

ZASADY CYBERBEZPIECZEŃSTWA

Cyberbezpieczeństwo – podstawowe informacje i zasady

Realizując obowiązek informacyjny nałożony na podmioty publiczne na mocy **ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa**

(t.j. Dz. U. z 2024 r. poz. 1077), zgodnie z art. 22 ust. 1 pkt 4 tej ustawy, przedstawiamy podstawowe informacje dotyczące zagrożeń występujących w cyberprzestrzeni oraz zasad bezpiecznego korzystania z systemów teleinformatycznych.

Zgodnie z obowiązującymi przepisami **cyberbezpieczeństwo** oznacza odporność systemów informacyjnych na działania naruszające:

- poufność,
- integralność,
- dostępność,
- autentyczność przetwarzanych danych lub związanych z nimi usług.

I. Najczęściej występujące zagrożenia w cyberprzestrzeni

Do najczęściej spotykanych zagrożeń należą:

- kradzież tożsamości,
- kradzież, modyfikacja lub niszczenie danych,
- blokowanie dostępu do usług (odmowa usługi),
- spam (niechciana korespondencja elektroniczna),
- złośliwe oprogramowanie (malware, wirusy, robaki),
- ataki socjotechniczne (np. phishing),
- ataki z użyciem szkodliwego oprogramowania.

1. Phishing

Atak polegający na podszywaniu się pod zaufaną osobę lub instytucję w celu wyłudzenia danych, takich jak hasła czy dane logowania.

Ochrona: zachowanie ostrożności przy otwieraniu wiadomości e-mail, SMS i linków, weryfikacja nadawcy.

2. Malware (złośliwe oprogramowanie)

Oprogramowanie wykonujące działania bez wiedzy użytkownika, m.in. kradzież danych, przejęcie kontroli nad urządzeniem, udział w atakach sieciowych.

Ochrona: aktualne oprogramowanie antywirusowe oraz regularne aktualizacje systemu.

3. Ransomware

Atak polegający na zaszyfrowaniu danych i żądaniu okupu za ich odzyskanie.

Ochrona: kopie zapasowe danych, aktualne oprogramowanie, ochrona antywirusowa.

4. Man in the Middle

Przechwycenie komunikacji pomiędzy użytkownikiem a usługą (np. bankowością elektroniczną).

Ochrona: szyfrowanie transmisji danych, certyfikaty bezpieczeństwa SSL/TLS.

5. Cross-site scripting (XSS)

Wstrzyknięcie złośliwego kodu na stronę internetową w celu wywołania niepożądanego działania użytkownika.

Ochrona: korzystanie z legalnego i aktualnego oprogramowania.

6. DDoS (Distributed Denial of Service)

Atak polegający na przeciążeniu serwera dużą liczbą żądań.

Ochrona: zabezpieczenia po stronie dostawcy usług internetowych, firewall.

7. SQL Injection

Nieuprawniony dostęp do bazy danych przez luki w aplikacjach.

Ochrona: odpowiednie zabezpieczenia aplikacji i baz danych.

8. Malvertising

Złośliwe oprogramowanie rozpowszechniane poprzez reklamy internetowe.

Ochrona: filtry reklam, aktualne oprogramowanie zabezpieczające.

II. Podstawowe zasady ochrony przed zagrożeniami

Użytkownikom systemów teleinformatycznych zaleca się w szczególności:

1. Zachowanie ograniczonego zaufania wobec wiadomości e-mail, SMS i stron internetowych żądających podania danych.
 2. Nieujawnianie danych osobowych i autoryzacyjnych bez weryfikacji rozmówcy.
 3. Instalowanie aplikacji wyłącznie z zaufanych źródeł.
 4. Nieotwieranie linków i załączników od nieznanych nadawców.
 5. Weryfikowanie adresów e-mail nadawców oraz nagłówek wiadomości.
 6. Skanowanie pobranych plików programem antywirusowym.
 7. Szyfrowanie danych poufnych przesyłanych drogą elektroniczną.
 8. Korzystanie z aktualnego oprogramowania antywirusowego i systemowego.
 9. Regularne wykonywanie kopii zapasowych danych.
 10. Stosowanie silnych, unikalnych haseł oraz ich regularna zmiana.
 11. Korzystanie z uwierzytelniania dwuskładnikowego tam, gdzie to możliwe.
-

12. Unikanie otwartych sieci Wi-Fi.

13. Sprawdzanie certyfikatów SSL stron internetowych.

14. Zabezpieczenie routerów i sieci Wi-Fi.

15. Ochronę urządzeń mobilnych przed dostępem osób trzecich.

III. Podmioty zajmujące się cyberbezpieczeństwem

- **Ministerstwo Cyfryzacji** – <https://www.gov.pl/cyfryzacja>
- **CSIRT GOV** – <https://csirt.gov.pl>
- **CSIRT NASK / CERT Polska** – <https://cert.pl>

Zgłaszanie incydentów:

<https://incydent.cert.pl>