Cyberbezpieczeństwo – podstawowe informacje i zasady

Realizując obowiązek informacyjny, nałożony na Podmioty publiczne na mocy ustawy z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczeństwa (Dz.U.2023.913), zgodnie z art. 22 ust. 1 pkt. 4 tej ustawy, przedstawiamy Państwu najważniejsze zagadnienia dot. niebezpieczeństw, które można napotkać w szeroko rozumianej cyberprzestrzeni oraz przedstawić podstawowe informacje o tych zagrożeniach. Cyberbezpieczeństwo, zgodnie z obowiązującymi przepisami, to „odporność systemów informacyjnych a działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy".

I. Najpopularniejsze zagrożenia w cyberprzestrzeni:

– kradzieże tożsamości,
– kradzieże (wyłudzenia), modyfikacje bądź niszczenie danych,
– blokowanie dostępu do usług,
– spam (niechciane lub niepotrzebne wiadomości elektroniczne),
– (malware, wirusy, robaki, itp.),
– ataki socjotechniczne (np. phishing), czyli wyłudzanie poufnych informacji przez podszywanie się pod godną zaufania osobę lub instytucję,
– ataki z użyciem szkodliwego oprogramowania:

Phishing – nazwa pochodzi od password ("hasło") oraz fishing ("wędkowanie"). Istotą ataku jest próba pozyskania hasła użytkownika, które służy do logowania się na portalach społecznościowych bądź do serwisów. Po uzyskaniu dostępu, przestępca może wykraść dane osobowe i w tym celu dokonywać oszustw. Jak się bronić? Ataki tego typu wymagają bardzo często interakcji ze strony człowieka w postaci odebrania maila lub potwierdzenia logowania.

Malware – zbitka wyrazowa pochodząca od wyrażenia malicious software ("złośliwe oprogramowanie"). Wspólną cechą programów uznawanych za malware jest fakt, że wykonują działania na komputerze bez jego zgody i wiedzy użytkownika, na korzyść osoby postronnej. Działania tego typu obejmują np. dołączenie maszyny do sieci komputerów "zombie", które służą do ataku na organizacje rządowe, zdobywanie wirtualnych walut lub kradzież danych osobowych i informacji niezbędnych do logowania do bankowości elektronicznej. Jak się bronić? Najskuteczniejszą obroną przed malware jest dobry system antywirusowy oraz regularnie aktualizowane oprogramowanie.

Ransomware – Celem ataku jest zaszyfrowanie danych użytkownika, a następnie ponowne ich udostępnienie w zamian za opłatę. Odbywa się głównie za sprawą okupu. Ataki tego typu działają na szkodę osoby fizycznej, i przedsiębiorców. Jak się bronić? Należy stosować aktualne oprogramowania antywirusowe oraz dokonywać regularnych aktualizacji systemu.

Man In the Middle – zwany "człowiekiem pośrodku", jest to typ ataku, w ramach, którego w transakcji b korespondencji między dwoma podmiotami (na przykład sklepem internetowym i klientem) bierze udział osoba trzecia. Celem takich ataków jest przechwycenie informacji lub środków pieniężnych. Celem może być również podsłuchanie poufnych informacji oraz ich modyfikacja. Jak się bronić? Szyfrowanie transmisji danych, certyfikaty bezpieczeństwa.

Cross-site scripting – jest to atak, który polega na umieszczeniu na stronie internetowej specjalnego kodu, który może skłonić użytkowników do wykonania działania, którego nie planowali. Jak się bronić? Przede wszystkim używać zaufanego (legalnego) oprogramowania oraz dobrego programu antywirusowego.

DDos (distributed denial of service) – rozproszona odmowa usługi, jest to atak polegający na jednoczesnym logowaniu się na stronę internetową wielu użytkowników, w celu jej zablokowania. Głównie wykorzystywana jest w walce politycznej oraz w e-commerce, gdy w czasie szczególnie atrakcyjnej promocji konkurencja wzmacnia sztucznym ruchem naturalne zainteresowanie użytkowników, by w ten sposób unieszkodliwić sklep.

Jak się bronić? Przed atakami DDoS brakuje skutecznych narzędzi ochrony, oprócz dobrze skonfigurowanego firewall u dostawcy usług internetowych.

SQL Injection – atak tego rodzaju polega na uzyskaniu nieuprawnionego dostępu do bazy danych poprzez lukę w zabezpieczeniach aplikacji, na przykład systemu do obsługi handlu internetowego. Dzięki temu, cyberprzestępca może wykraść informacje od firmy, na przykład dane kontaktowe klientów. Jak się bronić? Odpowiednie zabezpieczenia na poziomie bazy danych.

Malvertising – zalicza się do szczególnie złośliwego ataku, ponieważ pozwala dotrzeć do użytkowników przeglądających jedynie zaufane strony internetowe. Ich nośnikiem są reklamy internetowe wyświetlane poprzez sieci takie jak np. Google Adwords. Poprzez reklamy może być zainstalowane złośliwe oprogramowanie na komputerze. Takie oprogramowania wykorzystywane są również do wydobywania krypto walut poprzez urządzenia przeglądających. Jak się bronić? Należy stosować filtry blokujące reklamy.

II. Sposoby zabezpieczenia przed zagrożeniami:

1. Stosuj zasadę ograniczonego zaufania do odbieranych wiadomości e-mail, SMS, stron internetowych nakłaniających do podania danych osobowych, osób podających się za przedstawicieli firm, instytucji, którzy żądają podania danych autoryzacyjnych lub nakłaniających do instalowania aplikacji zdalnego dostępu.
2. Nie ujawniaj danych osobowych, w tym danych autoryzacyjnych dopóki nie ustalisz czy rozmawiasz z osobą uprawnioną do przetwarzania Twoich danych.
3. Instaluj aplikacje tylko ze znanych i zaufanych źródeł.
4. Nie otwieraj wiadomości e-mail i nie korzystaj z przesłanych linków od nadawców, których nie znasz.
5. Każdy e-mail można sfałszować, sprawdź w nagłówku wiadomości pole Received: from (ang. otrzymane od) w tym polu znajdziesz rzeczywisty adres serwera nadawcy.
6. Porównaj adres konta e-mail nadawcy z adresem w polu „From" oraz „Reply to" – różne adresy w tych polach mogą wskazywać na próbę oszustwa.
7. Nie otwieraj plików nieznanego pochodzenia, a wszystkie pobrane pliki skanuj programem antywirusowym.
8. Szyfruj dane poufne (szczególne, które w razie nieuprawnionego ujawnienia mogą narazić na stratę Ciebie lub osobę do której/ o której piszesz) wysyłane pocztą elektroniczną.
9. Bezpieczeństwo wiadomości tekstowych (SMS) - sprawdź adres url, z którego domyślnie dany podmiot/instytucja wysyła do Ciebie smsy, cyberprzestępca może podszyć się pod dowolną tożsamość (odpowiednio definiując numer lub nazwę), otrzymując smsa, w którym cyberprzestępca podszywa się pod numer zapisany w książce adresowej, telefon zidentyfikuje go jako nadawcę wiadomości sms.
10. Jeśli na podejrzanej stronie podałeś swoje dane do logowania lub jeżeli włamano się na Twoje konto e-mail – jak najszybciej zmień hasło.
11. Używaj aktualnego oprogramowania antywirusowego – stosuj ochronę w czasie rzeczywistym, włącz aktualizacje automatyczne, skanuj oprogramowaniem antywirusowym wszystkie urządzenia podłączane komputera – pendrive, płyty, karty pamięci.
12. Aktualizuj system operacyjny, aplikacje użytkowe, programy antywirusowe. Brak aktualizacji zwiększa podatność na cyberzagrożenia. Hakerzy, którzy znają słabości systemu/aplikacji, mają otwartą furtkę do korzystania z luk w oprogramowaniu.
13. Logowanie do e-usług publicznych, bankowości elektronicznej bez aktualnego (wspieranego przez producenta) systemu operacyjnego to duże ryzyko.
14. Nie korzystaj ze stron banków, poczty elektronicznej, które nie mają ważnego certyfikatu bezpieczeństwa. Jak to sprawdzić?
15. Pamiętaj, że żaden bank czy urząd nie wysyła e-maili do swoich klientów/interesantów z prośbą o podanie hasła lub loginu w celu ich weryfikacji.
16. Nie odwiedzaj stron oferujących darmowe filmy, muzykę albo łatwe pieniądze – najczęściej na takich stronach znajduje się złośliwe oprogramowanie.
17. Zwracaj uwagę na nazwę aplikacji, czy nie ma w niej błędów lub literówek – jeśli tak, może być fałszywa i podszywać się pod oficjalną wersję. Zawsze weryfikuj adres nadawcy wiadomości e-mail.
18. Cyklicznie wykonuj kopie zapasowe ważnych danych.

19. Zwracaj uwagę na komunikaty oraz czytaj treści wyświetlane na ekranie komputera.
20. Pamiętaj, aby chronić swój telefon przed osobami trzecimi – stosuj blokadę ekranu,
21. Nigdy nie instaluj aplikacji, do których namawiają cię nieznane osoby trzecie.
22. Popularne oszustwa telefoniczne „na pracownika banku" lub „policjanta" polegają na zmuszeniu ofiary do instalacji aplikacji służącej do przejmowania telefonu.
23. Korzystaj z różnych haseł do różnych usług elektronicznych.
24. Tam, gdzie to możliwe (konta społecznościowe, konto email, usługi e-administracji, usługi finansowe), stosuj dwuetapowe uwierzytelnienie za pomocą np. sms, pin, aplikacji generującej jednorazowe kody autoryzujące, tokenów, klucza fizycznego.
25. Regularnie zmieniaj hasła.
26. Nie udostępniaj nikomu swoich haseł.
27. Pracuj na najniższych możliwych uprawnieniach użytkownika.
28. Unikaj z korzystania otwartych sieci Wi-Fi.
29. Podając poufne dane sprawdź czy strona internetowa posiada certyfikat SSL. Protokół SSL to standard kodowania (zabezpieczania) przesyłanych danych pomiędzy przeglądarka a serwerem.
30. Zadbaj o bezpieczeństwo routera (ustal silne hasło do sieci WI-FI, zmień nazwę sieci Wi-Fi, zmień hasło do panelu administratora, ustaw poziom zabezpieczeń połączenia z siecią Wi-Fi np. WPA2 i wyższe, aktualizuj oprogramowanie routera, wyłącz funkcję WPS, aktywuj funkcję Gościnna Sieć Wi-Fi „Guest Network".

Wykaz podmiotów, które zajmują się cyberbezpieczeństwem:

1. Ministerstwo Cyfryzacji, https://mc.gov.pl
2. CSIRT GOV, https://csirt.gov.pl/
3. CSIRT NASK, https://nask.pl

Zachęcamy również do zapoznania się z cyberzagrożeniami w szerszym zakresie:

Baza wiedzy - cyberbezpieczeństwo
CERT - publikacje
Akademia NASK - publikacje

Zgłaszanie incydentów bezpieczeństwa:
https://incydent.cert.pl/