I. Cyberbezpieczeństwo

W związku z obowiązkiem nałożonym przez przepisy ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tj. Dz.U. z 2020 r., poz. 1369) przedstawiamy Państwu podstawowe informacje dotyczące cyberbezpieczeństwa, jego zagrożeń i sposobów zabezpieczenia się przed nimi.

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

Wszelkie zdarzenia mające lub mogące mieć niekorzystny wpływ na cyberbezpieczeństwo nazywane są **incydentami.**

Najczęściej występujące incydenty, czyli zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo to:

- **Phishing** – metoda oszustwa, w której cyberprzestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji, takich jak danych logowania czy danych karty bankowej;

- **Wiadomości SPAM** – niechciane lub niepotrzebne wiadomości elektroniczne, mogące zawierać odnośniki do szkodliwego oprogramowania;

-

Kradzież tożsamości;

-

Porada UODO;

-

Porada MSWiA.

-

Przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp.

-

Szkodliwe oprogramowanie.

Należy pamiętać, że najlepszym sposobem na ustrzeżenie się przed negatywnymi skutkami incydentów jest ochrona prewencyjna.

Poniżej przedstawiamy przykładowe sposoby na uniknięcie zagrożeń związanych z korzystaniem z cyberprzestrzeni:

-

Instalacja, użytkowanie i bieżące aktualizowanie oprogramowania antywirusowego;

-

Aktualizowanie systemu operacyjnego urządzenia oraz aplikacji na nim zainstalowanych;

-

Sprawdzanie plików pobranych z Internetu za pomocą programu antywirusowego;

-

Korzystanie ze stron internetowych posiadających ważny certyfikat bezpieczeństwa;

-

Regularne skanowanie komputera i sprawdzanie procesów sieciowych;

-

Każdorazowa weryfikacja adresu nadawcy wiadomości e-mail;

-

Niewysyłanie danych osobowych, logowania, karty kredytowej w niezabezpieczonej treści wiadomości e-mail;

-

Unikanie odwiedzin stron zawierających darmowe pliki muzyczne, obrazy, filmy;

-

Regularne tworzenie kopii zapasowych ważnych danych;

-

Baczne obserwowanie i czytanie komunikatów pojawiających się na ekranie komputera.

II. Cyberhigiena dla każdego.

III. Podarnik bezpieczny pracownik w sieci

Zachęcamy do zapoznania się z treściami zawartymi na stronie Ministerstwa Cyfryzacji w celu uzyskania dodatkowych szczegółowych informacji dotyczących cyberbezpieczeństwa.

IV. Obowiązki podmiotu publicznego.

- Wyznaczenie osoby kontaktowej do spraw cyberbezpieczeństwa, która będzie kontaktować się z organami właściwymi do spraw cyberbezpieczeństwa (CSIRT);
- Zapewnianie dostępu do wiedzy w zakresie cyberbezpieczeństwa, obsługa i zgłaszanie incydentów do właściwego CSIRT;
- Kontakt do osoby wyznaczonej:
  Izabela Jaszczanin
  Tel. 89 521 31 62
  E-mail: izabela.jaszczanin@olsztyn.so.gov.pl

V. Anonimowe zgłaszanie incydentów

Wiele osób zastanawia się nad tym, czy warto reagować? Czy warto sobie i innym zawracać głowę? Odpowiedź jest jedna – Tak, warto! Doświadczenia zespołu Dyżurnet.pl, Policji, Interpolu pokazują, że każda reakcja na niepokojące treści w sieci jest ważna. Czasami pojedyncze zgłoszenie jest brakującym puzzlem większej układanki, z której wyłania się obraz krzywdzonego dziecka. To jedno zgłoszenie może wiele zmienić. Jak to działa?

Poniżej znajduje się formularz zgłoszeniowy, za pomocą którego można anonimowo, łatwo i szybko zgłosić nielegalne i szkodliwe treści, na które trafimy w sieci. Zgłoszenie natychmiast trafia do zespołu, który poddaje je wstępnej klasyfikacji. Priorytetowo obsługiwane są zgłoszenia dotyczące treści CSAM, czyli seksualnego wykorzystania dziecka. Pozostałe kategorie zgłoszeń to: twarda pornografia, rasizm i ksenofobia, inne nielegalne treści.

Następnie zespół w zależności od tego, gdzie znajduje się serwer, z którego pochodzą nielegalne treści, zgłasza sprawę do Komendy Głównej Policji lub do innego zespołu reagującego zrzeszonego w Stowarzyszeniu INHOPE oraz do Interpolu. Szybka reakcja Policji i Interpolu również są bardzo ważne do tego, aby zabezpieczyć dane techniczne serwerów, plików. Jest to istotne dlatego, iż treści CSAM są szybko usuwane z sieci, a to uniemożliwia skuteczne przeciwdziałanie dalszemu wykorzystywaniu dziecka, zatrzymaniu nielegalnego procederu.

ZGŁOŚ INCYDENT

VI. Podmioty zajmujące się cyberbezpieczeństwem

- MINISTERSTWO CYFRYZACJI;
- CERT POLSKA;
- CSRiT GOV;

- CSRiT NASK;
- CSRiT MON;
- NIEBEZBPIECZNIK;
- ZAUFANA TRZECIA STRONA
- LEGALNIE W SIECI;
- CYBERDEFENCE24;
- CYBERRESCCUE
- NOMORERANSOM

VII. Komunikaty