RO

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

Ianuarie 2019 – aprilie 2020

Atacurile asupra aplicațiilor web

Raportul ENISA privind situația amenințărilor

Prezentare generală

Aplicațiile și tehnologiile web au devenit o parte esențială a internetului prin adoptarea de diferite utilizări și funcționalități. Creșterea complexității aplicațiilor web și a serviciilor lor generalizate creează dificultăți în a le proteja împotriva amenințărilor, cu diverse motivații, de la daune financiare sau reputaționale la furtul de informații critice sau cu caracter personal.[1] Serviciile și aplicațiile web depind în principal de bazele de date pentru a stoca sau a furniza informațiile solicitate. Tipul de atacuri SQL Injection (SQLi) este un exemplu bine cunoscut și constituie cele mai frecvente amenințări împotriva acestor servicii. Atacurile de scriptare inter-site-uri (cross-site scripting – XSS) constituie un alt exemplu. În acest tip de atac, actorul rău intenționat folosește abuziv punctele slabe din formulare sau alte funcționalități de intrare ale aplicațiilor web, ceea ce duce la alte caracteristici rău intenționate, cum ar fi redirecționarea către un site web rău intenționat.[2]

În timp ce organizațiile își sporesc competența și dezvoltă o automatizare mai coerentă în ciclul de viață al aplicațiilor lor web, acestea solicită ca securitatea să fie cea mai importantă parte a ofertei și prioritizării acestora. Această introducere a mediilor complexe conduce la adoptarea de noi servicii, cum ar fi interfețele de programare a aplicațiilor (API). API-urile, care creează noi provocări pentru securitatea aplicațiilor web, determină organizațiile implicate să ia în considerare mai multe măsuri de prevenire și detectare. De exemplu, aproximativ 80 % din organizațiile care adoptă API-uri au implementat controale asupra traficului lor de intrare.[3] În această secțiune analizăm situația amenințărilor la adresa aplicațiilor web în cursul anului 2019.

_Tendințe

*20 %*_ din companii și organizații au raportat atacuri DDoS asupra serviciilor lor de aplicații în fiecare zi[5]

Depășirea tamponului (buffer overflow) a fost tehnica utilizată cel mai frecvent (24 %). Inundația HTTP (23 %), reducerea resurselor (23 %), inundația HTTPS (21 %) și Low Slow 21 % au fost alte tehnici utilizate în mod frecvent.

*63 %*_ din respondenții la sondajul CyberEdge utilizează un firewall pentru aplicații web (WAF)

27,5 % au planuri de implementare a acestei tehnologii, iar 9,5 % nu au astfel de planuri.[15]

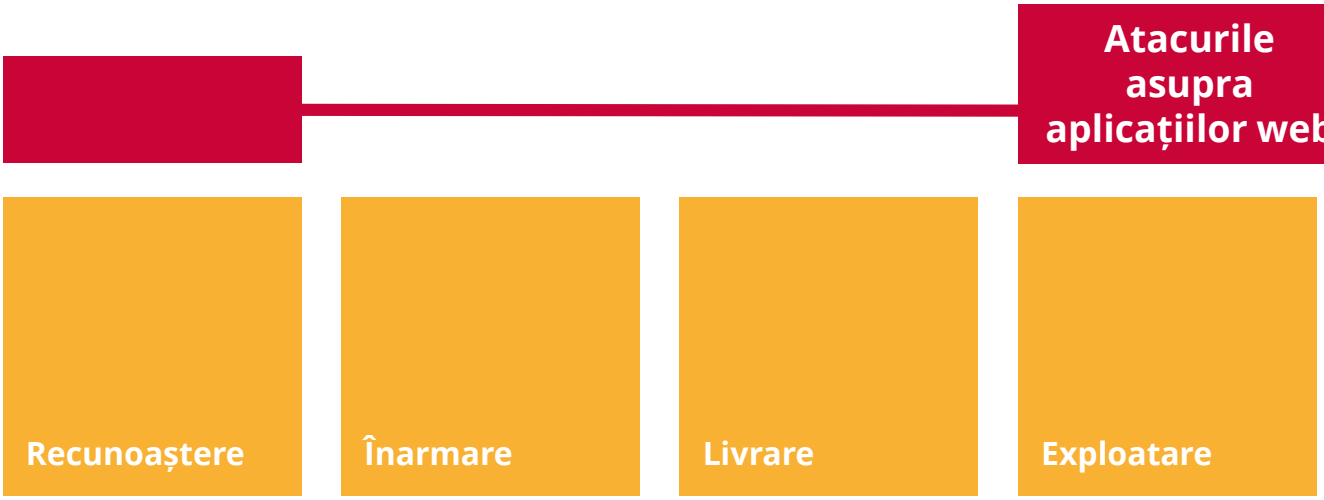
*52 %*_ creștere a numărului de atacuri asupra aplicațiilor web în 2019 comparativ cu 2018

Potrivit unui cercetător în domeniul securității, numărul atacurilor asupra aplicațiilor web a fost aproape constant comparativ cu 2018 și a crescut brusc mai târziu în cursul anului.[4]

*84 %*_ din vulnerabilitățile observate în aplicațiile web erau configurări greșite ale securității

Aceasta a fost urmată de scriptare inter-site-uri (53 %) și, interesant, de autentificare întreruptă (broken authentication) (45 %).[9]

Kill chain



Etapă din fluxul de activitate de atac

Amploarea scopului

Instalare

Comandă și control

Acțiuni privind obiectivele

Cadrul Cyber Kill Chain® a fost dezvoltat de Lockheed Martin, fiind adaptat după un concept militar legat de structura unui atac. Pentru a studia un anumit vector de atac, utilizați această diagramă kill-chain pentru a trasa fiecare etapă a procesului și a face referire la instrumentele, tehnicile și procedurile utilizate de atacator.

MAI MULTE INFORMAȚII

Descriere

_Colaborare îmbunătățită între securitatea aplicațiilor și dezvoltarea de aplicații

Conform sondajului realizat de un cercetător în domeniul securității[5], unul dintre factorii care contribuie la o astfel de securitate ineficace ar putea fi luarea deciziilor cu privire la proprietatea instrumentelor de securitate. Sondajul a prezentat punctele de vedere ale celor mai importanți influențatori din acest domeniu, și anume conducătorii și proprietarii de afaceri IT și nu responsabilul șef cu securitatea informațiilor (CISO).

_Importanța tot mai mare a interfețelor de programare a aplicațiilor (API)

API-urile nu sunt noi în arhitectura aplicațiilor web, iar utilizarea lor acceptată pe scară largă reintroduce riscurile existente și probabilitatea de exploatare a acestora ca urmare a lărgirii perspectivei amenințărilor. În consecință, Open Web Application Security Project (OWASP) a publicat o listă a primelor 10 măsuri de securitate API, 6 oferind o modalitate prioritară de securizare a acestei capacități în arhitectura aplicațiilor web. Un exemplu de astfel de amenințare este reprezentat de atacurile PHP API: potrivit unui alt cercetător în domeniul securității, 87 % din scanarea traficului API căuta API-uri PHP disponibile.[7]

_Eșecuri de autorizare și autentificare

Acestea reprezintă, de regulă, principala cauză pentru care actorii rău intenționați au acces la informații critice (și anume, încălcarea securității datelor la Fast Retailing).[8] Potrivit unui cercetător în domeniul securității, încălcările securității datelor critice reprezintă a doua cea mai presantă amenințare la adresa securității aplicațiilor web.[9]

Tendință de creștere cu injecție SQL (SQLi)

O cercetare recentă în domeniul securității a identificat că două treimi din atacurile asupra aplicațiilor web includ atacuri SQLi. În timp ce alți vectori utilizați în atacurile asupra aplicațiilor web fie au rămas stabili, fie sunt în creștere, atacurile SQLi au continuat să crească brusc și s-au intensificat, în special în timpul sărbătorilor din 2019.[11] Rezultatele acestei cercetări au arătat, de asemenea, că industria financiară se confruntă cu mai multe atacuri de includere a fișierelor locale (LFi) comparativ cu alte sectoare.[12]

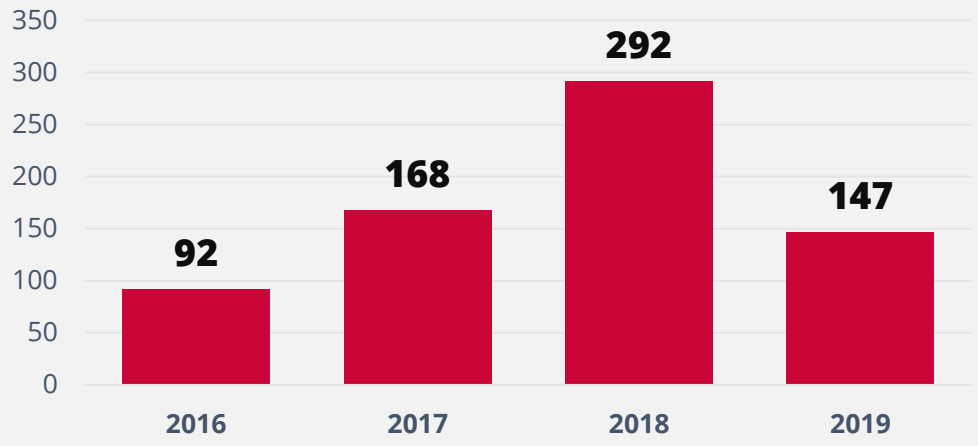


Figura 1: Reducerea numărului de fișiere curățate per site compromis. Sursa: Sucuri[10]

Vectori de atac

_Vectori utilizați în atacurile asupra aplicațiilor web

Există percepția generală că atacurile asupra aplicațiilor web sunt destul de diverse. Cu toate acestea, datele din cercetările în domeniul securității sugerează că majoritatea atacurilor asupra aplicațiilor web sunt limitate la SQLi sau LFi.[11,13,14] Un alt raport sugerează că SQLi, traversarea registrului (directory traversal), XSS, autentificarea întreruptă și gestionarea sesiunii se află printre cei mai importanți vectori de atac utilizați în acest tip de atacuri.[4]

SONICWALL a raportat, de asemenea, o tendință similară pentru cele mai importante atacuri asupra aplicațiilor web pentru 2019. SQLi, directory traversal, XSS, autentificarea întreruptă și gestionarea sesiunii se aflau pe primele locuri de pe listă.[4]

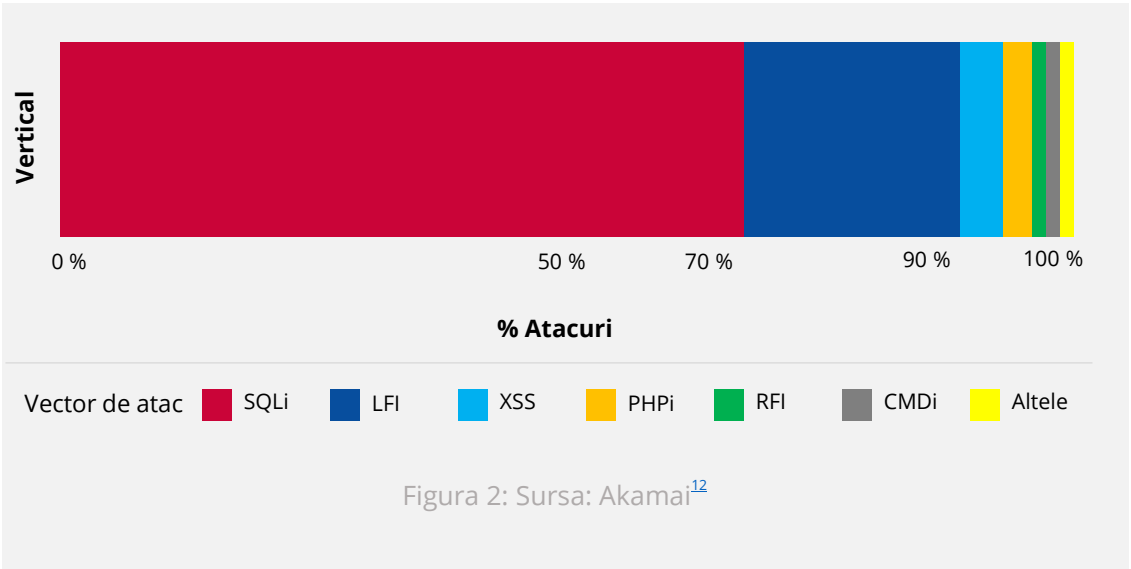


Figura 2: Sursa: Akamai[12]

Atacurile asupra aplicațiilor web

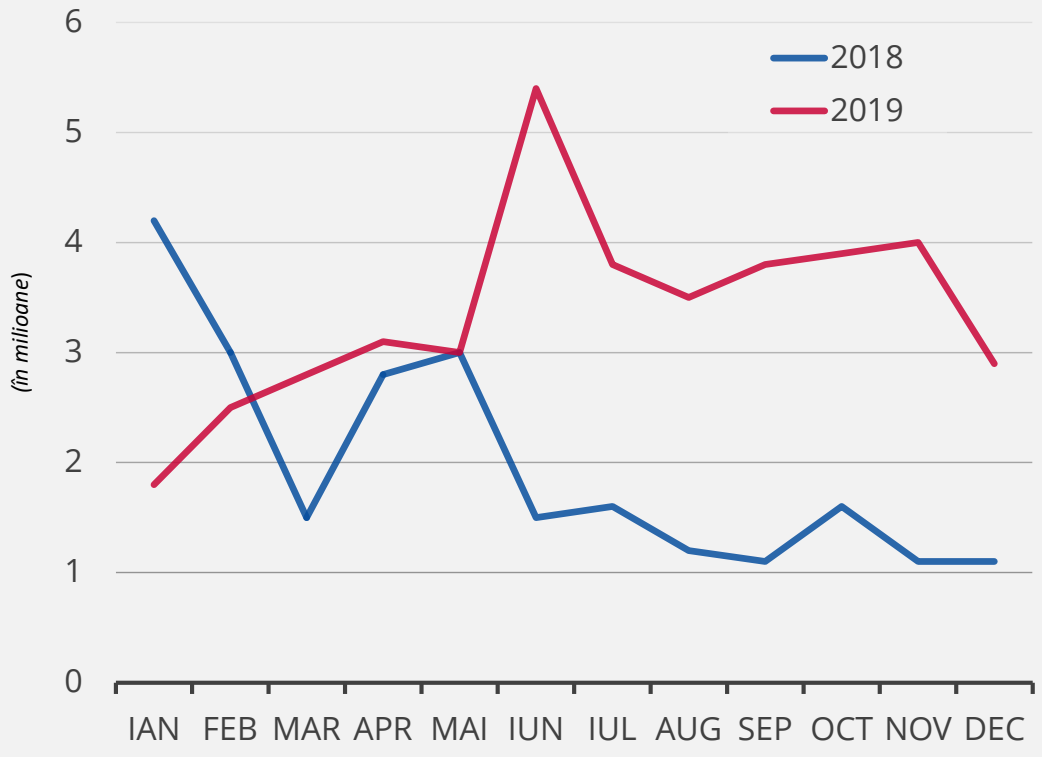


Figura 3 - Sursa: Sonicwall[4]

Măsuri de atenuare

Acțiuni propuse

- Utilizarea de tehnici de validare și izolare a intrărilor pentru atacuri de tip injecție (și anume, declarații parametrizate, evitarea intrărilor utilizatorului, validarea intrărilor etc.).[16]
- Aplicarea de firewall-uri pentru aplicații web pentru măsuri preventive și defensive (17) (cunoscute și sub denumirea de patch-uri virtuale).[18]
- Pentru API-urile aplicațiilor web:[19]
    - aplicarea și menținerea unui inventar de API-uri și validarea acestora împotriva scanărilor perimetrice și a descoperirii interne prin echipe de dezvoltare și operaționale;
    - criptarea comunicării și conexiunii API;
    - furnizarea mecanismelor de autentificare și a nivelurilor de autorizare corecte.
- Incorporarea proceselor de securitate a aplicației în ciclul de viață al dezvoltării și întreținerii aplicațiilor.[20]
- Limitarea accesului la traficul de intrare numai pentru serviciile necesare.[20]
- Implementarea de capacități de gestionare a traficului și a lățimii de bandă.
- Aplicarea întăririi serverului de aplicații web și menținerea unei bune gestionări a patch-urilor și a proceselor de testare.[21]
- Efectuare de evaluări ale vulnerabilității și riscurilor înainte și în timpul dezvoltării aplicației web.
- Efectuare de teste regulate de penetrare în timpul aplicării și după aplicare.

Aplicații web în funcție de gravitatea maximă a vulnerabilităților constatate

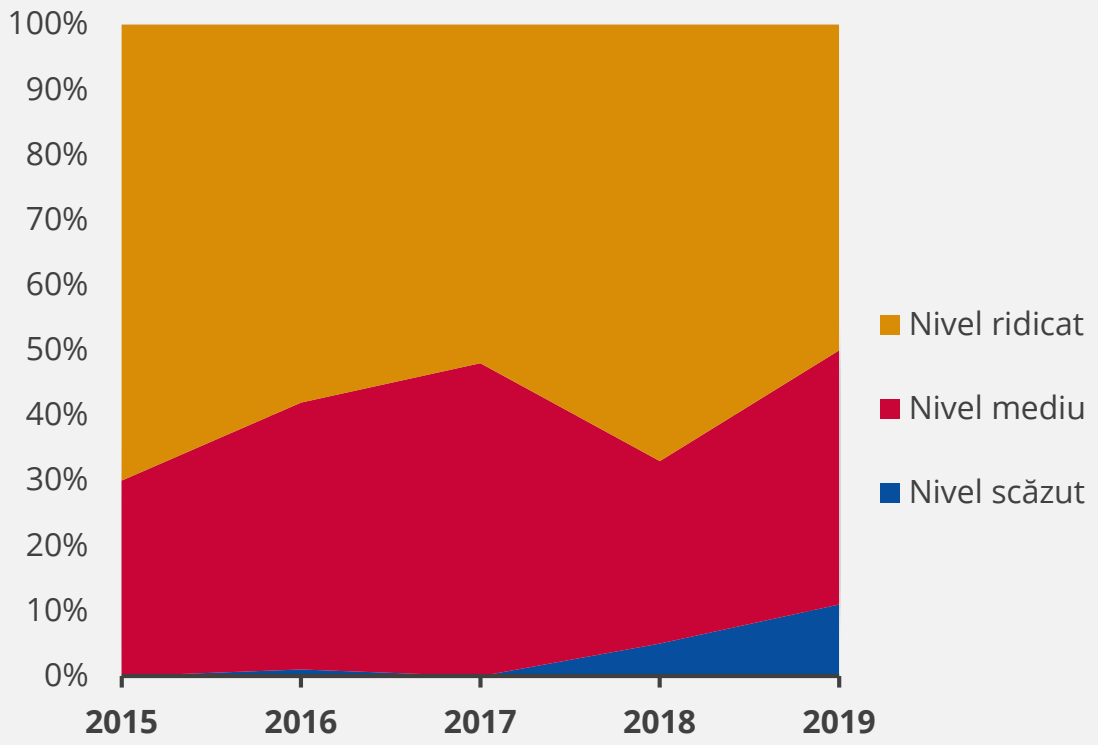


Figura 4 - Sursa: Positive Technologies[9]

Referințe

1. „The Future Is the Web! How to Keep It Secure?" (Viitorul este web! Cum să-l păstrăm în siguranță?) Octombrie 2019. Acunetix. https://www.acunetix.com/whitepaper-the-future-is-the-web/

2. „What Is a Web Application Attack and how to Defend Against It" (Ce este un atac asupra aplicațiilor web și cum să vă apărați împotriva acestuia). 2019. Acunetix.. https://www.acunetix.com/websitesecurity/web-application-attack/

3. „2020 State of Application Services Report" (Raportul 2020 privind situația serviciilor de aplicații), F5 Networks, 2020. https://www.f5.com/state-of-application-services-report

4. „Sonicwall Cyber Threat Report" (Raportul Sonicwall privind amenințările cibernetice). 2020. Sonicwall. https://www.sonicwall.com/resources/2020-cyber-threat-report-pdf/

5. „The State of Web Application Security, Protecting Application in the Microservice Era" (Situația securității aplicațiilor web, protejarea aplicației în era microserviciului). 2019. Radware. https://www.radware.com/resources/was-report-2019/

6. „API Security Top 10 2019" (Top 10 securitate API în 2019). OWASP. https://owasp.org/www-project-api-security/

7. Raymond Pompon, Sander Vinberg. „Application Protection Report 2019, Episode 5: API Breaches and the Visibility Problem" (Raport privind protecția aplicațiilor 2019, episodul 5: încălcări ale securității API și problema vizibilității). 13 august 2019. F5 Labs https://www.f5.com/labs/articles/threat-intelligence/application-protection-report-2019-episode-5-api-breaches-and-the-visibility-problem

8. „Unauthorized Logins on Fast Retailing Online Store Websites due to List Type Account Hacking and Request to Change Password" (Conectări neautorizate pe site-urile magazinelor online Fast Retailing din cauza piraterii List Type a contului și a cererii de modificare a parolei) 13 mai 2019. Fast Retailing. https://www.fastretailing.com/eng/group/news/1905132000.html

9. „Web Applications vulnerabilities and threats: statistics for 2019" (Vulnerabilități și amenințări la adresa aplicațiilor web: statistici pentru 2019) 13 februarie 2020. Positive Technologies. https://www.ptsecurity.com/ww-en/analytics/web-vulnerabilities-2020/#id9

10. Esrtevao Avillez. „2019 Website Threat Research Report" (Raport de cercetare a amenințărilor la adresa site-urilor internet 2019). 2019. Sucuri. https://sucuri.net/wp-content/uploads/2020/01/20-sucuri-2019-hacked-report-1.pdf

11. „State of the Internet / Security | Web Attacks and Gaming Abuse (Volume 5, Issue 3)" [Starea securității internetului | Atacuri pe internet și abuzul de jocuri (volumul 5, numărul 3)]. 2017-2019. Akamai. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-web-attacks-and-gaming-abuse-executive-summary-2019.pdf

12. „State of the Internet Security | Financial Services – Hostile Takeover Attempts (Volume 6, Issue 1)" [Starea securității internetului | Servicii financiare – încercări de preluare ostilă (volumul 6, numărul 1)]. 2020. Akamai. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-financial-services-hostile-takeover-attempts-report-2020.pdf

13. „Q4 2016 State of The Internet Security Report" (T4 2016 – Raportul privind starea securității internetului), 2016. Akamai. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2016-state-of-the-internet-security-report.pdf

14. "Q4 2017 State of the Internet Security Report" (T4 2017 – Raportul privind starea securității internetului), 2017. Akamai. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2017-state-of-the-internet-security-report.pdf

15. „2019 Cyberthreat Defense Report" (Raportul privind apărarea împotriva amenințărilor cibernetice 2019). 2019. CyberEdge Group. https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf

16. „AppSec Advisor: Injection Attacks" (Consilier AppSec: atacuri prin injecție) Octombrie 2019. CIS Center for Internet Security. https://www.cisecurity.org/newsletter/injection-attacks/

17. „Cybersecurity threatscape: Q3 2019" (Peisajul amenințărilor la adresa securității cibernetice: T3 2019). 2 decembrie 2019. Positive Technologies. https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2019-q3/#id5

18. „Virtual Patching Best Practices" (Cele mai bune practici de patch-uri virtuale). OWASP. https://owasp.org/www-community/Virtual_Patching_Best_Practices

19. Raymond Pompon, Sander Vinberg. „Application Protection Report 2019, Episode 5: API Breaches and the Visibility Problem" (Raport privind protecția aplicațiilor 2019, episodul 5: încălcări ale securității API și problema vizibilității). 13 august 2019. F5 Labs. https://www.f5.com/labs/articles/threat-intelligence/application-protection-report-2019-episode-5-api-breaches-and-the-visibility-problem

20. „2020 Cyber Threats, Business Email Compromise" (Amenințări cibernetice 2020, compromiterea e-mailului de afaceri). 22 octombrie 2019. https://www.uscloud.com/blog/top-cyber-threats-in-2020/

21. Sara Boddy, Remi Cohen. „Regional Threat Perspectives, Fall 2019: Asia" (Perspective asupra amenințărilor regionale, toamna 2019: Asia), 2019. F5 Labs. https://www.f5.com/labs/articles/threat-intelligence/regional-threat-perspectives--fall-2019--asia

„Creșterea complexității aplicațiilor web și a serviciilor lor generalizate creează dificultăți în a le proteja împotriva amenințărilor, cu diverse motivații, de la daune financiare sau reputaționale la furtul de informații critice sau cu caracter personal.”

în ETL 2020

Documente conexe

CITIȚI RAPORTUL

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

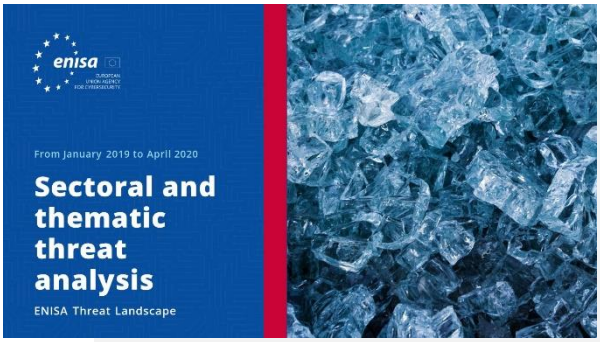
Raportul ENISA privind situația amenințărilor
Lista celor mai importante 15 amenințări

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

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.

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 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 rezervați câteva momente pentru a completa chestionarul. 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