Cyberbezpieczeństwo

Realizując zadania wynikające z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U.2023.913 t.j.), **przekazujemy Państwu informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady jak skutecznie zabezpieczyć się przed tymi zagrożeniami.**

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

Z raportu CERT Polska za 2022 rok wynika, iż obsłużono 39683 incydenty. Najczęściej występującymi typami incydentów są:

1. Oszustwa komputerowe (88,22%):

a) phishing, czyli wyłudzanie poufnych informacji przez podszywanie się pod godną zaufania osobę lub instytucję (64,57%),
b) nieuprawnione wykorzystanie zasobów,
c) kradzież tożsamości,
d) naruszenie praw autorskich.

2. Złośliwe oprogramowanie - *malware*, wirusy, robaki, trojany, *keyloggery* itp., czyli oprogramowanie, które bez zgody i wiedzy użytkownika wykonuje na komputerze działania na korzyść osoby trzeciej (8,59%).

3. Włamania i próby włamań (1,19%).

4. Obraźliwe i nielegalne treści (0,78%):

a) spam, czyli niechciane lub niepotrzebne wiadomości elektroniczne,
b) dyskredytacja, obrażanie,
c) pornografia, przemoc.

5. Podatne usługi, w tym otwarte serwisy podatne na nadużycia (0,47%).

6. Ataki na dostępność zasobów, w tym atak blokujący serwis (DoS, DDos), czyli ataki, których celem jest przejęcie i zaszyfrowanie danych użytkownika po to aby w następnym kroku udostępnić te same dane użytkownikowi pod warunkiem wniesienia przez niego "okupu" (0,44%).

7. Inne (0,12%)

8. Ataki na bezpieczeństwo informacji (0,10%):

a) nieuprawniony dostęp do informacji,
b) nieuprawniona zmiana informacji.

9. Gromadzenie informacji (0,08%):

a) skanowanie,
b) podsłuch,
c) inżynieria społeczna.

Phishing to typ ataku oparty o wiadomości e-mail lub SMS. Cyberprzestępcy podszywając się m.in. pod firmy kurierskie, urzędy administracji, operatorów telekomunikacyjnych, czy nawet naszych znajomych, starają się wyłudzić nasze dane do logowania np. do kont bankowych lub używanych przez nas kont społecznościowych, czy systemów biznesowych. Wiadomości phishingowe są tak przygotowywane przez cyberprzestępców, aby wyglądały na autentyczne, ale w rzeczywistości są fałszywe. Mogą próbować skłonić Cię do ujawnienia poufnych informacji, zawierać link do strony internetowej rozprzestrzeniającej szkodliwe oprogramowanie (często przestępcy używają podobnych do autentycznych nazw witryn) lub mieć zainfekowany załącznik. Dopóki nie masz pewności, że nadawca jest prawdziwy, nie powinieneś klikać w żadne linki ani na nie odpowiadać. W wiadomościach SMS lub mailach często wykorzystywane są tzw. tiny-URL, czyli skrócone adresy stron internetowych. Stąd też należy zwrócić szczególną uwagę na nazwy stron internetowych, które przesyłane są w podejrzanych mailach czy SMSach.

Podstawowe zasady cyberbezpieczeństwa:

1. Pamiętaj o uruchomieniu Firewalla (dla systemu firmy Microsoft jest to Windows Defender Firewall (Windows 10).
2. Używaj oprogramowania antywirusowego. Stosuj ochronę w czasie rzeczywistym (nie wyłączaj programu).
3. Na bieżąco aktualizuj system operacyjny, zainstalowane oprogramowanie oraz program antywirusowy (pozostaw włączoną funkcję automatycznych aktualizacji).
4. Nie otwieraj plików nieznanego pochodzenia oraz zwracaj uwagę na rozszerzenia pobieranych plików. Sprawdzaj
   za pomocą programu antywirusowego pliki pobrane z Internetu, nawet jeśli wydają się bezpieczne. Zrób to przed otworzeniem pliku.
5. Nie używaj niesprawdzonych programów antywirusowych. Nie pobieraj oprogramowania z nieoficjalnych źródeł.
6. Korzystaj z funkcji oprogramowania antywirusowego jaką jest skanowanie komputera i domowej sieci internetowej.
   W przypadku gdy się na tym nie znasz, poproś kogoś o pomoc.
7. Staraj się unikać stron, które oferują niesamowite okazje (pieniądze, darmowe filmy, muzykę lub łatwy zarobek).
   Często na takich stronach znajdują się ukryte wirusy i inne zagrożenia.
8. Nie korzystaj z jednakowego hasła do wszystkich stron i portali internetowych. Jeśli masz problem z tworzeniem
   i zapamiętywaniem haseł używaj menadżera haseł. Nikomu nie udostępniaj loginu i hasła do Twoich kont. Korzystaj
   z dwuskładnikowego uwierzytelniania.
9. Za pośrednictwem konta Google i Google Alerts możesz sprawdzić czy Twoje dane wyciekły do sieci.
10. Nie wysyłaj w e-mailach poufnych danych w formie otwartego tekstu. Powinny one stanowić zaszyfrowany załącznik

i być zabezpieczone hasłem. Hasło przekazuj w sposób bezpieczny innym kanałem komunikacji, np. sms, telefon.

11. Pamiętaj, że bank nie prosi telefonicznie i za pośrednictwem poczty email swoich klientów o podanie hasła i loginu w celu ich weryfikacji.
12. 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. Nie korzystaj z odnośników do ww. stron przesyłanych w podejrzanych wiadomościach email.
13. Jeśli nie masz pewności czy dzwoni do Ciebie pracownik banku, poproś o autoryzację w mobilnej aplikacji. Jeżeli z niej nie korzystasz zawsze możesz potwierdzić tożsamość konsultanta pod numerem infolinii lub sprawdzić, w jakim celu dzwonił pracownik banku.
14. Unikaj publicznych komputerów i publicznych sieci Wi-Fi.
15. Korzystaj z szyfrowania dysków i pendrive (w systemie firmy Microsoft jest to BitLocker (Windows 10)).
16. Korzystaj z szyfrowania i blokady ekranu w urządzeniach mobilnych.
17. Systematycznie wykonuj kopie zapasowe ważnych danych.
18. Dostosuj ustawienia prywatności w serwisach online i na urządzeniach. Dzięki nim możesz lepiej chronić swoje dane.
    Sam decyduj, jak wiele informacji na swój temat chcesz udostępnić innym.

Przepisy, które warto znać:

- Art. 190a Kodeksu karnego (§ 2) Podszywanie
- Art. 23 Kodeksu cywilnego – Dobra osobiste
- Art. 212 Kodeksu karnego – Zniesławienie
- Art. 46 Ustawy o usługach płatniczych – Odpowiedzialność banku w przypadku wystąpienia nieautoryzowanej transakcji płatniczej
- Art. 82 RODO – Prawo do odszkodowania

Przydatne linki:

- **STÓJ. POMYŚL. POŁĄCZ** jest polską wersją międzynarodowej kampanii STOP. THINK. CONNECT.™, mającej na celu podnoszenie poziomu świadomości społecznej w obszarze cyberbezpieczeństwa poprzez informowanie o zagrożeniach i sposobach radzenia sobie z nimi, promowanie zachowań służących poprawie bezpieczeństwa internautów oraz ich rodzin i otoczenia.
- **OUCH!** To cykliczny, darmowy zestaw porad bezpieczeństwa dla użytkowników komputerów. Każde wydanie zawiera krótkie, przystępne przedstawienie wybranego zagadnienia z bezpieczeństwa komputerowego wraz z listą wskazówek jak można chronić siebie, swoich najbliższych i swoją organizację.
- **Zespół CERT Polska** działa w strukturach **NASK** (Naukowej i Akademickiej Sieci Komputerowej) – państwowego instytutu badawczego prowadzącego działalność naukową, krajowy rejestr domen .pl i dostarczającego zaawansowane usługi teleinformatyczne. CERT to pierwszy powstały w Polsce zespół reagowania na incydenty, zagrożenia w sieciach komputerowych.
- Dla każdego - cyberhigiena - Baza wiedzy - Portal Gov.pl (www.gov.pl).

- Cyberpolicy NASK – Kompendium wiedzy na temat cyberbezpieczeństwa.
- Fundacja Wiedza To Bezpieczeństwo | Kampania społeczna Potencjalnie NIE bezpieczni (wtb.org.pl).
- Jeżeli chcesz anonimowo i łatwo zgłosić nielegalne i szkodliwe treści, na które natknąłeś się w sieci możesz zrobić to za pomocą tego formularza.
- Jeśli chcesz zgłosić podejrzany incydent (phising, oszustwo, podejrzane wiadomości sms, itp.) możesz to zrobić za pomocą tego formularza.