Cyerbezpieczeństwo

Realizując zadania wynikające z ustawy o krajowym systemie cyberbezpieczeństwa przekazujemy Państwu dostęp do informacji pozwalających na zrozumienie zagrożeń cyberbezpieczeństwa, oraz jak stosować skuteczne sposoby zabezpieczenia się przed tymi zagrożeniami.

Cyberbezpieczeństwo, w myśl ustawy (tj. Dz.U. z 2020 r., poz. 1369) 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.

Najważniejsze informacje dotyczące najczęściej występujących zagrożeń, incydentów oraz sposoby ochrony przed nimi. Zagrożenia, incydenty typu:

- Phishing

  Przestępcy tworzą fałszywe strony Internetowe, żeby wyłudzić Twoje dane (loginy i hasła). Najczęściej wysyłają maile zawierające odnośniki do tych stron.

  Jak się chronić?
  Dokładnie weryfikuj adres witryny zanim się na niej zalogujesz. Nie wpisuj swojego loginu i hasła na podejrzanych stronach internetowych.

- Malware/ ransomware Często stosowane są ataki z użyciem szkodliwego oprogramowania (malware, ransomware itp.), hakerzy mogą wysyłać złośliwe oprogramowanie za pośrednictwem e-mail, dołączonego do e-mail załącznika.

  Jak się chronić?
  Nie otwieraj podejrzanych wiadomości oraz załączników, ponieważ w przypadku instalacji złośliwego oprogramowania na Twoim urządzeniu, hakerzy mogą przejąć dostęp np. do konta w Twoim banku, zablokować wszystkie pliki znajdujące się w komputerze uniemożliwiając ich otwarcie.

- Vishing

  Przestępcy mogą do Ciebie zadzwonić i podawać się za pracownika Szpitala, instytucji np. SANEPID, Policji, Twojego przełożonego i prosić Cię o przekazanie Twojego loginu, hasła, nr PESEL, nr dowodu osobistego. Podanie tych danych może skutkować kradzieżą Twojej tożsamości, umożliwieniem przestępcy zalogowania się do Systemu.

  Jak się chronić?
  Nigdy nie podawaj swoich danych dopóki nie upewnisz się z kim rozmawiasz.

- Adware

  Wyskakujące okienka, reklamy najeżdżające z góry, z boku i z dołu ekranu, przeszkadzające, utrudniające dotarcie do właściwego tekstu, a nawet przekierowujące na niechciane strony – znasz to? Nawet jeśli wiele razy będziesz próbował zamknąć je wszystkie, one i tak powrócą, niczym rój komarów podczas wieczornego spaceru. Niejednokrotnie zrezygnujesz z dotarcia do interesującej Cię treści i zamkniesz przeglądarkę. Nie ma się co dziwić – właśnie zostałeś zaatakowany przez adware.

Jak się chronić?
Nie instaluj darmowego oprogramowania czytaj dokładnie regulamin przed zainstalowaniem oprogramowania, uważaj na fałszywe linki wyświetlające się na stronach, które odwiedzasz. Po kliknięciu odpowiedzi mogą przekierowywać do ściągnięcia oprogramowania adware, zainstaluj program blokujący pojawiające się reklamy typu AdBlock, zainstaluj program antywirusowy

- Worms

  Robak komputerowyWorms jest programem komputerowym samoreplikującym się. Uznać można, że jest pod wieloma względami podobny do wirusa komputerowego. Zasadniczą różnicą, że wirus potrzebuje pliku w roli nosiciela, zaś robak pod tym względem jest samodzielny. Worms rozprzestrzenia się w sieciach, które podłączone są do jednego zarażonego sprzętu. Dzieje się tak ponieważ wykorzystuje luki w programach operacyjnych, a często bazuje na naiwności użytkownika. Robak niszczy pliki, wysyła spam, lub pełni rolę konia trojańskiego.

  Jak się chronić?
  Niezbędne posiadanie jest programu antywirusowego

- Keylogger

  Zwany jest również rejestratorem klawiszy. Może być to rodzaj oprogramowania szkodliwego, które służy do zabierania haseł i danych. Niekiedy jest oprogramowaniem pożądanym instalowanym przez pracodawcę dla śledzenia aktywności pracownika.

  Jak się chronić?
  Niezbędne posiadanie programu antywirusowego który monitoruje pracę komputera, smartfonu

Dobre praktyki

- Zasada ograniczonego zaufania. Stosowanie zasady ograniczonego zaufania i zwiększonej ostrożności pozwoli Państwu zmniejszyć ryzyko zainfekowania swojego komputera lub utraty danych.
- Aktualizacja programów ochrony antywirusowej. Pamiętamy o zainstalowaniu i aktualizowaniu programu ochrony przed złośliwym oprogramowaniem.
- Korzystanie wyłącznie z legalnego oprogramowania.
- Nie korzystanie z sieci publicznych, jeżeli logujesz się do serwisów np. bankowego, poczty elektronicznej.
- Nie otwieraj podejrzanych e-maili oraz załączników. Zwracaj szczególną uwagę na załączniki posiadające kilka rozszerzeń plików jednocześnie np. faktura.pdf.zip, dokument.jar.doc.
- Nie korzystaj ze stron, które nie mają ważnego certyfikatu (np. brak protokołu https) chyba, że masz stuprocentową pewność z innego źródła, że strona taka jest bezpieczna.
- Nie zostawiaj swoich danych osobowych w niesprawdzonych serwisach i na stronach, zawsze czytaj dokładnie Regulaminy i Polityki, weryfikuj na co wyrażasz zgodę.
- Nie wysyłaj e-mailem poufnych danych bez ich szyfrowania.
- Pamiętaj, że Szpital, bank, czy urząd nie wysyła e-maili do swoich pacjentów/klientów /interesantów z prośbą o podanie hasła lub loginu do jakichkolwiek systemów w celu ich weryfikacji.
- Regularnie aktualizuj system operacyjny i zainstalowane oprogramowanie na Twoim komputerze.
- Aplikacje i programy pobieraj wyłącznie z oficjalnych źródeł np. strony producenta oprogramowania.

Dodatkowe środki bezpieczeństwa

- Blokuj ekran swojego urządzenia po odejściu od urządzenia (np. hasło, PIN).

- Włącz ustawienia blokady ekranu Twojego urządzenia po okresie bezczynności np. 5 min .
- Wpisując swoje hasło, pin, login zweryfikuj, czy nikt Cię nie nagrywa lub nie widzi tego, co wpisujesz.
- Nie udostępniaj nikomu swojego loginu i hasła do systemu, poczty elektronicznej itp..
- Unikaj stosowania haseł, które można łatwo z Tobą powiązać.
- Hasło powinno mieć co najmniej 8 znaków w tym litery, cyfry i znaki specjalne.
- Nie zapisuj haseł na kartkach, w notatniku
- Stosuj różne hasła w różnych systemach.
- Unikaj logowania do systemów z cudzych urządzeń.
- Nie zapisuj haseł w pamięci przeglądarki internetowej.
- Przed sprzedażą / oddaniem urządzenia innej osobie, usuń z niego wszystkie dane, najlepiej pozostaw dysk twardy u siebie. Dobrym rozwiązaniem jest wielokrotne nadpisanie danych na dysku przy zastosowaniu specjalistycznego oprogramowania (nie stosuj nadpisywania do dysków typu SDD).
- Jeżeli masz taką możliwość korzystaj z nakładek prywatyzujących na monitor.
- Smartfony i tablety coraz częściej zastępują inne urządzenia osobiste. Pamiętaj, że podobnie jak domowe komputery, nasze urządzenia mobilne wymagają odpowiedniej ochrony.
- Instaluj aktualizacje aplikacji i systemu operacyjnego w swoim urządzeniu mobilnym.
- Pobieraj i instaluj aplikacje wyłącznie z oficjalnych sklepów z aplikacjami.
- Nie uruchamiaj linków z wiadomości SMS lub e-mail, jeśli nie masz pewności, że pochodzą z bezpiecznego i zaufanego źródła.
- Jeżeli nie korzystasz w danej chwili z Wi-Fi lub Bluetooth, wyłącz je.
- Bezpieczne korzystanie z poczty elektronicznej.
    - Adresaci poczty. Zwracamy szczególną uwagę na poprawność adresata (adresatów) wiadomości elektronicznych.
    - Nadawca wiadomości. Zwracamy szczególna uwagę na nadawcę wiadomości.
    - Nie klikamy na linki umieszczone w załączniku poczty.
    - W przypadku przesyłania ważnych (wrażliwych) wiadomości stosujemy mechanizmy szyfrowania (hasło przesyłane innym kanałem).
- Dane osobowe. Ograniczamy do minimum podawanie swoich danych osobowych.

Przydatne linki

- Baza wiedzy – Serwis Rzeczypospolitej Polskiej
  https://www.gov.pl/web/baza-wiedzy/aktualnosci

- Akty prawne
    - **Ustawa o Krajowym Systemie Cyberbezpieczeństwa**
      Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 1560)
    - **Usługi kluczowe**
      Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz. U. poz. 1806)
    - **Incydenty poważne**
      Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz. U. poz. 2180)
    - **Dokumentacja**
      Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. poz. 2080)
    - **Warunki organizacyjne**
      Rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz.U. 2019 poz. 2479)

- Krajowy System Cyberbezpieczeństwa
  https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa-

- **Koordynatorzy obsługi incydentów**
  - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego
    https://csirt.gov.pl/
  - NASK
    https://www.nask.pl/pl/dzialalnosc/cyberbezpieczenstwo/3284,Cyberbezpieczenstwo.html
- portale zawierające poradniki i porady z zakresu cyberbezpieczeństwa:
- stojpomyslpolacz.pl, www.gov.pl/web/cyfryzacja/edukacja/, www.cert.pl, cyberpolicy.nask.pl,

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