WPROWADZENIE DO CYBERBEZPIECZEŃSTWA

KURS WSTĘPNY: PRZECIWDZIAŁANIE I OBRONA

ZARYS WYKŁADU

Dowiesz się jak ocenić różne perspektywy możliwych ataków oraz jak próbować im przeciwdziałać.

- Przegląd możliwości obronnych
- Przypadek użycia: NotPetya
- Obrona przed cyberatakami
- Ocena ryzyka

PRZEGLĄD MOŻLIWOŚCI OBRONNYCH

DLACZEGO OBRONA JEST WAŻNA?

- Zapobiega nieautoryzowanemu dostępowi
- Chroni dane osobowe
- Zapewnia bezpieczeństwo informacji organizacyjnych
- Zapobiega utracie i wyciekom danych

OBRONA OSOBISTA I HIGIENA CYBERNETYCZNA

Wiele osób zapisuje cenne dane
w formacie cyfrowym.

Dane można zapisywać na komputerach,
telefonach i wielu innych urządzeniach.

Każde urządzenie pozostawione samotnie
lub podłączone do sieci
może zostać „zhakowane”.

OBRONA W PRZEDSIĘBIORSTWIE

Każda organizacja
przechowuje dane na różne sposoby.

Zaszyfrowane, skradzione lub wyciekające dane mogą prowadzić do znacznych szkód.

Przedsiębiorstwa mogą również przechowywać wrażliwe informacje o klientach.

SPECJALIŚCI OD CYBERBEZPIECZEŃSTWA

- Każdego dnia powstają nowe technologie.
- Do testowania i odkrywania potencjalnych luk w zabezpieczeniach potrzebni są specjaliści ds. bezpieczeństwa.
- Profesjonaliści podpowiadają odpowiednie rozwiązania.

Aby zapewnić najlepsze rozwiązania,
specjalista ds. cyberbezpieczeństwa musi znać oba „światy”,
atakującego i obrońcy.

NAJLEPSZE PRAKTYKI OBRONNE

Wytyczne
Wielu producentów systemów i urządzeń udostępnia najlepsze praktyki w zakresie bezpieczeństwa.

Propozycje
Siła hasła, implementacje funkcji bezpieczeństwa, kopie zapasowe i nie tylko…

PRZYPADEK UŻYCIA: NOTPETYA

LUKI W ZABEZPIECZENIACH A ICH ŁAGODZENIE

Podatności
Luki w systemie, które potencjalnie mogą zostać wykorzystane przez osobę atakującą

Łagodzenie
Proces w systemie, który próbuje zidentyfikować potencjalne luki i je naprawić.

Znajdowanie i łagodzenie luk w zabezpieczeniach to niekończące się zadanie, a metody wdrażania stale się rozwijają.

NOTPETYA

Oprogramowanie ransomware,
które w 2017 r. atakowało głównie Ukrainę.

Ransomware rozprzestrzeniał się
pomiędzy komputerami
za pośrednictwem exploita EternalBlue.

Szacunkowe szkody wyniosły prawie
10 miliardów dolarów.

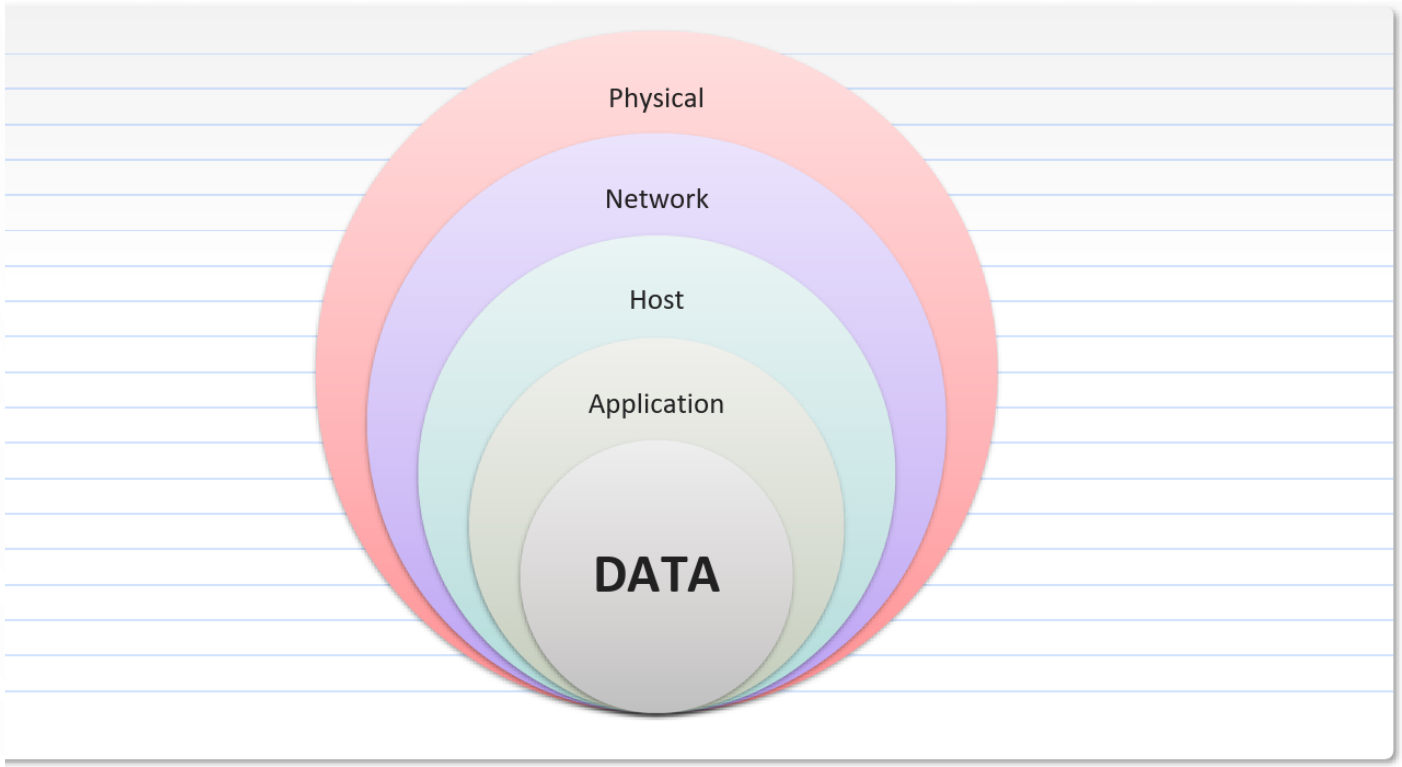
ZAPOBIEGANIE NOTPETYI

NotPetya wykorzystał lukę,
która została już załatana przez Microsoft.

Gdyby użytkownicy zainstalowali łatkę,
szkody można byłoby zmniejszyć
lub im zapobiec.

OBRONA PRZED CYBERATAKAMI

GŁĘBOKA OBRONA (DEFENSE IN DEPTH - DID)



DiD to koncepcja definiująca wielowarstwową strukturę bezpieczeństwa.

PRZEGLĄD ELEMENTÓW KONTROLNYCH

Kategoria	Przykład	Zastosowanie
Fizyczna	Ogrodzenie	Utrudnia dostęp
Fizyczna	Drzwi	Kontroluje dostęp
Fizyczna	Pracownik ochrony	Zgłaszanie i odpowiadanie
Techniczna	Antywirus	Wykrywa malware
Techniczna	Filtrowanie ruchu sieciowego	Kontroluje dostęp do stron internetowych
Administracyjna	Polityka bezpieczeństwa	Określa zasady postępowania

Środki fizyczne chronią aktywa w środowisku fizycznym.
Środki techniczne (logiczne) wykorzystują oprogramowanie i sprzęt do ochrony zasobów.
Środki administracyjne określają (i uczą) właściwe zachowania i działania.

ŚRODKI FIZYCZNE

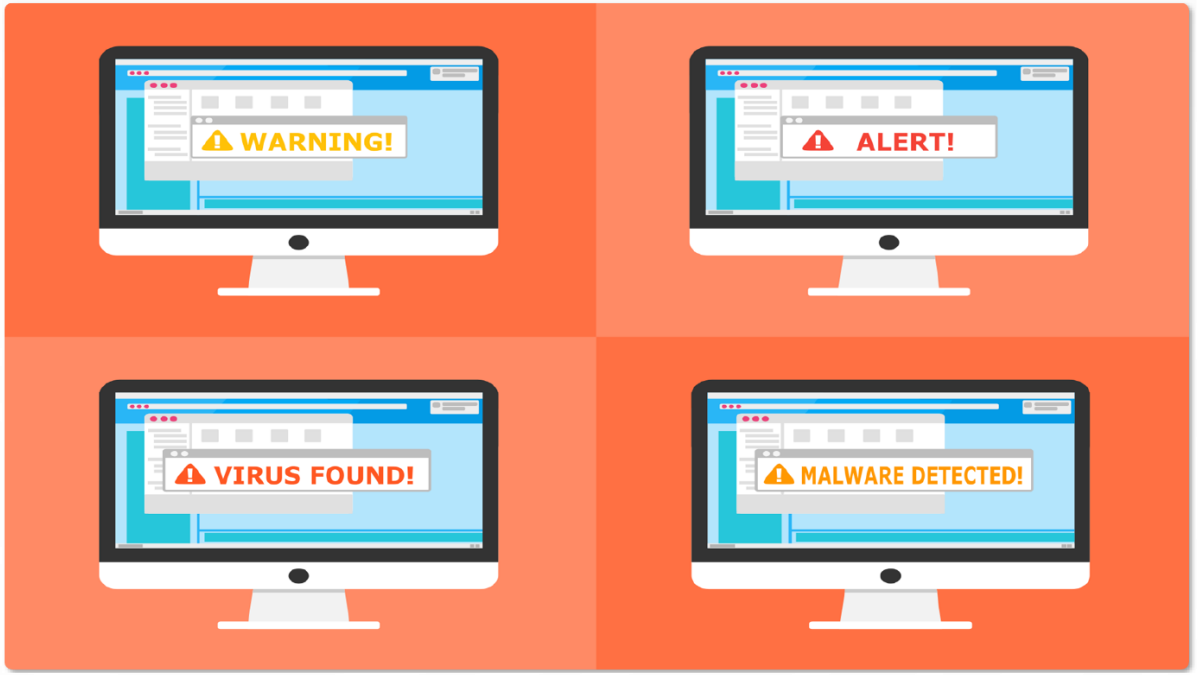
Wdrożenie fizycznych środków bezpieczeństwa, takich jak ogrodzenia, telewizja przemysłowa, drzwi, pracownicy ochrony itp.

Zapobieganie fizycznemu, nieograniczonemu dostępowi do ważnych systemów.

ŚRODKI TECHNICZNE

Wdrożenie ochrony oprogramowania i sprzętu, w tym zapory ogniowe, oprogramowanie antywirusowe i inne.

Zapobieganie nieautoryzowanemu dostępowi do sieci.



FIREWALL

- Zbiór reguł definiujących kontrolę ruchu sieciowego
- Kontroluje przychodzący ruch sieciowy
- Kontroluje wychodzący ruch sieciowy
- Może mieć postać oprogramowania lub urządzenia fizycznego

Typowymi dostawcami fizycznych zapór sieciowych są:
Check Point, FortiGate i Palo Alto.

ANTYWIRUS

- Chroni przed złośliwym oprogramowaniem
- Potrafi wykrywać, usuwać i zapobiegać działaniu złośliwego oprogramowaniu
- Implementuje identyfikację w oparciu o wiele parametrów
- Ochrona oparta na podpisach, metodach heurystycznych; działająca w czasie rzeczywistym

Typowe oprogramowanie antywirusowe: Avast, ESET i AVG.

ŁAGODZENIE SKUTKÓW ATAKÓW WOLUMETRYCZNYCH

Atak oparty na dużym wolumenie ruchu sieciowego (DDoS).

Ruch można rozróżnić na kilka sposobów.

Narzędzia wyszukują sygnatury, takie jak adresy IP, pliki cookie i nagłówki HTTP.

ŁAGODZENIE SKUTKÓW ATAKÓW NA SIECI BEZPRZEWODOWE

Cele ataku mogą obejmować Wi-Fi, Bluetooth i NFC.

Polityka „zero zaufania”: luki w zabezpieczeniach i zagrożenia stwarzają ryzyko ujawnienia danych w każdej sieci.

Łagodzenie skutków ataku obejmuje wiele warstw zabezpieczeń: aktualizacje, silne szyfrowanie, najnowsze protokoły, NAC, VPN, czy silne uwierzytelnianie.

ZAPORA SIECIOWA APLIKACJI INTERNETOWYCH

Monitoruje ruch internetowy w obu kierunkach.

Potrafi filtrować i blokować ataki internetowe, które mogą wyrządzić szkody w przedsiębiorstwie

ModSecurity to zapora sieciowa typu open source dla aplikacji internetowych.

IDS I IPS

Intrusion Detection System (IDS)
Monitoruje aktywność w sieci lub systemie
i zgłasza wszelkie podejrzane zachowania lub naruszenia.

Intrusion Prevention System (IPS)
Oprócz funkcji IDS, IPS zapobiega także złośliwej aktywności.

ĆWICZENIE

Zagraj w grę i podejmuj decyzje mające na celu ochronę przedsiębiorstwa i jego produktu.

Kliknij ten link, aby rozpocząć:
http://datacenterattacks.trendmicro.com/
http://targetedattacks.trendmicro.com/cyoa/en/
http://targetedattacks.trendmicro.com/cyoa/pol/

ŚRODKI ADMINISTRACYJNE

Wdrażanie zasad
i świadomości bezpieczeństwa.

Konfigurowanie uprawnień dostępu
i wytycznych dotyczących
bezpiecznego użytkowania.

Zapobieganie błędom ludzkim,
które mogą prowadzić do naruszeń.

POLITYKI BEZPIECZEŃSTWA

- Określa reguły dozwolonej aktywności użytkowników.
- Zdefiniuje uprawnienia i ograniczenia.
- Można skonfigurować tak, aby rejestrować aktywność użytkowników.

Powszechnym zastosowaniem zasad polityk bezpieczeństwa jest kontrola urządzeń, która, między innymi, może ograniczać korzystanie z płyt CD, USB itp. w przedsiębiorstwie.

ŚWIADOMOŚĆ BEZPIECZEŃSTWA

- Skłanianie użytkowników do zwrócenia uwagi na możliwe zagrożenia cybernetyczne.
- Demonstrowanie jak wygląda zagrożenie i jakie działania można podjąć przeciwko niemu.
- Minimalizcja ryzyka błędu ludzkiego.

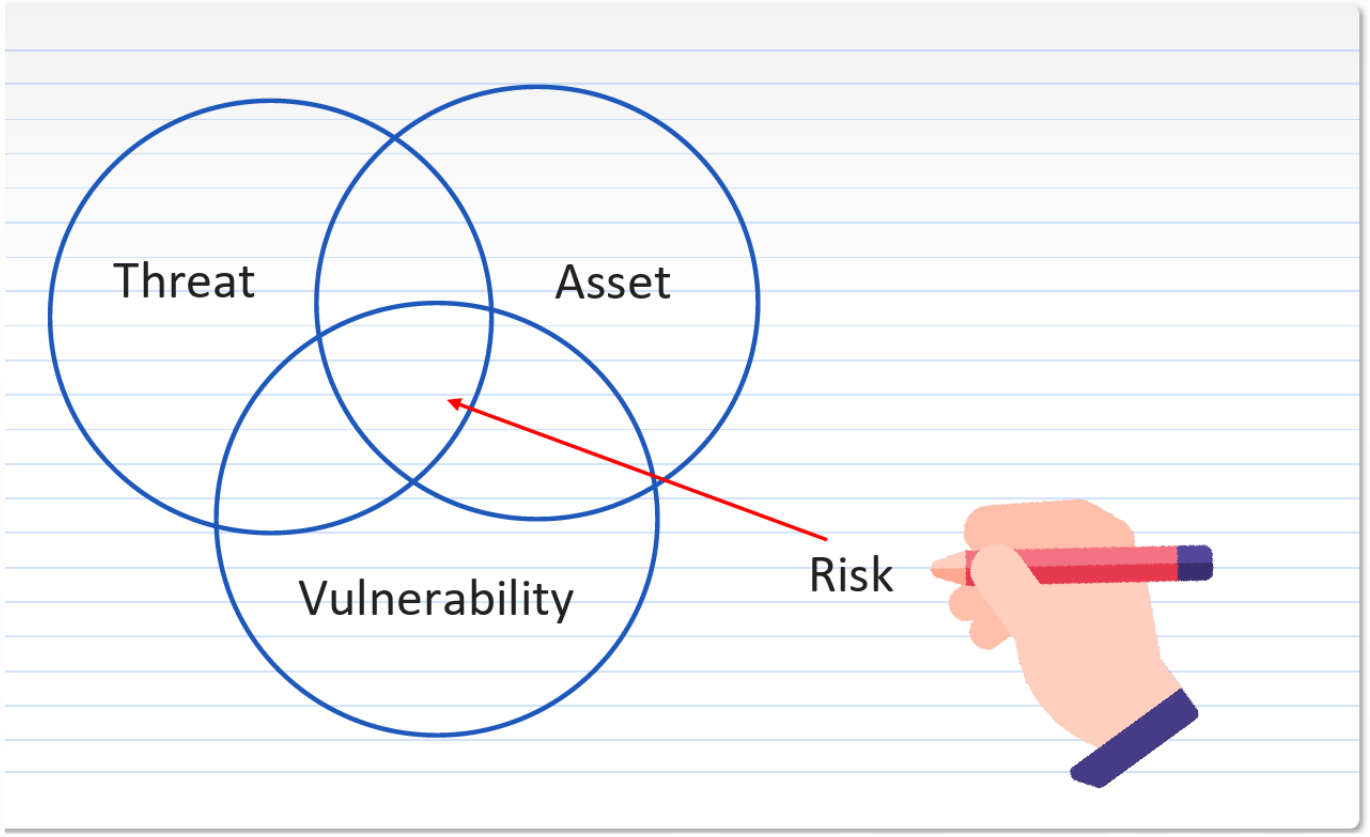
Każda organizacja powinna wprowadzić szkolenia podnoszące świadomość bezpieczeństwa swoich pracowników.

OCENA RYZYKA

OKREŚLENIE RYZYKA

Na określenie ryzyka wpływa zasób, podatność i zagrożenie.

Poziom ryzyka określa się poprzez oszacowanie tych trzech wielkości.



ZASOBY (AKTYWA)

Physical Assets

Information Assets

Human Assets

Reputation Assets

PODATNOŚĆ

- Możliwa luka w zabezpieczeniach.
- Może dotyczyć oprogramowania lub sprzętu.
- Może zostać wykorzystana przez atakującego.
- Może prowadzić do nieautoryzowanego dostępu do sieci, systemu czy aplikacji

ZAGROŻENIE

Kto zagraża aktywom?

Dlaczego stanowią zagrożenie?

W jaki sposób mogą wpłynąć na podatności aktywów?

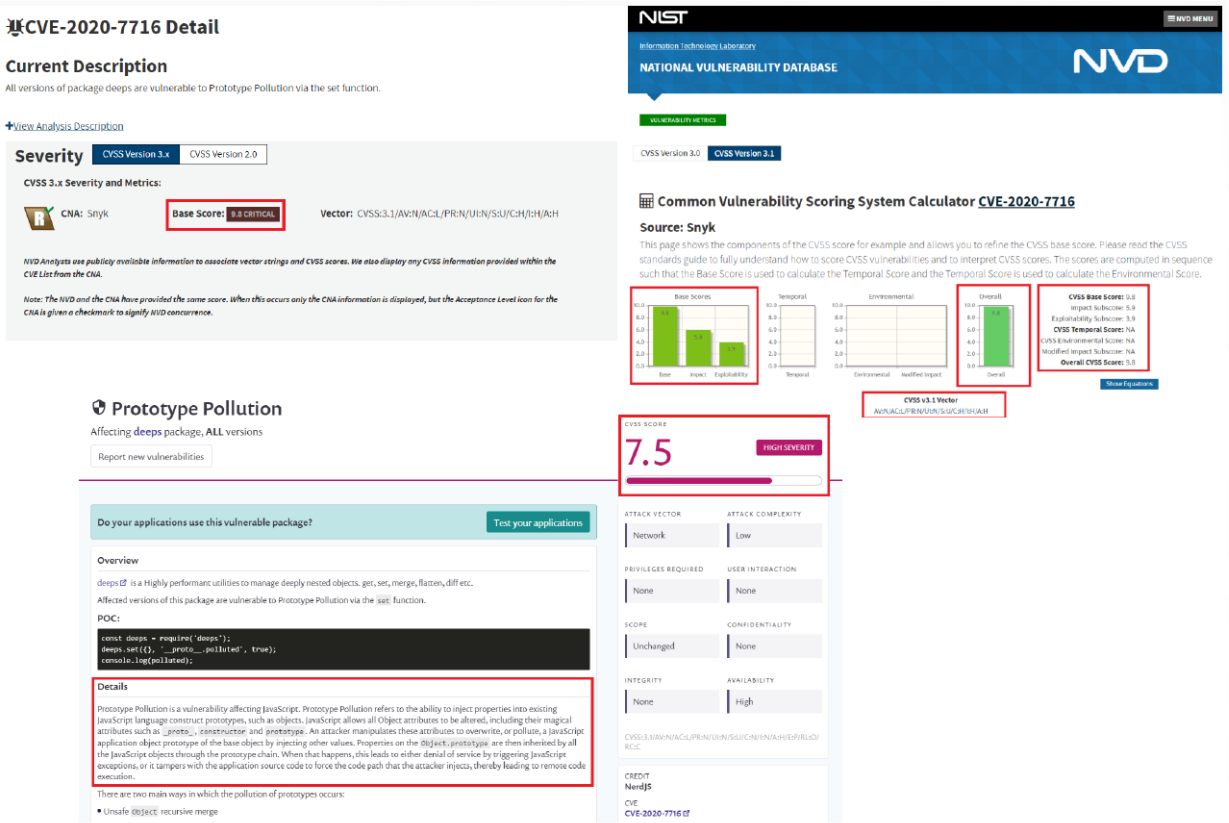
BAZA DANYCH PODATNOŚCI I RAPORTOWANIE ZAGROŻEŃ

Baza danych NVD śledzi znane luki w zabezpieczeniach (nvd.nist.gov).

Formuły wykorzystywane w raportach oceny ryzyka.

Szczegółowe informacje na temat podatności, zagrożenia i charakteru exploita.

Pomaga przedsiębiorstwom określić ryzyko.



ZARZĄDZANIE RYZYKIEM (PARAMETRY)

AV (Asset's Value)
Wartość zasobu

EF (Exposure Factor)
Procent oczekiwanej kwoty szkód wynikających z ryzyka.

ARO (Annual Rate of Occurrence)
Oczekiwanie wystąpienia ryzyka

OBLICZANIE RYZYKA

Obliczenie oczekiwanej pojedynczej straty
(Single-loss Expectancy - SLE),
czyli oczekiwanej szkody
w wyniku pojedynczego zdarzenia ryzyka

$$SLE = AV \times EF$$

Obliczenie oczekiwanej rocznej straty
(Annual Loss Expectancy - ALE),
czyli oczekiwanej rocznej szkody
spowodowanej ryzykiem

$$ALE = SLE \times ARO$$

ĆWICZENIE

Oblicz wartości SLE i ALE zgodnie z parametrami dla serwera o wartości 600 000 USD.

Jaka jest wartość zasobu?
Cyberatak ransomware spodziewany jest raz na cztery lata.
Jaka jest wartość SLE?
Jaka jest wartość ALE?

DZIĘKUJĘ ZA UWAGĘ!

MACIEJ.RYBCZYNSKI@UJK.EDU.PL