OCHRONA INFORMACJI W SYSTEMACH INFORMATYCZNO-KOMUNIKACYJNYCH

Wykonał:
Roman Borysenko
173596
2-EFDI

ZAGROŻENIA DLA INFORMACJI

Ataki cybernetyczne stanowią poważne zagrożenie dla dzisiejszych systemów informatyczno-komunikacyjnych. Definiujemy je jako złośliwe działania lub przestępstwa komputerowe, których celem jest naruszenie bezpieczeństwa danych i infrastruktury informatycznej. Istnieje wiele różnych rodzajów ataków cybernetycznych, w tym ataki DDoS, ataki wstrzykiwania SQL, ataki typu zero-day, phishing, ransomware i wiele innych.

SPOSOBY OBRONY PRZED ATAKAMI CYBERNETYCZNYMI:

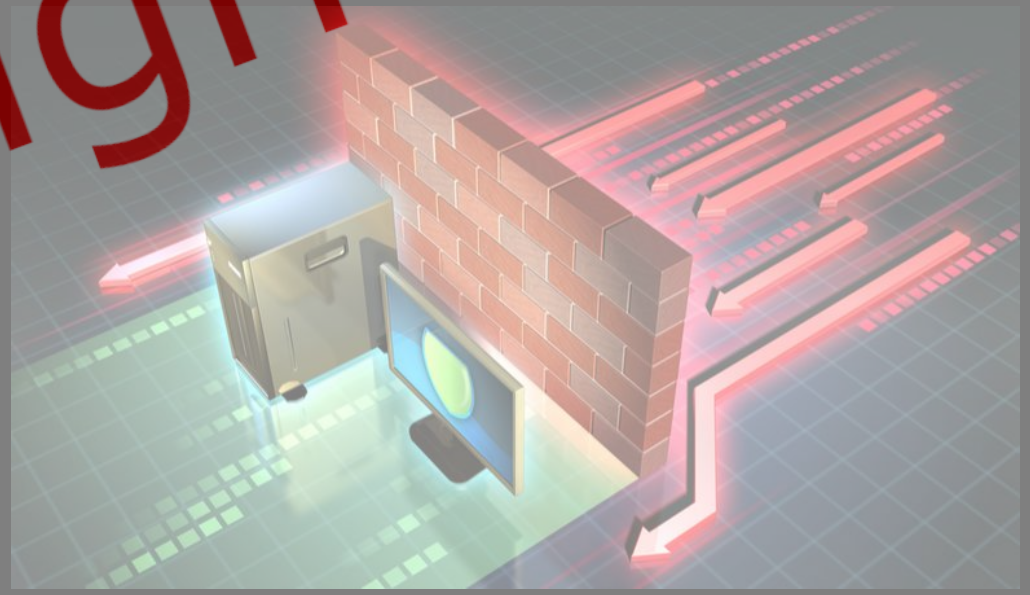
1. Firewall
2. **Antywirus**
3. **Szyfrowanie danych**
4. **Zarządzanie tożsamością i dostępem(IAM)**
5. **Sandboxing**
6. **Segmentacja sieci**
7. **Wielowarstwowe zabezpieczenia**

FIREWALL

Firewall to podstawowy element obrony sieci komputerowej. Jest to system filtrujący ruch sieciowy na podstawie określonych zasad. Firewall może blokować nieautoryzowany dostęp i ruch z podejrzanych źródeł.

Główne funkcje firewalla obejmują:

Filtrację ruchu, Kontrolę dostępu, Monitorowanie ruchu, Blokowanie niebezpiecznych treści, Logowanie zdarzeń



ANTYWIRUS

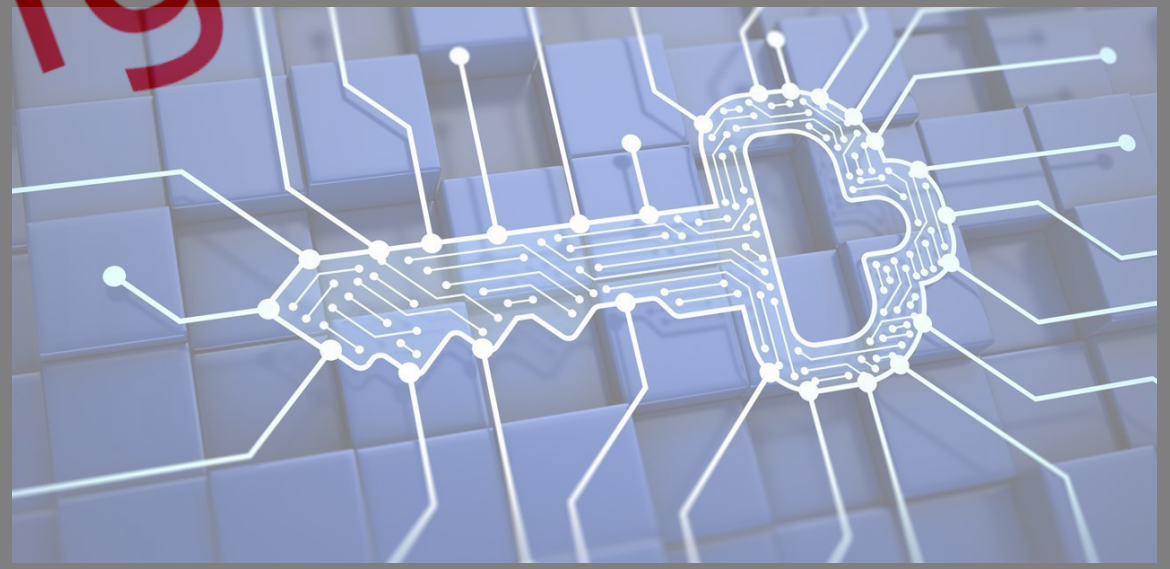
kluczowy element obrony przed złośliwym oprogramowaniem (malware), takim jak wirusy, trojany, ransomware i inne zagrożenia cybernetyczne. Działa on na zasadzie skanowania systemu lub urządzenia w poszukiwaniu potencjalnych zagrożeń i podejrzanych plików.

Główne funkcje firewalla obejmują:

Skanowanie systemu, Baza sygnatur, Heurystyka, Ochrona w czasie rzeczywistym, Aktualizacje definicji

SZYFROWANIE DANYCH

Szyfrowanie danych to kluczowa technika używana do ochrony poufnych informacji przed nieautoryzowanym dostępem. Polega na przekształceniu danych w sposób, który sprawia, że są one nieczytelne dla osób bez odpowiedniego klucza deszyfrującego.



Główne aspekty związane z szyfrowaniem danych:

Rodzaje szyfrowania, Klucze szyfrowania, Szyfrowanie w spoczynku i w trakcie transmisji, Protokoły i algorytmy szyfrowania.

IAM

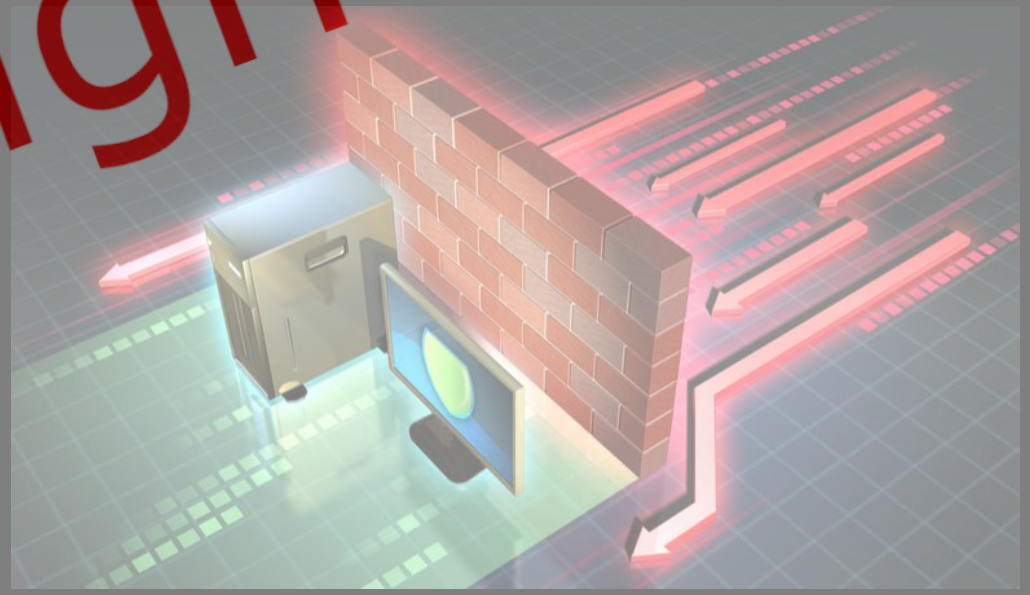
IAM to kompleksowy zestaw zasad, procesów i technologii, które pozwalają na skuteczne zarządzanie tożsamościami użytkowników oraz ich dostępem do zasobów i systemów w organizacji. Jest to kluczowy element zapewnienia bezpieczeństwa oraz ochrony poufnych informacji.

Główne aspekty związane z IAM:

Autentykacja tożsamości, Uprawnienia i kontrole dostępu, Zarządzanie hasłami, Polityka bezpieczeństwa i zgodność

SANDBOXING

Polega na izolowaniu i testowaniu podejrzanych plików lub aplikacji w odseparowanym i kontrolowanym środowisku, zwanych "piaskownicą" (sandbox). Głównym celem jest zapewnienie bezpieczeństwa systemu przed potencjalnie złośliwym oprogramowaniem.

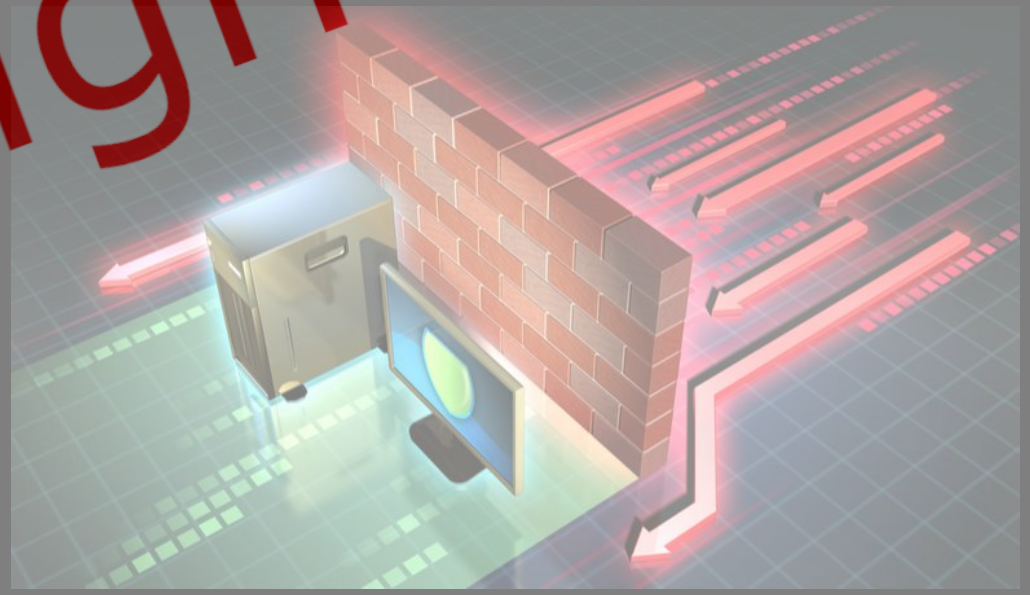


Główne aspekty związane z sandboxingiem:

Izolacja od reszty systemu, Monitorowanie zachowania, Testy i analiza, Bezpieczne środowisko testowe, Zautomatyzowane analizy

SEGMENTACJA SIECI

Jest to praktyka podziału jednej dużej sieci komputerowej na mniejsze, odseparowane od siebie segmenty lub podsieci. Celem segmentacji jest zwiększenie bezpieczeństwa, poprawa zarządzania i ograniczenie rozprzestrzeniania się ewentualnych ataków wewnątrz sieci.



Oto główne aspekty związane z segmentacją sieci:

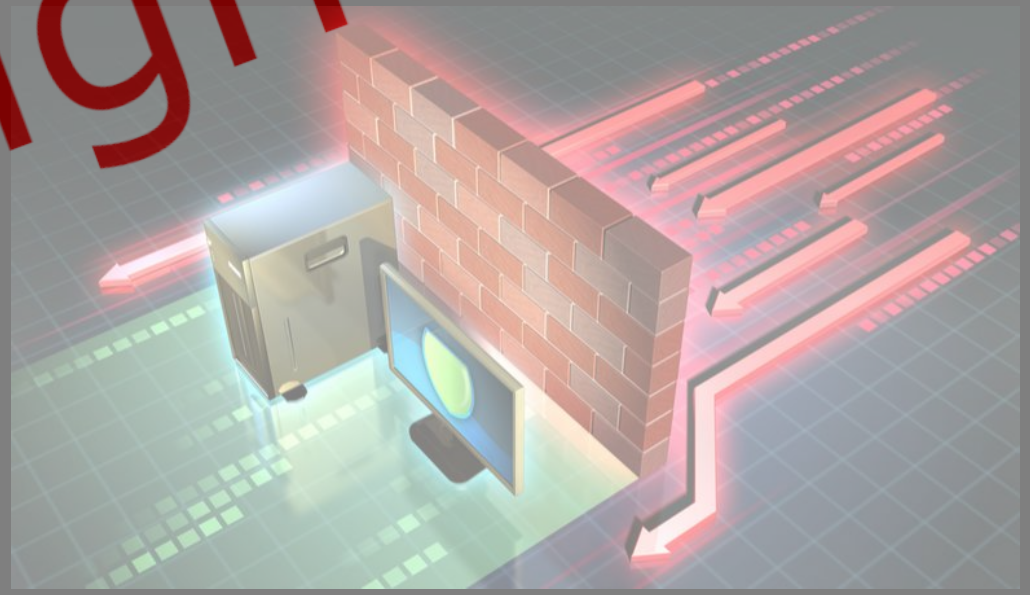
Podział na podsieci, Izolacja ruchu, Zarządzanie dostępem, Izolacja problemów, Zastosowanie wirtualizacji(segmentacja sieci na poziomie oprogramowania)

WIELOWARSTWOWE ZABEZPIECZENIA

Ta strategia zakłada, że żadna pojedyncza warstwa zabezpieczeń nie jest wystarczająca, dlatego stosuje się kilka warstw ochrony, które działać mogą niezależnie od siebie.

Główne aspekty związane z wielowarstwowymi zabezpieczeniami:

Zasada ograniczonej ekspozycji, Regularne aktualizacje, Wsparcie dla edukacji, Elastyczność i skalowalność



WNIOSKI

1. **Zarządzanie Informacją w Systemach Informatyczno-Komunikacyjnych:**

   1)Ochrona informacji w systemach informatyczno-komunikacyjnych to kluczowy element w zapewnieniu bezpieczeństwa danych i zasobów organizacji.

   2)Wdrożenie skutecznych środków ochrony, takich jak antywirusy, firewall, oraz szyfrowanie danych, jest niezbędne w walce z zagrożeniami.

2. **Zagrożenia dla Informacji:**

   1)Zrozumienie różnorodnych zagrożeń, takich jak ataki cybernetyczne, malware, phishing czy ransomware, jest kluczowe w opracowaniu odpowiednich strategii obronnych.

   2)Świadomość bezpieczeństwa informacji jest istotna dla pracowników, aby uniknąć przypadkowych naruszeń.

3. **Ataki Cybernetyczne:**

   1)Ataki cybernetyczne stanowią realne ryzyko dla organizacji i mogą powodować poważne konsekwencje, w tym utratę danych, straty finansowe i utratę reputacji.

   2)Stosowanie wielowarstwowych zabezpieczeń, takich jak firewall, antywirusy i monitorowanie ruchu, pomaga w zapobieganiu atakom i szybkiej reakcji na nie.

4. **Szyfrowanie Danych:**

   1)Szyfrowanie danych jest nieodłącznym elementem ochrony informacji w systemach informatyczno-komunikacyjnych.

   2)Poprawnie wdrożone szyfrowanie zapewnia poufność danych, nawet w przypadku ich utraty lub nieautoryzowanego dostępu.

WNIOSKI

5. Zarządzanie Tożsamością i Dostępem (IAM):

1)Zarządzanie tożsamością i dostępem jest kluczowym aspektem w kontrolowaniu dostępu do zasobów i systemów.

2)Zapewnia precyzyjne zarządzanie uprawnieniami użytkowników i minimalizuje ryzyko dostępu nieautoryzowanego.

6. Sandboxing:

1)Sandboxing pozwala na izolację i testowanie podejrzanych aplikacji w bezpiecznym środowisku, co jest skutecznym środkiem w zwalczaniu złośliwego oprogramowania.

2)Pomaga w analizie zachowań podejrzanych plików lub aplikacji i zapobiega rozprzestrzenianiu się ataków.

7. Segmentacja Sieci:

1)Segmentacja sieci jest strategią, która pozwala na izolację i kontrolowanie dostępu między różnymi częściami sieci.

2)Ogranicza ryzyko rozprzestrzeniania się ataków wewnątrz sieci i zwiększa kontrolę nad ruchem sieciowym.

8. Wielowarstwowe Zabezpieczenia:

1)Wielowarstwowe zabezpieczenia to podejście, które stosuje wiele warstw ochrony w celu zapewnienia kompleksowego bezpieczeństwa.

2)Skuteczna strategia obronna obejmuje zarówno zabezpieczenia techniczne, jak i procedury oraz edukację pracowników.

WNIOSKI

Skuteczne zarządzanie ryzykiem cybernetycznym i ochrona informacji w dzisiejszym środowisku informatycznym stają się coraz bardziej złożone i wymagają wielowarstwowych zabezpieczeń. Różnorodność zagrożeń, od zaawansowanych ataków cybernetycznych po przypadkowe naruszenia bezpieczeństwa, wymaga podejścia opartego na wielu warstwach ochrony.

Wielowarstwowe zabezpieczenia pozwalają na minimalizację ryzyka i zapewniają możliwość szybkiej reakcji na zmieniające się zagrożenia. Poprzez zastosowanie kilku warstw ochrony, organizacje zwiększają swoje szanse na wykrycie i zneutralizowanie potencjalnych zagrożeń, co jest kluczowe dla zachowania ciągłości działalności i ochrony danych oraz zasobów.