W ramach realizacji obowiązków wynikających z ustawy o krajowym systemie cyberbezpieczeństwa, dostarczamy Państwu informacje umożliwiające zrozumienie zagrożeń pojawiających się w cyberprzestrzeni oraz porady, jak skutecznie się przed nimi chronić.

Zgodnie z aktualnymi przepisami, cyberbezpieczeństwo definiowane jest jako „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 05.07.2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2024 r. poz. 1077)

Najczęściej występujące zagrożenia w cyberprzestrzeni obejmują:

- ataki z użyciem złośliwego oprogramowania (np. malware, wirusy),
- kradzież tożsamości,
- kradzież, modyfikację lub niszczenie danych,
- blokowanie dostępu do usług,
- spam,
- Ataki socjotechniczne takie jak phishing.

Phishing – nazwa pochodzi od password („hasło") oraz fishing („wędkowanie"). Istotą ataku jest próba pozyskania hasła użytkownika, które służy do logowania się na portalach społecznościowych bądź do serwisów. Po uzyskaniu dostępu, przestępca może wykraść dane osobowe i w tym celu dokonywać oszustw.
Jak się bronić? Ataki tego typu wymagają bardzo często interakcji ze strony człowieka w postaci odebrania maila lub potwierdzenia logowania.

Malware – zbitka wyrazowa pochodząca od wyrażenia malicious software („złośliwe oprogramowanie"). Wspólną cechą programów uznawanych za malware jest fakt, że wykonują działania na komputerze bez jego zgody i wiedzy użytkownika, na korzyść osoby postronnej. Działania tego typu obejmują np. dołączenie maszyny do sieci komputerów „zombie", które służą do ataku na organizacje rządowe, zdobywanie wirtualnych walut lub kradzież danych osobowych i informacji niezbędnych do logowania do bankowości elektronicznej.

Jak się bronić? Najskuteczniejszą obroną przed malware jest dobry system antywirusowy oraz regularnie aktualizowane oprogramowanie.

Ransomomware – Celem ataku jest zaszyfrowanie danych użytkownika, a następnie ponowne ich udostępnienie w zamian za opłatę. Odbywa się głównie za sprawą okupu. Ataki tego typu działają na szkodę osoby fizycznej, jak i przedsiębiorców.

Jak się bronić? Należy stosować aktualne oprogramowania antywirusowe oraz dokonywać regularnych aktualizacji systemu.

Man In the Middle – zwany „człowiekiem pośrodku", jest to typ ataku, w ramach, którego w transakcji lub korespondencji między dwoma podmiotami (na przykład sklepem internetowym i klientem) bierze udział osoba trzecia. Celem takich ataków jest przechwycenie informacji lub środków pieniężnych. Celem może być również podsłuchanie poufnych informacji oraz ich modyfikacja.

Jak się bronić? Szyfrowanie transmisji danych, certyfikaty bezpieczeństwa.

Jak zabezpieczyć się przed zagrożeniami:

- Używaj zainstalowanego oprogramowania antywirusowego i antyspyware z funkcją ochrony w czasie rzeczywistym,
- Reguralnie aktualizuj oprogramowanie antywirusowe i bazy danych wirusów, upewniając się, że program robi to automatycznie,
- Bez opóźnień aktualizuj system operacyjny oraz aplikacje,
- Nie otwieraj plików z nieznanego źródła,
- Korzystaj tylko z zaufanych stron internetowych banków, poczty elektronicznej czy portali społecznościowych z ważnym certyfikatem bezpieczeństwa,
- Unikaj używania niesprawdzonych programów do publikowania plików w Internecie, które mogą zawierać złośliwy kod,
- Regularnie skanuj komputer i monitoruj procesy sieciowe; w razie potrzeby poproś specjalistę o pomoc,
- Sprawdzaj pliki pobrane z Internetu za pomocą skanera,
- Nie udostępniaj danych osobowych na niezweryfikowanych stronach,
- Nie przesyłaj poufnych danych w e-mailach w formie otwartego tekstu; używaj, szyfrowania i bezpiecznego przekazywania haseł.

Zachęca się do regularnego zapoznawania się z treściami dotyczącymi cyberbezpieczeństwa zawartymi na stronach: - Ministerstwa Cyfryzacji pod adresem: https://www.gov.pl/web/cyfryzacja/cyberbezpieczenstwo .

NIE BĄDŹ OBOJĘTNY! ZGŁASZAJ PRZESTĘPSTWA DOKONYWANE W SIECI!
Nie bądź obojętny! Zgłaszaj przestępstwa dokonywane w sieci! - Aktualności - NASK