Bezpieczeństwo informacji i cyberbezpieczeństwo

Informacje na temat zagrożeń występujących w cyberprzestrzeni oraz porady jak się przed nimi zabezpieczyć

Realizując zadania wynikające z ustawy o krajowym systemie cyberbezpieczeństwa publikujemy informacje na temat zagrożeń występujących w cyberprzestrzeni.

Cyberbezpieczeństwo to zgodnie z obowiązującymi przepisami „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy" (art. 2 pkt 4 ustawy o krajowym systemie cyberbezpieczeństwa).

Najpopularniejsze zagrożenia w cyberprzestrzeni:

- **Phishing** - atak za pośrednictwem poczty e-mail polegający na nakłonieniu odbiorcy wiadomości e-mail do ujawnienia poufnych informacji lub pobrania złośliwego oprogramowania.
- **Spear Phishing** - bardziej wyrafinowana forma phishingu, w której napastnik podszywa się pod osobę bliską osoby atakowanej.
- **Malware** - oprogramowanie, które wykonuje złośliwe zadanie na urządzeniu docelowym lub w sieci, np. uszkadza dane lub przejmuje system, urządzenia mobilne są szczególnie podatne na ataki złośliwego oprogramowania.
- **Trojan** - (koń trojański) - oprogramowanie, które podszywa się pod przydatne lub ciekawe dla użytkownika aplikacje, implementując szkodliwe, ukryte przed użytkownikiem różne funkcje (oprogramowanie szantażujące - ransomware, szpiegujące - spyware etc.).
- **Ransomware** - atak polegający na zaszyfrowaniu danych w systemie docelowym i zażądaniu okupu w zamian za umożliwienie użytkownikowi ponownego dostępu do danych.
- **Atak typu „Man in the Middle"** - atak ten wymaga, aby napastnik znalazł się między dwiema stronami, które się komunikują i był w stanie przechwytywać wysyłane informacje.
- **Atak DoS lub DDoS** - atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów. DDoS atakuje z wielu miejsc równocześnie.
- **Atak IoT** - atak polegający na przejmowaniu kontroli nad urządzeniami w sieci Internet: inteligentnymi domami, budynkami, sieciami energetycznymi, urządzeniami gospodarstwa domowego - przemysłu etc.).
- **Data Breaches (naruszenie danych)** - atak tego typu polega na kradzieży danych. Motywy naruszeń danych obejmują przestępstwa: (tj. kradzieży tożsamości, chęci zawstydzenia instytucji, szpiegostwo i inne).

By zabezpieczyć się przed zagrożeniami należy:

- Stosować zróżnicowane hasła.
  Należy korzystać z różnych haseł do różnych usług elektronicznych. Nie da się obronić przed atakami używając prostych haseł, takich jak „1234". Odpowiednie, złożone hasło może ochronić przed zagrożeniami w cyberprzestrzeni.
- Regularnie zmieniać hasła.
- Uważać na prośby o podanie haseł.
  Należy pamiętać, że żadna instytucja nie wysyła e-maili do swoich klientów/interesantów z prośbą o podanie hasła lub loginu w celu ich weryfikacji, nawet pod pretekstem zablokowania konta, naliczenia opłat.
- Stosować uwierzytelnianie dwuetapowe.
  Tam gdzie to możliwe (konta społecznościowe, konto email, usługi e-administracji, usługi finansowe) należy stosować dwuetapowe uwierzytelnienie za pomocą np. sms, pin, aplikacji generującej jednorazowe kody autoryzujące, tokenów, klucza fizycznego.
- Chronić kartę kredytową/bankomatową.
  Nie należy udostępniać nikomu danych karty kredytowej lub bankomatowej w tym PINów, numeru karty, kodu weryfikacyjnego CVV/CVC znajdującego się na odwrocie karty, daty ważności karty. Nie należy zapisywać PINu na karcie lub przyklejonej karteczce. Należy stosować PIN składający się z różnych cyfr rozmieszczonych na całej klawiaturze. Należy chronić wpisywanie PINu przy operacjach w sklepie, gdzie przebywa dużo osób w kolejce za Tobą.
- Porównywać treść SMSa z operacją bankową.
  Przy dokonywaniu przelewów i autoryzacji np.: SMSem, należy sprawdzić czy treść z SMSa dotyczy dokładnie tej samej operacji, która jest wykonywana wraz z numerem konta. W przypadku otrzymania nietypowych SMSów typu zmiana numeru telefonu do konta, dodanie urządzenia do logowania, zmiana limitów na karcie – należy skontaktować się z bankiem i przerwać dalsze czynności autoryzacji i przepisywania hasła z SMSa.
- Sprawdzać domenę strony.
  Należy kontrolować nazwę domeny strony, na której zamierza się podać poufne dane. Jeśli strona logowania wygląda jak strona banku, lecz ma nietypowy adres www, należy sprawdzić czy strona nie jest próbą oszustwa (phishing).
- Sprawdzać certyfikat SSL strony.
  Podczas podawania poufnych danych należy sprawdzić czy strona internetowa posiada certyfikat SSL. Protokół SSL to standard kodowania (zabezpieczania) przesyłanych danych pomiędzy przeglądarka a serwerem.
- Zabezpieczać swoje dane osobowe.
  Nie należy zostawiać poufnych danych w niesprawdzonych serwisach i na stronach, jeżeli nie ma się absolutnej pewności, że nie będą one widoczne dla osób trzecich.
- Uważać na prośby dopłacenia do przesyłek.
  W przypadku otrzymania SMSa z prosbą o dokończenie procesu zamówienia przesyłki np.: w postaci brakującej kwoty (wymagana dopłata kilku groszy), należy zablokować nr skąd pochodzi SMS oraz skasować SMS.
- Aktualizować oprogramowanie.
  System operacyjny, aplikacje użytkowe, programy antywirusowe wymagają stałej aktualizacji i baz zagrożeń. Brak aktualizacji zwiększa podatność na cyberzagrożenia. Hakerzy, którzy znają słabości systemu/aplikacji, mają otwartą furtkę do korzystania z luk w oprogramowaniu. Logowanie do e-usług publicznych, bankowości elektronicznej bez aktualnego (wspieranego przez producenta) systemu operacyjnego to duże ryzyko.
- Uważać na strony z darmowym oprogramowaniem.
  Dotyczy to stron, które oferują darmowe atrakcje (filmiki, muzykę, aplikacje) - często na takich stronach znajdują się ukryte wirusy, trojany i inne zagrożenia.
- Kontrolować uprawnienia instalowanych aplikacji, szczególnie w urządzeniach mobilnych.
- Pracować na najniższych możliwych uprawnieniach użytkownika.
- Stosować sprawdzone oprogramowanie antywirusowe.
  Powinno się subskrybować dobrej jakości oprogramowanie antywirusowe oraz włączyć aktualizacje automatyczne systemu operacyjnego na swoim

Powinno się subskrybować dobrej jakości oprogramowanie antywirusowe oraz włączyć aktualizacje automatyczne systemu operacyjnego na swoim urządzeniu.

- Skanować podłączane urządzenia zewnętrzne.
  Przy podłączeniu do laptopa/komputera urządzenia typu pendrive, karta pamięci, dysk przenośny, smartfon - najpierw należy przeskanować nośnik zaktualizowanym oprogramowaniem antywirusowym.
- Nie otwierać plików nieznanego pochodzenia.
  Należy zachować ostrożność podczas otwierania załączników plików. Na przykład, w przypadku otrzymania wiadomość e-mail z załącznikiem PDF z opisem „zaległa faktura", nie należy go otwierać jeśli pochodzi on od nietypowego nadawcy, takiego jak ann23452642@gmail.com. Zaleca się przeskanować załącznik w serwisie np. : www.virustotal.com
- Wykonywać kopie bezpieczeństwa.
  Należy korzystać z oddzielnych nośników na kopie. Nie należy przechowywać kopii i oryginałów plików wyłącznie na tym samym nośniku.
- Szyfrować dyski.
  Należy zabezpieczać trudnym hasłem twarde dyski w laptopie, dyski przenośne, pendrivy i karty pamięci.
- Unikać publicznych WiFi.
  W miarę możliwości, nie należy korzystać z publicznych, otwartych (niezabezpieczonych) sieci Wi-Fi, stosowanych w hotelach, pubach, restauracjach do których dostęp ma wiele osób. Jeśli to możliwe, bezpieczniej jest udostępnić Internet LTE ze swojego smartfona poprzez kabel USB lub zabezpieczoną sieć Wi-Fi na swój laptop, zamiast korzystać z publicznego Wi-Fi np.: do logowania w banku. Po zakończeniu, należy wyłączyć udostępniany Internet w smartfonie.
- Zadbać o bezpieczeństwo routera.
  Powinno się ustawić silne hasło do swojej sieci Wi-Fi, zmienić nazwę sieci Wi-Fi ze standardowej na inną, zmienić hasło do panelu administratora, ustawić poziom zabezpieczeń połączenia z siecią Wi-Fi np. WPA2 lub WPA3, okresowo aktualizować oprogramowanie routera, wyłączyć funkcję szybkiego logowania do sieci przez przycisk WPS na routerze.
  Odnośniki do stron dotyczących cyberbezpieczeństwa:
- Poradniki w bazie wiedzy https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo
- Publikacje z zakresu cyberbezpieczeństwa: https://www.cert.pl
- Szczegółowe porady i ostrzeżenia przed zagrożeniami w sieci:https://niebezpiecznik.pl/
- Zestaw porad bezpieczeństwa dla użytkowników komputerów prowadzony na witrynie internetowej CSIRT NASK – Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym: https://www.cert.pl/ouch
- Kampania STÓJ. POMYŚL. POŁĄCZ mającej na celu zwiększanie poziomu świadomości społecznej i promowanie bezpieczeństwa w cyberprzestrzeni: https://stojpomyslpolacz.pl/stp

Zgłoszenie incydentu, szkodliwych treści:

Anonimowego i łatwego zgłoszenia incydentów cyberbezpieczeństwa lub nielegalnych i szkodliwych treści zamieszczonych w Internecie można dokonać za pomocą formularza: https://incydent.cert.pl/

Metryka strony

Udostępniający: **Urząd Miasta Bielsk Podlaski**
Wytwarzający/odpowiadający: Burmistrz Miasta Bielsk Podlaski
Data wytworzenia: **2023-07-13**
Wprowadzający: **Mirosław Karolczak**
Data modyfikacji: **2023-07-13**
Opublikował: **Mirosław Karolczak**
Data publikacji: **2023-07-13**