Gmina Chełmno Oficjalny portal informacyjny

Adres artykułu: https://gmina-chelmno.pl/artykul/202-7843-cyberbezpieczenstwo

CYBERBEZPIECZEŃSTWO

Cyberbezpieczeństwo

Celem zapewnienia Państwu bezpiecznego korzystania z usług opartych o systemy informacyjne, urząd sugeruje zapoznanie się z poniższymi informacjami.

W dzisiejszych czasach, wraz z rozwojem ilości usług opartych o systemy informacyjne, rośnie liczba zagrożeń naruszających tzw. cyberbezpieczeństwo. Jako cyberbezpieczeństwo należy rozumieć odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Krajowy System Cyberbezpieczeństwa powstał celem ograniczenia możliwości występowania oraz ograniczenia wpływu incydentów związanych z cyberbezpieczeństwem. Jego zadaniem jest koordynacja działań, a przede wszystkim skuteczna wymiana informacji na temat pojawiających się zagrożeń pomiędzy podmiotami. Działania te mają skutecznie ograniczyć skutki zdarzeń, które mogą mieć wpływ na ograniczenie świadczenia usług kluczowych, utratę danych oraz straty finansowe użytkowników systemów.

W związku z powyższym, celem szerzenia wiedzy i świadomości użytkowników, korzystających z usług świadczonych przez Urząd, opartych o systemy informacyjne, zachęcamy do zapoznania się z licznymi informacjami dostępnymi na poniższych stronach WWW:

- cert.pl
- cert.pl/ouch
- dyzurnet.pl
- it-szkola.edu.pl

https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo

Dodatkowo przypominamy o zasadach, których przestrzeganie zapewnia minimalny wymagany poziom bezpieczeństwa cybernetycznego.

1. Ochrona danych osobowych oraz finansowych. Nie należy podawać swoich danych na nieznanych stronach internetowych oraz przesyłać ich za pomocą popularnych komunikatorów lub mediów społecznościowych.

2. Zabezpieczenie urządzeń mobilnych. Laptopy, smartfony i tablety należy zabezpieczać przy pomocy PINu, odcisku palca lub innych metod oferowanych przez producentów urządzeń. Wskazane jest korzystanie z urządzeń znanych producentów, zapewniających ciągłe poprawki i aktualizacje do oficjalnego oprogramowania. Nie należy instalować aplikacji nieznanych producentów, bez autoryzacji sklepów z aplikacjami. Aplikacje nieznanych producentów mogą prowadzić do wycieku danych. Nie należy udostępnić swoich urządzeń mobilnych nieznanym osobą oraz pozostawiać ich bez osobistego nadzoru. Nie należy podłączać nieznanych nośników danych, które mogą zawierać zagrożenia w postaci szkodliwego oprogramowania.

3. Bezpieczne korzystanie z sieci Internet. Nie należy ujawniać swoich danych na stronach internetowych, jeśli nie jest to konsekwencją celowego działania użytkownika w procesie np. realizacji zamówienia.

4. Niebezpieczne jest logowanie się do systemów z danymi wrażliwymi za pomocą publicznych sieci Wi-Fi.

5. Dane logowania nie należy uzupełniać na stronach, które nie chronią ich w trakcie przesyłania do serwera – dane powinny być szyfrowane (https).

6. Nie należy otwierać wiadomości E-mail od nadawców nieznanych. Korespondencję, która wzbudza podejrzenia należy potwierdzać u źródła za pomocą innych kanałów komunikacji np. telefonicznie.

Metryczka

Opublikował w BIP:	Jarosław Zima
Data opublikowania:	26.04.2022 16:01
Ostatnio zaktualizował:	Jarosław Zima

Data ostatniej aktualizacji:	21.12.2023 13:39
Liczba wyświetleń:	293