NASK

CyberBHP

Najczęstsze rodzaje cyberataków

Coraz szybszy rozwój technologii sprawia, że obok korzyści niesie ona także coraz poważniejsze zagrożenia w zakresie cyberbezpieczeństwa firm i organizacji. Wiedza na ten temat oraz świadomość potencjalnych cyberzagrożeń ma kluczowe znaczenie dla prawidłowego funkcjonowania firmy.

Phishing

Oszustwo polegające na podszywaniu się pod inną osobę lub instytucję poprzez przesłanie wiadomości zawierających zazwyczaj:

- Groźbę lub obietnicę niespodziewanej nagrody
- Link kierujący do fałszywej strony internetowej, łudząco podobnej do strony ważnej instytucji, banku, sklepu
- Link do panelu wyłudzającego wrażliwe dane, zwłaszcza te umożliwiające dostęp do konta bankowego, karty płatniczej, kodów BLIK, danych osobowych
- Zainfekowany załącznik

Malware

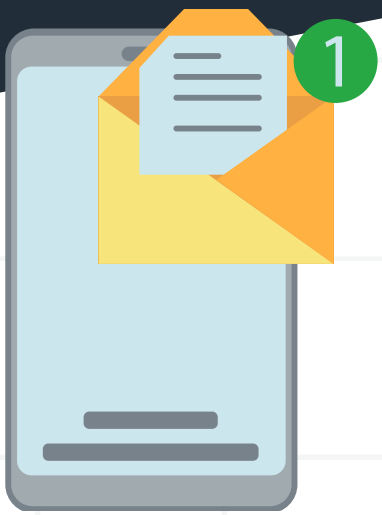
Oprogramowanie (aplikacja lub skrypt), które ma na celu złamanie zabezpieczeń i zainfekowanie urządzenia, a następnie przechwycenie jego zasobów lub danych. Mogą to być załączniki do wiadomości, pliki ściągane po kliknięciu w link, aplikacje podszywające się pod użyteczne programy czy gry internetowe.

Ransomware

Odmiana malware'u, która powoduje blokadę urządzenia lub zaszyfrowanie znajdujących się w nim plików. W zamian za odblokowanie, odszyfrowanie lub obietnicę nieupubliczniania wykradzionych danych i/lub informacji, przestępcy żądają okupu.

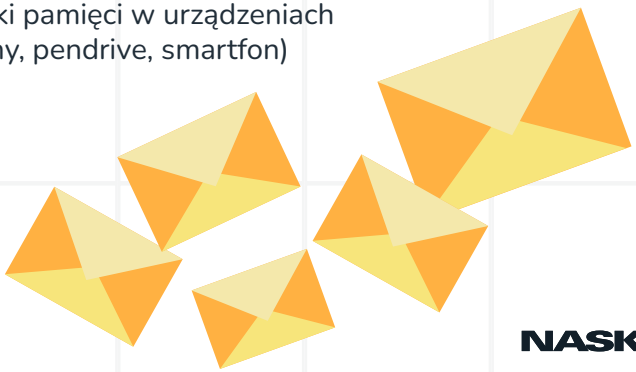
Spam

Niechciane, niepotrzebne lub szkodliwe wiadomości masowo rozsyłane w formie elektronicznej, np. uporczywe reklamy produktów, usług, portali, promocje, informacje o wygranej itp. Mogą zawierać niebezpieczne załączniki lub linki do zainfekowanych plików (malspam).



ŹRÓDŁA ATAKÓW

- Poczta e-mail, SMS-y: linki w treści wiadomości lub załączniki
- Wiadomości w komunikatorach (np. WhatsApp, Messenger) i serwisach społecznościowych (np. Facebook, Instagram)
- Rozmowy telefoniczne (np. fałszywa „pomoc techniczna" prosząca o instalację dodatkowego oprogramowania)
- Zewnętrzne nośniki pamięci w urządzeniach (np. dysk przenośny, pendrive, smartfon)



NASK

Potencjalne skutki ataków

Utrata środków finansowych

Kradzież tożsamości (np. imienia i nazwiska, adresu zameldowania, numeru dowodu osobistego, PESEL-u)

Kradzież poufnych danych (np. haseł dostępowych, numerów kart płatniczych, danych klientów, informacji stanowiących tajemnicę firmową)

Uszkodzenie lub skasowanie plików z urządzenia

Przejęcie urządzenia i zablokowanie dostępu do niego bądź do danych, które są w nim przechowywane

Naruszenie prywatności (np. szantaż, żądanie okupu, nękanie)

PAMIĘTAJ!
Jeśli adresat lub treść wiadomości budzą Twoje wątpliwości, nie klikaj w linki i nie otwieraj załączników.
Nie podawaj też żadnych poufnych informacji, takich jak hasła, dane do logowania itp.
Zawsze stosuj zasadę ograniczonego zaufania!

NASK

Finansowane ze środków Kancelarii Prezesa Rady Ministrów.
Publikacja wyraża jedynie poglądy autorów i nie może być utożsamiana z oficjalnym stanowiskiem Kancelarii Prezesa Rady Ministrów.