Cyberbezpieczeństwo

W związku z zadaniami wynikającymi z ustawy o krajowym systemie cyberbezpieczeństwa przedstawiamy Państwu podstawowe informacje dotyczące cyberbezpieczeństwa, zagrożeń i sposobów zabezpieczenia się przed nimi.

Cyberbezpieczeństwo zgodnie z obowiązującymi przepisami, to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Wszelkie zdarzenia mające lub mogące mieć niekorzystny wpływ na cyberbezpieczeństwo nazywane są **zagrożeniami lub incydentami**.

Najpopularniejsze zagrożenia w cyberprzestrzeni to:

- ataki socjotechniczne (przykładowo phishing, czyli metoda polegająca na wyłudzaniu poufnych informacji przez podszycie się pod godną zaufania osobę lub instytucję);
- kradzieże (wyłudzenia), modyfikacje lub niszczenie danych;
- kradzieże tożsamości;
- ataki z użyciem szkodliwego oprogramowania (malware, wirusy, robaki, itp.);
- blokowanie dostępu do usług;
- spam (niechciane lub niepotrzebne wiadomości elektroniczne mogące zawierać odnośniki do szkodliwego oprogramowania).

Przykładowe sposoby zabezpieczenia się przed zagrożeniami:

- aktualizowanie systemu operacyjnego i aplikacji bez zbędnej zwłoki;
- instalacja i użytkowanie oprogramowania przeciw wirusom i spyware. Najlepiej stosować ochronę w czasie rzeczywistym;
- aktualizacja oprogramowania antywirusowego oraz bazy danych wirusów;
- sprawdzanie plików pobranych z Internetu za pomocą programu antywirusowego;
- pamiętanie o uruchomieniu firewalla;
- nie otwieranie plików nieznanego pochodzenia;
- korzystanie ze stron banków, poczty elektronicznej czy portali społecznościowych, które mają ważny certyfikat bezpieczeństwa, chyba, że masz stuprocentową pewność z innego źródła, że strona taka jest bezpieczna;
- regularne skanowanie komputera i sprawdzanie procesów sieciowych. Jeśli się na tym nie znasz poproś o sprawdzenie kogoś, kto się zna. Czasami złośliwe oprogramowanie nawiązujące własne połączenia z Internetem, wysyłając twoje hasła i inne prywatne dane do sieci. Może również zainstalować się na komputerze mimo dobrej ochrony;
- nie używanie niesprawdzonych programów zabezpieczających czy też do publikowania własnych plików w Internecie (mogą one np. podłączać niechciane linijki kodu do źródła strony);
- regularne wykonywanie kopii zapasowych ważnych danych;
- staranie się aby nie odwiedzać zbyt często stron, które oferują niesamowite atrakcje (darmowe filmiki, muzykę, albo łatwy zarobek przy rozsyłaniu spamu) – często na takich stronach znajdują się ukryte wirusy, trojany i inne zagrożenia;
- nie zostawianie danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie ma się absolutnej pewności, że nie są one widoczne dla osób trzecich oraz nie wysyłanie w wiadomościach e-mail żadnych poufnych danych w formie otwartego tekstu przykładowo dane powinny być zabezpieczone hasłem i zaszyfrowane. Hasło najlepiej przekazuj w sposób bezpieczny przy użyciu innego środka komunikacji;

- należy pamiętać, że żaden bank czy Urząd nie wysyła e-maili do swoich klientów/interesantów z prośbą o podanie hasła lub loginu w celu ich weryfikacji.

Co to jest incydent?

Incydent to każde zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo.

Nie wszystkie incydenty niosą za sobą takie samo zagrożenie. Jak definiujemy te najgroźniejsze?

- Incydent krytyczny – to incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi. Incydenty jako krytyczne klasyfikują właściwe CSIRT (MON, NASK lub GOV).
- Incydent poważny – to incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej. (Usługa kluczowa – to usługa, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej – wykaz tych usług umieszcza się w wykazie usług kluczowych. Podmioty świadczące te usługi nazywamy operatorami usług kluczowych.)
- Incydent istotny - to incydent, który ma istotny wpływ na świadczenie usługi cyfrowej.
- Incydent w podmiocie publicznym - to incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny.

Incydenty klasyfikujemy zgodnie z następującym wykazem:

1. Złośliwe oprogramowanie
2. Przełamywanie zabezpieczeń
3. Niepożądane treści
4. Gromadzenie informacji
5. Dostępność zasobów
6. Bezpieczeństwo informacji
7. Naruszenie przepisów prawa
8. Inne
9. Zgłoszenie podatności

Jak zgłosić incydent?

W zależności gdzie wystąpił incydent i tak:

1. jeśli incydent wystąpił:

- w systemie Urzędu Miejskiego w Boguchwale
- w systemie jednostki podległej Urzędu Miejskiego w Boguchwale
- w systemie nadzorowanym przez Urzędu Miejskiego w Boguchwale
- w systemie innym niż opisany powyżej

zgłaszać incydent można poprzez wypełnienie **formularza** oraz przesłanie emailem na adres informatyk@um.boguchwala.pl wpisując w temacie wiadomości „Zgłoszenie incydentu”. W przypadku braku dostępu do sieci Internet incydent można zgłaszać telefonicznie na nr +48 17 87 55 219 w godzinach pracy Urzędu Miejskiego w Boguchwale.

2. jeśli incydent wystąpił w innym systemie niż opisane powyżej w pkt 1 to incydent należy

zgłaszać do jednego z poniższych podmiotów:

- Do **CSIRT GOV** w przypadku incydentu w systemach:
  - Jednostek sektora finansów publicznych.
  - Jednostek podległych lub nadzorowanych przez Prezesa Rady Ministrów.
  - Narodowego Banku Polskiego lub Banku Gospodarstwa Krajowego.
  - Podmiotu przekazanego do właściwości CSIRT GOV na podstawie porozumienia z CSIR MON lub CSIRT NASK.
- W pozostałych przypadkach incydenty należy zgłaszać do **CSIRT NASK**.

Zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie sposobów zabezpieczania się przed zagrożeniami to wiedza niezbędna każdemu użytkownikowi komputera, smartfona czy też usług internetowych. Należy pamiętać, że najlepszym sposobem na ustrzeżenie się przed negatywnymi skutkami zagrożeń jest działalność zapobiegawcza.

Zachęcamy do zapoznania się z poniżej zawartymi treściami w celu uzyskania szczegółowych informacji dotyczących cyberbezpieczeństwa:

- **Ministerstwo Cyfryzacji** oraz **baza wiedzy**
- **Zestaw porad bezpieczeństwa dla użytkowników komputerów CSIRT NASK** – Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym
- **Publikacje z zakresu cyberbezpieczeństwa**
- **Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV**

Szczegółowa klasyfikacja incydentów
1. Złośliwe oprogramowanie. Incydenty związane ze szkodliwym oprogramowaniem (np. wirusem, robakiem, koniem trojańskim, backdorem itp.) oraz wykryciem zainfekowanego komputera łączącego się z siecią botnetu.
1.1. Oprogramowanie złośliwe w poczcie elektronicznej
1.2. Oprogramowanie złośliwe na stronie WWW
1.3. Oprogramowanie złośliwe na zewnętrznym nośniku danych
1.4. Infekcja systemu operacyjnego
1.5. Klient botnetu
2. Przełamywanie zabezpieczeń. Incydenty związane z podejmowaniem nieuprawnionych prób uzyskania dostępu oraz związanych z uzyskaniem nieuprawnionego dostępu do zasobów.
2.1. Próba włamania
2.1.1. Próba nieuprawnionego logowania / włamania na konto
2.1.2. Próba wykorzystania luk w oprogramowaniu
2.1.3. Próba obejścia zabezpieczeń / wykorzystania podatności w urządzeniu
2.2. Włamanie
2.2.1. Nieuprawnione logowanie / włamanie na konto
2.2.2. Włamanie do aplikacji
2.2.3. Obejście zabezpieczeń / wykorzystanie podatności w urządzeniu
2.2.4. Nieuprawnione wykorzystanie zasobów
3. Niepożądane treści. Incydenty związane z rozpowszechnianiem lub umieszczeniem w

sieci bądź w systemie teleinformatycznym treści niechcianych / niepożądanych.
3.1. Treści obraźliwe
3.2. Spam
4. Gromadzenie informacji. Incydenty związane z nieuprawnionym gromadzeniem informacji o użytkownikach i zasobach systemu lub sieci teleinformatycznej.
4.1. Skanowanie
4.2. Podsłuch
4.3. Inżynieria społeczna
5. Dostępność zasobów. Incydenty związane z utrudnieniem lub zablokowaniem uprawnionego dostępu do zasobów systemu lub sieci teleinformatycznej (ataki, zawieszenie, unieruchomienie lub przeciążenie elementów systemu lub sieci teleinformatycznej mające wpływ na pracę systemu lub sieci).
5.1. Atak blokujący (DoS)
5.2. Rozproszony atak blokujący (DDoS)
5.3. Inny sposób ataku / sabotaż
6. Bezpieczeństwo informacji. Incydenty związane z nieuprawnionym dostępem, zmianą i wykorzystaniem informacji przetwarzanych w systemach teleinformatycznych (w tym kradzież tożsamości, podszycie się) oraz z wykonywaniem czynności mogących mieć negatywnym wpływ na bezpieczeństwo zasobów w systemach teleinformatycznych.
6.1. Nieuprawniony dostęp / wykorzystanie informacji
6.2. Nieuprawniona zmiana informacji
6.3. Naruszenie procedur (świadome, zaniedbanie, brak wiedzy)
6.3.1. Eksploatowanie oprogramowania spoza wykazu programów dopuszczonych do użytkowania
6.3.2. Użytkowanie oprogramowania, w którym nie zaimplementowano wydanych aktualizacji, mających wpływ na jego bezpieczeństwo.
6.3.3. Błędna konfiguracja urządzenia
7. Naruszenie przepisów prawa. Czyny wypełniające znamiona przestępstw o których mowa w art. 202 par. 1, 2, 3, 4a, 4b kodeksu karnego, działania noszące znamiona ataku terrorystycznego w Cyberprzestrzeni, incydenty związane z przesyłanie informacji niejawnych niezgodnie z obowiązującymi przepisami.
7.1. Kopiowanie / rozpowszechnianie plików niezgodnie z przepisami prawa
7.2. Naruszenie praw autorskich
7.3. Pornografia dziecięca
7.4. Przemoc, rasizm, nienawiść
7.5. Cyberterroryzm
7.6 Szpiegostwo
7.7. Pozostałe związane z naruszeniem przepisów prawa
8. Inne. Incydenty związane z awarią zasilania, łączy, sprzętu bądź oprogramowania oraz incydenty nie przyporządkowane do żadnej z powyższych kategorii.
8.1. Awarie (zasilania, łączy, sprzętowe, oprogramowania)
8.2. Pozostałe incydenty komputerowe
9. Zgłoszenie podatności. Zgłoszenia i informacje o potencjalnych podatnościach i zagrożeniach / nie incydenty.

ZAŁĄCZNIK:

Formularz_zglaszania_incydentow_CSIRT_GOV.pdf (Plik pdf 0,11 MB)