Briefing Dotyczący Cyberbezpieczeństwa

Streszczenie Wykonawcze

Niniejszy dokument stanowi kompleksową syntezę kluczowych zagadnieień z obszaru cyberbezpieczeństwa, opartą na analizie dostarczonych materiałów źródłowych. Dokument ten obejmuje fundamentalne koncepcje, obowiązujące ramy i regulacje prawne, podstawy kryptografii, zasady zarządzania kluczami kryptograficznymi oraz analizę najpowszechniejszych podatności w aplikacjach webowych.Kluczowe wnioski płynące z analizy są następujące:

1. **Dynamiczny Krajobraz Zagrożeń:** Cyberbezpieczeństwo jest krytycznym wyzwaniem dla organizacji i państw w obliczu rosnącej liczby i profesjonalizacji ataków, takich jak ransomware, phishing i ataki na łańcuch dostaw. Zrozumienie aktualnych trendów, poprzez analizę raportów ENISA czy CISA KEV, jest niezbędne do skutecznej obrony.
2. **Fundamentalne Koncepcje:** Podstawą bezpieczeństwa informacji jest triada CIA (Poufność, Integralność, Dostępność), rozszerzana o atrybuty takie jak autentyczność i rozliczalność. Modele bezpieczeństwa, takie jak Bell-LaPadula (poufność) i Biba (integralność), stanowią teoretyczny fundament dla systemów kontroli dostępu.
3. **Ramy Normatywne i Regulacje Prawne:** Organizacje opierają swoje strategie bezpieczeństwa na ramach takich jak NIST Cybersecurity Framework 2.0 oraz normach certyfikowalnych, jak ISO/IEC 27001. Jednocześnie, prawodawstwo unijne, w tym dyrektywa NIS2 (dla podmiotów kluczowych), rozporządzenie DORA (dla sektora finansowego), Cyber Resilience Act (dla produktów cyfrowych) i RODO (ochrona danych osobowych), nakłada rygorystyczne wymagania i przewiduje surowe sankcje za ich nieprzestrzeganie.
4. **Kryptografia jako Filar Bezpieczeństwa:** Kryptografia, zarówno symetryczna (np. AES), jak i asymetryczna (np. RSA), jest podstawowym narzędziem zapewniającym poufność, integralność i autentyczność danych. Zrozumienie jej zasad, w tym zasady Kerckhoffsa, oraz zagrożeń (np. ataki kwantowe) jest kluczowe dla projektowania bezpiecznych systemów.
5. **Krytyczna Rola Zarządzania Kluczami:** Bezpieczeństwo systemów kryptograficznych jest nierozerwalnie związane z prawidłowym zarządzaniem kluczami w całym ich cyklu życia – od bezpiecznego generowania, przez przechowywanie (np. w modułach HSM), aż po nieodwracalne niszczenie. Błędy w tym obszarze niweczą nawet najsilniejsze algorytmy.
6. **Powszechne Podatności Aplikacji Webowych:** Ataki takie jak Cross-Site Scripting (XSS), SQL Injection (SQLi) i Cross-Site Request Forgery (CSRF) pozostają jednymi z najpoważniejszych zagrożeń. Skuteczna obrona wymaga stosowania wielowarstwowych zabezpieczeń, w tym walidacji danych wejściowych, kodowania danych wyjściowych, stosowania zapytań sparametryzowanych oraz mechanizmów takich jak Content Security Policy i tokeny anty-CSRF.
7. **Odpowiedzialność Prawna:** Działania naruszające bezpieczeństwo systemów informatycznych, takie jak nieautoryzowany dostęp czy niszczenie danych, są penalizowane przez polski Kodeks karny (art. 267-269c), co podkreśla konieczność prowadzenia testów bezpieczeństwa w sposób etyczny i zgodny z prawem.

1. Wprowadzenie do Cyberbezpieczeństwa

Materiały źródłowe pochodzą z wykładu wprowadzającego do przedmiotu "Bezpieczeństwo systemów informatycznych", realizowanego na studiach I stopnia na kierunku Informatyka. Celem kursu jest przekazanie studentom fundamentalnej wiedzy teoretycznej i praktycznej, obejmującej definicje kluczowych pojęć (triada CIA, uwierzytelnianie, autoryzacja), rozpoznawanie zagrożeń, znajomość ram i regulacji (NIST CSF, ISO/IEC 27001, NIS2, RODO) oraz rozumienie zasad bezpiecznego projektowania systemów.

1.1. Krajobraz i Ewolucja Zagrożeń

Bezpieczeństwo systemów informatycznych jest jednym z kluczowych wyzwań współczesnych organizacji i państw. Systemy cyfrowe, stanowiące fundament funkcjonowania gospodarki i społeczeństwa, stały się głównym celem ataków.**Główne Trendy w Zagrożeniach:**

- **Wzrost liczby incydentów:** Obserwuje się eskalację ataków typu ransomware, DDoS, phishing oraz kompromitacji łańcucha dostaw.
- **Profesjonalizacja cyberprzestępców:** Grupy przestępcze działają jak zorganizowane przedsiębiorstwa, co zwiększa skuteczność i skalę ich operacji.
- **Wymierne skutki ataków:** Cyberataki prowadzą do strat finansowych, przerw w działaniu usług publicznych oraz naruszenia prywatności obywateli.
- **Geopolityczny wymiar cyberbezpieczeństwa:** Ataki stają się narzędziem w konfliktach międzynarodowych, obejmując cyberszpiegostwo, dezinformację i operacje państwowe.**Przykłady Powszechnych Ataków:**
- **Ransomware:** Szyfrowanie danych w celu wymuszenia okupu.
- **Phishing i spear-phishing:** Wyłudzanie danych uwierzytelniających za pomocą manipulacji psychologicznej.
- **Ataki DDoS:** Paraliżowanie usług poprzez przeciążenie serwerów.
- **Malware ukierunkowane:** Trojany, backdoory i rootkity umożliwiające przejęcie kontroli nad systemem.
- **Ataki na infrastrukturę krytyczną:** Celowanie w systemy energetyczne, transportowe czy wodociągowe.**Ewolucja Podatności Aplikacji Webowych (OWASP Top 10):** Porównanie list OWASP Top 10 z lat 2017 i 2021 pokazuje dynamiczną naturę zagrożeń. Podatności takie jak **Injection** (wstrzykiwanie) spadły w rankingu, podczas gdy na znaczeniu zyskały **Broken Access Control** (nieprawidłowa kontrola dostępu) oraz nowe kategorie, takie jak **Insecure Design** (niebezpieczny projekt) i **Software and Data Integrity Failures** (naruszenia integralności oprogramowania i danych).| Kategoria w 2017 | Pozycja w 2017 | Kategoria w 2021 | Pozycja w 2021 || ------ | ------ | ------ | ------ || Injection | A01 | Broken Access Control | A01 || Broken Authentication | A02 | Cryptographic Failures | A02 || Sensitive Data Exposure | A03 | Injection | A03 || XML External Entities (XXE) | A04 | Insecure Design (Nowa) | A04 || Broken Access Control | A05 | Security Misconfiguration | A05 || Security Misconfiguration | A06 | Vulnerable and Outdated Components | A06 || Cross-Site Scripting (XSS) | A07 | Identification and Authentication Failures | A07 || Insecure Deserialization | A08 | Software and Data Integrity Failures (Nowa) | A08 || Using Components with Known Vulnerabilities | A09 | Security Logging and Monitoring Failures | A09 || Insufficient Logging & Monitoring | A10 | Server-Side Request Forgery (SSRF) (Nowa) | A10 |

Rzetelne Źródła Informacji o Zagrożeniach:

- **ENISA Threat Landscape:** Coroczny raport Europejskiej Agencji ds. Cyberbezpieczeństwa.
- **CISA KEV (Known Exploited Vulnerabilities Catalog):** Lista podatności aktywnie wykorzystywanych w atakach, prowadzona przez amerykańską agencję CISA.
- **CERT Polska:** Analizy, ostrzeżenia i raporty dotyczące zagrożeń w Polsce.
- **OWASP:** Zasoby dotyczące bezpieczeństwa aplikacji webowych i API.
- **Raporty firm komercyjnych:** Analizy od firm takich jak Mandiant, Symantec czy Check Point.

1.2. Podstawowe Pojęcia i Modele Bezpieczeństwa

Celem bezpieczeństwa informacji jest ochrona danych w trzech kluczowych komponentach systemów informatycznych: **sprzęcie, oprogramowaniu i komunikacji** . Ochrona ta realizowana jest na poziomie **fizycznym, personalnym i organizacyjnym** .

1.2.1. Triada CIA i jej Rozszerzenia

Fundamentem bezpieczeństwa informacji jest tzw. **triada CIA** , składająca się z trzech kluczowych atrybutów:

- **Poufność (Confidentiality):** Zapewnienie, że informacja jest dostępna wyłącznie dla osób uprawnionych (np. przez szyfrowanie, kontrolę dostępu).
- **Integralność (Integrity):** Ochrona przed nieautoryzowaną modyfikacją danych, gwarancja ich spójności i poprawności (np. przez sumy kontrolne, podpisy cyfrowe).
- **Dostępność (Availability):** Zapewnienie, że systemy i dane są dostępne dla uprawnionych użytkowników, gdy są potrzebne (np. przez redundancję, kopie zapasowe).Współczesne podejście rozszerza triadę CIA o dodatkowe atrybuty:
- **Autentyczność (Authenticity):** Pewność co do pochodzenia danych i tożsamości.
- **Rozliczalność (Accountability):** Możliwość powiązania działań z konkretnym użytkownikiem.
- **Niezaprzeczalność (Non-repudiation):** Gwarancja, że nadawca nie może wyprzeć się wysłania komunikatu, a odbiorca jego odebrania.Projektowanie systemów wymaga znalezienia równowagi między tymi atrybutami, które często pozostają w konflikcie (np. wysoki poziom poufności może ograniczać dostępność).

1.2.2. Modele Bezpieczeństwa

Modele bezpieczeństwa to formalne opisy zasad kontroli dostępu do zasobów w systemie informatycznym.

- **Model Bell-LaPadula (BLP):** Skoncentrowany na **poufności** . Wprowadza zasady "no read up" (użytkownik o niższych uprawnieniach nie może czytać danych o wyższej klauzuli tajności) i "no write down" (użytkownik o wyższych uprawnieniach nie może zapisywać danych na niższym poziomie).
- **Model Biba:** Skoncentrowany na **integralności** . Działa odwrotnie do BLP, wprowadzając zasady "no write up" (proces o niższym poziomie zaufania nie może modyfikować danych o wyższym poziomie) i "no read down" (proces o wyższym poziomie zaufania nie może odczytywać danych z niższego poziomu).
- **Model Clark-Wilson:** Zorientowany na środowiska komercyjne, dba o integralność danych poprzez **dobrze uformowane transakcje** i **rozdział obowiązków** (separation of duties). Przykładem jest system bankowy, gdzie jedna osoba wprowadza przelew, a inna go zatwierdza.

- **Model Brewer-Nash (Chinese Wall):** Zapobiega **konfliktom interesów** poprzez dynamiczną kontrolę dostępu. Użytkownik, który uzyskał dostęp do danych firmy A, automatycznie traci dostęp do danych jej konkurenta, firmy B.
- **Model RBAC (Role-Based Access Control):** Uprawnienia są przypisywane do ról (np. "administrator", "pracownik HR"), a nie bezpośrednio do użytkowników. Upraszcza to zarządzanie dostępem w dużych organizacjach.

1.3. Ramy, Normy i Regulacje Prawne

Zarządzanie cyberbezpieczeństwem opiera się na ustandaryzowanych ramach (frameworkach), normach oraz obligatoryjnych regulacjach prawnych.

1.3.1. Frameworki i Normy

Cecha / Aspekt,NIST Cybersecurity Framework 2.0,ISO/IEC 27001:2022,EUCC (Common Criteria)
Charakter,"Ramy dobrych praktyk, przewodnik","Norma międzynarodowa, certyfikowalna",Schemat certyfikacji produktów ICT
Obowiązkowość,Dobrowolny,Może być wymagany przez klientów/regulatorów,Wymagany dla określonych produktów w UE
Zakres,Zarządzanie ryzykiem cyberbezpieczeństwa w całej organizacji,System Zarządzania Bezpieczeństwem Informacji (ISMS),"Konkretne produkty i systemy ICT (sprzęt, oprogramowanie)"
Struktura,"6 funkcji: Govern, Identify, Protect, Detect, Respond, Recover","Cykl PDCA, 93 kontrole w 4 kategoriach (organizacyjne, ludzkie, fizyczne, technologiczne)","3 poziomy zapewnienia: Basic, Substantial, High"
Cel główny,"Ocena dojrzałości, priorytetyzacja działań, komunikacja ryzyka","Budowa i certyfikacja ISMS, ciągłe doskonalenie",Potwierdzenie bezpieczeństwa konkretnego produktu
Organ nadzorczy,NIST (USA),ISO + jednostki akredytujące,ENISA + krajowe jednostki certyfikujące

1.3.2. Kluczowe Regulacje Prawne w Unii Europejskiej

- **Dyrektywa NIS2 (Network and Information Security Directive 2):** Akt prawny (UE 2022/2555) mający na celu podniesienie poziomu cyberbezpieczeństwa w całej UE. Rozszerza zakres podmiotów objętych regulacją (m.in. operatorzy usług kluczowych i podmioty ważne), nakłada obowiązek zarządzania ryzykiem, zgłaszania poważnych incydentów (w ciągu 24h) i wprowadza wysokie kary finansowe (do 10 mln EUR lub 2% globalnego obrotu) oraz odpowiedzialność zarządu. Termin implementacji w Polsce to 17 października 2024 r.
- **DORA (Digital Operational Resilience Act):** Rozporządzenie (UE 2022/2554) dotyczące odporności cyfrowej **sektora finansowego** . Obejmuje m.in. banki, ubezpieczycieli i ich dostawców ICT. Wymaga wdrożenia systemu zarządzania ryzykiem ICT, przeprowadzania zaawansowanych testów (np. TLPT) i zarządzania ryzykiem w łańcuchu dostaw. Stosowane od 17 stycznia 2025 r.
- **CRA (Cyber Resilience Act):** Rozporządzenie (UE 2024/2847) wprowadzające wymogi cyberbezpieczeństwa dla **produktów z elementami cyfrowymi** (od IoT po oprogramowanie). Nakłada na producentów obowiązek projektowania zgodnie z zasadą *security by design* , prowadzenia oceny ryzyka, zgłaszania podatności do

ENISA (w ciągu 24h) oraz zapewniania aktualizacji bezpieczeństwa. Główne obowiązki będą stosowane od 11 grudnia 2027 r.

- **RODO (GDPR):** Rozporządzenie (UE 2016/679) o ochronie danych osobowych. Wprowadza 7 zasad przetwarzania danych (m.in. minimalizacja, ograniczenie celu), prawa dla osób fizycznych (np. prawo do bycia zapomnianym) oraz obowiązki dla administratorów (m.in. zgłaszanie naruszeń w ciągu 72h). Naruszenia grożą karami do 20 mln EUR lub 4% globalnego obrotu.

1.4. Modele Zagrożeń i Podatności

- **CVE (Common Vulnerabilities and Exposures):** Globalny system identyfikacji podatności, gdzie każda luka otrzymuje unikalny numer (np. *CVE-2021-44228* dla Log4Shell). Stanowi podstawę dla innych narzędzi i baz danych.
- **CVSS (Common Vulnerability Scoring System) v4.0:** Standard oceny wagi podatności w skali od 0.0 do 10.0. Uwzględnia metryki bazowe (właściwości luki), zagrożenia (czy jest wykorzystywana) i środowiskowe (kontekst organizacyjny).
- **MITRE ATT&CK:** Baza wiedzy o taktykach, technikach i procedurach (TTPs) stosowanych przez cyberprzestępców. Umożliwia modelowanie zagrożeń, planowanie testów (Red Teaming) i mapowanie zdolności obronnych (Blue Teaming).
- **Katalog CISA KEV:** Lista podatności, które są **aktywnie wykorzystywane w atakach** . Służy do priorytetyzacji działań związanych z zarządzaniem podatnościami ("patch first").

1.5. Zasady Bezpieczeństwa w Praktyce i Ustawodawstwo Polskie

Fundamentalne Zasady Projektowania:

1. **Secure by Design:** Uwzględnianie bezpieczeństwa od samego początku cyklu życia oprogramowania, a nie jako dodatku. Obejmuje analizę zagrożeń na etapie projektu i stosowanie bezpiecznych domyślnych konfiguracji (*secure by default*).
2. **Defense in Depth (Obrona w Głąb):** Stosowanie wielu, zróżnicowanych warstw zabezpieczeń (technicznych, organizacyjnych, proceduralnych), zakładając, że każda pojedyncza warstwa może zostać przełamana.**OWASP Top 10:** OWASP publikuje listy najpoważniejszych zagrożeń dla aplikacji webowych, API oraz systemów opartych na modelach językowych (LLM). Stanowią one punkt wyjścia dla zabezpieczania aplikacji i wspólny słownik ryzyk dla zespołów deweloperskich i bezpieczeństwa.

- **Top 10 dla Aplikacji WWW (2021):** A01: Broken Access Control, A02: Cryptographic Failures, A03: Injection.
- **Top 10 dla API (2023):** API1: Broken Object Level Authorization, API2: Broken Authentication, API3: Broken Object Property Level Authorization.
- **Top 10 dla Aplikacji LLM:** LLM01: Prompt Injection, LLM02: Insecure Output Handling, LLM03: Training Data Poisoning.**Ustawodawstwo w Polsce:** Polski Kodeks karny zawiera przepisy penalizujące cyberprzestępczość:
- **Art. 267:** Bezprawne uzyskanie dostępu do informacji lub systemu informatycznego (hacking).
- **Art. 268 i 268a:** Niszczenie, uszkadzanie lub zmienianie danych informatycznych.
- **Art. 269a:** Zakłócanie pracy systemu informatycznego (np. ataki DDoS).
- **Art. 269b:** Wytwarzanie i udostępnianie narzędzi przeznaczonych do popełniania cyberprzestępstw (np. malware, narzędzia hakerskie).

- **Art. 269c:** Wprowadza **kontratyp** dla badaczy bezpieczeństwa, którzy działają w celu zabezpieczenia systemu, niezwłocznie powiadomili o zagrożeniu i nie wyrządzili szkody.

2. Fundamenty Kryptografii

Kryptografia to nauka o technikach bezpiecznej komunikacji w obecności potencjalnych przeciwników. Jest to dziedzina interdyscyplinarna, łącząca matematykę, informatykę, elektrotechnikę i fizykę. Jej głównym celem jest zapewnienie poufności, integralności, dostępności, uwierzytelniania i niezaprzeczalności.

2.1. Podstawowe Zasady i Pojęcia

- **Zasada Kerckhoffsa:** Bezpieczeństwo systemu kryptograficznego powinno zależeć wyłącznie od tajności klucza, a nie od tajności algorytmu.
- **Zasada otwartego projektu:** Algorytmy kryptograficzne powinny być publicznie znane i poddawane analizie przez ekspertów, co zwiększa zaufanie do ich bezpieczeństwa.
- **Klucz kryptograficzny:** Tajna informacja używana do szyfrowania i deszyfrowania. Jego długość (liczba bitów) determinuje odporność na ataki siłowe (brute-force).
- **Kryptografia vs Kryptoanaliza:** Kryptografia zajmuje się projektowaniem systemów, a kryptoanaliza ich łamaniem. Postęp w kryptoanalizie napędza rozwój silniejszych systemów kryptograficznych (np. ewolucja od DES, przez 3DES, do AES).

2.2. Kryptografia Symetryczna vs Asymetryczna

Cecha,Kryptografia Symetryczna,Kryptografia Asymetryczna (z kluczem publicznym)
Klucze,"Jeden, ten sam klucz do szyfrowania i deszyfrowania.",Para kluczy: publiczny (do szyfrowania/weryfikacji) i prywatny (do deszyfrowania/podpisywania).
Problem dystrybucji,Wymaga bezpiecznego kanału do wymiany klucza.,Rozwiązuje problem dystrybucji – klucz publiczny może być jawny.
Wydajność,"Bardzo szybka, idealna do szyfrowania dużych ilości danych.","Znacznie wolniejsza, używana do szyfrowania małych ilości danych (np. kluczy symetrycznych) i podpisów."
Przykłady,"AES, 3DES, Szyfr Vernama","RSA, ECC, Schemat Diffie-Hellmana (do uzgadniania kluczy)"
Główne zastosowanie,Szyfrowanie danych w spoczynku i w transmisji.,"Podpisy cyfrowe, bezpieczna wymiana kluczy symetrycznych (np. w TLS)."

2.3. Kluczowe Algorytmy i Mechanizmy

- **AES (Advanced Encryption Standard):** Najpopularniejszy algorytm symetryczny. Jest szyfrem blokowym działającym na 128-bitowych blokach danych z kluczami o długości 128, 192 lub 256 bitów. Jego bezpieczeństwo opiera się na zasadach **dyfuzji** (rozproszenie wpływu jednego bitu tekstu jawnego na wiele bitów szyfrogramu) i **konfuzji** (skomplikowanie relacji między kluczem a szyfrogramem). AES może działać w różnych trybach, np. **ECB** (niezalecany, nie ukrywa wzorców) i **CBC** (bezpieczniejszy, używa wektora inicjującego).

- **Szyfr Vernama (One-Time Pad):** Jedyny system kryptograficzny zapewniający **bezpieczeństwo absolutne** . Wymaga użycia klucza, który jest w pełni losowy, tak długi jak wiadomość i użyty tylko jeden raz.
- **Funkcje Skrótu (Hash Functions):** Funkcje takie jak SHA-256 i SHA-3 przekształcają dane dowolnej długości w skrót o stałej długości. Są jednokierunkowe i odporne na kolizje. Używa się ich do weryfikacji integralności danych, przechowywania haseł i w podpisach cyfrowych.

2.4. Kryptografia w Kontekście Współczesnych Zagrożeń

- **Ochrona przed ransomware:** Silne szyfrowanie kopii zapasowych uniemożliwia ich zaszyfrowanie przez atakujących.
- **Prywatność:** Szyfrowanie end-to-end chroni komunikację przed masową inwigilacją.
- **Chmura i IoT:** Szyfrowanie danych w spoczynku i w tranzycie jest kluczowe dla bezpieczeństwa w środowiskach rozproszonych.
- **Zagrożenia kwantowe:** Komputery kwantowe w przyszłości mogą złamać obecne algorytmy asymetryczne (RSA, ECC). W odpowiedzi rozwijana jest **kryptografia post-kwantowa (PQC)** – algorytmy odporne na ataki kwantowe.

3. Zarządzanie Kluczami Kryptograficznymi

*„Kryptografia bez odpowiedniego zarządzania kluczami jest jak pancerz ze stalowych drzwi, do których klucz leży pod wycieraczką”.*Prawidłowe zarządzanie kluczami jest równie ważne, co siła samych algorytmów. Najczęstsze błędy prowadzące do kompromitacji to słabe generowanie, niezabezpieczone przechowywanie (np. w kodzie źródłowym) i brak regularnej rotacji.

3.1. Cykl Życia Klucza Kryptograficznego

Zarządzanie kluczami obejmuje 7 faz:

1. **Generowanie:** Tworzenie kluczy przy użyciu kryptograficznie bezpiecznych generatorów liczb pseudolosowych (CSPRNG) i wystarczającej ilości entropii.
2. **Dystrybucja:** Bezpieczne przekazanie kluczy, np. za pomocą kryptografii asymetrycznej (schemat Diffie-Hellmana) lub z użyciem **Funkcji Wyprowadzania Kluczy (KDF)** .
3. **Przechowywanie:** Ochrona kluczy przed nieautoryzowanym dostępem.| Poziom Bezpieczeństwa | Metoda | Wady || ------ | ------ | ------ || **Poziom 0 (Nigdy!)** | Hardkodowanie w kodzie źródłowym | Klucz w repozytorium, trudna rotacja || **Poziom 1 (Niezalecane)** | Zmienne środowiskowe | Widoczne w procesach, mogą trafić do logów || **Poziom 2** | Pliki konfiguracyjne z uprawnieniami | Nadal plaintext na dysku, podatne na eskalację uprawnień || **Poziom 3** | Systemy zarządzania sekretami (np. HashiCorp Vault, AWS/Azure/Google KMS) | Centralne zarządzanie, szyfrowanie, audyt || **Poziom 4 (Najwyższy)** | **Hardware Security Modules (HSM)** | Dedykowany sprzęt, klucz nigdy go nie opuszcza, certyfikacja FIPS 140-3 |
4. **Użycie:** Stosowanie zasady rozdziału obowiązków (różne klucze do różnych celów) i **Key Wrapping** (szyfrowanie kluczy do danych - DEK, za pomocą kluczy do szyfrowania kluczy - KEK).
5. **Rotacja:** Regularna wymiana kluczy (np. co 1-2 lata dla AES) w celu ograniczenia skutków ewentualnej kompromitacji.

6. **Archiwizacja:** Długoterminowe, bezpieczne przechowywanie nieaktywnych kluczy w celu odzyskania archiwalnych danych.
7. **Niszczenie:** Bezpieczne i nieodwracalne usunięcie klucza, gdy nie jest już potrzebny. Zwykłe usunięcie pliku jest niewystarczające. Dla dysków SSD zalecane jest **kryptograficzne wymazywanie** (zniszczenie klucza szyfrującego dysk).

3.2. Funkcje Wyprowadzania Kluczy (KDF) i Haszowanie Haseł

- **Password Hashing (np. bcrypt, Argon2):** Służy do bezpiecznego przechowywania haseł. Funkcje te są celowo powolne i wymagają dużo zasobów (CPU, pamięć), aby utrudnić ataki brute-force. Wynik zawiera wbudowaną sól i jest niedeterministyczny.
- **Key Derivation Functions (KDF):** Służą do generowania kluczy kryptograficznych.
- **Password-based KDF (np. PBKDF2, scrypt, Argon2):** Przekształcają hasło o niskiej entropii w silny klucz kryptograficzny.
- **Key-based KDF (np. HKDF):** Przekształcają materiał o wysokiej entropii (np. wynik wymiany Diffie-Hellmana) w jeden lub więcej kluczy kryptograficznych.

4. Analiza Podatności Aplikacji Webowych

Testowanie bezpieczeństwa i symulowanie ataków na systemy produkcyjne bez zgody właściciela jest nielegalne i podlega karze zgodnie z polskim Kodeksem karnym (art. 267-269c).

4.1. Cross-Site Scripting (XSS)

- **Definicja:** Podatność polegająca na wstrzyknięciu złośliwego kodu (zwykle JavaScript) do strony internetowej, który jest następnie wykonywany w przeglądarce ofiary. Atak ten omija fundamentalny mechanizm bezpieczeństwa przeglądarek – **Same-Origin Policy (SOP)** , ponieważ złośliwy skrypt wykonuje się w kontekście zaufanej domeny.
- **Rodzaje XSS:**
- **Stored (Trwały):** Złośliwy kod jest trwale zapisywany na serwerze (np. w bazie danych) i serwowany każdemu użytkownikowi, który wyświetla zainfekowaną treść.
- **Reflected (Odbity):** Złośliwy kod jest częścią żądania (np. linku) i jest "odbijany" przez serwer w odpowiedzi, wykonując się jednorazowo w przeglądarce ofiary.
- **DOM-based:** Atak odbywa się w całości po stronie klienta; skrypt na stronie pobiera dane z kontrolowanego przez atakującego źródła (np. fragmentu URL) i niebezpiecznie wstawia je do struktury DOM.
- **Ochrona:**
- **Kodowanie wyjścia:** Traktowanie wszystkich danych pochodzących od użytkownika jako niezaufanych i kodowanie ich odpowiednio do kontekstu (HTML, JS, CSS).
- **Content Security Policy (CSP):** Nagłówek HTTP, który pozwala zdefiniować, z jakich źródeł mogą być ładowane zasoby (np. skrypty), blokując wykonanie nieautoryzowanego kodu.
- **Walidacja i sanityzacja danych wejściowych:** Odrzucanie lub oczyszczanie danych, które nie pasują do oczekiwanego formatu.
- **Używanie bezpiecznych metod manipulacji DOM** (np. element.textContent zamiast element.innerHTML).

4.2. SQL Injection (SQLi)

- **Definicja:** Technika ataku polegająca na wstrzyknięciu fragmentów kodu SQL do zapytań wysyłanych do bazy danych. Wynika z nieprawidłowego łączenia danych od użytkownika z zapytaniem SQL (konkatenacja stringów). Atakujący jest w stanie "przeskoczyć" z płaszczyzny danych do płaszczyzny logiki sterowania zapytaniem.
- **Rodzaje SQLi:**
- **UNION-based:** Wykorzystanie operatora UNION do dołączenia wyników złośliwego zapytania do wyników legalnego zapytania.
- **Error-based:** Celowe wywoływanie błędów bazy danych, aby w ich treści uzyskać poufne informacje (np. wersję bazy, nazwy tabel).
- **Blind SQL Injection:** Stosowany, gdy aplikacja nie zwraca błędów ani wyników. Atakujący wnioskuje o danych na podstawie:
- **Treści (Boolean-based):** Sprawdzanie, czy strona zachowuje się inaczej w zależności od tego, czy wstrzyknięty warunek jest prawdziwy czy fałszywy.
- **Czasu (Time-based):** Wprowadzanie opóźnień w odpowiedzi serwera (np. za pomocą funkcji SLEEP()), jeśli warunek jest prawdziwy.
- **Ochrona:**
- **Zapytania sparametryzowane (Prepared Statements):** Najskuteczniejsza metoda obrony. Zapytanie i dane są wysyłane do bazy oddzielnie, co uniemożliwia potraktowanie danych jako kodu.
- **Systemy ORM (Object-Relational Mapping):** Abstrakcja dostępu do bazy danych, która często domyślnie używa zapytań sparametryzowanych.
- **Walidacja typów danych i list dozwolonych wartości.**
- **Hardening bazy danych:** Stosowanie zasady najmniejszych uprawnień dla użytkownika bazy danych, wyłączanie niebezpiecznych procedur (np. xp_cmdshell).

4.3. Cross-Site Request Forgery (CSRF)

- **Definicja:** Atak, który zmusza zalogowanego użytkownika do wykonania niepożądanej akcji w aplikacji webowej. Wykorzystuje fakt, że przeglądarka automatycznie dołącza pliki cookie (w tym sesyjne) do każdego żądania do danej domeny, niezależnie od tego, skąd żądanie zostało zainicjowane.
- **Mechanizm:** Ofiara, będąc zalogowana w docelowej aplikacji (np. banku), odwiedza złośliwą stronę. Strona ta w tle (np. za pomocą ukrytego formularza lub skryptu) wysyła żądanie do aplikacji bankowej (np. wykonania przelewu). Przeglądarka dołącza cookie sesyjne, a aplikacja traktuje żądanie jako autentyczne.
- **Ochrona:**
- **Tokeny Anty-CSRF:** Unikalny, losowy token generowany dla każdej sesji użytkownika, umieszczany w ukrytym polu formularza. Serwer weryfikuje jego poprawność przed wykonaniem akcji.
- **Atrybut SameSite dla plików cookie:**
- SameSite=Strict: Blokuje wysyłanie cookie przy żądaniach z innych domen.
- SameSite=Lax: Zapewnia dobrą ochronę, zezwalając na wysłanie cookie tylko przy nawigacji najwyższego poziomu metodą GET.
- **Weryfikacja nagłówków Origin lub Referer :** Sprawdzanie, czy żądanie pochodzi z zaufanej domeny.
- **Ponowne uwierzytelnienie:** Wymaganie od użytkownika ponownego podania hasła przed wykonaniem krytycznych operacji.