PODSTAWOWE INFORMACJE ZWIĄZANE Z CYBERBEZPIECZEŃSTWEM

Co raz częściej słyszy się o cyberatakach, atakach hakerskich. Cyberbezpieczeństwo nabiera na sile i popularności w dobie dzisiejszej elektronizacji i przetwarzaniu dużej ilości danych w sieci. Warto jednak zwrócić uwagę na kilka podstawowych reguł, celem uchronienia się przed takimi atakami.

Fundamentalna zasada to używanie haseł do ochrony swoich danych. Hasła powinny mieć wysoki stopień trudności oraz różnić się od innych haseł których używamy. Zaczyna w głowie pojawiać się pytanie, jak sobie w takim razie radzić z zapamiętaniem tak znacznej ilości haseł. Dobrym rozwiązaniem są specjalnie tworzone aplikacje do przetrzymywania haseł. W ten sposób w naszej pamięci zostaje jedno, a całą resztę możemy sprawdzić w dedykowanej aplikacji. Tym samym, tworzone przez nas ciągi liter, cyfr i znaków specjalnych, mogą być bardziej losowe, dłuższe i trudne do odgadnięcia.

- https://www.gov.pl/web/baza-wiedzy/jak-tworzyc-bezpieczne-hasla

Należy pamiętać o tym, że nawet niewinne buszowanie w sieci powinno odbywać się w sprzyjających bezpieczeństwu warunkach. Korzystanie zatem ze sprawdzonych przeglądarek, używanie programów antywirusowych oraz regularna ich aktualizacja to podstawa.

- https://pl.safetydetectives.com/

Można sprawdzić w dostępnych rankingach bezpieczeństwa, jakie aplikacje do przeglądania internetu są najwyżej oceniane pod tym względem. Należy wyłączać wszystkie niepotrzebne i nieznane wtyczki. Nie tylko mogą one spowolnić sieć, ale także mogą narazić nasz sprzęt na ataki. Zaleca się wyłączanie także funkcji automatycznego zapamiętywania haseł i auto-uzupełniania formularzy.

Przykładowe najczęściej występujące zagrożenia:

1. PHISHING

To nie wszystkim znane angielskie słowo nie ma nic wspólnego z wędkarstwem, ale przez takie właśnie działania dajemy się złapać na haczyk. Haczyk polega na próbie wyłudzenia danych. Pod pozorem oferty, sprawdzenia poprawności danych lub innych wiarygodnie

brzmiących pretekstów – sami podajemy wrażliwe dane. Maile czy SMS-y z phishingiem wizualnie często naprawdę ciężko odróżnić. Pamiętać należy, aby zawsze potwierdzić prawdziwość e-maila/SMS-a, zanim cokolwiek zrobimy. Nie dajmy się też złapać na haczyk „darmowej wygranej", rzekoma nagroda miałaby do nas trafić, jeżeli podamy swoje dane. Takie nieoczekiwane „wygrane" zawsze są podejrzane.

2. MALWARE

Złośliwe oprogramowanie, infekujące urządzenia. Działa na szkodę użytkownika, powodując także straty finansowe. Najczęstszym źródłem infekcji są załączniki lub odnośniki tzw. linki w wiadomości e-mail, przejęta przez przestępców lub podstawiona, fałszywa strona, podstawione reklamy na zwykłych stronach. W jaki sposób można rozpoznać, że takowe oprogramowanie zainfekowało nasze urządzenie? Poprzez spowolnienie działania urządzenia, pojawienie się większej ilości spamu na poczcie, strony startowe, których użytkownik nie ustawiał w przeglądarce. Bardzo często użytkownik nic nie zauważy – albowiem celem działania tegoż oprogramowania jest skryte jego działanie. Można ustrzec się przed zainfekowaniem urządzenia poprzez aktualizację systemu i oprogramowania na nim zainstalowanego, posiadanie oprogramowania antywirusowego, regularne skanowanie urządzenia oprogramowania antywirusowego, tworzenie kopii zapasowych danych, włączenie firewall, systemy i aplikacje pobierane z zaufanych źródeł, nieotwieranie podejrzanych załączników, ostrożność przy podejrzanych linkach i stronach internetowych.

3. RANSOMWARE

Obecnie jest najczęściej występującym zagrożeniem w cyberprzestrzeni. Występuje poprzez złośliwe załączniki w wiadomościach mailowych zachęcających do kliknięcia, złośliwe strony www, złośliwe reklamy na legalnych stronach www, złośliwe oprogramowanie, którym komputer był już zagrożony wcześniej, nieuprawniony zdalny dostęp do komputera przez osoby trzecie. Najczęściej po zainfekowaniu maszyny użytkownik otrzymuje komunikat o tym, że jego dane zostały zaszyfrowane i aby odzyskać dane trzeba opłacić okup. W przypadku infekcji ransomware, należy pozostawić komputer włączony ale odłączony od sieci (internetu), żeby nie doszło do zainfekowania pozostałych urządzeń. Należy tworzyć na bieżąco kopię zapasowych swoich danych na zewnętrznych dyskach bądź przechowywanie ich w chmurach, używać aktualnego oprogramowania antywirusowego, zachować ostrożność przeglądając strony internetowe, zwrócić uwagę na natrętne reklamy.

Poniżej odnośniki do stron internetowych organów/instytucji zajmujących się cyberbezpieczeństwem w Polsce:

- *Krajowy System Cyberbezpieczeństwa*:

https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa-

- *Cyberbezpieczeństwo – NASK:*

https://www.nask.pl/pl/dzialalnosc/cyberbezpieczenstwo/3284,Cyberbezpieczenstwo.html

- *Ochrona informacji w przestrzeni wraz z poradnikiem:*

https://www.gov.pl/web/baza-wiedzy/poradnik--prcyber-01

Inne przydatne linki :

Jak wyczyścić telefon przed sprzedażą i usunąć wszelkie dane ?
https://www.netia.pl/pl/blog/jak-wyczyscic-telefon-przed-sprzedaza -

Znajdowanie lub blokowanie utraconego urządzenia z Androidem lub kasowanie z niego danych. https://support.google.com/accounts/answer/6160491?hl=pl –

Ranking najlepszych aplikacji do kontroli rodzicielskiej
https://www.pcworld.pl/ranking/Najlepsze-aplikacje-do-kontroli-rodzicielskiej-na-Androida,410645.html

Punkt kontaktowy do zgłaszania nielegalnych treści w Internecie - *https://dyzurnet.pl/*

Opracowała:
Katarzyna Barszczewska