CYBERBEZPIECZEŃSTWO

Zgodnie z art. 22 ust. 1 pkt 4 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, przekazujemy niezbędne informacje w przedmiocie zagadnienia jakim jest cyberbezpieczeństwo.

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

By przeciwdziałać wystąpieniu zagrożenia w obszarze cyberbezpiczeństwa należy przestrzegać podstawowych zasad, w tym m.in.:

- Pamiętaj, aby zawsze mieć aktualny system operacyjny oraz pozostałe oprogramowanie.
- Stosuj szyfrowanie w urządzeniach mobilnych, koniecznie ustaw PIN lub w inny sposób zabezpiecz dostęp do tych urządzeń.
- Stosuj szyfrowanie korzystając z przenośnych nośnikach danych.
- Chroń swoje urządzenia używając programów antywirusowych.
- Nie otwieraj podejrzanych wiadomości e-mail, załączników do tych wiadomości i linków w nich zawartych.
- Nie ufaj wiadomościom SMS i telefon z informacjami o komiczności dokonania zaległych płatności, nieodebranych niezamówionych przesyłkach, itp.
- Nie instaluj aplikacji z nieznanych i niezaufanych źródeł.
- Stosuj hasła o wysokim poziomie skomplikowania, regularnie zmieniaj hasła, nie stosuj tych samych haseł w różnych serwisach.
- Stosuj uwierzytelnianie dwuskładnikowe.
- Nie korzystaj z ogólnodostępnych sieci Wi-Fi.
- Przed wpisaniem danych do formularza zastanów się, jak się na nim znalazłeś i jaki jest zakres danych, które masz podać. Być może jesteś na stronie przygotowanej przez przestępców. Jeśli adres strony lub jakikolwiek jej element budzą Twoje wątpliwości – przerwij czynność i natychmiast zakończ działania.
- Przed zakupem sprawdź, od kogo kupujesz towar, jak długo istnieje dana firma, gdzie ma siedzibę, czy możesz dodzwonić się na infolinię

sklepu, czy odpisują na wiadomości oraz jakie opinie wystawili inni kupujący.
- Nie ujawniaj żadnych danych, dopóki nie upewnisz się z kim rozmawiasz. Nie ufaj nieznanym rozmówcom.
- Uważnie czytaj wszystkie wyświetlane na stronach komunikaty, nie wyrażaj zgody jeżeli nie przeczytałeś całej treści komunikatu, lub masz jakiekolwiek wątpliwości.

Zachęcamy do zgłaszania incydentów cyberbezpieczeństwa, być może uchroni to inne osoby przed zagrożeniem:

Zachęcamy również do śledzenia bieżących komunikatów dot. cyberbezpieczeństwia:

- Rozwój technik ataku grupy UNC1151/Ghostwriter
  19 lipca 2022
  W ostatnim czasie obserwujemy ataki grupy UNC1151/Ghostwriter z wykorzystaniem techniki Browser in the Browser. Grupa ta od ponad roku atakuje skrzynki pocztowe polskich obywateli. Wykorzystywane techniki z biegiem czasu ulegają zmianie, ale motyw przewodni używanych wiadomości, jak i cel pozostaje ten sam.
- Krajobraz bezpieczeństwa polskiego internetu w 2021 roku
  10 maja 2022
  Nowy raport, stare techniki – tak w skrócie można ująć kluczowe obserwacje z 2021 r. Przestępcy udoskonalili znane sposoby oszustw i częściej zaczęli sięgać po metody wcześniej rzadko używane. Zapraszamy do lektury.
- Trojany mobilne w Polsce w 2021 r.
  4 maja 2022
  Rynek urządzeń mobilnych z roku na rok powiększa się, a w raz z nim liczba ataków na urządzenia mobilne. W 2021 r. do zespołu zespołu CERT Polska trafiło ponad 17,5 tys. zgłoszeń dotyczących szkodliwych aplikacji na systemy operacyjne Android.
- Najważniejsze podatności 2021 r.

29 kwietnia 2022

Rok 2021 był wypełniony poważnymi podatnościami, które bardzo szybko były adaptowane i wykorzystywane przez cyberprzestępców, w szczególności przez grupy ransomware. Zaobserwowaliśmy wyraźny trend wzrostu wykorzystania podatności w oprogramowaniu używanym przez firmy np. Microsoft Exchange czy VMware vCenter, względem tych w oprogramowaniu wykorzystywanym przez użytkownika końcowego, takich jak pakiet Office czy przeglądarka.

- Statystyki obsługi incydentów w 2021 r.

  28 kwietnia 2022

  Sukcesywnie każdego roku CERT Polska rejestruje coraz większą liczbę zgłoszeń oraz incydentów cyberbezpieczeństwa. W 2021 r. CERT Polska zarejestrował 116 071 zgłoszeń. Spośród wszystkich zgłoszeń nasi specjaliści wytypowali 65 586, na podstawie których zarejestrowano łącznie 29 483 unikalnych incydentów cyberbezpieczeństwa.
- Kampanie fałszywych SMS-ów PGE/InPost/Blik

  12 kwietnia 2022

  Przestępcy rozsyłają wiadomości SMS z informacją o wymaganej płatności. W przypadku podania danych bankowych trafiają one bezpośrednio do przestępców, którzy następnie starają się wykraść jak najwięcej pieniędzy z konta ofiary.
- Kampanie fałszywych SMS-ów ze złośliwym oprogramowaniem Flubot

  12 kwietnia 2022

  Korzystając z zainfekowanych telefonów, przestępcy rozsyłają wiadomości SMS z informacją o konieczności podjęcia działań wraz z linkiem do złośliwej strony. Jeśli użytkownik zgodzi sie na pobranie i zainstalowanie aplikacji to po uzyskaniu odpowiednich uprawnień przejmuje ona kontrolę nad urządzeniem i wykradać dane z telefonu.
- Fałszywe inwestycje

  12 kwietnia 2022

  Reklamy opisują platformy inwestycyjne za pomocą których można rzekomo inwestować w kryptowaluty lub akcje firm. Po podaniu wymaganych danych kontaktowych, przedstawiciel firmy oferującej te

fałszywe inwestycje kontaktuje się telefonicznie z zainteresowanym i nakłania do zainwestowania przez wykonanie przelewu.

- Fałszywe panele logowania Facebook
  12 kwietnia 2022
  Przestępcy wykorzystują kilka metod propagowania oszustwa oraz zachęcania potencjalnej ofiary do podania poufnych danych związanych z portalem Facebook. Konta te też są wykorzystywane do wyłudzania środków finansowych od osób będących w kręgu znajomych przejętego konta.
- Oszustwa na portalach z ogłoszeniami
  12 kwietnia 2022
  Przestępcy przeszukują portale z ogłoszeniami, aby znaleźć potencjalne ofiary oszustwa. Oszust informuje, że jest chętny na zakup przedmiotu i że już za niego zapłacił, a sprzedający musi tylko odebrać środki na własne konto poprzez specjalną stronę. Oszut wysyła link do fałszywej bramki płatności. Podając na niej dane ofiara daje dostęp do konta przestępcom.

Źródło komunikatów: Cert.pl

Polecamy również specjalistyczne serwisy internetowe poświęcone cyberbezpiczeństwu, w tym m.in.:

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