Cyberbezpieczeństwo - ochrona przed zagrożeniami w sieci

W związku z realizacją obowiązku wynikającego z art. 22 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tekst jednolity ogłoszony w Dz.U. z 2026 r. poz. 20, z późn. zm.) przekazujemy informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady, jak przeciwdziałać tym zagrożeniom.

Czym jest cyberbezpieczeństwo?

Cyberbezpieczeństwo to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

Najczęstsze zagrożenia w cyberprzestrzeni

1. Ataki z użyciem szkodliwego oprogramowania – wirusy, ransomware, trojany.
2. Kradzież tożsamości i danych – wyłudzanie loginów, haseł i danych osobowych.
3. Blokowanie usług – ataki typu DDoS utrudniające dostęp do zasobów online.
4. Ataki socjotechniczne, np. phishing, czyli podszywanie się pod zaufane instytucje w celu wyłudzenia informacji.
5. Spam – masowe wysyłanie niechcianych lub niepotrzebnych wiadomości, często zawierających złośliwe linki.

Jak chronić siebie i swoje dane?

1. Stosuj zasadę ograniczonego zaufania do wiadomości e-mail, SMS, stron internetowych nakłaniających do podania danych osobowych oraz osób podających się za przedstawicieli firm lub instytucji, które żądają danych autoryzacyjnych albo nakłaniają do instalowania aplikacji zdalnego dostępu.
2. Nie ujawniaj danych osobowych, w tym danych autoryzacyjnych, dopóki nie ustalisz, czy rozmawiasz z osobą uprawnioną.
3. Instaluj aplikacje tylko ze znanych i zaufanych źródeł.
4. Nie otwieraj wiadomości e-mail i nie korzystaj z przesłanych linków od nadawców, których nie znasz.
5. Pamiętaj, że wiadomość e-mail może zostać sfałszowana; w razie wątpliwości sprawdź jej nagłówki i rzeczywiste źródło.
6. Porównaj adres nadawcy z adresami w polach „From” i „Reply-To” – rozbieżności mogą wskazywać na próbę oszustwa.
7. Szyfruj dane poufne wysyłane pocztą elektroniczną.
8. Zachowaj ostrożność wobec wiadomości SMS, zwłaszcza zawierających linki lub żądania podania danych.
9. Jeśli na podejrzanej stronie podałeś dane logowania lub doszło do włamania na konto – jak najszybciej zmień hasło.
10. Chroń komputer i urządzenia mobilne odpowiednim oprogramowaniem zabezpieczającym.
11. Aktualizuj system operacyjny, aplikacje użytkowe i oprogramowanie zabezpieczające.
12. Nie korzystaj z e-usług publicznych ani bankowości elektronicznej na niewspieranym, nieaktualnym systemie operacyjnym.
13. Korzystaj z różnych haseł do różnych usług elektronicznych.
14. Tam, gdzie to możliwe, stosuj uwierzytelnianie wieloskładnikowe (MFA).
15. Nie udostępniaj nikomu swoich haseł.

16. Pracuj na najniższych możliwych uprawnieniach użytkownika.
17. Wykonuj kopie bezpieczeństwa.
18. Skanuj podłączane urządzenia zewnętrzne.
19. Regularnie kontroluj stan bezpieczeństwa urządzeń i nośników danych.
20. Kontroluj uprawnienia instalowanych aplikacji.
21. Unikaj korzystania z otwartych sieci Wi-Fi do operacji wymagających podawania poufnych danych.
22. Przed podaniem poufnych danych sprawdź, czy połączenie ze stroną jest szyfrowane (HTTPS) i czy adres strony jest prawidłowy.
23. Zadbaj o bezpieczeństwo routera: ustaw silne hasła, aktualizuj oprogramowanie, stosuj aktualne standardy zabezpieczeń Wi-Fi i wyłącz niepotrzebne funkcje.
24. Szyfruj dyski, przede wszystkim komputerów i urządzeń przenośnych.

Gdzie szukać więcej informacji?

- CSIRT NASK / CERT Polska: https://www.cert.pl/
- Materiały OUCH!: https://cert.pl/ouch/
- Baza wiedzy o cyberbezpieczeństwie: https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo
- Cyberprofilaktyka NASK: https://cyberprofilaktyka.pl/publikacje/ Zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed nimi to wiedza potrzebna każdemu użytkownikowi komputera, smartfona i usług internetowych.

Opracował: Tomasz Piesiur – Inspektor Ochrony Danych, e-mail: abi@medialearning.pl