

Biuletyn Informacji Publicznej

Urząd Gminy Sławoborze

<https://bip.slawoborze.pl/arttykul/177/363>

Cyberbezpieczeństwo

Zgodnie z ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa podmioty publiczne są częścią Krajowego Systemu Cyberbezpieczeństwa.

Art. 22 ust. 1 pkt 4 ww. ustawy zobowiązuje podmioty publiczne do zapewnienia osobom, na rzecz których zadanie publiczne jest realizowane, dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, w szczególności przez publikowanie informacji w tym zakresie na swojej stronie internetowej.

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

Zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie sposobów zabezpieczania się przed zagrożeniami, to wiedza niezbędna każdemu użytkownikowi komputera, smartphona czy też usług internetowych.

Przykładowe zagrożenia cyberbezpieczeństwa:

1. Kradzież tożsamości - wyłudzenia, modyfikacje bądź niszczenie danych osobowych,
2. Spam - niechciane lub niepotrzebne wiadomości elektroniczne,
3. Ataki z użyciem szkodliwego oprogramowania:
 - a) malware – to rodzaj złośliwego oprogramowania, którego celem jest uszkodzenie lub wykorzystanie dowolnego urządzenia, aplikacji, usługi lub elementów sieci. Ataki typu malware są najczęściej rozpowszechniane przez:
 - załączniki poczty elektronicznej,
 - fałszywe reklamy,
 - zainfekowane aplikacje lub strony internetowe,
 - linki w smsach i mmsy multimedialne,

- b) trojan - program, który podszywa się pod legalny, godny zaufania plik. Jeżeli trojan znajdzie się na urządzeniu, hakerzy mogą go wykorzystać do uzyskania dostępu do sieci, szpiegowania, usuwania, modyfikacji i przechwycenia danych,
- c) robaki - to jeden z najczęstszych typów złośliwego oprogramowania. Aktywacja robaków następuje bez świadomości użytkownika, a ich replikacja odbywa się bez wprowadzania zmian w plikach i danych. Robaki rozprzestrzeniają się poprzez luki w oprogramowaniu lub ataki phishingowe. Gdy robak zainstaluje się w pamięci komputera, zaczyna infekować całe urządzenie, a w niektórych przypadkach nawet całą sieć,
4. Blokowanie dostępu do usług,
5. Ataki socjotechniczne - wyłudzenia poufnych informacji przez podszywanie się pod godną zaufania osobę lub instytucję.

Przykładowe zabezpieczenia przed ww. zagrożeniami:

1. Aktualizuj system operacyjny i aplikacje,
2. Używaj oprogramowania przeciwwirusowego,
3. Nie odpowiadaj na e-maile, sms z prośbą o podanie twojego hasła lub loginu,
4. Nie korzystaj ze stron internetowych, poczty elektronicznej czy portali społecznościowych, które nie mają ważnego certyfikatu SSL.
5. Nie wysyłaj w e-mailach żadnych poufnych informacji w formie otwartego tekstu. Zabezpieczaj maile zaszyfrowaniem, hasło przekazuj w sposób bezpieczny.
6. Nie zostawiaj swoich danych osobowych w niesprawdzonych serwisach i na stronach internetowych,

Zapoznaj się z informacjami:

1. Zestaw porad bezpieczeństwa dla użytkowników komputerów prowadzony na witrynie internetowej CSIRT NASK – Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym: <https://www.cert.pl/ouch/>
2. Poradniki na witrynie internetowej Ministerstwa Cyfryzacji: <https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo>
3. Publikacje z zakresu cyberbezpieczeństwa: <https://www.cert.pl/>

Metryczka

| | |
|-------------------------------------|---------------------|
| Wytworzył: | Marek Nikipierowicz |
| Data wytworzenia: | 08.07.2022 |
| Opublikował w BIP: | Marek Nikipierowicz |
| Data opublikowania: | 20.07.2022 11:51 |
| Ostatnio zaktualizował: | Marek Nikipierowicz |
| Data ostatniej aktualizacji: | 20.07.2022 11:53 |
| Liczba wyświetleń: | 640 |