CYBERBEZPIECZEŃSTWO

W związku z zadaniami wynikającymi z ustawy o krajowym systemie cyberbezpieczeństwa przedstawiamy podstawowe informacje dotyczące cyberbezpieczeństwa, zagrożeń i sposobów zabezpieczenia się przed nimi.

Cyberbezpieczeństwo 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 *zagrożeniami lub incydentami.*

Zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie sposobów zabezpieczania się przed zagrożeniami to wiedza niezbędna każdemu użytkownikowi komputera, smartphona czy też usług internetowych.
Należy pamiętać, że najlepszym sposobem na ustrzeżenie się przed negatywnymi skutkami zagrożeń jest działalność zapobiegawcza.

Najpopularniejsze zagrożenia w cyberprzestrzeni to:

- ataki socjotechniczne (przykładowo phishing, czyli metoda polegająca na wyłudzaniu poufnych informacji przez podszycie się pod godną zaufania osobę lub instytucję);
- kradzieże (wyłudzenia), modyfikacje lub niszczenie danych;
- kradzieże tożsamości;
- ataki z użyciem szkodliwego oprogramowania (malware, wirusy, robaki, itp.);
- blokowanie dostępu do usług;
- spam (niechciane lub niepotrzebne wiadomości elektroniczne mogące zawierać odnośniki do szkodliwego oprogramowania).

Przykładowe sposoby zabezpieczenia się przed zagrożeniami:

- aktualizowanie systemu operacyjnego i aplikacji bez zbędnej zwłoki;
- instalacja i użytkowanie oprogramowania przeciw wirusom i spyware. Najlepiej stosować ochronę w czasie rzeczywistym;
- aktualizacja oprogramowania antywirusowego oraz bazy danych wirusów;
- sprawdzanie plików pobranych z Internetu za pomocą programu antywirusowego;
- pamiętanie o uruchomieniu firewalla;
- nie otwieranie plików nieznanego pochodzenia;
- korzystanie ze stron banków, poczty elektronicznej czy portali społecznościowych, które mają ważny certyfikat bezpieczeństwa, chyba, że masz stuprocentową pewność z innego źródła, że strona taka jest bezpieczna;
- regularne skanowanie komputera i sprawdzanie procesów sieciowych. Jeśli się na tym nie znasz poproś o sprawdzenie kogoś, kto się zna. Czasami złośliwe oprogramowanie nawiązujące własne połączenia z Internetem, wysyłając twoje hasła i inne prywatne dane do sieci. Może również zainstalować się na komputerze mimo dobrej ochrony;
- nie używanie niesprawdzonych programów zabezpieczających czy też do publikowania własnych plików w Internecie (mogą one np. podłączać niechciane linijki kodu do źródła strony);
- regularne wykonywanie kopii zapasowych ważnych danych;
- staranie się aby nie odwiedzać zbyt często stron, które oferują niesamowite atrakcje (darmowe filmiki, muzykę, albo łatwy zarobek przy rozsyłaniu spamu) – często na takich stronach znajdują się ukryte wirusy, trojany i inne zagrożenia;
- nie zostawianie danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie ma się absolutnej pewności, że nie są one widoczne dla osób trzecich oraz nie wysyłanie w wiadomościach e-mail żadnych poufnych danych w formie otwartego tekstu przykładowo dane powinny być zabezpieczone hasłem i zaszyfrowane. Hasło najlepiej przekazuj w sposób bezpieczny przy użyciu innego środka komunikacji;
- należy pamiętać, że żaden bank czy Urząd nie wysyła e-maili do swoich klientów/interesantów prośbą o podanie hasła lub loginu w celu ich weryfikacji.
- **zgłaszanie incydentów poprzez stronę CERT lub zgłoszenie podejrzanych wiadomości SMS poprzez ich przekierowanie na bezpłatny nr tel. 8080**

CERT Polska to pierwszy powstały w Polsce zespół reagowania na incydenty. Działa w strukturach NASK – Państwowego Instytutu Badawczego, prowadzącego działalność naukową, krajowy rejestr domen .pl i dostarczającego zaawansowane usługi teleinformatyczne.
Warto zajrzeć: https://cert.pl/
Znajdziemy tu m.in. **OUCH!** – czyli cykliczny, darmowy zestaw porad bezpieczeństwa dla użytkowników komputerów. Każde wydanie zawiera krótkie, przystępne przedstawienie wybranego zagadnienia bezpieczeństwa komputerowego wraz z listą wskazówek jak można chronić siebie, swoich najbliższychi swoją organizację, m.in. Bezpieczeństwo kont bankowych, Utylizacja urządzeń mobilnych czy Zasady bezpiecznych rozmów

Liczne kampanie informacyjne z zagadnień cyberbezpieczeństwa mają na celu mają m.in.:

- Podnoszenie poziomu świadomości społecznej w obszarze cyberbezpieczeństwa poprzez informowanie o zagrożeniach i sposobach radzenia sobie z nimi.
- Promowanie zachowań służących poprawie bezpieczeństwa internautów, ich rodzin i otoczenia.
- Kształtowanie odpowiedzialnych postaw wszystkich użytkowników sieci.
- Zaangażowanie sektora publicznego i prywatnego w działania promujące cyberbezpieczeństwo.
- Budowanie środowiska sprzyjającego wymianie dobrych praktyk i edukacji z zakresu cyberbezpieczeństwa.

Baza wiedzy o cyberberpieczeństwie:
https://www.gov.pl/web/baza-wiedzy/aktualnosci
https://www.nask.pl/pl/dzialalnosc/cyberbezpieczenstwo/3284,Cyberbezpieczenstwo.html
https://www.cyfrowobezpieczni.pl/

CYBERBEZPIECZEŃSTWO - Co możesz zrobić?

ZADBAJ O AKTUALIZACJE I BEZPIECZEŃSTWO URZĄDZEŃ

- **Korzystaj z aktualnego oprogramowania:** Regularnie aktualizuj system operacyjny, program antywirusowy, przeglądarkę internetową. Dzięki aktualizacjom łatwiej ustrzeżesz się przed szkodliwym oprogramowaniem innymi zagrożeniami obecnymi w sieci.
- **Włącz aktualizacje automatyczne:** Wiele aplikacji oferuje możliwość automatycznego pobierania aktualizacji, w celu ochrony przed nowymi zagrożeniami. Skorzystaj z tego rozwiązania wszędzie tam, gdzie to możliwe.
- **Chroń urządzenia podłączane do sieci:** Nie tylko komputery, ale także smartfony, tablety i inne podłączane do Internetu urządzenia, potrzebują ochrony przed wirusami i złośliwym oprogramowaniem.
- **Skanuj przed użyciem:** Nie podłączaj do komputera nośników, których pochodzenie nie jest Ci znane. Dyski zewnętrzne, pendrive'y, czy inne nośniki danych mogą być niebezpieczne (zainfekowane przez szkodliwe oprogramowanie). Zanim otworzysz ich zawartość skorzystaj ze skanera antywirusowego.

ZABEZPIECZ DOSTĘP DO POSIADANYCH INFORMACJI

- **Dwuskładnikowe uwierzytelnianie:** Zadbaj o swoje konta w sieci. Logowanie oparte wyłącznie o nazwę użytkownika i hasło nie jest wystarczająco bezpieczne (szczególnie w przypadku konta e-mail, portalu społecznościowego czy bankowości internetowej). Aktywuj weryfikację tożsamości opartą o dodatkowy składnik, np. kod SMS, token, czy klucz sprzętowy.
- **Stwórz mocne hasło:** Dobre hasło składa się przynajmniej z 12 znaków. Skup się na pozytywnych zdaniach lub zwrotach o których lubisz myśleć i które łatwo zapamiętasz (np. „Kocham miasto muzyki"). Na wielu stronach internetowych, możesz przy wprowadzaniu hasła używać spacji.
- **Jedno hasło, jedno konto:** Jeżeli chcesz utrudnić działania przestępcom, dla każdego konta przypisz oddzielne hasło. Niezbędne minimum, to rozdzielenie kont używanych do pracy i celów prywatnych. Zadbaj o silne hasło do najistotniejszych serwisów (bankowość, poczta elektroniczna, portale społecznościowe)
- **Przechowuj bezpiecznie:** Każdy może zapomnieć swojego hasła. W celu ułatwienia nam życia stworzono aplikacje zwane menadżerami haseł. Służą do bezpiecznego przechowywania danych dostępowych. Możesz nich korzystać. Jeżeli zapisałeś hasło na kartce (lepiej tego nie rób), postaraj się umieścić ją w bezpiecznym miejscu, z dala od komputera.

KORZYSTAJ ROZWAŻNIE

- **Zatrzymaj się, jeśli masz wątpliwości:** Linki i załączniki w wiadomościach e-mail, spreparowane posty mediach społecznościowych oraz reklamy - to częste metody używane przez przestępców w celu kradzieży danych. Jeżeli wydają Ci się podejrzane, po prostu je zignoruj. Nawet, jeżeli źródło wygląda na zaufane.
- **Uważaj na hotspoty Wi-Fi:** Ogranicz aktywność w publicznie dostępnych sieciach Wi-Fi. Używając poza domem kluczowych serwisów (poczta e-mail, bankowość internetowa, portale społecznościowe) bezpieczniej

będzie użyć własnego modemu LTE lub połączenia VPN. Pamiętaj o wyłączaniu transmisji Wi-Fi i Bluetooth, kiedy z niej nie korzystasz.

- **Chroń swoje finanse:** Korzystając z bankowości internetowej i sklepów online, upewnij się, że połączenie jest objęte szyfrowaniem (zielona kłódka oraz prefiks „https://" w pasku adresu). Odczytując kod SMS uwierzytelniający transakcję, zweryfikuj kwotę przelewu i numer rachunku odbiorcy!

BĄDŹ ŚWIADOMYM UŻYTKOWNIKIEM

- **Pozostań na bieżąco:** Nie lekceważ informacji ze świata bezpieczeństwa IT. Jeśli coś podawane jest do publicznej wiadomości, najczęściej dotyczy także Ciebie.
- **Pomyśl, zanim zadziałasz:** Bądź ostrożny wobec korespondencji zachęcającej do natychmiastowych działań. Szczególnie, jeśli ktoś oferuje Ci łatwy zysk lub próbuje nakłonić do podania prywatnych danych. Robiąc zakupy w sieci, weryfikuj reputacje sklepów. Dziel się wiedzą z rodziną i znajomymi.
- **Zadbaj o kopie zapasowe:** Zabezpiecz efekty swojej pracy, muzykę, zdjęcia, cenne dokumenty. Twórz kopie zapasowe i przechowuj je w bezpiecznym miejscu.

CHROŃ SWOJĄ PRYWATNOŚĆ

- **Informacje mają wartość:** Dane na Twój temat, takie jak historia zakupów czy historia lokalizacji są cenne. Zwracaj uwagę kto i co (aplikacje, strony internetowe) próbuje uzyskać do nich dostęp.
- **Dostosuj ustawienia prywatności w serwisach online i na urządzeniach:** Dzięki nim, możesz lepiej chronić Twoje dane. Sam decyduj, jak wiele informacji na swój temat chcesz udostępnić innym.
- **Pomyśl, zanim udostępnisz:** Zwracaj uwagę na przesyłaną do sieci treść, zasięg komunikatu, a także sposób, jaki może zostać odebrany.

TWÓRZ KULTURĘ BEZPIECZNEJ SIECI

- **Twoje zachowanie w sieci ma znaczenie:** Stosowanie dobrych praktyk buduje kulturę bezpiecznej sieci. To, co robisz, ma znaczenie (w domu, w pracy, gdziekolwiek jesteś).
- **Traktuj innych tak, jak sam chciałbyś być traktowany.**
- **Wspieraj walkę z cyberprzestępczością:** Jeżeli zaobserwujesz niepokojące zjawiska, nie wahaj się o tym poinformować:
  https://incydent.cert.pl (zgłaszanie incydentów naruszających bezpieczeństwo w sieci) https://dyzurnet.pl (przyjmowanie zgłoszeń dotyczących nielegalnych treści w Internecie).