PL

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

Od stycznia 2019 r. do kwietnia 2020 r.

Tematyka badań

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

Informacje ogólne

Nowe koncepcje i pomysły rozwijają się w dziedzinie bezpieczeństwa cybernetycznego dzięki działalności badawczej i innowacyjnej prowadzonej przez naukowców, przedstawicieli branży i specjalistów na całym świecie. Są to ważne etapy, gdyż tempo wprowadzania innowacji przez przeciwników (np. sprawców szkodliwych działań) jest wyższe niż to, z jakim specjaliści w dziedzinie cyberbezpieczeństwa znajdują rozwiązania mające na celu ich odparcie. W istocie, oprócz podstawowych zabezpieczeń i szkoleń w zakresie cyberbezpieczeństwa, inwestowanie w badania i innowacyjność jest dla obrońców najbardziej realnym wariantem zbliżenia się do dysponowania środkami niezbędnymi do poprawy bezpieczeństwa cyberprzestrzeni. W tym raporcie podkreślamy niektóre z najważniejszych badań dotyczących cyberbezpieczeństwa oraz tematy innowacji badane w UE i na całym świecie.

Lepsze zrozumienie wymiaru ludzkiego

Cyberbezpieczeństwo jest nadal określane jako metoda zabezpieczania sieci, systemów komputerowych i danych. Definicję tę należy rozszerzyć tak, by wykraczała poza zagadnienia techniczne i obejmowała zagadnienia socjoekonomiczne, behawioralne i ekonomiczne oraz różne role pełnione przez zaangażowane strony. Powinno to stanowić priorytet dla przyszłych badań na temat cyberbezpieczeństwa i dyskusji o innowacyjności. Lepsze zrozumienie wymiaru ludzkiego ma kluczowe znaczenie dla definicji każdej strategii cyberbezpieczeństwa, aby decyzje dotyczące bezpieczeństwa były podejmowane z myślą o zaspokojeniu potrzeb, umiejętnościach i oczekiwaniach.

Badania dotyczące cyberbezpieczeństwa oraz innowacje

W roku 2019 zaobserwowaliśmy wzrost liczby laboratoriów testowych i platform do zwalczania cyberzagrożeń[1], zarówno lokalnych, jak i w chmurze. Są to niezbędne zasoby służące badaczom do symulacji ataków, opracowywania scenariuszy wykorzystania, pozyskiwania danych operacyjnych i testowania strategii obronnych w wielofunkcyjnym środowisku wirtualnym. W istniejących środowiskach testowych brak jednak możliwości odtworzenia wielu luk w zabezpieczeniach, które zazwyczaj zagrażają bezpieczeństwu, takich jak m.in. czynniki ludzkie i techniczne. Aby umożliwić poprawę wydajności, konieczne jest prowadzenie badań i tworzenie innowacji dotyczących zakresu i rzetelności tych laboratoriów testowych oraz proponowanie nowych rozwiązań technicznych.

Informacje ogólne

Bezpieczeństwo 5G

Wprowadzenie sieci mobilnych 5G w niektórych krajach rozpoczęło się w roku 2019 r., lecz przypuszcza się, że liczba instalacji wzrośnie w 2021 r. Ta kolejna generacja łączności komórkowej ma ogromne znaczenie dla społecznego i ekonomicznego postępu w Unii Europejskiej. Dlatego też przyszłe badania i rozwój rozwiązań w zakresie bezpieczeństwa sieci 5G mają kluczowe znaczenie dla zrównoważonego rozwoju i niezawodności tej technologii. W 2019 r. ENISA opublikowała raport dotyczący krajobrazu zagrożeń dla sieci 5G, oceniając pewne krytyczne aspekty bezpieczeństwa związane z tą rozwijającą się technologią.[2]. Kluczowe tematy działań badawczo-innowacyjnych dotyczących sieci 5G powinny uwzględniać poniższe aspekty.

- Prace badawczo-rozwojowe nad metodami kontroli zabezpieczeń powinny obejmować zabezpieczenia sieci, elementy fizyczne i warstwy danych, w ten sposób tworząc rozwiązanie zabezpieczające oparte na wielu warstwach. W przypadku sieci 5G dane będą przechowywane na scentralizowanych serwerach chmurowych, pośrednich węzłach mgły obliczeniowej i urządzeniach brzegowych, co zwiększa złożoność wdrożenia rozwiązania zabezpieczającego.

- Standardy i wymagania działań badawczo-rozwojowych dotyczących metod kontroli zabezpieczeń powinny być wdrażane w połączonych sieciach mających wielu właścicieli, o różnych topologiach i operatorach, jak również w przypadku różnorodnych urządzeń i warstw sieciowych.

- Działania badawczo-rozwojowe dotyczące kluczowych możliwości zarządczych umożliwiających bezpieczną interoperacyjność między węzłami łączącymi ograniczone pod względem zasobów urządzenia brzegowe i IoT. Możliwość ta powinna uwzględniać skuteczną kontrolę dostępu, uwierzytelnianie, kryptografię oraz kluczowe techniki zarządzania węzłami o ograniczonych zasobach.

Badania i projekty innowacyjne dotyczące bezpieczeństwa w Unii Europejskiej

- W UE trwają prace nad stworzeniem pilotażowej sieci kompetencji w zakresie cyberbezpieczeństwa. CONCORDIA[3], ECHO[4], SPARTA[5] i CyberSec4Europe[6] to cztery zwycięskie projekty pilotażowe w ramach zaproszenia do składania wniosków w programie „Horyzont 2020" w 2018 r., dotyczącym „utworzenia i prowadzenia pilotażowej europejskiej sieci kompetencji w zakresie cyberbezpieczeństwa oraz opracowania wspólnego europejskiego planu działań na rzecz badań i innowacji w sferze cyberbezpieczeństwa". UE przewiduje, że dzięki tym czterem projektom pilotażowym na rzecz bezpieczniejszego jednolitego rynku cyfrowego wzmocni swoje zdolności w zakresie cyberbezpieczeństwa i będzie mogła sprostać przyszłym wyzwaniom związanym z cyberbezpieczeństwem.
- UE przeznacza 38 mln EUR na ochronę infrastruktury krytycznej przed cyberzagrożeniami. Komisja Europejska ogłosiła, że przeznacza ponad 38 mln EUR na unijny program badań i innowacyjności w ramach programu „Horyzont 2020". Celem programu jest wspieranie kilku innowacyjnych projektów z dziedziny ochrony infrastruktury krytycznej przed cyberzagrożeniami i zagrożeniami fizycznymi oraz rozwijanie inteligentnych i bezpieczniejszych miast.[7]
- UE ogłosiła zaproszenie do składania wniosków na projekty w zakresie cyberbezpieczeństwa o wartości 10,5 mln EUR. Komisja ogłosiła nowe zaproszenie o wartości 10,5 mln EUR w ramach instrumentu „Łącząc Europę" i dotyczące projektów, które przyczynią się do zwiększenia zdolności Europy w zakresie cyberbezpieczeństwa i współpracy między państwami członkowskimi.[8]

Badania i innowacyjność w zakresie CTI

Błyskawiczne rozpowszechnianie metod i treści CTI

W okresie sprawozdawczym zidentyfikowane zostały różne potrzeby badawcze i zaproponowano działania mające na celu realizację tych potrzeb. Zostały one podzielone na kilka kategorii mających lepiej odzwierciedlać ich zakres. Choć kategorie te mogą się zazębiać, wskazują obszary, w których możliwe są udoskonalenia CTI.

- **Konieczna jest ocena projektów badawczych w dziedzinie CTI i dokonanie ich mapowania na szerszy kontekst CTI** w celu zidentyfikowania części wspólnych i luk oraz sprawienia, by stały się porównywalne z istniejącymi komercyjnymi produktami, usługami i praktykami w zakresie CTI. Pomoże to w rozpowszechnianiu wyników w społeczności użytkowników. Równocześnie istniejące luki będą wypełniane dodatkowymi funkcjami, treściami i procesami. Projekty UE o znaczeniu dla CTI (Horyzont 2020) są doskonałymi kandydatami do tego zadania, przyczyniając się do poprawy praktyk CTI.
- **Należy promować dostarczanie i wykorzystywanie otwartych materiałów CTI**. Ułatwi to transfer wiedzy, lecz także obniży próg umiejętności CTI. Platforma Open-CTI jest idealną kandydatką do tego celu, ponieważ wspiera wprowadzanie danych CTI z wielu źródeł do jednej bazy, która może zostać udostępniona różnym użytkownikom, a równocześnie oferuje zestaw funkcji do zarządzania tymi informacjami. Korzystając z Open-CTI, użytkownicy będą mogli pozyskiwać cenne informacje przy stosunkowo niskim progu umiejętności.

_Badania skutkujące wyłonieniem nowych trendów

Potrzeba **wzmocnienia CTI** przy użyciu innych uznanych narzędzi cyberbezpieczeństwa wymaga strukturalnej i kontekstowej ewolucji tej dziedziny. Równocześnie postępy technologii osiągnięte dzięki tym nowym technologiom zachęcają do zadania pytania, w jaki sposób CTI może odnieść korzyści z tych nowości. Potrzeby w zakresie **badań prospektywnych** w dziedzinie CTI przyczynią się więc do doskonalenia procesów, funkcji, automatyzacji, struktury i weryfikacji treści, świadczenia usług, stosunku szybkości do liczby użytkowników/rozpowszechniania, wdrożenia CTI i mapowania.

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

Badania i innowacyjność w zakresie CTI

Funkcjonalność, poziom automatyzacji oraz zgodność z wymaganiami w zakresie dojrzałości

- **Automatyzacja procesów odegra kluczową rolę w CTI**. Nowoczesne cyberataki zostały w dużym stopniu zautomatyzowane, zaś organizacje próbują się przed nimi bronić ręcznie lub z częściowym zastosowaniem automatyzacji. To nierówna walka, która ma negatywny wpływ na szybkość i zdolność reagowania. Badanie potencjalnej automatyzacji procesów CTI będzie miało kluczowe znaczenie dla uzyskania równowagi pomiędzy atakującymi a obrońcami. Uzyskanie jej będzie wymagać dogłębnej analizy etapów i opcji procesów CTI z myślą o automatyzacji tych etapów z użyciem istniejących i nowo powstałych technologii.
- **Konieczna będzie bardziej szczegółowa identyfikacja wymagań CTI w zakresie dojrzałości**. Chociaż dla różnych profili użytkowników CTI zostały opracowane pewne kryteria czy wymagania dotyczące wyboru funkcji CTI (np. platformy analizy zagrożeń: Threat Intelligence Platforms (TIP)), podobne wymagania będą konieczne w przypadku innych produktów, usług i narzędzi CTI. Niektóre wymagania będą powiązane z wieloma poziomami dojrzałości użytkowników oraz wydatkami i rodzajami CTI. Podobne kryteria czy wymagania są także niezbędne dla innych elementów infrastruktury CTI, takich jak narzędzia, dobre praktyki, platformy udostępniania itp. Dlatego też, poza rozwojem modeli dojrzałości dla zdolności CTI, konieczne są badania mające na celu wykazanie, w jaki sposób funkcje CTI odpowiadają różnym poziomom dojrzałości CTI. Prace te przyczynią się do zwiększenia szybkości wprowadzania praktyk CTI.
- **Zalecana jest także dalsza analiza wykorzystania sztucznej inteligencji i uczenia maszynowego w CTI**. Zaowocuje to zmniejszeniem liczby wykonywanych ręcznie etapów analizy CTI i zwiększeniem wartości funkcji uczenia maszynowego w obrębie działań CTI.

Budowanie mostów między obszarami powiązanymi

- Konieczne jest stworzenie **nowatorskich metod przyswajania wiedzy CTI z podziałem na dziedziny,** które mogą dzięki temu odnieść korzyści. Wśród przykładów można wymienić platformy do odpierania cyberzagrożeń, zagrożenia hybrydowe, łańcuchy dostaw oraz oceny geopolityczne i kryzysy. Należy zatem zadać sobie następujące pytania: W których punktach należy uwzględnić CTI? Które treści CTI są istotne? Jakie są kryteria weryfikacji trafności informacji CTI? Wjaki sposób można „podłączyć" CTI do informacji o danej dziedzinie? Jakie rodzaje informacji z tych dziedzin można dodać do CTI? Synergie, jakie odzwierciedlają te pytania, mogą istotnie zwiększyć liczbę przypadków użycia i poprawić jakość treści w sposób wielokierunkowy.

- **CTI ma znaczenie zasadnicze dla szeregu dziedzin.** Wśród przykładów można wymienić ocenę ryzyka / zarządzanie ryzykiem oraz definiowanie wymagań zabezpieczeń i certyfikacji. Dziedziny te odniosą korzyści z prawidłowego stosowania CTI. Wkład CTI w te dziedziny można zidentyfikować przy użyciu takich informacji, jak modele zagrożeń, informacje o sprawcach stanowiących zagrożenie (zdolności, motywy), metody ataku i exploity. Choć pewne przydatne materiały już istnieją (np. struktura ataków ATT&CK[8]), niezbędne będą szeroko zakrojone prace w celu identyfikacji i standaryzacji takich interfejsów.

Badania i innowacyjność w zakresie CTI

Skuteczność działań CTI

- **Metody skutecznego wykorzystania CTI będą stanowić narzędzie do podejmowania decyzji.** Takie metody skutecznego wdrażania CTI skutecznie pomogą decydentom w zrozumieniu, na czym polega wartość CTI, a praktykom – w ocenie stopy zwrotu z CTI. Metody te lub KPI będą musiały uwzględniać czynniki wykraczające poza treści CTI, z wzięciem pod uwagę uzyskanych ulepszeń w całym cyklu życia zarządzania bezpieczeństwem i zmniejszania ryzyka. W ujęciu optymalnym pomiar efektywności inwestycji w CTI będzie stanowić część znacznie szerszych rozważań na temat ekonomii cyberbezpieczeństwa w organizacjach różnego rodzaju (np. z podziałem na wymagania bezpieczeństwa, poziomy dojrzałości itp.).

- Choć dominują niedrogie narzędzia do agregowania, analizy i rozpowszechniania CTI, **konieczne może być przeprowadzenie badań w celu znalezienia zautomatyzowanych narzędzi** do zarządzania wykorzystywanymi i wytwarzanymi danymi CTI. Przedmiotem takich badań mogą być inne niż standardowe formaty danych (np. pliki CSV, STIX, czy TAXII) lub standardowe funkcje CTI, a następnie tworzenie niedrogich, opartych na modelu open-source narzędzi wspomagających takie funkcje.

Ewolucja struktury i treści CTI

- Ponieważ CTI przenika dziedziny dodatkowe, **konieczne jest przekazanie informacji z tych kontekstów z powrotem do oryginalnej bazy wiedzy CTI**. Konieczne jest na przykład zdefiniowanie struktur CTI odzwierciedlających informacje geopolityczne i dotyczące zagrożeń hybrydowych. To samo dotyczy znaczenia CTI dla ryzyka, incydentów, analiz kryminalistycznych, poziomów pewności itp. Istniejące formaty CTI muszą ewoluować tak, aby uwzględnić informacje wynikające z tych zależności w CTI.

- **Nowe technologie, jak sztuczna inteligencja,** mogą zostać użyte do weryfikacji analizowanych danych CTI. Narzędzia takie mogą poszerzać lub nawet zastępować ręczną analizę CTI, ale także zapewniać wsparcie przez cały cykl życia CTI (np. badać trafność CTI w oparciu o istniejące informacje o incydentach). Tak nowatorskie podejścia do CTI zaowocują poprawą jakości i trafności informacji.

Bibliografia

1. 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.

2. „ENISA Threat Landscape for 5G Networks". 21 listopada 2019 r. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

3. https://www.concordia-h2020.eu/

4. https://echonetwork.eu/

5. https://www.sparta.eu/news/

6. https://cybersec4europe.eu/

7. https://ec.europa.eu/programmes/horizon2020/en/news/eu-grants-%E2%82%AC38-million-protection-critical-infrastructure-against-cyber-threats

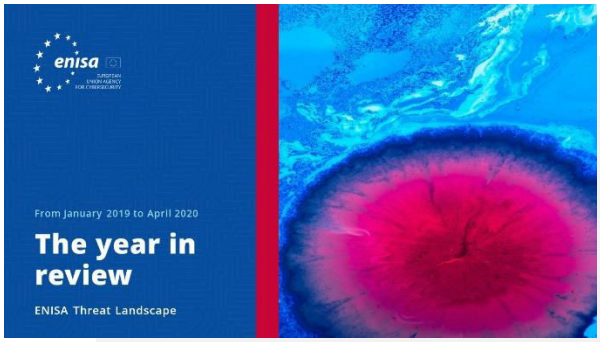
8. https://ec.europa.eu/digital-single-market/en/news/eu105-million-eu-funding-available-projects-stepping-eus-cybersecurity-capabilities-and

9. https://attack.mitre.org/

„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 **Przegląd roku**

Podsumowanie głównych trendów w cyberbezpieczeństwie w roku.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń **Wykaz piętnastu największych zagrożeń**

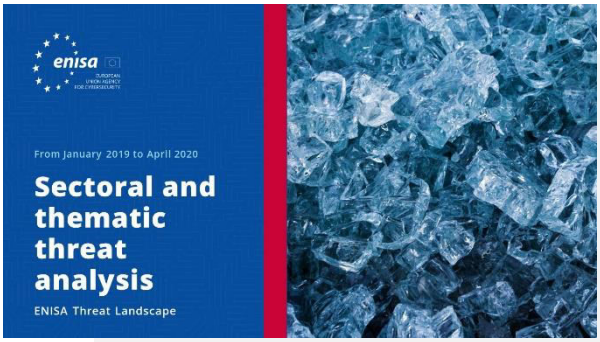
Agencja ENISA: wykaz piętnastu największych zagrożeń w okresie od stycznia 2019 r. do kwietnia 2020 r.

PRZECZYTAJ RAPORT

Raport ENISA o krajobrazie zagrożeń **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 **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

Mapa współpracy między siecią CSIRTS a organami ścigania

Plan działań dotyczący współpracy pomiędzy zespołami CSIRT, w szczególności z krajowymi i rządowymi – organami ścigania (LE) oraz sądownictwem.

PRZECZYTAJ RAPORT

Raport dotyczący stanu rozwoju reagowania na incydenty w państwach członkowskich UE

Badanie obejmujące analizę obecnego systemu reagowania operacyjnego na incydenty w sektorach NISD i wskazanie ostatnich zmian.

PRZECZYTAJ RAPORT

Model oceny dojrzałości ENISA dla sieci CSIRT

Zaktualizowana wersja opracowania „Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity" – publikacja ENISA, 2017 r.

PRZECZYTAJ RAPORT

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

w: ETL 2020

Informacje

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 odpornością 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