Komunikaty dotyczące cyberbezpieczeństwa

Szanowni Państwo,
realizując obowiązki z art. 22 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, cyt.:
Podmiot publiczny [...] zapewnia osobom, na rzecz których zadanie publiczne jest realizowane, dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, w szczególności przez publikowanie informacji w tym zakresie na swojej stronie internetowej
przekazujemy Państwu podstawowe informacje dot. cyberbezpieczeństwa i propozycje zabezpieczenia się przed cyberatakami.

Cyberbezpieczeństwo to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez ww. systemy. Każde zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo, to incydent. Poniżej pozwalamy sobie przekazać Państwu informacje o najczęściej powtarzających się cyber-zagrożeniach oraz możliwych działaniach profilaktycznych, służących obniżeniu ryzyka wystąpienia incydentu.

Najczęściej powtarzające się zagrożenia:

1. Malware - oprogramowanie, które wykonuje złośliwe zadanie na urządzeniu docelowym lub w sieci, np. uszkadza dane lub przejmuje system.
2. Phishing - atak za pośrednictwem przede wszystkim poczty e-mail polegający na nakłonieniu odbiorcy wiadomości e-mail do ujawnienia poufnych informacji lub pobrania złośliwego oprogramowania.
3. Spear Phishing - bardziej wyrafinowana forma phishingu, w której napastnik podszywa się pod osobę bliską osoby atakowanej.
4. Atak typu “Man in the Middle” (MitM) - atak ten wymaga, aby napastnik znalazł się między dwiema stronami, które się komunikują i był w stanie przechwytywać wysyłane informacje.
5. 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.).
6. Ransomware - atak polegający na zaszyfrowaniu danych w systemie docelowym i żądaniu okupu w zamian za umożliwienie użytkownikowi ponownego dostępu do danych.
7. 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.
8. Ataki IoT w Internecie rzeczy - atak polegający na przejmowaniu kontroli nad urządzeniami w sieci Internet: inteligentnymi domami, budynkami, sieciami energetycznymi, urządzeniami gospodarstwa domowego - przemysłu etc.).
9. 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).
10. Ataki socjotechniczne, czyli ataki oparte o wiadomości e-mail lub SMS, za pomocą których cyberprzestępcy (podszywając się m.in. pod firmy kurierskie, urzędy

administracji, operatorów telekomunikacyjnych, nawet znajomych), starają się wyłudzić nasze dane do logowania np. do kont bankowych lub używanych przez nas kont społecznościowych, czy systemów biznesowych).

Podstawowe zasady bezpieczeństwa w sieci:

1. Nigdy nie umieszczajmy informacji pozwalających w prosty sposób nas zidentyfikować!
2. Ostrożnie dobierajmy zdjęcia!
3. Dobre hasło to podstawa! Nie zapisujmy haseł w przeglądarkach!
4. Włączmy uwierzytelnienie dwuskładnikowe!
5. Korzystajmy z bezpieczniejszych komunikatorów, np. Signal
6. Nie przyjmujmy do znajomych osób, których nie znamy!
7. Nigdy nie oddawajmy swojego telefonu komukolwiek do ręki!
8. Uczmy się nieklikania w linki!
9. Uczmy się nieodbierania wiadomości, jeżeli się ich nie spodziewamy!
10. Uczmy się korzystania ze stron certyfikowanych.
11. Uczmy się uważnego czytania treści.
12. Korzystajmy z zabezpieczeń własnych kont (dwustopniowe logowanie, blokady informacji, których inni nie muszą widzieć)!

Wybrane sposoby na uniknięcie zagrożeń:

1. Instalacja, użytkowanie i bieżące aktualizowanie oprogramowania antywirusowego i spyware.
2. Aktualizowanie systemu operacyjnego urządzenia oraz aplikacji na nim zainstalowanych.
3. Sprawdzanie plików pobranych z Internetu za pomocą programu antywirusowego.
4. Nieotwieranie plików nieznanego pochodzenia.
5. Korzystanie ze stron internetowych posiadających ważny certyfikat bezpieczeństwa.
6. Regularne skanowanie komputera i sprawdzanie procesów sieciowych.
7. Uruchomienie firewalla.
8. Każdorazowa weryfikacja adresu nadawcy wiadomości e-mail.
9. Niewysyłanie danych osobowych, logowania, karty kredytowej w niezabezpieczonej treści wiadomości e-mail; żaden bank czy urząd nie wysyła do swoich klientów e-maili z prośbą o podanie hasła czy loginu w celu ich weryfikacji.
10. Unikanie odwiedzin stron zawierających darmowe pliki muzyczne, obrazy, filmy.
11. Regularne tworzenie kopii zapasowych ważnych danych.
12. Baczne obserwowanie i czytanie komunikatów pojawiających się na ekranie komputera.
13. Higiena hasła – nie da się obronić przed atakami używając prostych haseł, takich jak „1234”. Odpowiednie, złożone hasło może ochronić konsumentów przed zagrożeniami cybernetycznymi.

Poradniki:

1. Cyberhigiena dla każdego – serwis RP
2. Poradnik bezpieczny pracownik w sieci – poradnik Ministerstwa Cyfryzacji

wyznaczenie osoby kontaktowej do spraw cyberbezpieczeństwa, która będzie kontaktować się z organami właściwymi do spraw cyberbezpieczeństwa (CSIRT);
zapewnianie dostępu do wiedzy w zakresie cyberbezpieczeństwa, obsługa i zgłaszanie incydentów do właściwego CSIRT.

Anonimowe zgłaszanie incydentów:
Dyżurnet.pl to zespół ekspertów Naukowej i Akademickiej Sieci Komputerowej, działający jako punkt kontaktowy do zgłaszania nielegalnych treści w Internecie, szczególnie związanych z seksualnym wykorzystywaniem dzieci. Zgłoszenia o potencjalnie nielegalnych treściach można przekazać za pomocą formularza, na adres mailowy lub za pomocą infolinii 0 801 615 005. Zgłoś incydent

Pomocne podmioty:
1. Ministerstwo Cyfryzacji;
2. CyberDefence24;
3. CSRiT NASK;
4. Sekurak
5. Niebezpiecznik