CYBERBEZPIECZEŃSTWO

Realizując zadania wynikające z ustawy o krajowym systemie cyberbezpieczeństwa poniżej prezentujemy najważniejsze informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady jak skuteczne stosować sposoby zabezpieczenia się przed tymi zagrożeniami.

Cyberbezpieczeństwo to „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy” (art. 2 pkt 4) Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560).

Celem cyberprzestępców zwykle jest kradzież naszych danych za pomocą różnych technik mające na celu nakłonienie nas do wykonania czynności, wskutek których ujawnione zostaną nasze hasła i stosowane zabezpieczenia. Wśród tych technik są między innymi: zainfekowane załączniki do poczty e-mail, wiadomości e-mail czy też fałszywe strony internetowe - najczęściej strony bankowe.
Najpopularniejsze rodzaje ataków:

• **Malware**, czyli złośliwe oprogramowanie, które bez naszej zgody i wiedzy wykonuje na komputerze działania na korzyść osoby trzeciej. Działania tego typu obejmują między innymi zdobywanie wirtualnych walut, kradzież danych osobowych i informacji niezbędnych do logowania do bankowości elektronicznej. Złośliwe oprogramowanie może przyjąć formę wirusów, robaków, koni trojańskich i innych.
• **Phishing** to jeden z najpopularniejszych typów ataków dokonywanych przy użyciu wiadomości e-mail, rozmów telefonicznych czy wysyłanych wiadomości SMS. Cyberprzestępcy podszywając się pod różne instytucje (np. firmy kurierskie, urzędy, operatorów telekomunikacyjnych, banki) a nawet naszych znajomych, starają się wyłudzić nasze dane do logowania np. do kont bankowych lub używanych przez nas kont społecznościowych. Wiadomości phishingowe są tak przygotowywane, aby wyglądały na autentyczne.
• **Man in the Middle** jest rodzajem ataku, w którym cyberprzestępca uczestniczy w komunikacji między osobami, bez ich wiedzy. Wydaje nam się, że połączenie jest bezpośrednie i prywatne, natomiast w rzeczywistości ktoś potajemnie uczestniczy w komunikacji i ją zmienia. Celem takich ataków jest przechwycenie informacji lub środków pieniężnych (np. uzyskanie danych niezbędnych do logowania w systemie bankowości elektronicznej).
• **Ransomware** to rodzaj ataku, którego celem jest przejęcie i zaszyfrowanie danych zgromadzonych na komputerze a następnie zażądanie okupu za ich odzyskanie. Zagrożenie może dostać się do komputera za pośrednictwem pobranego pliku lub nawet przez wiadomość tekstową. Atak nie ma na celu kradzieży danych, lecz wymuszenie okupu.
•**Malvertising** pozwala przestępcom na dotarcie do nas poprzez reklamy udostępniane nam na przeglądanych zaufanych stronach internetowych. W następnym kroku atakujący instaluje, bez naszej wiedzy i zgody, złośliwe oprogramowanie na urządzeniach.
Pamiętaj, że twoja świadomość zagrożeń i zastosowanie środków bezpieczeństwa ma znaczenie dla zapewnienia ochrony Twoich danych – tożsamości, danych finansowych czy prywatności.
Zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie sposobów zabezpieczania się przed zagrożeniami to wiedza niezbędna każdemu użytkownikowi komputera, telefonu komórkowego czy też usług internetowych.

Rekomendacje dla użytkowników cyberprzestrzeni:

- Zainstaluj i używaj oprogramowania przeciw wirusom i spyware. Sprawdź czy w twoim systemie uruchomiony jest firewalla (czyli zapory sieciowa).

- Monitoruj, sprawdzaj działanie i aktualizuj oprogramowanie antywirusowe.
- Aktualizuj na bieżąco system operacyjny i aplikacje.
- Nie otwieraj plików i załączników do poczty e-mail nieznanego pochodzenia.
- Korzystaj tylko z legalnego oprogramowania.
- Nie korzystaj ze stron banków, poczty elektronicznej czy portali społecznościowych, które nie mają ważnego certyfikatu.
- Sukcesywnie skanuj komputer pod obecność wystąpienia wirusów.
- Sprawdzaj pliki pobrane z Internetu za pomocą skanera antywirusowego.
- Nie zostawiaj danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie masz absolutnej pewności, że nie są one widoczne dla osób trzecich.
- Nie wysyłaj w e-mailach żadnych poufnych danych w formie otwartego tekstu – niech np. będą zabezpieczone hasłem i zaszyfrowane – hasło przekazuj w sposób bezpieczny.
- Wykonuj kopie zapasowe ważnych danych.
- Pamiętaj, że żaden bank czy Urząd nie wysyła e-maili do swoich klientów/interesantów z prośbą o podanie hasła lub loginu w celu ich weryfikacji.

Więcej informacji na temat cyberbezpieczeństwa można znaleźć na następujących stronach:

- CERT Polska (Strona zespołu do spraw reagowania na incydenty cyberbezpieczeństwa)
- STÓJ. POMYŚL. POŁĄCZ. (Polska wersja międzynarodowej kampanii STOP. THINK. CONNECT.™, mającej na celu podnoszenie poziomu świadomości społecznej w obszarze cyberbezpieczeństwa)
- Biuletyn OUCH! (darmowy zestaw porad bezpieczeństwa dla użytkowników komputerów).
- Baza wiedzy w serwisie gov.pl
- Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT
- CSIRT NASK
- CSIRT MON