Realizując zadania wynikające z art. 22 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560 z późn. zm.), Muzeum Samorządowe Ziemi Strzyżowskiej im. Zygmunta Leśniaka w Strzyżowie przekazuje Państwu informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady jak skuteczne stosować sposoby zabezpieczenia się przed tymi zagrożeniami.

Cyberbezpieczeństwo to ochrona danych i systemów wewnętrznych przed zagrożeniami, jakie niosą za sobą cyberataki. W takiej definicji mieści się nie tylko technologia, lecz także cały proces, który kontroluje i ochrania sieć, programy i urządzenia. Najważniejszym celem zapewnienia bezpieczeństwa w sieci jest zmniejszenie ryzyka ataków cybernetycznych oraz skuteczna ochrona przed nieuprawnionym wykorzystaniem danych i programów.

Najpopularniejsze zagrożenia w cyberprzestrzeni:

- Kampanie phishingowe wykorzystujące wizerunek banków – Głównym celem tego oszustwa jest zachęcenie potencjalnej ofiary do podania danych logowania do swojego konta bankowości internetowej, aby następnie wyłudzić przechowywane pieniądze.
- Oszustwa na portalach z ogłoszeniami – 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. Oszust wysyła link do fałszywej bramki płatności. Podając na niej dane ofiara daje dostęp do konta przestępcom.
- Fałszywe panele logowania Facebook – 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.
- Fałszywe inwestycje – 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.
- Kampanie fałszywych SMS-ów ze złośliwym oprogramowaniem Flubot – Korzystając z zainfekowanych telefonów, przestępcy rozsyłają wiadomości SMS z informacją o konieczności podjęcia działań wraz z linkiem do złośliwej strony. Jeśli użytkownik zgodzi się na pobranie i zainstalowanie aplikacji to po uzyskaniu odpowiednich uprawnień przejmuje ona kontrolę nad urządzeniem i wykradać dane z telefonu.
- Kradzieże (wyłudzenia), modyfikacje bądź niszczenie danych
- Ataki socjotechniczne (np. phishing, czyli wyłudzenie informacji przez podszywanie się pod godną zaufania osobę lub instytucję)
- Ataki z wykorzystaniem złośliwego kodu na stronach internetowych
- Ataki na aplikacje internetowe
- Ataki DDoS – czyli blokowanie dostępu do usług poprzez sztuczne generowanie wzmożonego ruchu
- Naruszenie poufności, integralności lub dostępności danych
- Wyciek danych
- Ataki ransomware w celu wyłudzenia okupu za odszyfrowanie lub nieujawnianie wykradzionych danych
- Cyberszpiegostwo

Wskazówki jak można chronić siebie i swoich najbliższych

1. Używaj tylko silnych, indywidualnych dla każdego systemu haseł i nie udostępniaj ich nikomu.
2. Zainstaluj i używaj oprogramowania antywirusowe. Najlepiej stosuj ochronę w czasie rzeczywistym.
3. Aktualizuj oprogramowanie antywirusowe oraz bazy danych wirusów (dowiedz się czy twój program do ochrony przed wirusami posiada taką funkcję i robi to automatycznie).
4. Aktualizuj system operacyjny i aplikacje bez zbędnej zwłoki.
5. Nie otwieraj plików nieznanego pochodzenia.
6. Nie korzystaj ze stron internetowych (zwłaszcza ze stron banków, poczty elektronicznej czy portali społecznościowych), które nie mają ważnego certyfikatu, chyba, że masz stuprocentową pewność z innego źródła, że strona taka jest bezpieczna.
7. Nie używaj niesprawdzonych programów zabezpieczających czy też do publikowania własnych plików w Internecie (mogą one np. podłączać niechciane linijki kodu do źródła strony).
8. Regularnie skanuj komputer i sprawdzaj procesy sieciowe – jeśli się na tym nie znasz poproś o sprawdzenie kogoś, kto się zna. Czasami złośliwe oprogramowanie nawiązujące własne połączenia z Internetem, wysyłające twoje hasła i inne prywatne dane do sieci może się zainstalować na komputerze mimo dobrej ochrony – należy je wykryć i zlikwidować.
9. Sprawdzaj pliki pobrane z Internetu za pomocą programu antywirusowego.
10. Unikaj odwiedzania stron, które oferują wyjątkowe atrakcje (darmowe filmiki, muzykę, łatwy zarobek, cudowną dietę) – często na takich stronach znajdują się ukryte wirusy, trojany i inne zagrożenia.
11. Nie zostawiaj danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie masz absolutnej pewności, że nie są one widoczne dla osób trzecich.
12. Nie wysyłaj w e-mailach żadnych poufnych danych (np. danych osobowych, logowania, karty kredytowej) w formie otwartego tekstu – powinny być zabezpieczone hasłem i zaszyfrowane – hasło przekazuj w sposób bezpieczny, tj. innym kanałem niż dane.
13. Pamiętaj o uruchomieniu firewalla.
14. Wykonuj kopie zapasowe ważnych danych.
15. Pamiętaj, że żaden bank czy Urząd nie wysyła e-maili do swoich klientów z prośbą o podanie hasła lub loginu w celu ich weryfikacji.
16. Zwracaj uwagę na komunikaty pojawiające się na ekranie i nigdy nie ignoruj ostrzeżeń dotyczących bezpieczeństwa.

Przed podaniem danych na stronie internetowej sprawdź do kogo należy domena

Krajowy Rejestr Domen:
https://www.dns.pl/whois

Zgłoszenia incydentów do CSIRT NASK

Od dnia 28 sierpnia 2018 r. zespołowi CERT Polska zostały powierzone obowiązki CSIRT NASK wynikające z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa: https://incydent.cert.pl/#!/lang=pl

Lista ostrzeżeń przed niebezpiecznymi stronami

https://www.cert.pl/posts/2020/03/ostrzezenia_phishing/

Zachęcamy również do regularnego zapoznawania się z treściami dotyczącymi cyberbezpieczeństwa zawartymi na stronach:

- Ministerstwa Cyfryzacji
- NASK
- CSIRT
- CERT

DYREKTOR
Muzeum Samorządowego
Ziemi Strzyżowskiej
mgr Magdalena Wilusz