

Cyberbezpieczeństwo

Cyberbezpieczeństwo – najważniejsze informacje

W związku z realizacją zadań wynikających z **Ustawy o krajowym systemie cyberbezpieczeństwa**, przedstawiamy podstawowe informacje o zagrożeniach w sieci oraz sposobach skutecznej ochrony przed nimi.

Czym jest cyberbezpieczeństwo?

Cyberbezpieczeństwo to odporność systemów informatycznych na działania, które mogą naruszyć:

- **poufność danych** – ochrona przed nieuprawnionym dostępem,
- **integralność informacji** – pewność, że dane nie zostały zmienione lub sfałszowane,
- **dostępność usług** – możliwość ciągłego korzystania z systemów i zasobów,
- **autentyczność komunikacji** – pewność, że nadawca i odbiorca są tymi, za których się podają.

Zdarzenia zagrażające bezpieczeństwu nazywane są **incydentami**.

Najczęstsze zagrożenia w sieci

- **Phishing** – fałszywe wiadomości podszywające się pod banki, urzędy lub inne instytucje,
- **Kradzież danych i tożsamości**,
- **Szkodliwe oprogramowanie** (np. wirusy, trojany, ransomware),
- **Blokowanie dostępu do usług** (np. ataki DDoS),
- **Spam i niebezpieczne linki** prowadzące do zainfekowanych stron.

Jak się chronić?

- Regularnie **aktualizuj system i aplikacje**,
- Korzystaj z **oprogramowania antywirusowego i zapory sieciowej (firewall)**,
- **Nie otwieraj załączników ani linków** z nieznanymi źródłami,
- Sprawdzaj, czy odwiedzane strony posiadają **certyfikat bezpieczeństwa (https://)**,
- Twórz regularne **kopie zapasowe danych**,
- **Nie udostępniaj danych osobowych** w niesprawdzonych serwisach,
- **Szyfruj poufne informacje** wysyłane pocztą elektroniczną.

WAŻNE: Żaden bank ani urząd nigdy nie prosi o podanie loginu czy hasła drogą mailową.

Gdzie szukać więcej informacji?

Przydatne źródła:

- gov.pl – baza wiedzy w zakresie cyberbezpieczeństwa
- [CERT Polska – komunikaty](#)
- [CERT Polska – strona główna](#) (wejdź do bazy wiedzy i poszukaj przydatnych poradników)

Wyznaczenie osoby odpowiedzialnej za kontakty z krajowym systemem cyberbezpieczeństwa

Zespół Parków Krajobrazowych Województwa Śląskiego informuje, że zgodnie z art. 21 ustawy o krajowym systemie cyberbezpieczeństwa, został wyznaczony przedstawiciel odpowiedzialny za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.

Funkcję tę pełni pracownik odpowiedzialny za obsługę informatyczną w ZPKWŚ.

Administrator Systemów Informatycznych został zgłoszony do CSIRT NASK (Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy).

Adres kontaktowy: admin@zpk.com.pl

Wyznaczenie osoby kontaktowej ma na celu zapewnienie sprawnej komunikacji oraz współpracy z właściwymi organami i zespołami reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), zgodnie z obowiązującymi przepisami prawa.

ZPKWŚ podejmuje działania na rzecz zapewnienia wysokiego poziomu bezpieczeństwa systemów informatycznych, zgodnie z krajowymi i europejskimi standardami w zakresie cyberbezpieczeństwa.