Security: Spis pojęć

Pojęcia

Robak

Robak to złośliwe oprogramowanie, które ma zdolność do samodzielnego rozprzestrzeniania się poprzez sieci komputerowe. W odróżnieniu od wirusów, robaki nie wymagają interakcji użytkownika do skopiowania się na inne systemy. Mogą wykorzystywać luki w zabezpieczeniach, aby przenikać do nowych maszyn, często powodując poważne zakłócenia w działalności sieci.

SPAM

Spam to niechciane wiadomości elektroniczne, najczęściej masowo wysyłane, które mają na celu reklamowanie produktów lub usług. SPAM może także zawierać złośliwe oprogramowanie lub phishing, co zagraża bezpieczeństwu użytkowników. Próby zablokowania spamu w komunikacji e-mail i na platformach społecznościowych są standardem w branży bezpieczeństwa

Wirus komputerowy

Wirus komputerowy to rodzaj złośliwego oprogramowania, które wymaga interakcji użytkownika, aby zainfekować system. Wirusy przyczepiają się do innych programów lub plików i są aktywowane, gdy te pliki są uruchamiane. Mogą powodować różnorodne problemy, od uszkodzenia danych po kradzież informacji.

Koń trojański

Koń trojański to rodzaj złośliwego oprogramowania, które podszywa się pod legalny program, aby skłonić użytkownika do jego zainstalowania. Po zainstalowaniu, koń trojański może umożliwić atakującemu dostęp do systemu, kradzież danych lub inne szkodliwe działania. Ważne jest, aby być ostrożnym przy pobieraniu i instalowaniu oprogramowania, zwłaszcza z nieznanych źródeł.

Rootkit

Rootkit to złośliwe oprogramowanie, które umożliwia osobom nieuprawnionym uzyskanie oraz utrzymanie dostępu do systemu komputerowego bez wiedzy użytkownika. Nazwa „rootkit” pochodzi od słowa „root”, które odnosi się do konta administracyjnego w systemach UNIX, oraz „kit”, co oznacza zestaw narzędzi. Rootkity często zmieniają komponenty systemu operacyjnego, aby ukryć swoją obecność, co sprawia, że są wyjątkowo trudne do wykrycia. Główne cechy rootkitów:

- Cicha instalacja: Rootkity mogą być instalowane na systemie przez atakującego po uzyskaniu dostępu administracyjnego.

- Ukrywanie: Potrafią ukrywać swoją obecność oraz inne złośliwe oprogramowanie.
- Trudność w wykryciu: Używają technik, które mogą uniemożliwiać ich wykrycie przez oprogramowanie zabezpieczające, w tym zmieniając pliki systemowe.

Spyware

Spyware to rodzaj złośliwego oprogramowania, które przeszukuje i zbiera dane z komputera, często bez wiedzy użytkownika. Może rejestrować działania użytkownika, takie jak wprowadzone dane osobowe, historie przeglądania czy lokalizacje, a następnie przesyłać te informacje do zdalnego serwera. Główne cechy spyware:

- Zbieranie danych: Spyware gromadzi dane osobowe, a także może śledzić działania użytkownika w Internecie.
- Niekontrolowana aktywność: Spyware może zmieniać ustawienia przeglądarki, wprowadzać reklamy lub inne niechciane programy.
- Ukryty charakter: Działa w tle, niezauważenie dla użytkownika, co czyni go równie niebezpiecznym jak rootkit.

Rozszerzenia plików najczęściej zawierających wirusy

Największe ryzyko stwarzają pliki **.exe**, ponieważ są to aplikacje, które mogą bezpośrednio działać na systemie. Pliki .docx i .xlsx z makrami mogą być również niebezpieczne, zwłaszcza gdy użytkownicy nie są ostrożni. Pliki .pdf są najbezpieczniejsze, ale również mogą zawierać zagrożenia. Ważne jest, aby zawsze skanować pliki przed ich otwarciem, zwłaszcza jeśli pochodzą z nieznanych źródeł. Jeśli potrzebujesz dodatkowych informacji na temat zabezpieczeń przed wirusami, daj znać!

Rozszerzenie	Opis
.exe	Programy wykonywalne, które są najczęściej używane do rozprzestrzeniania wirusów. Po uruchomieniu mogą zainstalować złośliwe oprogramowanie na komputerze.
.pdf	Choć pliki PDF są zazwyczaj bezpieczne, mogą zawierać złośliwe skrypty i linki, które prowadzą do szkodliwego oprogramowania.
.docx	Pliki Microsoft Word mogą być wykorzystane do rozprzestrzeniania makr, które uruchamiają złośliwe oprogramowanie, zwłaszcza, gdy użytkownik zezwala na ich uruchomienie.
.xlsx	Pliki Excel również mogą zawierać makra, które mogą być wykorzystane do infekowania systemu złośliwym oprogramowaniem, jeśli są uruchamiane przez użytkowników.

Ataki spoofingowe w różnych warstwach

Warstwa	Typ ataku spoofingowego
1. Warstwa fizyczna	Spoofing fizyczny: podszywanie się pod sygnały sieciowe, by przejąć kontrolę lub zbierać dane.
2. Warstwa łącza danych	MAC Spoofing: zmiana adresu MAC urządzenia w celu ukrycia tożsamości lub podszywania się pod inne urządzenie w sieci lokalnej.
3. Warstwa sieciowa	IP Spoofing: podszywanie się pod adres IP innego urządzenia, co może umożliwić atak DDoS lub obejście zabezpieczeń.

Warstwa	Typ ataku spoofingowego
4. Warstwa transportowa	TCP Spoofing: manipulacja pakietami TCP w celu przejęcia sesji lub autoryzacji użytkownika.
5. Warstwa sesji	Session Hijacking: przejęcie aktywnej sesji użytkownika, co pozwala atakującemu na udawanie innego użytkownika.
6. Warstwa prezentacji	Słabe szyfrowanie lub brak zabezpieczeń powodują, że przesyłane dane mogą być manipulowane lub fałszowane.
7. Warstwa aplikacji	HTTP Spoofing: podszywanie się pod dalekozasięgowe serwery w celu wykonania ataku na aplikacje webowe.

Rodzaje algorytmów szyfrowania i funkcji skrótu

Algorytmy szyfrowania symetryczne

Algorytmy szyfrowania symetrycznego wykorzystują ten sam klucz do szyfrowania i deszyfrowania danych. Klucz musi być bezpiecznie przesyłany pomiędzy stronami.

Algorytm	Opis
AES (Advanced Encryption Standard)	Jeden z najczęściej stosowanych algorytmów, wykorzystywany w różnych standardach, takich jak protokół SSL/TLS.
DES (Data Encryption Standard)	Starszy algorytm, obecnie uważany za niebezpieczny z powodu krótkiego klucza (56 bitów).
3DES (Triple DES)	Zabezpiecza dane poprzez potrójne zastosowanie algorytmu DES. Jest bezpieczniejszy, ale wolniejszy.
Blowfish	Szybki algorytm, który jest elastyczny pod względem długości klucza (od 32 do 448 bitów).
RC4	Strumieniowy algorytm, który był popularny w szyfrowaniu komunikacji, obecnie uznawany za niebezpieczny.

Algorytmy szyfrowania asymetryczne

Algorytmy szyfrowania asymetrycznego używają pary kluczy: publicznego do szyfrowania i prywatnego do deszyfrowania.

Algorytm	Opis
RSA (Rivest-Shamir-Adleman)	Najpopularniejszy algorytm asymetryczny, oparty na faktoryzacji dużych liczb.
DSA (Digital Signature Algorithm)	Używany głównie do podpisów cyfrowych z wykorzystaniem kluczy publicznych i prywatnych.
ECC (Elliptic Curve Cryptography)	Wykorzystuje matematyczne krzywe eliptyczne, oferując wysoki poziom bezpieczeństwa przy krótszych kluczach.
ElGamal	Algorytm wykorzystujący klucze asymetryczne, często stosowany w kryptografii klucza publicznego.

Funkcje skrótu

Funkcje skrótu (hash functions) służą do przekształcania danych wejściowych na wartości o stałej długości, zapewniając integralność danych.

Funkcja	Opis
SHA-256	Część rodziny SHA-2, popularny w kryptografii, generuje skrót o długości 256 bitów.
SHA-3	Najnowsza wersja algorytmu SHA, która działa na różnych długościach skrótów.
MD5	Starsza funkcja skrótu, obecnie uznawana za niebezpieczną z powodu podatności na kolizje.
RIPEMD-160	Funkcja skrótu, która generuje 160-bitowy skrót, używana w różnych zastosowaniach.

Typy ataków na systemy komputerowe i sieci

Atak krzyżowy (Cross-Site Scripting - XSS)

Atak krzyżowy polega na wprowadzeniu złośliwego skryptu do strony internetowej, co pozwala atakującemu na wykonywanie nieautoryzowanych działań w kontekście przeglądarki ofiary. Może prowadzić do kradzieży sesji, danych użytkownika lub przejęcia kontroli nad kontem. Ataki te mogą być różnych typów:

- Stored XSS: złośliwy skrypt jest przechowywany na serwerze, np. w bazie danych.
- Reflected XSS: skrypt jest odsyłany jako część żądania HTTP i natychmiast wykonywany.

Atak przy pomocy węzłów pośredniczących (Man-in-the-Middle - MitM)

Atak MitM polega na przechwyceniu i modyfikacji komunikacji między dwoma stronami, które są przekonane, że komunikują się bezpośrednio. Atakujący może:

- Podsłuchiwać dane przesyłane między użytkownikiem a serwerem.
- Zmieniać wiadomości przed ich dostarczeniem do odbiorcy.
- Wprowadzać złośliwe oprogramowanie.

Atak rozproszony (Distributed Denial of Service - DDoS)

Atak DDoS jest formą ataku, w którym wiele zainfekowanych komputerów (zombie) wysyła dużą ilość ruchu do celu, co powoduje przeciążenie serwera lub sieci. Celem jest uniemożliwienie normalnego funkcjonowania usługi. Może być wykonywany na wiele sposobów:

- Flooding: nadmiernie zalewa serwer żądaniami.
- Amplification: wykorzystuje podatności serwerów do zwiększenia ilości wysyłanych danych.

Atak skoncentrowany (Single Point of Failure)

Atak skoncentrowany odnosi się do słabych punktów w infrastrukturze IT, które mogą być atakowane w celu doprowadzenia do awarii systemu. W tym kontekście mogą występować różne zagrożenia, takie jak:

- Złośliwe oprogramowanie: celowe zainfekowanie kluczowych komponentów.
- Usunięcie danych: zniszczenie lub kradzież danych przechowywanych w wrażliwych lokalizacjach.

Zmiana czasu złamania w zależności od długości klucza

Zmiana czasu złamania w zależności od długości klucza

Przykład dla algorytmu XOR: Security: Przestrzeń kluczy XOR Vernam

Czas złamania algorytmu szyfrującego jest proporcjonalny do liczby możliwych kombinacji kluczy. Przy każdym zwiększeniu długości klucza o jeden bit, liczba kombinacji podwaja się. Z matematycznego punktu widzenia, dla klucza o długości n bitów, liczba możliwych kluczy wynosi 2^n. Przykład: Wydłużenie klucza o 6 bitów

- Liczba kluczy dla obecnego klucza $n: 2^n$
- Liczba kluczy dla klucza przedłużonego o 6 bitów: $2^{(n+6)}=2^n×2^6=64×2^n$

Przykład obliczeniowy

Załóżmy, że mamy klucz 64-bitowy:

- Liczba możliwych kluczy: 264 (około 18.4 tryliona kluczy).
- Po wydłużeniu klucza o 6 bitów (do 70 bitów):
- Liczba możliwych kluczy: 270 (około 1.18 kwintyliona kluczy).

Zmiana czasu łamania

Jeżeli założymy, że czas potrzebny do złamania danego klucza jest równy T, to:

- Czas złamania dla klucza 64-bitowego: T.
- Czas złamania dla klucza 70-bitowego: 64 razy dłuższy (64T).

Moc Haseł

Wybór silnego hasła jest kluczowy dla ochrony danych i systemów. Przyjrzyjmy się podanym hasłom, oceniając ich złożoność, długość oraz elementy utrudniające złamanie.

"jestemgeniuszem"

- Długość: 15 znaków
- Złożoność: Używa jedynie małych liter, brak znaków specjalnych i cyfr.
- Ocena: Mimo że hasło jest stosunkowo długie, jego brak zróżnicowania (tylko małe litery) czyni je łatwym celem dla ataków słownikowych. Atakujący może szybko sprawdzić popularne frazy w danym języku.

"Myślę więc jestem"

- Długość: 19 znaków (wraz z spacjami)
- Złożoność: Zawiera znaki diakrytyczne (ć, ń), jednak przestrzenie między słowami mogą być problematyczne.
- Ocena: Choć hasło jest długie i zawiera znaki specjalne, obecność spacji czyni je mniej praktycznym. Ponadto, może być łatwiejsze do odgadnięcia, ponieważ to znana fraza filozoficzna.

"Bolek&Lolektobajka"

- Długość: 20 znaków
- Złożoność: Zawiera małe i wielkie litery oraz znak specjalny (&).
- Ocena: To hasło jest na dobrej drodze, ale odniesienie do znanych postaci z bajek czyni je bardziej podatnym na ataki. Osoby próbujące złamać to hasło mogą z łatwością zgadywać, opierając się na popularnych motywach kulturowych.

"Alibaba+40rozbójników"

- Długość: 22 znaki
- Złożoność: Zawiera wielkie i małe litery, znak specjalny (+) oraz liczby.
- Ocena: Jest to zdecydowanie najtrudniejsze hasło do złamania spośród wszystkich wymienionych. Wysoka długość, różnorodność znaków oraz unikalna kombinacja sprawiają, że jest znacznie mniej podatne na ataki.