

Temat 5 .

Cyberbezpieczeństwo i zagrożenia w cyberprzestrzeni

dr inż. Michał Malinowski

<https://www.drmalinowski.edu.pl>

BEZPIECZEŃSTWO
INFORMACJI



- Cyberbezpieczeństwo
- Cyberataki
- Cyberprzemoc
- Cyberobrona

Zadanie

Treść

Prezentacja zadania podczas zajęć.

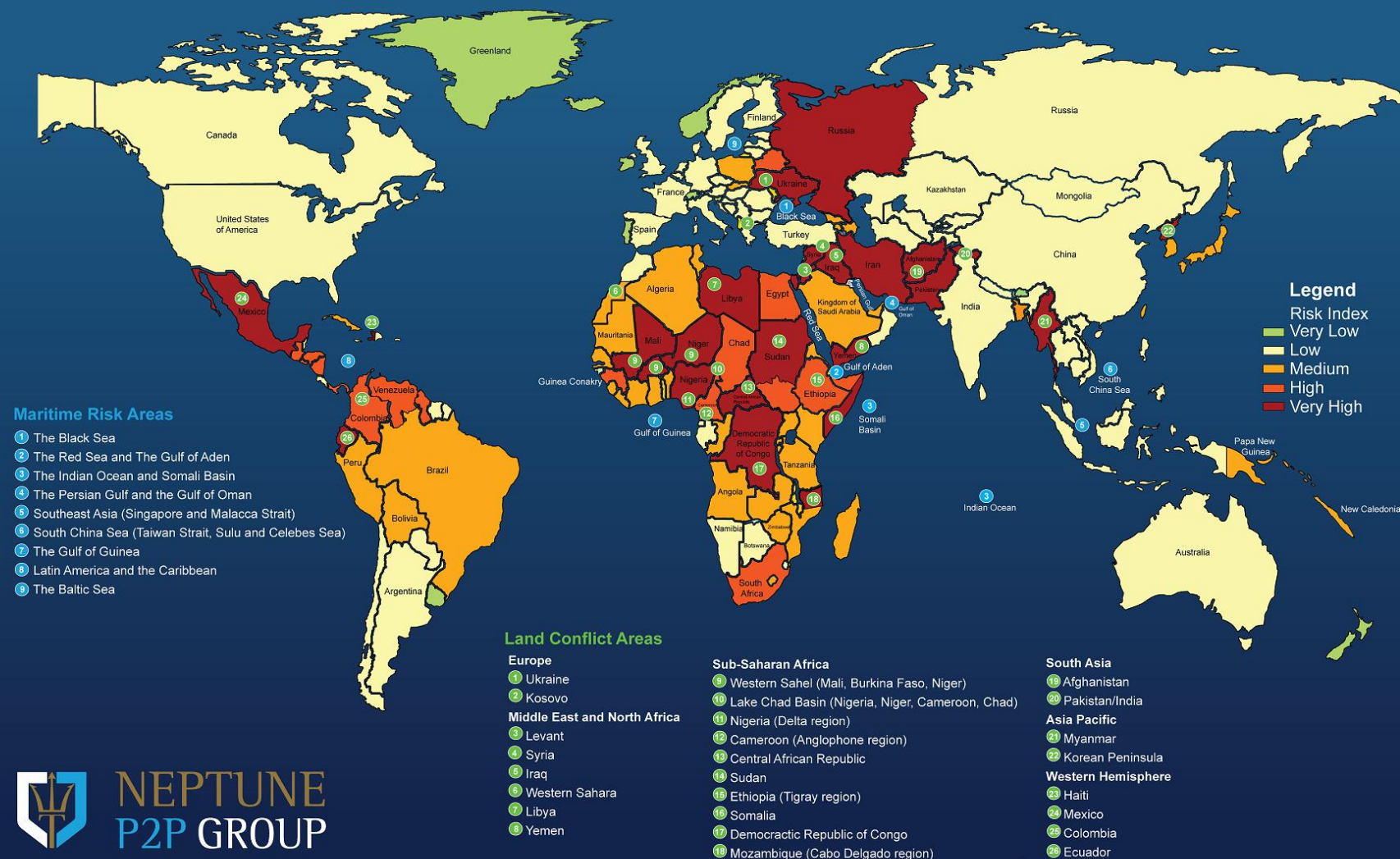
Okolo 9 osób podczas zajęć

(0-2 pkt)

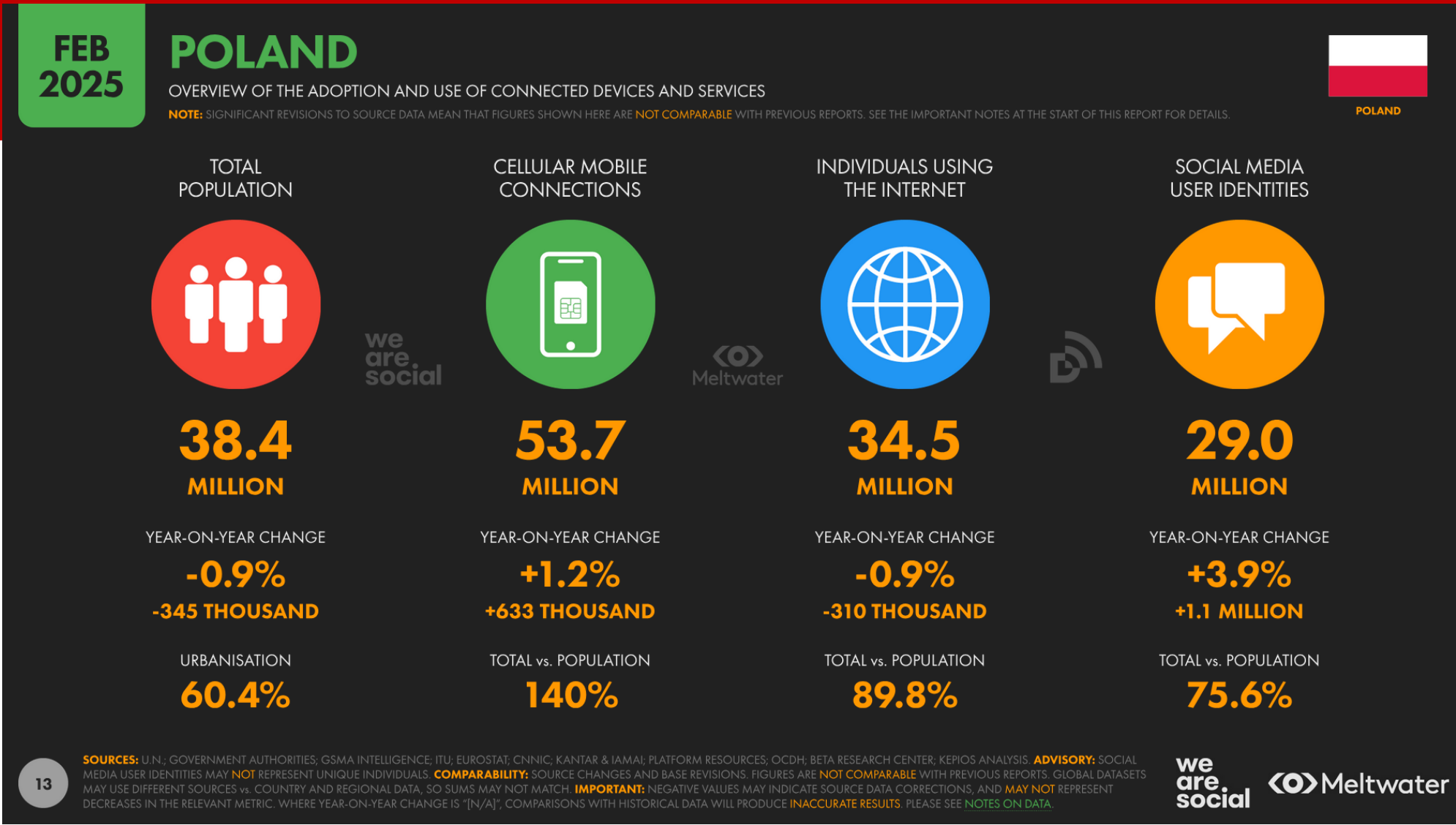


Global Risk and Security Assessment

Visualising Maritime and Terrestrial Risk Q1 2025



Cyberbezpieczeństwo



Cyberbezpieczeństwo

Cyberbezpieczeństwo

odnosi się do praktyk, technologii i procesów mających na celu ochronę systemów komputerowych, sieci, urządzeń oraz danych przed nieautoryzowanym dostępem, atakami, uszkodzeniami lub kradzieżą.

Jest to kluczowy element zarządzania ryzykiem w środowisku cyfrowym, który zapewnia integralność, poufność i dostępność informacji.

Zarządzanie ryzykiem:

- Identyfikacja, ocena i priorytetyzacja ryzyka związanego z bezpieczeństwem informacji.

Kontrola dostępu:

- Ograniczenie dostępu do systemów i danych tylko do autoryzowanych użytkowników.

Ochrona danych:

- Szyfrowanie danych w spoczynku i podczas transmisji, aby zapobiec ich nieautoryzowanemu odczytowi.

Zapobieganie atakom:

- Implementacja zapór sieciowych (firewall), systemów wykrywania i zapobiegania włamaniom (IDS/IPS) oraz oprogramowania antywirusowego.

Odpowiedź na incydenty:

- Opracowanie planów reakcji na incydenty, które określają kroki do podjęcia w przypadku naruszenia bezpieczeństwa.

Szkolenie i świadomość użytkowników:

- Edukacja pracowników i użytkowników na temat zagrożeń cyberbezpieczeństwa oraz najlepszych praktyk w zakresie bezpiecznego korzystania z technologii.

Zgodność:

- Audyty i oceny zgodności z wymogami regulacyjnymi oraz standardami branżowymi, takimi jak ISO 27001.

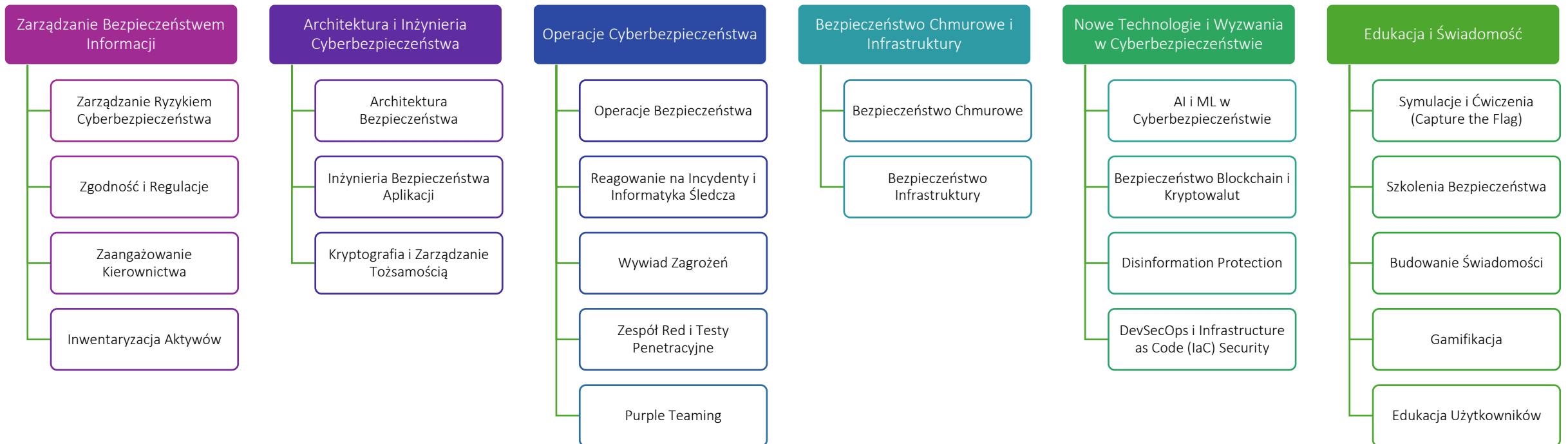
Cyberbezpieczeństwo

Warstwy cyberbezpieczeństwa

Warstwa	Opis
1. Warstwa ludzka (Human Layer)	Edukacja użytkowników w zakresie identyfikowania zagrożeń oraz bezpiecznych praktyk cyfrowych.
2. Warstwa bezpieczeństwa granicznego (Perimeter Security Layer)	Ochrona organizacji przed zewnętrznymi atakami poprzez monitorowanie i kontrolowanie ruchu na granicy sieci.
3. Warstwa bezpieczeństwa sieci (Network Security Layer)	Zmniejszenie powierzchni ataku i szybka detekcja podejrzanego ruchu wewnątrz sieci.
4. Warstwa bezpieczeństwa aplikacji (Application Security Layer)	Zapobieganie wstrzyknięciom, XSS, CSRF i innym atakom na aplikacje.
5. Warstwa bezpieczeństwa punktów końcowych (Endpoint Security Layer)	Monitorowanie i szybka reakcja na zagrożenia pojawiające się na stacjach roboczych i urządzeniach mobilnych.
6. Warstwa bezpieczeństwa danych (Data Security Layer)	Ochrona danych wrażliwych przed nieautoryzowanym dostępem i wyciekiem.
7. Warstwa zasobów krytycznych (Mission-Critical Assets Layer)	Zapewnienie dostępności kluczowych systemów nawet w przypadku poważnych incydentów lub awarii.

Cyberbezpieczeństwo

Domeny cyberbezpieczeństwa



Cyberbezpieczeństwo

Incydent Bezpieczeństwa

to każde zdarzenie, które skutkuje naruszeniem poufności, integralności lub dostępności danych, systemów komputerowych, sieci lub usług

Identyfikacja:

- Szybkie wykrycie incydentu i jego zakresu.

Kontrola:

- Natychmiastowe działania mające na celu powstrzymanie dalszego rozprzestrzeniania się incydentu.

Analiza:

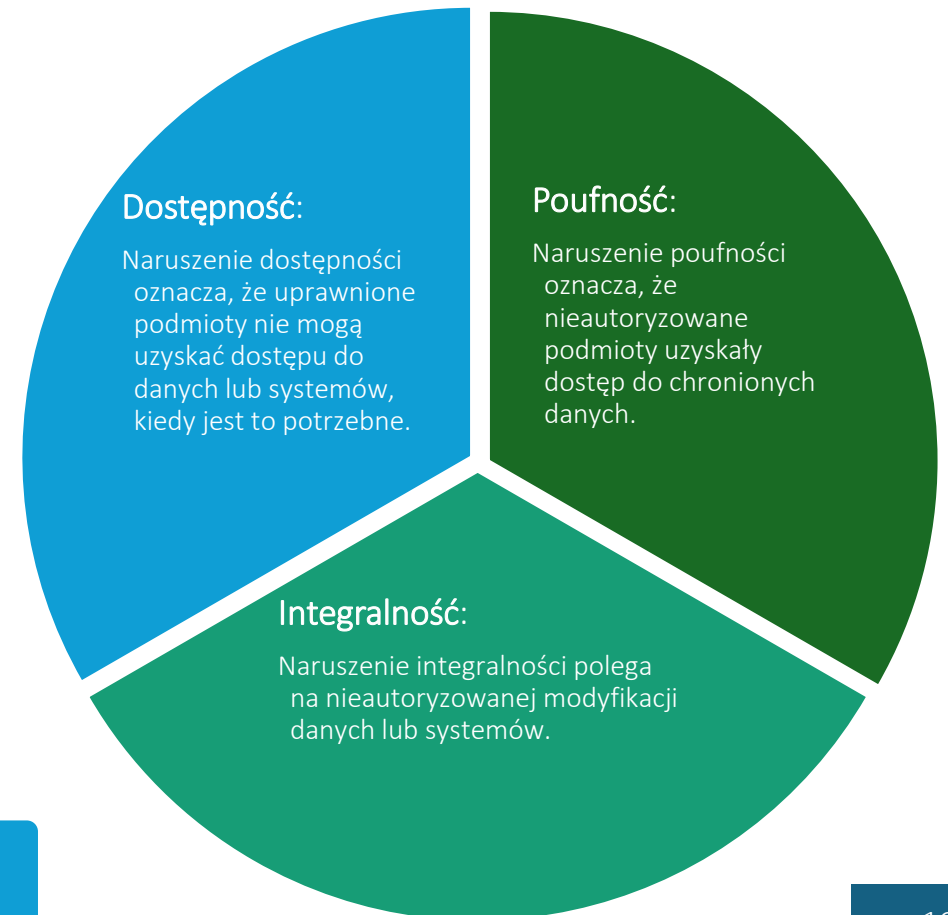
- Ocena przyczyn incydentu i jego skutków.

Naprawa:

- Usunięcie skutków incydentu i przywrócenie normalnego działania systemów.

Komunikacja:

- Informowanie odpowiednich stron, w tym użytkowników i organów regulacyjnych.



Popularne cyberataki

Phishing (Wyłudzenie informacji)

to podszywanie się pod zaufane podmioty w celu wyłudzenia poufnych informacji, takich jak hasła i numery kart kredytowych.

W 2020 roku hakerzy wysłali fałszywe e-maile, podszywając się pod WHO (Światową Organizację Zdrowia) w związku z pandemią COVID-19, aby wyłudzić dane logowania.



Popularne cyberataki

Ransomware (Oprogramowanie wymuszające okup)

to ataki polegające na zablokowaniu dostępu do systemów lub danych i żądaniu okupu za ich odblokowanie.

Atak ransomware WannaCry w 2017 roku, który zainfekował ponad 200,000 komputerów na całym świecie, w tym systemy brytyjskiej służby zdrowia (NHS).



Popularne cyberataki

Malware (Złośliwe oprogramowanie)

to złośliwe oprogramowanie zaprojektowane do uszkodzenia, zakłócenia lub uzyskania nieautoryzowanego dostępu do urządzenia.

Oprogramowanie szpiegujące (spyware) Pegasus, które było używane do szpiegowania dziennikarzy, aktywistów i polityków na całym świecie.



Popularne cyberataki

Social Engineering (Socjotechnika)

to techniki manipulacyjne, które mają na celu skłonienie użytkowników do ujawnienia poufnych informacji lub wykonania określonych działań.

Atak na firmę Twitter w 2020 roku, gdzie socjotechniczne metody pozwoliły hakerom przejąć konta znanych osób i firm, aby realizować oszustwo kryptowalutowe.



Popularne cyberataki

Business Email Compromise (BEC) (Kompromitacja e-maila firmowego)

po uzyskaniu dostępu do konta e-mail firmowego, cyberprzestępcy mogą wysyłać fałszywe e-maile, kraść poufne informacje lub używać konta do przeprowadzania ataków.

Atak BEC na firmę Ubiquiti Networks w 2015 roku, w wyniku którego firma straciła 46,7 miliona dolarów.



Popularne cyberataki

DDoS (Distributed Denial-of-Service) (Rozproszona odmowa usługi)

to ataki, które uniemożliwiają użytkownikom sieci lub systemu dostęp do informacji lub usług poprzez przeciążenie sieci dużą ilością ruchu.

Atak DDoS na Dyn w 2016 roku, który spowodował przerwy w działaniu wielu popularnych serwisów internetowych, w tym Twittera, Spotify i Reddita.

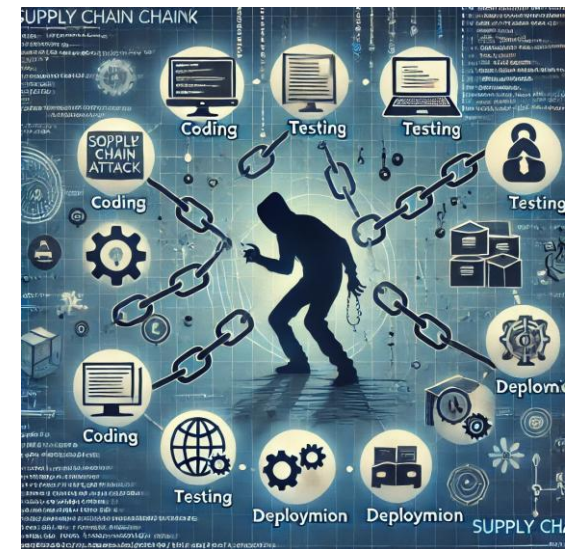


Popularne cyberataki

Supply Chain Attacks (Ataki na łańcuch dostaw)

Hakerzy infiltrują technologie łańcucha dostaw, aby uzyskać dostęp do kodu źródłowego, budować kody i inne komponenty infrastruktury aplikacji.

Atak na firmę SolarWinds w 2020 roku, gdzie złośliwe oprogramowanie zostało wprowadzone do aktualizacji oprogramowania, które było dystrybuowane do klientów na całym świecie.



Popularne cyberataki

Insider Threats (Zagrożenia wewnętrzne)

to zagrożenia wewnętrzne, które po uzyskaniu dostępu do systemu mogą stanowić większe zagrożenie niż ataki zewnętrzne.

Edward Snowden, były pracownik NSA, który ujawnił tajne informacje dotyczące programów inwigilacji prowadzonych przez USA.



Popularne cyberataki

Cyberzagrożenie	Opis	Przykład
Vulnerabilities (Luki w zabezpieczeniach)	Nowo odkryte luki w zabezpieczeniach, takie jak te w Microsoft Exchange, oraz postępy w phishingu tworzą nowe obszary do monitorowania.	Luka w zabezpieczeniach Log4Shell odkryta w 2021 roku, która dotyczyła biblioteki Log4j, powszechnie używanej w aplikacjach internetowych.
Crime-as-a-Service (CaaS) (Przestępczość jako usługa)	Usługi oferowane na podziemnych rynkach, które dostarczają narzędzi, usług i wiedzy specjalistycznej do przeprowadzania cyberprzestępstw.	Serwis Genesis Market, który sprzedaje skradzione dane logowania i cyfrowe odciski palców, umożliwiając dostęp do kont online.
IoT Device Hacking (Hakowanie urządzeń IoT)	Ataki na urządzenia Internetu Rzeczy (IoT), z których wiele pracowników uzyskuje dostęp do wrażliwych danych firmy z różnych punktów końcowych.	Atak Mirai botnet w 2016 roku, który przejął kontrolę nad tysiącami urządzeń IoT, aby przeprowadzić ataki DDoS.
Drive-by Compromises (Złośliwe ataki podczas przeglądania)	Ataki, w których ofiary są zwabiane na złośliwe strony internetowe za pomocą technik takich jak pozycjonowanie SEO i malwertising.	Ataki Watering Hole, gdzie złośliwe oprogramowanie jest wstrzykiwane na popularne strony odwiedzane przez konkretną grupę użytkowników.
Cloud-based Attacks (Ataki na infrastrukturę chmurową)	Ataki na infrastrukturę chmurową, która staje się coraz bardziej złożona, co czyni ją łatwym celem dla cyberprzestępców.	Atak na Capital One w 2019 roku, gdzie dane osobowe ponad 100 milionów klientów zostały skradzione z chmurowego systemu przechowywania danych.
Zero-Day Exploits (Wykorzystanie luk dnia zerowego)	Ataki wykorzystujące nieznane wcześniej luki w oprogramowaniu, które nie zostały jeszcze załatane przez producenta.	Atak Stuxnet, który wykorzystał luki dnia zerowego w systemach SCADA do zakłócenia programu nuklearnego Iranu.
Credential Stuffing (Nadmuchiwanie poświadczeń)	Ataki polegające na używaniu dużych list skradzionych poświadczeń (loginów i haseł) do uzyskania nieautoryzowanego dostępu do kont użytkowników.	Atak na sieć gier online, gdzie hakerzy używali skradzionych poświadczeń, aby uzyskać dostęp do kont graczy.
Cross-Site Scripting (XSS) (Ataki między stronami)	Ataki polegające na wstrzyknięciu złośliwego kodu do stron internetowych odwiedzanych przez użytkowników, co pozwala atakującym na kradzież informacji lub przejęcie sesji.	Atak XSS na popularną platformę mediów społecznościowych, gdzie złośliwy kod był wstrzykiwany w komentarze użytkowników.
Password Attacks (Ataki na hasła)	Ataki polegające na próbach złamania haseł za pomocą technik takich jak brute force, słownikowe ataki i analizowanie hashów haseł.	Atak brute force na popularną platformę e-commerce, gdzie hakerzy próbowali różnych kombinacji haseł, aby uzyskać dostęp do kont użytkowników.
SQL Injection (Wstrzykiwanie SQL)	Ataki polegające na wstrzykiwaniu złośliwych zapytań SQL do formularzy w celu uzyskania nieautoryzowanego dostępu do bazy danych.	Atak na firmę TalkTalk w 2015 roku, gdzie hakerzy wykorzystali lukę SQL Injection, aby uzyskać dostęp do danych osobowych klientów.

Ataki w Mediach Społecznościowych



Zagrożenia

Doxing (ujawnianie prywatnych informacji):

- Ujawnianie prywatnych informacji osoby bez jej zgody.

Sextortion (szantażowanie treściami seksualnymi):

- Szantażowanie osoby ujawnieniem jej prywatnych zdjęć lub filmów o charakterze seksualnym.

Cyberbullying (cyberprzemoc):

- Systematyczne nękanie, zastraszanie i obrażanie innych osób w internecie.

Trolling:

- Działania mające na celu wywołanie negatywnych reakcji lub zakłócanie dyskusji.

Ataki w Mediach Społecznościowych

Hejt vs Hape

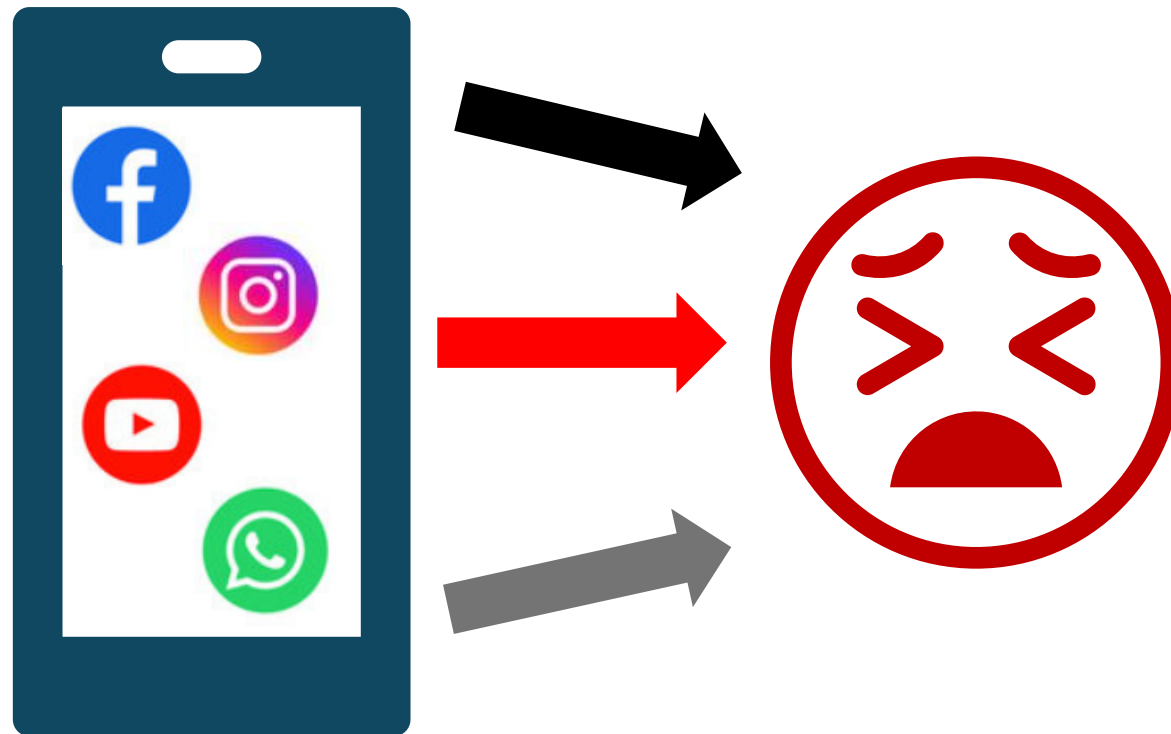
Aspekt	Hejt (Hate)	Hape (Hope)
Cel	Zaszkodzenie, obrażanie, wywołanie negatywnych emocji	Wspieranie, motywowanie, wywołanie pozytywnych emocji
Formy	Obrażliwe komentarze, nienawistne posty, groźby	Komplementy, słowa wsparcia, pozytywne historie
Skutki	Stres, problemy emocjonalne, spadek samooceny	Poprawa nastroju, wzrost samooceny, budowanie społeczności
Przykłady	Groźby w mediach społecznościowych, cyberbullying	Kampanie zdrowia psychicznego, inspirujące posty

Narcystyczne zaburzenie osobowości (NPD)



Zaburzenie Dysmorficzne Ciała (BDD)

FOMO – Strach przed przegapieniem



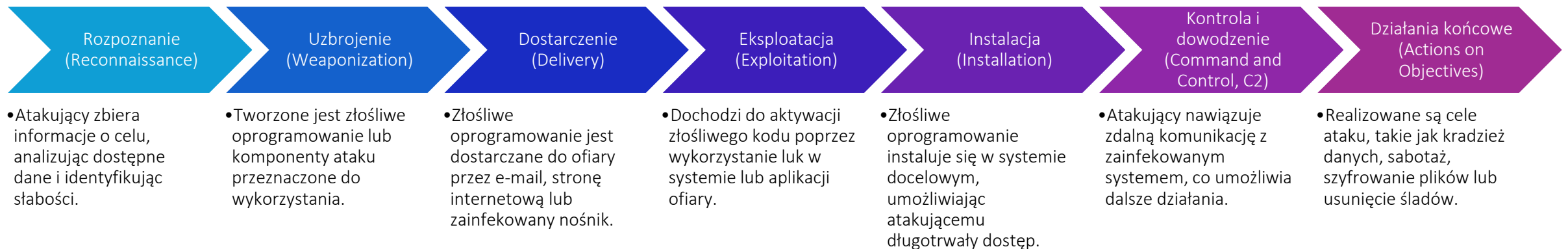
FOMO 2.0 – Lęk przed niedokumentowaniem

The Cyber Kill Chain - etapy ataku cybernetycznego

The Cyber Kill Chain

to model opracowany przez firmę Lockheed Martin, który opisuje etapy ataku cybernetycznego od momentu planowania aż po realizację i ewentualne uszkodzenie docelowych zasobów.

Jego celem jest lepsze zrozumienie procesu ataków, co pozwala organizacjom na proaktywne podejście do cyberbezpieczeństwa i skuteczniejszą obronę.



Cyberprzemoc

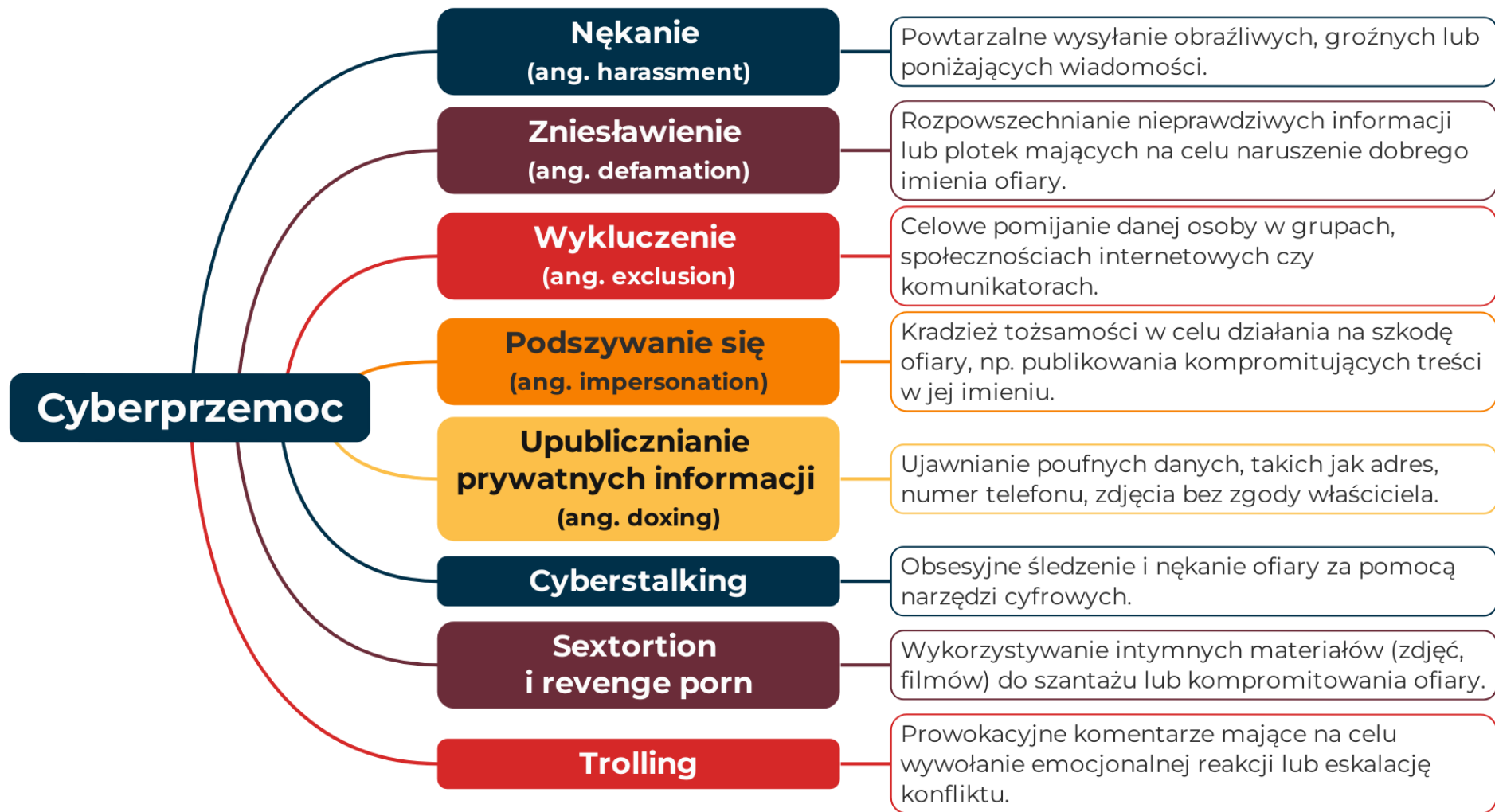
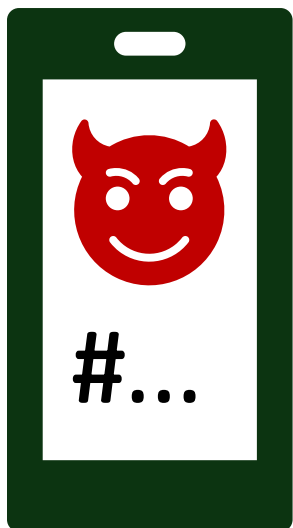
Cyberprzemoc (ang. cyberbullying) to forma przemocy, która ma miejsce w cyberprzestrzeni, głównie za pośrednictwem Internetu i urządzeń mobilnych.

Polega na celowym i powtarzalnym działaniu mającym na celu zaszkodzenie drugiej osobie, często w sposób trudny do wykrycia i udowodnienia.

Cyberprzemoc jest szczególnie niebezpieczna, ponieważ może mieć trwały wpływ na zdrowie psychiczne ofiary (uraz) i jest trudna do kontrolowania z uwagi na anonimowość sprawców oraz szybkość rozprzestrzeniania się informacji w sieci.



Cyberprzemoc



Cyberprzemoc

Cechy

Anonimowość sprawcy

- Sprawcy często ukrywają swoją tożsamość, co utrudnia ich identyfikację.

Szeroki zasięg

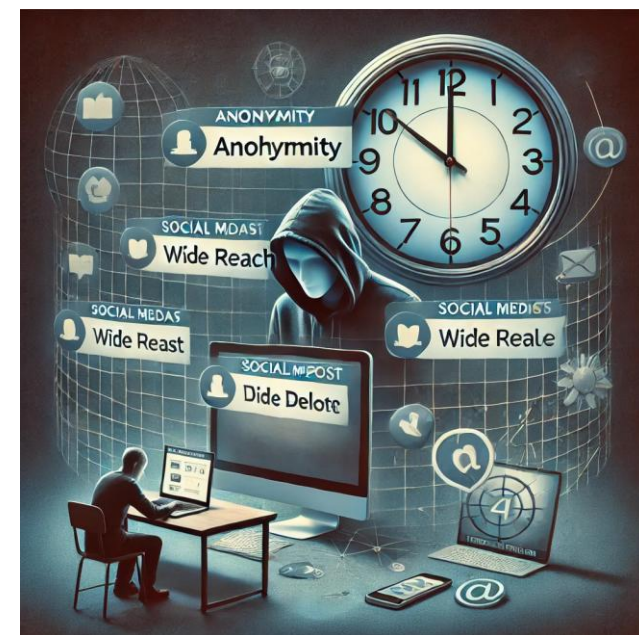
- Treści publikowane w Internecie mogą dotrzeć do szerokiego grona odbiorców w krótkim czasie.

Brak granic czasowych

- Cyberprzemoc może odbywać się przez całą dobę.

Trudność usunięcia treści

- Usunięcie kompromitujących materiałów z internetu bywa praktycznie niemożliwe.



Cyberprzemoc

Skutki



Psychiczne

- lęk, depresja, obniżone poczucie własnej wartości, a w skrajnych przypadkach myśli samobójcze.

Społeczne

- wycofanie z życia społecznego, trudności w budowaniu relacji międzyludzkich.

Zawodowe i edukacyjne

- obniżenie wyników w nauce lub pracy, absencje.

Prawne

- sprawcy mogą zostać pociągnięci do odpowiedzialności prawnej, np. za zniesławienie czy groźby karalne.

Finansowe

- koszty związane z utratą prywatnych danych (np. oszustwa finansowe, kradzież tożsamości), utrata dochodów z powodu uszczerbku na reputacji zawodowej lub społecznej.

Cyberprzemoc

Jak przeciwdziałać

Edukacja i świadomość

- Uświadamianie dzieci i młodzieży na temat zagrożeń w internecie.
- Nauka krytycznego podejścia do treści w sieci i rozpoznawania sytuacji cyberprzemocy.

Tworzenie bezpiecznej przestrzeni online

- Platformy internetowe powinny oferować narzędzia do raportowania nadużyć.
- Administratorzy powinni aktywnie monitorować i reagować na nieodpowiednie zachowania.



Cyberprzemoc

Jak przeciwdziałać



Ochrona prywatności

- Unikanie udostępniania zbyt wielu danych osobowych w sieci.

Wsparcie psychologiczne

- Zapewnienie psychologicznej pomocy ofiarom cyberprzemocy.
- Zachęcanie do rozmowy o problemie z zaufaną osobą.

Cyberprzemoc

Jak przeciwdziałać

Zgłaszanie przypadków cyberprzemocy

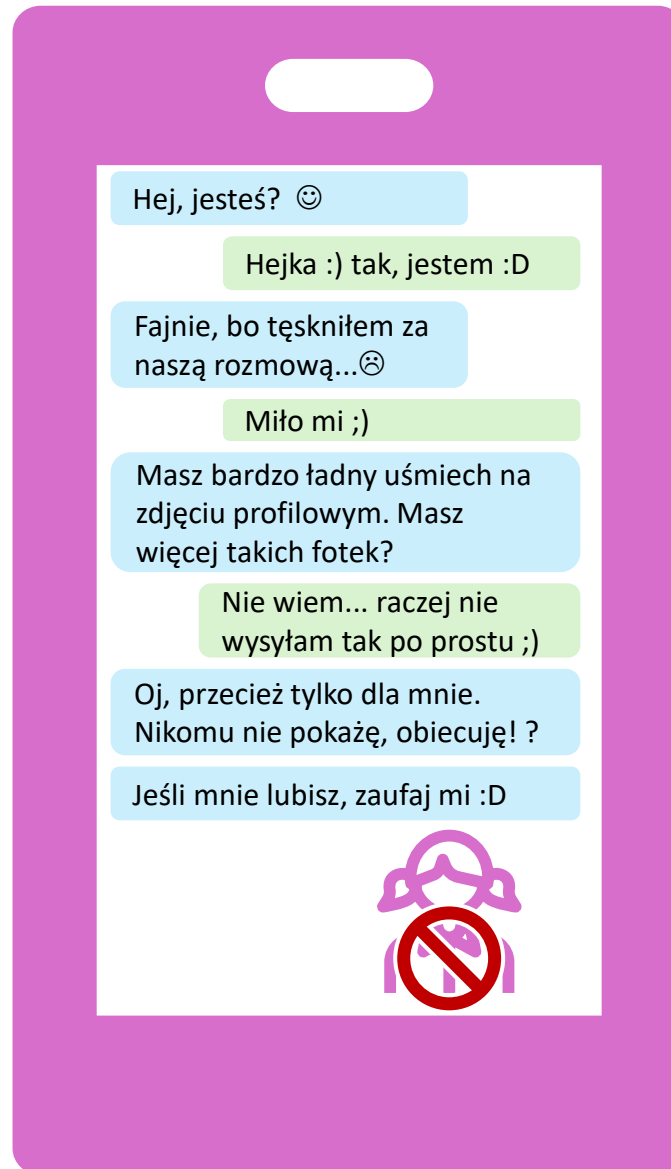
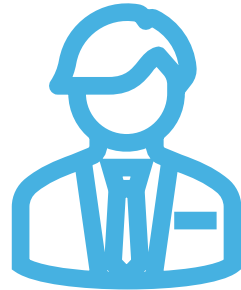
- Informowanie odpowiednich organów, np. policji, gdy dochodzi do łamania prawa.
- Zbieranie dowodów (zrzuty ekranu, zapis wiadomości) w celu ułatwienia działań prawnych.

Prawne regulacje

- Cyberprzemoc jest ścigana na podstawie przepisów kodeksu karnego, np. za stalking, groźby czy naruszenie dóbr osobistych.



Grooming – wyłudzenie intymności online



Cyberobrona

Komponenty bezpieczeństwa urządzeń

Zapora sieciowa (Firewall)

- Oprogramowanie lub sprzęt, który monitoruje i kontroluje ruch sieciowy w celu zapobiegania nieautoryzowanemu dostępowi.

Antywirus i Antymalware

- Oprogramowanie zaprojektowane do wykrywania, zapobiegania i usuwania wirusów oraz złośliwego oprogramowania.

Szyfrowanie danych (Data Encryption)

- Technika kodowania danych w taki sposób, że tylko autoryzowane strony mogą je odczytać.

Autoryzacja i uwierzytelnianie (Authentication and Authorization)

- Procesy zapewniające, że tylko uprawnieni użytkownicy mają dostęp do zasobów.

System wykrywania włamań (Intrusion Detection System, IDS)

- System monitorujący sieć lub systemy komputerowe w celu wykrywania nieautoryzowanych działań.

VPN (Virtual Private Network)

- Sieć prywatna rozszerzona na publiczną sieć, która umożliwia bezpieczne przesyłanie danych.

Bezpieczne aktualizacje oprogramowania (Secure Firmware Updates)

- Mechanizmy zapewniające, że aktualizacje oprogramowania są autentyczne i bezpieczne przed atakami.

Segmentacja sieci (Network Segmentation)

- Podział sieci na mniejsze, odseparowane segmenty w celu ograniczenia ryzyka rozprzestrzeniania się ataków.

Systemy zarządzania dostępem (Access Management Systems)

- Narzędzia do zarządzania i kontrolowania dostępu użytkowników do zasobów sieciowych.

Bezpieczne bootowanie (Secure Boot)

- Proces uruchamiania urządzenia, który zapewnia, że tylko zaufane oprogramowanie może zostać załadowane.

Monitorowanie i analiza (Monitoring and Analytics)

- Systemy śledzenia aktywności sieciowej i analizowania logów w celu wczesnego wykrywania anomalii i zagrożeń.

Bezpieczne protokoły komunikacyjne (Secure Communication Protocols)

- Protokół zapewniający bezpieczną wymianę danych między urządzeniami, np. HTTPS, TLS.

Cyberobrona

Zapora sieciowa (Firewall)

to oprogramowanie lub sprzęt, który monitoruje i kontroluje ruch sieciowy w celu zapobiegania nieautoryzowanemu dostępowi.

Monitorowanie ruchu sieciowego:

- Analizuje dane przychodzące i wychodzące w sieci, identyfikując potencjalne zagrożenia.

Kontrola dostępu:

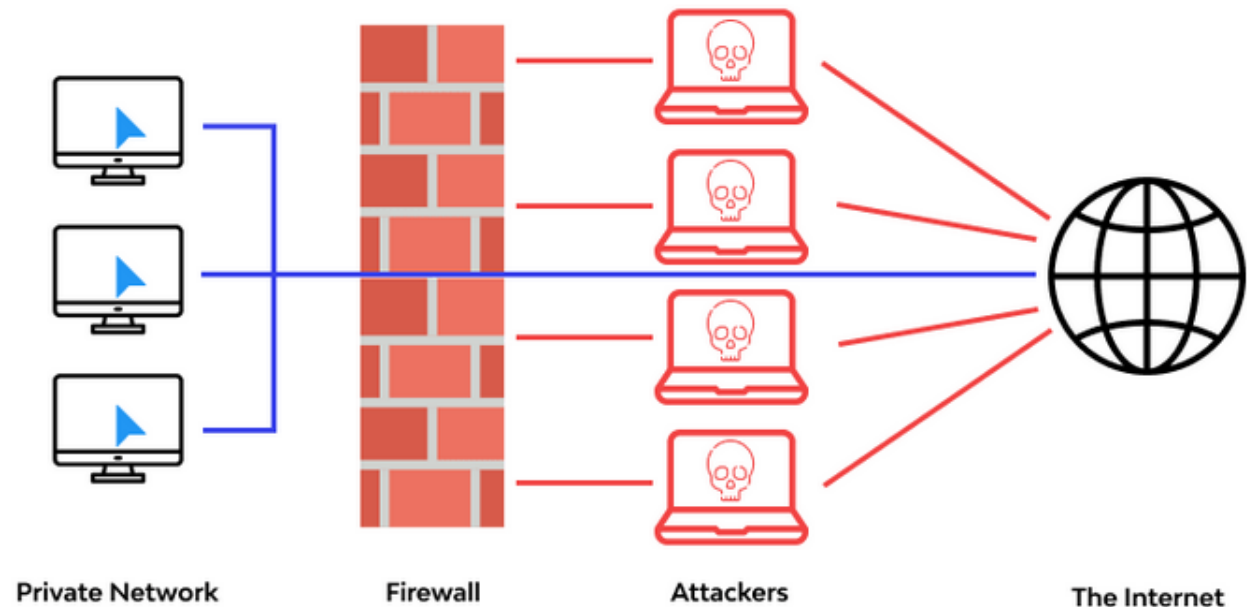
- Określa, które dane mogą przechodzić przez sieć, na podstawie ustalonych reguł bezpieczeństwa.

Ochrona przed atakami:

- Zapobiega różnym rodzajom cyberataków, takim jak ataki typu DDoS, próby włamań czy infekcje złośliwym oprogramowaniem.

Rejestrowanie i raportowanie:

- Śledzi zdarzenia związane z bezpieczeństwem i generuje raporty, które mogą być użyte do analizy i audytów.



Cyberobrona

VPN (Virtual Private Network)

to technologia, która umożliwia użytkownikom bezpieczne i prywatne połączenie z siecią internetową poprzez tworzenie zaszyfrowanego tunelu między urządzeniem użytkownika a serwerem VPN.

Dzięki temu połączenie jest chronione przed nieautoryzowanym dostępem, a tożsamość użytkownika i jego aktywność online pozostają prywatne.

Jak działa VPN?

Połączenie z serwerem VPN:

- Użytkownik nawiązuje połączenie z serwerem VPN za pomocą klienta VPN.



Szyfrowanie danych:

- Dane przesyłane między urządzeniem użytkownika a serwerem VPN są szyfrowane, co zapewnia ich bezpieczeństwo.



Maskowanie adresu IP:

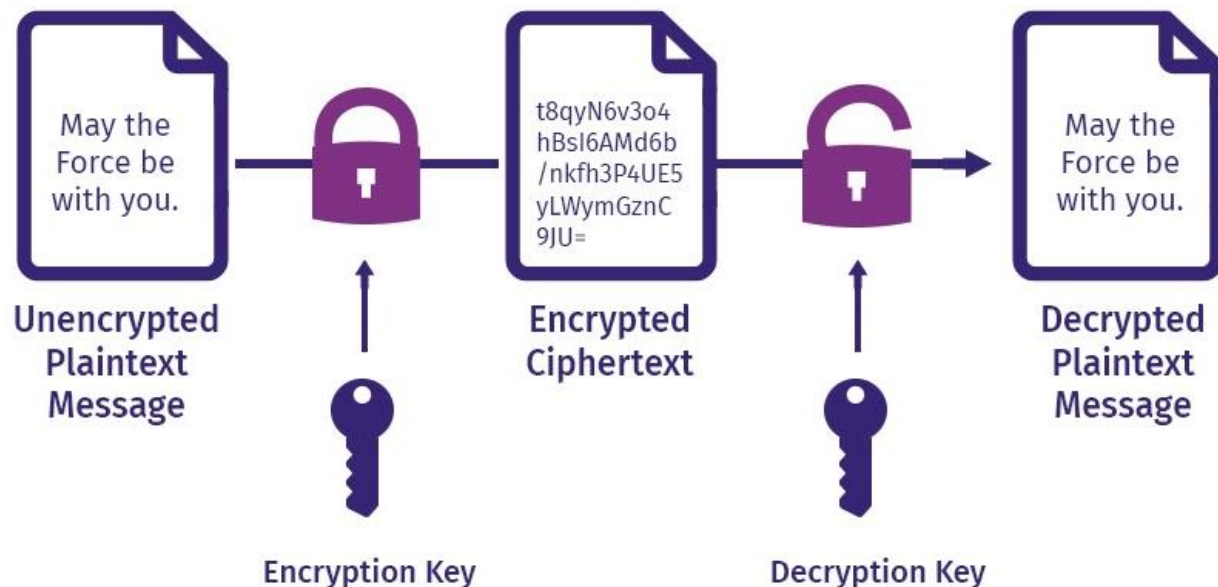
- Adres IP użytkownika jest zamaskowany przez adres IP serwera VPN, co utrudnia śledzenie lokalizacji i aktywności użytkownika.

Cyberobrona

Szyfrowanie danych (Data Encryption)

to proces przekształcania danych w taki sposób, aby były one nieczytelne dla osób nieautoryzowanych.

Tylko osoby posiadające odpowiedni klucz szyfrowania mogą odszyfrować i odczytać zaszyfrowane informacje.



Poufność:

- Zapewnia, że tylko upoważnione osoby mogą uzyskać dostęp do danych.

Integralność:

- Chroni dane przed nieautoryzowaną modyfikacją.

Autentyczność:

- Umożliwia weryfikację, że dane pochodzą od zaufanego źródła.

Bezpieczeństwo podczas przesyłania:

- Chroni dane podczas przesyłania przez sieci publiczne, takie jak Internet.

Cyberobrona

Autoryzacja wielostopniowa (MFA, Multi-Factor Authentication)

to metoda zabezpieczania systemów informatycznych, która wymaga od użytkowników przedstawienia dwóch lub więcej niezależnych dowodów tożsamości (tzw. czynników) w celu uzyskania dostępu do zasobu. Celem MFA jest zwiększenie poziomu bezpieczeństwa poprzez wymaganie więcej niż jednego rodzaju uwierzytelnienia.

Czynniki wiedzy:

- Hasło/PIN: Informacje, które użytkownik zna.
- *Przykład: Tradycyjne hasła, kody PIN.*

Czynniki posiadania:

- Tokeny fizyczne/wirtualne: Coś, co użytkownik posiada.
- *Przykład: Karty, tokeny RSA, aplikacje generujące kody jednorazowe*

Czynniki cech biometrycznych:

- Biometria: Coś, co użytkownik jest.
- *Przykład: Odcisk palca, rozpoznawanie twarzy, skanowanie tęczówki.*

Czynniki lokalizacyjne:

- Lokalizacja: Gdzie użytkownik jest.
- *Przykład: Uwierzytelnianie na podstawie lokalizacji geograficznej.*

Czynniki czasowe:

- Czas: Kiedy użytkownik jest.
- *Przykład: Ograniczenia czasowe dostępu do systemu.*

Cyberobrona



7 Podstawowych Zasad Korzystania z Aplikacji Bankowych

Nr	Zasada	Opis	Przykład
1	Używaj silnych i unikalnych haseł	Twórz silne hasła, które są trudne do odgadnięcia, i używaj unikalnych haseł dla każdej aplikacji.	<i>Kombinacja liter (dużych i małych), cyfr i symboli, np. "P@ssw0rd!23".</i>
2	Włącz uwierzytelnianie dwuskładnikowe (2FA)	Włącz dodatkowy poziom zabezpieczeń, który wymaga podania drugiego kodu (np. z aplikacji uwierzytelniającej lub SMS)	<i>Aplikacje takie jak Google Authenticator, Authy lub kody SMS od banku.</i>
3	Aktualizuj oprogramowanie	Regularnie aktualizuj system operacyjny swojego urządzenia i aplikacje bankowe, aby mieć pewność, że korzystasz z najnowszych zabezpieczeń.	<i>Włącz automatyczne aktualizacje w ustawieniach telefonu i aplikacji.</i>
4	Uważaj na podejrzaną wiadomości i linki	Nie klikaj na linki w podejrzanym e-mailach, SMS-ach lub wiadomościach, które mogą prowadzić do stron phishingowych.	<i>Sprawdź dokładnie adresy URL stron, na które jesteś przekierowywany, zanim wprowadzisz swoje dane.</i>
5	Korzystaj tylko z zaufanych sieci	Unikaj logowania się do aplikacji bankowych przez publiczne Wi-Fi. Używaj sieci zaufanych lub korzystaj z VPN.	<i>Jeśli musisz skorzystać z publicznego Wi-Fi, włącz VPN, aby zabezpieczyć swoje połączenie.</i>
6	Monitoruj swoje konto regularnie	Regularnie sprawdzaj swoje transakcje bankowe, aby szybko wykryć i zgłosić nieautoryzowane operacje.	<i>Ustaw powiadomienia SMS lub e-mail o transakcjach na swoim koncie.</i>
7	Nie zapisuj danych logowania	Nie zapisuj swoich danych logowania do aplikacji bankowych w przeglądarkach internetowych ani w aplikacjach notatek.	<i>Zapamiętaj swoje hasła lub używaj bezpiecznych menedżerów haseł.</i>

Czy twój telefon jest bezpieczny?



Sprawdź te numery:

***#62#**

***#21#**

***#06#**

Cyberobrona



7 Zasad Bezpiecznego Korzystania z Wi-Fi

Nr	Zasada	Opis	Przykład
1	Unikaj korzystania z publicznych sieci Wi-Fi	Publiczne Wi-Fi jest często niezabezpieczone, co zwiększa ryzyko przechwycenia danych przez osoby trzecie.	<i>Korzystaj z danych mobilnych lub prywatnych, zabezpieczonych sieci Wi-Fi.</i>
2	Wyłącz udostępnianie plików na urządzeniach w publicznych sieciach Wi-Fi	Udostępnianie plików może prowadzić do nieautoryzowanego dostępu do Twoich danych przez inne osoby w tej samej sieci.	<i>Wyłącz funkcję udostępniania plików w ustawieniach swojego systemu operacyjnego.</i>
3	Sprawdzaj, do jakiej sieci się łączysz	Upewnij się, że łączysz się z właściwą siecią, a nie z fałszywą siecią utworzoną przez cyberprzestępców.	<i>Sprawdź nazwę sieci (SSID) i upewnij się, że jest zgodna z nazwą podaną przez właściciela miejsca.</i>
4	Wyłącz automatyczne łączenie z sieciami Wi-Fi	Automatyczne łączenie z sieciami Wi-Fi może sprawić, że urządzenie połączy się z niezabezpieczoną lub fałszywą siecią.	<i>Wyłącz automatyczne łączenie w ustawieniach Wi-Fi swojego urządzenia.</i>
5	Stosuj silne hasła do swojej domowej sieci Wi-Fi	Silne hasła utrudniają nieautoryzowany dostęp do Twojej sieci.	<i>Użyj kombinacji liter, cyfr i symboli, np. "H@rd2Gu3ssP@ssw0rd".</i>
6	Zmień domyślne nazwy użytkownika i hasła routera	Domyślne dane logowania do routera są łatwe do odgadnięcia, co może umożliwić atak na Twoją sieć.	<i>Zmień nazwę użytkownika i hasło na coś bardziej skomplikowanego i unikalnego.</i>
7	Aktualizuj oprogramowanie routera	Regularne aktualizacje oprogramowania routera naprawiają luki bezpieczeństwa i chronią sieć przed nowymi zagrożeniami.	<i>Sprawdź, czy Twój router ma opcję automatycznych aktualizacji lub ręcznie sprawdzaj dostępność aktualizacji.</i>

Cyberobrona

Macierz MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge)

to publiczna baza wiedzy, klasyfikująca **techniki, taktyki i procedury** (TTPs) stosowane przez cyberprzestępców w rzeczywistych incydentach.

<https://attack.mitre.org/matrices/enterprise/>

Struktura macierzy

- Taktyki (Tactics) — odpowiadają celom atakujących (np. uzyskanie dostępu do systemu, wykradanie danych)
- Techniki (Techniques) — to sposoby osiągania tych celów (np. fałszywy e-mail z załącznikiem, pozyskiwanie haseł z pamięci)
- Podtechniki (Sub-techniques) — bardziej szczegółowe wersje technik (np. odczyt haseł z procesu LSASS w Windowsie)
- Procedury (Procedures) — to konkretne przykłady z prawdziwych ataków (np. grupa APT29 użyła narzędzia Mimikatz)

Zastosowanie w praktyce

- Analiza zagrożeń (threat intelligence)
- Budowanie strategii obronnych (threat-informed defense)
- Testowanie bezpieczeństwa (red teaming, purple teaming)
- Ocena dojrzałości cyberbezpieczeństwa (security maturity assessment)

Zalety stosowania ATT&CK

- Ujednolicenie języka bezpieczeństwa IT
- Wspomaganie detekcji i reagowania na incydenty
- Transparentna dokumentacja technik APT i grup cyberprzestępczych

Reconnaissance	Resource Development	Initial Access	Execution	Persistence
10 techniques	8 techniques	11 techniques	16 techniques	23 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (12)	BITS Jobs
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	ESXi Administration Command	Cloud Application Integration
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Exploitation for Client Execution	Compromise Host Software Binary
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Input Injection	Create Account (3)
	Stage Capabilities (6)		Inter-Process Communication	

Cyberobrona

Security Content Automation Protocol (SCAP)

to zestaw standardów opracowany przez NIST, który umożliwia automatyzację oceny bezpieczeństwa systemów IT oraz zgodności z politykami i regulacjami.

Główne cele

Automatyzacja
skanowania systemów
pod kątem luk i
błędnych konfiguracji

Standaryzacja
formatów wymiany
informacji o
zagrożeniach

Wspieranie zgodności
z normami (np.
ISO/IEC 27001, NIST
800-53, PCI-DSS)

Security Content Automation Protocol (SCAP)

SCAP to zbiór wzajemnie powiązanych specyfikacji:

Komponent SCAP	Opis funkcji	Link
NVD National Vulnerability Database	Centralne repozytorium informacji o lukach. Zawiera checklisty, opisy błędów i oceny wpływu.	nvd.nist.gov
CVE Common Vulnerabilities and Exposures	Uniwersalny system identyfikacji publicznie znanych luk. Zarządzany przez MITRE.	cve.mitre.org
CVSS Common Vulnerability Scoring System	System oceniania powagi luk w zabezpieczeniach. Ułatwia priorytetyzację zagrożeń.	first.org/cvss
CPE Common Platform Enumeration	Standard nazewnictwa systemów operacyjnych, aplikacji i urządzeń.	nvd.nist.gov/products/cpe
CCE Common Configuration Enumeration	System identyfikacji błędów i problemów konfiguracyjnych.	cve.mitre.org
XCCDF Extensible Configuration Checklist Description Format	Format opisu list kontrolnych bezpieczeństwa w postaci XML.	csrc.nist.gov/projects/.../xccdf
OVAL Open Vulnerability and Assessment Language	Język do definiowania i testowania podatności oraz błędów konfiguracyjnych.	oval.mitre.org
OCIL Open Checklist Interactive Language	Język do tworzenia interaktywnych pytań oceniających zgodność (np. dla audytów).	csrc.nist.gov/projects/.../ocil
AID Asset Identification	Standard jednoznacznej identyfikacji zasobów IT (systemów, urządzeń).	csrc.nist.gov/projects/scap/aid
ARF Asset Reporting Format	Format łączenia, raportowania i korelowania informacji o zasobach.	csrc.nist.gov/projects/scap/arf
CCSS Common Configuration Scoring System	System oceniania krytyczności błędów konfiguracyjnych.	csrc.nist.gov/projects/scap/ccss
TMSAD Trust Model for Security Automation Data	Model przetwarzania danych XML z uwzględnieniem podpisów, hashy i tożsamości.	csrc.nist.gov/projects/scap/tmsad

Zależności między CVE, CPE i CVSS

CVE (Common Vulnerabilities and Exposures) - podatności

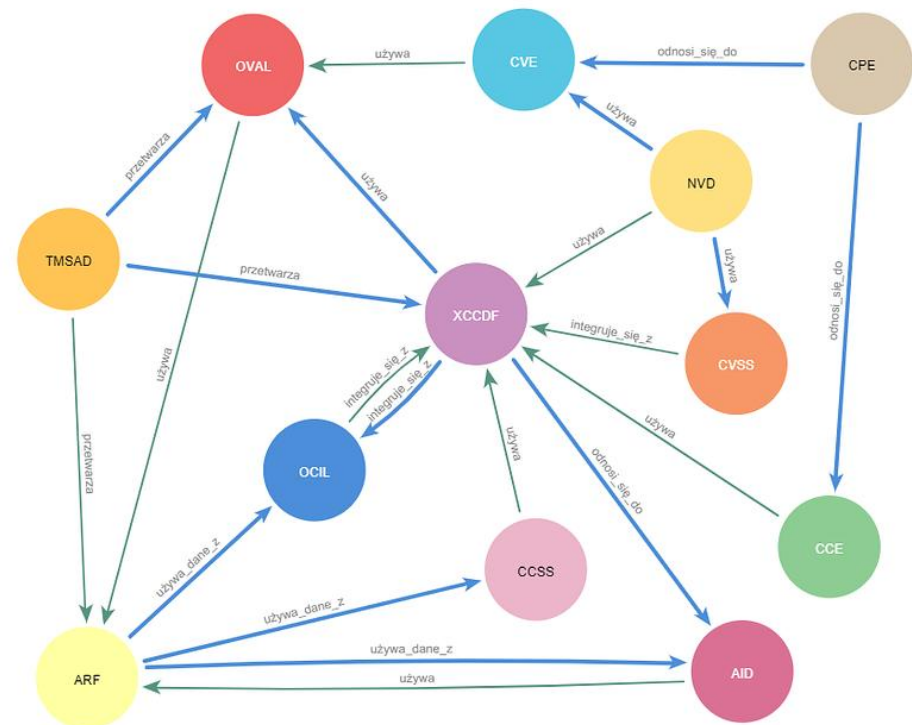
- To **główny byt** opisujący podatność (np. CVE-2021-44228).
- Każdy rekord CVE zawiera:
 - ♦ opis podatności
 - ♦ listę dotkniętych produktów (CPE)
 - ♦ ocenę powagi (CVSS)

CPE (Common Platform Enumeration) - infrastruktura

- CPE jest **przypisany do CVE** — mówi, które konkretne systemy, aplikacje lub wersje są podatne
- Przykład: dany CVE może dotyczyć Log4j w wersjach 2.0 do 2.14.1.
- Te wersje mają unikalne identyfikatory CPE.

CVSS (Common Vulnerability Scoring System) - ocena

- CVSS to **metryka przypisana do danego CVE**.
- Nie ocenia systemu, ale **konkretną podatność (CVE)** — np. czy pozwala na zdalne wykonanie kodu, czy wymaga fizycznego dostępu itp.
- CVSS nie jest zależny od CPE, ale jest **powiązany z CVE**.




```
{  
  "cve_id": "CVE-2021-12345",  
  "description": "Remote code execution in ExampleApp via crafted request.",  
  "cpe": "cpe:2.3:a:examplevendor:exampleapp:1.0.0:*:*:*:*:*:*:*:",  
  "cvss": {  
    "vector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H",  
    "base_score": 9.8,  
    "severity": "CRITICAL"  
  },  
  "published": "2021-06-01",  
  "last_modified": "2021-06-02",  
  "reference": "https://example.com/security/advisory/CVE-2021-12345"  
}
```

Cyberobrona

NIST (National Institute of Standards and Technology) Narodowy Instytut Standaryzacji i Technologii w Stanach Zjednoczonych.

To rządowa instytucja podległa Departamentowi Handlu USA, której zadaniem jest:

- Tworzenie standardów technicznych (np. pomiarów, kryptografii, bezpieczeństwa IT)
- Opracowywanie wytycznych i norm bezpieczeństwa cybernetycznego
- Badania naukowe i inżynieryjne wspierające innowacje technologiczne



NIST i cyberbezpieczeństwo:

- NIST jest autorem wielu kluczowych dokumentów i ram bezpieczeństwa, m.in.:
- NIST Cybersecurity Framework (CSF) – szeroko stosowany model zarządzania ryzykiem cybernetycznym
- NIST SP 800-53 / SP 800-171 – standardy dla zabezpieczania systemów informatycznych
- SCAP, CVSS, XCCDF, OVAL – komponenty standaryzacji bezpieczeństwa automatycznego

<https://www.nist.gov>

Instytut ten pełni kluczową rolę również w rozwoju algorytmów kryptograficznych (np. AES, SHA-2, SHA-3).



<https://youtu.be/5Y9Mb0tNPy4?si=rioA7ZX6zPKSltU>

Zadanie

(0-2 pkt)



Treść

Opisz w jakie mechanizmy lub zasady Cyberobrony stosujesz lub są stosowane

1. U ciebie w domu.
2. W miejscu gdzie pracujesz lub uczysz się.

Należy opisać 1. i 2.

Przykładowe zagadnienia, które możesz opisać:

- Stosowanie menedżera haseł w celu bezpiecznego zarządzania danymi logowania.
- Zabezpieczenie domowej sieci Wi-Fi poprzez silne hasło, protokół WPA3 i ewentualną segmentację sieci (np. osobna sieć dla urządzeń IoT).
- Włączenie uwierzytelniania dwuskładnikowego (2FA) w serwisach online jako dodatkowy poziom ochrony.
- Regularne aktualizowanie systemu operacyjnego oraz zainstalowanego oprogramowania w celu eliminowania znanych podatności.
- Rozpoznawanie i unikanie zagrożeń socjotechnicznych (phishing, spoofing, manipulacje komunikacyjne).
- Uczestnictwo w szkoleniach z zakresu podstaw cyberbezpieczeństwa

Termin przesłania sprawozdania,
wskazany w zadaniu w Moodle.



Bezpieczny internet

www.demotywatory.pl