

Cyberbezpieczeństwo – ochrona przed cyberzagrożeniami

oprac. Barbara Góral, Dawid Leśniak

Bezpieczeństwo

stan braku zagrożeń, dający poczucie pewności i ochrony przed niebezpieczeństwem.

Cyberbezpieczeństwo

zespół zagadnień związanych z zapewnianiem ochrony w obszarze cyberprzestrzeni.

Cyberzagrożenie

wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób

Przykłady cyberzagrażeń:

- Phishing
- Ransomware

PHISHING

To podszywanie się pod obdarzoną zaufaniem społeczną instytucję finansową np. bank, instytucję finansową np. urząd, firmę prywatną w celu wyłudzenia poufnych danych, zainstalowania na komputerze złośliwego oprogramowania lub skłonienia ofiary do konkretnego działania.

Rodzaje PHISHINGU

- **Spear phishing**
- **Whaling**
- **Clone phishing**
- **Spoofing**
- **Smishing**

Spear phishing

to zaawansowana forma phishingu, w której przestępcy ukierunkowują ataki na konkretne osoby lub organizacje, aby wyłudzić poufne dane lub zainstalować złośliwe oprogramowanie

Przykład Spear phishingu:

Atak na Pracownika Działu Finansowo-Księgowego: Wiadomość e-mail z prośbą o autoryzację przelewu, podszywająca się pod Głównego Księgowego

Whailing (atak na wieloryba)

zaawansowany rodzaj phishingu, skierowany do osób na wysokich stanowiskach w organizacji (np. prezesi, dyrektorzy) w celu kradzieży poufnych informacji lub pieniędzy.

Przykład Whailingu

Hakerzy mogą podszyć się pod prezesa firmy i wysłać e-mail do Głównego Księgowego z prośbą o pilne przelanie dużej kwoty na wskazany rachunek bankowy.

Clone phishing

rodzaj ataku phishingowego, w którym przestępcy wykorzystują treść wcześniej wysłanej, legalnej wiadomości e-mail, aby stworzyć fałszywą wiadomość, która wygląda jak autentyczna, ale zawiera złośliwe linki lub załączniki

Przykłady Clone phishingu

- E-mail z linkiem do aktualizacji swojego konta bankowego. Oryginalny e-mail był legalny, ale przestępca podmienił link na fałszywą stronę, która zbiera dane logowania.
- E-mail z fakturą od firmy, z którą współpracujesz. Oryginalny e-mail był legalny, ale przestępca podmienił link do płatności na swój rachunek bankowy.

Spoofing

to rodzaj ataku, w którym przestępcy podszywają się pod banki, instytucje i urzędy państwowe, firmy, a nawet osoby fizyczne w celu wyłudzenia od swoich ofiar danych lub pieniędzy

Rodzaje Spoofingu (między innymi):

- **Spoofing e-mailowy** – atakujący fałszuje adres nadawcy w wiadomości, co sprawia, że wygląda ona na wysłaną przez zaufane źródło. Może to być stosowane w celu wyłudzenia danych logowania, instalacji złośliwego oprogramowania lub wyłudzenia pieniędzy.
- **Spoofing telefoniczny** – atakujący podszywa się pod znane numery telefonów, np. banki, firmy kurierskie czy urzędy. Ofiara odbiera połączenie, myśląc, że rozmawia z zaufanym podmiotem, a w rzeczywistości przekazuje dane przestępcy.

Smishing

to forma phishingu wykorzystująca wiadomości SMS. Polega na wysyłaniu fałszywych wiadomości, które mają na celu nakłonienie odbiorcy do ujawnienia poufnych danych (np. loginów, haseł, numerów kart kredytowych) lub zainstalowania złośliwego oprogramowania.

Przykłady Smishingu

Wiadomości o zaległych opłatach za energię elektryczną, niedopłacie za paczkę kurierską, informacja o wpłacie BLIK z podanym linkiem kierującym do płatności czy wezwanie banku do uzupełnienia albo aktualizacji naszych danych

RANSOMWARE

to rodzaj złośliwego oprogramowania , które może zainfekować komputer, smartfon czy tablet.

Oprogramowanie blokuje dostęp do systemu komputerowego lub zaszyfrowuje pliki, a następnie żąda okupu za przywrócenie dostępu lub odblokowanie danych.

Ransomware może uniemożliwić zalogowanie się do systemu lub zablokować dostęp do konkretnych plików i folderów oraz aplikacji.

Zaawansowane formy ransomware szyfrują pliki, uniemożliwiając ich odczyt bez klucza deszyfrującego.

Rodzaje oprogramowania Ransomware:

- **Screen-locker** – zablokowanie ekranu urządzenia ofiary, bez szyfrowania plików.
- **Crypto-ransomware** – zaszyfrowanie plików znajdujących się na dysku zaatakowanego.
- **Disk-encryptor** – atakujący szyfruje cały dysk użytkownika, co uniemożliwia uruchomienie systemu operacyjnego.

Przykład ataku Ransomware:

Celem hakerów padł w 2022r łódzki Instytut Centrum Zdrowia Matki Polki. By zminimalizować skutki cyberataku, szpital zdecydował się na czasowe wyłączenie systemów informatycznych i obsługiwanie pacjentów przy wykorzystaniu tradycyjnej papierowej dokumentacji. Poważnie zakłóciło to normalne funkcjonowanie tej instytucji, opóźniając wydawanie dokumentacji medycznej, wypisywanie pacjentów i szereg innych, niezwykle wrażliwych procedur.

Jak się chronić?

Działania należy podejmować na poziomie zabezpieczenia samego systemu informatycznego (zadania Pracowników Działu Informatyki) jak również na poziomie bezpośrednich użytkowników systemów oraz sprzętu.

Zadania Działu Informatyki to między innymi:

- Regularne aktualizowanie systemu operacyjnego i oprogramowania
- Instalacja oprogramowania antywirusowego
- Stosowanie zapór typu firewall
- Tworzenie kopii zapasowych
- Odpowiednia konfiguracja komputerów (zablokowane porty usb)

Obowiązki każdego użytkownika:

- Unikaj otwierania podejrzanych załączników i klikania w linki od nieznanych nadawców, zwróć uwagę na format załącznika, faktury i dokumenty to zazwyczaj PDF
- Uważaj na prośby e-mail czy wiadomości SMS o natychmiastowe zaktualizowanie danych, potwierdzenie płatności czy weryfikację konta. Cyberprzestępcy zwykle liczą na to, że pośpiech i presja skłonią odbiorcę do szybkiego kliknięcia linka lub otwarcia załącznika bez zastanowienia.
- Uważaj na nietypowe prośby o dane osobowe lub firmowe. Firmy rzadko proszą o poufne informacje przez e-mail. Jeśli wiadomość zawiera prośbę o podanie haseł, danych logowania, numerów kont czy innych wrażliwych danych, jest to poważny sygnał ostrzegawczy.

Obowiązki każdego użytkownika (ciąg dalszy):

- Zwracaj uwagę na niespójność z wcześniejszymi kontaktami. Jeśli treść wiadomości jest niespójna z wcześniejszą korespondencją, np. dotyczy faktury, której nie kojarzysz, czy zmiany danych bankowych bez wcześniejszego powiadomienia należy być czujnym.
- Uważaj na podejrzone domeny w adresach URL. Cyberprzestępcy często używają domen podobnych do prawdziwych, np. zamiast „firmaXYZ.com” może pojawić się „firmaXYZ-co.com”. Uważne sprawdzenie adresu URL, zwłaszcza w przypadku logowania na stronach, jest bardzo istotne.

Dziękujemy za uwagę

Wrzesień 2025