de a proteja o suprafață imensă de atac, introdusă de platformele media digitale. Pentru organizațiile mass-media online, atacurile care provoacă daune reputației reprezintă una dintre cele mai mari amenințări.
Servicii profesionale/ digitale	Deși stabil, acest sector a fost vizat în 2020 de diferite campanii, în încercarea de a extrage informații de la utilizatorii serviciilor digitale de telemuncă de acasă în timpul pandemiei de COVID-19.
Arte, divertisment și jocuri	Trecerea de la un model de afaceri licențiat la unul bazat pe abonament adoptat de industria jocurilor a sporit atractivitatea acestui sector pentru infractorii cibernetici[8].
Sectorul manufacturier	Atacurile din lanțul de aprovizionare și atacurile împotriva sistemelor de control industrial reprezintă principalele amenințări pentru întreprinderi din sectorul manufacturier deoarece acestea pot să oprească o întreagă linie de producție. Furtul de date de proprietate intelectuală este o altă amenințare serioasă pentru acest sector.

Amenințări asupra tehnologiilor emergente

Următoarea generație de comunicații mobile sau 5G

COMPONENTE CONEXE – GRUPURI DE ACTIVE	EXPUNERE LA AMENINȚĂRI
Rețea de bază	Abuz determinat de accesul la distanță, vârfuri de trafic de autentificare, abuz de date de autentificare/autorizare a utilizatorilor, abuz de funcții de rețea găzduite de terți, abuz de funcții de interceptare legală, exploatarea interfeței de programare a aplicației (API), exploatarea arhitecturii și planificării prost concepute, exploatarea de sisteme/rețele greșit sau slab configurate, utilizarea sau administrarea eronată a rețelei, sistemelor și dispozitivelor, scenarii de fraudă legate de interconectări în roaming, mișcarea laterală, ștergerea memoriei, manipularea traficului de rețea, recunoașterea rețelei și colectarea de informații, manipularea datelor de configurare a rețelei, Inundarea rău intenționată a componentelor de bază ale rețelei, deturnarea rău intenționată a traficului, manipularea orchestratorului de resurse ale rețelei, utilizarea incorectă a instrumentelor de audit, utilizări oportuniste și frauduloase ale resurselor partajate, înregistrarea funcțiilor de rețea dăunătoare, detectarea traficului, atacuri pe canale laterale
Acces la rețea	Abuz de resurse de spectru, intoxicația cu Protocolul de Rezoluție a Adreselor (ARP), nod de rețea de acces fals, atac de inundații, atacuri de captare IMSI, blocarea frecvenței radio, trișarea (spoofing) MAC, manipularea datelor de configurare a rețelei de acces, interferențe radio, manipularea traficului radio, deturnarea sesiunii, semnalizarea fraudelor, semnalizarea furtunilor

COMPONENTE CONEXE – GRUPURI DE ACTIVE	EXPUNERE LA AMENINȚĂRI
Calcul MultiEdge	Gateway MEC fals, supraîncărcare a nodului Edge, abuz de interfețe de programare a aplicațiilor (API) Edge Open
Virtualizarea funcțiilor de rețea și rețelele definite de software	Abuz pe protocolul de interconectare a centrelor de date (DCI), abuz de resurse de calcul cloud, ocolirea virtualizării rețelei, abuz de gazdă virtualizată
Infrastructură fizică	Manipularea echipamentelor hardware, dezastre naturale care afectează infrastructura de rețea, sabotaj fizic/vandalism al infrastructurii de rețea, amenințare din partea personalului terților care accesează mecanismele MNO, exploatarea formatului cardului cu circuit integrat universal (UICC), compromiterea echipamentelor utilizatorilor
Toate grupurile de active 5G de mai sus	Blocarea serviciului (DoS), încălcarea securității datelor, scurgerea de informații, furtul, distrugerea și manipularea informațiilor, ascultarea, exploatarea vulnerabilităților software și hardware, cod sau software rău intenționat, lanț de aprovizionare compromis, furnizori și furnizori de servicii compromiși, amenințări/atacuri țintite, exploatarea deficiențelor în procedurile de securitate, gestionare și operaționale, abuz de autentificare, furt de identitate sau spoofing

Amenințări asupra tehnologiilor emergente

Internetul lucrurilor (IoT)

COMPONENTE CONEXE – GRUPURI DE ACTIVE	EXPUNERE LA AMENINȚĂRI
Factorul uman	Amenințări din interior, probleme legate de munca în echipă, limitări interne, hacktivism, pierderea serviciilor de asistență, întreruperea utilităților, întrerupere de rețea, modificări neintenționate, sabotaj, încălcarea normelor și reglementărilor, încălcarea legislației, cerințe contractuale, nerespectarea cerințelor contractuale (de exemplu, întreținerea programelor informatice), exploatarea software-ului, inginerie socială, furt de identitate.
Proiectare de software	Amenințări din interior, hacktivism, modificări neintenționate, utilizarea sau administrarea eronată a dispozitivelor și sistemelor, sabotaj, deficiențe ale procesului SDLC, eșecuri ale unor terți, nerespectarea cerințelor contractuale (de exemplu, întreținerea programelor informatice), exploatarea programelor informatice, pierdere/scurgere de informații.
Dezvoltare de software	Amenințări din interior, hacktivism, pierderea serviciilor de asistență, modificări neintenționate, utilizare sau administrare eronată de dispozitive și sisteme, sabotaj, vandalism și furt, vulnerabilități ale programelor informatice, deficiențe ale procesului SDLC, defecțiuni de întreținere, abuz de autorizare, exploatarea programelor informatice, manipularea infrastructurii SDLC, pierdere/scurgere de informații.
Implementare de software	Amenințări din interior, hacktivism, pierderea serviciilor de asistență, modificări neintenționate, utilizare sau administrare eronată de dispozitive și sisteme, sabotaj, vandalism și furt, vulnerabilități ale programelor informatice, deficiențe ale procesului SDLC, eșecuri ale unor terți, abuz de autorizare, exploatarea programelor informatice, manipularea infrastructurii SDLC, blocarea serviciului, manipularea informațiilor, divulgare, pierdere/scurgere de informații.

COMPONENTE CONEXE – GRUPURI DE ACTIVE	EXPUNERE LA AMENINȚĂRI
Date	Amenințări din interior, hacktivism, pierderea serviciilor de asistență, modificări neintenționate, utilizare sau administrare eronată de dispozitive și sisteme, sabotaj, vandalism și furt, vulnerabilități ale programelor informatice, deficiențe ale procesului SDLC, eșecuri ale unor terți, abuz de autorizare, exploatarea programelor informatice, manipularea infrastructurii SDLC, blocarea serviciului, manipularea informațiilor, divulgare, pierdere/scurgere de informații.
Întreținere	Amenințări din interior, hacktivism, întreruperea utilităților, întrerupere de rețea, modificări neintenționate, utilizare sau administrare eronată de dispozitive și sisteme, daune cauzate de un terț, sabotaj, vandalism și furt, atacuri cu acces fizic, acces forțat, cerințe contractuale, vulnerabilități ale programelor informatice, deficiențe ale procesului SDLC, eșecuri ale unor terți, nerespectarea cerințelor contractuale (de exemplu, întreținerea programelor informatice), defecțiuni de întreținere, abuz de autorizare, exploatarea programelor informatice, manipularea infrastructurii SDLC, blocarea serviciului, manipularea informațiilor, divulgare, pierdere/scurgere de informațiilor
Componente ale programelor informatice	Amenințări din interior, hacktivism, pierderea serviciilor de asistență, modificări neintenționate, utilizare sau administrare eronată a dispozitivelor și sistemelor, daune cauzate de un terț, scurgeri de informații, sabotaj, vandalism și furt, atacuri cu acces fizic, acces forțat, cerințe contractuale, vulnerabilități ale programelor informatice, deficiențe ale procesului SDLC, eșecuri ale unor terți, nerespectarea cerințelor contractuale (de exemplu, întreținerea programelor informatice), defecțiuni de întreținere, abuz de autorizare, exploatarea programelor informatice, manipularea infrastructurii SDLC, blocarea serviciului, manipularea informațiilor, divulgare, pierdere/scurgere de informații

Amenințări asupra tehnologiilor emergente

Mașini inteligente

COMPONENTE CONEXE – GRUPURI DE ACTIVE	EXPUNERE LA AMENINȚĂRI
Senzori și actuatoare auto	Blocarea serviciului, malware, manipularea informațiilor, atacuri țintite împotriva OEM, activități neautorizate, furt de identitate, abuz de autorizații, manipularea informațiilor, amenințări care vizează senzori autonomi, amenințări împotriva IA și ML, sabotaj, vandalism, furt, atacuri pe canale laterale, injecție de erori, furt, defectarea sau funcționarea necorespunzătoare a unui senzor/actuator, exploatarea vulnerabilităților programelor informatice, deturnarea protocolului de comunicare, atac tip om-la-mijloc/deturnarea sesiunii, modificarea neintenționată a datelor sau a configurației componentelor mașinii, utilizarea de informații și/sau dispozitive dintr-o sursă nesigură, utilizarea eronată a configurației componentelor mașinii, întrerupere de rețea, nerespectarea cerințelor contractuale, încălcarea normelor și reglementărilor/încălcarea legislației/abuzul de date cu caracter personal.
Algoritmi de luare a deciziilor **ECU-uri auto, componente de procesare și luare a deciziilor** **Infrastructură de mașini inteligente și sisteme de backend**	Blocarea serviciului, malware, manipularea informațiilor, atacuri țintite împotriva OEM, activități neautorizate, furt de identitate, abuz de autorizații, manipularea informațiilor, amenințări împotriva IA și ML, sabotaj, vandalism, furt, furt, defectarea sau funcționarea necorespunzătoare a unui senzor/actuator, exploatarea vulnerabilităților programelor informatice, defectarea sau întreruperea serviciului, deturnarea protocolului de comunicare, redarea datelor, atac tip om-la-mijloc/deturnarea sesiunii, modificarea neintenționată a datelor sau a configurației componentelor mașinii, utilizarea de informații și/sau dispozitive dintr-o sursă nesigură, utilizarea eronată a configurației componentelor mașinii, pierderea semnalului GNSS, întrerupere de rețea, nerespectarea cerințelor contractuale, încălcarea normelor și reglementărilor/încălcarea legislației/abuzul de date cu caracter personal

COMPONENTE CONEXE – GRUPURI DE ACTIVE	EXPUNERE LA AMENINȚĂRI
Funcțiile vehiculului **Senzori și actuatoare auto** **ECU-uri auto, componente de procesare și luare a deciziilor**	Blocarea serviciului, malware, manipularea informațiilor, atacuri țintite împotriva OEM, activități neautorizate, furt de identitate, abuz de autorizații, manipularea informațiilor, amenințări care vizează senzori autonomi, amenințări împotriva IA și ML, sabotaj, atacuri pe canale laterale, injecție de erori, furt, defectarea sau funcționarea necorespunzătoare a unui senzor/actuator, exploatarea vulnerabilităților programelor informatice, defectarea sau întreruperea serviciului, deturnarea protocolului de comunicare, redarea datelor, atac tip om-la-mijloc/deturnarea sesiunii, modificarea neintenționată a datelor sau a configurației componentelor mașinii, utilizarea de informații și/sau dispozitive dintr-o sursă nesigură, utilizarea eronată a configurației componentelor mașinii, bateria descărcată a mașinii, întrerupere de rețea, nerespectarea cerințelor contractuale, încălcarea normelor și reglementărilor/încălcarea legislației/abuzul de date cu caracter personal
Gestionarea programelor **ECU-uri auto, componente de procesare și luare a deciziilor** **Componente de comunicare în vehicul**	Blocarea serviciului, malware, manipularea informațiilor, atacuri țintite împotriva OEM, activități neautorizate, furt de identitate, abuz de autorizații, sabotaj, atacuri pe canale laterale, injecție de erori, furt, defectarea sau funcționarea necorespunzătoare a unui senzor/actuator, exploatarea vulnerabilităților programelor informatice, defectarea sau întreruperea serviciului, deturnarea protocolului de comunicare, atac tip om-la-mijloc/deturnarea sesiunii, modificarea neintenționată a datelor sau a configurației componentelor mașinii, utilizarea de informații și/sau dispozitive dintr-o sursă nesigură, întrerupere de rețea, nerespectarea cerințelor contractuale, încălcarea normelor și reglementărilor/încălcarea legislației/abuzul de date cu caracter personal
Componente de comunicare în interiorul vehiculului	Blocarea serviciului, malware, manipularea informațiilor, atacuri țintite împotriva OEM, activități neautorizate, furt de identitate, abuz de autorizații, manipularea informațiilor, sabotaj, atacuri pe canale laterale, injecție de erori, furt, defectarea sau funcționarea necorespunzătoare a unui senzor/actuator, exploatarea vulnerabilităților programelor informatice, deturnarea protocolului de comunicare, redarea datelor, atac tip om-la-mijloc/deturnarea sesiunii, modificarea neintenționată a datelor sau a configurației componentelor mașinii, utilizarea de informații și/sau dispozitive dintr-o sursă nesigură, utilizarea eronată a configurației componentelor mașinii, întrerupere de rețea, nerespectarea cerințelor contractuale, încălcarea normelor și reglementărilor/încălcarea legislației/abuzul de date cu caracter personal

Amenințări asupra tehnologiilor emergente

_ Mașini inteligente

COMPONENTE CONEXE – GRUPURI DE ACTIVE	EXPUNERE LA AMENINȚĂRI
Rețele și protocoale de comunicare. **ECU-uri auto, componente de procesare și luare a deciziilor** **Componente de comunicare în vehicul**	Blocarea serviciului, malware, manipularea informațiilor, atacuri țintite împotriva OEM, activități neautorizate, furt de identitate, abuz de autorizații, sabotaj, furt, defectarea sau funcționarea necorespunzătoare a unui senzor/actuator, exploatarea vulnerabilităților programelor informatice, deturnarea protocolului de comunicare, redarea datelor, atac tip om-la-mijloc/deturnarea sesiunii, modificarea neintenționată a datelor sau a configurației componentelor mașinii, utilizarea de informații și/sau dispozitive dintr-o sursă nesigură, utilizarea eronată a configurației componentelor mașinii, întrerupere de rețea, nerespectarea cerințelor contractuale, încălcarea normelor și reglementărilor/încălcarea legislației/abuzul de date cu caracter personal.
Componente externe din apropiere **Infrastructură de mașini inteligente și sisteme de backend**	Blocarea serviciului, malware, manipularea informațiilor, atacuri țintite împotriva OEM, activități neautorizate, furt de identitate, abuz de autorizații, manipularea informațiilor, sabotaj, vandalism, furt, exploatarea vulnerabilităților programelor informatice, defectarea sau întreruperea serviciului, deturnarea protocolului de comunicare, atac tip om-la-mijloc/deturnarea sesiunii, modificarea neintenționată a datelor sau a configurației componentelor mașinii, utilizarea de informații și/sau dispozitive dintr-o sursă nesigură, pierderea semnalului GNSS, întrerupere de rețea, nerespectarea cerințelor contractuale, încălcarea normelor și reglementărilor/încălcarea legislației/abuzul de date cu caracter personal

COMPONENTE CONEXE – GRUPURI DE ACTIVE	EXPUNERE LA AMENINȚĂRI
Servere, sisteme și cloud computing **Infrastructură de mașini inteligente și sisteme de backend**	Blocarea serviciului, malware, manipularea informațiilor, atacuri țintite împotriva OEM, activități neautorizate, furt de identitate, abuz de autorizații, manipularea informațiilor, sabotaj, exploatarea vulnerabilităților programelor informatice, defectarea sau întreruperea serviciului, deturnarea protocolului de comunicare, redarea datelor, atac tip om-la-mijloc/deturnarea sesiunii, modificarea neintenționată a datelor sau a configurației componentelor mașinii, utilizarea de informații și/sau dispozitive dintr-o sursă nesigură, pierderea semnalului GNSS, întrerupere de rețea, nerespectarea cerințelor contractuale, încălcarea normelor și reglementărilor/încălcarea legislației/abuzul de date cu caracter personal
Informații	Blocarea serviciului, malware, manipularea informațiilor, atacuri țintite împotriva OEM, activități neautorizate, Furt de identitate, abuz de autorizații, manipularea informațiilor, amenințări care vizează senzori autonomi, amenințări împotriva IA și ML, sabotaj, vandalism, furt, atacuri pe canale laterale, injecție de erori, furt, defectarea sau funcționarea necorespunzătoare a unui senzor/actuator, exploatarea vulnerabilităților programelor informatice, defectarea sau întreruperea serviciului, deturnarea protocolului de comunicare, redarea datelor, atac tip om-la-mijloc/deturnarea sesiunii, modificarea neintenționată a datelor sau a configurației componentelor mașinii, scurgeri de informații, utilizarea de informații și/sau dispozitive dintr-o sursă nesigură, utilizarea eronată a configurației componentelor mașinii, pierderea semnalului GNSS, întrerupere de rețea, nerespectarea cerințelor contractuale, încălcarea normelor și reglementărilor/încălcarea legislației/abuzul de date cu caracter personal
Oameni	Blocarea serviciului, malware, manipularea informațiilor, atacuri țintite împotriva OEM, activități neautorizate, furt de identitate, abuz de autorizații, manipularea informațiilor, sabotaj, vandalism, furt, defectarea sau funcționarea necorespunzătoare a unui senzor/actuator, exploatarea vulnerabilităților programelor informatice, defectarea sau întreruperea serviciului, deturnarea protocolului de comunicare, redarea datelor, atac tip om-la-mijloc/deturnarea sesiunii, modificarea neintenționată a datelor sau a configurației componentelor mașinii, scurgeri de informații, utilizarea de informații și/sau dispozitive dintr-o sursă nesigură, utilizarea eronată a configurației componentelor mașinii, pierderea semnalului GNSS, bateria descărcată a mașinii, întrerupere de rețea, nerespectarea cerințelor contractuale, încălcarea normelor și reglementărilor/încălcarea legislației/abuzul de date cu caracter personal

Referințe

1. „April 2020 Cyber Attacks Statistics” (Statistici despre atacurile cibernetice din aprilie 2020). 3 iunie 2019. HACKMAGEDDON. https://www.hackmageddon.com/2020/06/03/april-2020-cyber-attacks-statistics/

2. „Data Breach Investigation Report” (Raport de investigație a încălcărilor securității datelor), 2019. Verizon. https://enterprise.verizon.com/resources/reports/dbir/

3. „CIRCL - Operational Statistics” (CIRCL – Statistici operaționale), 2019. CIRCL. https://www.circl.lu/opendata/statistics/

4. „Survey: The Third Annual Study on the State of Endpoint Security Risk” (Al treilea studiu anual privind situația riscului de securitate al punctului final). 2020. https://engage.morphisec.com/2020-endpoint-security-risk-study

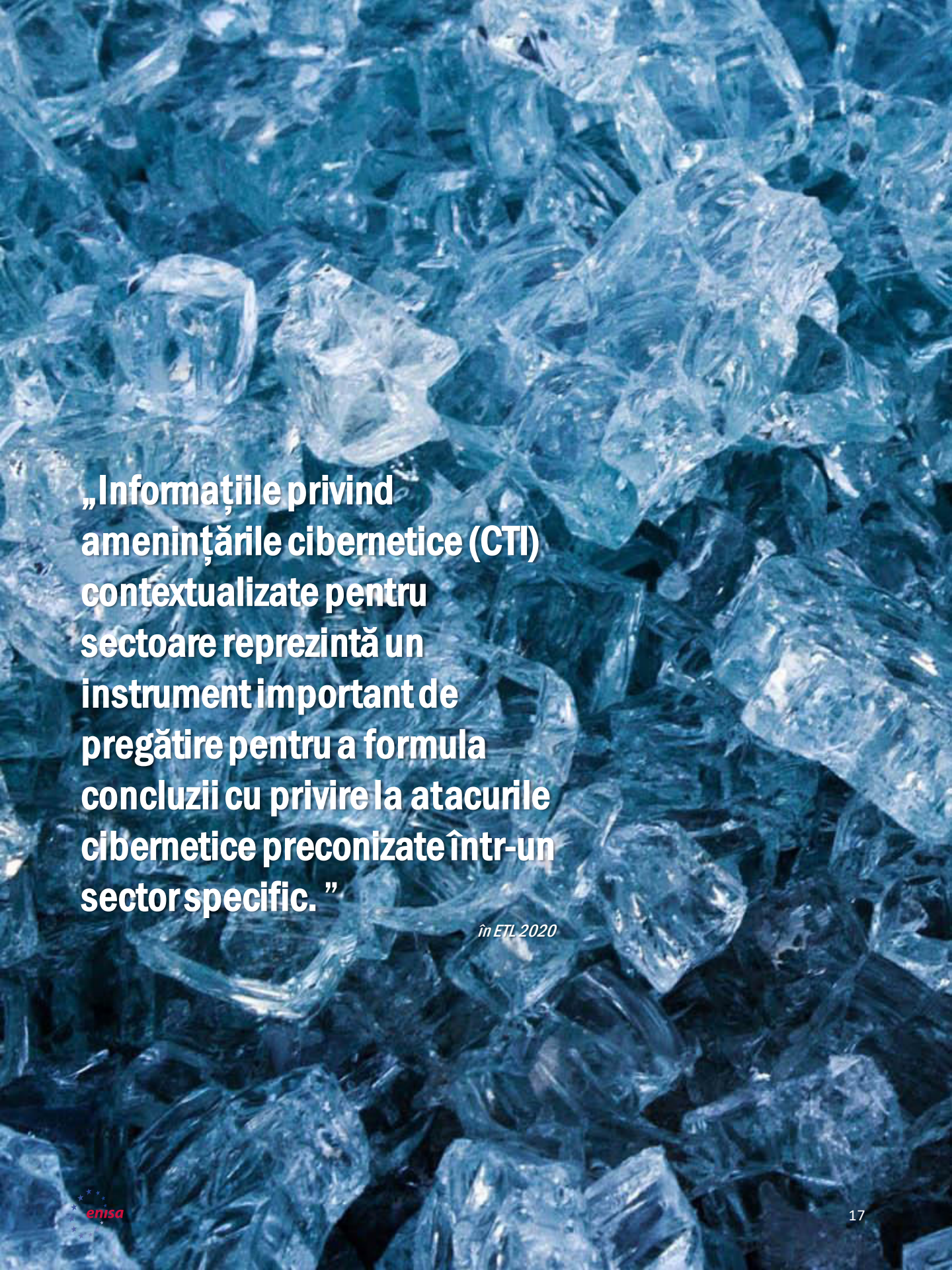
5. „Good Practices for Security of IoT - Secure Software Development Lifecycle” (Bune practici pentru securitatea IoT – Ciclul de viață al dezvoltării de software sigur). 19 noiembrie 2019. ENISA. https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1

6. „ENISA good practices for security of Smart Cars” (Bune practici ENISA pentru securitatea mașinilor inteligente). 25 noiembrie 2019. https://www.enisa.europa.eu/publications/smart-cars

7. Ordinea selectată a sectoarelor a fost realizată prin consolidarea statisticilor din diferite rapoarte bazate pe incidente. Aceasta oferă valori mediane pentru perioada de raportare (2019-T1 2020) și se poate abate ușor de la valorile prezentate în rapoarte lunare sau trimestriale.

8. „Player vs. Hacker: Cyberthreats to Gaming Companies and Gamers” (Jucător vs. Hacker: amenințări cibernetice pentru companiile de jocuri și jucători). 16 martie 2020. Security Intelligence. https://securityintelligence.com/posts/player-vs-hacker-cyberthreats-to-gaming-companies-and-gamers/

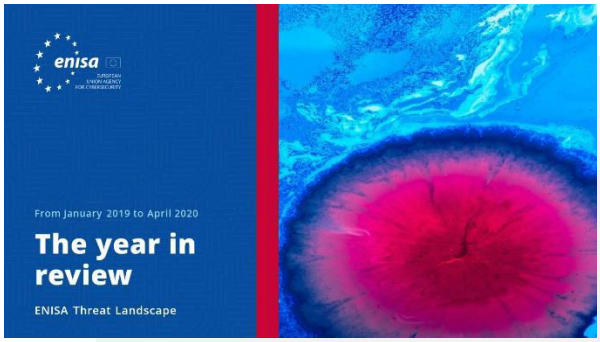
9. Trebuie menționat faptul că expunerea la amenințări a fost evaluată prin intermediul categoriilor detaliate de amenințări care au fost definite de ENISA (vezi https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view) și este utilizată pentru diferite evaluări sectoriale. Din cauza absenței datelor privind incidentele pentru sectoarele emergente, evaluarea amenințărilor este mai detaliată pentru a obține o abordare mai exhaustivă.



„Informațiile privind amenințările cibernetice (CTI) contextualizate pentru sectoare reprezintă un instrument important de pregătire pentru a formula concluzii cu privire la atacurile cibernetice preconizate într-un sector specific. ”

în ETL 2020

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 în diferite sectoare din securitatea cibernetică și informațiile privind amenințările cibernetice.

CITIȚI RAPORTUL

Raportul ENISA privind situația amenințărilor **Principalele incidente din UE și din întreaga lume**

Principalele incidente de securitate cibernetică survenite 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 la 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 privind 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