enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

PL

Od stycznia 2019 r. do kwietnia 2020 r.

Zagrożenia wewnętrzne

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

Informacje ogólne

Zagrożenie wewnętrzne to działanie, które może skutkować incydentem, przeprowadzane przez osobę lub grupę będącą związaną z potencjalną ofiarą lub dla niej pracującą. Zagrożenia wewnętrzne mają wiele wzorców. Dobrze znanym wzorcem zagrożenia wewnętrznego (zwanym również „nadużyciem uprawnień") jest przypadek, gdy osoby z zewnątrz współpracują z podmiotami wewnętrznymi celem uzyskania nieupoważnionego dostępu do zasobów. Osoby z wewnątrz mogą spowodować szkody nieumyślnie lub wskutek braku wiedzy. Takie osoby z wewnątrz często cieszą się zaufaniem i posiadają uprawnienia, jak również znają zasady, procesy i procedury obowiązujące w organizacji, zatem trudno jest odróżnić, czy uzyskanie dostępu do aplikacji, danych i systemów było uprawnione, miało na celu działania przestępcze, czy też było wynikiem błędu[1].

Można zdefiniować pięć rodzajów zagrożeń wewnętrznych w zależności od celu działania:

a) nieuważni pracownicy, którzy nieodpowiednio obchodzą się z danymi, łamią zasady użytkowania oraz instalują nieautoryzowane aplikacje;

b) szpiedzy, którzy wykradają informacje dla osób z zewnątrz;

c) niezadowoleni pracownicy, którzy chcą zaszkodzić organizacji;

d) osoby z wewnątrz, które mają przestępcze zamiary, wykorzystujące istniejące uprawnienia wcelu kradzieży informacji lub uzyskania osobistych korzyści;

e) nieodpowiedzialne podmioty zewnętrzne, które poprzez działania wywiadowcze, nadużycia lub mające na celu szkodliwe działania, dostęp do zasobu lub jego wykorzystanie powodują naruszenie zasad bezpieczeństwa.

Wszystkie pięć wymienionych rodzajów zagrożeń wewnętrznych należy stale badać, jako że świadomość ich istnienia i sposób działania powinny definiować strategię bezpieczeństwa i ochrony danych w organizacji.

Wnioski

65% skutków zagrożeń wewnętrznych obejmuje szkody dla reputacji i finansów organizacji[12]

88% badanych organizacji uznaje zagrożenia wewnętrzne za powód do alarmu[10]

11,45 mln EUR to średni roczny koszt incydentów związanych z cyberbezpieczeństwem, spowodowanych przez podmiot wewnętrzny organizacji[8]

40% badanych organizacji obawia się ujawnienia poufnych informacji biznesowych[11]

Kill chain

Proces etapów ataku

Zakres działania

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

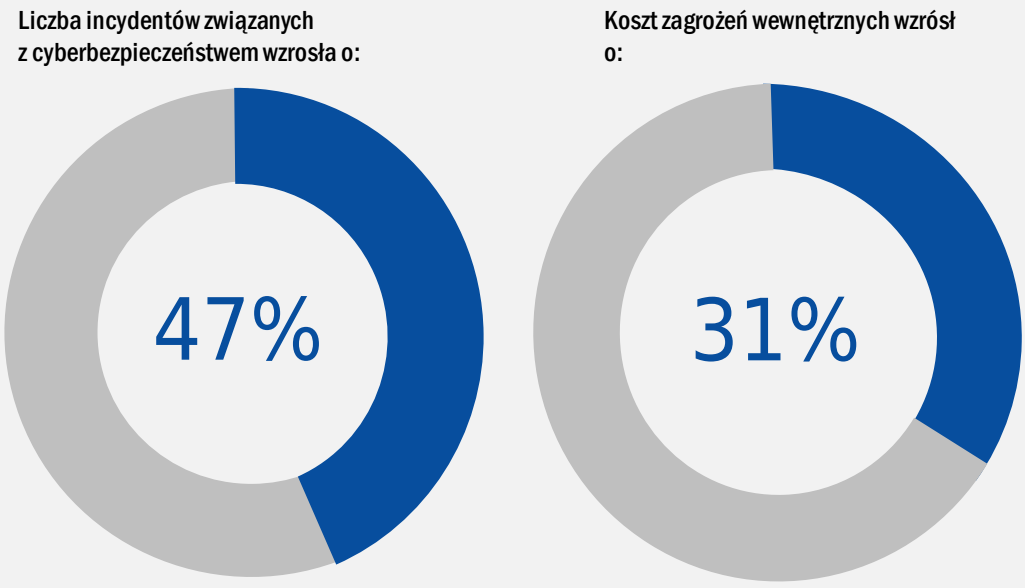
Opis

_Rządzą pieniądze

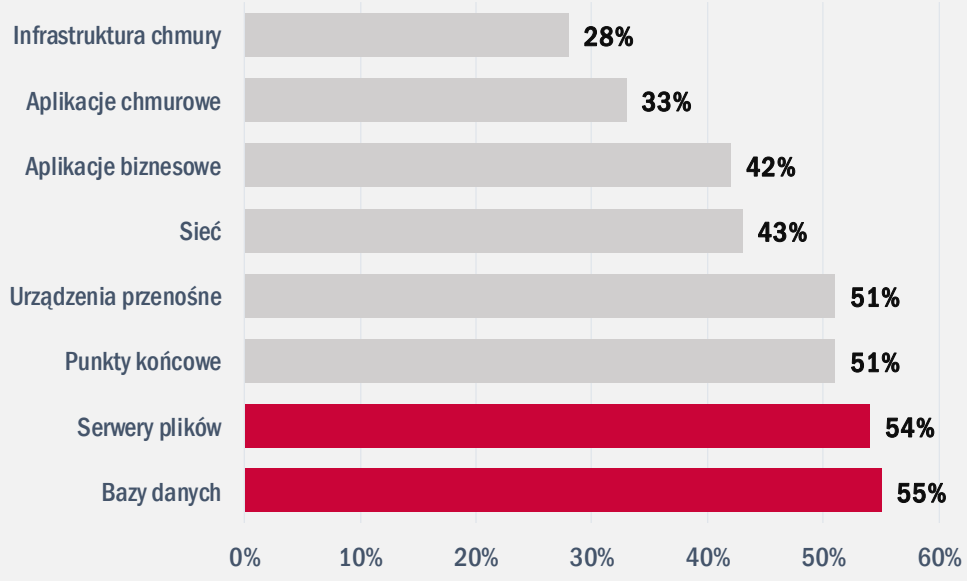
Z uwagi na rosnący koszt wektorów ataku przestępcy są chętni oferować osobom z wewnątrz duże sumy pieniędzy. Cena przekupienia takiej osoby może być różna w zależności od jej pozycji w firmie, samej firmy, rodzaju i złożoności usługi, jaka ma być wykonana, typu pożądanych danych oraz poziomu zabezpieczeń w firmie. Niektóre sposoby rekrutacji osób z wewnątrz: (1) opublikowanie oferty na forach obejmującej nagrodę za pewne informacje; (2) zamaskowanie działań tak, by pracownicy nie zdawali sobie sprawy, że działają nielegalnie, ujawniają dane osobowe lub w inny sposób działają na szkodę firmy; (3) szantaż[4].

_Nielegalne działania – urbi et orbi

Były programista firmy świadczącej usługi w chmurze wykorzystał źle skonfigurowaną zaporę sieciową aplikacji internetowej i uzyskał dostęp do kont oraz rekordów kart kredytowych ponad 100 milionów klientów. Firma od tamtego czasu załatała lukę w zabezpieczeniach i oświadczyła, że „żadne numery kart kredytowych ani dane logowania nie zostały narażone". Ten przypadek zagrożenia wewnętrznego jest szczególnie interesujący z uwagi na to, że były pracownik, który zhakował firmę, nie dbał o ukrycie swojej tożsamości. Haker opisał metodę ataku na czacie współpracownikom z firmy Capital One. Opublikował również te informacje w serwisie GitHub (pod nazwiskiem) i chwalił się tym w mediach społecznościowych. Tego rodzaju zachowanie to zjawisko, które psychologowie określają „wyciekaniem informacji" – gdy osoby z wewnątrz, które planują poczynić szkody, ujawniają plany. Firma Capital One ocenia, że naruszenie bezpieczeństwa danych będzie ją kosztować do 150 mln USD (ok. 127 mln EUR)[5].



Rysunek 2: Trendy dotyczące incydentów i ich kosztów. Źródło: ObservelT[8]



Rysunek 2: Zasoby IT podatne na zagrożenia wewnętrzne. Źródło: Help Systems[9]

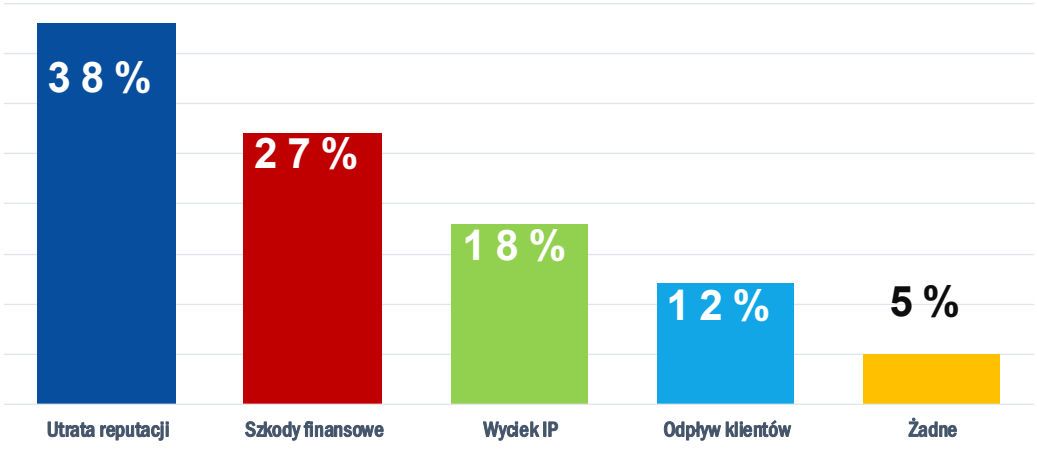
Wektory ataku

_Jak

Jak wynika z niedawno przeprowadzonego badania[14], największe niebezpieczeństwo w kontekście zagrożeń wewnętrznych w firmach i innych organizacjach stanowią grupy.

Eksperci w zakresie cyberbezpieczeństwa[15] twierdzą, że w przypadku nieumyślnie spowodowanych zagrożeń wewnętrznych największą rolę odgrywa phishing (38%). Dalej na liście są ataki ukierunkowane, tzw. spear phishing (21%), słabe lub wielokrotnie używane hasła (16%), osierocone konta (10%) oraz przeglądanie podejrzanych stron (7%).

_ Obszary skutków incydentów związanych z zagrożeniem wewnętrznym



Rysunek 3 – źródło: Egress[12]


„Osoby z wewnątrz mogą spowodować szkody nieumyślnie lub wskutek braku wiedzy”.
w: ETL 2020

Ograniczenie ryzyka

Proponowane działania

- Wdrożenie technologii głębokiej inspekcji pakietów (deep packet inspection, DPI) dla wykrytych anomalii, która użytkownikom przemysłowym oferuje zaufaną platformę monitorowania przepływów poleceń sterowania procesem oraz danych telemetrycznych, jak również ochrony przed zagrożeniami z zewnątrz. Jednocześnie technologia ta ogranicza ryzyko zakłóceń z wewnątrz ze strony „zaawansowanych" użytkowników, takich jak inżynierowie, operatorzy systemu SCADA czy inni pracownicy wewnętrzni mający bezpośredni dostęp do systemów[16].
- Wprowadzenie planu przeciwdziałania zagrożeniom wewnętrznym do ogólnej strategii i zasad bezpieczeństwa. Plan taki zazwyczaj obejmuje ramy zarządzania ryzykiem, plan ciągłości działania (BCP), plan przywrócenia gotowości do pracy po katastrofie (DRP), zasady zarządzania finansami i księgowością oraz zarządzanie kwestiami regulacyjnymi[1].
- Stworzenie programu bezpieczeństwa obejmującego: prowadzenie działań mających na celu wykrywanie zagrożeń, skanowanie podatności na zagrożenie oraz testy penetracyjne, wdrożenie środków bezpieczeństwa osobowego, fizycznego, sieciowego i punktów końcowych, stosowanie środków bezpieczeństwa danych, wdrożenie zarządzania tożsamością i dostępem, zadbanie o zdolność do zarządzania incydentami, zapewnienie usług śledztwa informatycznego oraz wykorzystanie sztucznej inteligencji do zapobiegania atakom z wewnątrz.
- Opracowanie zasad bezpieczeństwa w zakresie zagrożeń wewnętrznych opartych na świadomości użytkowników – jest to jeden z najskuteczniejszych środków przeciwdziałania tego rodzaju cyberzagrożeniom.
- Wdrożenie mocnych technicznych mechanizmów kontrolnych. Tradycyjne środki bezpieczeństwa zazwyczaj ukierunkowane są na zagrożenia z zewnątrz, jednak zazwyczaj są one nieskuteczne w zakresie identyfikacji wewnętrznych zagrożeń pochodzących z samej organizacji. Aby chronić zasoby, należy wdrożyć narzędzia, takie jak ochrona przed utratą danych (data loss prevention, DLP), aby zapobiec wyciekowi danych[1].

- Zmniejszenie liczby użytkowników mających uprawnienia i dostęp do informacji wrażliwych. Jeśli pracownik nie musi mieć dostępu do pewnych informacji, by wykonać swoją pracę, lepiej jest ograniczyć ich widoczność, unikając ewentualnego nieuprawnionego dostępu[17].
- Uszczelnienie środowiska informatycznego, co obejmuje wzmocnienie zabezpieczeń sieci, systemów, aplikacji, danych i kont[1].

Bibliografia

1. „Insider Threat Report", 2019. Verizon. https://enterprise.verizon.com/resources/reports/insider-threat-report.pdf

2. „Insider Threat Statistics Facts and Figures". Ekran System. https://www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures

3. „CyberEdge 2019 CDR Report" 2019. CyberEdge. https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf

4. „Corporate Security Predictions 2020". 2019. 3 grudnia 2019 r. Kaspersky.

https://securelist.com/corporate-security-predictions-2020/95387/

5. „Famous Insider Threat Cases" wrzesień 2019 r. Security Boulevard. https://securityboulevard.com/2019/09/famous-insider-threat-cases-insider-threat-awareness-month/

6. „The rise of insider threats: Key trends to watch" 2019. Tech Beacon.

https://techbeacon.com/security/rise-insider-threats-key-trends-watch

7. „Cost of Cybercrime study" 2019. Accenture. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

8. „Cost of Insider Threats", 2020. Observer IT. https://www.observeit.com/cost-of-insider-threats/

9. „Cybersecurity Insiders 2019 Insider Threat Report", 2019. Help Systems.https://www.helpsystems.com/cta/2019-cybersecurity-insiders-insider-threat-report

10. „Forcepoint Insider threat Data Protection" 2017. Force Point.

https://www.forcepoint.com/sites/default/files/resources/files/brochure_insider_threat_data_protection_en.pdf

11. „State of Insider Threats in the Digital Workplace" 2019. Better Cloud. https://www.bettercloud.com/monitor/wp-content/uploads/sites/3/2019/03/BetterCloud-State-of-Insider-Threats-2019-FINAL.pdf

12. „Insider Data Breach Survey 2019". 2019. Egress. https://scoop-cms.s3.amazonaws.com/566e8c75ca2f3a5d5d8b45ae/documents/egress-opinionmatters-insider-threat-research-report-a4-uk-digital.pdf

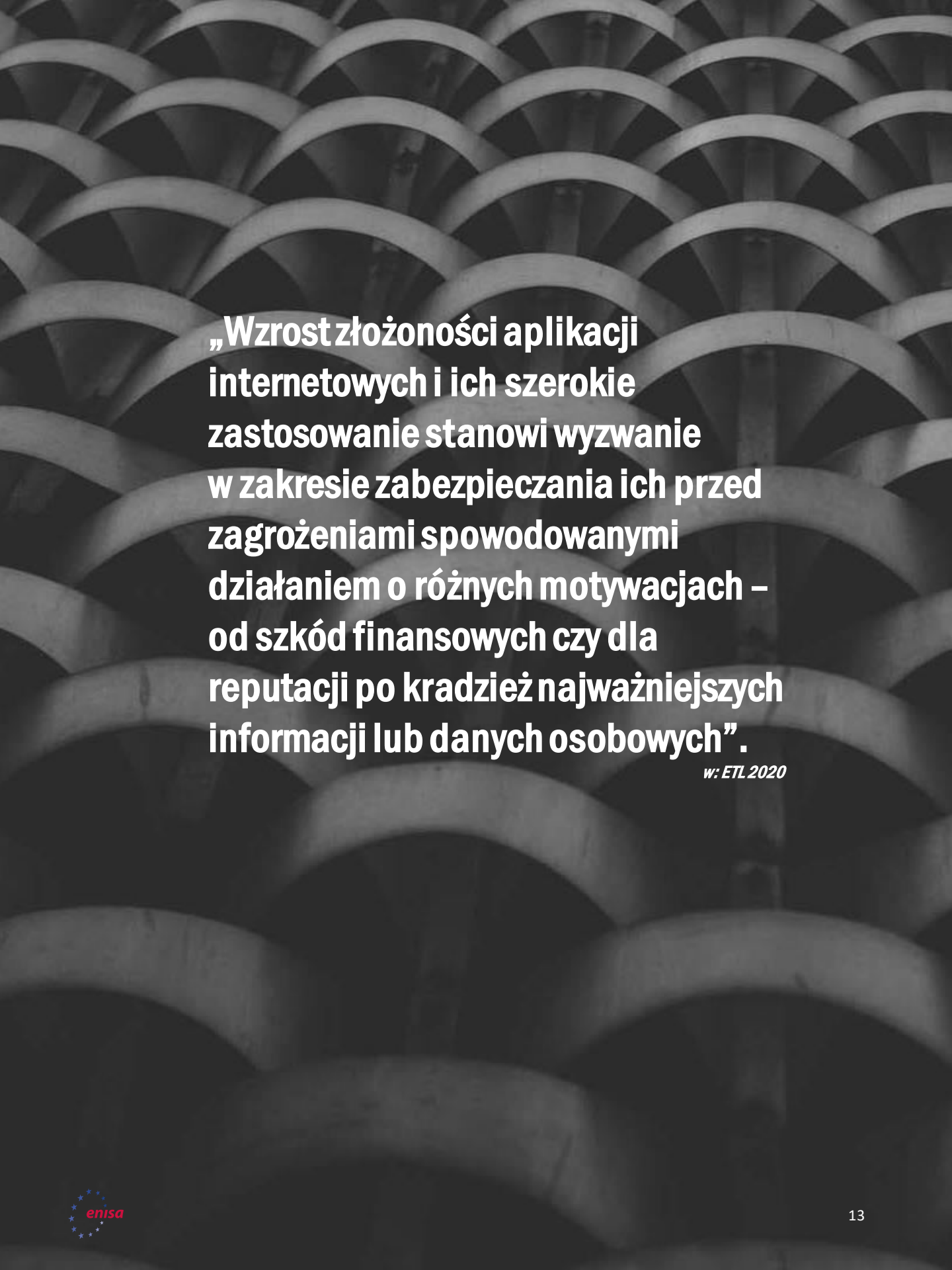
13. „Insider Threat Report". 2019. Nucleos Cyber. https://nucleuscyber.com/wp-content/uploads/2019/07/2019_Insider-Threat-Report_Nucleus_Final.pdf

14. „Insider Threat Report". 2019. Haystax. https://haystax.com/wp-content/uploads/2019/07/Haystax-Insider-Threat-Report-2019.pdf

15. „Insider Threat Report". 2019. Fortinet. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/insider-threat-report.pdf

16. „Kaspersky Industrial CyberSecurity: solution overview 2019". 2019. Kaspersky. https://ics.kaspersky.com/media/KICS-Solution-overview-2019-EN.pdf

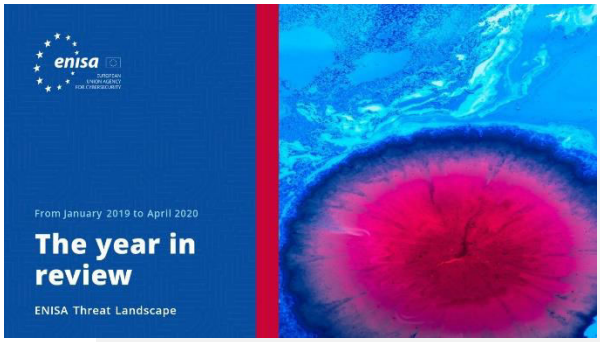
17. „Post-vacation cybersecurity tuneup: Get your company ready!". 1 września 2017 r. Panda. https://www.pandasecurity.com/mediacenter/adaptive-defense/cyber-security-get-company-ready/



„Wzrost złożoności aplikacji internetowych i ich szerokie zastosowanie stanowi wyzwanie w zakresie zabezpieczania ich przed zagrożeniami spowodowanymi działaniem o różnych motywacjach – od szkód finansowych czy dla reputacji po kradzież najważniejszych informacji lub danych osobowych”.

w: ETL 2020

Powiązany



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

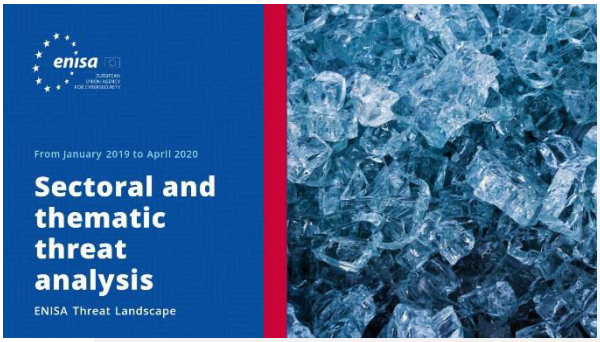
Agencja ENISA: wykaz piętnastu największych zagrożeń w okresie od stycznia 2019 r. do kwietnia 2020 r.

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



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