Zastosowanie AI w Zadaniach Cyberbezpieczeństwa

Wykład II

90 min · Zagrożenia · Ochrona danych · Bezpieczeństwo org. · Narzędzia & dobre praktyki

Plan wykładu

90 minut · 4 główne bloki tematyczne

01	Wprowadzenie: podstawowe rodzaje zagrożeń I ataków	30 min
02	Domeny CISSP	20 min
03	Bezpieczeństwo w organizacji	20 min
04	Narzędzia i dobre praktyki	15 min
Q&A	Pytania i dyskusja	5 min

01

Wprowadzenie

Podstawowe rodzaje zagrożeń i ataków

Klasyfikacja zagrożeń cybernetycznych

Podział wg rodzaju ataku i wektora

Złośliwe oprogramowanie

Wirusy, trojany, ransomware, spyware

Ataki sieciowe

DDoS, MITM, sniffing, spoofing

Inżynieria społeczna

Phishing, spear-phishing, vishing

Ataki na aplikacje

SQL injection, XSS, CSRF, IDOR

Zagrożenia wewnętrzne

Insider threat, privilege misuse

APT

Advanced Persistent Threat – długofalowe ataki

Inżynieria społeczna – najgroźniejszy wektor

80% naruszeń bezpieczeństwa zaczyna się od czynnika ludzkiego

Rodzaje ataków

- Phishing – masowy, e-mail
- Spear-phishing – celowany
- Whaling – atak na kadrę zarządzającą
- Vishing – przez telefon
- Smishing – przez SMS
- Pretexting – fałszywy scenariusz
- Baiting – pendrive w miejscu publicznym

Jak się bronić?

- Weryfikacja nadawcy (SPF, DKIM, DMARC)
- Szkolenia z bezpieczeństwa (cykliczne)
- MFA na wszystkich kontach
- Zero Trust – nigdy nie ufaj, zawsze weryfikuj
- Procedury weryfikacji tożsamości
- Regularne testy phishingowe w org.

Ransomware – anatomia ataku

Jeden z najbardziej dotkliwych ataków finansowych

1	2	3	4	5
Infekcja	**Rekonesans**	**Eskalacja**	**Szyfrowanie**	**Okup**
phishing / exploit	mapowanie sieci, dane	privilege escalation	AES + RSA, shadow copy	crypto, dark web

$5.08M

średni koszt ataku (2025)

241 dni

Czas od ataku do pełnego opanowania sytuacji

37%

firm zapłaciło okup

Źródło: https://www.ibm.com/reports/data-breach

02

Domeny CISSP

Certified Information System Security Professional

CISSP – 8 Domen Bezpieczeństwa

Security and Risk Management
Definiuje cele, zasady I przepisy, które organizacja musi przestrzegać, aby być zgodna z prawem.

Identity and Access Management
Kontroluje, kto I do czego ma dostęp w organziacji, zarówno fizycznie, jak I cyfrowo.

Asset Security
Odpowiada za ochronę, przechowywanie I bezpieczne niszczenie danych oraz sprzętu.

Security Assessment and Testing
Regularnie sprawdza I testuje systemy bezpieczeństwa, aby wykryć luki I podatności.

Security Architecture and Engineering
Zapewnia, że systemy I narzędzia techniczne, takie jak firewalle, są prawidłowo skonfigurowane I chornią organizację.

Integralność
Monitoruje sieć na bieżąco I reaguje na incydenty oraz zagrożenia w czasie rzeczywistym.

Communications and Network Security
Chroni sieci fizyczne I bezprzewodowe przed nieautoryzowanym dostępem I podsłuchem.

Software Development Security
Zapewnia, że aplikacje I systemy są tworzone zgodnie z zasadami bezpiecznego kodowania.

03

Bezpieczeństwo w organizacji

Polityki, procedury, role i kultura bezpieczeństwa

Ramy i standardy bezpieczeństwa

Wybrane standardy używane w organizacjach

NIST CSF	National Institute of Standards – 5 funkcji: Identify, Protect, Detect, Respond, Recover
ISO/IEC 27001	Międzynarodowy standard systemu zarządzania bezpieczeństwem (ISMS)
CIS Controls	20 priorytetowych kontroli bezpieczeństwa – praktyczny punkt startowy
Zero Trust	Architektura 'nigdy nie ufaj, zawsze weryfikuj' - BeyondCorp (Google)

Role w cyberbezpieczeństwie organizacji

Kto za co odpowiada?

CISO

Strategia bezpieczeństwa, zarządzanie ryzykiem, compliance

Security Analyst

Monitoring SIEM, analiza incydentów, triage alertów

Pentester / Red Team

Symulowane ataki, znajdowanie podatności przed złymi aktorami

Blue Team / SOC

Ochrona, detekcja, reagowanie na incydenty w czasie rzeczywistym

DevSecOps

Integracja bezpieczeństwa w pipeline CI/CD, SAST/DAST

Zarząd / Rada

Decyzje budżetowe, akceptacja ryzyka, odpowiedzialność prawna

Cykl reagowania na incydenty (IR)

NIST SP 800-61 – Incident Response Lifecycle

1

Przygotowanie

Plany IR, playbooki, testy

2

Wykrycie & Analiza

SIEM, IDS, korelacja

3

Izolacja

Containment, eradication

4

Odtworzenie

Recovery, powrót do normy

5

Wnioski

Lessons learned, raport

↻ Cykl ciągły – każdy incydent doskonali procesy

04

Narzędzia i dobre praktyki

Technologie, techniki ochrony i codzienne nawyki

Kluczowe kategorie narzędzi

Przegląd typowych rozwiązań w ekosystemie bezpieczeństwa

Skanowanie i recon

Nmap, Shodan, Masscan, Amass

Testy penetracyjne

Metasploit, Burp Suite, OWASP ZAP

SIEM / Log mgmt

Splunk, Elastic SIEM, Graylog, Wazuh

EDR / Antywirus

CrowdStrike, SentinelOne, Defender ATP

Analiza złośl. kodu

Ghidra, IDA Pro, Any.run, VirusTotal

Zarządzanie hasłami

Bitwarden, 1Password, CyberArk PAM

10 dobrych praktyk dla każdego specjalisty IT

Minimum, które każdy powinien stosować

1. MFA wszędzie – authenticator app, nie SMS
2. Silne, unikalne hasła + menedżer haseł
3. Regularne aktualizacje i patch management
4. Szyfrowanie dysków (BitLocker, LUKS)
5. Zasada minimalnych uprawnień (PoLP)
6. Regularne backupy (3-2-1 rule)
7. Segmentacja sieci – VLAN, firewall rules
8. Monitoring i logowanie zdarzeń
9. Security awareness dla całego zespołu
10. Testy bezpieczeństwa – DAST, pentest, bug bounty

OWASP Top 10 – 2025

Najpoważniejsze zagrożenia aplikacji webowych

A01 **Broken Access Control**
Niewłaściwa kontrola dostępu

A02 **Security Misconfiguration**
Domyślne konfiguracje, otwarte S3

A03 **Software Data Integrity Failures**
CI/CD bez walidacji, insecure deserialization

A04 **Cryptographic Failures**
Słabe szyfrowanie, brak HTTPS

A05 **Injection**
SQL, NoSQL, OS, LDAP injection

A06 **Insecure Design**
Brak security by design

A08 **Data Integrity Failures**
Błędy integralności danych

A07 **Security Logging Failures**
Błędy identyfikacji I uwierzytelnienia

A09 **Security Logging and Alerting Failures**
Błędy logowania I alertowania

A10 **Mishandling of Exceptional Conditions**
Nieprawidłowa obsługa wyjątków

Dziękuję za uwagę

Pytania? Dyskusja?