enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

PL

Od stycznia 2019 r. do kwietnia 2020 r.

Sektorowa i tematyczna analiza zagrożeń

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

Informacje ogólne

Analiza ta, oprócz wskazywania motywacji przeciwników, dostarcza danych dotyczących najczęściej stosowanych technik ataku oraz narażenia w poszczególnych sektorach, a przez to wskazuje wymogi i priorytety ochrony. Jeśli chodzi o tematy przewodnie, to analiza zagrożeń i wyzwań związana z konkretnymi nowymi technologiami pomaga w procesie oceny przyszłych zagrożeń i przeciwdziałania im.

Uwzględniające kontekst rozpoznawanie cyberzagrożeń (cyber threat intelligence, CTI) dla sektorów to ważne narzędzie wspomagające przygotowanie i pozwalające na wyciąganie wniosków co do przewidywanych cyberataków w danym sektorze.

Statystyki incydentów w sektorach vs. szacowane narażenie sektorów rozwijających się

Uwzględnienie kontekstu w sektorowej analizie CTI opiera się przede wszystkim na incydentach związanych z cyberbezpieczeństwem, które miały miejsce w danym sektorze. Jest to metoda standardowa w przypadku istniejących i uznanych elementów infrastruktury IT i usług cyfrowych, jednak nie obejmuje nowo powstających technologii. Dzieje się tak przede wszystkim dlatego, że dla technologii będących dopiero w fazie pilotażu lub eksperymentów nie istnieją dane o incydentach. CTI dla nowych technologii osadza się w kontekście poprzez ocenę zagrożeń dla kategorii zasobów odnoszących się do konkretnego sektora. ENISA wykonuje takie oceny dla rozwijających się sektorów, takich jak 5G, IoT[5] oraz inteligentne samochody[6].Aby uwzględnić kontekst w CTI, ENISA stosuje sektorową i tematyczną analizę krajobrazów zagrożeń oraz oceny ochrony podstawowej.

W niniejszym raporcie, oprócz sektorowego wywiadu CTI opartego na statystykach incydentów, przedstawiamy podsumowanie ocenianych CTI dla sektorów nowych technologii wykonane na podstawie prac ENISA.


„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

Informacje ogólne

_Pilne zapotrzebowanie na dokładne i aktualne sektorowe statystyki incydentów

Sektorowe statystyki incydentów mają zasadnicze znaczenie dla zrozumienia dynamiki ewolucji zagrożeń, motywów przeciwników, narażenia zasobów i działań ukierunkowanych na cele. Ze względu na złożoność ataków, zależności pomiędzy zasobami będącymi ich celem oraz międzysektorową naturą wykorzystywanych podatności, statystyki incydentów obarczone są niedającą się wyeliminować niepewnością, której przyczyny są następujące.

- W różnych statystykach dla sektorów widzimy pewną liczbę **incydentów w kategorii „nieznane”**[1,2]. Ich udział waha się od 1,5% do 5%. Gdyby można było powiązać te incydenty z pewnymi znanymi sektorami, udział ten mógłby mieć wpływ na kolejność celów. Niepewność do oceny motywów sprawców zagrożeń wprowadza także znaczna liczba nieznanych technik ataku (około 15%).
- W przypadku większości **ataków do osiągnięcia ostatecznego celu potrzebny jest więcej niż jeden etap** (średnio są to trzy etapy). W wielu przypadkach pojedynczy atak obejmuje wiele celów z różnych sektorów. Dlatego też incydent zarejestrowany w danym sektorze może być wynikiem kilku incydentów w innych sektorach, które stanowiły pośrednie etapy ataku. Takie zależności między incydentami mogą wpłynąć na dokładność statystyk incydentów.
- Ważnym elementem analizy statystycznej, oprócz liczby incydentów w poszczególnych sektorach, jest **rodzaj wykorzystanych technik ataku**. Takie informacje mogą stanowić użyteczne dane dotyczące najczęściej wykorzystywanych wektorów ataku i mogą przyczynić się do lepszej priorytetyzacji środków ochrony potrzebnych dla danego sektora.

- Urzeczywistnienie tych zagrożeń zależy w dużym stopniu od istniejących **okazji wykorzystywanych przez przeciwników**. Na przykład z uwagi na pandemię COVID-19 środowiska IT uległy decentralizacji. Powoduje to osłabienie korporacyjnych mechanizmów kontroli bezpieczeństwa stosowanych w sieciach firmowych, co wyjaśnia przesunięcie części ataków z celów korporacyjnych na osoby fizyczne[1]. Ten przykład wskazuje na konieczność wyjaśniania obserwowanych zmian w statystykach z uwzględnieniem nowych możliwości.
- Aktualne statystyki są opracowywane na podstawie różnych kryteriów. **Zmiany kryteriów** statystyk utrudniają porównania pomiędzy statystykami incydentów. Na przykład:
    - w zależności od bazy danych statystycznych, jakich dostarczają osoby zainteresowane lub inne podmiotowi zbierającemu dane, statystyki mogą nie obejmować wszystkich sektorów w tym samym stopniu;
    - klasyfikacja incydentów może być oparta o częstotliwość ich występowania, niezależnie od rozmiarów szkody (np. ilości wykradzionych danych) czy jej skutków.
- Zasadniczym elementem statystyk sektorowych jest **częstotliwość występowania** poszczególnych cyberzagrożeń. Pozwala to zobaczyć, jaka w danym sektorze jest najczęściej stosowana metoda ataku. Statystyki takie mogą dostarczyć wytycznych dotyczących wymaganego poziomu przygotowania czy też dopracowania poszczególnych środków bezpieczeństwa zmniejszających narażenie na dane cyberzagrożenia.
- W świetle powyższych faktów odnoszących się do statystyk incydentów, w niniejszym raporcie podano przybliżony ranking sektorów pod kątem obserwowanych incydentów wraz z trendem wywiedzionym z dynamiki potencjalnego narażenia dla każdego sektora. Podano także pewne informacje dotyczące najpopularniejszych wektorów ataku w danych sektorach. Skonsolidowano w tym celu dane z różnych publikacji[1,2,3,4].

Trendy dotyczące

SEKTOR	NAJCZĘSTSZE ZAGROŻENIA / WEKTORY ATAKU	TRENDY INCYDENTÓW
Osoba fizyczna	• Phishing • Złośliwe oprogramowanie • Wyciek informacji • Kradzież danych	Stabilny
Wiele branż	• Ataki oparte na aplikacjach sieciowych • Phishing • Złośliwe oprogramowanie	Rosnący
Administracja publiczna, obronność, opieka społeczna	• Złośliwe oprogramowanie • Phishing • Ataki przez strony internetowe	Stabilny, lekko malejący
Finanse / bankowość / ubezpieczenia	• Ataki oparte na aplikacjach sieciowych • Zagrożenie wewnętrzne (nieumyślne nadużycie) • Złośliwe oprogramowanie • Kradzież danych	Stabilny
Zdrowie/medycyna	• Złośliwe oprogramowanie • Zagrożenie wewnętrzne (nieumyślne nadużycie / błąd) • Ataki oparte na aplikacjach sieciowych	Rosnący
Edukacja	• Złośliwe oprogramowanie • Oprogramowanie ransomware • Ataki przez strony internetowe	Stabilny, lekko malejący
Informacje i komunikacja	• Ataki oparte na aplikacjach sieciowych • Zagrożenie wewnętrzne (nieumyślne nadużycie / błąd) • Złośliwe oprogramowanie	Stabilny
Usługi specjalistyczne/ cyfrowe	• Ataki oparte na aplikacjach sieciowych • Zagrożenie wewnętrzne (nieumyślne nadużycie / błąd) • Złośliwe oprogramowanie	Stabilny
Sztuka, rozrywka i gry[8]	• Ataki oparte na aplikacjach sieciowych • Złośliwe oprogramowanie • Phishing	Stabilny
Produkcja	• Złośliwe oprogramowanie • Ataki oparte na aplikacjach sieciowych • Zagrożenie wewnętrzne (nieumyślne nadużycie / błąd)	Stabilny

SEKTOR	CZYNNIKI WPŁYWU
Osoba fizyczna	Samoizolacja związana z pandemią COVID-19 i lockdownem doprowadziła do powstania rozproszonych/zdecentralizowanych środowisk IT i izolacji użytkowników, których łatwiej jest zwieść i którzy mają mniej zainstalowanych zabezpieczeń niż w przypadku środowisk scentralizowanych.
Wiele branż	Przejście użytkowników na pracę zdalną w związku z pandemią COVID-19 ułatwiło ataki typu phishing oraz wyciek informacji wrażliwych (np. danych uwierzytelniających).
Administracja publiczna, obronność, opieka społeczna	Wykorzystanie usług w chmurze mogło wpłynąć na bezpieczeństwo usług publicznych. Jednak znaczna liczba ataków ukierunkowanych na opiekę społeczną była związana z pomocą finansową, jaką obywatele otrzymywali podczas pandemii COVID-19.
Finanse / bankowość / ubezpieczenia	Złożoność sektora finansowego utrudnia interpretację krajobrazu zagrożeń, ponieważ w różnych domenach usług finansowych i bankowości mogą występować zupełnie inne czynniki ryzyka i zagrożenia związane z cyberprzestępczością.
Zdrowie/medycyna	Branża opieki zdrowotnej stała się przedmiotem istotnie wzmożonego zainteresowania ze strony cyberprzestępców z powodów finansowych oraz w związku z tym, że sektor ten podczas pandemii COVID-19 stał się jeszcze ważniejszy.
Edukacja	Trend jest stabilny, natomiast sektor ten w 2020 r. stał się przedmiotem kampanii cyberszpiegowskich z uwagi na zainteresowanie wynikami badań dotyczących COVID-19.
Informacje i komunikacja	Sektor ten znajduje się pod ciągłą presją z powodu trudności w ochronie olbrzymiej powierzchni ataku stworzonej przez platformy mediów cyfrowych. Dla organizacji mediów internetowych jednym z największych zagrożeń są ataki powodujące szkody dla reputacji.
Usługi specjalistyczne/ cyfrowe	Przy stabilnym trendzie w 2020 r. zaobserwowano jednak ukierunkowanie różnych kampanii na wyciek danych od użytkowników usług cyfrowych pracujących zdalnie z domu podczas pandemii COVID-19.
Sztuka, rozrywka i gry	Zmiana modelu biznesowego z licencjonowania na subskrypcyjny w branży gier spowodowała, że sektor ten stał się bardziej atrakcyjny dla cyberprzestępców[8].
Produkcja	Głównym zagrożeniem dla firm produkcyjnych są ataki na łańcuchy dostaw oraz na systemy sterowania w przemyśle, ponieważ mogą one doprowadzić do całkowitego wstrzymania produkcji. Innym poważnym ryzykiem dla tej branży jest kradzież własności intelektualnej.

Zagrożenia związane z nowymi technologiami

Następna generacja urządzeń mobilnych i 5G

POWIĄZANE ELEMENTY – GRUPY ZASOBÓW	NARAŻENIE NA ZAGROŻENIA
Sieć szkieletowa	Nadużycia dostępu zdalnego, skoki ruchu związanego z uwierzytelnianiem, nadużycia związane z uwierzytelnianiem użytkownika / danymi uwierzytelniającymi, nadużycia związane z hostowaniem usług u podmiotów zewnętrznych, nadużycia związane z funkcją przekazywania danych do organów władzy, wykorzystanie podatności interfejsu programowania aplikacji (API), wykorzystanie nieodpowiednio zaprojektowanej architektury lub nieodpowiedniego planowania, wykorzystanie złej lub nieodpowiedniej konfiguracji systemów/sieci, błędy przy korzystaniu z sieci, systemów i urządzeń lub przy zarządzaniu nimi, scenariusze oszustw związane z połączeniami mobilnymi, przemieszczanie poziome, sczytywanie pamięci, manipulacja ruchem sieciowym, rekonesans sieciowy i gromadzenie danych, manipulacja danymi konfiguracji sieci, ataki zalewowe na elementy sieci szkieletowej, szkodliwe przekierowanie ruchu, manipulacja orkiestratorem zasobów sieciowych, nadużycia narzędzi do audytu, sytuacyjne i nieuczciwe wykorzystanie zasobów dzielonych, rejestracja szkodliwych funkcji sieciowych, podsłuchiwanie ruchu, ataki bocznym kanałem
Sieć dostępowa	Nadużycia zasobów pasma, skażenie protokołu ARP (Address Resolution Protocol), fałszywy węzeł sieci dostępowej, atak zalewowy, przechwytywanie IMSI, zagłuszanie częstotliwości radiowej, fałszowanie adresu MAC, manipulacja danymi konfiguracyjnymi sieci dostępowej, zakłócanie sygnału radiowego, manipulacja ruchem w sieci radiowej, przechwytywanie sesji, oszustwa związane z przesyłaniem sygnałów, burze sygnałowe

POWIĄZANE ELEMENTY – GRUPY ZASOBÓW	NARAŻENIE NA ZAGROŻENIA
Multi Edge Computing	Fałszywa lub nielegalna bramka MEC, przeciążenie węzła brzegowego, nadużycie otwartych interfejsów programowania aplikacji (API) na krawędzi systemu
Wirtualizacja funkcji sieci i sieci definiowane programowo	Nadużycia protokołu DCI (Data Centres Interconnect), nadużycia zasobów obliczeniowych chmury, omijanie wirtualizacji sieci, nadużycia hostów wirtualnych
Infrastruktura fizyczna	Manipulacja sprzętem, klęski żywiołowe wpływające na infrastrukturę sieci, fizyczny sabotaż/uszkodzenie infrastruktury sieciowej, zagrożenia ze strony personelu podmiotów zewnętrznych mającego dostęp do obiektów operatora sieci mobilnej, wykorzystanie podatności formatu UICC (Universal Integrated Circuit Card), atak na sprzęt użytkowników
Wszystkie powyższe grupy zasobów 5G	Atak typu Denial of Service (DoS), naruszenie bezpieczeństwa danych, wyciek, kradzież i zniszczenie danych oraz manipulacja nimi, podsłuchiwanie, wykorzystanie podatności w oprogramowaniu i sprzęcie, złośliwy kod lub oprogramowanie, naruszenie bezpieczeństwa w łańcuchu dostaw, u dostawców i usługodawców, zagrożenia/ataki celowane, wykorzystanie luk w procedurach zabezpieczeń, zarządzania i działania, nadużycia związane z uwierzytelnianiem, kradzież lub fałszowanie tożsamości

Zagrożenia związane z nowymi technologiami

Internet rzeczy (IoT)

POWIĄZANE ELEMENTY – GRUPY ZASOBÓW	NARAŻENIE NA ZAGROŻENIA
Czynnik ludzki	Zagrożenia wewnętrzne, problemy z pracą w zespole, haktywizm, utrata wsparcia, przerwy w działaniu usług komunalnych, przerwy w działaniu sieci, nieumyślne zmiany, sabotaż, naruszenia regulaminu, naruszenia prawa, wymogi kontraktowe, niespełnienie wymogów kontraktowych (np. dotyczących utrzymywania oprogramowania), wykorzystanie podatności w oprogramowaniu, inżynieria społeczna, kradzież tożsamości.
Projektowanie oprogramowania	Zagrożenia wewnętrzne, haktywizm, nieumyślne zmiany, błędne użycie urządzeń i systemów lub błędne administrowanie nimi, sabotaż, niepowodzenia związane z procesem SDLC, niepowodzenia związane z podmiotami zewnętrznymi, niespełnienie wymogów kontraktowych (np. dotyczących utrzymywania oprogramowania), wykorzystanie podatności w oprogramowaniu, utrata/wyciek danych.
Programowanie	Zagrożenia wewnętrzne, haktywizm, utrata wsparcia, nieumyślne zmiany, błędne użycie urządzeń i systemów lub błędne administrowanie nimi, sabotaż, wandalizm i kradzież, podatności w oprogramowaniu, niepowodzenia związane z procesem SDLC, niepowodzenia w utrzymywaniu, nadużycia związane z autoryzacją, wykorzystanie podatności w oprogramowaniu, manipulacja infrastrukturą SDLC, utrata/wyciek danych.
Wdrażanie oprogramowania	Zagrożenia wewnętrzne, haktywizm, utrata wsparcia, nieumyślne zmiany, błędne użycie urządzeń i systemów lub błędne administrowanie nimi, sabotaż, wandalizm i kradzież, podatności w oprogramowaniu, niepowodzenia związane z procesem SDLC, niepowodzenia związane z podmiotami zewnętrznymi, nadużycia związane z autoryzacją, wykorzystanie podatności w oprogramowaniu, manipulacja infrastrukturą SDLC, ataki typu Denial of Service, manipulacja danymi, ujawnienie, utrata/wyciek danych.

POWIĄZANE ELEMENTY – GRUPY ZASOBÓW	NARAŻENIE NA ZAGROŻENIA
Dane	Zagrożenia wewnętrzne, haktywizm, utrata wsparcia, nieumyślne zmiany, błędne użycie urządzeń i systemów lub błędne administrowanie nimi, sabotaż, wandalizm i kradzież, podatności w oprogramowaniu, niepowodzenia związane z procesem SDLC, niepowodzenia związane z podmiotami zewnętrznymi, nadużycia związane z autoryzacją, wykorzystanie podatności w oprogramowaniu, manipulacja infrastrukturą SDLC, ataki typu Denial of Service, manipulacja danymi, ujawnienie, utrata/wyciek danych.
Utrzymanie	Zagrożenia wewnętrzne, haktywizm, przerwy w działaniu usług komunalnych, przerwy w działaniu sieci, nieumyślne zmiany, błędne użycie urządzeń i systemów lub błędne administrowanie nimi, szkody spowodowane przez podmioty zewnętrzne, sabotaż, wandalizm i kradzież, ataki z dostępem fizycznym, wymuszony dostęp, wymogi kontraktowe, podatności w oprogramowaniu, niepowodzenia związane z procesem SDLC, niepowodzenia związane z podmiotami zewnętrznymi, niespełnienie wymogów kontraktowych (np. dotyczących utrzymywania oprogramowania), niepowodzenia w utrzymywaniu, nadużycia związane z autoryzacją, wykorzystanie podatności w oprogramowaniu, manipulacja infrastrukturą SDLC, ataki typu Denial of Service, manipulacja danymi, ujawnienie, utrata/wyciek danych
Elementy oprogramowania	Zagrożenia wewnętrzne, haktywizm, utrata wsparcia, nieumyślne zmiany, błędne użycie urządzeń i systemów lub błędne administrowanie nimi, szkody spowodowane przez podmioty zewnętrzne, wyciek informacji, sabotaż, wandalizm i kradzież, ataki z dostępem fizycznym, wymuszony dostęp, wymogi kontraktowe, podatności w oprogramowaniu, niepowodzenia związane z procesem SDLC, niepowodzenia związane z podmiotami zewnętrznymi, niespełnienie wymogów kontraktowych (np. dotyczących utrzymywania oprogramowania), niepowodzenia w utrzymywaniu, nadużycia związane z autoryzacją, wykorzystanie podatności w oprogramowaniu, manipulacja infrastrukturą SDLC, ataki typu Denial of Service, manipulacja danymi, ujawnienie, utrata/wyciek danych

Zagrożenia związane z nowymi technologiami

Inteligentne samochody

POWIĄZANE ELEMENTY – GRUPY ZASOBÓW	NARAŻENIE NA ZAGROŻENIA
Czujniki i aktuatory samochodu	Ataki typu Denial of Service, złośliwe oprogramowanie, manipulacja danymi, ataki ukierunkowane na OEM, nieautoryzowane działania, kradzież tożsamości, nadużycia związane z autoryzacją, zagrożenia ukierunkowane na czujniki autonomiczne, zagrożenia ukierunkowane na sztuczną inteligencję i język maszynowy, sabotaż, wandalizm, kradzież, ataki bocznym kanałem, wstrzykiwanie błędów, awaria lub usterka czujnika/aktuatora, wykorzystanie podatności w oprogramowaniu, przechwycenie protokołu komunikacyjnego, atak typu „man-in-the-middle" / przechwytywanie sesji, nieumyślna zmiana danych lub konfiguracji komponentów pojazdu, wykorzystywanie danych lub urządzeń zniepewnych źródeł, błędne zastosowanie konfiguracji komponentów samochodu, przerwy w działaniu sieci, niespełnienie wymogów kontraktowych, naruszenie regulaminu / naruszenie prawa / naruszenie ochrony danych osobowych.
Algorytmy podejmowania decyzji **Sterowniki silników samochodowych, elementy odpowiedzialne za przetwarzanie i podejmowanie decyzji** **Infrastruktura inteligentnych samochodów i systemy backend**	Ataki typu Denial of Service (DoS), złośliwe oprogramowanie, manipulacja danymi, ataki ukierunkowane na OEM, nieautoryzowane działania, kradzież tożsamości, nadużycia związane z autoryzacją, manipulacja danymi, zagrożenia ukierunkowane na sztuczną inteligencję i język maszynowy, sabotaż, wandalizm, kradzież, awaria lub usterka czujnika/aktuatora, wykorzystanie podatności w oprogramowaniu, awaria lub zakłócenie usługi, przechwycenie protokołu komunikacyjnego, ponowne odtworzenie danych, atak typu „man-in-the-middle" / przechwytywanie sesji, nieumyślna zmiana danych lub konfiguracji komponentów pojazdu, wykorzystywanie danych lub urządzeń zniepewnych źródeł, błędne zastosowanie konfiguracji komponentów samochodu, utrata sygnału GNSS, przerwy w działaniu sieci, niespełnienie wymogów kontraktowych, naruszenie regulaminu / naruszenie prawa / naruszenie ochrony danych osobowych

POWIĄZANE ELEMENTY – GRUPY ZASOBÓW	NARAŻENIE NA ZAGROŻENIA
Funkcje pojazdu **Czujniki i aktuatory samochodu** **Sterowniki silników samochodowych, elementy odpowiedzialne za przetwarzanie i podejmowanie decyzji**	Ataki typu Denial of Service, złośliwe oprogramowanie, manipulacja danymi, ataki ukierunkowane na OEM, nieautoryzowane działania, kradzież tożsamości, nadużycia związane z autoryzacją, manipulacja danymi, zagrożenia ukierunkowane na czujniki autonomiczne, zagrożenia ukierunkowane na sztuczną inteligencję i język maszynowy, sabotaż, ataki bocznym kanałem, wstrzykiwanie błędów, kradzież, awaria lub usterka czujnika/aktuatora, wykorzystanie podatności w oprogramowaniu, awaria lub zakłócenie usługi, przechwycenie protokołu komunikacyjnego, ponowne odtworzenie danych, atak typu „man-in-the-middle" / przechwytywanie sesji, nieumyślna zmiana danych lub konfiguracji komponentów pojazdu, wykorzystywanie danych lub urządzeń z niepewnych źródeł, błędne zastosowanie konfiguracji komponentów samochodu, rozładowanie akumulatora samochodu, przerwy w działaniu sieci, niespełnienie wymogów kontraktowych, naruszenie regulaminu / naruszenie prawa / naruszenie ochrony danych osobowych
Zarządzanie oprogramowaniem **Sterowniki silników samochodowych, elementy odpowiedzialne za przetwarzanie i podejmowanie decyzji** **Elementy komunikacyjne wewnątrz pojazdu**	Ataki typu Denial of Service, złośliwe oprogramowanie, manipulacja danymi, ataki ukierunkowane na OEM, nieautoryzowane działania, kradzież tożsamości, nadużycia związane z autoryzacją, sabotaż, ataki bocznym kanałem, wstrzykiwanie błędów, kradzież, awaria lub usterka czujnika/aktuatora, wykorzystanie podatności w oprogramowaniu, awaria lub zakłócenie usługi, przechwycenie protokołu komunikacyjnego, atak typu „man-in-the-middle" / przechwytywanie sesji, nieumyślna zmiana danych lub konfiguracji komponentów pojazdu, wykorzystywanie danych lub urządzeń z niepewnych źródeł, przerwy w działaniu sieci, niespełnienie wymogów kontraktowych, naruszenie regulaminu / naruszenie prawa / naruszenie ochrony danych osobowych
Elementy komunikacyjne w pojeździe	Ataki typu Denial of Service, złośliwe oprogramowanie, manipulacja danymi, ataki ukierunkowane na OEM, nieautoryzowane działania, kradzież tożsamości, nadużycia związane z autoryzacją, manipulacja danymi, sabotaż, ataki bocznym kanałem, wstrzykiwanie błędów, kradzież, awaria lub usterka czujnika/ aktuatora, wykorzystanie podatności w oprogramowaniu, przechwycenie protokołu komunikacyjnego, ponowne odtworzenie danych, atak typu „man-in-the-middle" / przechwytywanie sesji, nieumyślna zmiana danych lub konfiguracji komponentów pojazdu, wykorzystywanie danych lub urządzeń z niepewnych źródeł, błędne zastosowanie konfiguracji komponentów samochodu, przerwy w działaniu sieci, niespełnienie wymogów kontraktowych, naruszenie regulaminu / naruszenie prawa / naruszenie ochrony danych osobowych

Zagrożenia związane z nowymi technologiami

Inteligentne samochody

POWIĄZANE ELEMENTY – GRUPY ZASOBÓW	NARAŻENIE NA ZAGROŻENIA
Sieci i protokoły komunikacyjne. Sterowniki silników samochodowych, elementy odpowiedzialne za przetwarzanie i podejmowanie decyzji Elementy komunikacyjne wewnątrz pojazdu	Ataki typu Denial of Service, złośliwe oprogramowanie, manipulacja danymi, ataki ukierunkowane na OEM, nieautoryzowane działania, kradzież tożsamości, nadużycia związane z autoryzacją, sabotaż, kradzież, awaria lub usterka czujnika/ aktuatora, wykorzystanie podatności w oprogramowaniu, przechwycenie protokołu komunikacyjnego, ponowne odtworzenie danych, atak typu „man-in-the-middle" / przechwytywanie sesji, nieumyślna zmiana danych lub konfiguracji komponentów pojazdu, wykorzystywanie danych lub urządzeń z niepewnych źródeł, błędne zastosowanie konfiguracji komponentów samochodu, przerwy w działaniu sieci, niespełnienie wymogów kontraktowych, naruszenie regulaminu / naruszenie prawa / naruszenie ochrony danych osobowych.
Pobliskie komponenty zewnętrzne **Infrastruktura inteligentnych samochodów i systemy backend**	Ataki typu Denial of Service, złośliwe oprogramowanie, manipulacja danymi, ataki ukierunkowane na OEM, nieautoryzowane działania, kradzież tożsamości, nadużycia związane z autoryzacją, manipulacja danymi, sabotaż, wandalizm, kradzież, wykorzystanie podatności w oprogramowaniu, awaria lub zakłócenie usługi, przechwycenie protokołu komunikacyjnego, atak typu „man-in-the-middle" / przechwytywanie sesji, nieumyślna zmiana danych lub konfiguracji komponentów pojazdu, wykorzystywanie danych lub urządzeń z niepewnych źródeł, utrata sygnału GNSS, przerwy w działaniu sieci, niespełnienie wymogów kontraktowych, naruszenie regulaminu / naruszenie prawa / naruszenie ochrony danych osobowych

POWIĄZANE ELEMENTY – GRUPY ZASOBÓW	NARAŻENIE NA ZAGROŻENIA
Serwery, systemy i chmury obliczeniowe Infrastruktura inteligentnych samochodów i systemy backend	Ataki typu Denial of Service, złośliwe oprogramowanie, manipulacja danymi, ataki ukierunkowane na OEM, nieautoryzowane działania, kradzież tożsamości, nadużycia związane z autoryzacją, manipulacja danymi, sabotaż, wykorzystanie podatności w oprogramowaniu, awaria lub zakłócenie usługi, przechwycenie protokołu komunikacyjnego, ponowne odtworzenie danych, atak typu „man-in-the-middle" / przechwytywanie sesji, nieumyślna zmiana danych lub konfiguracji komponentów pojazdu, wykorzystywanie danych lub urządzeń z niepewnych źródeł, utrata sygnału GNSS, przerwy w działaniu sieci, niespełnienie wymogów kontraktowych, naruszenie regulaminu / naruszenie prawa / naruszenie ochrony danych osobowych
Informacje	Ataki typu Denial of Service, złośliwe oprogramowanie, manipulacja danymi, ataki ukierunkowane na OEM, nieautoryzowane działania, kradzież tożsamości, nadużycia związane z autoryzacją, manipulacja danymi, zagrożenia ukierunkowane na czujniki autonomiczne, zagrożenia ukierunkowane na sztuczną inteligencję i język maszynowy, sabotaż, wandalizm, kradzież, ataki bocznym kanałem, wstrzykiwanie błędów, kradzież, awaria lub usterka czujnika/aktuatora, wykorzystanie podatności w oprogramowaniu, awaria lub zakłócenie usługi, przechwycenie protokołu komunikacyjnego, ponowne odtworzenie danych, atak typu „man-in-the-middle" / przechwytywanie sesji, nieumyślna zmiana danych lub konfiguracji komponentów pojazdu, wyciek informacji, wykorzystywanie danych lub urządzeń z niepewnych źródeł, błędne zastosowanie konfiguracji komponentów samochodu, utrata sygnału GNSS, przerwy w działaniu sieci, niespełnienie wymogów kontraktowych, naruszenie regulaminu / naruszenie prawa / naruszenie ochrony danych osobowych
Ludzie	Ataki typu Denial of Service, złośliwe oprogramowanie, manipulacja danymi, ataki ukierunkowane na OEM, nieautoryzowane działania, kradzież tożsamości, nadużycia związane z autoryzacją, manipulacja danymi, sabotaż, wandalizm, kradzież, awaria lub usterka czujnika/aktuatora, wykorzystanie podatności w oprogramowaniu, awaria lub zakłócenie usługi, przechwycenie protokołu komunikacyjnego, ponowne odtworzenie danych, atak typu „man-in-the-middle" / przechwytywanie sesji, nieumyślna zmiana danych lub konfiguracji komponentów pojazdu, wyciek informacji, wykorzystywanie danych lub urządzeń z niepewnych źródeł, błędne zastosowanie konfiguracji komponentów samochodu, utrata sygnału GNSS, rozładowanie akumulatora samochodu, przerwy w działaniu sieci, niespełnienie wymogów kontraktowych, naruszenie regulaminu / naruszenie prawa / naruszenie ochrony danych osobowych

Bibliografia

1. „April 2020 Cyber Attacks Statistics". 3 czerwca 2019 r. HACKMAGEDDON. https://www.hackmageddon.com/2020/06/03/april-2020-cyber-attacks-statistics/

2. „Data Breach Investigation Report" 2019. Verizon. https://enterprise.verizon.com/resources/reports/dbir/

3. „CIRCL – Operational Statistics" 2019. CIRCL. https://www.circl.lu/opendata/statistics/

4. „Survey: The Third Annual Study on the State of Endpoint Security Risk". 2020. https://engage.morphisec.com/2020-endpoint-security-risk-study

5. „Good Practices for Security of IoT – Secure Software Development Lifecycle". 19 listopada 2019 r. ENISA. https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1

6. „ENISA good practices for security of Smart Cars". 25 listopada 2019 r. https://www.enisa.europa.eu/publications/smart-cars

7. Kolejność sektorów ustalono, konsolidując statystyki dla raportów z poszczególnych incydentów. Dają one przeciętne wartości dla okresu raportowania (2019 – I kw. 2020), które mogą się nieco różnić od wartości przedstawionych w raportach miesięcznych lub kwartalnych.

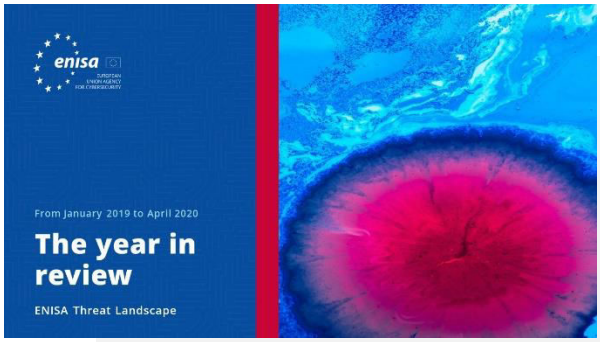
8. „Player vs. Hacker: Cyberthreats to Gaming Companies and Gamers". 16 marca 2020 r. Security Intelligence. https://securityintelligence.com/posts/player-vs-hacker-cyberthreats-to-gaming-companies-and-gamers/

9. Warto tu wspomnieć, że narażenie na zagrożenia oszacowano z uwzględnieniem szczegółowych kategorii zagrożeń opracowanych przez ENISA (patrz https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view), wykorzystywanych dla różnego rodzaju ocen sektorowych. Ponieważ dla nowych sektorów brakuje danych o incydentach, w celu wyczerpującego opracowania tematu przeprowadzono bardziej szczegółową ocenę zagrożeń.

„Uwzględniające kontekst rozpoznawanie cyberzagrożeń (cyber threat intelligence, CTI) dla sektorów to ważne narzędzie wspomagające przygotowanie i pozwalające na wyciąganie wniosków co do przewidywanych cyberataków w danym sektorze.”

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 **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 wywiadu dotyczącego cyberzagrożeń w UE.

Informacje o agencji

_ Agencja

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) jest unijną agencją działającą na rzecz osiągnięcia wysokiego ogólnego poziomu cyberbezpieczeństwa w całej Europie. Utworzona w roku 2004 i wzmocniona przez Akt o cyberbezpieczeństwie Agencja Unii Europejskiej ds. Cyberbezpieczeństwa wnosi wkład w politykę cybernetyczną UE; zwiększa wiarygodność produktów, usług i procesów informacyjno-komunikacyjnych dzięki systemom certyfikacji cyberbezpieczeństwa; współpracuje z państwami członkowskimi i organami UE oraz pomaga przygotować Europę na przyszłe wyzwania cybernetyczne. Poprzez wymianę informacji, budowanie zdolności i pogłębianie wiedzy Agencja współdziała z kluczowymi zainteresowanymi stronami, aby zwiększać zaufanie do gospodarki opartej na łączności i odporność unijnej infrastruktury oraz w efekcie, zapewnić cyfrowe bezpieczeństwo społeczeństwa i mieszkańców Europy. Więcej informacji na temat ENISA i jej działalności można znaleźć na stronie www.enisa.europa.eu.

Współautorzy

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) oraz *wszyscy członkowie ENISA CTI Stakeholders Group:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) i Thomas Hemker.

Wydawcy

Marco Barros Lourenço (ENISA) i Louis Marinos (ENISA).

Dane kontaktowe

Zapytania dotyczące tego dokumentu można kierować na adres enisa.threat.information@enisa.europa.eu.

Zapytania prasowe dotyczące tego dokumentu można kierować na adres press@enisa.europa.eu.

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

Zastrzeżenia prawne

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

Źródła zewnętrzne zostały odpowiednio zacytowane. ENISA nie ponosi odpowiedzialności za treść źródeł zewnętrznych, w tym zewnętrznych stron internetowych, do których odniesienia znajdują się w niniejszej publikacji.

Niniejsza publikacja ma charakter wyłącznie informacyjny. Musi ona być dostępna nieodpłatnie. Ani ENISA, ani żadna osoba działająca w jej imieniu nie ponoszą odpowiedzialności za wykorzystanie informacji zawartych w niniejszym sprawozdaniu.

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Grecja
Tel.: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu