CYBERBEZPIECZEŃSTWO – PODSTAWOWE INFORMACJE I ZASADY

W świetle obowiązującej ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 art. 2 pkt 4) Cyberbezpieczeństwo to „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy".

Pragniemy przedstawić Państwu najważniejsze zagadnienia dot. niebezpieczeństw, które mogą Państwo napotkać w szeroko rozumianej cyberprzestrzeni oraz przedstawić podstawowe informacje.

Cyberatak to przede wszystkim celowe i świadome działanie, do którego wykorzystywane są systemy i sieci komputerowe, by przy użyciu złośliwego oprogramowania dokonać kradzieży lub zniszczenia danych. Brak naszej ostrożności, naiwność czy socjotechnika stosowana przez popełniających takie ataki sprawia, że z roku na rok liczba cyberataków rośnie.

Do najpopularniejszych zagrożeń w cyberprzestrzeni możemy zaliczyć:

- kradzieże tożsamości,
- kradzieże (wyłudzenia), modyfikacje bądź niszczenie danych,
- blokowanie dostępu do stron i usług elektronicznych,
- 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.

NAJWAŻNIEJSZE POJĘCIA ZWIĄZANE Z CYBERATAKAMI:

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, jak 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 lub 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 ich do wykonania działania, którego nie planowali.

Jak się bronić ? Przede wszystkim korzystanie z zaufanego oprogramowania oraz dobrego programu antywirusowego.

Atak typu 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 skonfigurowanemu firewallowi 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.

W każdym systemie bezpieczeństwa najsłabszym ogniwem jest człowiek dlatego w celu ochrony przed zagrożeniami należy stosować możliwie najwięcej z poniżej wyszczególnionych zabezpieczeń:

1. Używaj aktualnego oprogramowania antywirusowego – stosuj ochronę w czasie rzeczywistym, włącz aktualizacje automatyczne,
2. Skanuj oprogramowaniem antywirusowym wszystkie urządzenia podłączane do komputera – pendrivy, płyty, karty pamięci,
3. Aktualizuj system operacyjny i posiadane oprogramowanie,
4. Nie otwieraj plików nieznanego pochodzenia, a wszystkie pobrane pliki skanuj programem antywirusowym,
5. Nie korzystaj ze stron banków, poczty elektronicznej, które nie mają ważnego certyfikatu bezpieczeństwa,

   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,
6. Cyklicznie skanuj komputer oprogramowaniem antywirusowym,
7. Nie odwiedzaj stron oferujących darmowe filmy, muzykę albo łatwe pieniądze – najczęściej na takich stronach znajduje się złośliwe oprogramowanie,
8. Nie podawaj swoich danych osobowych na stronach internetowych, co do których nie masz pewności, że nie są one widoczne dla osób trzecich,
9. Zwracaj uwagę na nazwę aplikacji, czy nie ma w niej błędów lub literówek – jeśli tak, może być fałszywa i podszywać się pod oficjalną wersję, czytaj opinie i komentarze osób, które już z niej korzystają. Jeśli są negatywne lub niskie, poszukaj innego rozwiązania,

10. Zawsze weryfikuj adres nadawcy wiadomości e-mail,
11. Zawsze zabezpieczaj hasłem lub szyfruj wiadomości e-mail zawierające poufne dane – hasło przekazuj innym sposobem komunikacji,
12. Cyklicznie wykonuj kopie zapasowe ważnych danych,
13. Zawsze miej włączoną - zaporę sieciową „firewall”,
14. Zwracaj uwagę na komunikaty oraz czytaj treści wyświetlane na ekranie komputera,
15. Pamiętaj, aby chronić swój telefon przed osobami trzecimi – stosuj blokadę ekranu,
16. Nigdy nie instaluj aplikacji, do których namawiają cię nieznane osoby trzecie. Popularne oszustwa telefoniczne „na pracownika banku” lub „policjanta” polegają na zmuszeniu ofiary do instalacji aplikacji służącej do przejmowania telefonu.

REKOMENDACJE DLA OBYWATELI:

- Zapoznaj się z poradnikiem dotyczącym bezpieczeństwa skrzynek pocztowych i kont w mediach społecznościowych oraz zastosuj się do jego rekomendacji.
- Bądź wyczulony na sensacyjne informacje, w szczególności zachęcające do natychmiastowego podjęcia jakiegoś działania. Weryfikuj informacje w kilku źródłach. Upewnij się, że informacja jest prawdziwa przed podaniem jej dalej w mediach społecznościowych. Jeśli masz jakieś wątpliwości, wstrzymaj się.
- Uważaj na wszelkie linki w wiadomościach mailowych i SMS-ach, zwłaszcza te sugerujące podjęcie jakiegoś działania, np. konieczność zmiany hasła, albo podejrzaną aktywność na koncie. Obserwowaliśmy w przeszłości tego typu celowane ataki na prywatne konta, gdzie celem było zdobycie informacji zawodowych.
- Upewnij się, że posiadasz kopię zapasową wszystkich ważnych dla siebie plików i potrafisz je przywrócić w przypadku takiej potrzeby.
- Zgłaszaj każdą podejrzaną aktywność przez formularz na stronie incydent.cert.pl lub mailem na cert@cert.pl. Podejrzane SMS-y prześlij bezpośrednio na numer 799 448 084. Rekomendujemy zapisanie go w kontaktach.

MATERIAŁY

- **Ustawa o Krajowym Systemie Cyberbezpieczeństwa (pdf, 1,28 MB)**
- **Najczęściej zgłaszane incydenty do CERT Polska w latach 2017-2020 (pdf, 1,15 MB)**
- **Przykłady zagrożeń (pdf, 1,40 MB)**
- **Poradnik dotyczący bezpieczeństwa skrzynek pocztowych i kont w mediach społecznościowych (pdf, 418 KB)**

Aby zrozumieć zagrożenia i umiejętnie stosować zabezpieczenia przedstawiamy Państwu kilka ciekawych propozycji z którymi warto się zapoznać :

Aktualności oraz Baza wiedzy.
Link: https://www.gov.pl/web/baza-wiedzy/aktualnosci

OUCH! To cykliczny, darmowy zestaw porad bezpieczeństwa dla użytkowników komputerów. Każde wydanie zawiera krótkie, przystępne przedstawienie wybranego zagadnienia z bezpieczeństwa komputerowego wraz z listą wskazówek jak można chronić siebie, swoich najbliższych i swoją organizację.
Link: https://cert.pl/ouch/

STÓJ. POMYŚL. POŁĄCZ. jest polską wersją międzynarodowej kampanii STOP. THINK. CONNECT.™, mającej na celu podnoszenie poziomu świadomości społecznej w obszarze cyberbezpieczeństwa.
Link: https://stojpomyslpolacz.pl/
oraz materiały do pobrania: https://stojpomyslpolacz.pl/stp/materialy-do-pobrania

Zespół CERT Polska działa w strukturach NASK – Państwowego Instytutu Badawczego, prowadzącego działalność naukową, krajowy rejestr domen .pl i dostarczającego zaawansowane usługi teleinformatyczne. CERT Polska to pierwszy powstały w Polsce zespół reagowania na incydenty. Dzięki prężnej działalności od 1996 roku w środowisku zespołów reagujących, stał się rozpoznawalnym i doświadczonym podmiotem w dziedzinie bezpieczeństwa komputerowego.
Link : https://www.cert.pl/

Podmioty zajmujące się cyberbezpieczeństwem:

Ministerstwo Cyfryzacji:

- CERT Polska, https://cert.pl/
- CSIRT GOV, https://csirt.gov.pl/
- CSIRT NASK, https://www.nask.pl/pl/dzialalnosc/csirt-nask/3424,CSIRT-NASK.html

---