Cyberbezpieczeństwo

Podtytuł: Cyberbezpieczeństwo - dobre praktyki

Realizując zadania, wynikające z art. 22 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r., poz. 1369 ze zm.) przekazujemy Państwu informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady jak skuteczne stosować sposoby zabezpieczenia się przed tymi zagrożeniami.

Cyberbezpieczeństwo, zgodnie z obowiązującymi przepisami, to „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy”, zgodnie z art. 2 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Najpopularniejsze zagrożenia w cyberprzestrzeni:
a) ataki z użyciem szkodliwego oprogramowania oraz ataki socjotechniczne (phishing – podszywanie się pod osobę godną zaufania lub instytucję, spyware – oprogramowanie szpiegujące, ransomware – oprogramowanie blokujące dostęp do danych, polegające na szyfrowaniu i/lub bezpowrotnym usunięciu danych itp.),
b) kradzieże tożsamości, wyłudzenia, modyfikacje danych,
c) blokowanie dostępu do usług,
d) spam (niechciane lub niepotrzebne wiadomości elektroniczne),

Sposoby zabezpieczenia się przed zagrożeniami:
• Zainstaluj i używaj oprogramowania antywirusowego, zapewniającego ochronę w czasie rzeczywistym.
• Aktualizuj system operacyjny, bazy danych programu antywirusowego (najlepiej, jeżeli są wykonywane automatycznie) oraz inne aplikacje bez zbędnej zwłoki.
• Nie otwieraj plików nieznanego pochodzenia.
• Nie klikaj w linki przesyłane od nieznanych adresatów - stosuj zasadę "zero zaufania", ponieważ ktoś może podszywać się pod Twojego znajomego, kontrahenta lub instytucję.
• Nie korzystaj ze stron banków, poczty elektronicznej czy portali społecznościowych, które nie mają ważnego certyfikatu SSL (zamknięta kłódka w polu adresu internetowego).
• Nie używaj niesprawdzonych programów zabezpieczających i użytkowych.
• Pamiętaj, że żaden bank czy Urząd nie wysyła e-maili do swoich klientów z prośbą o podanie hasła lub loginu w celu ich weryfikacji.
• Nie odwiedzaj stron, które zawierają podejrzane oferty (nagrody, darmowe filmy i muzykę, darmowe – nielegalne oprogramowanie) – często na takich stronach znajdują się ukryte wirusy i inne zagrożenia.
• Nie wysyłaj w e-mailach żadnych poufnych danych w formie otwartego tekstu – najlepiej, jeżeli będą zabezpieczone hasłem i zaszyfrowane – hasło przekazuj w sposób bezpieczny.
• Nie zostawiaj danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie masz absolutnej pewności, że nie są one widoczne dla osób trzecich.
• Regularnie wykonuj kopie zapasowe wszystkich cennych danych na inne urządzenie (np. dysk zewnętrzny).
• Nie używaj tych samych haseł na różnych portalach internetowych.
• O ile to możliwe, stosuj uwierzytelnianie dwuskładnikowe.

Zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie sposobów zabezpieczania się przed zagrożeniami, to wiedza niezbędna każdemu użytkownikowi komputera, smartfona czy też usług internetowych.

Dodatkowe informacje:
• Zestaw porad bezpieczeństwa dla użytkowników komputerów prowadzony na witrynie internetowej CSIRT NASK – Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym: https://www.cert.pl/ouch/
• Poradniki na witrynie internetowej Ministerstwa Cyfryzacji: https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo
• Publikacje z zakresu cyberbezpieczeństwa: https://www.cert.pl/