

Cyberbezpieczeństwo

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 913 z późn. zm.)

Przedmiotem Ustawy, która weszła w życie z dniem 28 sierpnia 2018 r. jest organizacja krajowego systemu cyberbezpieczeństwa i określenie zadań oraz obowiązków podmiotów wchodzących w jego skład. Ustawa reguluje również kwestie sprawowania nadzoru i kontroli przestrzegania jej przepisów oraz tryb ustanawiania Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej. Treść ustawy określa zarówno podmioty będące uczestnikami krajowego systemu cyberbezpieczeństwa, jak i ich obowiązki.

Realizując zadania wynikające z Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Urząd Gminy w Wodyniach przekazuje dostęp do materiałów zawierających wiedzę o zagrożeniach cyberbezpieczeństwa i stosowaniu skutecznych sposobów zabezpieczania się przed tymi zagrożeniami.

Zachęcamy do śledzenia informacji publikowanych w szczególności na stronach zespołów reagowania na incydenty bezpieczeństwa informatycznego, np.:

1. na stronie internetowej pierwszego w Polsce zespołu reagowania na incydenty informatyczne CERT.PL: <https://www.cert.pl/>
2. przygotowanych przez CERT.PL publikacji: <https://www.cert.pl/publikacje/>
3. cyklicznego, bezpłatnego biuletynu porad bezpieczeństwa dla użytkowników komputerów OUCH!: <https://www.cert.pl/ouch/>

Zgłaszanie incydentów bezpieczeństwa: <https://incydent.cert.pl/>

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

Rodzaje cyberataków

1. **Malware**, czyli złośliwe oprogramowanie, które bez zgody i wiedzy użytkownika wykonuje na komputerze działania na korzyść osoby trzeciej.
2. **Man in the Middle** jest rodzajem ataku polegającym na uczestniczeniu osoby trzeciej np. w transakcji pomiędzy sklepem internetowym a klientem. Celem takich ataków jest przechwycenie informacji lub środków pieniężnych (np. uzyskanie danych niezbędnych do logowania w systemie bankowości elektronicznej).
3. **Cross site scripting** polegający na umieszczeniu na stronie internetowej specjalnego kodu, którego kliknięcie przez użytkownika powoduje przekierowanie na inną stronę internetową (np. na witrynę konkurencji).
4. **Phishing** jest to atak polegający na dokonywaniu prób przejęcia haseł służących użytkownikowi do logowania na np. portalach społecznościowych, do których dostęp umożliwia atakującym uzyskanie danych osobowych użytkownika.
5. **DDoS**, czyli atak, którego celem jest zablokowanie możliwości logowania użytkownika na stronę internetową poprzez jednoczesne logowanie na tę samą stronę się wielu użytkowników. Wywoływany w ten sposób sztuczny ruch wzmacnia zainteresowanie użytkowników np. produktem dostępnym w sklepie internetowym.

6. **SQL Injection** jest atakiem polegającym na wykorzystywaniu przez przestępców luk występujących w zabezpieczeniach np. aplikacji i pozwalającym na uzyskanie przez osoby nieuprawnione danych osobowych.
7. **Ransomware** to rodzaj ataku, którego celem jest przejęcie i zaszyfrowanie danych użytkownika po to aby w następnym kroku udostępnić te same dane użytkownikowi pod warunkiem wniesienia przez niego "okupu".
8. **Malvertising** pozwala przestępcom na dotarcie do użytkowników przeglądających zaufane strony internetowe poprzez nośniki jakimi są udostępniane na stronach internetowych reklamy, a następnie na instalowanie bez wiedzy i zgody użytkownika złośliwego oprogramowania na urządzeniach użytkownika.



Dodatkowo pamiętaj o kilku podstawowych zasadach:

1. Chronić dostęp do urządzenia hasłem/pinem/kartą.
2. Pracuj na najniższych możliwych uprawnieniach.
3. Instaluj aktualizacje bezpieczeństwa.
4. Korzystaj z różnych haseł do różnych serwisów
5. Nie udostępniaj nikomu swoich haseł.
6. Regularnie zmieniaj hasła.
7. Włącz blokowanie ekranu.
8. Korzystaj z różnych haseł do różnych serwisów.
9. Używaj zawsze aktualnego oprogramowania antywirusowego.
10. Nie używaj bez skanowania w komputerach podłączonych do sieci pendriva, który był podłączony do innego komputera
11. Szyfruj twarde dyski komputera, pendriva.
12. Wykonuj kopie bezpieczeństwa (poza siedzibą).
13. Szyfruj kopie bezpieczeństwa.