CYBERBEZPIECZEŃSTWO

Realizując zadania wynikające z ustawy o krajowym systemie cyberbezpieczeństwa przekazujemy informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady jak skuteczne stosować sposoby zabezpieczenia się przed tymi zagrożeniami.

Cyberbezpieczeństwo zgodnie z obowiązującymi przepisami to „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępnośći autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy".

Najpopularniejsze zagrożenia w cyberprzestrzeni:

- ataki z użyciem szkodliwego oprogramowania (malware, wirusy, robaki, itp.),
- blokowanie dostępu do usług,
- kradzieże tożsamości,
- kradzieże (wyłudzenia), modyfikacje bądź niszczenie danych,
- spam (niechciane lub niepotrzebne wiadomości elektroniczne),
- ataki socjotechniczne.

Malware - to szkodliwe lub złośliwe oprogramowanie. Jest to ogół programów mających szkodliwe działanie w stosunku do systemu komputerowego lub jego użytkownika. Złośliwe oprogramowanie może przyjąć formę wirusów, robaków, koni trojańskich i innych.

Ransomware – to oprogramowanie szantażujące, które blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych (często poprzez techniki szyfrujące), a następnie żąda od ofiary okupu za przywrócenie stanu pierwotnego.

Najprostsze typy programów-szantażystów zakładają jedynie blokadę na system, która jest stosunkowo łatwa do zlikwidowania dla doświadczonych użytkowników komputera, natomiast bardziej zaawansowane formy takiego oprogramowania stosują technikę zwaną kryptowirusowym wymuszeniem – szyfrują one pliki ofiary, uniemożliwiając ich normalny odczyt i żądają okupu w zamian za deszyfrację. W prawidłowo przeprowadzonym ataku wymuszeniowym, przywrócenie danych bez posiadania klucza deszyfrującego jest praktycznie niemożliwe. Jednymi z najbardziej znanych i szkodliwych tego typu ataków były WannaCry i NotPetya. Ofiara ataku najczęściej proszona jest o dokonanie płatności (często w kryptowalutach, jak Bitcoin), w celu odblokowania komputera (lub dostępu do zaszyfrowanych danych), jednak pomimo zapłacenia okupu, nie ma gwarancji, że uzyska dostęp do komputera lub plików.

Phishing (podszywanie się) - to jeden z najpopularniejszych typów ataków opartych o wiadomości e-mail lub SMS. Wykorzystuje inżynierię społeczną, czyli technikę polegającą na tym, że przestępcy internetowi próbują oszukać ofiarę i spowodować, aby podjęła działania zgodnie z ich zamierzeniami. Cyberprzestępcy podszywają się m.in. pod firmy kurierskie, urzędy administracji, operatorów telekomunikacyjnych, czy nawet znajomych, starając się wyłudzić dane do logowania np. do kont bankowych lub używanych przez kont społecznościowych, czy systemów biznesowych. Wiadomości phishingowe są tak przygotowywane przez cyberprzestępców, aby wyglądały na autentyczne, ale w rzeczywistości są fałszywe. Mogą próbować skłonić do ujawnienia poufnych informacji, zawierać link do strony internetowej rozprzestrzeniającej szkodliwe oprogramowanie (często przestępcy używają podobnych do autentycznych nazw witryn) lub mieć zainfekowany załącznik.

Spear-phishing - szczególny rodzaj phishingu – zdecydowanie bardziej niebezpiecznym czyli ukierunkowany na konkretnego adresata atak, mający na celu wywarcie określonego wpływu lub wymuszenie działania w stosunku do odbiorcy. Przestępcy mogą podszywać się pod partnerów biznesowych, z którymi współpracujmy, a wiadomość może być spersonalizowana, tzn. bezpośrednio odwoływać się do naszych relacji. Taki typ ataku jest często poprzedzony dokładnym rozpoznaniem przez atakującego naszej firmy, urzędu lub dostępnych o nas danych w mediach społecznościowych.

Vishing – jest to wariant phishingu w wersji głosowej, a dokładnie w formie rozmowy telefonicznej. Atakujący podszywa się pod pracownika instytucji bankowej lub doradcę inwestycyjnego i w taki sposób manipuluje rozmówcę, że ten ujawnia mu wrażliwe dane.

DDos – ataki mają za zadanie zajęcie wszystkich dostępnych i wolnych zasobów w celu uniemożliwienia funkcjonowania

całej usługi w sieci Internet (np. strony internetowej i poczty znajdującej się na hostingu). Atak DDoS polega na przeprowadzeniu ataku równocześnie z wielu miejsc jednocześnie (z wielu komputerów). Atak taki przeprowadzany jest głównie z komputerów, nad którymi przejęta została kontrola przy użyciu specjalnego oprogramowania (np. boty i trojany). Oznacza to, że właściciele tych komputerów mogą nawet nie wiedzieć, że ich komputer, laptop lub inne urządzenie podłączone do sieci, może być właśnie wykorzystywane (bez ich świadomości) do przeprowadzenia ataku DDoS. Atak DDoS rozpoczyna się w momencie, gdy wszystkie przejęte komputery zaczynają jednocześnie atakować usługę WWW lub system ofiary.

Brute force – polega na wykorzystaniu oprogramowania do „odgadywania" danych uwierzytelniających metodą prób i błędów. Ataki siłowe wprowadzają popularne frazy słownikowe, często używane hasła lub określone kombinacje liter i cyfr, dopóki nie uzyskają dopasowania w celu odgadnięcia danych logowania, kluczy bezpieczeństwa lub innych poufnych informacji.

Key Logger – program przechwytuje i rejestruje informacje o wciskanych klawiszach na klawiaturze i wysyła je osobie atakującej, dzięki temu może ona poznać login i hasło użytkownika zainfekowanego komputera.

Sposoby zabezpieczenia się przed zagrożeniami:

1. Używaj oprogramowania antywirusowego. Program powinien posiadać ochronę w czasie rzeczywistym.
2. Aktualizuj system operacyjny, oprogramowanie antywirusowe i aplikacje użytkowe.
3. Zwracaj uwagę na komunikaty programu antywirusowego i przeglądarek internetowych.
4. Nie otwieraj plików nieznanego pochodzenia.
5. Nie wchodź na strony z linków w podejrzanych wiadomościach e-mail i nie otwieraj dodanych do nich załączników.
6. Nie wysyłaj w e-mailach żadnych poufnych danych w formie otwartego tekstu.
7. Twórz bezpieczne hasła – unikatowe, nie zawierające oczywistych słów.
8. Nie używaj tego samego hasła.
9. Zachowaj ostrożność podczas wpisywania haseł, zwłaszcza w sytuacjach, gdzie istnieje ryzyko obserwacji przez osoby trzecie.
10. Włącz uwierzytelnianie dwuetapowe, w szczególności dla ważnych usług
11. Podczas logowania dwa razy sprawdź adres www strony.
12. Nie korzystaj ze stron banków, poczty elektronicznej czy portali społecznościowych, które nie mają ważnego certyfikatu,
13. Nie zostawiaj swoich danych osobowych w niesprawdzonych serwisach i na stronach, zawsze czytaj dokładnie Regulaminy i Polityki, weryfikuj na co wyrażasz zgodę
14. Unikaj logowania do serwisów z cudzych urządzeń.
15. Nie loguj się do ważnych usług, wykorzystując publiczne sieci Wi-Fi.
16. Regularnie wykonuj kopie zapasowe danych, których utrata wiąże się z dużymi stratami.
17. Zadbaj o bezpieczeństwo routera (zmień domyślne dane do logowania).
18. Urządzenia mobilne zabezpiecz hasłem.
19. Weryfikuj smsy/maile wzywające do dopłaty za zakupy lub usługi.
20. Przy otrzymaniu połączenia telefonicznego od przedstawiciela banku, przerwij rozmowę i samodzielnie skontaktuj się z bankiem, używając zweryfikowanych i oficjalnych danych kontaktowych banku.
21. Ustal wśród bliskich i znajomych bezpieczne hasło które potwierdzi tożsamość rozmówcy.

Dodatkowe informacje dotyczące cyberbezpieczeństwa:
Dla każdego - cyberhigiena - Baza wiedzy - Portal Gov.pl (www.gov.pl)
OUCH! to cykliczny, darmowy zestaw porad bezpieczeństwa dla użytkowników komputerów