enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

PL

Od stycznia 2019 r. do kwietnia 2020 r.

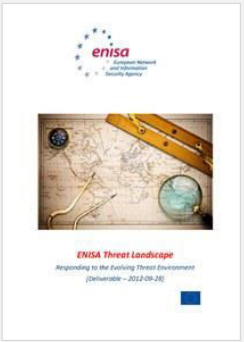
Przegląd roczny

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

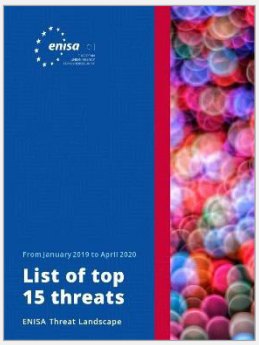
Na początek

_ Osiem lat obserwacji krajobrazu zagrożeń

W tym roku **Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)** obchodzi rocznicę wejścia w życie nowego aktu o cyberbezpieczeństwie i publikuje ósmą edycję raportu Krajobraz zagrożeń (Threat Landscape Report – ETL). Akt o cyberbezpieczeństwie[1] zmienia i umacnia rolę ENISA, przyznając jej stałe uprawnienia, więcej zasobów i nowe zadania. Agencja wkracza ponadto w nowy rozdział dzięki nowemu dyrektorowi wykonawczemu, nowej strategii i nowej strukturze organizacyjnej. W obliczu wszystkich tych zmian nadszedł również czas na zmiany w raporcie ETL: wprowadzenie nowej struktury, zapewnianie nowoczesnego charakteru i wyglądu, odejście od obszernego i statycznego raportu. Nowa identyfikacja wizualna i format sprawią, że raport ETL stanie się wszechstronnym, dynamicznym i łatwym w użyciu raportem cyfrowym, podejmującym próbę spełnienia oczekiwań coraz liczniejszych i coraz bardziej wymagających odbiorców.



ETL 2012



ETL 2020

Krajobraz zagrożeń wg Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA): na przestrzeni lat 2012 – 2020

Format raportu ETL

W tym wydaniu omówiono krajobraz zagrożeń w okresie od stycznia 2019 do kwietnia 2020 według poniższej struktury.

PRZEGLĄD ROCZNY. W niniejszym raporcie przedstawiono ogólne informacje na temat krajobrazu zagrożeń, w tym najważniejszych zagadnień wymienionych w pozostałych raportach. Przedstawiono również piętnaście największych zagrożeń wytypowanych przez ENISA, wnioski oraz zalecenia.

OMÓWIENIE KWESTII ROZPOZNAWANIA CYBERZAGROŻEŃ. Raport ten stanowi podsumowanie najważniejszych tematów dotyczących społeczności rozpoznawania cyberzagrożeń (CTI) oraz omawianych na różnych forach.

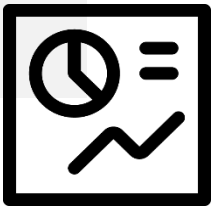
SEKTOROWA I TEMATYCZNA ANALIZA ZAGROŻEŃ. Raport ten podsumowuje najnowsze prace prowadzone przez ENISA i opisuje krajobraz zagrożeń dla poszczególnych sektorów i technologii. W tym roku przedstawiamy wnioski z prac dotyczących technologii 5G, internetu rzeczy (IoT) oraz inteligentnych samochodów.

NAJWAŻNIEJSZE INCYDENTY W UE I NA ŚWIECIE. W raporcie tym omówiono najważniejsze incydenty związane z cyberbezpieczeństwem, do jakich doszło w UE i na świecie, z podkreśleniem wniosków, jakie można wyciągnąć na ich podstawie.

TEMATYKA BADAŃ. W tym raporcie przedstawiono kluczowe aspekty dotyczące badań i innowacji w dziedzinie cyberbezpieczeństwa.

NOWE TRENDY. W tym raporcie zidentyfikowano nowe trendy i skupiono się na przyszłych wyzwaniach i możliwościach w sektorze cyberbezpieczeństwa.

WYKAZ PIĘTNASTU NAJWIĘKSZYCH ZAGROŻEŃ. Po jednym raporcie dla każdego zagrożenia, z przedstawieniem opisu ogólnego, wniosków, najważniejszych incydentów, danych statystycznych, wektorów ataku i odpowiadających im metod ograniczenia ryzyka.



Na początek

Metodologia

Treści tworzone z myślą o raporcie ETL opierają się na publicznie dostępnych źródłach informacji, głównie o charakterze strategicznym, i dotyczą więcej niż jednego sektora, technologii czy kontekstu. Przy sporządzaniu raportu staraliśmy się zachować neutralność wobec branż i dostawców, odnosi się on więc lub cytuje prace dotyczące różnych badań związanych z bezpieczeństwem, blogi na temat bezpieczeństwa i artykuły prasowe, jednoznacznie zidentyfikowane w tekście przy użyciu licznych przypisów końcowych.

Tworząc raport ENISA o krajobrazie zagrożeń, zastosowaliśmy podejście dwutorowe. Po pierwsze, przeprowadziliśmy dogłębną analizę dostępnego piśmiennictwa z publicznie dostępnych źródeł, jak artykuły prasowe, ekspertyzy, raporty wywiadowcze, analizy incydentów i raporty z badań bezpieczeństwa. Po drugie, przeprowadziliśmy rozmowy z członkami grup interesariuszy ETL, którzy są ekspertami w tej dziedzinie oraz członkami społeczności Cyber Threat Intelligence (CTI) w UE. Drugie z tych działań pomogło nam stworzyć wykaz piętnastu największych zagrożeń i dokonać oceny założeń dotyczących trendów i przyszłych wyzwań związanych cyberbezpieczeństwem.

Pragniemy równie podziękować członkom grupy interesariuszy CTI za całe wsparcie, jakie nam oferowali podczas tworzenia wszystkich ośmiu edycji tego raportu. Członkowie tej grupy oceniają i weryfikują analizy tworzone z myślą o każdym raporcie ETL oraz wybierają piętnaście największych zagrożeń dla bezpieczeństwa cyfrowego w minionym roku.

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

Kto powinien zapoznać się z poszczególnymi częściami

Raport ETL ma częściowo charakter strategiczny, a częściowo techniczny, i zawiera informacje interesujące zarówno dla czytelników zainteresowanych technologiami, jak i innych. Raport ETL jest skierowany do różnych odbiorców i operuje językiem technicznym na różnych poziomach, w zależności od dziedziny i znaczenia tematu dla czytelników bez wiedzy technicznej. W poniższej tabeli opisano rodzaje odbiorców i treści dla każdego raportu ETL.

RAPORT ETL	RODZAJ TREŚCI	DOCELOWI ODBIORCY
OCENIANY ROK	Ogólne	Wszyscy
OMÓWIENIE CTI	Szczegółowe	Członkowie społeczności CTI i praktycy.
SEKTOROWA I TEMATYCZNA ANALIZA ZAGROŻEŃ	Strategiczne	Eksperci ds. zarządzania strategicznego, twórcy polityki i decydenci, analitycy ryzyka, menedżerowie i liderzy z dziedziny cyberbezpieczeństwa.
NAJWAŻNIEJSZE INCYDENTY W UE I NA ŚWIECIE	Strategiczne	Eksperci ds. zarządzania strategicznego, twórcy polityki i decydenci, analitycy ryzyka, menedżerowie i liderzy z dziedziny zarządzania ryzykiem.
TEMATYKA BADAŃ	Strategiczne	Eksperci ds. zarządzania strategicznego, twórcy polityki i decydenci, analitycy ryzyka, menedżerowie i liderzy z dziedziny zarządzania ryzykiem.
NOWE TRENDY	Strategiczne	Eksperci ds. zarządzania strategicznego, twórcy polityki i decydenci, analitycy ryzyka, menedżerowie i liderzy z dziedziny zarządzania ryzykiem.
WYKAZ PIĘTNASTU NAJWIĘKSZYCH ZAGROŻEŃ	Techniczne	Menedżerowie ds. bezpieczeństwa informacji (ISM), dyrektorzy ds. bezpieczeństwa informacji (CISO), specjaliści ds. cyberbezpieczeństwa i analitycy CTI.

Piętnaście największych zagrożeń

Największe zagrożenia, 2018		Ocenione trendy
1	Złośliwe oprogramowanie	---
2	Ataki przez strony internetowe	↗
3	Ataki oparte na aplikacjach sieciowych	---
4	Wyłudzanie informacji (phishing)	↗
5	Odmowa usługi (DoS)	↗
6	Spam	---
7	Botnety	↗
8	Naruszenia bezpieczeństwa danych	↗
9	Zagrożenie wewnętrzne	↙
10	Ingerencja fizyczna, uszkodzenie, kradzież i utrata	---
11	Wyciek informacji	↗
12	Kradzież tożsamości	↗
13	Cryptojacking	↗
14	Oprogramowanie ransomware	↙
15	Szpiegostwo w sieci	↙

Największe zagrożenia, 2019–2020		Ocenione trendy	Zmiana w rankingu
1	Złośliwe oprogramowanie	---	---
2	Ataki przez strony internetowe	---	↗
3	Wyłudzanie informacji (phishing)	↗	↗
4	Ataki oparte na aplikacjach sieciowych	---	↙
5	Spam	↙	↗
6	Odmowa usługi (DoS)	↙	↙
7	Kradzież tożsamości	↗	↗
8	Naruszenia bezpieczeństwa danych	---	---
9	Zagrożenie wewnętrzne	↗	---
10	Botnety	↙	↙
11	Ingerencja fizyczna, uszkodzenie, kradzież i utrata	---	↙
12	Wyciek informacji	↗	↙
13	Oprogramowanie ransomware	↗	↗
14	Szpiegostwo w sieci	↙	↗
15	Złośliwe wydobywanie kryptowalut (cryptojacking)	↙	↙

Legenda: Trendy: ↙ Malejący, --- Stabilny, ↗ Rosnący **Ranking:** ↗ W górę, --- Bez zmian, ↙ W dół

Informacje ogólne

Co się zmieniło w krajobrazie

Lata 2019 i 2020 przyniosły znaczne zmiany w krajobrazie zagrożeń cybernetycznych opisanych w tych raportach. Do powstania tych zmian przyczyniły się dwa odrębne fakty: unikatowe z historycznego punktu widzenia siły błyskawicznej transformacji uwolnione przez **pandemię koronawirusa 2019 (COVID-19)** oraz ciągły trend wzrostowy w sferze **zaawansowanych możliwości działania przeciwników w przypadku twórców zagrożeń**. Co istotne, ten drugi przyczynił się do zwiększenia wpływu pandemii COVID-19 w cyberprzestrzeni.

Pandemia COVID-19 wymusiła na szeroką skalę wprowadzanie technologii w celu stawienia czoła różnym krytycznych aspektom kryzysu, jak koordynacja usług opieki zdrowotnej, międzynarodowa reakcja na rozprzestrzenianie się COVID-19, wdrażanie systemów pracy zdalnej, nauczanie na odległość, komunikacja międzyludzka, kontrola środków blokady gospodarki, telekonferencje i wiele innych. W obliczu tej sytuacji liderzy przedsiębiorstw ocenili nowo powstałe ryzyka związane z błyskawicznym wprowadzaniem zmian (technicznych), które wynikły z transformacji wymuszonej pandemią COVID-19[2]. Zaś sfera **cyberbezpieczeństwa stanęła w obliczu paradoksu: z transformacją wiązały się zarówno wyzwania, jak i możliwości**. Zmiany wymuszone przez krajobraz informatyczny (IT) osłabiły istniejące środki cyberbezpieczeństwa, przez co błyskawiczne ich wprowadzanie stało się wyzwaniem. Równocześnie **cyberbezpieczeństwo jest czynnikiem ułatwiającym rozwijanie zaufania w przypadku nowych przypadków użycia usług cyfrowych, a zatem może ułatwiać transformację.**

W przypadku pracy zdalnej **specjaliści w dziedzinie cyberbezpieczeństwa musieli dostosować istniejące zabezpieczenia** do nowego paradygmatu infrastruktury, podejmując próby minimalizacji narażenia na różnorodne nowe rodzaje ataków, dla których punktami dostępu są połączeni przez internet pracownicy przebywający w domach i inne urządzenia inteligentne. W tym samym czasie i pod presją musieli oni wdrożyć rozwiązania oparte na komponentach cieszących się dotąd mniejszym zaufaniem, jak dostęp zdalny z użyciem publicznej sieci Internet, usługi chmurowe, niezabezpieczone usługi przesyłania strumieniowego, jak również urządzenia i aplikacje mobilne. Niezbędne sposoby reagowania na pandemię COVID-19, które miały na celu zagwarantowanie bezpieczeństwa i równocześnie zmniejszenie jej wpływu na działalność firm sprawiły, że firmy zostały zmuszone do ekstremalnych wysiłków związanych z reagowaniem na zmiany. Ponadto liczne sposoby działania szybko dostosowano do zmiennych trybów pracy, **profesjonaliści w dziedzinie bezpieczeństwa szybko odkryli, że osiągnęli kres swoich możliwości**.

Dysponując bardzo krótkim czasem realizacji, specjaliści w dziedzinie bezpieczeństwa informatycznego musieli szybko reagować na wyzwania, jakie pojawiły się wraz z wprowadzeniem pracy z domu, jak przesyłanie danych przedsiębiorstwa w przypadkach, gdy pracownicy wykorzystują domowe łącze internetowe w celu uzyskania dostępu do aplikacji chmurowych, oprogramowania firmowego, wideokonferencji i udostępniania plików.

Ponieważ pandemia COVID-19 nie została jeszcze całkowicie opanowana i nie wiemy, co przyniesie przyszłość, przewiduje się, że specjaliści w dziedzinie cyberbezpieczeństwa nadal będą musieli stawiać czoła wyzwaniom. Ponadto, jeśli uwzględnić czas, jaki mija od incydentu do jego wykrycia i przeanalizowania, sytuacja ta będzie pozostawiać ślad na krajobrazie zagrożeń jeszcze przez długi czas. Pandemia COVID-19 ujawniła, że sprawcy szkodliwych działań dysponują możliwością szybkiego dostosowania się do tych zmian. W latach 2019–2020 sposoby działania przeciwników skupiały się na personalizacji wektorów ataku. Zaawansowane metody kradzieży poświadczeń, ataki typu „wypychanie poświadczeń", ataki oparte na phishingu ze starannie wybranym celem, ataki z wykorzystaniem metod zaawansowanej inżynierii społecznej, zaawansowane techniki ukrywania złośliwego oprogramowania oraz szersza penetracja platform mobilnych to główne osiągnięcia przeciwników w okresie objętym raportem. Jeśli cyberprzestępcy zaczną łączyć te nowości ze sztuczną inteligencją i uczeniem maszynowym, w przyszłości doświadczymy wzrostu liczby udanych ataków i niewykrywalnych kampanii.

Informacje ogólne

_ Podsumowanie

Poniższa lista stanowi podsumowanie głównych trendów zaobserwowanych w krajobrazie cyberzagrożeń w okresie objętym raportem. Omówiono je także w poszczególnych raportach składających się na krajobraz zagrożeń w roku 2020.

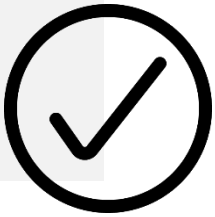
01_ **Powierzchnia ataku w dziedzinie cyberbezpieczeństwa nadal się powiększa, gdy wkraczamy w nową fazę transformacji cyfrowej.**

02_ **Po ustaniu pandemii COVID-19 wytworzą się nowe normy społeczne i ekonomiczne, w jeszcze większym stopniu zależne od bezpiecznej i niezawodnej cyberprzestrzeni.**

03_ **Wykorzystanie serwisów społecznościowych do ukierunkowanych ataków to wyraźny trend widoczny w różnych dziedzinach i rodzajach zagrożeń.**

04_ **Precyzyjnie ukierunkowane i uporczywe ataki dotyczące danych wysokiej wartości (np. dotyczących własności intelektualnej i tajemnic państwowych) są starannie planowane i wykonywane przez sprawców sponsorowanych przez struktury państwowe.**

05_ **Ataki na szeroką skalę i o krótkim czasie trwania i znacznym oddziaływaniu są stosowane z myślą o wielu celach, jak kradzież poświadczeń.**



_ Podsumowanie

06_ Motywacja kryjąca się za większą cyberataków jest nadal finansowa.

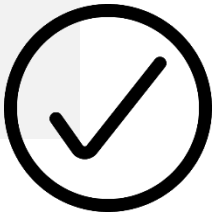
07_ Oprogramowanie ransomware jest nadal szeroko rozpowszechnione i skutkuje kosztownymi konsekwencjami dla wielu organizacji.

08_ Wiele incydentów związnaych z cyberbezpieczeństwem nadal pozostaje niezauważonych lub ich wykrycie zajmuje dużo czasu.

09_ Większa automatyzacja zabezpieczeń pozwoli organizacjom inwestować więcej w przygotowania z wykorzystaniem danych wywiadowczych na temat cyberzagrożeń jako głównej opcji.

10_ Liczba ofiar ataków typu phishing nadal rośnie, gdyż wykorzystują one cechy ludzkie stanowiące najsłabsze ogniwo.

Z powodu wszystkich zmian w krajobrazie cyberzagrożeń i wyzwań, jakie pojawiły się z powodu pandemii COVID-19, musi minąć dużo czasu, nim cyberprzestrzeń znów stanie się godnym zaufania i bezpiecznym środowiskiem dla wszystkich.



Informacje ogólne

_ Czy obywatele Unii Europejskiej stali się bardziej świadomi zagrożeń i wyzwań, jakie wiążą się z cyberprzestrzenią?

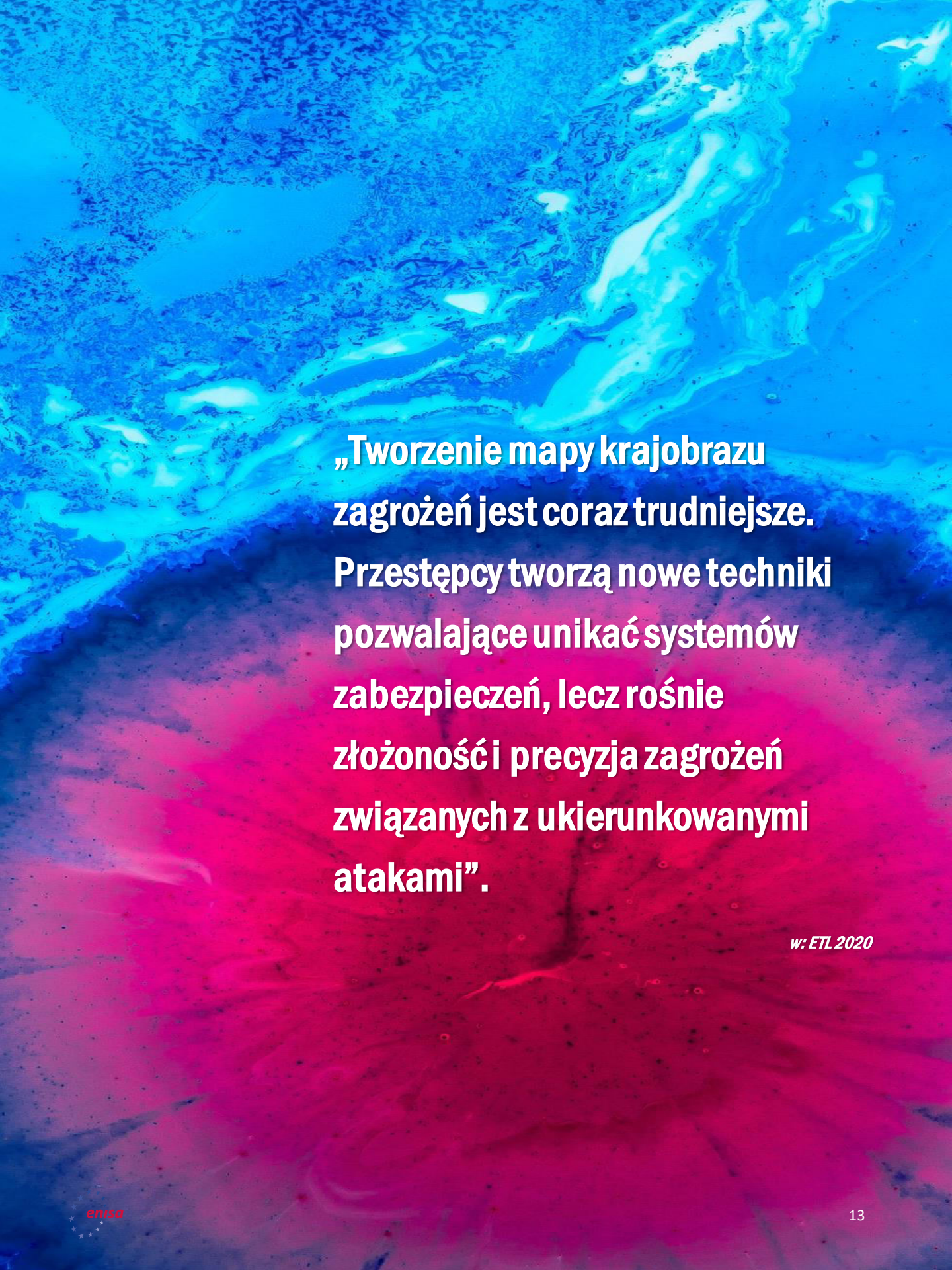
W 2019 r. Komisja Europejska przygotowała specjalne badanie w ramach projektu Eurobarometr[4], którego celem jest zrozumienie świadomości, doświadczeń oraz opinii dotyczących cyberbezpieczeństwa.

EUROBAROMETR

Wyniki tego badania wykazały, że coraz więcej ludzi w Europie korzysta z internetu, zwłaszcza z użyciem smartfonów, a obywatele są bardziej świadomi potencjalnych zagrożeń związanych z korzystaniem z sieci.

Zgodnie z wynikami tego badania obawy o prywatność i bezpieczeństwo w sieci doprowadziły już ponad 9 na 10 internautów do zmiany zachowań w internecie – najczęściej poprzez nieotwieranie wiadomości e-mail od nieznanych nadawców, instalowanie oprogramowania antywirusowego, odwiedzanie tylko znanych i witryn stron internetowych oraz korzystanie wyłącznie z własnych komputerów.

Choć wyniki te są dość zachęcające, wielu użytkowników nadal pada ofiarą oszustw internetowych i wiadomości e-mail wykorzystujących metody phishingu. Ujawnia to, że sprawcy szkodliwych działań używają zaawansowanych ataków, które trudno jest wykryć i uniknąć. Dlatego strategie zapobiegania muszą być regularnie aktualizowane, by uwzględniały najnowsze dane wywiadowcze (CTI) dotyczące technik ataku.



„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

Czego należy oczekiwać

_Sprawcy sponsorowani przez struktury państwowe prawdopodobnie będą

TREND	OPIS	ZAGROŻENIE
→	**Nadal** wykorzystywać cyberprzestrzeń do ataków przeciwko procesowi wyborów, zagrażających systemom demokratycznym i prawom człowieka w innych krajach[5].	**Ataki przeciwko prawom człowieka i systemom demokratycznym**
→	**Nadal** nękać opozycję i śledzić obywateli, manipulując informacjami z użyciem platform społecznościowych, w połączeniu z kampaniami wykorzystującymi oprogramowanie szpiegujące.	**Ataki przeciwko prawom człowieka i systemom demokratycznym**
↗	**Prowadzić** zaawansowane kampanie dezinformacyjne[6], których celem jest wpływanie na percepcję lub manipulowanie opiniami na korzyść pewnych idei politycznych lub celów związanych ze spekulacjami finansowymi.	**Kampanie dezinformacyjne**
↗	**Przyspieszać** wyścig cyberzbrojeń[7], podejmując próby rozwijania możliwości w cyberprzestrzeni. Ponieważ cyberprzestrzeń jest traktowana jako miejsce prowadzenia działań wojennych, władze państwowe będą poszukiwać cyberbroni za pośrednictwem sponsorowanych agentów, przygotowując się do cyberwojny.	**Niekontrolowany wyścig cyberzbrojeń**
↗	**Realizować** cele strategiczne, jak: pozyskiwanie tajemnic przemysłowych z użyciem szpiegostwa, uzyskanie przewagi związanej z podejmowaniem decyzji politycznych, finansowanie reżimów za pośrednictwem oszustw finansowych, prowadzenie operacji informacyjnych w cyberprzestrzeni, a także osłabianie przeciwników lub ich morale poprzez działania zakłócające lub niszczące.	**Kradzież danych**

Cyberprzestępcy prawdopodobnie będą

TREND	OPIS	ZAGROŻENIE
→	**Nadal** zagrażać nastolatkom i młodym ludziom poprzez próby szantażowania przy pomocy zdjęć lub filmów (szantaż z użyciem kamer internetowych), co może mieć na ofiary wpływ psychiczny, a ostatecznie i fizyczny[8].	**Szantażowanie przy pomocy zdjęć lub filmów (szantaż z użyciem kamer internetowych)**
↗	**Zwiększać** liczbę przypadków cyberprzemocy podczas epidemii COVID-19 i po jej opanowaniu wśród nastolatków korzystających z platform cyfrowych w celach prywatnych (częściej) lub edukacyjnych[9].	**Cyberprzemoc**

Cyberprzestępcy prawdopodobnie będą

TREND	OPIS	ZAGROŻENIE
↗	**Zwiększać** wykorzystywanie narzędzi opartych na sztucznej inteligencji w celu tworzenia wysoce wiarygodnych fałszerstw (obraz, dźwięk i film), powszechnie określanych jako deepfake, w celu oszukiwania firm.	**Deepfake**
→	**Doskonalić** taktykę w celu narażenia na szwank procesów biznesowych i uzyskiwania przewagi finansowej.	**Narażenie na szwank procesów biznesowych**
→	**Uderzać** w niższe o jeden poziom struktury organizacji – poniżej kadry zarządzającej – by narażać na szwank służbowe wiadomości e-mail.	**Włamanie do poczty służbowej**
→	**Zwiększać** wykorzystanie dostawców usług zarządzanych w celu dystrybucji złośliwego oprogramowania.	**Złośliwe oprogramowanie**

Wnioski oraz zalecenia

Wnioski/zalecenia dotyczące polityki

- Na przestrzeni ostatnich dziesięcioleci twórcy polityki i technologowie żyli w dwóch zupełnie różnych światach i mówili różnymi językami. Aby sprostać wyzwaniom związanym z cyfryzacją, powinni oni **współpracować** od podstaw i wypracować wspólne podejście. Ponieważ większość współczesnych technologii jest związana z cyberprzestrzenią, wkład ekspertów w dziedzinie cyberbezpieczeństwa w wiele z tych dyskusji ma znaczenie zasadnicze.
- Ponieważ liczba innowacji technicznych rośnie, a cyberprzestrzeń się rozwija, skuteczne i wszechstronne polityki UE dotyczące cyberbezpieczeństwa mają ogromne znaczenie. **Dojrzałe polityki z zakresu cyberbezpieczeństwa** zapewnią niezbędne możliwości związane z bezpieczeństwem na wszystkich poziomach społeczeństwa: od struktur rządowych, przez infrastrukturę krytyczną, firmy, sektor usług i osoby fizyczne. Możliwości związane z bezpieczeństwem muszą być efektywne i elastyczne, by możliwe było sprostanie nowym wyzwaniom w miarę ich pojawiania się, z myślą o okiełznaniu ciągle się zmieniającego charakteru cyberprzestrzeni.
- W obliczu rosnącej liczby interesariuszy z UE i państw członkowskich zaangażowanych w działania CTI **współpraca i koordynacja** działań CTI w skali całej Unii Europejskiej jest bardzo ważna. ENISA zamierza promować współpracę z różnymi interesariuszami i podjąć początkową próbę identyfikacji wymagań CTI dla różnych grup interesariuszy, szczególnie w Unii Europejskiej (tj. Komisja, organy UE, agencje i państwa członkowskie).
- CTI należy uznać za główne narzędzie **gotowości w zakresie cyberbezpieczeństwa** oraz ułatwienie dla metod opartych na ryzyku. Integracja CTI z procesami zarządzania zabezpieczeniami pomoże społeczności CTI wkraczać do dziedzin powiązanych i zwiększy sprawność zwykle wydłużonych procesów, jak certyfikacja i ocena ryzyka. Ponadto CTI należy postrzegać jako moderatora decyzji awaryjnych niezbędnych w zarządzaniu ryzykiem.
- Trafność CTI dla decyzji strategicznych i politycznych jest powszechnie uznawana i uważana za zasadniczy element tworzenia **powiązań z informacjami geopolitycznymi** oraz systemami cybernetyczno-fizycznymi. Pozwoli to na włączenie CTI do obejmującego całą UE procesu podejmowania decyzji, lecz umożliwi także rozszerzenie jego kontekstu w celu identyfikacji zagrożeń hybrydowych.

Wnioski/zalecenia dotyczące firm

- W roku 2019 pojawiło się wiele **laboratoriów testowych i platform do zwalczania cyberzagrożeń**[10], zarówno lokalnych, jak i w chmurze. Są to istotne zasoby z punktu widzenia personelu szkoleniowego, symulowania ataków i testowania wielu strategii obrony. Wszystko to odbywa się w wielozadaniowym środowisku wirtualnym.
- Choć niektóre kryteria i wymogi CTI zostały stworzone dla różnorodnych profili użytkowników CTI**, podobne wymagania** będą niezbędne dla innych produktów, usług i narzędzi CTI. Dostawcy CTI będą musieli w większym stopniu uwzględnić wymagania użytkowników związane z ułatwianiem wprowadzania produktów i usług CTI.
- Inwestycje w niektóre podstawowe koncepcje CTI, w szczególności **hierarchie dojrzałości i zagrożeń CTI**, są bardzo użyteczne z punktu widzenia rozpowszechniania CTI. Dostawcy będą musieli tworzyć ofertę z myślą o różnych poziomach dojrzałości CTI, aby ułatwić efektywne wykorzystanie CTI w organizacjach o różnej wielkości i budżecie.
- W perspektywie długofalowej można uznać, że **OpenCTI**[11] może być dobrym rozwiązaniem problemu rozdrobnienia oferty CTI, przy uwzględnieniu jego wewnętrznej możliwości integracji różnego rodzaju źródeł CTI w jedno środowisko narzędziowe. Dostawcy CTI będą musieli stworzyć niezbędne „mosty" pomiędzy swymi produktami, umożliwiające ich integrację z OpenCTI. Koncepcja Cyber Range została początkowo zdefiniowana w 2013 r. przez Europejską Agencję Obrony (EDA) w raporcie „Common staff target for military cooperation on cyber ranges in the European Union" („Wspólny cel kadrowy dla współpracy wojskowej w zakresie platform do odpierania cyberzagrożeń w Unii Europejskiej") jako wielozadaniowe środowisko wspierające trzy główne procesy: rozwój wiedzy, zabezpieczenie i rozpowszechnienie.

Wnioski oraz zalecenia

Wnioski badawcze i edukacyjne oraz zalecenia

- Unia Europejska powinna nadal inwestować w **prace badawczo-rozwojowe nad cyberbezpieczeństwem**, z naciskiem na długofalowe inicjatywy badawcze dotyczące wysokiego ryzyka. Długofalowe badania i innowacyjność to kosztowne zadania, pozostające poza zasięgiem większości organizacji z sektora prywatnego.
- Poszerzanie wiadomości i wiedzy eksperckiej z dziedziny cyberbezpieczeństwa ma kluczowe znaczenie dla gotowości i odporności na ataki. Unia Europejska powinna nadal **budować potencjał** poprzez inwestycje w programy szkoleniowe dotyczące cyberbezpieczeństwa, certyfikację zawodową, ćwiczenia i kampanie zwiększające świadomość.
- Cyberbezpieczeństwo powinno obejmować wiedzę ekspercką z dyscyplin społecznych, behawioralnych i ekonomicznych. Należy promować **badania interdyscyplinarne** dotyczące cyberbezpieczeństwa i zachęcać do nich w całej Unii Europejskiej.
- Konieczne jest ocenienie wyników projektów badawczych z dziedziny cyberbezpieczeństwa oraz zmapowanie ich w szerszym kontekście w celu zidentyfikowania **części wspólnych i luk** oraz zapewnienie ich porównywalności z istniejącymi produktami, usługami i praktykami komercyjnymi. Pomoże to w rozpropagowaniu tych wyników w społeczności użytkowników.
- Należy stworzyć nowatorskie metody przekazywania wiedzy CTI z podziałem na poszczególne dziedziny, które mogą odnieść z nich korzyści. **Wśród przykładów można wymienić platformy do odpierania cyberzagrożeń, zagrożenia hybrydowe i oceny geopolityczne**. Uzyskane w ten sposób synergie mogą istotnie zwiększyć liczbę przypadków użycia i ilość wysokiej jakości treści w sposób wielokierunkowy.
- Konieczna jest dalsza analiza zastosowania **sztucznej inteligencji** i uczenia maszynowego w działaniach CTI. Spowoduje to zmniejszenie liczby wykonywanych ręcznie etapów czynności podczas analizy CTI i zwiększenie wartości funkcji uczenia maszynowego dla działań CTI.
- Należy promować dostarczanie i wykorzystywanie otwartych materiałów CTI. Ułatwi to **transfer wiedzy**, lecz także obniży próg wymaganych umiejętności CTI.

„Rok 2019 przyniósł wzrost wyrafinowania potencjalnych zagrożeń w związku z używaniem przez wielu cyberprzestępców exploitów, kradzieży poświadczeń i ataków wieloetapowych”.

w: ETL 2020

Bibliografia

1. „Akt o cyberbezpieczeństwie" Kwiecień 2019 r. Parlament Europejski i Rada https://eur-lex.europa.eu/eli/reg/2019/881/oj?locale=pl

2. „COVID-19 Risks Outlook: A Preliminary Mapping and its Implications". 19 maja 2020 r. WEF. https://www.weforum.org/reports/covid-19-risks-outlook-a-preliminary-mapping-and-its-implications

3. „Wspólny komunikat do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Społeczno-Ekonomicznego i Komitetu Regionów. Walka z dezinformacją wokół COVID-19 – dajemy dojść do głosu faktom". Czerwiec 2020 r. Komisja Europejska. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52020JC0008

4. „Special Eurobarometer 499: Europeans' attitudes towards cyber security". 29 stycznia 2020 r. https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

5. „EUvsDosinfo" https://euvsdisinfo.eu/european-elections-2019/

6. „Manipulating Social Media to Undermine Democracy". 2017. Freedom House. https://freedomhouse.org/report/freedom-net/2017/manipulating-social-media-undermine-democracy

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

8. „How online 'sextortion' drove one young man to suicide". 8 lutego 2018 r. Today. https://www.today.com/parents/how-online-sextortion-drove-one-young-man-suicide-t122735

9. „Cyberbullying may increase during COVID-19 pandemic, expert says". 30 marca 2020 r. Healio. https://www.healio.com/news/pediatrics/20200330/cyberbullying-may-increase-during-covid19-pandemic-expert-says

10. Koncepcja Cyber Range została początkowo zdefiniowana w 2013 r. przez Europejską Agencję Obrony (EDA) w raporcie „Common staff target for military cooperation on cyber ranges in the European Union" („Wspólny cel kadrowy dla współpracy wojskowej w zakresie platform do odpierania cyberzagrożeń w Unii Europejskiej") jako wielozadaniowe środowisko wspierające trzy główne procesy: rozwój wiedzy, zabezpieczenie i rozpowszechnienie.

11. Open CTI. https://www.opencti.io/en/

„CTI ma ugruntowaną pozycję w dziedzinie bezpieczeństwa cybernetycznego jako podstawowe narzędzie zwiększania sprawności i skuteczności w obronie przed cyberatakami.”

w: ETL 2020

Powiązany

Raport ENISA o krajobrazie zagrożeń
Wykaz piętnastu największych zagrożeń

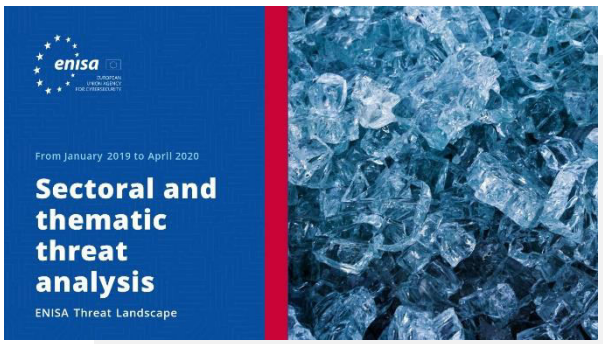
Agencja ENISA: wykaz piętnastu największych zagrożeń w okresie od stycznia 2019 r. do kwietnia 2020 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń
Tematyka badań

Zalecenia dotyczące tematów badawczych z różnych kwadrantów w dziedzinie bezpieczeństwa cybernetycznego 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

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń **Najważniejsze incydenty w UE i na świecie**

Najważniejsze incydenty związane z cyberbezpieczeństwem 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 rozpoznawania 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 przedstawicieli mediów dotyczące tego raportu należy przesyłać na adres press@enisa.europa.eu.

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