Kryptografia i bezpieczeństwo danych - bezpieczeństwo informacji najważniejsze obszary

Sławomir Samolej
ssamolej.kia.prz.edu.pl
ssamolej@prz.edu.pl

Przegląd najważniejszych obszarów

- Identyfikowanie i uwierzytelnianie
- Autoryzacja i kontrola dostępu
- Audytowanie i rozliczalność
- Kryptografia
- Zgodność, prawo i przepisy
- Bezpieczeństwo operacyjne
- Bezpieczeństwo czynniki ludzkiego
- Bezpieczeństwo fizyczne
- Bezpieczeństwo sieciowe
- Bezpieczeństwo systemu operacyjnego
- Bezpieczeństwo urządzeń mobilnych
- Bezpieczeństwo aplikacji

Identyfikacja i uwierzytelnienie

- **Identyfikacja** – pozwala stwierdzić, czym jest ktoś lub coś
- **Uwierzytelnienie** – pozwala stwierdzić, czy to stwierdzenie jest prawdziwe
- Przykład
  - Zbliżenie karty oznacza, że jesteś osobą wskazaną na karcie
  - Podanie PIN udowadnia, że jesteś prawidłowym posiadaczem karty

Identyfikacja

- Podanie tożsamości – za kogo się podajemy

- Weryfikacja tożsamości to nie uwierzytelnienie
  - Ktoś ogląda dowód, paszport i może na tej podstawie stwierdzić, że rzeczywiście to jest osoba o określonym imieniu, nazwisku i wyglądzie
- Tożsamość można łatwo sfałszować

Uwierzytelnienie

- To zbiór metod używanych do ustalenia, czy dane twierdzenie o tożsamości jest prawdziwe
- Nie należy go mylić z autoryzacją. Uwierzytelnienie mówi kim ktoś jest, autoryzacja – co ktoś może zrobić.

Składniki uwierzytelnienia

- Coś, co znasz – hasło, PIN (niepewne, jeśli zostaną ujawnione, to metoda traci wiarygodność)
- Coś, czym jesteś (biometria)
- Coś, co posiadasz (karty, tokeny, telefony)
- Coś, co robisz (jak chodzisz, jak uderzasz w klawiaturę – duży procent odrzuceń?)
- To, gdzie jesteś (zmiany PIN po zablokowaniu musisz dokonać w siedzibie banku, po potwierdzeniu twojej tożsamości)

- Do uwierzytelnienia będziemy się starać zastosować jak najwięcej z tych składników.

Autoryzacja i kontrola dostępu

- Po identyfikacji i uwierzytelnieniu można zdecydować, do czego dana osoba ma dostęp
  - Autoryzacja = określenie, co może dana osoba robić z naszym systemem i danymi
  - Kontrola dostępu = narzędzie do przydzielania dostępu

Czym są mechanizmy kontroli dostępu?

- Przyznawanie dostępu
  - Udzielenie osobie lub aplikacji możliwości korzystania z zasobów
- Odmawianie dostępu
  - Zabronienie osobie lub aplikacji możliwości korzystania z zasobów
- Ograniczenie dostępu
  - Określenie zbioru zasobów dostępnych (np. sandboxing)
- Cofnięcie dostępu
  - Zablokowanie osobie, aplikacji możliwości korzystania z zasobów np. z powodu zwolnienia itp.

Wdrażanie kontroli dostępu

- Listy ACL (Access Control List)
  - Na poziomie plików
  - Na poziomie sieciowym
    - MAC, IP, port
    - Atak „problem zdezorientowanego zastępcy”: użytkownik dysponuje programem posiadającym większe uprawnienia niż on i „przekonuje” program do skorzystania z tych „rozszerzonych” uprawnień.
  - Tokeny dostępu

Fizyczna kontrola dostępu

- Wchodzenie „na ogonie”
- Dobra praktyka – procedura wchodzenia na lotnisko i na pokład samolotu

Audytowanie i rozliczalność

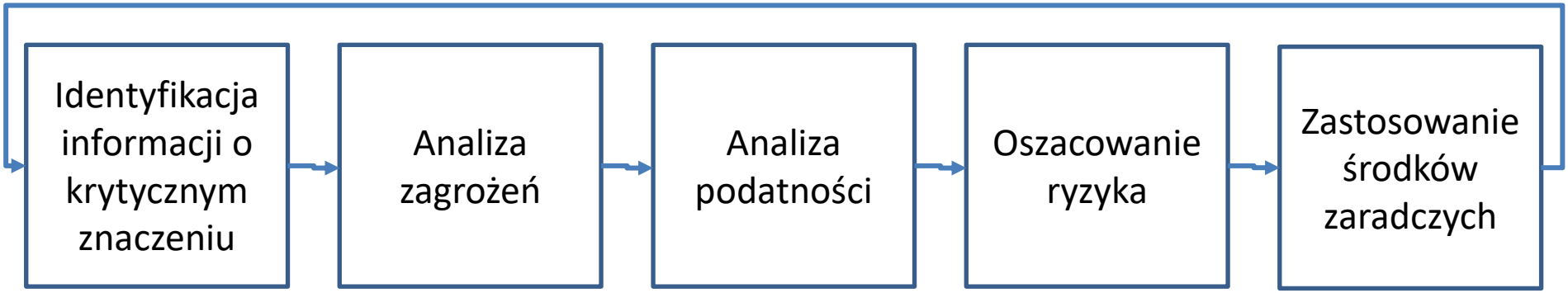
- Audytowanie
  - sprawdzanie, jak użytkownicy zachowują się po uzyskaniu dostępu do danych
  - testy penetracyjne – wykrywanie podatności
- Rozliczalność – prowadzenie „dzienników” korzystania użytkowników z zasobów
  - Uruchomienie i pielęgnacja dzienników systemowych
    - Niezaprzeczalność (ktoś nie będzie mógł zaprzeczyć, że coś robił, jeśli będzie na to dowód)
    - Efekt odstraszania (użytkownicy świadomi, że są rozliczani będą mniej skłonni do wykroczeń)
    - Na podstawie logów można wdrożyć system alarmów i zapobiec incydentom lub je ograniczyć
    - Logi muszą być gromadzone i zabezpieczone zgodnie z wymogami formalno-prawnymi, wtedy można je wykorzystać jako materiał dowodowy

Kryptografia

- Ochrona danych w spoczynku
  - Zaszyfrowanie
- Ochrona danych w ruchu
  - Szyfrowanie
  - VPN
- Ochrona danych w użyciu
  - Są osoby, które mogą korzystać z danych i je ujawnić (Edward Snowden)

Bezpieczeństwo operacyjne

- wdrażanie mechanizmów bezpieczeństwa
- identyfikacja, przed czym się bronić



Bezpieczeństwo czynnika ludzkiego

- Człowiek to „najsłabsze ogniwo” w systemie zabezpieczeń
  - Możliwe jest przeprowadzenie na nim ataków socjotechnicznych
  - Ataki można **przygotować**:
    - Śledzenie celu
    - Biały wywiad
    - Życiorysy i oferty pracy
    - Media społecznościowe
    - Google Hacking https://www.exploit-db.com/google-hacking-database
    - Metadane plików (https://www.opentext.com/products/encase-forensic)
    - Shodan (https://www.shodan.io/) – wyszukiwanie urządzeń i systemów podłączonych do Internetu
    - Maltego (https://www.maltego.com) – wyszukiwanie relacji pomiędzy poszczególnymi punktami danych

Rodzaje ataków socjotechnicznych

- Atak pretekstowy (wcielenie się w rolę, wiarygodny scenariusz)
- Phishing (zebranie danych lub zainstalowanie złośliwego oprogramowania)
- Tailgating (wchodzenie na ogonie)

Budowanie świadomości użytkowników 1/2

- Zasady tworzenia i przechowywania haseł
- Szkolenia z zakresu inżynierii behawioralnej
- Szkolenia z korzystania z sieci
  - Publiczne sieci bezprzewodowe
  - Zasady podłączania urządzeń do sieci firmowej
  - VPN
- Złośliwe oprogramowanie
  - Załączniki do email od nieznanych nadawców
  - Załączniki do email potencjalnie wykonywalne
  - Skrócone łącza internetowe (weryfikować: https://linkexpander.com)
  - Łącza internetowe o nieznacznie różniących się nazwach
  - Aplikacje na smartfony do pobrania spoza oficjalnych sklepów
  - Pirackie oprogramowanie

Budowanie świadomości użytkowników 2/2

- Prywatny sprzęt komputerowy
  - Co do zasady żadne prywatnie urządzenie nie powinno być podłączone do sieci firmy
- Polityka czystego biurka
  - Żadne wrażliwe dane nie powinny być pozostawione „na biurku” jeśli opuszczamy miejsce pracy
  - Należy opracować sposób pozbywania się wrażliwych danych (niszczarki papieru i sprzętu)
- Jeśli jesteś osobą odpowiedzialną za bezpieczeństwo, to prowadź szkolenia i dostarcz z nich materiały. Mało prawdopodobne, że ktoś z własnej woli przeczyta przygotowany przez Ciebie materiał tekstowy i od razu zacznie stosować politykę bezpieczeństwa.

Bezpieczeństwo fizyczne

- Ochrona ludzi
- Ochrona danych

Identyfikacja zagrożeń fizycznych

- Kategorie zagrożeń fizycznych
  - Wibracje i przemieszczenia
  - Ogień i dym
  - Toksyny
  - Ludzie
  - Przerwy w dostawach energii
  - Ekstremalne temperatury
  - Gazy
  - Płyny
  - Organizmy żywe
  - Pociski

Ochrona danych

- Fizyczne zagrożenie dla danych
  - Nośniki magnetyczne
    - Zniszczenie może spowodować: silne pole magnetyczne lub drgania
  - Nośniki flash
    - Zniszczenie może spowodować: zgniecenie, impulsy i przepięcia elektryczne
  - Nośniki optyczne
    - Zniszczenie może spowodować: zadrapanie, temperatura
- Dostępność danych
  - Kopie zapasowe
  - RAID (Redundant Arrays of Independent Disks)
  - Replikacja danych
- Szczątkowe pozostałości danych
- Ochrona wyposażenia
  - Fizyczne zagrożenie dla sprzętu (temperatury, ciecze, org. żywe, wibracje, dym i ogień
  - Wybór lokalizacji
  - Zabezpieczenia dostępu (zamki, ogrodzenia, strażnicy)

Bezpieczeństwo sieciowe

Ochrona sieci

- Projektowanie bezpiecznych sieci
  - Segmentacja (podział na podsieci i kontrola ruchu pomiędzy nimi)
  - Tworzenie nadmiarowości
- Zastosowanie zapór sieciowych
  - Filtrowanie pakietów
  - Pełnostanowa inspekcja pakietów (obserwacja ruchu w ramach danego połączenia)
  - Głęboka inspekcja pakietów (odczytywanie pakietów, przed przekazaniem dalej)
  - Strefa zdemilitaryzowana (kilka poziomów zapór sieciowych)
  - Sieciowe systemy wykrywania włamań

Ochrona ruchu sieciowego

- VPN (virtual private network)
  - Zdalny dostęp do wewnętrznych zasobów organizacji
  - Ochrona lub anonimizacja ruchu przesyłanego przez niezaufane połączenie (odłączenie dostawcy od śledzenia naszego ruchu)
- Sieci bezprzewodowe
  - Publiczne sieci bezprzewodowe (brak szyfrowania, brak haseł)
  - Wrogie punkty dostępu
- Dobór bezpiecznych protokołów komunikacyjnych
  - ftp -> SFTP
  - telnet -> SSH
- Narzędzia do ochrony sieci
  - Skanery (np. nmap)
  - Sniffery (np. wireshark)

Bezpieczeństwo systemu operacyjnego

- Utwardzanie SO
  - Usuwanie niepotrzebnego oprogramowania
  - Usuwanie niepotrzebnych usług
  - Modyfikacja domyślnych kont użytkowników
  - Zastosowanie reguły najmniejszych uprawnień
  - Aktualizacja
  - Implementacja logowania i audytowania
- Ochrona przed złośliwym oprogramowaniem
  - Antywirusy
  - Ochrona przestrzeni wykonywalnej
  - Programowe zapory sieciowe i wykrywania włamań
  - Skanery
  - Narzędzia do wykrywania podatności i luk

Bezpieczeństwo aplikacji

Luki w zabezpieczeniach oprogramowania

- Przepełnienie bufora (wprowadzenie na wejście większej liczby danych, niż przewidział autor oprogramowania -> nadpisanie pamięci własnej lub innych aplikacji)
- Warunki wyścigu (systemy współbieżne – dwa programy równocześnie modyfikują te same dane -> niespójność danych)
- Ataki na weryfikację danych wejściowych (nieprawidłowe dane)
- Ataki uwierzytelniające (uwierzytelnienie powinno się znaleźć po stronie serwera, a nie klienta, bo wtedy jest łatwiejsze do sfałszowania)
- Ataki autoryzacyjne (przejęcie zasobów, do których nie ma się uprawnień)
- Ataki kryptograficzne

Bezpieczeństwo sieci WEB

- Ataki po stronie klienta:
  - XXS (cross-site scripting) – umieszczenie dodatkowych skryptów na stronie, którą otwiera klient
  - CSRF (cross-site request forgery) – umieszcznie na stronie odsyłaczy do innych, które wykonają się automatycznie (my pracujemy na jednej zakładce, a na drugiej, gdzie też jesteśmy zalogowani, ktoś robi za nas zakupy za nasze pieniądze)
- Ataki po stronie serwera:
  - Brak weryfikacji danych po stronie serwera -> directory traversal
  - Przypisanie niewłaściwych uprawnień użytkownikom -> możliwość przejęcia wrażliwych danych
  - Zbędne pliki (po deweloperce)

Bezpieczeństwo baz danych

- Problemy z protokołami (połączenie z bazą przez sieć może mieć luki)
- Dostęp do funkcjonalności bez uwierzytelnienia (użytkownik nie jest uwierzytelniany i dostaje duże przywileje)
- Arbitralne wykonanie kodu (specyfika SQL)
- Eskalacja uprawnień (wstrzykiwanie kodu)