enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

PL

Od stycznia 2019 r. do kwietnia 2020 r.

Ataki oparte na aplikacjach sieciowych

Krajobraz zagrożeń wg Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)

Informacje ogólne

Aplikacje i technologie internetowe stały się podstawową częścią internetu, przyjmując różne zastosowania i funkcje. Wzrost złożoności aplikacji internetowych i ich szerokie zastosowanie stwarza wyzwania związane z zabezpieczeniem ich przed zagrożeniami o różnych motywacjach, od szkód finansowych lub utraty reputacji po kradzież najważniejszych informacji lub danych osobowych[1]. Usługi i aplikacje internetowe opierają się głównie na bazach danych służących do przechowywania lub dostarczania wymaganych informacji. Dobrze znanym i najczęstszym zagrożeniem dla takich usług są ataki typu SQL Injection (SQLi). Innym przykładem są ataki typu cross-site scripting (XSS). Do tego typu ataku sprawca szkodliwych działań wykorzystuje słabe punkty formularzy lub innych funkcji wejściowych aplikacji internetowych, co umożliwia szkodliwe działania, takie jak przekierowanie do złośliwej witryny[2].

Choć organizacje nabierają wprawy w rozwijaniu automatyzacji cyklu życia aplikacji internetowych, najważniejszą kwestią i priorytetem pozostaje bezpieczeństwo. Wprowadzanie złożonych środowisk powoduje przyjęcie nowych komponentów, takich jak interfejsy programowania aplikacji (API). Stwarzają one nowe wyzwania w zakresie bezpieczeństwa aplikacji internetowych, co wymaga od zaangażowanych organizacji uwzględnienia dodatkowych środków zapobiegania i wykrywania. Na przykład około 80% organizacji, które korzystają z interfejsów API, wdrożyło mechanizmy kontroli ruchu przychodzącego[3]. W tej części dokonamy przeglądu zagrożeń związanych z aplikacjami internetowymi w 2019 roku.

_Trendy

20%_ firm i organizacji codziennie zgłaszało ataki DDoS na swoje usługi aplikacji[5]

Najczęściej stosowaną techniką było przepełnienie buforu (24%). Inne powszechnie stosowane techniki to HTTP flood (23%), redukcja zasobów (23%), HTTPS flood (21%) oraz Low Slow (21%).

63%_ respondentów ankiety CyberEdge korzysta z zapory aplikacji internetowych (WAF)

27,5% planuje wdrożyć tę technologię, a 9,5% nie ma takich planów[15].

52%_ – wzrost liczby ataków opartych na aplikacjach sieciowych w 2019 r. w porównaniu z 2018 r.

Według analityka bezpieczeństwa liczba ataków opartych na aplikacjach sieciowych była prawie równa tej z 2018 r. i gwałtownie wzrosła w dalszej części roku[4].

84%_ zaobserwowanych słabych punktów aplikacji internetowych to błędy konfiguracji zabezpieczeń

Następny był cross-site scripting (53%) i, co ciekawe, wadliwe uwierzytelnianie (45%).[9]

Kill chain

Proces etapów ataku

Zakres działania

Instalacja

Dowodzenie i kontrola

Działania dotyczące celów

Rozwiązanie Cyber Kill Chain® zostało opracowane przez Lockheed Martin na podstawie wojskowej koncepcji związanej ze strukturą ataku. Aby zbadać określony wektor ataku, należy użyć poniższego schematu Cyber Kill Chain w celu stworzenia mapy każdego etapu procesu i określić narzędzia, techniki i procedury, z jakich skorzystał atakujący.

WIĘCEJ INFORMACJI

Opis

_Lepsza współpraca między odpowiedzialnymi za bezpieczeństwo aplikacji a jej twórcami

Według ankiety przeprowadzonej przez analityka bezpieczeństwa[5], jednym z czynników przyczyniających się do deficytu bezpieczeństwa może być decydowanie o własności narzędzi bezpieczeństwa. W badaniu przedstawiono poglądy najbardziej wpływowych osób w tej dziedzinie, wymieniając liderów IT i właścicieli firm, a nie dyrektora ds. bezpieczeństwa informacji (CISO).

_Rosnące znaczenie interfejsów programowania aplikacji (API)

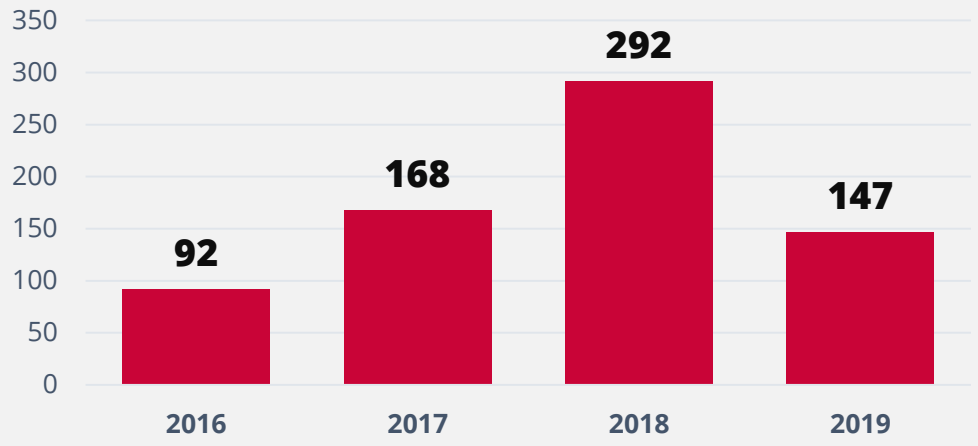
Interfejsy API nie są nowością w architekturze aplikacji internetowych, a ich powszechnie akceptowane użycie przywraca istniejące zagrożenia i prawdopodobieństwo wykorzystania w efekcie poszerzenia krajobrazu zagrożeń. W związku z tym OWASP (Open Web Application Security Project) opublikował listę 10 najważniejszych środków bezpieczeństwa API (6), zapewniając uszeregowany według priorytetów sposób zabezpieczenia takiej możliwości w architekturze aplikacji internetowych. Jednym z przykładów takiego zagrożenia są ataki PHP API: według innego analityka bezpieczeństwa 87% skanowania ruchu API polegało na wyszukiwaniu dostępnych API PHP[7].

_Niepowodzenia autoryzacji i uwierzytelniania

Są to zwykle główne przyczyny uzyskiwania dostępu do krytycznych informacji przez sprawców szkodliwych działań (np. włamania do sklepów internetowych[8]). Według analityka bezpieczeństwa drugim pod względem istotności zagrożeniem dla bezpieczeństwa aplikacji internetowych są naruszenia bezpieczeństwa krytycznych danych[9].

Wzrostowy trend SQLi (SQL injection)

Przeprowadzone niedawno badanie bezpieczeństwa wykazało, że dwie trzecie ataków opartych na aplikacjach sieciowych obejmują ataki SQLi. Podczas gdy inne wektory ataków opartych na aplikacjach sieciowych pozostały stabilne lub rosną, ataki SQLi wciąż gwałtownie rosły, a szczególnie nasiliły się w okresie świątecznym 2019 roku[11]. Wyniki tego badania wykazały również, że w porównaniu z innymi sektorami branża finansowa jest narażona na więcej ataków LFi (Local File inclusion)[12].



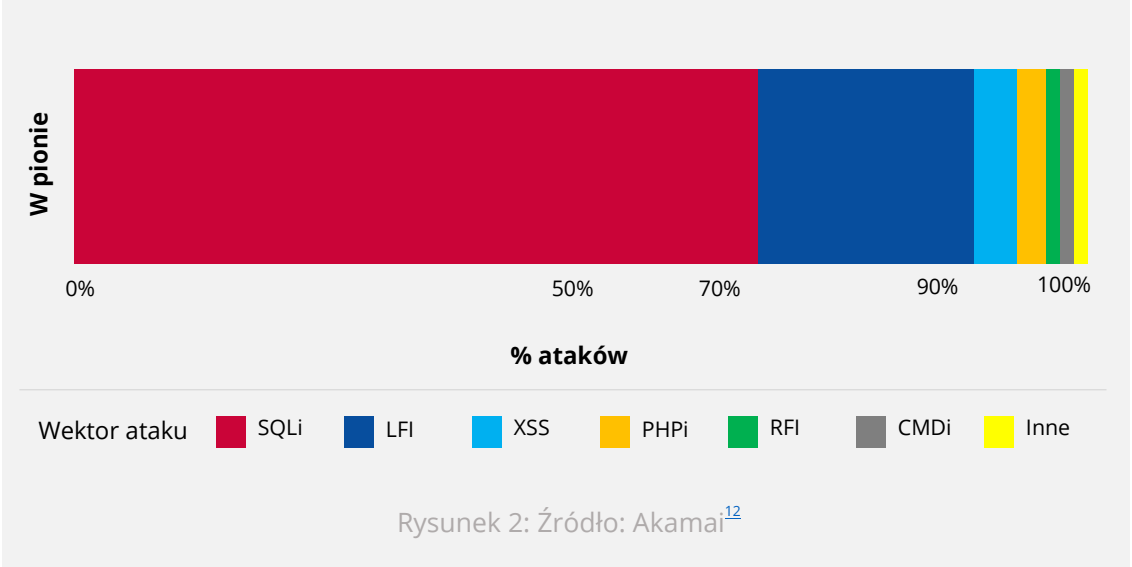
Rysunek 1: Zmniejszenie liczby czyszczonych plików na zaatakowaną witrynę. Źródło: Sucuri[10]

Wektory ataku

Wektory ataków opartych na aplikacjach sieciowych

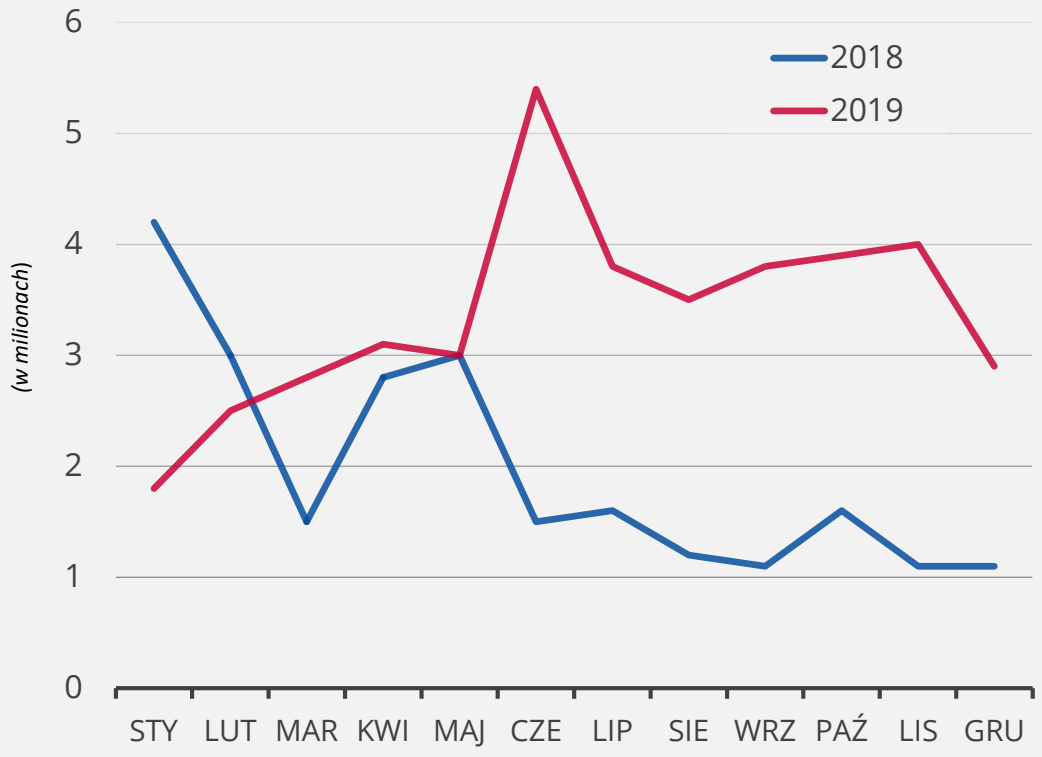
Istnieje ogólne przekonanie, że ataki oparte na aplikacjach sieciowych są dość zróżnicowane. Jednak dane z badań bezpieczeństwa wskazują, że większość ataków opartych na aplikacjach sieciowych ogranicza się do ataków typu SQLi lub LFi[11,13,14]. Inny raport sugeruje, że w czołówce wektorów wykorzystywanych w tego typu atakach znajdują się SQLi, Directory Traversal, XSS, wadliwe uwierzytelnianie i zarządzanie sesjami[4].

Na podobny trend w przypadku najważniejszych ataków opartych na aplikacjach sieciowych w 2019 r. wskazuje również SONICWALL. Na szczycie listy znalazły się ataki SQLi, Directory Traversal, XSS, wadliwe uwierzytelnianie i zarządzanie sesjami.[4]



Rysunek 2: Źródło: Akamai[12]

Ataki oparte na aplikacjach sieciowych



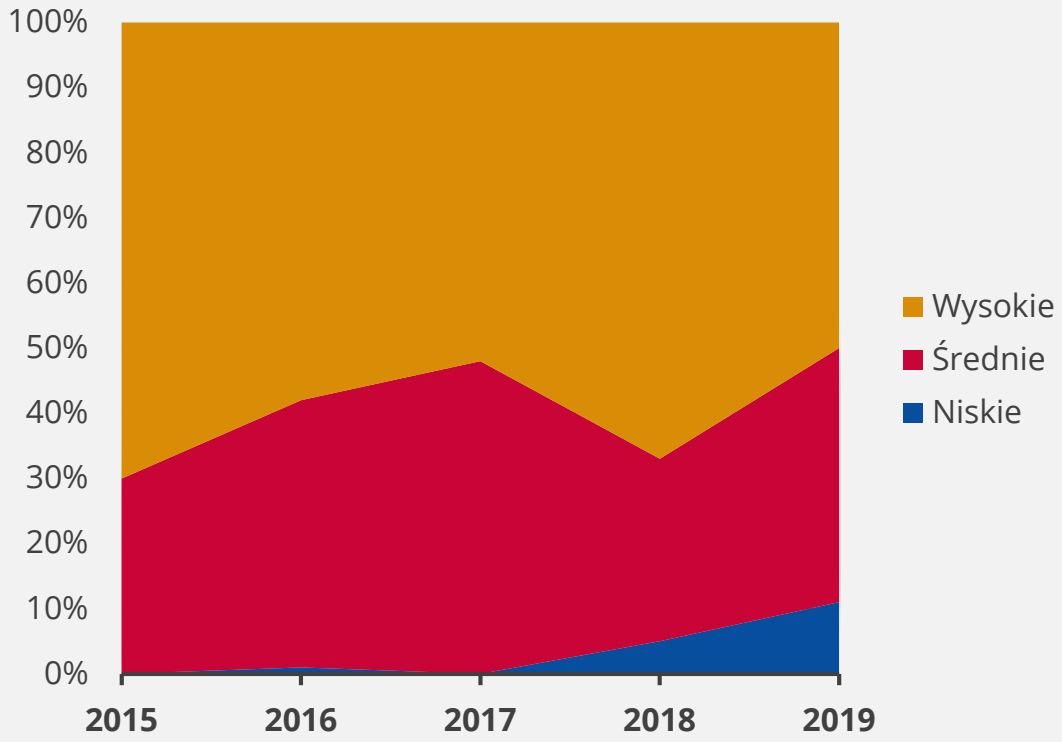
Rysunek 3 – źródło: Sonicwall[4]

Ograniczenie ryzyka

Proponowane działania

- Używanie technik weryfikacji i izolacji danych wejściowych w przypadku ataków typu iniekcyjnego (tj. sparametryzowanych instrukcji, wprowadzania sekwencji escape przez użytkownika, weryfikacji danych wejściowych itp.)[16].
- Wdrożenie zapór sieciowych aplikacji internetowych w celu zapewnienia środków zapobiegawczych i obronnych17 (tzw. virtual patching)[18].
- W przypadku interfejsów API aplikacji internetowych[19]:
  - Wdrożenie i utrzymywanie wykazu interfejsów API oraz zapewnienie ich weryfikowania pod kątem skanowania obwodu i wewnętrznego wykrywania przez zespoły programistyczne i operacyjne
  - Szyfrowanie komunikacji i połączeń API
  - Zapewnienie odpowiednich mechanizmów uwierzytelniania i poziomów autoryzacji
- Włączenie procesów bezpieczeństwa aplikacji do cyklu rozwoju i utrzymania aplikacji[20].
- Ograniczenie dostępu do ruchu przychodzącego tylko dla wymaganych usług[20].
- Wdrożenie funkcji zarządzania ruchem i przepustowością.
- Egzekwowanie wzmocnienia serwera aplikacji internetowych i zapewnienie prawidłowego zarządzania poprawkami oraz procesów testowania[21].
- Przeprowadzanie oceny słabych punktów i ryzyka przed tworzeniem i podczas tworzenia aplikacji internetowych.
- Przeprowadzanie regularnych testów penetracyjnych podczas wdrażania i po wdrożeniu.

Aplikacje internetowe według maksymalnego zagrożenia ze strony wykrytych słabych punktów



Rysunek 4 – źródło: Positive Technologies[9]

Bibliografia

1. „The Future Is the Web! How to Keep It Secure? ", październik 2019 r. Acunetix. https://www.acunetix.com/whitepaper-the-future-is-the-web/

2.„What Is a Web Application Attack and how to Defend Against It". 2019. Acunetix. https://www.acunetix.com/websitesecurity/web-application-attack/

3. „2020 State of Application Services Report" F5 Networks, 2020. https://www.f5.com/state-of-application-services-report

4. „Sonicwall Cyber Threat Report". 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". 2019. Radware. https://www.radware.com/resources/was-report-2019/

6. „API Security Top 10 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". 13 sierpnia 2019 r. 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". 13 maja 2019 r. Fast Retailing. https://www.fastretailing.com/eng/group/news/1905132000.html

9. „Web Applications vulnerabilities and threats: statistics for 2019". 13 lutego 2020 r. Positive Technologies. https://www.ptsecurity.com/ww-en/analytics/web-vulnerabilities-2020/#id9

10. Esrtevao Avillez. „2019 Website Threat Research Report". 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)". 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)". 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" 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" 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". 2019. CyberEdge Group. https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf

16. „AppSec Advisor: Injection Attacks". październik 2019 r. CIS Center for Internet Security. https://www.cisecurity.org/newsletter/injection-attacks/

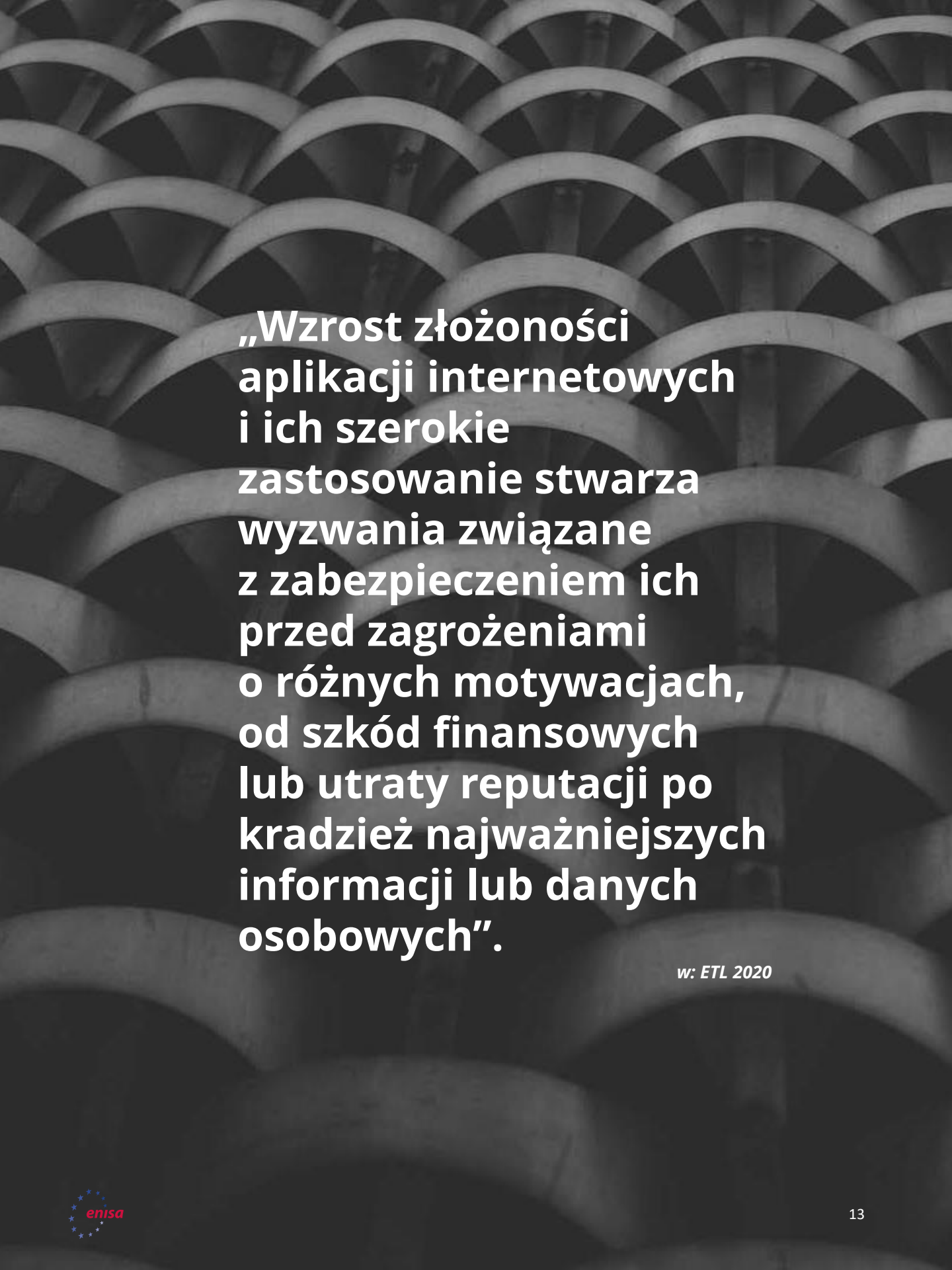
17. „Cybersecurity threatscape: Q3 2019. " 2 grudnia 2019 r. Positive Technologies. https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2019-q3/#id5

18. „Virtual Patching Best Practices". 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". 13 sierpnia 2019 r. 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". 22 października 2019 r. https://www.uscloud.com/blog/top-cyber-threats-in-2020/

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



„Wzrost złożoności aplikacji internetowych i ich szerokie zastosowanie stwarza wyzwania związane z zabezpieczeniem ich przed zagrożeniami o różnych motywacjach, od szkód finansowych lub utraty reputacji po kradzież najważniejszych informacji lub danych osobowych”.

w: ETL 2020

Powiązany

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Przegląd roku

Zestawienie trendów w cyberbezpieczeństwie w okresie od stycznia 2019 r. do kwietnia 2020 r.

PRZECZYTAJ RAPORT

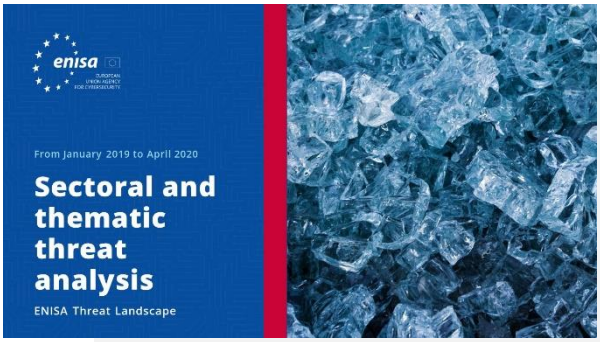
Raport ENISA o krajobrazie zagrożeń
Wykaz piętnastu największych zagrożeń

Agencja ENISA: wykaz piętnastu największych zagrożeń w okresie od stycznia 2019 r. do kwietnia 2020 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Tematyka badań

Zalecenia dotyczące tematów badawczych z różnych kwadrantów w dziedzinie cyberbezpieczeństwa i rozpoznawania zagrożeń cybernetycznych.



PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Sektorowa i tematyczna analiza zagrożeń

Kontekstualna analiza zagrożeń w okresie od stycznia 2019 r. do kwietnia 2020 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Nowe trendy

Główne trendy w cyberbezpieczeństwie w okresie od stycznia 2019 r. do kwietnia 2020 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Omówienie kwestii rozpoznawania cyberzagrożeń

Aktualny stan wywiadu dotyczącego cyberzagrożeń w UE.

Informacje o agencji

_ Agencja

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) jest unijną agencją działającą na rzecz osiągnięcia wysokiego ogólnego poziomu cyberbezpieczeństwa w całej Europie. Utworzona w roku 2004 i wzmocniona przez akt o cyberbezpieczeństwie Agencja Unii Europejskiej ds. Cyberbezpieczeństwa wnosi wkład w politykę cybernetyczną UE; zwiększa wiarygodność produktów, usług i procesów informacyjno-komunikacyjnych dzięki systemom certyfikacji cyberbezpieczeństwa; współpracuje z państwami członkowskimi i organami UE oraz pomaga przygotować Europę na przyszłe wyzwania cybernetyczne. Poprzez wymianę informacji, budowanie zdolności i pogłębianie wiedzy Agencja współdziała z kluczowymi zainteresowanymi stronami, aby zwiększać zaufanie do gospodarki opartej na łączności i odporność unijnej infrastruktury oraz w efekcie, zapewnić cyfrowe bezpieczeństwo społeczeństwa i mieszkańców Europy. Więcej informacji na temat ENISA i jej działalności można znaleźć na stronie www.enisa.europa.eu.

Współautorzy

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) oraz *wszyscy członkowie ENISA CTI Stakeholders Group:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) i Thomas Hemker.

Wydawcy

Marco Barros Lourenço (ENISA) i Louis Marinos (ENISA).

Dane kontaktowe

Zapytania dotyczące tego dokumentu można kierować na adres enisa.threat.information@enisa.europa.eu.

Zapytania prasowe dotyczące tego dokumentu można kierować na adres press@enisa.europa.eu.

Chcielibyśmy poznać opinie czytelników na temat tego raportu!
Poświęć chwilę, by wypełnić kwestionariusz. Aby uzyskać dostęp do formularza, kliknij tutaj.

Zastrzeżenia prawne

Informujemy, że niniejsza publikacja przedstawia poglądy i interpretacje ENISA, o ile nie stwierdzono inaczej. Niniejsza publikacja nie powinna być interpretowana jako działanie prawne ENISA ani organów ENISA, chyba że została przyjęta zgodnie z rozporządzeniem (UE) nr 526/2013. Niniejsza publikacja nie musi przedstawiać aktualnego stanu wiedzy i ENISA może ją okresowo aktualizować.

Źródła zewnętrzne zostały odpowiednio zacytowane. ENISA nie ponosi odpowiedzialności za treść źródeł zewnętrznych, w tym zewnętrznych stron internetowych, do których odniesienia znajdują się w niniejszej publikacji.

Niniejsza publikacja ma charakter wyłącznie informacyjny. Musi ona być dostępna nieodpłatnie. Ani ENISA, ani żadna osoba działająca w jej imieniu nie ponoszą odpowiedzialności za wykorzystanie informacji zawartych w niniejszym sprawozdaniu.

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Grecja
Tel.: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu