Ataki na systemy komputerowe

Cz. 2. Rodzaje ataków

Źródła zagrożeń:

- Dołączony zainfekowany nośnik: Może to być pendrive, płyta CD/DVD, dysk zewnętrzny lub inny nośnik danych, który zawiera złośliwe oprogramowanie. Podłączenie takiego nośnika do komputera może spowodować infekcję systemu.
- Pobieranie i uruchamianie programów z nieznanych źródeł może zwiększać ryzyko zainfekowania systemu złośliwym oprogramowaniem.
- Złośliwe e-maile i załączniki: Otwarcie podejrzanego e-maila lub pobranie i otwarcie załącznika może prowadzić do infekcji systemu lub uruchomienia szkodliwego oprogramowania.
- Fałszywe aktualizacje oprogramowania: Atakujący mogą udawać, że oferują aktualizacje oprogramowania lub poprawki zabezpieczeń, które w rzeczywistości zawierają złośliwe oprogramowanie. Jeśli użytkownik pobierze i zainstaluje taką fałszywą aktualizację, może narazić system na ryzyko.
- Niebezpieczne witryny internetowe: Odwiedzanie witryn internetowych o wątpliwej reputacji, takich jak strony z nielegalną zawartością, strony udające serwisy bankowe lub witryny udostępniające pirackie oprogramowanie, może prowadzić do zainfekowania systemu.
- Wykorzystanie podatności oprogramowania: Atakujący mogą wykorzystać istniejące luki w oprogramowaniu, które nie zostały jeszcze naprawione, aby zdalnie uzyskać dostęp do systemu. W takich przypadkach ważne jest regularne stosowanie aktualizacji i łatek bezpieczeństwa.
- Złośliwe skrypty na stronach internetowych: Niektóre witryny internetowe mogą zawierać złośliwe skrypty, które są automatycznie uruchamiane podczas odwiedzania strony. Mogą one wykorzystać podatności w przeglądarce lub wtyczkach, aby zainfekować system.
- Słabe hasła i ataki brute force: Używanie słabych lub łatwo odgadnianych haseł do kont użytkownika lub systemów może umożliwić atakującym uzyskanie nieautoryzowanego dostępu. Ataki brute force polegają na próbach automatycznego odgadnięcia hasła poprzez przetestowanie różnych kombinacji.

Rodzaje

Rodzaj ataku	Charakterystyka	Sposoby zabezpieczenia
Wirus	Szkodliwe oprogramowanie, które **replikuje** się przez **zainfekowanie** innych plików, co umożliwia jego rozprzestrzenianie się.	Regularne aktualizacje systemu operacyjnego i oprogramowania, stosowanie antywirusów, ostrożność podczas pobierania plików.
Robak	Szkodliwe oprogramowanie, które **replikuje** się **samodzielnie** i rozprzestrzenia się na inne komputery poprzez **sieć**.	Regularne aktualizacje systemu operacyjnego i oprogramowania, stosowanie antywirusów, zapór sieciowa, ostrożność podczas pobierania plików i korzystania z sieci komputerowych.
Trojan	Szkodliwe oprogramowanie, które **ukrywa** się w legalnej aplikację i wykorzystuje jej uprawnienia, aby wykonać niepożądane działania.	Stosowanie oprogramowania antywirusowego i zapory sieciowej, ostrożność podczas pobierania i instalowania aplikacji, unikanie klikania w podejrzane linki lub załączniki.

Rodzaje

Rodzaj ataku	Charakterystyka	Sposoby zabezpieczenia
Inżynirria społeczna (Social engineering)	Wykorzystanie ludzkiej natury, takiej jak zaufanie, nieostrożność lub niewiedza, w celu uzyskania nieautoryzowanego dostępu lub informacji.	Edukacja w zakresie zasad bezpieczeństwa, ostrożność.
Phishing	Oszustwo wykorzystujące e-mail, SMS, w którym przestępcy **podszywają** się pod zaufane źródło w celu wyłudzenia poufnych informacji.	Edukacja w zakresie zasad bezpieczeństwa podczas korzystania z sieci, ostrożność podczas korzystania z poczty elektronicznej i innych form komunikacji, stosowanie oprogramowania antyspamowego i filtrowania wiadomości.
Spoofing	Technika polegająca zaawansowanym na **podszywaniu** się pod prawdziwe adresy IP, numer telefonu aby ukryć swoją tożsamość i wprowadzić w błąd systemy zabezpieczeń.	Uwierzytelnienie nadawcy.

Rodzaje

Rodzaj ataku	Charakterystyka	Sposoby zabezpieczenia
Exploit	Wykorzystanie znanych błędów w oprogramowaniu lub systemie operacyjnym w celu uzyskania nieautoryzowanego dostępu lub wykonania określonych działań.	Regularne aktualizacje systemu operacyjnego i oprogramowania, stosowanie zapór sieciowych i programów antywirusowych, stosowanie zasad bezpieczeństwa podczas korzystania z sieci.
„Zero day” exploit	Podatność w oprogramowaniu, znana atakującym, ale nie są znana producentowi oprogramowania ani ogółowi użytkowników. Jest to szczególnie niebezpieczne, ponieważ atakujący mogą wykorzystać tę podatność, zanim zostanie opracowana łatka lub środki zabezpieczające	

Rodzaje

Rodzaj ataku	Charakterystyka	Sposoby zabezpieczenia
Exploit	Wykorzystanie znanych błędów w oprogramowaniu lub systemie operacyjnym w celu uzyskania nieautoryzowanego dostępu lub wykonania określonych działań.	Regularne aktualizacje systemu operacyjnego i oprogramowania, stosowanie zapór sieciowych i programów antywirusowych, stosowanie zasad bezpieczeństwa podczas korzystania z sieci.
„Zero day” exploit	Podatność w oprogramowaniu, znana atakującym, ale nie są znana producentowi oprogramowania ani ogółowi użytkowników. Jest to szczególnie niebezpieczne, ponieważ atakujący mogą wykorzystać tę podatność, zanim zostanie opracowana łatka lub środki zabezpieczające	
Backdoor	Ukryty mechanizm umożliwiający ominięcie standardowych procedur uwierzytelniania lub bezpieczeństwa w systemie komputerowym. Może być celowo pozostawiony przez programistów w celu rozwiązywania problemów lub zarządzania systemem.	Regularne aktualizacje oprogramowania, skanowanie systemów, ścisła kontrola dostępu do systemu.

Rodzaje

Rodzaj ataku	Charakterystyka	Sposoby zabezpieczenia
Malware	**Szkodliwe** oprogramowanie, które może pełnić różne funkcje, od infekowania systemu po kradzież poufnych informacji.	Regularne aktualizacje systemu operacyjnego i oprogramowania, stosowanie antywirusów i zapór sieciowych, ostrożność podczas pobierania plików i korzystania z sieci.
Spyware	Spyware to rodzaj złośliwego oprogramowania, które ma na celu nieautoryzowane **śledzenie** i gromadzenie informacji o użytkowniku lub jego działaniach na komputerze lub urządzeniu mobilnym. Spyware może rejestrować wpisy klawiatury, monitorować aktywność sieciową, przechwytywać dane osobowe, śledzić nawigację internetową oraz wyświetlać niechciane reklamy.	Regularne aktualizacje systemu operacyjnego i oprogramowania, stosowanie antywirusów i zapór sieciowych, ostrożność podczas pobierania plików i korzystania z sieci.
Ransomware	Szkodliwe oprogramowanie, które **blokuje** dostęp do plików lub całego systemu, a następnie **żąda okupu** za ich odblokowanie.	Regularne tworzenie kopii zapasowych danych, stosowanie oprogramowania antywirusowego i zapór sieciowych, unikanie otwierania podejrzanych wiadomości e-mail lub załączników, unikanie pobierania plików z nieznanych źródeł.

Rodzaje

Rodzaj ataku	Charakterystyka	Sposoby zabezpieczenia
Atak DoS, DDoS (Denial of Service)	Atak mający na celu przeciążenie sieci lub serwera poprzez wysłanie dużej liczby zapytań lub żądań, co uniemożliwia dostęp do usługi.	Stosowanie zapór sieciowych, ograniczenie liczby połączeń sieciowych, stosowanie rozwiązań do wykrywania zwalczania ataków DDoS.
Botnet	Grupa komputerów zainfekowanych szkodliwym oprogramowaniem pozostającym w ukryciu przed użytkownikiem i pozwalającym jego twórcy na sprawowanie zdalnej kontroli nad wszystkimi komputerami w ramach botnetu.	Stosowanie zapór sieciowych i filtrów spamu. Systemy wykrywania intruzó (IDS – Intrusion Detection System), Honeypot
Keylogger	Szkodliwe oprogramowanie, które **rejestruje klawisze** naciskane na klawiaturze, w celu przechwytywania poufnych informacji, takich jak hasła czy numery kart kredytowych.	Stosowanie oprogramowania antywirusowego i zapory sieciowej, ostrożność podczas korzystania z komputera w miejscach publicznych, unikanie pobierania plików z nieznanych źródeł, stosowanie silnych haseł i autoryzowanych narzędzi do autoryzacji dostępu.

Metody ataków:

Najpopularniejsze metody ataków komputerowych:

- Phishing - atak polegający na podszywaniu się pod zaufane źródło (np. bank, firma) w celu wyłudzenia poufnych informacji, takich jak hasła czy dane karty kredytowej.
- Spoofing - technika polegająca na podszywaniu się np. pod prawdziwe adresy IP, aby ukryć swoją tożsamość i wprowadzić w błąd systemy zabezpieczeń.
- Denial of Service (DoS) - atak, którego celem jest spowodowanie przerwy w działaniu usługi lub systemu poprzez zalewienie go zapytaniami i żądaniami.
- Man-in-the-middle (MITM) - atak polegający na przechwyceniu komunikacji między dwoma punktami w celu podsłuchania lub manipulacji przesyłanymi informacjami.
- Ataki brute force - polegające na próbie zgadnięcia lub złamania hasła poprzez ciągłe próby logowania, wykorzystując różne kombinacje znaków.
- Exploity - atak polegający na wykorzystaniu luki w oprogramowaniu lub systemie operacyjnym w celu uzyskania nieautoryzowanego dostępu do systemu.
- Social engineering - technika polegająca na manipulowaniu ludźmi w celu uzyskania poufnych informacji lub dostępu do systemów.
- Typosquatting - technika polegająca na wykorzystaniu literówek w adresach URL w celu wprowadzenia w błąd użytkowników i przekierowania ich na fałszywe strony internetowe.

Phishing przykład

[https://kdbs.com.pl/bezpieczenstwo-w-internecie/phishing-co-to-jest/]

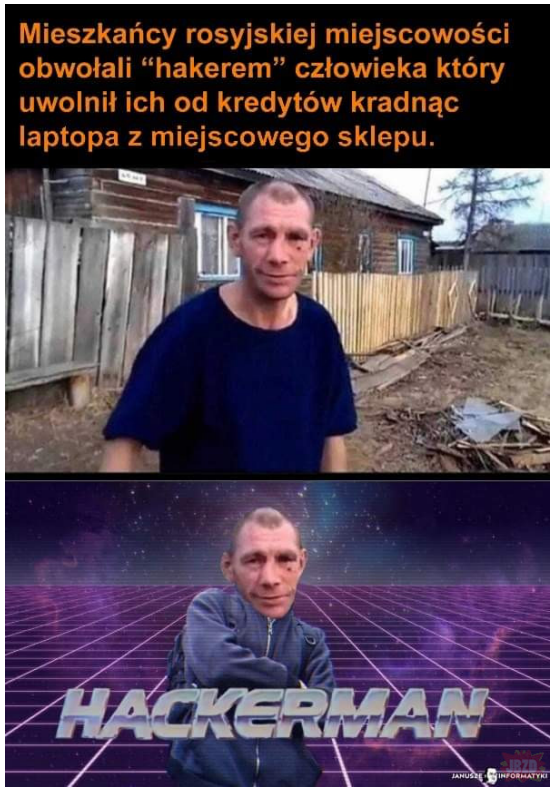
Czego najczęściej dotyczą fałszywe wiadomości?

- niewielkiej kwoty, którą masz dopłacić do przesyłki
- bonów, kuponów oraz innych darmowych „nagród", które możesz zdobyć
- podejrzanych logowań na Twoim koncie
- problemów z Twoim kontem lub płatnością
- niekompletnych danych, które musisz potwierdzić
- niezapłaconej faktury, którą masz opłacić.

Jak przebiega takie oszustwo?

- Dostajesz e-maila lub SMS-a. Wiadomość wygląda jak z firmy, którą dobrze znasz.
- Masz pilnie zalogować się na stronę banku przez link z wiadomości. Najczęściej po to, aby odebrać rzekome pieniądze.
- Link przekierowuje Cię na fałszywą stronę, która przypomina stronę Twojego banku.
- Logujesz się – podajesz swoje dane oraz kod z SMS-a.
- Masz wpisać kolejne kody SMS, aby zaktualizować swoje dane.
- Widzisz komunikat o błędzie, więc wpisujesz je kilka razy.
  Pamiętaj: zawsze dokładnie czytaj kody SMS – czy treść powiadomienia z kodem odpowiada temu co akurat chcesz zrobić na stronie? Zwracaj też uwagę na to, które urządzenia dodajesz do zaufanych.
- Oszust dostał dostęp do Twojego konta. Od teraz może się na nie logować i z niego korzystać, np. zlecać przelewy czy wypłacać pieniądze z bankomatu za pomocą BLIKA.

Hakerzy


Mieszkańcy rosyjskiej miejscowości obwołali “hakerem” człowieka który uwolnił ich od kredytów kradnąc laptopa z miejscowego sklepu.
HACKERMAN

Hakerzy

Haker to osoba, która używa swoich umiejętności technicznych do manipulowania systemami komputerowymi, sieciami lub urządzeniami elektronicznymi. Hakerzy mogą działać w różnych celach i z różnymi motywacjami, co prowadzi do ich klasyfikacji na różne kategorie:

- **White Hat Hackers** (Etyczni hakerzy) - Pracują legalnie i często są zatrudniani przez firmy, aby znaleźć i naprawić luki w zabezpieczeniach systemów komputerowych. Ich celem jest poprawa bezpieczeństwa.
- **Black Hat Hackers** (Kryminalni hakerzy) - Działają nielegalnie, wykorzystując swoje umiejętności do kradzieży danych, oszustw, zakłócania działania systemów i innych złośliwych działań.
- **Grey Hat Hackers** - Znajdują się pomiędzy etycznymi a kryminalnymi hakerami. Mogą łamać zabezpieczenia bez pozwolenia, ale ich celem nie zawsze jest złośliwe działanie. Czasami informują oni właścicieli systemów o lukach, które odkryli, ale ich działania mogą być legalnie wątpliwe.
- **Script Kiddies** - Osoby, które wykorzystują istniejące narzędzia i skrypty stworzone przez innych hakerów, zamiast tworzyć własne narzędzia. Często mają ograniczoną wiedzę techniczną.
- **Hacktivists** - Hakerzy działający z powodów politycznych lub ideologicznych. Używają swoich umiejętności do promowania określonych celów społecznych lub politycznych.

Hakerzy

APT – Advanced Persistenet Threat

[https://en.wikipedia.org/wiki/Advanced_persistent_threat]

CTF – Capture The Flag

[https://en.wikipedia.org/wiki/Capture_the_flag_(cybersecurity)]

Praktyka

1. WAP (Wi-Fi Access Point)
2. Wyciek danych
3. Bannery
4. DDoS
5. Phishing – hasła do banku

[https://www.youtube.com/watch?v=EGVELy8qX7U]
[https://www.youtube.com/watch?v=DWhIxCgyR9I]

KONIEC

- pobieraj pliki wyłącznie z zaufanych źródeł,
- korzystaj z legalnego systemu operacyjnego,
- sprawdź, jaką politykę dotyczącą aktualizacji własnego oprogramowania i usuwania luk stosuje producent,
- nie otwieraj maili od niezaufanych nadawców ani znajdujących się w nich załączników,
- nie klikaj w wyskakujące reklamy,
- używaj zapory sieciowej firewall,
- korzystaj z systemu antywirusowego z funkcją ochrony sieci w czasie rzeczywistym,
- pamiętaj o aktualizacjach systemu oraz zainstalowanych programów,
- upewniaj się, że razem z programami nie instalujesz dodatkowych narzędzi, które mogą zawierać wirusy,
- przeskanuj zapisane na zewnętrznych nośnikach pliki przed ich otwarciem.