RO

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

ianuarie 2019 – aprilie 2020

Trecerea în revistă a anului

Raportul ENISA privind situația amenințărilor

Înainte de a începe

_ 8 ani de revizuire a situației amenințărilor

Anul acesta, **Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA)** sărbătorește un an de la adoptarea noului Regulament privind securitatea cibernetică și a opta ediție a Raportului privind situația amenințărilor (ETL). Regulamentul privind securitatea cibernetică[1] reînnoiește și consolidează rolul ENISA, acordându-i un mandat permanent, mai multe resurse și noi sarcini. În plus, agenția începe un nou capitol cu un nou director executiv, o nouă strategie și o nouă structură organizațională. Având în vedere toate aceste schimbări, se impune și modificarea ETL , precum și adoptarea unei noi structuri și a unui aspect modern, renunțându-se la tipul de raport lung și rigid. Cu noua sa identitate și noul format vizual, raportul ETL a devenit un raport digital versatil, dinamic și ușor de utilizat, care urmărește să îndeplinească așteptările unui public exigent și în creștere.

ETL 2012

ETL 2020

Evoluția raportului ENISA privind situația amenințărilor din 2012 până în 2020

_ format ETL

Această ediție trece în revistă situația amenințărilor pentru perioada ianuarie 2019 - aprilie 2020 și este structurată în felul următor.

TRECEREA ÎN REVISTĂ A ANULUI Acest raport oferă o prezentare generală a situației amenințărilor, evidențiind cele mai importante teme la care se face referire în toate celelalte rapoarte. De asemenea, prezintă lista ENISA a celor mai importante 15 amenințări, concluzii și recomandări.

PREZENTARE GENERALĂ A INFORMAȚIILOR PRIVIND AMENINȚĂRILE CIBERNETICE Acest raport rezumă cele mai importante teme relevante pentru comunitatea de informații privind amenințările cibernetice (CTI) și cele discutate pe diferite forumuri.

ANALIZA SECTORIALĂ ȘI TEMATICĂ A AMENINȚĂRILOR Acest raport rezumă cele mai recente lucrări elaborate de ENISA, descriind situația amenințărilor pentru sectoare și tehnologii specifice. Anul acesta vă prezentăm concluziile din activitatea desfășurată în ceea ce privește rețeaua 5G, Internetul obiectelor (IoT) și mașinile inteligente.

PRINCIPALELE INCIDENTE DIN UE ȘI DIN ÎNTREAGA LUME Acest raport oferă o prezentare generală a incidentelor majore de securitate cibernetică care au loc în UE și în întreaga lume, subliniind lecțiile pe care le putem învăța din acestea.

TEME DE CERCETARE Acest raport prezintă aspecte cheie legate de cercetarea și inovarea în domeniul securității cibernetice.

TENDINȚE EMERGENTE Acest raport identifică tendințele emergente și se concentrează asupra provocărilor și oportunităților pentru viitor în domeniul securității cibernetice.

LISTA CELOR MAI IMPORTANTE 15 AMENINȚĂRI Un raport pentru fiecare amenințare, prezentând o imagine de ansamblu, constatările, incidentele majore, statisticile, vectorii de atac și măsurile de atenuare corespunzătoare.

Înainte de a începe

Metodologie

Conținutul produs pentru raportul ETL se bazează pe informații disponibile din surse deschise, în principal de natură strategică, și acoperă mai multe sectoare, tehnologii și contexte. Raportul urmărește să fie nepărtinitor în raport cu industria și furnizorii și face referiri sau citează lucrări din diverse cercetări în domeniul securității, bloguri din domeniul securității și articole din mass-media, identificate clar în text în mai multe note finale.

Pentru producerea raportului „ENISA privind situația amenințărilor", am urmat o abordare cu două componente. În primul rând, am efectuat cercetări documentare detaliate ale literaturii disponibile din surse deschise, cum ar fi articole de presă, opinii ale experților, rapoarte de date operative, analize ale incidentelor și rapoarte de cercetare în domeniul securității. În al doilea rând, am realizat interviuri cu membrii grupului de părți interesate din ETL, care sunt experți în domeniu și membri ai comunității UE de informații privind amenințările cibernetice (CTI). Aceștia din urmă ne-au ajutat să stabilim lista celor mai importante 15 amenințări și să validăm ipotezele cu privire la tendințele și provocările viitoare în domeniul securității cibernetice.

Mulțumim, de asemenea, membrilor Grupului părților interesate CTI pentru tot sprijinul oferit pentru realizarea rapoartelor în aceste opt ediții. Membrii acestui grup analizează și validează analiza produsă pentru fiecare raport ETL și votează lista anuală a celor mai importante 15 amenințări cibernetice.

Dorim să aflăm părerea dumneavoastră despre acest raport!
Vă rugăm să acordați câteva momente completării chestionarului. Pentru a accesa formularul, faceți clic aici.

Cui i se adresează anumite părți din raport

Raportul ETL este și strategic, și tehnic, conținând informații relevante atât pentru cititorii tehnici, cât și pentru cei non-tehnici. ETL se adresează diferitelor categorii de public și adoptă diferite niveluri de limbaj tehnic, în funcție de domeniu și de importanța subiectului pentru cititorii non-tehnici. Tabelul următor descrie tipul de public și de conținut pentru fiecare raport ETL.

RAPORTUL ETL	TIPUL DE CONȚINUT	PUBLICUL VIZAT
TRECEREA ÎN REVISTĂ A ANULUI	Generic	Toate
PREZENTARE GENERALĂ A CTI ↗	Specific	Membrii și practicienii comunității CTI.
ANALIZA SECTORIALĂ ȘI TEMATICĂ A AMENINȚĂRII ↗	Strategic	Experți în management strategic, factori de decizie politică și factori de decizie, analiști de risc, manageri și lideri în domeniul securității cibernetice.
PRINCIPALELE INCIDENTE DIN UE ȘI DIN ÎNTREAGA LUME ↗	Strategic	Experți în management strategic, factori de decizie politică și factori de decizie, analiști de risc, manageri de risc și lideri.
TEME DE CERCETARE ↗	Strategic	Experți în management strategic, factori de decizie politică și factori de decizie, analiști de risc, manageri de risc și lideri.
TENDINȚE EMERGENTE ↗	Strategic	Experți în management strategic, factori de decizie politică și factori de decizie, analiști de risc, manageri de risc și lideri.
LISTA CELOR MAI IMPORTANTE 15 AMENINȚĂRI ↗	Tehnic	Manageri de securitate a informațiilor (ISM), responsabili șefi pentru securitatea informațiilor (CISO), specialiști în securitate cibernetică și analiști CTI.

Cele mai importante 15 amenințări

Cele mai importante amenințări din 2018		Tendințe evaluate
1	Programele malware	---
2	Atacurile online	↗
3	Atacurile asupra aplicațiilor web	---
4	Phishing	↗
5	Blocarea serviciului	↗
6	Spamul	---
7	Rețelele botnet	↗
8	Încălcarea securității datelor	↗
9	Amenințările din interior	↙
10	Manipularea fizică, deteriorarea, furtul sau pierderea	---
11	Scurgerile de informații	↗
12	Furtul de identitate	↗
13	Criptojacking (minarea ilicită de criptomonede)	↗
14	Ransomware (programele de șantaj digital)	↙
15	Spionajul cibernetic	↙

Cele mai importante amenințări în 2019-2020		Tendințe evaluate	Schimbare în clasament
1	Programele malware	---	---
2	Atacurile online	---	↗
3	Phishing	↗	↗
4	Atacurile asupra aplicațiilor web	---	↙
5	Spamul	↙	↗
6	Blocarea serviciului	↙	↙
7	Furtul de identitate	↗	↗
8	Încălcarea securității datelor	---	---
9	Amenințările din interior	↗	---
10	Rețelele botnet	↙	↙
11	Manipularea fizică, deteriorarea, furtul sau pierderea	---	↙
12	Scurgerile de informații	↗	↙
13	Ransomware	↗	↗
14	Spionajul cibernetic	↙	↗
15	Criptojacking	↙	↙

Legendă: Tendințe: ↙ În declin, --- Stabil, ↗ În creștere **Clasament:** ↗ Urcă, --- Aceeași, ↙ Coboară

Prezentare generală

_ Ce s-a schimbat în peisaj

Anii 2019 și 2020 au adus schimbări semnificative în situația amenințărilor cibernetice descrisă în aceste rapoarte. Două fapte distincte au contribuit în mod semnificativ la aceste schimbări: forțele de transformare bruscă, unice din punct de vedere istoric, declanșate de **pandemia bolii cauzate de coronavirus 2019 (COVID-19)** și tendința continuă de creștere a **capacităților adverse avansate ale factorilor de amenințare**. În mod remarcabil, acestea din urmă au ajuns să amplifice impactul pandemiei COVID-19 în spațiul cibernetic.

Pandemia de COVID-19 a forțat adoptarea la scară largă a tehnologiei pentru a aborda o varietate de aspecte critice ale crizei, cum ar fi coordonarea serviciilor de sănătate, răspunsul internațional la răspândirea COVID-19, adoptarea regimurilor de telemuncă, învățământul la distanță, comunicarea interpersonală, controlul măsurilor de izolare, teleconferința și multe altele. Având în vedere această situație, liderii mediului de afaceri au evaluat riscurile generate de adoptarea bruscă a soluțiilor (tehnologice), care au apărut ca urmare a transformării forțate de pandemia de COVID-19[2]. Și **securitatea cibernetică s-a confruntat cu un paradox: ea a fost atât provocarea, cât și oportunitatea acestei transformări.** Schimbările impuse în peisajul tehnologiei informației (IT) au slăbit măsurile de securitate cibernetică existente, făcând din adaptarea lor rapidă o provocare. În același timp, **securitatea cibernetică este facilitatorul încrederii în cazurile de utilizare emergente pentru serviciile digitale și, prin urmare, are posibilitatea de a facilita transformarea.**

În timp ce lucrau de acasă, **specialiștii în securitate cibernetică au trebuit să adapteze modalitățile de apărare existente** la o nouă paradigmă a infrastructurii, încercând să reducă la minimum expunerea la o varietate de atacuri noi în care punctele de intrare sunt casa conectată la internet și alte dispozitive inteligente ale angajaților. În același timp și sub o mare presiune, aceștia au fost nevoiți să aplice soluții bazate pe componente care anterior erau mai puțin fiabile, cum ar fi accesul de la distanță prin internet public, servicii cloud, servicii de streaming video nesecurizate și dispozitive și aplicații mobile. Reacția necesară la pandemia de COVID-19 pentru a garanta siguranța și, în același timp, pentru a reduce impactul asupra întreprinderilor a împins organizațiile la limitele capacității lor de a răspunde la schimbări. De asemenea, numeroase moduri de operare s-au adaptat rapid la tiparele de lucru în schimbare, iar **profesioniștii din domeniul securității cibernetice s-au găsit în situația de a acționa la limitele capacităților lor**.

Într-o perioadă scurtă de timp, profesioniștii din domeniul securității IT au trebuit să răspundă rapid provocărilor introduse de formulele de lucru de acasă, cum ar fi circulația datelor întreprinderii ori de câte ori angajații își folosesc internetul de acasă pentru a accesa aplicații bazate pe cloud, software corporativ, videoconferință și partajare de fișiere.

Deoarece pandemia de COVID-19 nu este încă în totalitate sub control și din cauza incertitudinii răspândirii sale viitoare, se preconizează că aceasta va continua să reprezinte o provocare pentru profesioniștii din domeniul securității cibernetice. Mai mult, având în vedere timpul scurs înainte ca incidentele să fie observate și analizate, acestea își vor lăsa amprenta asupra situației amenințărilor cibernetice pentru mult timp de acum înainte. Pandemia de COVID-19 a arătat că actorii rău intenționați aveau un nivel de capacitate care le permitea să se adapteze rapid la această transformare. În 2019-2020, modurile de operare ale adversarilor s-au concentrat pe personalizarea vectorilor de atac. Metode avansate de furt de date de identificare, umplutura de date de identificare (*credential stuffing*), atacuri de phishing foarte țintite, atacuri avansate de inginerie socială, tehnici avansate de deghizare a programelor malware și penetrarea mai extinsă a platformelor mobile sunt principalele realizări ale adversarilor în perioada de raportare. În cazul în care criminalii cibernetici încep să combine aceste progrese cu inteligența artificială și învățarea automatizată, în viitor va crește numărul de atacuri reușite și campanii nedetectabile.

Prezentare generală

_ Rezumat

Lista de mai jos rezumă principalele tendințe observate în situația amenințărilor cibernetice în perioada de raportare. Acestea sunt revizuite, de asemenea, în detaliu pe parcursul diferitelor rapoarte care alcătuiesc situația amenințărilor din 2020.

01_ Suprafața atacului în securitatea cibernetică continuă să se extindă pe măsură ce intrăm într-o nouă fază a transformării digitale.

02_ Va exista o nouă normă socială și economică după pandemia de COVID-19 care va fi și mai dependentă de un spațiu cibernetic sigur și de încredere.

03_ Utilizarea platformelor de socializare în atacurile țintite este o tendință semnificativă și cuprinde diferite domenii și tipuri de amenințări.

04_ Atacurile țintite exact și persistente asupra datelor cu valoare ridicată (de exemplu, proprietatea intelectuală și secretele de stat) sunt planificate și executate meticulos de actori susținuți de stat.

05_ Atacurile distribuite masiv, cu durată scurtă și impact larg, sunt utilizate cu obiective multiple, cum ar fi furtul de date de identificare.

_ Rezumat

06_ **Motivația din spatele majorității atacurilor cibernetice este în continuare una financiară.**

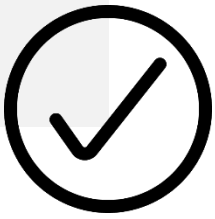
07_ **Ransomware-ul rămâne răspândit, cu consecințe costisitoare pentru multe organizații.**

08_ **Cu toate acestea, multe incidente de securitate cibernetică trec neobservate sau durează mult timp pentru a fi detectate.**

09_ **În contextul unei automatizări mai mari a securității, organizațiile vor investi mai mult în pregătire, folosind CTI drept principală capacitate.**

10_ **Numărul victimelor phishing-ului continuă să crească, întrucât acesta exploatează dimensiunea umană ca fiind veriga cea mai slabă.**

Cu toate schimbările observate în situația amenințărilor cibernetice și provocările create de pandemia de COVID-19, există încă un drum lung de parcurs până când spațiul cibernetic va deveni un mediu demn de încredere și sigur pentru toată lumea.



Prezentare generală

_ Sunt cetățenii UE mai conștienți de riscurile și provocările generate de spațiul cibernetic?

În 2019, Comisia Europeană a pregătit un sondaj Eurobarometru special[4] cu scopul de a înțelege gradul de sensibilizare a cetățenilor UE, experiențele și percepțiile lor cu privire la securitatea cibernetică.

EUROBAROMETRU

Rezultatele acestui sondaj arată că utilizarea internetului în Europa continuă să crească, în special prin intermediul telefoanelor inteligente, iar cetățenii sunt mai conștienți de potențialele pericole când intră online.

Conform concluziilor sondajului, îngrijorările cu privire la confidențialitatea și securitatea online au determinat deja mai mult de 9 din 10 utilizatori de internet să-și schimbe comportamentul online – cel mai adesea prin faptul că nu deschid e-mailuri de la persoane necunoscute, nu instalează programe antivirus, vizitează doar site-uri cunoscute și de încredere și folosesc doar propriile calculatoare.

Deși aceste rezultate sunt destul de încurajatoare, mulți utilizatori cad pradă în continuare fraudelor online și momelilor în atacurile de tip phishing prin e-mail. Aceasta relevă faptul că actorii rău intenționați folosesc atacuri sofisticate care sunt mai greu de detectat și de evitat. Prin urmare, strategiile de atenuare trebuie să fie actualizate în mod regulat pentru a lua în considerare cele mai recente informații disponibile (CTI) privind tehnicile de atac.

„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

La ce să vă așteptați

Este probabil ca actori susținuți de state-națiune

TENDINȚĂ	DESCRIERE	AMENINȚARE
→	**să continue** să utilizeze spațiul cibernetic pentru a lansa atacuri împotriva proceselor electorale ale țărilor străine, amenințând sistemele democratice și drepturile omului.[5]	**Atacuri împotriva drepturilor omului și a sistemelor democratice**
→	**să continue** să hărțuiască opozițiile și să-și monitorizeze cetățenii prin manipularea informațiilor de pe rețelele de socializare, atacurile fiind însoțite de campanii de spyware.	**Atacuri împotriva drepturilor omului și a sistemelor democratice**
↗	**să lanseze** campanii sofisticate de dezinformare[6] concepute pentru a influența percepțiile sau pentru a manipula opiniile în favoarea unei anumite agende politice sau a unor obiective de speculație financiară.	**Campanii de dezinformare**
↗	**să intensifice** cursa înarmării cibernetice[7] în încercarea de a dezvolta capacități cibernetice. Având în vedere că spațiul cibernetic este considerat un domeniu de război, statele-națiune sunt susceptibile să caute arme cibernetice prin intermediul agenților susținuți de acestea, în pregătirea unui conflict cibernetic.	**Cursa necontrolată a înarmării cibernetice**
↗	**să urmărească** obiective strategice precum: obținerea de secrete industriale prin spionaj, obținerea de influență asupra luării deciziilor politice, finanțarea regimului prin fraude financiare, efectuarea de operațiuni de informare cibernetice și, în cele din urmă, slăbirea sau demoralizarea adversarului prin activități perturbatoare sau distructive.	**Furtul de date**

Este probabil ca delincvenții cibernetici

TENDINȚĂ	DESCRIERE	AMENINȚARE
→	**să continue** să vizeze adolescenții și tinerii adulți cu atacuri de extorcare sexuală (șantaj prin webcam) care afectează psihologic și, în cele din urmă, fizic victimele.[8]	**Extorcarea sexuală (șantaj prin webcam)**
↗	**să crească** numărul de atacuri de hărțuire cibernetică în timpul pandemiei de COVID-19 și după aceasta, în contextul în care adolescenții utilizează platforme digitale chiar mai mult în scopuri personale sau educaționale.[9]	**Hărțuirea cibernetică**

Este probabil ca infractorii cibernetici

TENDINȚĂ	DESCRIERE	AMENINȚARE
↗	**să crească** nivelul de utilizare a instrumentelor bazate pe inteligență artificială pentru a crea falsuri extrem de credibile (format imagine, audio și video) – cunoscute în mod obișnuit sub denumirea de deep-fakes – pentru a frauda întreprinderi.	**Conținut audiovizual fals (deep fake)**
→	**să îmbunătățească** tactica care compromite procesele de afaceri pentru a obține un avantaj financiar.	**Compromiterea procesului de afaceri (Business process compromise – BPC)**
→	**să coboare** un nivel în organizație – sub nivelul executiv – pentru a compromite e-mailurile de afaceri.	**Compromiterea e-mailului de afaceri (Business e-mail compromise – BEC)**
→	**să crească** nivelul de utilizare a prestatorilor de servicii gestionate (*managed service providers* – MSPs) pentru a distribui malware.	**Programele malware**

Concluzii și recomandări

Concluzii/recomandări privind politicile

- În ultimele decenii, factorii de decizie politică și specialiștii în tehnologie au trăit în două lumi separate și au vorbit limbi diferite. Pentru a aborda provocările generate de digitalizare, aceștia ar trebui **să lucreze împreună** în mod ascendent și să dezvolte o abordare comună. Întrucât cea mai mare parte a tehnologiei actuale este conectată la spațiul cibernetic, contribuția experților în securitate cibernetică în multe dintre aceste discuții este de o importanță capitală.
- Odată cu inovația tehnologică în creștere și extinderea rapidă a spațiului cibernetic, politicile europene eficace și cuprinzătoare în materie de securitate cibernetică sunt de o importanță crucială. **Politicile mature în materie de securitate cibernetică** vor asigura capacitatea de securitate necesară la toate nivelurile societății: guverne, infrastructuri critice, întreprinderi, sectorul terțiar și persoane fizice. Capacitatea de securitate trebuie să fie eficace și flexibilă pentru a răspunde noilor provocări pe măsură ce acestea apar, pentru a face față schimbărilor permanente din spațiul cibernetic.
- Având în vedere numărul tot mai mare de părți interesate din UE și din statele membre implicate în activitățile CTI, **cooperarea și coordonarea** activităților CTI la nivelul UE este esențială. ENISA va promova cooperarea cu diverse părți interesate și va face o primă încercare de a identifica cerințele CTI ale diferitelor grupuri de părți interesate, în special în cadrul UE (și anume, Comisia, organismele UE, agențiile și statele membre).
- CTI ar trebui să fie considerat instrumentul principal pentru **pregătirea în materie de securitate cibernetică** și facilitarea abordărilor bazate pe risc. Integrarea CTI cu procesele de gestionare a securității va ajuta CTI să prolifereze răspândindu-se în domenii conexe și va crește agilitatea proceselor de obicei lungi precum certificarea și evaluarea riscurilor. Mai mult, CTI va fi văzut ca un facilitator al deciziilor de urgență necesare în gestionarea crizelor.
- Relevanța CTI pentru deciziile strategice și politice este larg acceptată și considerată esențială pentru a facilita **conectarea la informațiile geopolitice** și sistemele cibernetice. Aceasta va permite includerea CTI în procesele de luare a deciziilor la nivelul UE, dar va facilita, de asemenea, extinderea contextului său pentru a identifica amenințări hibride.

Concluzii/recomandări privind întreprinderile

- În cursul anului 2019, un număr din ce în ce mai mare de **laboratoare de testare și medii cibernetice de simulare în scopuri de antrenament (cyber ranges)**[10] au devenit disponibile la sediu și cu oferte cloud. Acestea sunt resurse importante pentru instruirea personalului, simularea atacurilor și testarea multiplelor strategii de apărare. Totul se desfășoară într-un mediu virtual multifuncțional.
- Deși au fost elaborate anumite criterii și cerințe CTI pentru diferite profiluri de utilizatori CTI, vor fi necesare **cerințe similare** pentru alte produse, servicii și instrumente CTI. Furnizorii CTI vor trebui să țină cont într-o măsură mai mare de cerințele utilizatorilor pentru a facilita adoptarea produselor și serviciilor CTI.
- Investițiile în unele concepte de bază CTI, în special **maturitatea CTI și ierarhiile amenințărilor**, sunt foarte utile pentru asimilarea CTI. Furnizorii vor trebui să își orienteze ofertele către diferite niveluri de maturitate CTI pentru a facilita utilizarea eficientă a CTI în cadrul organizațiilor de diferite dimensiuni și cu bugete diferite.
- Pe termen lung, se pare că **OpenCTI**[11] ar putea fi o soluție bună la fragmentarea ofertelor CTI, având în vedere capacitatea sa inerentă de a integra diferite tipuri de surse CTI într-un singur mediu de instrumente. Furnizorii CTI vor trebui să ofere „punțile” necesare de la produsele lor pentru a permite integrarea acestora cu OpenCTI. 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.

Concluzii și recomandări

Concluzii și recomandări în domeniul educației și cercetării

- UE trebuie să continue să investească în **cercetarea și dezvoltarea în domeniul securității cibernetice**, cu accent pe inițiativele de cercetare pe termen lung și cu risc mare. Cercetarea și inovarea pe termen lung reprezintă un exercițiu costisitor, care nu este la îndemâna majorității organizațiilor din sectorul privat.
- Extinderea cunoștințelor și expertizei în domeniul securității cibernetice este crucială pentru a îmbunătăți pregătirea și reziliența. UE trebuie să continue **dezvoltarea capacităților** prin investiții în programe de formare în domeniul securității cibernetice, certificare profesională, exerciții și campanii de sensibilizare.
- Cercetarea în domeniul securității cibernetice trebuie să includă expertiză din discipline sociale, comportamentale și economice. **Cercetarea multidisciplinară** în domeniul securității cibernetice trebuie promovată și stimulată în întreaga UE.
- Rezultatele proiectelor de cercetare în domeniul securității cibernetice și, în special, în ceea ce privește CTI trebuie să fie evaluate și puse în corespondență cu un context mai larg pentru a identifica **suprapunerile și lacunele** și pentru a le face comparabile cu produsele, serviciile și practicile comerciale existente. Aceasta va contribui la diseminarea rezultatelor respective către comunitatea de utilizatori.
- Trebuie dezvoltate noi abordări pentru asimilarea cunoștințelor CTI de către domenii care pot beneficia de pe urma acestora. **Exemple de astfel de domenii sunt mediile cibernetice de simulare în scopuri de antrenament (cyber ranges), amenințările hibride și evaluările geopolitice.** Sinergiile realizate pot spori cazurile de utilizare și calitatea conținutului într-o manieră multidirecțională.
- Trebuie să se analizeze în continuare utilizarea **inteligenței artificiale (IA)** și a învățării automatizate (*machine learning* - ML) în cadrul CTI. Aceasta va reduce numărul de etape manuale în analiza CTI și va crește valoarea funcțiilor de învățare automatizată în cadrul activităților CTI.
- Trebuie să se promoveze furnizarea și utilizarea materialului CTI cu sursă deschisă. Aceasta va facilita **transferul de cunoștințe**, dar va reduce, de asemenea, pragul pentru competențele CTI necesare.

„Sofisticarea 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

Referințe

1. „Regulamentul UE privind securitatea cibernetică". Aprilie, 2019. Parlamentul European și Consiliul European https://eur-lex.europa.eu/eli/reg/2019/881/oj

2. "COVID-19 Risks Outlook: A Preliminary Mapping and its Implications" (Perspectiva riscurilor COVID-19: o cartografiere preliminară și implicațiile sale) 19 mai 2020. WEF. https://www.weforum.org/reports/covid-19-risks-outlook-a-preliminary-mapping-and-its-implications

3. „Comunicare comună către Parlamentul European, Consiliul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor: Combaterea dezinformării în legătură cu COVID-19 – Asigurarea unei informări corecte". iunie 2020 Comisia Europeană. https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A52020JC0008

4 „Special Eurobarometer 499: Europeans' attitudes towards cyber security" (Eurobarometru special 499: atitudinile europenilor față de securitatea cibernetică) 29 ianuarie 2020. https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

5. „EUvsDosinfo" https://euvsdisinfo.eu/european-elections-2019/

6. „Manipulating Social Media to Undermine Democracy" (Manipularea mijloacelor de comunicare socială pentru a submina democrația) 2017. Freedom House. https://freedomhouse.org/report/freedom-net/2017/manipulating-social-media-undermine-democracy

7. „Conceptualising Cyber Arms Races" 2016 (Conceptualizarea curselor înarmărilor cibernetice, 2016) NATO CCD COE. https://ccdcoe.org/uploads/2018/10/Art-10-Conceptualising-Cyber-Arms-Races.pdf

8. „How online 'sextortion' drove one young man to suicide" (Modul în care extorcarea sexuală online l-a determinat pe un tânăr să se sinucidă) 8 februarie 2018. Today. https://www.today.com/parents/how-online-sextortion-drove-one-young-man-suicide-t122735

9. „Cyberbullying may increase during COVID-19 pandemic, expert says" (Hărțuirea online se poate intesifica în timpul pandemiei de COVID-19, afirmă un expert) 30 martie 2020. Healio. https://www.healio.com/news/pediatrics/20200330/cyberbullying-may-increase-during-covid19-pandemic-expert-says

10. Conceptul de mediu cibernetic de simulare în scopuri de antrenament (cyber range) a fost inițial definit 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.

11. Open CTI. https://www.opencti.io/en/

„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

CITIȚI RAPORTUL

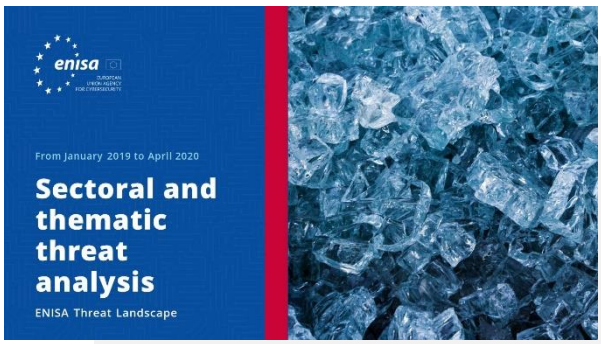
Raportul ENISA privind situația amenințărilor
Lista celor mai importante 15 amenințări

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 **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.

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 acest raport, vă rugăm să utilizați adresa press@enisa.europa.eu.

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 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.

Aviz privind drepturile de autor

© Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), 2020 Reproducerea este autorizată cu condiția menționării sursei.

Drepturile de autor pentru imaginea de pe copertă: © Wedia. Pentru orice utilizare sau reproducere a fotografiilor sau a altor materiale pentru care ENISA nu deține dreptul de autor trebuie solicitată direct permisiunea deținătorilor drepturilor de autor.

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

Toate drepturile rezervate. Copyright ENISA 2020.

https://www.enisa.europa.eu