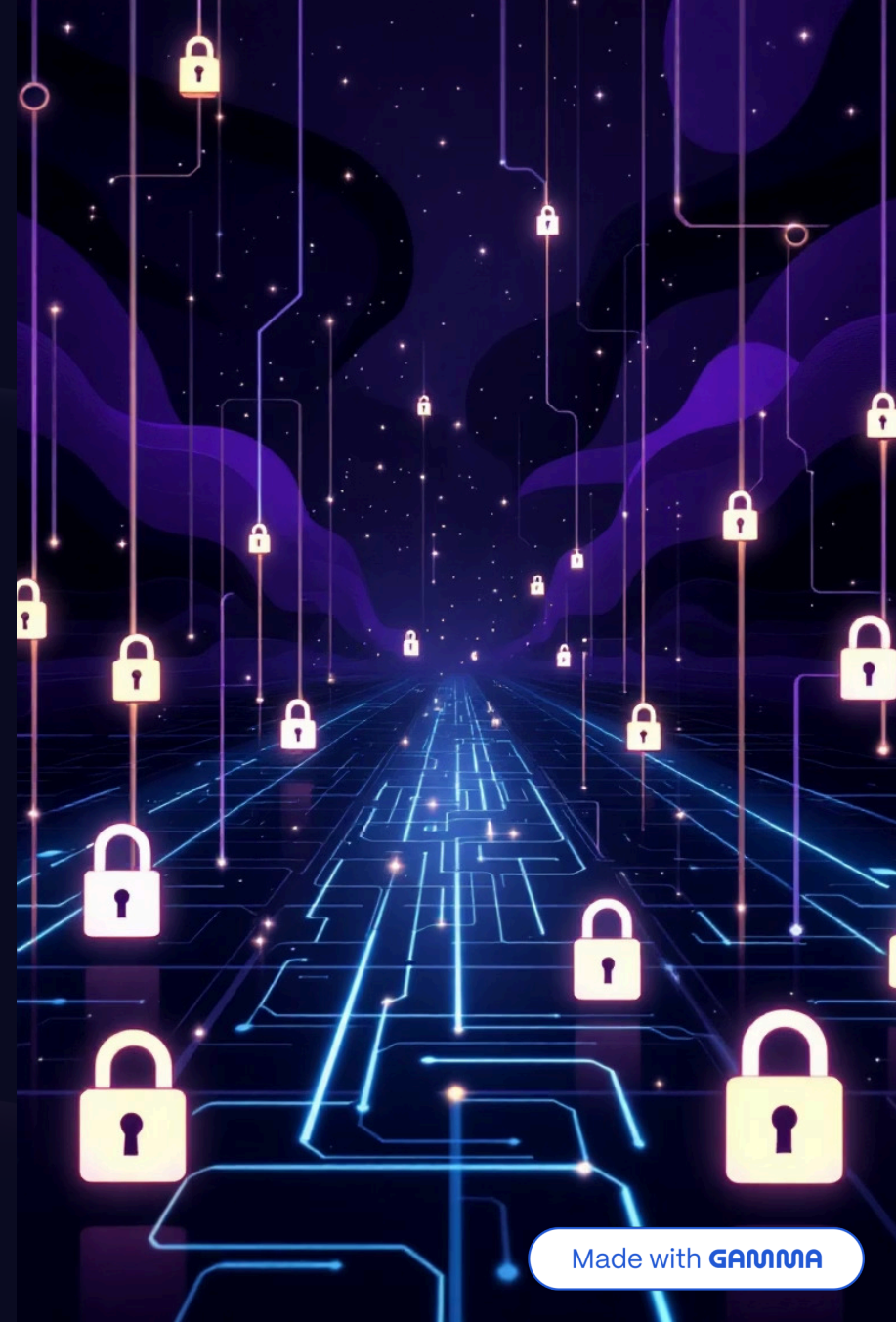


Mini słownik pojęć Cybersecurity

Przygotuj się do szkolenia! Ten słownik pomoże Ci poznać kluczowe terminy z cyberbezpieczeństwa, które będą podstawą dalszej nauki.



Podstawowe pojęcia

Cyberbezpieczeństwo

Ochrona systemów komputerowych, sieci i danych przed nieautoryzowanym dostępem, atakami i zniszczeniem.

Atak

Próba uzyskania nieautoryzowanego dostępu do systemu, aplikacji lub danych. Może być automatyczna (malware) lub manualna (pentest).

Zagrożenie

Każde potencjalne źródło szkody dla systemu – wirus, luka bezpieczeństwa czy błędna konfiguracja.

Luka (Vulnerability)

Słabość w systemie, aplikacji lub konfiguracji, którą można wykorzystać do przeprowadzenia ataku.

Ryzyko (Risk)

Prawdopodobieństwo wykorzystania luki pomnożone przez jej potencjalne skutki dla organizacji.





Typy ataków

1

Exploit

Fragment kodu lub narzędzie wykorzystujące lukę w systemie do przeprowadzenia ataku.

2

Payload

Część exploita wykonująca właściwe działanie po włamaniu – np. instalację malware'u lub uzyskanie dostępu.

3

Brute Force

Metoda łamania haseł przez automatyczne sprawdzanie wszystkich możliwych kombinacji znaków.



Phishing

Podszywanie się pod zaufaną instytucję (bank, firmę), aby wyłudzić dane logowania lub informacje osobowe.



Ransomware

Złośliwe oprogramowanie szyfrujące dane ofiary i żądające okupu za ich odszyfrowanie.



Malware

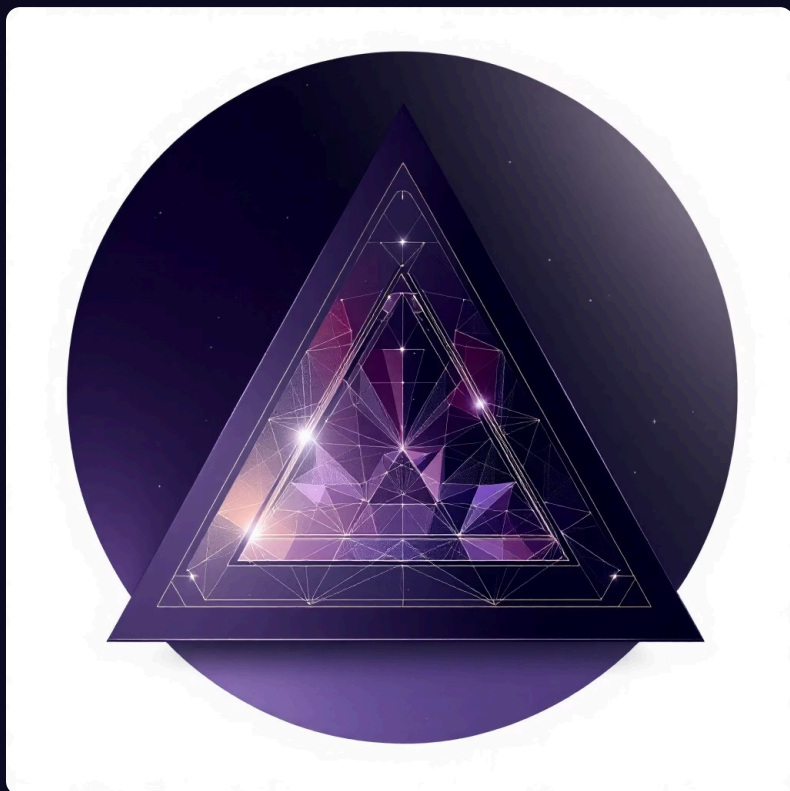
Ogólny termin oznaczający złośliwe oprogramowanie: wirusy, trojany, spyware, ransomware.



Social Engineering

Manipulowanie ludźmi, by nakłonić ich do ujawnienia informacji lub wykonania niebezpiecznych działań.

Podstawowe zasady bezpieczeństwa



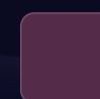
CIA Triad

Trzy filary bezpieczeństwa informacji:



Confidentiality (Poufność)

Tylko uprawnione osoby
mogą uzyskać dostęp do
danych.



Integrity (Integralność)

Dane nie mogą być
zmieniane bez autoryzacji.



Availability (Dostępność)

Systemy i dane muszą być dostępne, gdy są potrzebne.



Authentication

Potwierdzenie tożsamości
użytkownika (login i hasło,
biometria).



Authorization

Przyznanie użytkownikowi
określonych uprawnień – dostępu
do plików czy panelu admina.



Least Privilege

Użytkownik lub proces powinien
mieć tylko niezbędne uprawnienia.

⚙️ Narzędzia i pojęcia techniczne

1 Recon (Reconnaissance)

Zbieranie informacji o celu: domeny, adresy IP, wersje oprogramowania przed właściwym atakiem.

2 Enumeration

Aktywne wyszukiwanie dostępnych zasobów – użytkowników, serwerów, otwartych portów.

3 Pentest

Kontrolowany atak na system w celu wykrycia luk bezpieczeństwa zanim zrobią to przestępcy.

4 Privilege Escalation

Uzyskanie wyższych uprawnień niż przyznane – np. z użytkownika do administratora.

Patch

Poprawka bezpieczeństwa usuwająca znane luki w oprogramowaniu.

Firewall

Filtr decydujący, jaki ruch sieciowy jest dozwolony lub blokowany.

VPN


Szyfrowane połączenie chroniące dane w sieci publicznej.



Aplikacje webowe i sieć

OWASP

Open Web
Application Security
Project – organizacja
tworząca standardy
bezpieczeństwa
aplikacji webowych.

 **OWASP
Top 10** –
lista 10
najczęstszy
ch
podatności
w
aplikacjach
webowych,
regularnie
aktualizow
ana.

→ SQL Injection (SQLi)

Atak wstrzykujący własne zapytania SQL do formularza lub adresu URL aplikacji.

→ Cross-Site Scripting (XSS)

Wstrzyknięcie i uruchomienie złośliwego kodu JavaScript w przeglądarce użytkownika.

→ CSRF

Cross-Site Request Forgery – podstępne nakłonienie użytkownika do wykonania niechcianych działań.

→ API Security

Interfejs komunikacji między aplikacjami – potencjalny wektor ataku bez odpowiedniego zabezpieczenia.



Sieci, systemy i dodatkowe pojęcia

IP Address

Unikalny identyfikator urządzenia w sieci.

Port

Logiczny punkt komunikacji (80–HTTP, 22–SSH, 443–HTTPS).

TCP/IP

Zestaw protokołów stanowiących fundament komunikacji internetowej.

DNS

System tłumaczący nazwy domen na adresy IP.

SSH

Bezpieczny protokół do zdalnego logowania i administracji systemami.

Warto zapamiętać

Hash

Skrót kryptograficzny danych (SHA-256, MD5) – nie można go odwrócić, ale można sprawdzić zgodność.

Salt

Losowa wartość dodawana do hasła przed hashowaniem, by utrudnić łamanie.

Incident

Zdarzenie naruszające lub zagrażające bezpieczeństwu danych w organizacji.

Threat Intelligence

Analiza aktualnych zagrożeń i ataków w celu lepszego reagowania.