Bezpieczeństwo systemów informatycznych

Wykład 1 – Wprowadzenie do cyberbezpieczeństwa

Marek Miśkiewicz

2025-12-27

Spis treści I

Organizacja i cele kursu

Informacje organizacyjne

- Przedmiot **Bezpieczeństwo systemów informatycznych** realizowany jest na I stopniu studiów kierunku Informatyka.
- Forma zajęć: wykład + laboratorium.
- Wykłady mają na celu przekazanie podstaw teoretycznych, laboratoria umożliwią praktyczne ćwiczenie omawianych zagadnień.
- Zaliczenie:
  - laboratoria: dwa kolokwia, zadania w trakcie semestru,
  - wykład: egzamin pisemny.
- Materiały dydaktyczne dostępne są na platformie MS Teams i na stronie z ćwiczeniami.
- Komunikacja ze studentami odbywa się głównie przez system uczelniany oraz podczas zajęć.

Efekty uczenia się

Po zakończeniu kursu student:

- definiuje i objaśnia podstawowe pojęcia związane z bezpieczeństwem systemów informatycznych, takie jak triada CIA, uwierzytelnianie, autoryzacja i kontrola dostępu;
- rozpoznaje najważniejsze zagrożenia i ataki, a także rozumie ich konsekwencje dla organizacji i użytkowników;
- zna podstawowe ramy, normy i regulacje (NIST CSF, ISO/IEC 27001, NIS2, RODO) i potrafi wyjaśnić ich rolę w kształtowaniu polityk bezpieczeństwa;
- potrafi wskazać zasady bezpiecznego projektowania systemów i aplikacji;
- rozumie znaczenie etyki i prawa w obszarze cyberbezpieczeństwa;
- posiada umiejętność krytycznego korzystania z raportów i źródeł aktualnych informacji o zagrożeniach.

Dlaczego bezpieczeństwo systemów?

Krajobraz zagrożeń

Bezpieczeństwo systemów informatycznych jest dziś jednym z kluczowych wyzwań organizacji i państw. Systemy cyfrowe są niezbędne do funkcjonowania administracji, gospodarki i życia codziennego, a jednocześnie stają się celem ataków.

- Wzrost liczby incydentów: ransomware, ataki typu DDoS, phishing, kompromitacja łańcucha dostaw.
- Coraz większa profesjonalizacja cyberprzestępców – grupy działają jak zorganizowane firmy.
- Cyberataki mają wymierne skutki ekonomiczne i społeczne: przerwy w dostępie do usług publicznych, straty finansowe, naruszenie prywatności obywateli.
- Wzrost znaczenia geopolitycznego cyberataków: operacje państwowe, cyberszpiegostwo, dezinformacja.

Krajobraz zagrożeń

Przykłady

- **Ransomware** - szyfrowanie danych i żądanie okupu.
- **Phishing i spear-phishing** - manipulacja psychologiczna, aby wyłudzić dane logowania.
- **Ataki DDoS** – paraliżowanie usług przez przeciążenie serwerów.
- **Malware ukierunkowane** - trojany, backdoory, rootkity pozwalające na przejęcie kontroli nad systemem.
- **Ataki na infrastrukturę krytyczną** - systemy energetyczne, transportowe czy wodociągowe.

Raporty i źródła aktualności

Aby śledzić zmieniający się krajobraz zagrożeń, należy korzystać z rzetelnych źródeł:

- **ENISA Threat Landscape** - coroczny raport Europejskiej Agencji ds. Cyberbezpieczeństwa podsumowujący najważniejsze trendy i incydenty.

  https://www.enisa.europa.eu/topics/threat-landscape

- **CISA KEV (Known Exploited Vulnerabilities Catalog)** – lista podatności faktycznie wykorzystywanych w atakach, publikowana i aktualizowana przez amerykańską agencję CISA.

  https://www.cisa.gov/known-exploited-vulnerabilities-catalog

- **Raporty firm komercyjnych** (np. Mandiant, Symantec, Kaspersky, Check Point) – przeglądy incydentów i analizy zagrożeń.

  https://www.mandiant.com/resources/reports

Raporty i źródła aktualności

- **CERT Polska** – analizy zagrożeń, ostrzeżenia o kampaniach phishingowych i podatnościach krytycznych.

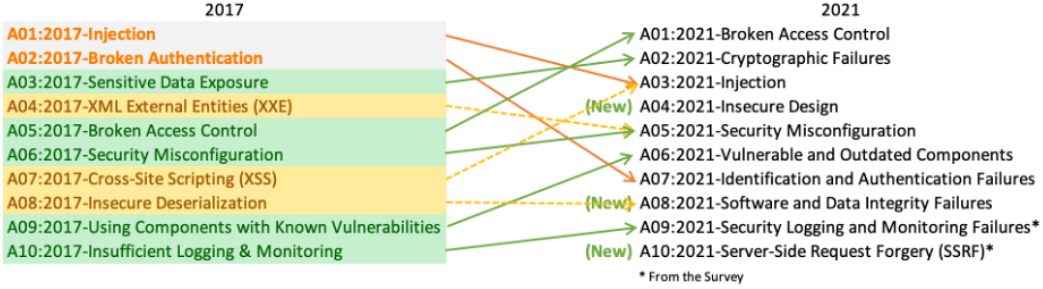
  https://cert.pl

- **OWASP i projekty otwartoźródłowe** – źródła wiedzy o podatnościach w aplikacjach webowych i API.

  https://owasp.org

Dlaczego to ważne?

- Krajobraz zagrożeń zmienia się dynamicznie – to, co było dominującym atakiem 5 lat temu, dziś może mieć marginalne znaczenie.



- Rozumienie aktualnych trendów pozwala na lepsze planowanie zabezpieczeń i priorytetyzację działań.
- Umiejętność analizy raportów i ostrzeżeń to kluczowa kompetencja każdego specjalisty ds. bezpieczeństwa.

Podstawowe pojęcia

Podstawowe pojęcia bezpieczeństwa informacji

Systemy informatyczne składają się z trzech podstawowych komponentów: **sprzętu, oprogramowania i komunikacji**. Celem bezpieczeństwa informacji jest ochrona danych w tych obszarach poprzez stosowanie branżowych standardów i mechanizmów zabezpieczeń.

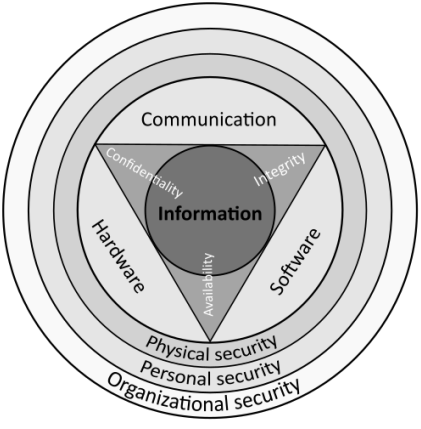
Podstawowe pojęcia bezpieczeństwa informacji

Ochrona realizowana jest na trzech poziomach:

- **fizycznym**,
- **personalnym**,
- **organizacyjnym**.

W centrum bezpieczeństwa znajduje się **informacja**, która musi zachować trzy kluczowe atrybuty:

- **poufność (Confidentiality)**,
- **integralność (Integrity)**,
- **dostępność (Availability)**.



Procedury i polityki bezpieczeństwa określają, w jaki sposób administratorzy, użytkownicy i operatorzy powinni korzystać z systemów i produktów, aby zapewnić właściwy poziom ochrony w organizacji.

Triada CIA i rozszerzenia

Triada CIA to fundament bezpieczeństwa systemów informatycznych. Składa się z trzech podstawowych atrybutów:

- **Poufność (Confidentiality)** – zapewnienie, że informacje są dostępne wyłącznie dla osób uprawnionych.
- **Integralność (Integrity)** – ochrona przed nieautoryzowaną modyfikacją danych, gwarancja spójności i poprawności informacji.
- **Dostępność (Availability)** – zapewnienie, że systemy i dane są dostępne zawsze wtedy, gdy są potrzebne uprawnionym użytkownikom.

Triada CIA – przykłady

- Poufność: szyfrowanie danych przesyłanych przez sieć, stosowanie haseł i mechanizmów wieloskładnikowych.
- Integralność: sumy kontrolne, podpisy cyfrowe, mechanizmy kontroli wersji.
- Dostępność: redundancja serwerów, kopie zapasowe, ochrona przed atakami DDoS.

Rozszerzenia triady CIA

Współczesne podejście do bezpieczeństwa systemów informatycznych poszerza tradycyjną triadę o kolejne atrybuty:

- **Autentyczność (Authenticity)** – pewność, że dane i tożsamości pochodzą od deklarowanego źródła.
- **Rozliczalność (Accountability)** – możliwość powiązania działań w systemie z konkretnym użytkownikiem lub procesem.
- **Niezaprzeczalność (Non-repudiation)** – gwarancja, że nadawca nie może wyprzeć się wysłania komunikatu, a odbiorca – jego odebrania.

Triada CIA i rozszerzenia

Znaczenie

- CIA + rozszerzenia tworzą fundament polityk i systemów bezpieczeństwa.
- W praktyce atrybuty te bywają w konflikcie – np. wysoki poziom poufności może utrudniać dostępność.
- Zrozumienie równowagi między atrybutami jest kluczowe dla projektowania i zarządzania systemami informatycznymi.

Modele bezpieczeństwa

Modele bezpieczeństwa to formalne lub półformalne opisy tego, jak system informatyczny powinien chronić zasoby i kontrolować dostęp. Są one fundamentem projektowania systemów operacyjnych, baz danych i aplikacji.

Dwa podstawowe modele to

- **BLP**
- **Biba**

Model Bell-LaPadula (BLP)

- skoncentrowany na ochronie poufności danych. Został opracowany w latach 70. XX wieku dla systemów wojskowych i rządowych, gdzie kluczowe było zapobieganie nieuprawnionemu ujawnieniu informacji.
- **Reguła „no read up" (simple security property)** – użytkownik na niższym poziomie uprawnień nie może czytać danych oznaczonych jako bardziej poufne.
  Przykład: pracownik z klauzulą „zastrzeżone" nie może odczytać dokumentu „ściśle tajne".
- **Reguła „no write down" (star property)** – użytkownik na wyższym poziomie uprawnień nie może zapisywać danych na poziomie niższym, aby zapobiec ich przypadkowemu lub celowemu wyciekom.
  Przykład: analityk z dostępem do informacji „tajne" nie może zapisać ich w pliku dostępnym dla pracowników z niższymi uprawnieniami.

Model Kennetha J. Biba

- skoncentrowany na ochronie integralności danych. Został zaprojektowany jako przeciwieństwo Bell-LaPadula, z myślą o zapewnieniu, że dane pozostaną wiarygodne i nie zostaną zanieczyszczone przez mniej zaufane źródła.
- **Reguła „no write up" (integrity star property)** – użytkownik z niższym poziomem integralności nie może modyfikować danych na poziomie wyższym.
  Przykład: aplikacja niskiego zaufania nie może zmieniać konfiguracji systemu operacyjnego.
- **Reguła „no read down" (simple integrity property)** – użytkownik na wyższym poziomie integralności nie może czytać danych z poziomu niższego, aby nie opierać swoich decyzji na danych potencjalnie zafałszowanych.
  Przykład: administrator systemu nie może wykorzystywać niesprawdzonych danych wejściowych z aplikacji niezweryfikowanej.

Modele bezpieczeństwa – przykłady

Model Clark-Wilson

Model Clark-Wilson opiera się na koncepcji dobrze uformowanych transakcji i obowiązkowej kontroli dostępu do danych biznesowych. Jego głównym celem jest zapewnienie integralności danych w środowiskach komercyjnych.

- Dane mogą być modyfikowane tylko poprzez zatwierdzone i zweryfikowane programy (tzw. well-formed transactions).
- Wprowadza obowiązek rozdzielenia obowiązków (separation of duties), co zmniejsza ryzyko nadużyć.
- Przykład: system bankowy, w którym jeden pracownik wprowadza przelew, a inny go zatwierdza.

Modele bezpieczeństwa – przykłady

Model Brewer-Nash (Chinese Wall)

Model Brewer-Nash, nazywany także modelem „chińskiego muru”, opiera się na dynamicznej kontroli dostępu. Jego celem jest unikanie konfliktu interesów, szczególnie w środowiskach doradczych i finansowych.

- Użytkownik może uzyskać dostęp do danych określonej firmy, ale wówczas automatycznie traci możliwość dostępu do poufnych danych firm konkurencyjnych.
- Decyzje o dostępie zależą od historii wcześniejszych działań użytkownika.
- Przykład: analityk finansowy pracujący nad dokumentacją jednej spółki nie może później pracować nad dokumentami konkurenta.

Modele bezpieczeństwa – przykłady

Model RBAC (Role-Based Access Control)

RBAC to model kontroli dostępu oparty na rolach. Zamiast przypisywać uprawnienia bezpośrednio użytkownikom, system przypisuje je do ról, a użytkownicy otrzymują role zgodne z ich funkcją w organizacji.

- Upraszcza zarządzanie uprawnieniami w dużych systemach.
- Role można łatwo modyfikować i przypisywać nowym pracownikom.
- Przykład: w organizacji role mogą obejmować „administrator systemu”, „pracownik działu HR” czy „użytkownik standardowy”.

Modele bezpieczeństwa

Znaczenie modeli

- Modele bezpieczeństwa są podstawą implementacji mechanizmów kontroli dostępu.
- Pozwalają zrozumieć kompromisy między poufnością, integralnością a dostępnością.
- Wspierają projektowanie systemów zgodnych z wymaganiami prawnymi i normami (np. ISO/IEC 27001).
- Choć wywodzą się z teorii, znajdują praktyczne zastosowania w systemach operacyjnych, bazach danych i systemach krytycznych.

Klasyfikacja zasobów i zagrożeń

Klasyfikacja zasobów informatycznych jest podstawą skutecznego zarządzania bezpieczeństwem. Pozwala określić, które elementy infrastruktury wymagają szczególnej ochrony, a także jakie ryzyka są z nimi związane.

- **Zasoby informacyjne** – dane przechowywane w systemach (np. dokumenty, bazy danych, archiwa).
- **Zasoby techniczne** – sprzęt i oprogramowanie (serwery, stacje robocze, urządzenia sieciowe).
- **Zasoby ludzkie** – użytkownicy systemów, administratorzy, pracownicy organizacji.
- **Zasoby organizacyjne** – procesy biznesowe, polityki bezpieczeństwa, procedury.

Klasyfikacja zagrożeń

Zagrożenia można podzielić według różnych kryteriów. Najczęściej stosowany podział obejmuje:

- **Zagrożenia naturalne** – np. pożar, powódź, trzęsienie ziemi, awarie infrastruktury energetycznej.
- **Zagrożenia techniczne** – wynikające z awarii sprzętu, błędów oprogramowania, utraty zasilania.
- **Zagrożenia ludzkie – nieumyślne** – np. przypadkowe usunięcie danych, błędy konfiguracji, utrata nośników.
- **Zagrożenia ludzkie – umyślne** – działania przestępcze, sabotaż, cyberataki prowadzone w celu osiągnięcia korzyści lub wyrządzenia szkody.

Dlaczego klasyfikacja jest ważna?

- Ułatwia priorytetyzację działań w ramach polityki bezpieczeństwa – nie wszystkie zasoby są jednakowo istotne.
- Pozwala lepiej planować środki ochrony i inwestycje w bezpieczeństwo.
- Stanowi fundament oceny ryzyka i zgodności z normami (np. ISO/IEC 27005).
- Umożliwia skuteczniejsze reagowanie na incydenty poprzez wcześniejsze przypisanie wartości i krytyczności zasobom.

Ramy i normy

NIST Cybersecurity Framework 2.0

Wprowadzenie

NIST Cybersecurity Framework (CSF) to dokument opracowany przez **National Institute of Standards and Technology (NIST)** w USA. Jest to zestaw wytycznych, najlepszych praktyk i standardów, które pomagają organizacjom zarządzać ryzykiem cyberbezpieczeństwa.

- Pierwsza wersja powstała w 2014 roku, głównie dla infrastruktury krytycznej.
- W lutym 2024 opublikowano **wersję 2.0**, która rozszerza zakres na wszystkie organizacje, niezależnie od sektora czy wielkości.
- Strona oficjalna: https://www.nist.gov/cyberframework

NIST CSF 2.0

Struktura

Framework opiera się na sześciu głównych funkcjach, które obejmują pełny cykl zarządzania bezpieczeństwem:

1. **Govern (GOV)** – ustanawianie strategii, polityk i ról odpowiedzialnych za cyberbezpieczeństwo.
2. **Identify (ID)** – rozpoznanie zasobów, środowiska i ryzyk.
3. **Protect (PR)** – wdrożenie środków zabezpieczających zasoby i dane.
4. **Detect (DE)** – zdolność do wykrywania incydentów i anomalii.
5. **Respond (RS)** – podejmowanie działań zaradczych i ograniczających skutki incydentu.
6. **Recover (RC)** – przywracanie systemów i usług do normalnego działania po incydencie.

Źródło: NIST CSF 2.0 – dokument PDF

Zastosowanie

- Framework nie jest normą obowiązkową, lecz **dobrowolnym przewodnikiem** stosowanym globalnie.
- Ułatwia budowę systemów zarządzania bezpieczeństwem i integrację z innymi normami, np. ISO/IEC 27001.
- Pomaga organizacjom:
  - ocenić dojrzałość w obszarze cyberbezpieczeństwa,
  - ustalić priorytety działań,
  - komunikować ryzyka i potrzeby między zespołami technicznymi a zarządem.
- Może być stosowany w małych firmach, organizacjach non-profit i dużych korporacjach.

Profil startowy

- CSF 2.0 wprowadza tzw. **Profile**, które odzwierciedlają stan obecny i docelowy organizacji.
- **Profil startowy** pozwala organizacji ocenić, gdzie się znajduje w kontekście bezpieczeństwa i jakie działania są najpilniejsze.
- Wersja 2.0 zawiera także przewodniki dla małych i średnich przedsiębiorstw.
- Przykład zastosowania: organizacja może wskazać, że mocno rozwinęła funkcje **Protect** i **Detect**, ale zaniedbuje obszar **Recover** – co ujawnia luki w planowaniu ciągłości działania.

Źródło: NIST CSF 2.0 Resource Center

Wprowadzenie

ISO/IEC 27001 to międzynarodowa norma określająca wymagania dla Systemu Zarządzania Bezpieczeństwem Informacji (ISMS). Jest najczęściej stosowaną normą w obszarze cyberbezpieczeństwa i zarządzania ryzykiem informacyjnym.

- Pierwsze wydanie: 2005 r.
- Aktualna wersja: **ISO/IEC 27001:2022**, która zastąpiła wersję z 2013 roku.
- Norma jest certyfikowalna – organizacje mogą uzyskać niezależne potwierdzenie spełniania jej wymagań.
- Strona oficjalna: https://www.iso.org/standard/82875.html

ISO/IEC 27001:2022

Główne założenia

- Oparta na cyklu **PDCA (Plan–Do–Check–Act)**, znanym z innych systemów zarządzania (np. ISO 9001).
- Celem jest zapewnienie **ciągłego doskonalenia** bezpieczeństwa informacji.
- Uwzględnia podejście oparte na **analizie ryzyka** – organizacja identyfikuje ryzyka i dobiera odpowiednie zabezpieczenia.
- Skupia się nie tylko na technologii, ale także na procesach i ludziach.

Źródło: ISO/IEC 27001 overview – IT Governance

ISO/IEC 27001:2022

Kluczowe zmiany

Wersja z 2022 r. wprowadziła istotne modyfikacje w porównaniu do edycji 2013:

- Uproszczona struktura załącznika A – kontrole bezpieczeństwa zostały zredukowane z 114 do 93.
- Zastosowano 4 kategorie kontroli: organizacyjne, ludzkie, fizyczne, technologiczne.
- Dodano nowe obszary, m.in.:
  - ochrona danych w chmurze,
  - zarządzanie tożsamością,
  - gotowość na incydenty,
  - monitoring i analiza bezpieczeństwa.
- Zwiększony nacisk na integrację z innymi systemami zarządzania ISO (np. ISO 22301 – ciągłość działania).

Źródło: ISO/IEC 27001:2022 update – BSI Group

ISO/IEC 27001:2022 –

Zastosowanie

- Stosowana globalnie w sektorze prywatnym, publicznym i organizacjach non-profit.
- Certyfikacja zwiększa zaufanie klientów, partnerów i regulatorów.
- Pomaga spełniać wymagania prawne i regulacyjne (np. RODO, NIS2).
- Integruje się z innymi normami bezpieczeństwa, w tym z **ISO/IEC 27002** (szczegółowe wytyczne do kontroli).

Przykład praktyczny:

Firma wdraża ISO/IEC 27001, aby zapewnić zgodność z wymaganiami klientów z sektora finansowego i jednocześnie usprawnić procesy bezpieczeństwa wewnętrznego.

NIST CSF 2.0 vs ISO/IEC 27001:2022 – porównanie

Cecha / aspekt	**NIST CSF 2.0**	**ISO/IEC 27001:2022**
Charakter	Ramy dobrych praktyk, przewodnik	Norma międzynarodowa, certyfikowalna
Obowiązkowość	Dobrowolny, stosowany globalnie	Może być wymagany przez klientów/regulatorów
Zakres	Cyberbezpieczeństwo (szeroko, w tym governance)	System Zarządzania Bezpieczeństwem Informacji (ISMS)
Struktura	6 funkcji: Govern, Identify, Protect, Detect, Respond, Recover	Cykl PDCA, wymagania + 93 kontrole w 4 kategoriach
Cel główny	Ocena dojrzałości, priorytetyzacja działań, komunikacja	Budowa i certyfikacja ISMS, ciągłe doskonalenie
Docelowi użytkownicy	Wszystkie organizacje, niezależnie od sektora i wielkości	Organizacje chcące formalnie zarządzać bezpieczeństwem i uzyskać certyfikat
Relacja	Może być używany jako punkt wyjścia i uzupełnienie ISO 27001	Może być wzbogacony o elementy CSF w zakresie oceny dojrzałości

Regulacje i prawo

Dyrektywa NIS2

Wprowadzenie

Dyrektywa NIS2 (ang. **Network and Information Security Directive 2**) to akt prawny Unii Europejskiej przyjęty w grudniu 2022 r., który zastąpił wcześniejszą dyrektywę NIS z 2016 r. Celem NIS2 jest podniesienie poziomu bezpieczeństwa sieci i systemów informatycznych w całej UE.

- Wejście w życie: **16 stycznia 2023**
- Termin implementacji do prawa krajowego: **17 października 2024**
- Tekst aktu: EUR-Lex – Dyrektywa (UE) 2022/2555

Zakres podmiotowy

Obowiązki dyrektywy obejmują:

- **Operatorów usług kluczowych** (np. energia, transport, zdrowie, bankowość, infrastruktura cyfrowa).
- **Podmioty ważne i istotne** (np. poczta i usługi kurierskie, gospodarka odpadami, produkcja urządzeń krytycznych).
- **Dostawców usług cyfrowych** (np. usługi chmurowe, platformy handlu elektronicznego).

Nowością w stosunku do NIS1 jest znaczne rozszerzenie listy sektorów i firm objętych regulacją.

Wymagania

Organizacje objęte NIS2 muszą:

- wdrożyć **zarządzanie ryzykiem** w obszarze cyberbezpieczeństwa,
- stosować środki techniczne i organizacyjne, m.in. w zakresie:
  - polityk bezpieczeństwa,
  - obsługi incydentów,
  - zarządzania kryzysowego i ciągłości działania,
  - bezpieczeństwa łańcucha dostaw,
  - kryptografii i kontroli dostępu.
- zgłaszać **poważne incydenty** (wstępne powiadomienie w ciągu 24h, raport szczegółowy w ciągu 72h).

Dyrektywa NIS2

Konsekwencje

- Państwa członkowskie ustanawiają krajowe organy nadzorcze i system kar za naruszenia.
- Sankcje mogą obejmować:
  - kary finansowe (do 10 mln EUR lub 2% globalnego obrotu rocznego firmy),
  - odpowiedzialność zarządu za brak wdrożenia wymaganych środków.
- Dyrektywa wspiera harmonizację regulacji w UE i współpracę transgraniczną w reagowaniu na incydenty.

DORA – Digital Operational Resilience Act

DORA - Digital Operational Resilience Act (Rozporządzenie (UE) 2022/2554) to akt prawny UE dotyczący odporności cyfrowej w sektorze finansowym. Obowiązuje od **16 stycznia 2023**, i zaczął być stosowany **od 17 stycznia 2025**.

- Cel: zapewnienie odporności operacyjnej instytucji finansowych wobec incydentów ICT.
- Zakres: banki, ubezpieczyciele, fundusze inwestycyjne, giełdy, firmy świadczące usługi płatnicze, a także dostawcy technologii ICT działający na rzecz sektora finansowego.
- Tekst aktu: EUR-Lex – Rozporządzenie (UE) 2022/2554

Wymagania

Instytucje finansowe muszą:

- wdrożyć **system zarządzania ryzykiem ICT** (identyfikacja, ochrona, wykrywanie, reagowanie, przywracanie),
- przeprowadzać **testy penetracyjne i odpornościowe** (np. TLPT – Threat-Led Penetration Testing),
- ustanowić procedury raportowania incydentów ICT do właściwych organów,
- zarządzać ryzykiem w łańcuchu dostaw ICT (umowy z dostawcami).

Konsekwencje naruszeń: wysokie kary finansowe oraz ryzyko ograniczenia działalności.
Link: https://resilia.pl/blog

Cyber Resilience Act (CRA)

Cyber Resilience Act (Rozporządzenie (UE) 2024/2847) to nowe europejskie prawo dotyczące bezpieczeństwa produktów z komponentami cyfrowymi. Akt dotyczący cyberodporności wszedł w życie 10 grudnia 2024 r. Główne obowiązki wprowadzone ustawą będą miały zastosowanie od dnia 11 grudnia 2027 r.

- Cel: zapewnienie, że sprzęt i oprogramowanie sprzedawane na rynku UE spełnia minimalne wymogi cyberbezpieczeństwa.
- Zakres: wszystkie produkty z elementami cyfrowymi – od urządzeń IoT, przez systemy przemysłowe, po oprogramowanie.
- Tekst aktu: EUR-Lex – Rozporządzenie (UE) 2024/2847

Cyber Resilience Act

Wymagania

Producenci i dostawcy muszą:

- projektować produkty zgodnie z zasadą **security by design i by default**,
- prowadzić ocenę ryzyka i dokumentację techniczną,
- zgłaszać podatności i incydenty bezpieczeństwa do **ENISA** w ciągu 24 godzin od wykrycia,
- zapewniać aktualizacje i poprawki bezpieczeństwa przez cały cykl życia produktu.

DORA vs CRA – porównanie

Cecha / zakres	**DORA**	**Cyber Resilience Act (CRA)**
Obszar	Sektor finansowy i jego dostawcy ICT	Wszystkie produkty z komponentami cyfrowymi
Charakter	Rozporządzenie sektorowe	Rozporządzenie horyzontalne
Główne wymagania	Zarządzanie ryzykiem ICT, testy, raportowanie incydentów, łańcuch dostaw	Security by design, zgłaszanie podatności, aktualizacje
Adresaci	Banki, ubezpieczyciele, instytucje finansowe, dostawcy ICT	Producenci, importerzy i dystrybutorzy produktów cyfrowych
Data stosowania	od 17 stycznia 2025	od 11 grudnia 2024 r.

Wprowadzenie

RODO (ang. GDPR – General Data Protection Regulation, Rozporządzenie o ochronie danych osobowych (UE) 2016/679) to unijne rozporządzenie dotyczące ochrony danych osobowych. Obowiązuje od **25 maja 2018 roku** we wszystkich państwach członkowskich UE.

- Cel: ujednolicenie przepisów dotyczących ochrony danych osobowych w UE.
- Dotyczy każdej organizacji przetwarzającej dane osobowe osób fizycznych na terenie UE.
- Tekst aktu: EUR-Lex – Rozporządzenie (UE) 2016/679

Podstawowe zasady

RODO opiera się na siedmiu głównych zasadach przetwarzania danych:

1. **Zgodność z prawem, rzetelność i przejrzystość** – dane muszą być przetwarzane w sposób legalny i przejrzysty.
2. **Ograniczenie celu** – dane zbierane tylko w określonych, legalnych celach.
3. **Minimalizacja danych** – przetwarzanie wyłącznie danych niezbędnych do celu.
4. **Prawidłowość** – dane muszą być poprawne i aktualne.
5. **Ograniczenie przechowywania** – dane przechowywane nie dłużej niż jest to konieczne.
6. **Integralność i poufność** – ochrona przed nieuprawnionym dostępem i modyfikacją.
7. **Rozliczalność** – administrator musi być w stanie wykazać zgodność z zasadami.

Źródło: European Data Protection Board

Prawa osób, których dane dotyczą

Osoby fizyczne mają szerokie prawa wynikające z RODO, m.in.:

- Prawo dostępu do swoich danych.
- Prawo do sprostowania danych.
- Prawo do usunięcia danych („prawo do bycia zapomnianym”).
- Prawo do ograniczenia przetwarzania.
- Prawo do przenoszenia danych do innego administratora.
- Prawo do sprzeciwu wobec przetwarzania danych.

Obowiązki administratorów i podmiotów przetwarzających

- Prowadzenie rejestru czynności przetwarzania danych.
- Stosowanie **privacy by design** i **privacy by default**.
- Zapewnienie odpowiednich środków technicznych i organizacyjnych dla ochrony danych.
- Obowiązek zgłaszania naruszeń ochrony danych do organu nadzorczego w ciągu 72h.
- Powołanie Inspektora Ochrony Danych (IOD) w niektórych organizacjach.

Sankcje i znaczenie praktyczne

- Naruszenie przepisów RODO może skutkować karami finansowymi:
  - do 20 mln EUR, lub
  - do 4% całkowitego rocznego obrotu przedsiębiorstwa – w zależności od tego, która kwota jest wyższa.
- RODO powinno mieć wpływ na praktyki IT, w tym:
  - projektowanie systemów z myślą o ochronie danych,
  - uwzględnianie minimalizacji danych w aplikacjach,
  - konieczność raportowania incydentów bezpieczeństwa danych osobowych.

Wprowadzenie

EUCC (European Union Cybersecurity Certification Scheme) to unijny system certyfikacji bezpieczeństwa ICT. Powstał w oparciu o **Rozporządzenie (UE) 2019/881 – tzw. Cybersecurity Act**, które wprowadziło ramy europejskiej certyfikacji cyberbezpieczeństwa.

- EUCC opiera się na międzynarodowym standardzie **Common Criteria (ISO/IEC 15408)**.
- Zastępuje krajowe schematy (np. niemiecki BSI, francuski ANSSI, hiszpański CCN) wspólnym europejskim podejściem.
- Koordynacją zajmuje się **ENISA (European Union Agency for Cybersecurity)**.
- Strona ENISA o EUCC: https://www.enisa.europa.eu/topics/certification/eucc

Cele i znaczenie

- Ujednolicenie systemów certyfikacji cyberbezpieczeństwa w UE.
- Ułatwienie wzajemnego uznawania certyfikatów między państwami członkowskimi.
- Zwiększenie zaufania do produktów ICT poprzez jednolite wymagania bezpieczeństwa.
- Wsparcie dla rynku wewnętrznego – producenci nie muszą uzyskiwać wielu certyfikatów w różnych krajach.

Poziomy zapewnienia bezpieczeństwa

EUCC definiuje różne poziomy zapewnienia bezpieczeństwa:

- **Basic (podstawowy)** – minimalny poziom ochrony.
- **Substantial (znaczący)** – ochrona przed bardziej zaawansowanymi zagrożeniami.
- **High (wysoki)** – dla produktów wymagających najwyższego poziomu bezpieczeństwa (np. infrastruktura krytyczna).

Każdy poziom określa zestaw wymagań dotyczących projektowania, testowania i oceny produktu.
Źródło: ENISA – EUCC

Zastosowanie w praktyce

- Stosowany do produktów i systemów ICT – np. sprzętu sieciowego, oprogramowania zabezpieczającego, systemów przemysłowych.
- Certyfikaty wydawane są przez akredytowane jednostki oceniające w państwach członkowskich.
- EUCC ułatwia instytucjom publicznym i firmom wybór produktów o potwierdzonym poziomie bezpieczeństwa.
- Przykład: producent firewalli uzyskuje certyfikat EUCC na poziomie „High”, co potwierdza ich przydatność w infrastrukturze krytycznej.

EUCC vs ISO/IEC 27001 vs NIST CSF – porównanie

Cecha / aspekt	EUCC (oparty na Common Criteria)	ISO/IEC 27001:2022	NIST CSF 2.0
Charakter	Schemat certyfikacji produktów ICT	Norma systemu zarządzania bezpieczeństwem	Ramy dobrych praktyk, przewodnik
Zakres	Produkty i systemy ICT (sprzęt, oprogramowanie)	Organizacja i procesy (ISMS)	Organizacja i procesy (cybersecurity risk mgmt)
Certyfikacja	Tak – certyfikat wydawany przez jednostki akredytowane	Tak – audyt i certyfikat ISMS	Nie – stosowanie dobrowolne, brak certyfikacji
Poziomy	Basic, Substantial, High	Brak poziomów, zgodność / niezgodność	Brak poziomów, stosowanie profili
Cel główny	Potwierdzenie bezpieczeństwa konkretnego produktu	Budowa i utrzymanie systemu zarządzania bezpieczeństwem informacji	Ocena dojrzałości, priorytetyzacja działań
Organ nadzorczy	ENISA + krajowe jednostki certyfikujące	ISO + jednostki akredytujące (np. BSI, TÜV)	NIST (USA), stosowany globalnie

Modele zagrożeń i podatności

CVE – Common Vulnerabilities and Exposures

CVE to globalny system identyfikacji podatności, utrzymywany przez MITRE i sponsorowany przez US CISA. Każda luka bezpieczeństwa otrzymuje unikalny numer CVE, np. *CVE-2024-12345*.

- Celem CVE jest zapewnienie **jednoznacznego odniesienia** dla podatności i ekspozycji w różnych bazach i narzędziach.
- CVE nie zawiera szczegółowych informacji technicznych, a jedynie standardowy identyfikator i krótki opis.
- Na CVE opierają się:
  - **CVSS** – ocena wagi podatności,
  - **KEV** – lista podatności faktycznie wykorzystywanych,
  - **NVD (National Vulnerability Database)** i inne bazy bezpieczeństwa.

Źródło: https://www.cve.org

CVE™ Program Mission

Identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

There are currently over **295,000** CVE Records accessible via **Download** or **Keyword Search** above.

The CVE Program partners with community members worldwide to grow CVE content and expand its usage. Click below to learn more about the role of **CVE Numbering Authorities (CNAs)** and **Roots**.

Learn More | Become a Partner

Access

- List of Partners
- CNA Rules
- CVE Record Lifecycle
- CVEProject on GitHub for Development
- Idea tracker

Learn

- About CVE
- Process
- Program Organization
- CVE 25th Anniversary Report
- Related Efforts
- Terminology
- CVE Services for CNAs

Report/Request

- Report vulnerability/Request CVE ID
- Request CVE Record be published/updated
- Report the use of a reserved CVE ID

News

- Searching for Patterns Now Available in "CVE List Keyword Search" on CVE.ORG Website
- HackRTU Added as CVE Numbering Authority (CNA)
- Vulnerability Data Enrichment for CVE Records: 243 CNAs on the Enrichment Recognition List for September 2, 2025
- CVE Program Report for Quarter 2 Calendar Year (Q2 CY) 2025

NEWS ICONS

MORE NEWS

Events

Przykłady historycznie ważnych CVE

- **CVE-2017-0144 (EternalBlue)** — podatność w protokole SMBv1 w systemach Windows, wykorzystana do ataków WannaCry oraz NotPetya. Pozwalała na zdalne wykonanie kodu i była szczególnie groźna ze względu na automatyczne rozprzestrzenianie się po sieci bez interakcji użytkownika.
- **CVE-2021-44228 (Log4Shell)** — krytyczna luka w bibliotece Apache Log4j, pozwalająca na zdalne wykonanie kodu przez wysłanie odpowiednio skonstruowanego żądania. Szeroko wykorzystywana przez cyberprzestępców do kompromitacji serwerów na całym świecie.
- **CVE-2019-0708 (BlueKeep)** — podatność w usłudze RDP w systemach Windows, umożliwiająca zdalne wykonanie kodu przez nieuwierzytelnionego użytkownika. Uznana za krytyczną ze względu na możliwość automatycznego rozprzestrzeniania się (wormable).
- **CVE-2010-2568** — luka wykorzystywana przez robaka Stuxnet do ataku na infrastruktury przemysłowe (systemy SCADA). To jeden z pierwszych przypadków zaawansowanej cyberbroni wykorzystywanej do sabotażu infrastruktury krytycznej.

- **CVE-2015-5119** — podatność typu „use-after-free” w Adobe Flash, szeroko wykorzystywana przez grupy APT i przestępców na całym świecie do ataków przez przeglądarkę internetową.
- **CVE-2017-5638** — krytyczna luka w frameworku Apache Struts 2, która umożliwiła masowy wyciek danych z Equifax — jednej z największych firm kredytowych na świecie.
- **CVE-2016-5195 (Dirty COW)** — bardzo znana luka w jądrze Linuksa, pozwalająca na eskalację uprawnień lokalnych użytkowników do roota przez mechanizm copy-on-write. Trudna do wykrycia, nie zostawiała śladów w logach systemowych.
- **CVE-2024-3094 (XZ Utils Backdoor)** — zaawansowana podatność (backdoor) w bibliotece xz (liblzma), wykryta w marcu 2024, potencjalnie umożliwiająca zdalne przejęcie kontroli nad wieloma systemami Linux.
- **CVE-2014-0160 (Heartbleed)** — słynna luka w bibliotece OpenSSL, pozwalająca na odczytanie części pamięci serwera, w tym kluczy prywatnych i danych użytkowników. Szybko zyskała ogromny rozgłos i spowodowała falę pilnych aktualizacji na świecie.

Dodatkowe przykłady szeroko wykorzystywanych CVE

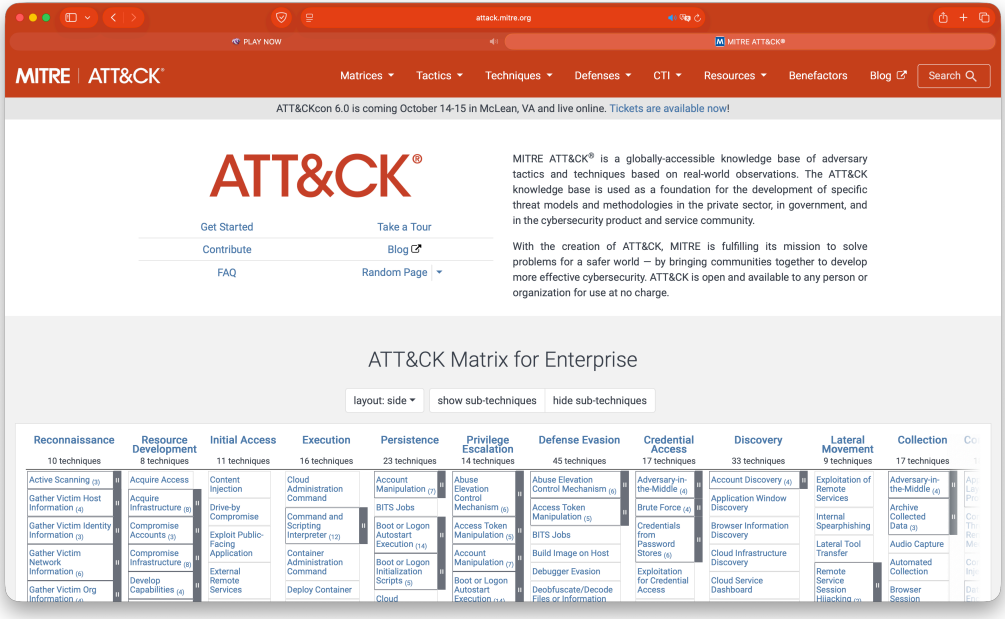
- **CVE-2021-21985, CVE-2021-22005** — krytyczne luki w oprogramowaniu VMware vCenter wykorzystywane w masowych atakach na infrastrukturę wirtualizacji.
- **CVE-2020-0601 (CurveBall/ChainOfFools)** — luka kryptograficzna w Windows CryptoAPI, pozwalająca na podszywanie się pod certyfikaty.

Każda z powyższych podatności była wykorzystywana w realnych atakach, posiada liczne opisy w prasie branżowej i uchodzi za kanoniczny przykład znaczenia szybkiego wdrażania aktualizacji bezpieczeństwa oraz monitorowania środowisk

Wprowadzenie

MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) to publicznie dostępna baza wiedzy o taktykach, technikach i procedurach (TTPs) stosowanych przez cyberprzestępców. Została opracowana przez organizację **MITRE** i jest rozwijana od 2013 roku.

- ATT&CK to **model zagrożeń oparty na obserwacjach rzeczywistych ataków**.
- Służy do klasyfikowania i opisywania sposobów działania przeciwników.
- Dostęp online: https://attack.mitre.org


attack.mitre.org
PLAY NOW
MITRE ATT&CK®
MITRE | ATT&CK
Matrices
Tactics
Techniques
Defenses
CTI
Resources
Benefactors
Blog
Search
ATT&CKcon 6.0 is coming October 14-15 in McLean, VA and live online. Tickets are available now!
ATT&CK®
Get Started
Take a Tour
Contribute
Blog
FAQ
Random Page
MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.
With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.
ATT&CK Matrix for Enterprise
layout: side
show sub-techniques
hide sub-techniques
Reconnaissance
10 techniques
Active Scanning (3)
Gather Victim Host Information (4)
Gather Victim Identity Information (3)
Gather Victim Network Information (6)
Gather Victim Org Information (4)
Resource Development
8 techniques
Acquire Access
Acquire Infrastructure (8)
Compromise Accounts (3)
Compromise Infrastructure (8)
Develop Capabilities (4)
Initial Access
11 techniques
Content Injection
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Execution
16 techniques
Cloud Administration Command
Command and Scripting Interpreter (12)
Container Administration Command
Deploy Container
Persistence
23 techniques
Account Manipulation (7)
BITS Jobs
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Cloud
Privilege Escalation
14 techniques
Abuse Elevation Control Mechanism (6)
Access Token Manipulation (5)
Account Manipulation (7)
Boot or Logon Autostart Execution (14)
Defense Evasion
45 techniques
Abuse Elevation Control Mechanism (6)
Access Token Manipulation (5)
BITS Jobs
Build Image on Host
Debugger Evasion
Deobfuscate/Decode Files or Information
Credential Access
17 techniques
Adversary-in-the-Middle (4)
Brute Force (4)
Credentials from Password Stores (6)
Exploitation for Credential Access
Discovery
33 techniques
Account Discovery (4)
Application Window Discovery
Browser Information Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (2)
Collection
17 techniques
Adversary-in-the-Middle (4)
Archive Collected Data (3)
Audio Capture
Automated Collection
Browser Session

Struktura

Model zorganizowany jest w formie **matrycy**, w której:

- **Kolumny** – reprezentują taktyki (cele atakującego, np. Initial Access, Persistence, Exfiltration).
- **Wiersze** – zawierają konkretne techniki i podtechniki (np. phishing, credential dumping, exfiltration over HTTPS).
- Każda technika posiada opis, przykłady zastosowania, znane grupy APT, a także metody wykrywania i przeciwdziałania.

Zastosowania

ATT&CK wykorzystywane jest w praktyce w wielu obszarach:

- **Threat Intelligence** – lepsze zrozumienie, jak działają konkretne grupy atakujących.
- **Red Teaming** – planowanie symulacji ataków, opartych na rzeczywistych technikach.
- **Blue Teaming** – mapowanie zabezpieczeń i detekcji w odniesieniu do matrycy ATT&CK.
- **Gap analysis** – identyfikacja luk w możliwościach detekcji i reagowania organizacji.
- **Szkolenia** – standaryzowany sposób prezentowania scenariuszy ataków.

Przykład techniki

- **Taktyka**: Initial Access (uzyskanie wstępnego dostępu).
- **Technika**: Phishing (T1566).
- **Opis**: Atakujący wysyła wiadomość e-mail z załącznikiem lub linkiem prowadzącym do złośliwego oprogramowania.
- **Środki obronne**: szkolenia użytkowników, filtrowanie poczty, sandboxing załączników.
- **Źródło**: MITRE ATT&CK – T1566

Znaczenie dla praktyki

- ATT&CK stał się **standardem branżowym** w modelowaniu zagrożeń.
- Umożliwia organizacjom porównywanie poziomu zabezpieczeń w sposób spójny i mierzalny.
- Jest dynamicznie aktualizowany i rozszerzany, co pozwala nadążać za ewolucją technik ataków.
- Wspiera wdrażanie zasad **threat-informed defense** – budowania obrony w oparciu o wiedzę o realnych przeciwnikach.

Wprowadzenie

CVSS (Common Vulnerability Scoring System) to standard oceny podatności opracowany przez organizację **FIRST**. Najnowsza wersja – **CVSS v4.0** – została opublikowana w listopadzie 2023 r.

- Celem CVSS jest umożliwienie spójnej i porównywalnej oceny podatności bezpieczeństwa.
- Wynik podawany jest w skali od 0,0 (brak zagrożenia) do 10,0 (najwyższe zagrożenie).
- Strona oficjalna: https://www.first.org/cvss

Struktura metryk

CVSS v4.0 składa się z kilku grup metryk, które razem pozwalają ocenić ryzyko podatności (FIRST – CVSS v4.0 Specification):

- **Base Metrics** – opisują właściwości podatności niezależnie od środowiska. Np. wektor ataku (sieć/lokalny), złożoność ataku, wymagane uprawnienia, wpływ na CIA.
- **Threat Metrics** – odzwierciedlają, czy podatność jest faktycznie wykorzystywana w atakach. Wprowadzają kontekst praktyczny (czy exploit jest dostępny, czy podatność jest aktywnie wykorzystywana).
- **Environmental Metrics** – uwzględniają znaczenie podatności w danym środowisku organizacji. Np. czy system obsługuje krytyczne dane, czy ma redundancję, czy jest kluczowy dla ciągłości działania.

Ocena końcowa powstaje z połączenia wszystkich metryk i może różnić się w zależności od kontekstu organizacji.

Przykład oceny

- **Podatność**: Zdalne wykonanie kodu w serwerze WWW.
- **Base Score**: 9.0 (wysoka podatność – łatwość wykorzystania, duży wpływ).
- **Environmental Metrics**: może podnieść ocenę do 9.8, jeśli system obsługuje dane krytyczne.
- **Interpretacja**: wymaga natychmiastowej reakcji (patchowanie, mitygacje).

CVSS v4.0 – przykład kalkulacji

Założenie: zdalne wykonanie kodu (RCE) w publicznej aplikacji webowej, bez uwierzytelnienia i bez interakcji użytkownika; pełny wpływ na CIA.

Wektor (Base): `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H`

Wynik bazowy: 10.0 (Critical)

Interpretacja:

- **`AV:N, AC:L, AT:N, PR:N, UI:N`** → łatwe zdalne wykorzystanie, brak wymagań wstępnych.
- **`VC:H, VI:H, VA:H`** → wysoki wpływ na poufność, integralność i dostępność.
- Działanie: natychmiastowe łatanie, mitygacje tymczasowe, blokada wektorów ataku.

Kalkulator (FIRST): https://www.first.org/cvss/calculator/4.0

CVSS v4.0 – przykład kalkulacji

Założenie: zdalne wykonanie kodu (RCE) w publicznej aplikacji webowej, bez uwierzytelnienia i bez interakcji użytkownika; pełny wpływ na CIA.

Wektor (Base): `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H`

Wynik bazowy: 10.0 (Critical)

Metryki (skrót – znaczenie):

- **AV (Attack Vector): N – Network** → atak możliwy przez sieć.
- **AC (Attack Complexity): L – Low** → niski poziom trudności, brak dodatkowych warunków.
- **AT (Attack Requirements): N – None** → brak dodatkowych wymagań środowiskowych.
- **PR (Privileges Required): N – None** → brak potrzeby posiadania konta lub uprawnień.
- **UI (User Interaction): N – None** → nie wymaga interakcji użytkownika.
- **VC (Vulnerability Confidentiality Impact): H – High** → pełne ujawnienie danych.
- **VI (Vulnerability Integrity Impact): H – High** → pełna modyfikacja danych.
- **VA (Vulnerability Availability Impact): H – High** → pełna utrata dostępności systemu.

Interpretacja:

- Wysoka krytyczność: łatwe zdalne wykorzystanie i pełny wpływ na poufność, integralność i dostępność.
- **Działanie:** natychmiastowe łatanie, wdrożenie mitygacji tymczasowych, blokada wektorów ataku.

Katalog KEV

Wprowadzenie

KEV (Known Exploited Vulnerabilities Catalog) to katalog prowadzony przez amerykańską agencję **CISA**. Obejmuje podatności, które są faktycznie wykorzystywane w atakach.

- KEV wskazuje, które luki powinny być łatane priorytetowo przez organizacje.
- Zawiera datę dodania podatności i termin, w którym federalne instytucje w USA muszą ją usunąć.
- Strona oficjalna: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Znaczenie w praktyce

- Organizacje mogą traktować KEV jako **listę priorytetów patchowania**.
- Pomaga wprowadzić zasadę „patch first” – w pierwszej kolejności łatać luki aktywnie wykorzystywane przez cyberprzestępców.
- KEV uzupełnia CVSS:
  - CVSS ocenia teoretyczną wagę podatności.
  - KEV wskazuje podatności faktycznie używane w atakach.
- Połączenie obu źródeł daje skuteczniejszą strategię zarządzania podatnościami.

Zasady bezpieczeństwa w praktyce

Secure by design

Secure by design oznacza projektowanie systemów i aplikacji w taki sposób, aby bezpieczeństwo było uwzględnione od samego początku cyklu życia oprogramowania. Nie chodzi o „doklejanie” zabezpieczeń później, lecz o ich integralne wkomponowanie w architekturę.

- Analiza zagrożeń i ryzyk już na etapie projektu.
- Stosowanie sprawdzonych wzorców i praktyk bezpieczeństwa.
- Regularne testy bezpieczeństwa (code review, fuzzing, testy penetracyjne).
- Dokumentowanie decyzji projektowych dotyczących bezpieczeństwa.

Źródło: CISA – Secure by Design

Secure by design

Przykłady praktyczne

- Wymuszenie silnego uwierzytelniania i szyfrowania komunikacji w aplikacji od samego początku.
- Minimalizacja powierzchni ataku poprzez usuwanie zbędnych funkcji.
- Domyślne ustawienia skonfigurowane w sposób bezpieczny („secure by default”).
- Automatyczne aktualizacje i poprawki bezpieczeństwa.
- Projektowanie API w taki sposób, aby zapobiegało nadużyciom (np. ograniczenia rate limiting).

Defense in depth

Defense in depth (obrona w głąb) to zasada polegająca na stosowaniu wielu warstw zabezpieczeń. Zakłada, że pojedyncze zabezpieczenie może zostać przełamane, dlatego konieczne są redundancje i kombinacja różnych mechanizmów.

- Zabezpieczenia techniczne, organizacyjne i proceduralne uzupełniają się nawzajem.
- Każda warstwa spowalnia atakującego i daje czas na detekcję i reakcję.
- Ważne: różnorodność zabezpieczeń – nie należy opierać się wyłącznie na jednej technologii.

Źródło: ENISA – Defense in Depth

Defense in depth

Przykłady praktyczne

- **Sieć:** segmentacja, firewalle, systemy IDS/IPS, monitoring ruchu.
- **Systemy:** regularne aktualizacje, kontrola dostępu, zarządzanie uprawnieniami.
- **Aplikacje:** walidacja danych wejściowych, mechanizmy sesji, logowanie zdarzeń.
- **Organizacja:** polityki bezpieczeństwa, szkolenia pracowników, procedury reagowania na incydenty.

Secure by design & defense in depth

Podsumowanie

- Secure by design = bezpieczeństwo wbudowane w projekt od podstaw.
- Defense in depth = wielowarstwowa ochrona zapewniająca odporność w przypadku przełamania pojedynczej bariery.
- Oba podejścia są **komplementarne** i stanowią fundament nowoczesnego zarządzania bezpieczeństwem systemów informatycznych.

OWASP Top 10 (WWW i API)

Wstęp – co to jest OWASP

- **OWASP** (Open Web Application Security Project) to organizacja non-profit, która publikuje darmowe zasoby, narzędzia i wytyczne dotyczące bezpieczeństwa aplikacji.
- Jednym z najbardziej znanych projektów OWASP jest **OWASP Top 10** — lista dziesięciu najpoważniejszych zagrożeń dla aplikacji WWW.
- Dla interfejsów API istnieje osobna wersja: **OWASP API Security Top 10**, skupiona na specyficznych ryzykach związanych z API.

OWASP Top 10 dla aplikacji WWW

Lista zagrożeń (edytowana w 2021) obejmuje m.in.:

```
A01: Broken Access Control
A02: Cryptographic Failures
A03: Injection
A04: Insecure Design
A05: Security Misconfiguration
A06: Vulnerable and Outdated Components
A07: Identification and Authentication Failures
A08: Software and Data Integrity Failures
A09: Security Logging and Monitoring Failures
A10: Server-Side Request Forgery (SSRF)
```

Źródło: OWASP Top 10 2021

Dla każdego zagrożenia isnieje opis: co oznacza (opis); przykłady ataków; jak temu zapobiegać (środki ochronne).

OWASP API Security Top 10

Wersja 2023 listy API obejmuje zagrożenia takie jak:

```
API1:  2023 Broken Object Level Authorization
API2:  2023 Broken Authentication
API3:  2023 Broken Object Property Level Authorization
API4:  2023 Unrestricted Resource Consumption
API5:  2023 Broken Function Level Authorization
API6:  2023 Unrestricted Access to Sensitive Business Flows
API7:  2023 Server Side Request Forgery (SSRF)
API8:  2023 Security Misconfiguration
API9:  2023 Improper Inventory Management
API10: 2023 Unsafe Consumption of APIs
```

Cechy szczególne zagrożeń API: większa ekspozycja usług, masowe przetwarzanie, mechanizmy autoryzacji i ograniczeń zasobów (rate limiting).

Źródło: OWASP API Security Project

Dlaczego OWASP Top 10 ma znaczenie?

- To **punkt startowy** dla zabezpieczania aplikacji i API — jest powszechnie znany i rozumiany w branży.
- Pomaga w komunikacji między zespołami deweloperskimi, testerskimi i bezpieczeństwa — wspólny słownik ryzyk.
- Wiele narzędzi, audytów i standardów (np. PCI-DSS) odwołuje się do OWASP Top 10 jako do minimalnego zestawu kwestii bezpieczeństwa.
- Lista jest aktualizowana regularnie, uwzględniając nowe techniki ataków i trendy.

Przykład: Broken Access Control (WWW) i BOLA (API)

- **Broken Access Control** (WWW): niedostateczne sprawdzenie uprawnień prowadzi do dostępu użytkownika tam, gdzie nie powinien mieć dostępu. Środek ochronny: weryfikacja uprawnień w warstwie serwera, testy penetracyjne.
- **BOLA (Broken Object Level Authorization)** (API): użytkownik z dostępem do zasobu A może manipulować identyfikatorami i uzyskać dostęp do zasobu B, bez kontroli autoryzacyjnej. (jest to API1:2023) Środek ochronny: weryfikacje autoryzacji na poziomie obiektu, nie tylko na endpointach.

OWASP Top 10 dla aplikacji LLM

OWASP opracowało listę 10 kluczowych zagrożeń specyficznych dla systemów korzystających z modeli językowych (LLM).

Źródło: OWASP Top 10 for LLM Applications

Id	Zagrożenie	Opis
LLM01	Prompt Injection	Manipulacja promptami w celu zmiany zachowania modelu lub ujawnienia danych.
LLM02	Insecure Output Handling	Nieodpowiednia walidacja lub filtrowanie wyjścia modelu prowadząca do zagrożeń downstream.
LLM03	Training Data Poisoning	Zanieczyszczenie danych treningowych, co prowadzi do niepożądanych lub złośliwych odpowiedzi.
LLM04	Model Denial of Service	Przeciążenie modelu specyficznymi zapytaniami, obniżenie wydajności lub dostępności.
LLM05	Supply Chain Vulnerabilities	Luki w komponentach używanych do budowy lub integracji modelu (biblioteki, dane, pluginy).
LLM06	Sensitive Information Disclosure	Model ujawnia informacje poufne zawarte w danych treningowych.
LLM07	Insecure Plugin Design	Wtyczki lub rozszerzenia modelu mogą mieć słabe zabezpieczenia — otwierają możliwość exploitów.
LLM08	Excessive Agency	Model działa zbyt autonomicznie, podejmując działania bez wystarczającej kontroli.
LLM09	Overreliance	Zaufanie modelowi bez dodatkowej walidacji może prowadzić do błędów i podatności.
LLM10	Model Theft	Nieautoryzowany dostęp lub kopiowanie modelu, wyciek własności intelektualnej modelu.

Ustawodawstwo w Polsce – cyberprzestępczość

Ustawodawstwo w Polsce – cyberprzestępczość

Art. 265. Ujawnianie lub wykorzystanie informacji niejawnych

§ 1. Kto ujawnia lub wbrew przepisom ustawy wykorzystuje informacje niejawne o klauzuli "tajne" lub "ściśle tajne", podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 2. Jeżeli informację określoną w § 1 ujawniono osobie działającej w imieniu lub na rzecz podmiotu zagranicznego, sprawca podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 3. Kto nieumyślnie ujawnia informację określoną w § 1, z którą zapoznał się w związku z pełnieniem funkcji publicznej lub otrzymanym upoważnieniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 266. Ujawnianie informacji w związku z wykonywaną funkcją

§ 1. Kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Funkcjonariusz publiczny, który ujawnia osobie nieuprawnionej informację niejawną o klauzuli "zastrzeżone" lub "poufne" lub informację, którą uzyskał w związku z wykonywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes, podlega karze pozbawienia wolności do lat 3.

§ 3. Ściganie przestępstwa określonego w § 1 następuje na wniosek pokrzywdzonego.

Ustawodawstwo w Polsce – cyberprzestępczość

Art. 267. Bezprawne uzyskanie informacji

§ 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.

§ 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

§ 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1-3 ujawnia innej osobie.

§ 5. Ściganie przestępstwa określonego w § 1-4 następuje na wniosek pokrzywdzonego.

Ustawodawstwo w Polsce – cyberprzestępczość

Art. 268. Utrudnianie zapoznania się z informacją

§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.
§ 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
§ 4. Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego.

Ustawodawstwo w Polsce – cyberprzestępczość

Art. 268a. Niszczenie danych informatycznych

§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.

§ 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 3. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

Ustawodawstwo w Polsce – cyberprzestępczość

Art. 269. Uszkodzenie danych informatycznych

§ 1. Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając informatyczny nośnik danych lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych.

Ustawodawstwo w Polsce – cyberprzestępczość

Art. 269a. Zakłócenie systemu komputerowego

Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Ustawodawstwo w Polsce – cyberprzestępczość

Art. 269b. Wytwarzanie programów komputerowych

§ 1. Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 1 lub 2, art. 269a, art. 270 § 1 albo art. 270a § 1, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, systemie teleinformatycznym lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 1a. Nie popełnia przestępstwa określonego w § 1, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej przed popełnieniem przestępstwa wymienionego w tym przepisie albo opracowania metody takiego zabezpieczenia.

§ 2. W razie skazania za przestępstwo określone w § 1, sąd orzeka przepadek określonych w nim przedmiotów, a może orzec ich przepadek, jeżeli nie stanowiły własności sprawcy.

Ustawodawstwo w Polsce – cyberprzestępczość

Art. 269c. Kontratyp działania w celu wykrycia błędów w zabezpieczeniach systemów informatycznych

Nie podlega karze za przestępstwo określone w art. 267 § 2 lub art. 269a, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej albo opracowania metody takiego zabezpieczenia i niezwłocznie powiadomił dysponenta tego systemu lub sieci o ujawnionych zagrożeniach, a jego działanie nie naruszyło interesu publicznego lub prywatnego i nie wyrządziło szkody.

Źródło: https://sip.lex.pl