RO

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

ianuarie 2019 – aprilie 2020

Teme de cercetare

Raportul ENISA privind situația amenințărilor

Prezentare generală

Datorită activităților de cercetare și inovare desfășurate de cadre universitare, industrie și profesioniști din întreaga lume, apar noi concepte și idei în domeniul securității cibernetice. Sunt pași importanți deoarece ritmul inovării adoptat de adversari (de exemplu, actorii rău intenționați) este mai mare decât cel al specialiștilor în securitate cibernetică care găsesc soluții pentru a-i descuraja. De fapt, în afară de igiena și instruirea de bază în materie de securitate cibernetică, investițiile în cercetare și inovare reprezintă cea mai viabilă opțiune pentru ca apărătorii să se apropie de ceea ce este necesar pentru a îmbunătăți securitatea spațiului cibernetic. În acest raport evidențiem unele dintre cele mai importante subiecte de cercetare și inovare în domeniul securității cibernetice explorate în UE și în întreaga lume.

O mai bună înțelegere a dimensiunii umane

Securitatea cibernetică este văzută în continuare ca o practică de protejare a rețelelor, a sistemelor de informații și a datelor (NIS). Această definiție trebuie extinsă în continuare dincolo de problemele tehnice pentru a include preocupări sociale, comportamentale și economice și diferitele roluri îndeplinite de părțile implicate. Aceasta ar trebui să constituie o prioritate în viitoarele cercetări în materie de securitate cibernetică și discuții despre inovare. O mai bună înțelegere a dimensiunii umane este esențială în definirea oricărei strategii de securitate cibernetică, astfel încât deciziile de securitate să fie luate pentru a satisface nevoile, abilitățile și așteptările oamenilor.

Cercetare și inovare în domeniul securității cibernetice

În cursul anului 2019 am observat o creștere a numărului de laboratoare de testare și medii cibernetice de simulare în scopuri de antrenament (cyber ranges)[1] care devin disponibile la fața locului și în ofertele cloud. Acestea sunt resurse esențiale pentru cercetători pentru simularea de atacuri, dezvoltarea de scenarii de exploatare, obținerea de date operaționale și testarea strategiilor de apărare într-un mediu virtual multifuncțional. Cu toate acestea, mediile de testare existente au lipsuri în ceea ce privește replicarea multor vulnerabilități care compromit de regulă securitatea, cum ar fi, printre altele, factorii umani și de inginerie. Pentru a îmbunătăți eficiența, este important să se cerceteze și să se inoveze domeniul de aplicare și fidelitatea acestor laboratoare de testare și să se propună noi soluții tehnice.

Prezentare generală

Securitatea rețelelor 5G

Lansarea rețelelor mobile 5G a început în unele țări în 2019, dar se așteaptă ca numărul de instalații să crească în 2021. Această nouă generație de comunicații mobile are o importanță capitală pentru progresul social și economic al Uniunii Europene. Prin urmare, cercetarea și dezvoltarea viitoare a soluțiilor de securitate 5G sunt cruciale pentru durabilitatea și fiabilitatea acestei tehnologii. În 2019, ENISA a publicat un raport privind situația amenințărilor în cazul rețelelor 5G care analizează unele aspecte critice de securitate legate de această tehnologie emergentă.[2] Subiectele cheie în cercetarea și inovarea securității rețelelor 5G trebuie să ia în considerare următoarele aspecte.

- Cercetarea și dezvoltarea controalelor de securitate pentru a acoperi protecția rețelei, a elementelor fizice și a straturilor de date, oferind astfel o soluție de protecție pe mai multe niveluri. Odată cu rețelele 5G, datele vor fi localizate pe servere de cloud centralizate, noduri „fog" intermediare și dispozitive „edge", sporind complexitatea în ceea ce privește implementarea unei soluții de securitate.

- Cercetarea și dezvoltarea standardelor și cerințelor pentru controalele de securitate pentru punerea în aplicare în cadrul rețelelor interconectate cu mai mulți proprietari, topologii, operatori și o varietate diversificată de dispozitive și straturi de rețea.

- Cercetarea și dezvoltarea de capacități cheie de gestionare care permit interoperabilitatea sigură între nodurile care conectează dispozitive periferice cu resurse limitate și dispozitive IoT. Această capacitate trebuie să includă un control eficace al accesului, autentificare, criptografie și tehnici cheie de gestionare pentru noduri cu resurse limitate.

Proiecte UE de cercetare și inovare în domeniul securității cibernetice

- UE lucrează la stabilirea unui proiect-pilot pentru o rețea de competențe în materie de securitate cibernetică. CONCORDIA[3], ECHO[4], SPARTA[5] și CyberSec4Europe[6] sunt cele patru proiecte pilot câștigătoare ale cererii de propuneri de securitate cibernetică Orizont 2020 din 2018, în vederea „stabilirii și operării unui proiect pilot pentru o rețea europeană de competență în materie de securitate cibernetică și dezvoltarea unei foi de parcurs europene comune pentru cercetare și inovare în domeniul securității cibernetice". UE se așteaptă să-și consolideze capacitatea de securitate cibernetică și să abordeze provocările viitoare în materie de securitate cibernetică cu aceste patru proiecte pilot, pentru o piață unică digitală a UE mai sigură.
- UE acordă 38 de milioane EUR pentru protecția infrastructurii critice împotriva amenințărilor cibernetice. Comisia Europeană a anunțat angajamente de peste 38 de milioane EUR prin Orizont 2020 pentru programul de cercetare și inovare al UE. Programul este menit să sprijine mai multe proiecte inovatoare în domeniul protecției infrastructurii critice împotriva amenințărilor cibernetice și fizice și să facă orașele mai inteligente și mai sigure.[7]
- UE a lansat o cerere de propuneri în valoare de 10,5 milioane EUR pentru proiecte în domeniul securității cibernetice. Comisia a lansat o nouă cerere de propuneri în valoare de 10,5 milioane EUR prin programul Mecanismul pentru interconectarea Europei (MIE) pentru proiecte care să contribuie la consolidarea capacităților de securitate cibernetică ale Europei și a cooperării între statele membre.[8]

Cercetare și inovare în domeniul CTI

Diseminarea rapidă a metodelor și conținutului CTI

Au fost identificate diverse nevoi de cercetare în perioada de raportare, iar în continuare sunt propuse acțiunile pentru soluționarea acestor nevoi. Acestea au fost grupate în unele categorii pentru a reflecta mai bine domeniul de aplicare. Deși pot exista suprapuneri, aceste categorii sunt indicative pentru domeniile potențialelor îmbunătățiri ale CTI.

- **Rezultatele proiectelor de cercetare în domeniul CTI trebuie evaluate și cartografiate într-un context mai larg al CTI** pentru a identifica suprapunerile și lacunele și pentru a le face comparabile cu produsele, serviciile și practicile comerciale CTI existente. Acest lucru va contribui la diseminarea rezultatelor către comunitatea de utilizatori. În același timp, decalajele existente vor fi completate de funcții, conținuturi și procese suplimentare. Proiectele UE (Orizont H2020) cu relevanță CTI sunt candidate excelente pentru această sarcină, contribuind la îmbunătățirea practicilor CTI.
- **Trebuie să se promoveze furnizarea și utilizarea materialului CTI de tip sursă deschisă.** Acest lucru va facilita transferul de cunoștințe, dar va reduce, de asemenea, pragul de competențe CTI. Open-CTI este candidatul perfect pentru acest scop deoarece susține absorbția de CTI din mai multe surse într-o singură bază care poate fi partajată între diferiți utilizatori, oferind în același timp un set de funcții pentru gestionarea acestor informații. Prin adoptarea Open-CTI, utilizatorii vor fi în măsură să obțină informații valoroase la un prag de calificare relativ scăzut.

_Cercetări care rezultă în noi tendințe

Necesitatea **consolidării CTI** cu alte instrumente de securitate cibernetică stabilite necesită evoluția structurală și contextuală a acestui domeniu. În același timp, progresele tehnologice aduse de tehnologiile emergente pun problema modului în care CTI poate beneficia de aceste evoluții. Astfel, necesitățile **viitoare de cercetare** în domeniul CTI vor contribui la îmbunătățirea proceselor, funcțiilor, automatizării, structurii și validării conținutului, furnizării de servicii, vitezei către utilizator/diseminării, implementării și corelărilor CTI.

CTI s-a impus ferm în domeniul securității cibernetice ca un instrument esențial pentru îmbunătățirea agilității și a eficienței în apărarea împotriva atacurilor cibernetice.

Cercetare și inovare în domeniul CTI

Funcționalitate, nivel de automatizare și respectarea cerințelor de maturitate

- **Automatizarea proceselor își va asuma un rol cheie în CTI.** În timp ce atacurile cibernetice moderne au devenit puternic automatizate, organizațiile încearcă să se apere împotriva lor manual sau utilizând parțial automatizarea. Aceasta este o competiție inegală, care încetinește viteza și capacitatea de reacție. Investigarea potențialei automatizări a proceselor CTI va fi vitală pentru a ajunge la un echilibru între atacatori și apărători. Pentru a realiza acest lucru va fi nevoie de o analiză aprofundată a etapelor procesului CTI și a opțiunilor pentru automatizarea acestor etape prin intermediul tehnologiilor disponibile și emergente.
- **Cerințele de maturitate a CTI vor trebui identificate mai detaliat.** Deși au fost dezvoltate anumite criterii/cerințe pentru selectarea funcțiilor CTI (de exemplu, platforme de informații privind amenințările sau TIP-uri) pentru diferite profiluri de utilizatori CTI, vor fi necesare cerințe similare pentru alte produse, servicii și instrumente CTI. Astfel de cerințe vor fi asociate cu mai multe niveluri de maturitate și cheltuieli ale utilizatorilor și tipuri de CTI. Sunt necesare criterii/cerințe similare pentru diferite alte elemente ale unei infrastructuri CTI, cum ar fi instrumente, bune practici, platforme de partajare etc. Prin urmare, în afară de dezvoltarea modelelor de maturitate a capacității CTI, este necesară cercetarea pentru a arăta modul în care funcțiile CTI corespund unor niveluri diferite de maturitate CTI. Această activitate va contribui la creșterea vitezei de adoptare a practicilor CTI.
- **Utilizarea AI/ML în CTI trebuie investigată în continuare.** Aceasta va reduce numărul de etape manuale în analiza CTI și va crește valoarea funcțiilor ML în cadrul activităților CTI.

Construirea de punți către domenii conexe

- Trebuie dezvoltate **noi abordări pentru absorbția de cunoștințe CTI de către domenii** care pot profita de acestea. Exemplele includ medii cibernetice de simulare în scopuri de antrenament (cyber ranges), amenințări hibride, lanțuri de aprovizionare și evaluări și crize geopolitice. Întrebările care trebuie puse în acest sens includ: Care sunt punctele în care poate fi luat în considerare CTI? Ce conținut CTI este relevant? Care sunt criteriile de validare pentru adecvarea informațiilor CTI? Cum poate fi „conectat" CTI la informații despre domeniul în cauză? Ce fel de informații din aceste domenii pot fi adăugate la CTI? Sinergiile reflectate în aceste întrebări pot spori cazurile de utilizare și calitatea conținutului într-o manieră omnidirecțională.

- **CTI este esențială pentru o serie de discipline.** Exemplele includ evaluarea/gestionarea riscurilor și definirea cerințelor de protecție și certificare. Va fi benefic pentru aceste discipline să utilizeze CTI în mod corect. Contribuția CTI la aceste discipline poate fi identificată folosind informații precum modele de amenințare, informații despre factorii de amenințare (capacități, motive), metode de atac și exploit-uri. Deși există unele materiale relevante (de exemplu, cadrul de atac ATT&CK®), sunt necesare eforturi semnificative pentru a identifica și a standardiza astfel de interfețe de informații.

Cercetare și inovare în domeniul CTI

Eficacitatea operațiunilor CTI

- **Metodele de utilizare eficace a CTI vor constitui un instrument pentru luarea deciziilor.** Astfel de metode de implementare eficientă a CTI vor sprijini factorii de decizie să înțeleagă valoarea CTI, precum și practicienii să evalueze rentabilitatea investițiilor în CTI. Astfel de metode/indicatori de performanță vor trebui să ia în considerare factori independenți de conținutul CTI, având în vedere îmbunătățirile realizate pe parcursul întregului ciclu de viață de management al securității și de atenuare a riscurilor. În mod optim, măsurarea eficacității investițiilor în CTI va face parte dintr-o analiză mult mai largă a economiei securității cibernetice în diferite tipuri de organizații (de exemplu, în funcție de cerințele de securitate, nivelurile de maturitate etc.).

- Deși instrumentele cu costuri reduse prevalează pentru agregarea, analizarea și diseminarea CTI, **pot fi necesare unele cercetări pentru a identifica instrumente automate pentru gestionarea CTI** consumate și produse. În afară de formatele de date standardizate (de exemplu, fișiere CSV, STIX, TAXII), funcțiile CTI standard pot face obiectul unor astfel de cercetări, urmate de dezvoltarea unor instrumente ieftine cu sursă deschisă care să susțină astfel de funcții.

Evoluția structurii și conținutului CTI

- Pe măsură ce CTI pătrunde în domenii suplimentare, **informațiile din aceste contexte trebuie să fie reintroduse în baza de cunoștințe CTI originală**. De exemplu, structurile CTI trebuie definite pentru a capta informații geopolitice și despre amenințări hibride. Același lucru este valabil, de asemenea, pentru relevanța CTI pentru riscuri, incidente, analize criminalistice, niveluri de asigurare etc. Formatele CTI existente trebuie să evolueze pentru a capta informațiile care provin din aceste dependențe în CTI.

- **Tehnologii emergente, cum ar fi inteligența artificială,** pot fi utilizate pentru validarea CTI analizate. Astfel de instrumente pot să completeze sau chiar să înlocuiască analiza manuală a CTI, dar pot, de asemenea, să ofere asistență pe tot parcursul ciclului de viață a CTI (de exemplu, verificarea relevanței CTI pe baza informațiilor existente despre incident). Astfel de abordări noi ale CTI vor spori calitatea și relevanța informațiilor.

Referințe

1. Conceptul de mediu cibernetic de simulare în scopuri de antrenament (cyber range) a fost definit inițial în 2013 de Agenția Europeană de Apărare (AEA) în raportul „Obiectiv comun al personalului pentru cooperare militară în mediile cibernetice de simulare în scopuri de antrenament (cyber ranges) din Uniunea Europeană" ca mediu multifuncțional în sprijinul a trei procese principale: dezvoltarea, asigurarea și diseminarea cunoștințelor.

2. „ENISA Threat Landscape for 5G Networks" (Raportul ENISA privind situația amenințărilor pentru rețelele 5G) 21 noiembrie 2019. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

3. https://www.concordia-h2020.eu/

4 https://echonetwork.eu/

5. https://www.sparta.eu/news/

6. https://cybersec4europe.eu/

7. https://ec.europa.eu/programmes/horizon2020/en/news/eu-grants-%E2%82%AC38-million-protection-critical-infrastructure-against-cyber-threats

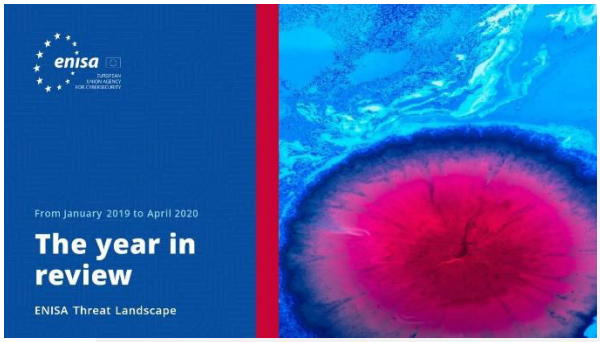
8. https://ec.europa.eu/digital-single-market/en/news/eu105-million-eu-funding-available-projects-stepping-eus-cybersecurity-capabilities-and

9. https://attack.mitre.org/

„CTI s-a impus ferm în domeniul securității cibernetice ca un instrument esențial pentru îmbunătățirea agilității și eficienței în apărarea împotriva atacurilor cibernetice.”

în ETL 2020

Documente conexe



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

Rezumat al principalelor tendințe de securitate cibernetică pentru anul respectiv.

CITIȚI RAPORTUL

Raportul ENISA privind situația amenințărilor
Lista celor mai importante 15 amenințări

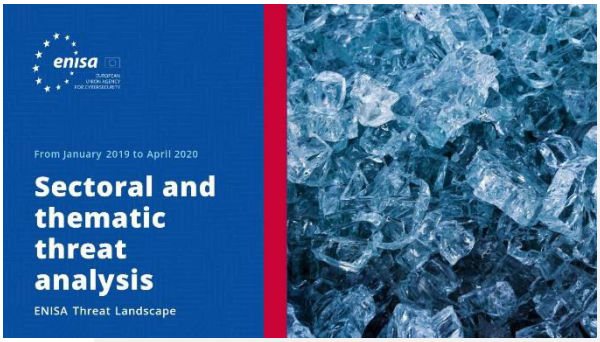
Lista ENISA a celor mai importante 15 amenințări din perioada ianuarie 2019 – aprilie 2020.

CITIȚI RAPORTUL

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

Principalele incidente de securitate cibernetică care au loc în perioada ianuarie 2019 - aprilie 2020.

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**

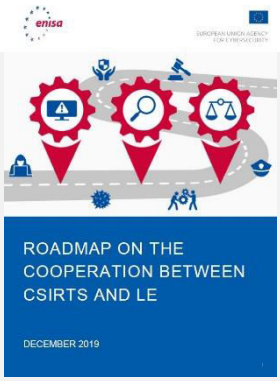
Principalele tendințe în securitatea cibernetică observate în perioada ianuarie 2019 - aprilie 2020.

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



Foaie de parcurs privind cooperarea dintre echipele CSIRT și autoritățile de aplicare a legii

Foaie de parcurs privind cooperarea între echipele CSIRT, în special cu autoritățile de aplicare a legii naționale și guvernamentale și cu sistemul judiciar.

CITIȚI RAPORTUL

Raport privind starea dezvoltării răspunsului la incidente al statelor membre UE

Studiu care vizează analizele actualului set operațional de răspuns la incidente în sectoarele NISD și identifică modificările recente.

CITIȚI RAPORTUL

Modelul ENISA de evaluare a maturității CSIRT

Versiune actualizată a studiului „Provocări pentru echipele CSIRT naționale în Europa în 2016: studiu privind maturitatea CSIRT” publicat de ENISA în 2017

CITIȚI RAPORTUL

„Complexitatea capacităților de amenințare a crescut în 2019, mulți adversari folosind exploit-uri, furtul de date de identificare și atacurile în mai multe etape.”

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 pentru completarea 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