Cyberbezpieczeństwo

W celu realizacji zadań wynikających z ustawy o krajowym systemie cyberbezpieczeństwa przekazujemy Państwu podstawowe zasady bezpiecznego poruszania się w cyberprzestrzeni oraz dostęp do informacji z zakresu cyberbezpieczeństwa

Podstawowe zasady bezpiecznego poruszania się w cyberprzestrzeni

- Zawsze stosuj sprawdzone oprogramowanie przeciw wirusom i spyware, najlepiej z funkcjonalnością firewalla,
- Przeprowadzaj regularne aktualizacje oprogramowania oraz baz danych wirusów,
- Nie otwieraj plików nieznanego pochodzenia,
- Zawsze skanuj pobrane pliku z Internetu za pomocą programu antywirusowego,
- Regularnie skanuj swój komputer oprogramowaniem antywirusowym,
- Nie podawaj swoich danych osobowych, informacji dot. kart płatniczych na niezweryfikowanych stronach, które nie wzbudzają Twojego zaufania,
- Przed wysłaniem w wiadomości swoich danych poufnych, pamiętaj o ich zaszyfrowaniu,
- **Pamiętaj, że żaden bank nie wysyła e-maili do swoich klientów z prośbą o podanie hasła lub loginu w celu ich weryfikacji,**
- Nie podłączaj do komputera nośników (pendrive, płyty DVD, CD i inne) niewiadomego pochodzenia,
- Stosuj tzw. mocne hasła, składające się z co najmniej 12 znaków, zawierające cyfry, wielkie oraz małe litery, znaki specjalne,
- Pamiętaj aby stosować różne hasła do różnych usług oraz aplikacji,
- Unikaj korzystania z publicznych dostępów Wi-Fi, a w szczególności nie korzystaj z nich przy realizacji transakcji finansowych.

Poradnik zabezpieczania się przed cyberzagrożeniami

Ataki wymierzone w urządzenia sieciowe

W gospodarstwie domowym oraz w firmie większość urządzeń takich jak SmartTV, urządzenia mobilne, Smart House, czujniki oraz wiele innych jest już podłączona do Internetu. Często te urządzenia są dość słabo zabezpieczone oraz nie aktualizowane, stąd też stanowią łatwy łup dla cyberprzestępców.

Porady:

a. regularnie aktualizuj oprogramowanie na wszystkich urządzeniach podłączonych do Internetu,
b. ogranicz dostęp z Internetu do urządzeń, które nie wymagają takiego połączenia,
c. regularnie monitoruj swoją infrastrukturę sieciową.

Zalecenia:

a. podzielenie sieci na segmenty, z wydzieleniem sieci dla urządzeń potencjalnie zagrożonych takich jak np. monitoring, systemy przeciwpożarowe, wszelkiego rodzaju czujniki.
b. zminimalizowanie zbędnej komunikacji z Internetem dla wrażliwych segmentów.

Ransomware

Oprogramowanie tego typu ogranicza dostęp do systemu komputerowego i wymaga opłacenia okupu, aby blokada została usunięta. Najbardziej popularne ataki ransomware były spowodowane przez złośliwe oprogramowanie WannaCry, Petya, Cryptlolocker i Locky.

Porady:

a. regularnie wykonuj kopie bazy danych i przechowuj je na urządzeniach, które nie są permanentnie podłączone do Twojego komputera lub serwera,
b. zabezpiecz komputery pracowników za pomocą programów antywirusowych,
c. organizuj szkolenia budujące świadomość zagrożeń. Jedną z najczęstszych metod infekowania komputerów przez oprogramowanie ransomware jest inżynieria społeczna. Dlatego warto poznawać sposoby wykrywania tego typu zagrożeń, podejrzanych stron i innych prób oszustwa.

Zalecenia:

a. aby chronić się przed takimi atakami przydatne są urządzenia bezpieczeństwa brzegu sieci. Dzięki takim urządzeniom realne staje się wykrycie złośliwego kodu szyfrującego jeszcze zanim zablokowany zostanie dostęp do najbardziej newralgicznych danych.
b. na każdej stacji roboczej powinien być zainstalowany aktualny program antywirusowy.

Ataki wykorzystujące luki w oprogramowaniu

Cyberprzestępcy stawiają coraz większy nacisk na wyszukiwanie podatności istniejących we wszystkich - dostępnych z poziomu Internetu - elementach infrastruktury. Wykryte luki mogą zostać wykorzystane do przeprowadzenia ataku.

Porady:

a. opracuj politykę aktualizacji oprogramowania na wszystkich urządzeniach podłączonych do sieci, aktualizacje w większości przypadków zawierają w sobie łatki na te luki,
b. systematycznie modernizuj swoje rozwiązania sieciowe i aplikacyjne,
c. podczas tworzenia programu opieraj się na dobrych praktykach tworzenia kodu,
d. wykorzystuj dodatkowe usługi, oferowane przez operatorów, np. WAF (Web Application Firewall).

Zalecenia:

a. tak jak w pierwszym opisywanym przypadku separuj segmenty sieci infrastruktury krytycznej od Internetu,
b. dokonaj oceny poziomu bezpieczeństwa swojej infrastruktury sieciowej. Znajdź w niej słabe i mocne strony. W tym obszarze pomocne są m.in. testy penetracyjne, które mogą być wykonywane na zlecenie zewnętrznych firm,
c. Warto również użyć firewalla aplikacyjnego (WAF), który ukierunkowany jest na wykrywanie ataków i ochronę aplikacji w wyższych warstwach komunikacji.

Rozproszone ataki DDoS

Celem ataków DDoS jest doporowadzenie do sytuacji, w której konkretne usługi obecne w Internecie będą niedostępne, a sam atak – chociażby z tytułu rozproszenia – będzie trudny do zablokowania.

Porady:

a. monitoruj sprawność infrastruktury sieciowej,
b. wykorzystuj usługi ochrony przez atakami na poziomie ISP,
c. prewencyjne wykorzystaj rozwiązania odseparowujące ruch DDoS lub skorzystaj z usług dostawcy Internetu.

Zalecania:

a. wykorzystaj wsparcie ze strony dostawcy usług infrastrukturalnych, w tym dostawcy Internetu,
b. przeanalizuj infrastrukturę sieci pod kątem wykrycia newralgicznych punktów i tzw. „wąskich gardeł”,

c. wdróż systemy monitoringu infrastruktury na potrzeby wczesnego wykrywania ataków DDoS,
d. zapewnienij jak najwyższą skalowalność środowiska sieciowo-aplikacyjnego.

Phishing

Ataki phishingowe mają na celu podszycie się pod znaną markę, osobę lub bank, aby uzyskać dostęp do Twoich wrażliwych danych. Najczęściej do rozsyłania phishingu wykorzystywane są e-maile.

Porady:

a. zainstaluj oraz regularnie aktualizuj oprogramowanie antywirusowe i antyspamowe pozwalające weryfikować poprawność wiadomości,
b. weryfikuj nadawców wiadomości lub komunikatów,
c. przeprowadź szereg szkoleń i buduj dobre nawyki wśród użytkowników.

Zalecenia:

a. wprowadź politykę postępowania w najbardziej newralgicznych obszarach – jak akceptacja wydatków, przekazywanie danych dostępowych, czy praca z załącznikami,
b. regularnie monitoruj działania infrastruktury IT.

Przydatne linki:

- Informacje z zakresu cyberbezpieczeństwa: https://www.cert.pl/
- Cykliczny, darmowy zestaw porad bezpieczeństwa dla użytkowników komputerów: https://www.cert.pl/ouch/