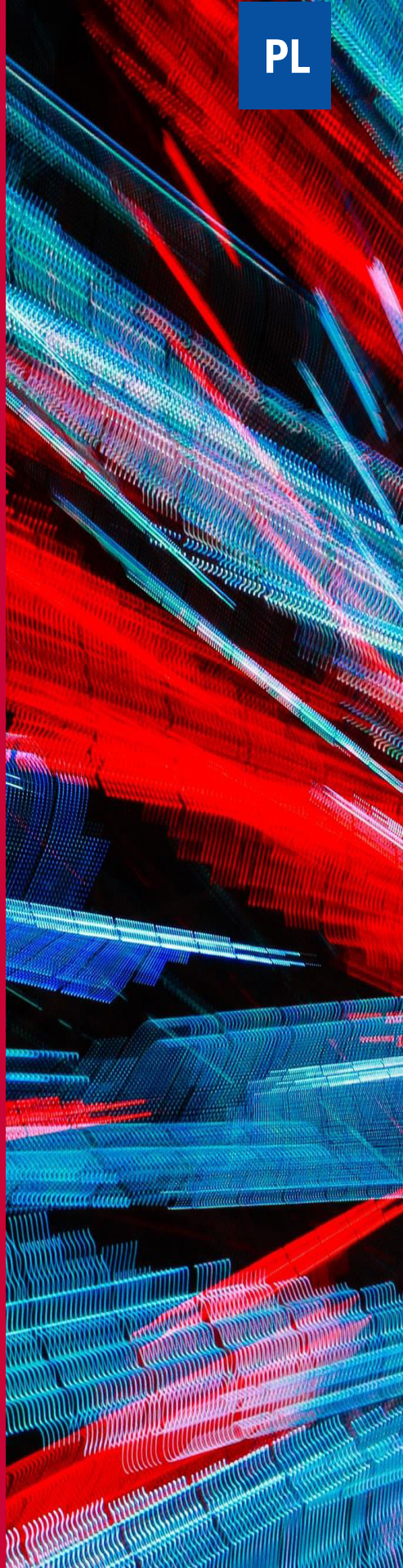
enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

PL



Od stycznia 2019 r. do kwietnia 2020 r.

Nowe trendy

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

Informacje ogólne

_Czego należy oczekiwać

Wkraczając w nową dekadę, możemy spodziewać się istotnych zmian w postrzeganiu cyberbezpieczeństwa, czyli bezpieczeństwa w cyberprzestrzeni. Cyberprzestrzeń zgodnie z definicją w normie **ISO/IEC 27032:2012**[1] to ***„złożone środowisko powstałe wskutek interakcji ludzi, oprogramowania i usług w Internecie za pomocą podłączonych do niego urządzeń technicznych i sieci, które nie istnieje w żadnej formie fizycznej”***. Ochrona tego złożonego środowiska stanie się jeszcze trudniejsza, gdy połączymy jeszcze więcej ludzi, urządzeń i systemów, i będziemy uruchamiać w nim jeszcze więcej procesów i usług. Jesteśmy również w coraz większym stopniu zależni od jego niezawodności, uczciwości, dostępności i wiarygodności w pracy, relacjach z ludźmi i wykonywaniu wielu codziennych czynności. Wraz ze wzrostem zależności pojawia się coraz więcej okazji, z których mogą skorzystać sprawcy szkodliwych działań, by manipulować, zastraszać, zwodzić, nękać oraz oszukiwać osoby fizyczne i organizacje. W ciągu najbliższej dekady nastąpi zmiana koncepcji ochrony osób fizycznych, firm i organizacji, od tradycyjnego pojmowania zabezpieczeń sieci i informacji do szerszej koncepcji obejmujące treści i usługi.

W ciągu ostatniego dziesięciolecia „czwarta rewolucja przemysłowa” spowodowała znaczne przyspieszenie tempa zmian, zmieniając to, co ludzie robią i jak to robią, jakie umiejętności są wymagane, gdzie jest wykonywana praca, jaka jest struktura relacji pracowniczych i w jaki sposób praca jest organizowana, dystrybuowana i wynagradzana.

Z powodu nadal trwającej pandemii COVID-19 wkraczamy w nową dekadę z nowymi standardami i istotnymi zmianami w świecie fizycznym i cyberprzestrzeni. Z powodu dystansowania społecznego czy ograniczeń w poruszaniu się ludzie w większym stopniu korzystają z przestrzeni wirtualnej do komunikowania się, podtrzymywania więzi i socjalizowania się. Spowoduje to pojawienie się nowych wyzwań w całym cyfrowym łańcuchu wartości, a szczególnie w branży związanej z cyberprzestrzenią.

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.

Istnieje zbyt wiele zmiennych, jakie musimy uwzględnić, by zarządzanie zagrożeniami dla cyberbezpieczeństwa było skuteczne. Ważnym czynnikiem jest techniczna różnorodność, jakiej dziś doświadcza wiele organizacji. Kolejny aspekt to stopień zaawansowania narzędzi, techniki taktyczne i procedury (TTP) wykorzystywane przez przeciwników do dokonywania ataków. Sprawcy szkodliwych działań dostosowują TTP do środowiska swoich ofiar zależnie od potrzeb i współpracują ze sobą, by osiągać cele.

Definiowanie kategorii ryzyka, zarządzanie danymi, stosowanie odpowiednich wskaźników oraz reagowanie na zmiany to przeszkody na drodze do stworzenia skutecznej strategii zarządzania zagrożeniami dla cyberbezpieczeństwa. **W kolejnym dziesięcioleciu konieczne będzie stworzenie nowych metod, które umożliwią wyzwolenie się z analizy przebiegającej w silosach i zbliżenie się do powiązanych czynników, zmiennych i warunków przypominających macierz**. Stanowi to istotne wyzwanie dla wielu organizacji próbujących chronić swoją infrastrukturę, operacje i dane przed silniejszymi, lepiej wyposażonymi i dysponującymi lepszymi zasobami przeciwnikami.

Nowe trendy

Dziesięć wyzwań dla cyberbezpieczeństwa

01_Radzenie sobie z zagrożeniami systemowymi i złożonymi.

Zagrożenia cybernetyczne charakteryzują się szybkością i skalą propagacji, jak również potencjalnymi zamiarami cyberprzestępców. Wzajemne powiązania różnych systemów i sieci umożliwiają szybkie i szeroko zakrojone rozprzestrzenianie się incydentów w sieci, co utrudnia ocenę i ograniczanie zagrożeń cybernetycznych.

02_Powszechne wykrywanie zagrożeń wykorzystujących SI.

Wykrywanie zagrożeń wykorzystujących sztuczną inteligencję do przeprowadzania ataków lub unikania wykrycia będzie stanowić istotne wyzwanie dla przyszłych systemów cyberobrony[14].

03_Zmniejszenie liczby przypadkowych błędów.

Z powodu coraz większej liczby systemów i urządzeń podłączonych do sieci przypadkowe błędy nadal są jedną z najczęściej wykorzystywanych luk w incydentach związanych z cyberbezpieczeństwem. Nowe rozwiązania, których celem jest zmniejszenie liczby tych błędów, będą stanowić istotny wkład w zmniejszenie liczby incydentów.

04_Łańcuch dostaw i zagrożenia ze strony podmiotów zewnętrznych.

Zróżnicowany łańcuch dostaw, który obecnie jest cechą przemysłu technicznego, stwarza nowe możliwości wykorzystania przez cyberprzestępców próbujących wykorzystać złożoność tych systemów oraz różnorodne luki w zabezpieczeniach, jakie wprowadza heterogeniczny ekosystem zewnętrznych dostawców[16].

05_Orkiestracja i automatyzacja zabezpieczeń.

Wywiad dotyczący cyberzagrożeń oraz analiza behawioralna zyskają na znaczeniu wraz z automatyzacją procesów i analiz. Inwestowanie w automatyzację i orkiestrację umożliwi specjalistom z dziedziny cyberbezpieczeństwa inwestycję w tworzenie solidniejszych strategii cyberbezpieczeństwa.

06_Zmniejszenie liczby fałszywych alarmów.

Ta obietnica, na spełnienie której czekamy od tak dawna, ma kluczowe znaczenie dla przyszłości branży cyberbezpieczeństwa i walki z utratą czujności spowodowaną fałszywymi alarmami.

07_Strategie bezpieczeństwa oparte na całkowitym braku zaufania.

Z powodu rosnącej presji na systemy informatyczne, związanej z wymaganiami, jakie stawiają nowe firmy, jak praca zdalna, cyfryzacja modelu biznesowego i rozproszenie danych, wielu decydentów postrzega zasadę całkowitego braku zaufania jako rzeczywiste rozwiązanie umożliwiające ochronę majątku firmy.

08_Błędy migracji do chmury przedsiębiorstwa.

Ponieważ wiele firm przenosi swoje dane do rozwiązań opartych na chmurze, liczba błędów konfiguracji zwiększy się, narażając dane na potencjalne naruszenia. Dostawcy rozwiązań chmurowych będą próbowali rozwiązać ten problem, wdrażając systemy automatycznie rozpoznające błędy tego rodzaju.

09_Zagrożenia hybrydowe.

Nowe sposoby działania przejmują zagrożenia ze świata wirtualnego i fizycznego. Na przykład szerzenie dezinformacji lub fałszywych informacji stanowi kluczowy element krajobrazu zagrożeń hybrydowych. EUvsDisinfo[15] to flagowy projekt grupy zadaniowej Europejskiej Służby Działań Zewnętrznych (ang. European External Action Service's East StratCom Task Force) stworzonej w celu zwalczania zagrożeń związanych z dezinformacją.

10_Zwiększy się atrakcyjność infrastruktury w chmurze jako celu.

Coraz powszechniejsze korzystanie z publicznej infrastruktury chmurowej zwiększy ryzyko awarii. Nieprawidłowa konfiguracja zasobów w chmurze jest nadal najważniejszym powodem ataków,
lecz wśród hakerów zyskują na popularności ataki wymierzone bezpośrednio w dostawców usług chmurowych.

Nowe trendy

Wydatki na cyberbezpieczeństwo

Według firmy Gartner[17] wiele zarządów będzie się domagać lepszej jakości danych i wykazania korzyści po latach intensywnego inwestowania w cyberbezpieczeństwo. Jest to głównie spowodowane wzrostem wydatków na cyberbezpieczeństwo, proporcjonalnie do inwestycji w nowe technologie. Zgodnie z raportem firmy IDC[22] wydatki na cyberbezpieczeństwo sięgnęły osiągnęły wartość 103 mld USD (ok. 87,5 mld EUR) w 2019 r., co stanowi wzrost o 9,4% w stosunku do poprzedniego roku. Menedżerowie ds. bezpieczeństwa zostaną wkrótce rozliczeni z wyników uzyskanych z lat inwestycji i konieczne będzie dalsze przedstawianie udoskonalonych danych na temat uzyskanych rezultatów.

Wywiad dotyczący cyberzagrożeń pomoże w stworzeniu strategii cyberbezpieczeństwa

Wywiad dotyczący cyberzagrożeń (CTI) ma na celu pomaganie organizacjom w lepszym przygotowaniu dzięki poszerzaniu wiedzy na temat krajobrazu zagrożeń. Zamiast opierać się wyłącznie na informacjach generowanych przez wewnętrzne systemy lub kanały (co wiemy o tym, co znamy), skuteczność CTI zostanie określona poprzez wiedzę na temat tego, *dlaczego*, *jak* i *czego* jeszcze nie wie zespół ds. cyberbezpieczeństwa. Wartościową propozycją dotyczącą dowolnej zdolności lub programu CTI jest poprawa gotowości organizacji do ochrony jej zasobów o znaczeniu krytycznym przed nieznanymi zagrożeniami.

Poznanie krajobrazu zagrożeń

W związku ze wzrostem automatyzacji i orkiestracji bezpieczeństwa **zespoły ds. cyberbezpieczeństwa będą spędzać mniej czasu na działaniach związanych z monitorowaniem, a więcej na zadaniach związanych z gotowością i przygotowaniem**. Dobrze zaplanowane możliwości CTI mogą zapewnić opartą na kontekście i użyteczną wiedzę na temat zagrożeń, która umożliwi informowanie strategicznych, operacyjnych i taktycznych interesariuszy w całej organizacji. Pod względem praktycznym zdolność CTI powinna mieć na celu udzielenie odpowiedzi na poniższe pytania dotyczące wymagań interesariuszy oraz kontekstu organizacji i środowiska:

- Jaka jest powierzchnia ataku?
- Jakie są najcenniejsze aktywa firmy i jej obszar cybernetyczny?
- Jakie są najbardziej istotne luki w zabezpieczeniach?
- Jakie są najczęściej używane wektory ataku?
- Jak zwykle zachowują się i działają przeciwnicy?
- Jak wygląda krajobraz zagrożeń w przypadku:
    - sektora i rodzaju branży, w jakich działa firma?
    - środowiska technicznego przyjętego przez organizację?
- Kto powinien podjąć działania i co należy zrobić, by zmniejszyć ryzyka związane z tymi zagrożeniami?

Zbyt małe umiejętności w zakresie cyberbezpieczeństwa

Brak wysoko wykwalifikowanych specjalistów już teraz stanowi problem dla europejskich ambicji związanych z cyfryzacją. Według wyników badania[23] ponad 70% firm europejskich informuje, że brak umiejętności utrudnia im realizację strategii inwestycyjnych, podczas gdy 46% firm zgłasza trudności w obsadzaniu wolnych stanowisk z powodu braku umiejętności w kluczowych obszarach, takich jak cyberbezpieczeństwo.

Nowe trendy

Pięć trendów dotyczących cyberzagrożeń

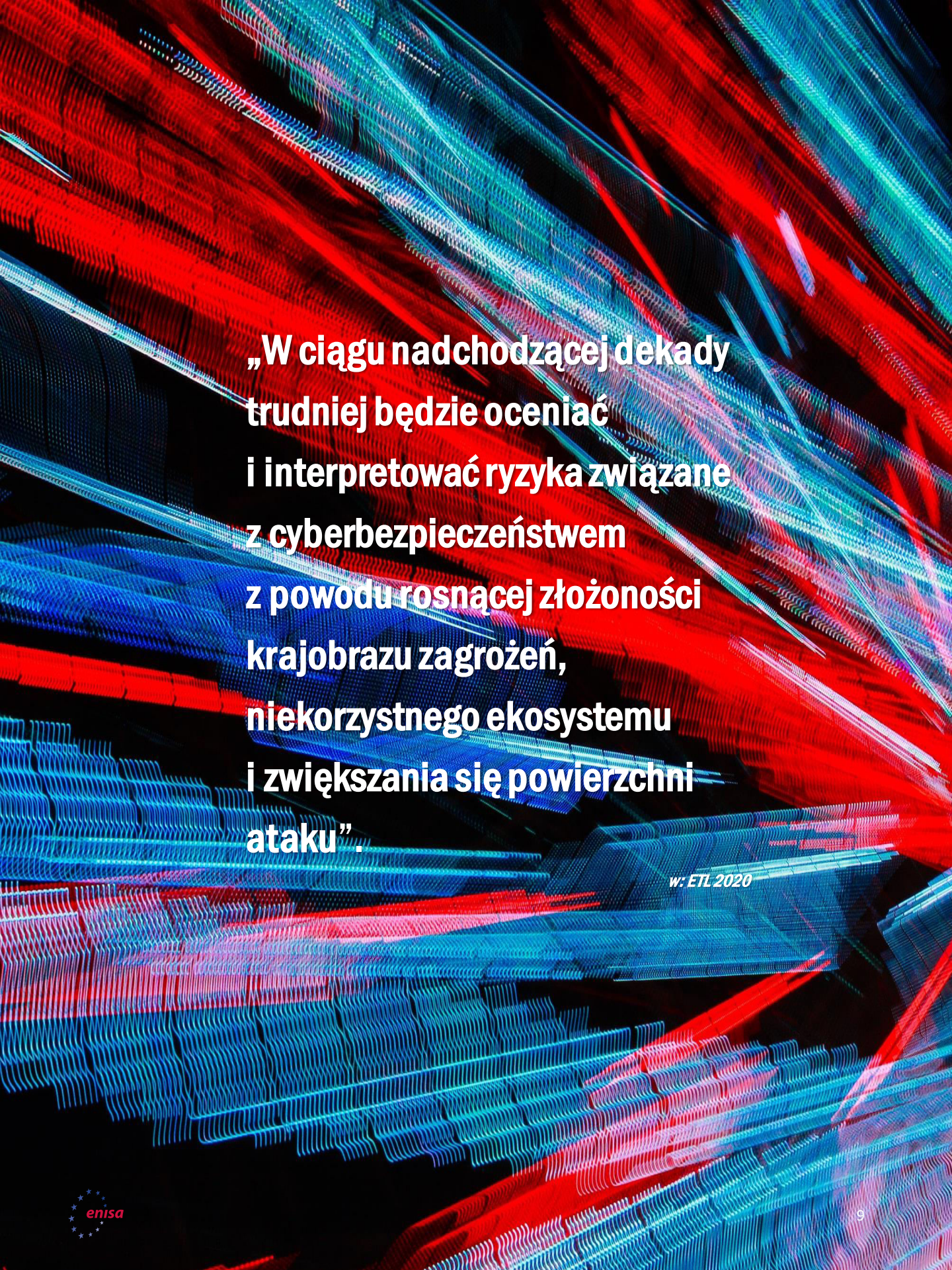
01_Złośliwe oprogramowanie jest coraz lepsze. Odmiany złośliwego oprogramowania są aktualizowane do nowych wersji zawierających nowe funkcje oraz mechanizmy dystrybucji i rozpowszechniania. Na przykład Emotet, złośliwe oprogramowanie stworzone pierwotnie jako bankowy koń trojański w 2014 r., stało się jednym z najbardziej skutecznych dystrybutorów złośliwego oprogramowania w 2019 r.[2]

02_Zagrożenia zostały dostosowane do urządzeń mobilnych. Użytkownicy są w coraz większym stopniu zależni od urządzeń mobilnych, których używają do uzyskiwania dostępu do najbardziej poufnych kont. Jednym z przykładów jest użycie uwierzytelniania wielopoziomowego powiązanego z aplikacją uwierzytelniającą lub za pomocą wiadomości tekstowej. Ponieważ coraz więcej złośliwych programów jest całkowicie dostosowanych do urządzeń mobilnych, oszukańcze aplikacje, przejmowanie kart SIM i exploity systemów operacyjnych sprawiają, że urządzenia te stanowią najsłabsze ogniwo, a co za tym idzie – są wyjątkowo podatne na ataki.

03_Przestępcy wykorzystują nowe rodzaje plików, jak pliki obrazów dyskowych (ISO i IMG), do rozpowszechniania złośliwego oprogramowania. Pliki DOC, PDF, ZIP i XLS są nadal najpopularniejszymi rodzajami plików służącymi do rozpowszechniania złośliwego oprogramowania, lecz inne rodzaje zyskują na popularności. W 2019 r. odkryto, że kilka kampanii rozprowadzających programy AgentTesla InfoStealer i NanoCore RAT wykorzystywało pliki obrazów.

04_Wzrost liczby ataków celowanych i skoordynowanych z użyciem oprogramowania ransomware. W 2019 r. doszło do eskalacji liczby exploitów wyrafinowanego i celowanego oprogramowania ransomware w sektorze publicznym, organizacjach ochrony zdrowia i niektórych branżach ze szczytu listy. Przestępcy przeznaczają więcej czasu na działania wywiadowcze wymierzone w ofiarę, doskonale zatem wiedzą, co należy zaszyfrować, przez co osiągają maksymalną uciążliwość i wyższe kwoty okupu.

05_Upowszechnią się ataki z użyciem „wypychania poświadczeń”. „Wypychanie poświadczeń” – automatyczne wstrzykiwanie wykradzionych kombinacji nazwy użytkownika i hasła za pomocą dużych, zautomatyzowanych zapytań o logowanie skierowanych do aplikacji internetowej – będzie się upowszechniać w skutek wyjątkowo dużej liczby naruszeń bezpieczeństwa danych w ciągu ostatniej dekady i bilionów wykradzionych rekordów danych osobowych.


„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

Nowe trendy

Dziesięć nowych trendów dotyczących wektorów ataku

01_ Ataki będą się odbywać na skalę masową w krótkim czasie i charakteryzować się większym oddziaływaniem

Celem tych ataków jest dotarcie do jak największej liczby urządzeń mogących wykraść dane osobowe lub zablokować dostęp do danych poprzez zaszyfrowanie plików.

02_ Precyzyjnie ukierunkowane i uporczywe ataki będą skrupulatnie planowane, z dobrze określonymi i długoterminowymi celami

Sprawcy szkodliwych działań planują ataki tego rodzaju, by dotrzeć do danych o dużej wartości, jak informacje finansowe, materiały chronione prawem własności intelektualnej, tajemnice handlowe, informacje zastrzeżone itp.

03_ Sprawcy szkodliwych działań będą wykorzystywać platformy cyfrowe do ataków celowanych

Sprawcy szkodliwych działań będą badać potencjał cyfrowych platform w zakresie wspierania ataków celowanych (np. media społecznościowe, gry, przesyłanie wiadomości, przesyłanie strumieniowe itp.). Od kradzieży danych osobowych z użyciem techniki spear-phishing po szeroką dystrybucję złośliwego oprogramowania, platformy cyfrowe z dużą liczbą subskrybentów stanowią skuteczne wektory ataku, zyskujące na popularności pośród sprawców szkodliwych działań.

04_ Wykorzystywanie procesów biznesowych ulegnie zwiększeniu

Z powodu rozwoju automatyzacji i mniejszej liczby ludzkich interwencji procesy biznesowe będą narażone na złośliwe zmiany w celu generowania zysków na rzecz przestępców. Technika ta, znana jako Business Process Compromise (BPC), jest często niedoceniana przez specjalistów w dziedzinie inżynierii procesów z powodu braku właściwej oceny ryzyka.

05_ Powierzchnia ataku będzie się nadal powiększać

Poczta e-mail nie jest już podstawowym i jedynym narzędziem i najczęściej wykorzystywanym wektorem w przypadku wyłudzania danych. Sprawcy szkodliwych działań wykorzystują teraz inne platformy do komunikowania się i przyciągają ofiary na niebezpieczne witryny internetowe. Nowe trendy pojawiają się wraz z upowszechnianiem się wiadomości SMS, aplikacji WhatsApp i SnapChat oraz komunikatorów serwisów społecznościowych.

06_ Praca zdalna ułatwi ataki z użyciem urządzeń domowych

Ponieważ coraz więcej osób pracuje zdalnie i łączy swoje urządzenia z sieciami firmowymi, rośnie ryzyko powstania nowych punktów ataku, z jakich mogą skorzystać przestępcy. Z powodu pandemii COVID-19 trend ten wymusi na menedżerach ds. IT zaostrzenie zasad bezpieczeństwa i wprowadzenie pilnych zmian w infrastrukturze IT.

07_ Przestępcy będą coraz lepiej przygotowani

Przestępcy ostrożnie dobierają cele, przeprowadzają wywiad skierowany przeciwko konkretnym pracownikom i dokonują ataku z użyciem techniki „spear-phishing" w celu uzyskania użytecznych poświadczeń, które następnie mogą posłużyć do ataku na organizację. Gdy przestępcy uzyskają dostęp do konkretnego urządzenia, mogą zastosować narzędzia do testowania z użyciem penetracji, jak Mimikatz, by zbierać i wykorzystywać poświadczenia umożliwiające uzyskanie przywilejów wyższego poziomu.

08_ Techniki zaciemniania staną się bardziej wyrafinowane

Sprawcy zagrożeń nieustannie wprowadzają innowacje, by zagrożenia stawały się bardziej skuteczne i mniej podatne na wykrycie. Anibus, bankowy koń trojański dla systemu Android i bot, był rozprowadzany jako niewinnie wyglądająca aplikacja, głównie za pośrednictwem sklepu Google Play.[1]

09_ Wzrośnie liczba zautomatyzowanych ataków na systemy, do których nie wprowadzono poprawek, i na wycofane aplikacje

Zaobserwowany w 2019 r. nietypowy wzrost ruchu w usłudze Telnet na porcie 445 ujawnił ekspansję robaków i exploitów, jak Eternal Blue. W tym okresie zaobserwowano rekordowy ruch związany z usługą Telnet, która obecnie jest używana wyłącznie w przypadku urządzeń IoT.

10_ Zagrożenia cybernetyczne przesuwają się w stronę krawędzi systemów

Urządzenia brzegowe to takie, które znajdują się na granicach między połączonymi sieciami. Obserwujemy rosnący trend, w ramach którego ataki na te urządzenia – takie jak routery, switche i zapory – mają znaczący wpływ na przedsiębiorstwo i podłączony do niego cyfrowy ekosystem.

Bibliografia

1. „ISO/IEC 27032:2012". ISO. https://www.iso.org/standard/44375.html

2. „Triple Threat: Emotet Deploys TrickBot to Steal Data & Spread Ryuk". 2 kwietnia 2019 r. Cybereason. https://www.cybereason.com/blog/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware

3. „Understanding the relationship between Emotet, Ryuk and TrickBot". 14 kwietnia 2019 r. Intel471. https://blog.intel471.com/2020/04/14/understanding-the-relationship-between-emotet-ryuk-and-trickbot/

4. „Investigating WMI Attacks", 9 lutego 2019 r. SANS. https://www.sans.org/blog/investigating-wmi-attacks/

5. „RDP Abuse and Swiss Army Knife Tool Used to Pillage, Encrypt and Manipulate Data", 18 grudnia 2019 r. Bitdefender. https://labs.bitdefender.com/2019/12/rdp-abuse-and-swiss-army-knife-tool-used-to-pillage-encrypt-and-manipulate-data/

6. „Europe's huge privacy fines against Marriott and British Airways are a warning for Google and Facebook", 10 lipca 2019 r. CNBC. https://www.cnbc.com/2019/07/10/gdpr-fines-vs-marriott-british-air-are-a-warning-for-google-facebook.html

7. „This is how we might finally replace passwords", 27 maja 2019 r. C | Net. https://www.cnet.com/news/this-is-how-we-might-finally-replace-passwords/

9. „Authentication standards to help reduce the world's over-reliance on passwords". FIDO. https://fidoalliance.org/overview/

10. „How Much Cyber Sovereignty is Too Much Cyber Sovereignty?" 3 października 2019 r. Council on Foreign Relations. https://www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty

11. „Conceptualising Cyber Arms Races". 2016. NATO. https://ccdcoe.org/uploads/2018/10/Art-10-Conceptualising-Cyber-Arms-Races.pdf

12. „Journalism, 'Fake News' and Disinformation: A Handbook for Journalism Education and Training" 2018 r. UNESCO. https://en.unesco.org/fightfakenews

13. „The Big Connect: How Data Science is Helping Cybersecurity". 12 czerwca 2019 r. Info Security Group. https://www.infosecurity-magazine.com/blogs/data-science-helping-cybersecurity-1/

14. „Are You Ready For The Age Of Adversarial AI? Attackers Can Leverage Artificial Intelligence Too". 9 stycznia 2020 r. Forbes. https://www.forbes.com/sites/forbestechcouncil/2020/01/09/are-you-ready-for-the-age-of-adversarial-ai-attackers-can-leverage-artificial-intelligence-too/#2a76dee14703

15. https://euvsdisinfo.eu/

16. „FBI Alerts Companies of Cyber Attacks Aimed at Supply Chains". 21 lutego 2020 r. Bitsight. https://www.bitsight.com/blog/fbi-alerts-companies-of-cyber-attacks-supply-chains

17. „Gartner Identifies the Top Seven Security and Risk Management Trends for 2019". 5 marca 2019 r. Gartner. https://www.gartner.com/en/newsroom/press-releases/2019-03-05-gartner-identifies-the-top-seven-security-and-risk-ma

18. „Android banking trojan". 3 października 2019 r. Cyare https://cyware.com/news/exploring-the-nature-and-capabilities-of-anubis-android-banking-trojan-6ea7dec4

19. „5 Top Trends for Mobile Cyber Security in 2020". 9 stycznia 2020 r. Corrata. https://corrata.com/5-top-trends-for-mobile-cyber-security-in-2020/

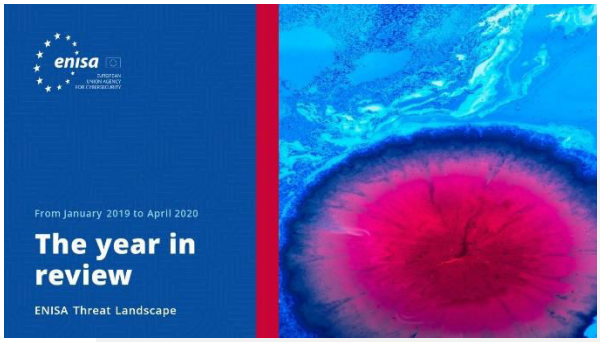
20. „Malicious Attachments Remain a Cybercriminal Threat Vector Favorite". 27 sierpnia 2020 r. Threat Post. https://threatpost.com/malicious-attachments-remain-a-cybercriminal-threat-vector-favorite/158631/

21. „10 trends shaping the future of work". Październik 2019 r. EPS. https://op.europa.eu/en/publication-detail/-/publication/e77a1580-0cf5-11ea-8c1f-01aa75ed71a1/language-en/format-PDF/source-121729338

22. „Global security spending to top $103 billion in 2019, says IDC", 20 marca 2019 r. ZDNet. https://www.zdnet.com/article/global-security-spending-to-top-103-billion-in-2019-says-idc/

23. „Insights into skills shortages and skills mismatch. learning from Cedefop's European skills and jobs survey". 2018 r. CEDEFOP. https://www.cedefop.europa.eu/files/3075_en.pdf

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**

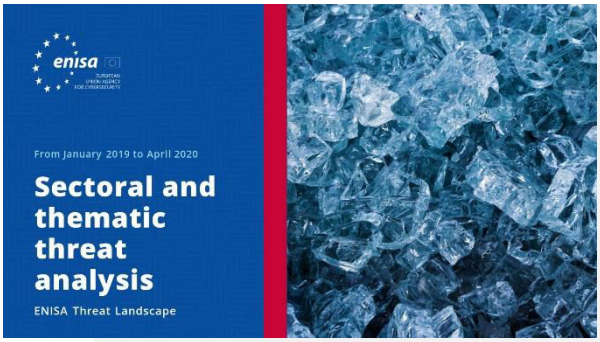
Agencja ENISA: wykaz piętnastu największych zagrożeń w okresie od stycznia 2019 r. do kwietnia 2020 r.

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



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.

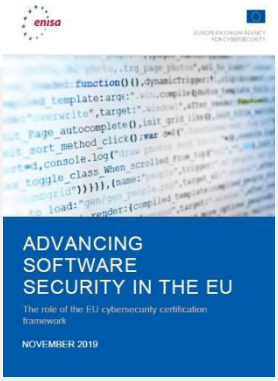
PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń **Omówienie kwestii rozpoznawania cyberzagrożeń**

Aktualny stan wywiadu dotyczącego cyberzagrożeń w UE.

PRZECZYTAJ RAPORT

Inne publikacje



Zwiększanie bezpieczeństwa oprogramowania w UE

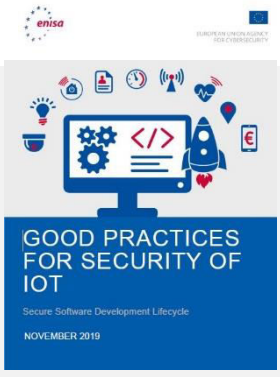
Przedstawia kluczowe elementy bezpieczeństwa oprogramowania i oferuje zwięzły przegląd najistotniejszych dotychczasowych metod i standardów w sferze bezpiecznego rozwoju oprogramowania.

PRZECZYTAJ RAPORT

Dobre praktyki ENISA dotyczące bezpieczeństwa inteligentnych samochodów

Dobre praktyki dotyczące bezpieczeństwa inteligentnych samochodów, a mianowicie połączonych i (pół)autonomicznych pojazdów, mające na celu poprawę wrażeń użytkowników i bezpieczeństwa samochodów.

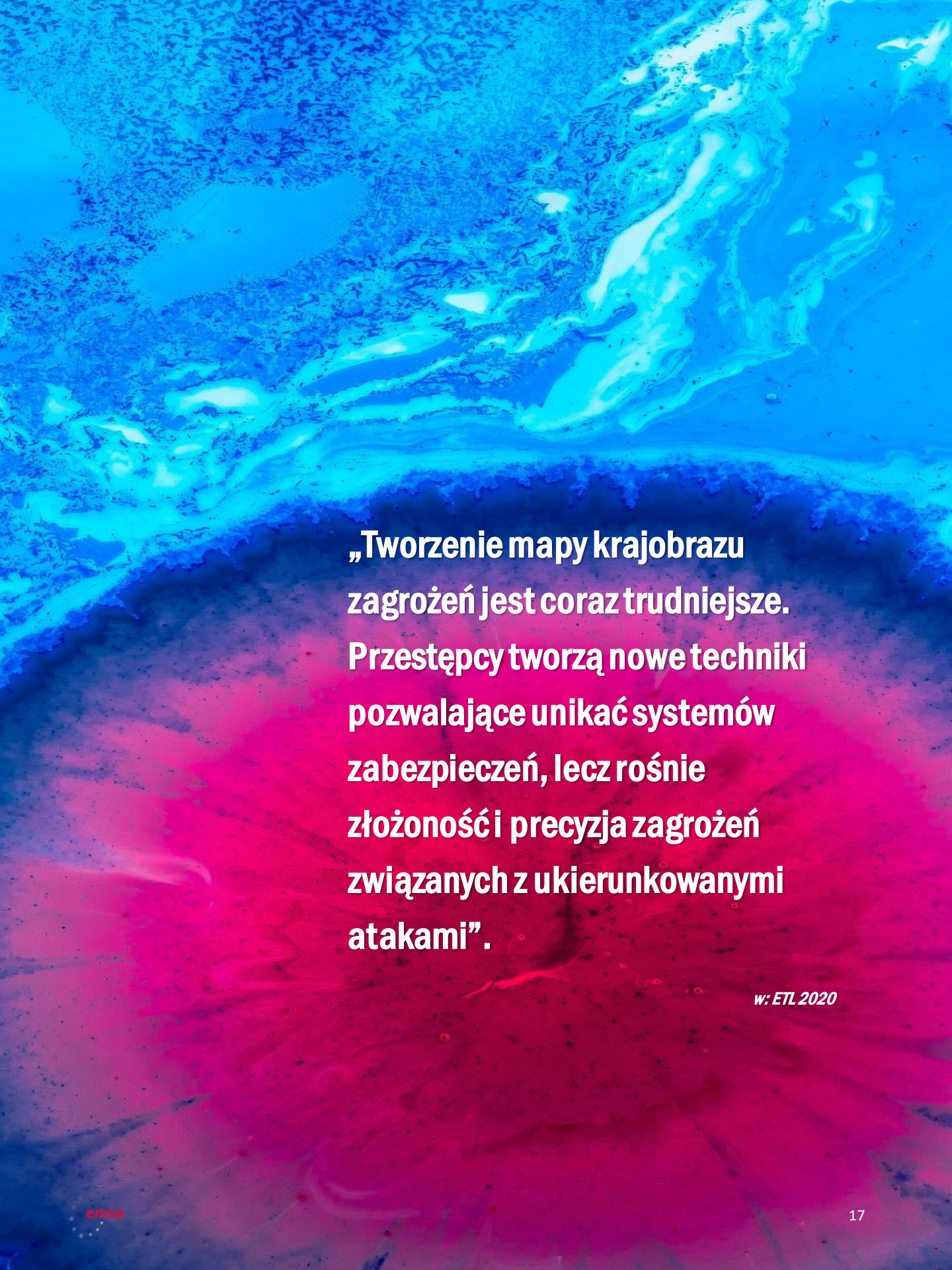
PRZECZYTAJ RAPORT



Dobre praktyki dotyczące bezpieczeństwa IoT – cykl życia tworzenia bezpiecznego oprogramowania

Bezpieczeństwo IoT ze szczególnym uwzględnieniem wytycznych dotyczących tworzenia oprogramowania.

PRZECZYTAJ RAPORT



„Tworzenie mapy krajobrazu zagrożeń jest coraz trudniejsze. Przestępcy tworzą nowe techniki pozwalające unikać systemów zabezpieczeń, lecz rośnie złożoność i precyzja zagrożeń związanych z ukierunkowanymi atakami”.

w: ETL 2020

Informacje o age

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

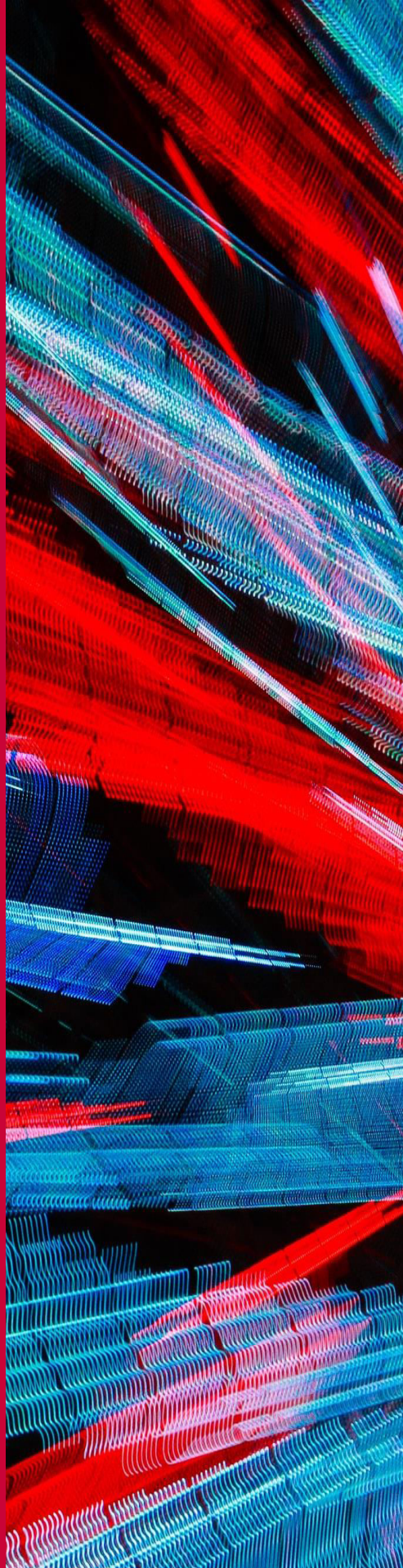
Informujemy, że niniejsza publikacja przedstawia poglądy i interpretacje ENISA, o ile nie stwierdzono inaczej. Niniejsza publikacja nie powinna być interpretowana jako działanie prawne ENISA ani organów ENISA, chyba że została przyjęta zgodnie z rozporządzeniem (UE) nr 526/2013. Niniejsza publikacja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



https://www.enisa.europa.eu