Zasady cyberbezpieczeństwa BIP

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, firewalle.

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 nagłówków 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

Jeśli chcesz, mogę dodatkowo:

- przygotować **krótszą wersję „dla obywatela”**,
- dopasować tekst **dokładnie pod strukturę BIP (HTML, sekcje)**,
- albo opracować **oddzielną zakładkę „Cyberbezpieczeństwo”** zgodną z WCAG 2.1 AA.

dopasować tekst dokładnie pod strukturę BIP

Poniżej masz **gotowy tekst dopasowany dokładnie do struktury BIP**, w formie **oficjalnej informacji publicznej**, przygotowany tak, aby można go było **wkleić bezpośrednio do zakładki BIP** (HTML/edytor treści).
Układ jest zgodny z praktyką urzędów, NASK i MC oraz czytelny dla obywatela.

Cyberbezpieczeństwo

Podstawa prawna

Na podstawie **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,
23 Wojskowy Szpital Uzdrowiskowo-Rehabilitacyjny SP ZOZ w Lądku-Zdroju realizuje obowiązek informacyjny w zakresie cyberbezpieczeństwa.

Czym jest cyberbezpieczeństwo?

Cyberbezpieczeństwo oznacza odporność systemów informacyjnych na działania naruszające:

- poufność danych,
- integralność danych,
- dostępność danych,
- autentyczność przetwarzanych informacji oraz usług świadczonych przy użyciu systemów teleinformatycznych.

Najczęściej występujące zagrożenia w cyberprzestrzeni

Do najczęściej występujących zagrożeń należą w szczególności:

- kradzież tożsamości,
- kradzież, modyfikacja lub niszczenie danych,

- blokowanie dostępu do usług,
- spam (niechciana korespondencja elektroniczna),
- złośliwe oprogramowanie (malware),
- ataki socjotechniczne (np. phishing),
- ataki typu DDoS.

Opis wybranych zagrożeń

Phishing

Podszywanie się pod instytucje lub osoby w celu wyłudzenia danych logowania, haseł lub danych osobowych.
Jak się chronić: nie klikać w podejrzane linki, weryfikować nadawcę wiadomości.

Malware

Złośliwe oprogramowanie instalowane bez wiedzy użytkownika, służące m.in. do kradzieży danych.
Jak się chronić: stosować aktualne oprogramowanie antywirusowe oraz aktualizacje systemu.

Ransomware

Zaszyfrowanie danych użytkownika i żądanie okupu za ich odzyskanie.
Jak się chronić: regularne kopie zapasowe danych, aktualne oprogramowanie.

Man in the Middle

Przechwycenie komunikacji pomiędzy użytkownikiem a usługą (np. bankowością elektroniczną).
Jak się chronić: korzystać z połączeń szyfrowanych i certyfikatów SSL.

DDoS

Atak polegający na przeciążeniu systemu dużą liczbą zapytań.
Jak się chronić: zabezpieczenia po stronie dostawców usług.

Podstawowe zasady bezpiecznego korzystania z Internetu

Zaleca się w szczególności:

1. Nieujawnianie danych osobowych i haseł osobom trzecim.
2. Ostrożność wobec wiadomości e-mail i SMS z linkami.
3. Instalowanie aplikacji wyłącznie z zaufanych źródeł.
4. Regularne aktualizowanie systemu operacyjnego i aplikacji.
5. Stosowanie silnych, unikalnych haseł.
6. Korzystanie z uwierzytelniania dwuskładnikowego.
7. Regularne wykonywanie kopii zapasowych danych.
8. Unikanie otwartych sieci Wi-Fi.
9. Sprawdzanie certyfikatów bezpieczeństwa stron internetowych.
10. Zabezpieczenie urządzeń mobilnych przed dostępem osób trzecich.

Gdzie szukać pomocy i informacji

- **Ministerstwo Cyfryzacji**
  https://www.gov.pl/cyfryzacja
- **CSIRT GOV**
  https://csirt.gov.pl
- **CERT Polska (NASK)**
  https://cert.pl

Zgłaszanie incydentów cyberbezpieczeństwa

Incydenty bezpieczeństwa można zgłaszać za pośrednictwem strony:

https://incydent.cert.pl