2024-03-14

Cyberbezpieczeństwo

Cyberbezpieczeństwo

Zgodnie art. 22 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2023 r., poz. 913) przedstawiamy Państwu podstawowe informacje dotyczące cyberbezpieczeństwa, jego zagrożeń i sposobów, w jaki sposób uchronić się przed incydentami.

Celem ustawy o krajowym systemie cyberbezpieczeństwa jest określenie organizacji oraz sposobu funkcjonowania krajowego systemu cyberbezpieczeństwa, a także sposoby sprawowania nadzoru i kontroli w zakresie stosowania jej przepisów.

Cyberbezpieczeństwo to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy (art. 2 pkt 4 u.k.s.c.). Pojęcie to stanowi normatywną konstrukcję myślową oznaczającą bezpieczeństwo systemów i sieci (IT).

Incydenty - wszelkie zdarzenia mające lub mogące mieć niekorzystny wpływ na cyberbezpieczeństwo.

Najczęstszą przyczyną skutecznych cyberataków nie są jednak wadliwe zabezpieczenia fizyczne czy źle napisane oprogramowanie. Najczęstszą przyczyną skutecznych ataków cyberprzestępców są stosowane przez nich skuteczne socjotechniki, czyli przemyślane oszustwa, manipulacja i pozyskiwanie informacji niekoniecznie za pośrednictwem Internetu.

Najczęściej występujące zdarzenia, mające niekorzystny wpływ na cyberbezpieczeństwo:

1. Phishing - metoda oszustwa internetowego, za którego pośrednictwem przestępca podszywa się pod jakąś instytucję lub osobę. Działanie to ma na celu wyłudzenie osobistych danych, takich jak: numery kont bankowych i kart kredytowych, hasła do logowania oraz inne poufne informacje.
2. Ransomware - atak z użyciem szkodliwego oprogramowania („wirus komputerowy”, „robak”, „koń trojański”).
3. Wiadomości SPAM- niechciana, niezamówiona wiadomość/korespondencja wysyłana za pomocą poczty elektronicznej.
4. Kradzież tożsamości - nielegalne wykorzystanie danych osobowych ofiary przez oszusta, dająca mu możliwość podszycia się pod te osobę w celu uzyskania korzyści (zazwyczaj majątkowych).
5. Przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp.

Aby zmniejszyć ryzyko skutków ataków hakerskich i incydentów utraty danych należy stosować się do niżej wymienionych zasad:

1. Ograniczone zaufanie - zdecydowana większość wiadomości phishingowych jest dostarczana za

pośrednictwem poczty elektronicznej lub portali społecznościowych. Zazwyczaj banki, firmy usługowe nie wysyłają e-maili z prośbą o podanie swoich danych do zalogowania się na ich stronach;
2. Hiperłącza (linki) - nie należy otwierać hiperłączy (linków) bezpośrednio z otrzymanego e-maila (szczególnie jeżeli pochodzi od nieznanej osoby lub organizacji). Stosunkowo łatwo można zmodyfikować treść hiperłącza (linku) w taki sposób, by pozornie wskazujące na autentyczną witrynę kierowały do nieautoryzowanej podszywającej się strony;
3. Aktualizacje - należy regularnie uaktualniać system i oprogramowanie w szczególności przeglądarkę. Nowsze wersje przeglądarek mają wbudowane mechanizmy antyphishingowe, które nawet po kliknięciu w spreparowane łącze mogą zablokować do niego dostęp;
4. Instalacja, użytkowanie i bieżące aktualizowanie oprogramowania antywirusowego, posiadającego pełen pakiet bezpieczeństwa, tj. możliwość sprawdzania poczty pod kątem niebezpiecznych programów czy zabezpieczenie w postaci prostego firewalla.

Ważne: Darmowe wersje programów antywirusowych często nie posiadają istotnych aktualizacji oraz rozszerzeń, które zapewniają dużo lepszą ochronę komputera oraz jego zawartości. Płatne wersje programów chroniących przed wirusami posiadają nie tylko firewall, ale również usługę skanowania poszczególnych linków oraz witryn, a także bardzo potrzebne- zabezpieczenie internetowych transakcji bankowych, które narażone są na działanie hakerów;

1. Dbałość o hasła - przestrzeganie zasad nadawania i zmiany hasła, wystrzeganie się automatycznego zapisywania haseł i loginów;
2. Dbałość o dane osobowe- unikanie przesyłania poprzez wiadomości e-mail wiadomości z danymi osobistymi, hasłami, numerami kart kredytowych, pełnych danych logowania do systemu w postaci niezaszyfrowanej.
   Bezwzględne należy w przypadkach konieczności wysyłania danych stosować procedury szyfrowania danych;
3. Regularne tworzenie kopii zapasowych ważnych danych;
4. Korzystanie ze stron internetowych posiadających ważny certyfikat bezpieczeństwa - uwaga na fałszywe certyfikaty, które stały się obecnie bardzo łatwe do wystawienia i przestępcy chętnie z tej opcji korzystają, aby podnieść wiarygodność fałszywej strony;
5. Każdorazowa weryfikacja adresu nadawcy wiadomości e-mail oraz treści wiadomości, wszystkie podejrzane maile muszą być sprawdzone - szczególnie mailowe zlecenia przelewów, pochodzące od nieznajomych użytkowników.

Czerwona lampka powinna zapalić się nam, gdy:

- w pustej wiadomości znajduje się załącznik,
- wiadomość nie zawiera żadnych osobistych zwrotów,
- wiadomość podpisana jest przez nadawcę, którego dane adresowe ze stopki e-mail nie odpowiadają danym w domenie, z której e-mail został wysłany,
- wiadomość pochodzi z nieznanego źródła i zawiera skompresowany zaszyfrowany załącznik,
- załącznik ma nazwę o podwójnym rozszerzeniu- należy zwracać uwagę na przesyłane pliki zakończone rozszerzeniami .exe, .bat, .cmd, .com, .lnk, .pif, .scr, .vb, .vbs, .wsh. Lista ta nie jest wyczerpująca. Hakerzy mogą ukrywać złośliwe programy za fałszywymi rozszerzeniami. Domyślnie Windows ukrywa rozszerzenia plików. Plik image.jpg może w rzeczywistości być plikiem image.jpg.exe, a po dwukrotnym kliknięciu uruchomi się złośliwy plik .exe.

Hakerzy mogą również ustawić dowolną ikonę dla pliku .exe. Plik o nazwie image.jpg.exe korzystający ze standardowej ikony obrazu będzie wyglądał jak nieszkodliwy obraz z domyślnymi ustawieniami systemu Windows. Warto sprawdzać rozszerzenia w ustawieniach.

1. Edukacja - podnoszenie świadomości oraz rozwijanie wiedzy użytkowników o aktualnych trendach w bezpieczeństwie są kluczowe do dalszego bezpiecznego korzystania z sieci.

Rekomenduje się zapoznanie się z niżej wymienionymi poradnikami:

- Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego;
- Cyberhigiena dla każdego - serwis Rzeczypospolitej Polskiej;
- Bezpieczny pracownik w sieci.

Podmioty zajmujące się cyberbezpieczeństwem:

- Strona internetowa Ministerstwa Cyfryzacji;
- Strona internetowa CERT Polska;
- Strona internetowa Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego;
- Strona Państwowego Instytutu Badawczego - NASK;
- Strona internetowa Ministerstwa Obrony Narodowej;
- Strona internetowe Niebezpiecznik;
- Strona internetowa Zaufana Trzecia Strona;
- Strona internetowa Legalne w Sieci;
- Strona internetowa Cyberdefence24;
- Strona internetowa Cyberresccue;
- Strona internetowa Nomoreransom.

Zachęcamy również do zapoznania się z treściami zawartymi na stronie Ministerstwa Cyfryzacji pod adresem: https://www.gov.pl/web/cyfryzacja/cyberbezpieczeństwow celu uzyskania szczegółowych informacji dotyczących cyberbezpieczeństwa.