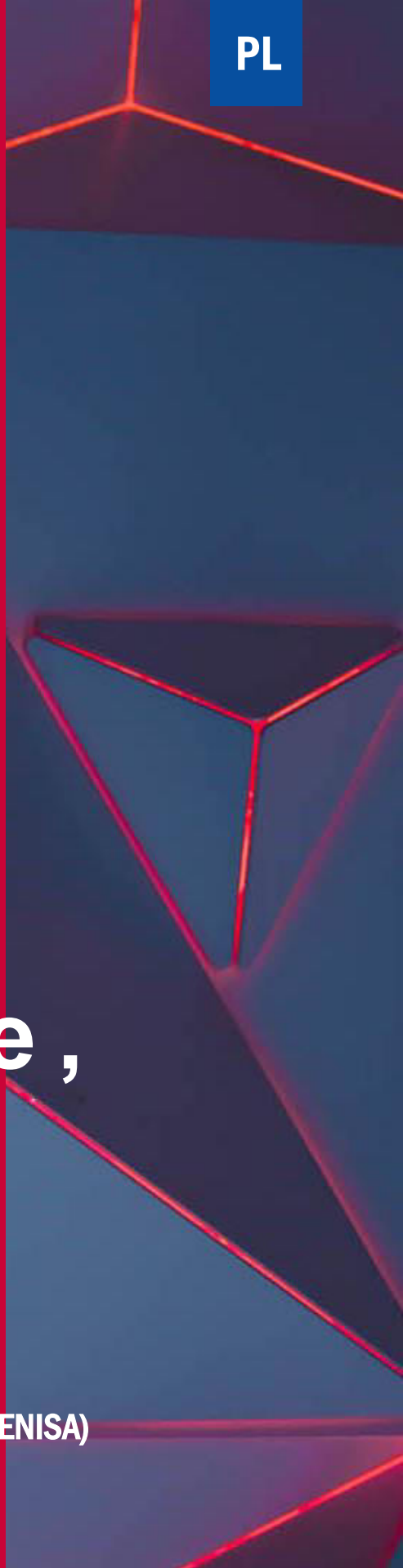
PL

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Od stycznia 2019 r. do kwietnia 2020 r.

Ingerencja fizyczna, uszkodzenie, kradzież i utrata

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

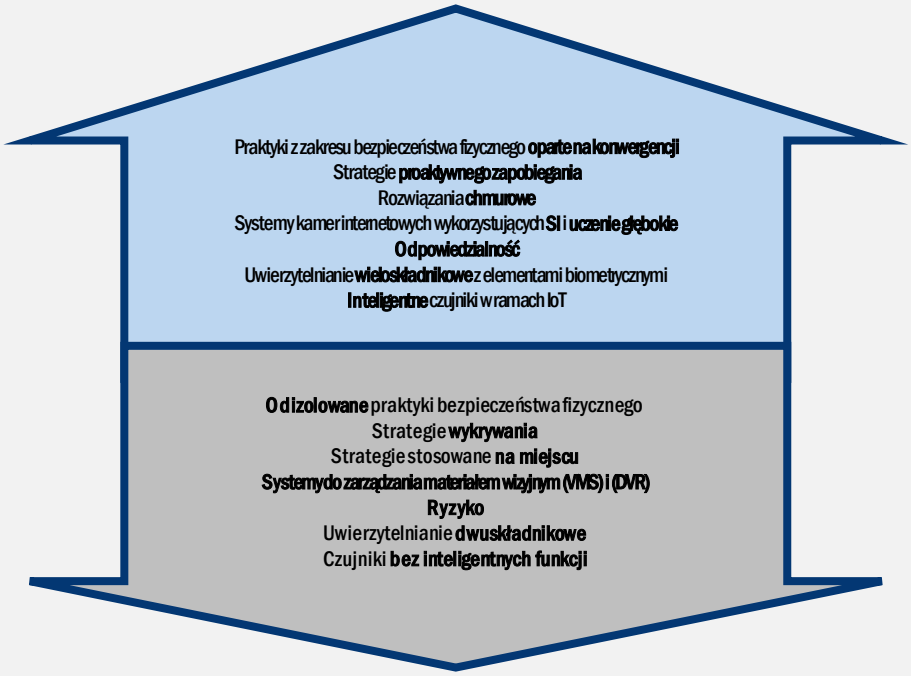


Informacje ogólne

Ingerencja fizyczna, uszkodzenie, kradzież i utrata uległy drastycznym zmianom w ciągu kilku ostatnich lat. Integralność urządzeń jest bardzo istotna dla zapewnienia mobilności technologii i dla większości wdrożeń internetu rzeczy (IoT). IoT może poprawiać bezpieczeństwo fizyczne dzięki bardziej zaawansowanym i złożonym rozwiązaniom[1]. Dzięki temu systemy oparte na zabezpieczeniach IP z inteligentnymi czujnikami, kamerami podłączonym do Wi-Fi, inteligentnym oświetleniem zabezpieczającym, dronami i zamkami elektronicznymi mogą gromadzić dane z dozoru, które są oceniane przez mechanizmy sztucznej inteligencji (AI) i uczenia maszynowego (ML) w celu identyfikacji zagrożeń i reagowania z minimalnym opóźnieniem i maksymalną dokładnością[2]. Jednakże inteligentne budynki, urządzenia mobilne i inteligentne urządzenia do noszenia na ciele mogą zostać wykorzystane do ominięcia fizycznych środków bezpieczeństwa[3].

W 2019 r. nadal trwały ataki fizyczne na bankomaty i punkty sprzedaży w Europie i na całym świecie, lecz straty, do jakich w ten sposób doszło, były niższe niż średnia dla ostatniej dekady. Dobra wiadomość jest taka, że menedżerowie IT i osoby odpowiedzialne za podejmowanie decyzji skłaniają się ku hybrydowym planom, łączącym bezpieczeństwo w sieci z fizycznym – choć to drugie w przeszłości nie było priorytetem.

Nowe i przestarzałe praktyki z zakresu bezpieczeństwa fizycznego

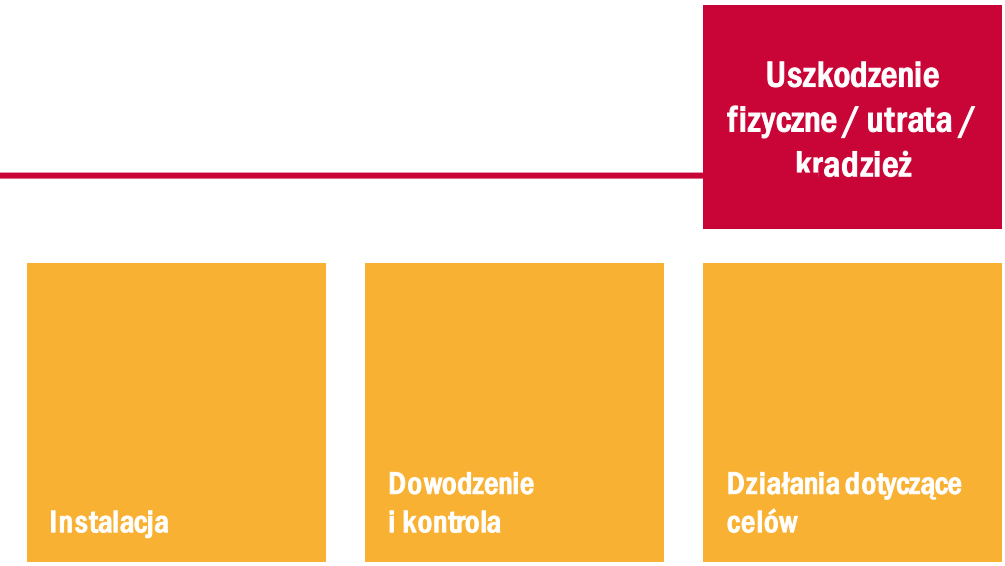


Rysunek 1 – źródło: Blog Boonedam[4]

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

_ Dostęp fizyczny to najważniejsze „tylne wejście”

W kwietniu 2019 r. Vishwanath Akuthota przyznał się do wandalizmu: zniszczył elementy wyposażenia ładunkiem elektrycznym, korzystając z urządzenia USB. Zniszczone wyposażenie należało do College of Saint Rose w Albany, stan Nowy Jork, uczelni, której absolwentem był Akuthota. Aby dokonać tego ataku, uzyskał on dostęp do 66 stacji roboczych oraz licznych monitorów i pulpitów cyfrowych. Szkodliwe urządzenie USB, którego użył, zakupił przez internet. Uczelnia wydała ponad 50 000 USD (ok.42 452 EUR) na wymianę wyposażenia i ponad 7000 USD (ok. 5943 EUR) na wynagrodzenie pracownika, który usuwał skutki incydentu. Akuthocie groziło 10 lat więzienia i grzywna w maksymalnej wysokości 250 000 USD (ok. 212 257 EUR)[5].

_ Przedsiębiorstwa nie zwracają uwagi na bezpieczeństwo fizyczne

W 2019 r. przeprowadzono wiele ankiet na temat bezpieczeństwa fizycznego. Niektóre z tych ankiet były skierowane do dyrektorów zarządzających, menedżerów IT i osób podejmujących decyzje w kilku branżach, a ich wyniki dają dobre wyobrażenie o tym, jak przedsiębiorstwa podchodzą do bezpieczeństwa fizycznego. Dyrektorzy zarządzający z różnych branż przemysłowych wydają się skłaniać ku połączonemu planowi bezpieczeństwa cybernetycznego i fizycznego, który miałby chronić aktywa przed zagrożeniami, z uwzględnieniem takich czynników, jak zagrożenia wewnętrzne, znaczenie infrastruktury i integralność sieci przedsiębiorstwa. W tych połączonych planach bezpieczeństwa położono największy nacisk oraz przeznaczono największe zasoby finansowe i osobowe na inwestycje w bezpieczeństwo cybernetyczne (tj. odpowiednio 83–86% środków), natomiast 14–17% środków firmy przeznaczono na bezpieczeństwo fizyczne W Europie większość menedżerów IT (77%) poinformowała, że środki zapewnienia bezpieczeństwa fizycznego w ich firmach są przestarzałe[7].

Bezpieczeństwo fizyczne jako usługa

W 2019 r. widoczny był trend poprawy bezpieczeństwa fizycznego poprzez wprowadzenie hostowanych rozwiązań z zakresu bezpieczeństwa. Większość związanych z bezpieczeństwem fizycznym planów menedżerów IT już skłania się w kierunku systemu wykorzystującego chmurę lub IoT lub planuje wprowadzenie takich zmian w ciągu 12 miesięcy. Osoby odpowiedzialne za podejmowanie decyzji informowały, że już teraz oceniają rozwiązania typu „dozór wizyjny jako usługa" (VSaaS) i „kontrola dostępu jako usługa" (ACaaS), by usprawnić wykrywanie incydentów i zminimalizować czas reakcji oraz zmniejszyć odsetek wyników fałszywie dodatnich. VSaaS i ACaaS wpłynęły pozytywnie na poprawę zarówno bezpieczeństwa fizycznego, jak i cyberbezpieczeństwa, choć zaledwie kilku menedżerów IT określiło bezpieczeństwo fizyczne jako priorytet[8].

Bezpieczeństwo fizyczne nie wytrzymuje próby czasu

Jak zauważono w 2018 r., w okresie objętym raportem bankomaty były podatne na ingerencję i uszkodzenia fizyczne, a ich ostatecznym celem była kradzież znajdującej się w nich gotówki. W Irlandii tylko w roku 2019 zarejestrowano dziewięć takich incydentów[9]. Niektóre z tych ataków miały bardzo dramatyczny przebieg: przestępcy używali skradzionych koparek, burzyli ściany i umieszczali bankomaty w furgonetkach lub samochodach. W innych przypadkach ataki trwały zaledwie kilka minut: przestępcy używali materiałów wybuchowych, wyciągali bankomaty przy użyciu łańcuchów lub stosowali taran[10]. W Holandii zaledwie w jeden listopadowy weekend miało miejsce 71 ataków na bankomaty z użyciem materiałów wybuchowych (określanych w języku niderlandzkim jako „plofkraken"), w porównaniu z 43 podobnymi atakami przez cały rok 2018. Bank ABN AMRO został zmuszony do likwidacji 470 podatnych bankomatów, zaś Holenderskie Stowarzyszenie Bankowości (NVB) podjęło decyzję o wyłączaniu w grudniu wszystkich bankomatów w kraju co noc od 23:00 do 7:00[11]. Rok 2019 to czwarty z rzędu rok, w którym wzrosła liczba fizycznych ataków na bankomaty.

Trendy

Nieuprawnione ingerencje w bankomaty

W roku 2019 najczęściej spotykanymi skutkami nieuprawnionych ingerencji w bankomaty były: zatrzymywanie kart, zatrzymywanie gotówki i oszustwo z anulowaniem transakcji. Najbardziej ogólny wniosek dla tego roku sugeruje, że dzięki zwiększeniu odsetka transakcji bezgotówkowych z użyciem standardu EMV zmniejszyła się liczba nieuprawnionych ingerencji w bankomaty i dystrybutory na stacjach paliw. Standard EMV (nazwę utworzono od pierwszych liter nazw firm, które go wprowadziły, tj. Europay, Mastercard i Visa) opisuje specyfikacje inteligentnych kart, terminali płatniczych i bankomatów. Karty EMV (tj. karty chronione chipem i kodem PIN lub karty chipowe) są wyposażone w układy scalone. Wprowadzenie kart EMV przynajmniej częściowo utrudniło przestępcom oszustwa dokonywane kartą okazywaną w miejscu dokonywania płatności[12]. Niestety karty EMV nie zostały jeszcze szeroko wprowadzone poza Europą, a nawet w Europie tylko kilka krajów przyjęło kontrolę opartą na lokalizacji, narzędzie do zwalczania nadużyć finansowych dostępne dzięki kartom EMV[13].

Incydenty

- Naruszenie z użyciem szkodliwego urządzenia USB podkreśla potrzebę bezpieczeństwa fizycznego. Vishwanath Akuthota, absolwent College of Saint Rose w Albany, w stanie Nowy Jork, przyznał się do uszkodzenia elementów wyposażenia z użyciem szkodliwego urządzenia USB[5].
- Przestępcy używają koparki do kradzieży bankomatu w Irlandii Północnej. Liczba ataków fizycznych na bankomaty w całej Unii Europejskiej rośnie[9].
- Ataki „plofkraken" w Holandii. Ataki z użyciem materiałów wybuchowych na bankomaty w Holandii (określane tam jako „plofkraken"). Z powodu luk w zabezpieczeniach ich celem były głównie bankomaty ABN AMRO. Skłoniły one bank do likwidacji około 470 bankomatów w całej Holandii[11].

Wnioski

4% naruszeń było spowodowanych działaniami fizycznymi[12]

20% incydentów związanych z cyberbezpieczeństwem rozpoczęło się od działania fizycznego lub zakończyło na nim[12]

Piąte *najczęściej stosowane niebezpieczne działanie wymierzone przeciwko aktywom to ataki fizyczne na bankomaty*[12]

54% przypadków naruszeń danych wiązało się z atakiem fizycznym jako główną metodą

48% menedżerów z branży IT używa dozoru wizyjnego lub metod kontroli dostępu opartych na chmurze[8]

72% pracowników uważa pozostawianie informacji szczególnie chronionych w dostępnych publicznie miejscach za największe zagrożenie dla bezpieczeństwa danych[14]

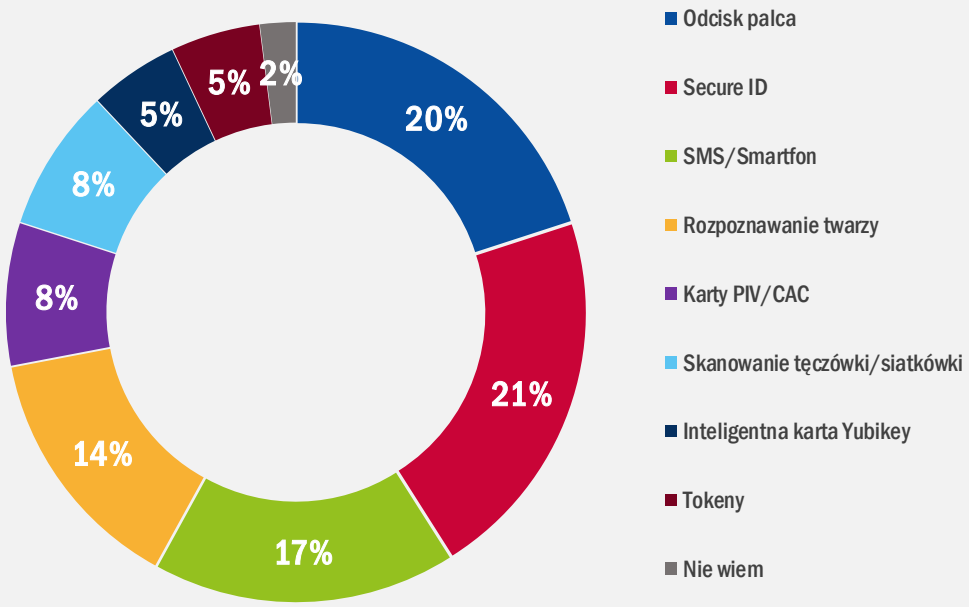
65% z ponad 1000 pracowników objętych badaniem poinformowało o zachowaniach i stosowaniu praktyk uznawanych za ryzykowne w odniesieniu do bezpieczeństwa fizycznego[15]

Ograniczenie ryzyka

Proponowane działania

- Stosowanie szyfrowania we wszystkich operacjach związanych z przechowywaniem i przesyłaniem informacji poza obwodem zabezpieczeń (urządzenia, sieci, usługi w chmurze itp.).
- Używanie wykazów zasobów w celu śledzenia urządzeń użytkowników i przypominanie użytkownikom o sprawdzaniu dostępności.
- Zapewnienie ograniczonego dostępu do obszarów zawierających informacje lub urządzenia szczególnie chronione.
- Wdrożenie dobrze udokumentowanych zasad bezpieczeństwa fizycznego i zintegrowanie środków bezpieczeństwa fizycznego z cyfrowymi w celu uzyskania holistycznego podejścia.
- Korzystanie z polis ubezpieczeniowych do pokrywania strat wynikłych zarówno z zagrożeń fizycznych, jak i związanych z cyberprzestrzenią.
- Opracowanie instrukcji obsługi dla użytkowników urządzeń mobilnych (smartfony, tablety, laptopy itp.) i postępowanie zgodne z najlepszymi praktykami.
- Stworzenie i rozpowszechnienie procedur ochrony fizycznej zasobów, także przed utratą, uszkodzeniem i kradzieżą.
- Zapewnienie, że urządzenia są wycofywane z eksploatacji po usunięciu danych osobowych lub informacji szczególnie chronionych[6].
- Skrócenie czasu reakcji na incydenty związane z kradzieżą, uszkodzeniem i utratą.
- Wdrożenie uwierzytelniania wieloskładnikowego, łączącego poświadczenia użytkownika z elementami biometrycznymi, inteligentnymi kartami i innymi tokenami fizycznymi[16].
- Okresowa kontrola urządzeń pod kątem zmian czy wymiany[6].
- Wdrożenie procesów mających na celu wykrywanie uprawnionych gości czy pracowników i przydzielanie odpowiednich praw dostępu[6].
- Wdrożenie systemów monitorowania dostępu, systemów kontroli dostępu, silnych poświadczeń dostępu i inteligentnych urządzeń dostępu (np. inteligentne zamki, inteligentne klucze) do pomieszczeń, gdzie znajdują się szczególnie chronione urządzenia[6].

Najbardziej preferowane alternatywy dla poświadczeń użytkownika w uwierzytelnianiu wieloskładnikowym (MFA)



Rysunek 2 – źródło: ORACLE i KPMG[16]

Bibliografia

1. „Physical Security Guide". Kisi. https://pages.getkisi.com/physical-security-guide

2. Jonathan Wackrow. „Security Convergence: Addressing Evolving Cyber and Physical Security Threats". 2019. Teneo. https://www.teneo.com/vision-book/2019/security-convergence-addressing-evolving-cyber-and-physical-security-threats/

3. Pierluigi Paganini. „Modern Physical Security Awareness Is More Than Dumpster Diving [Updated 2019]". 27 sierpnia 2019 r. Infosec Institute. https://resources.infosecinstitute.com/modern-physical-security-awareness-is-more-than-dumpster-diving/#gref

4. Pierre Bourgeix. „2019: What's In & Out in Physical Security". 2019. Boon Edam. https://blog.boonedam.us/2019-whats-in-out-in-physical-security

5. Danny Bradbury. „Killer USB Breach Highlights Need For Physical Security". 23 kwietnia 2019 r. Infosec Magazine. https://www.infosecurity-magazine.com/infosec/usb-breach-physical-security-1-1-1/

6. „PCI DSS Quick Reference". Lipiec 2018 r. PCI Security Standards Council. https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

7. „76% Security Professionals Face Cybersecurity Skills Shortage: Report". 7 maja 2020 r. CISOMAG. https://cisomag.eccouncil.org/security-leaders-lack-cybersecurity-skills/

8. „2019 Landscape Report: Hosted Security Adoption In Europe". 2019. Morphean. https://morphean.com/whitepaper/

9. Catalin Cimpanu. „Crooks use digger to steal ATMs in Northern Ireland as ATM physical attacks rise across the EU". 16 kwietnia 2019 r. ZDNet. https://www.zdnet.com/article/crooks-use-digger-to-steal-atms-in-northern-ireland-as-atm-physical-attacks-rise-across-the-eu/

10. Jovi Umawing. „Everything you need to know about ATM attacks and fraud: Part 1". 29 maja 2019 r. Malwarebytes Labs. https://blog.malwarebytes.com/101/2019/05/everything-you-need-to-know-about-atm-attacks-and-fraud-part-1/

11. „ATM Explosive Attacks – Dutch ATMs to be shut down overnight to counter ATM explosive attacks". 19 grudnia 2019 r. European Association for Secure Transactions (EAST). https://www.association-secure-transactions.eu/dutch-atms-to-be-shut-down-overnight-to-counter-atm-explosive-attacks/

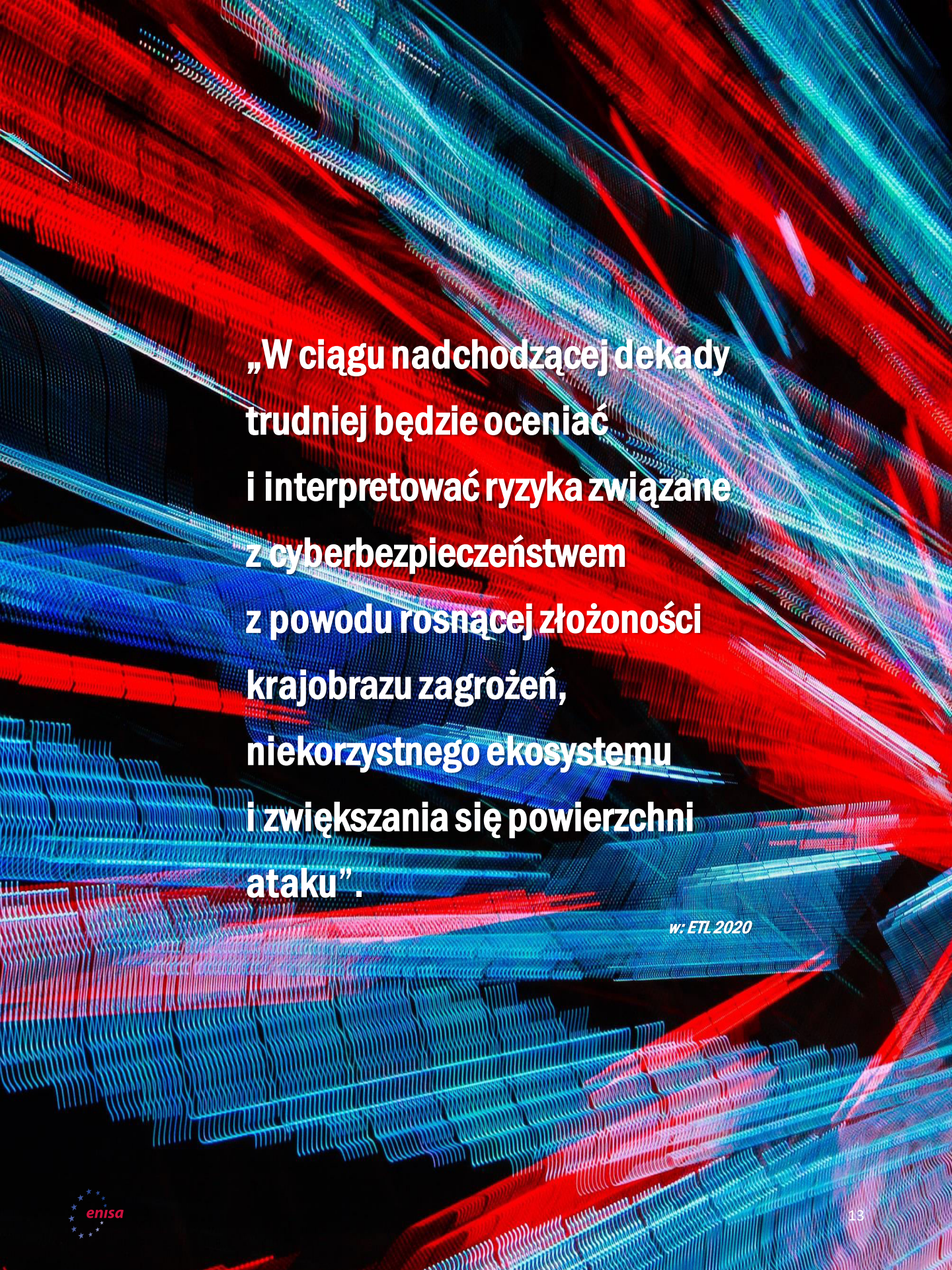
12. „2019 Payment Security Report", „2019 Data Breach Investigations Report". Verizon. https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

13. „2019 Payment Threats and Fraud Trends Report". 9 grudnia 2019 r. European Payments Council. https://www.europeanpaymentscouncil.eu/document-library/other/2019-payment-threats-and-fraud-trends-report

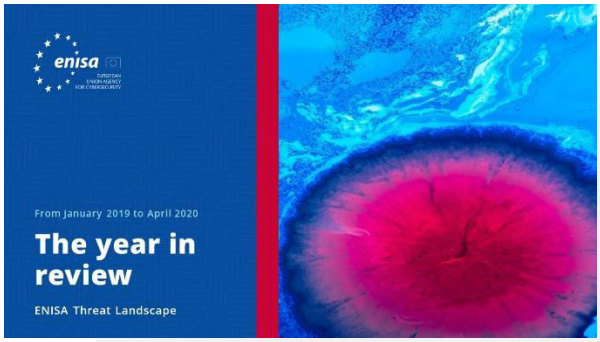
14. „2019 Eye on Privacy Report". 2019. MediaPRO. https://pages.mediapro.com/Eye-on-Privacy-Report-2019-LP.html

15. „Report: 2020 State of Privacy and Security Awareness". 2020. MediaPRO. https://www.mediapro.com/report-2020-state-of-privacy-security-awareness/

16. „Oracle and KPMG Cloud Threat Report". 2019. ORACLE i KPMG. https://www.oracle.com/fr/a/ocom/docs/dc/final-oracle-and-kpmg-cloud-threat-report-2019.pdf


„W ciągu nadchodzącej dekady
trudniej będzie oceniać
i interpretować ryzyka związane
z cyberbezpieczeństwem
z powodu rosnącej złożoności
krajobrazu zagrożeń,
niekorzystnego ekosystemu
i zwiększania się powierzchni
ataku”.
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

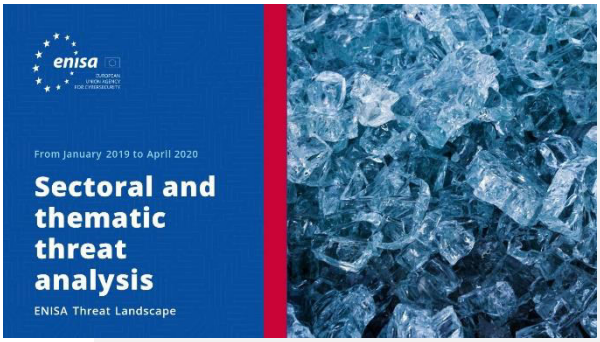
Agencja ENISA: wykaz piętnastu największych zagrożeń w okresie od stycznia 2019 r. do kwietnia 2020 r.

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. Cyberbezpieczeństwawnosi 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

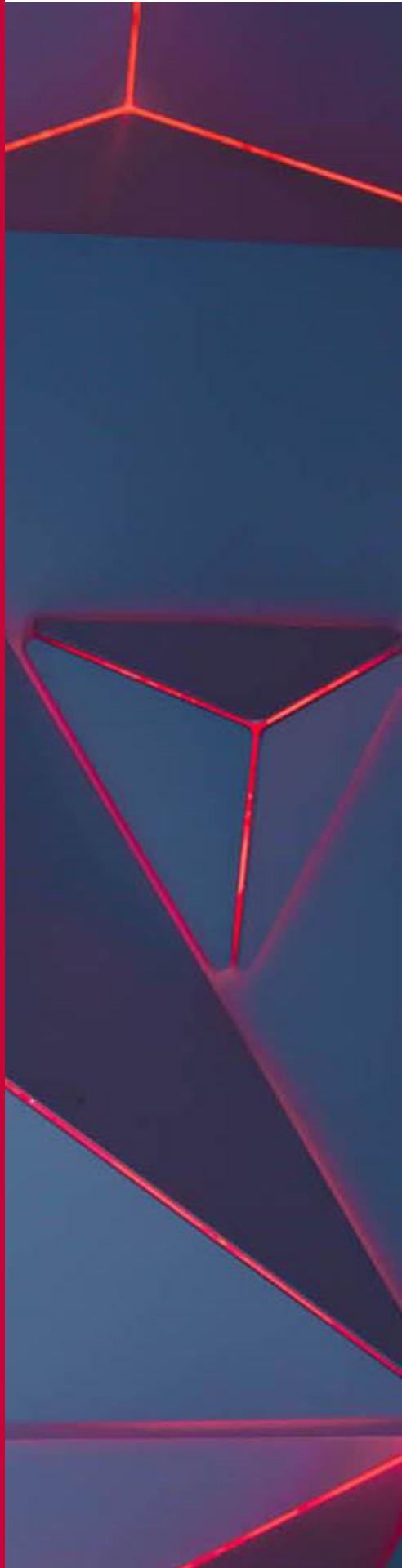
Informujemy, że niniejsza publikacja przedstawia poglądy i interpretacje ENISA, o ile nie stwierdzono inaczej. Niniejsza publikacja nie powinna być interpretowana jako działanie prawne ENISA ani organów ENISA, chyba że została przyjęta zgodnie z rozporządzeniem (UE) nr 526/2013. Niniejsza publikacja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