**LITERATURA**

1. Poradnik jak chronić się przed cyberatakami – gov.pl/cyfryzacja
2. Poradnik dla samorządowców – ustawa o krajowym systemie cyberbezpieczeństwa.
3. Poradnik – PRCyber-01- jak chronić nasze informacje przed atakami w cyberprzestrzeni?.
4. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

**PRZEBIEG ZAJĘĆ**

****

**Cyberbezpieczeństwo to bezpieczeństwo w świecie cyfrowym** (tzw. cyberprzestrzeni). To

działania niezbędne do ochrony systemów informacyjnych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami. Cyberzagrożenia dotyczą przede wszystkim możliwości utraty poufności, dostępności i integralności danych oraz usług cyfrowych. Na rynku dostępne są różne narzędzia programowe i sprzętowe wspomagające cyberbezpieczeństwo. Żadne z nich nie będą skuteczne, jeśli nie będziemy przestrzegać podstawowych zasad korzystania z usług cyfrowych.

**Incydent w podmiocie publicznym** – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny.

**Organ administracji publicznej** ma obowiązek wyznaczyć jedną osobę kontaktową w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jednostki jemu podległe lub przez niego nadzorowane.

**Jednostka samorządu terytorialnego** może wyznaczyć jedną osobę kontaktową w zakresie zadań publicznych zależnych od systemów informacyjnych realizowanych przez jej jednostki organizacyjne.

Dane osoby kontaktowej należy przekazać do właściwego CSIRT (dla samorządów będzie to CSIRT NASK). Podmiot publiczny, który realizuje zadanie publiczne zależne od systemu informacyjnego, ma obowiązek zapewnić zarządzanie incydentem w podmiocie publicznym**.**

*a) Zgłoszenie incydentu*

**Incydent powinien zostać zgłoszony niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia** do właściwego CSIRT. Zgłoszenie przekazywane jest w postaci elektronicznej, poprzez uzupełnienie formularza internetowego znajdującego się na stronie: https://incydent.cert.pl.

Zgłoszenie zawiera:

* dane podmiotu zgłaszającego, w tym nazwę podmiotu, numer we właściwym rejestrze, siedzibę i adres;
* imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby składającej zgłoszenie;
* imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji;
* opis wpływu incydentu w podmiocie publicznym na realizowane zadanie publiczne (wskazanie zadania publicznego, na które incydent miał wpływ, liczbę osób, na które incydent miał wpływ, moment wystąpienia i wykrycia incydentu oraz czas jego trwania, zasięg geograficzny obszaru, którego dotyczy incydent, przyczynę zaistnienia incydentu i sposób jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne podmiotu publicznego;
* informacje o przyczynie i źródle incydentu;
* informacje o podjętych działaniach zapobiegawczych;
* informacje o podjętych działaniach naprawczych;
* inne istotne informacje.

W momencie zgłoszenia podmiot podaje znane sobie informacje, które mogą być uzupełniane w trakcie obsługi incydentu.

Obowiązek informacyjny

Obsługa incydentu wiąże się również z obowiązkiem przekazania informacji osobom, na rzecz których realizuje się zadanie publiczne. Osoby mają prawo dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami.

**Obowiązek informacyjny może zostać spełniony poprzez publikacje stosownego komunikatu na stronie internetowej.**

**Jak ograniczyć ryzyko cyberataków? - krok po kroku**

**Zainstaluj oprogramowanie antywirusowe**

Obowiązkowo - powinno się znaleźć na każdym komputerze, a także smartfonie i innych urządzeniach podłączonych do internetu, w których możliwe jest instalowanie aplikacji. Współczesne oprogramowanie antywirusowe, stale aktualizowane, zapewnia ponad 95% ochronę przed złośliwym oprogramowaniem - dołączanym do treści wiadomości lub umieszczanym w witrynach internetowych, często specjalnie preparowanych przez cyberprzestępców. Codziennie trwa wyścig pomiędzy twórcami złośliwego oprogramowania a metodami jego wykrywania, ostatnio wspomaganymi tzw. sztuczną inteligencją. Dlatego tak ważne są regularne aktualizacje.

**Aktualizuj oprogramowanie**

Tak jak wspominaliśmy - w świecie technologii cyfrowych trwa nieustanny wyścig pomiędzy producentami sprzętu i oprogramowania, a przestępcami. Ci drudzy cały czas szukają luk i błędów, które mogliby wykorzystać do swoich celów, a firmy po ich wykryciu podejmują działania związane z wprowadzeniem poprawek i dodatkowych zabezpieczeń. Dlatego też **regularna aktualizacja systemu operacyjnego, oprogramowania aplikacyjnego, w tym przeglądarek internetowych, komunikatorów oraz oprogramowania do odbierania i wysyłania poczty e-mail, jest bardzo ważna dla cyberhigieny.**

Takie aktualizacje zawierają bowiem poprawki, które mają ochronić przed znalezionymi podatnościami i błędami. Ich pominięcie to wręcz otwarte zaproszenie dla cyberprzestępców.

**Dbaj o prywatność**

Anonimowość w Internecie nie istnieje, każde działanie pozostawia po sobie cyfrowe ślady, które w jakiś sposób określają daną osobę. Warto zadbać o to, żeby informacje o sobie udostępniać w sposób rozsądny i tylko w takim zakresie, w jakim jest to konieczne. Przede wszystkim należy unikać podawania swoich danych personalnych czy kontaktowych w miejscach, w których nie ma takiej potrzeby.

**Rozsądek przede wszystkim**

Przestępcy do perfekcji mają opanowane najróżniejsze techniki psychologiczne i socjotechniczne, które mają na celu skłonić nieświadomych użytkowników do wykonania określonej czynności. Podszywają się pod znane osoby i firmy, obiecują nagrody czy wykorzystują ciekawość - a wszystko po to, żeby skłonić nas do kliknięcia w link czy otwarcia jakiegoś pliku. Łatwo się domyślić, co się dzieje potem - cyberprzestępcy przejmują kontrolę nad naszym środowiskiem cyfrowym i mogą wykorzystać je do swoich celów. Dlatego też przy korzystaniu z usług internetowych konieczne jest zachowanie odpowiedniej ostrożności.

PAMIĘTAJ!

**Nie otwieraj nieznanych załączników, w szczególności pochodzących od nieznanych nadawców. Nie klikaj w podejrzane linki, choćby miały atrakcyjne brzmiące tytuły... Stosuj się do zasady ograniczonego zaufania.**

**Phishing - cyberprzestępcy na łowach**

Wiele cyberataków jest realizowanych przez phishing. Phishing to metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji (np. danych do logowania, danych zawartych na karcie płatniczej, haseł, kodów PIN), zainfekowania komputera szkodliwym oprogramowaniem, czy też nakłonienia ofiary do określonych działań w celu wyłudzenia pożądanych danych - w szczególności danych do logowania (identyfikator i hasło).

Cyberprzestępcy mogą wysyłać na pozór autentycznie wyglądające wiadomości dotyczące np. konserwacji konta, konieczności zmiany hasła, pilne komunikaty o rzekomych problemach finansowych, żądania kontaktu, powiadomienia o zmianie w usługach lub łącza do dokumentów wymagających do ich otwarcia podania identyfikatora i hasła.

Nazwa phishing budzi dźwiękowe skojarzenia z angielskim słowem „fishing" - czyli łowieniem ryb. Przestępcy, podobnie jak wędkarze, stosują bowiem odpowiednio przygotowaną „przynętę". Do tego wykorzystują sfałszowane e-maile, SMS-y czy wiadomości. Coraz częściej oszuści działają także za pośrednictwem komunikatorów i portali społecznościowych.

**PAMIĘTAJ!**

**Zachowaj szczególną ostrożność w przypadku podejrzanych linków wysyłanych przez e-mail, SMS lub wiadomości z popularnych komunikatorów internetowych i mediów**

**Jak dbać o bezpieczeństwo haseł?**

Za pomocą haseł uzyskujemy dostęp do urządzeń, takich jak laptop lub smartfon, logujemy się do poczty elektronicznej, mediów społecznościowych czy bankowości elektronicznej oraz dokonujemy zakupów w sklepach internetowych. Można powiedzieć, że w wielu przypadkach hasła są niczym klucze do sejfu. W związku z tym, jeśli ktoś byłby w posiadaniu naszego hasła, mógłby dokonać przejęcia naszego konta w mediach społecznościowych, kradzieży naszej tożsamości, transferu pieniędzy lub uzyskać dostęp do naszych prywatnych danych.

**PAMIĘTAJ!**

**Zadbaj o to, aby Twoje hasło było trudne do odgadnięcia**

**Jakich haseł nie powinno się stosować?**

*Ni* Nie stosuj najpopularniejszych haseł, jak: „**hasło", „123456**", „**qwerty**", „**piłka nożna**" itp.; Hasło nie powinno być takie samo jak nazwa użytkownika lub część tej nazwy;

* Hasło nie powinno być imieniem nikogo z naszego najbliższego otocznia (członka rodziny, znajomego ani zwierzaka);
* Nie powinno zawierać danych osobowych Twoich lub Twojej rodziny. Mowa tu o informacjach, które łatwo zdobyć, takie jak data urodzenia, numer telefonu, numer rejestracyjny samochodu, nazwa ulicy, numer mieszkania/domu itd.;
* Nie używaj sekwencji kolejnych liter, liczb lub innych znaków. Na przykład: **„abcde”**, „**12345"**, „**QWERTY”**;
* Nie używaj pojedynczego wyrazu dowolnego języka pisanego normalnie lub wspak, ani tego wyrazu poprzedzonego lub/i zakończonego znakiem specjalnym lub cyfrą;

*N* Nie używaj więcej niż trzech kolejnych znaków na klawiaturze, takich jak „**abc**” lub „**123"**;

* Nie używaj więcej niż dwóch kolejno powtarzających się ciągów znaków np. **”bbbb2bbb”**;
* Nie używaj oczywistych wyrażeń, takich jak np. „**wpuscmnie**".

**Jak stwierdzić, czy zabezpieczenia naszego konta w serwisie społecznościowym zostały złamane?**

Jeśli nie stosujesz podstawowych zasad bezpieczeństwa - uzyskanie dostępu do Twoich kont w serwisach społecznościowych jest dla cyberprzestępców łatwiejsze niż się wydaje.

**Co może świadczyć o włamaniu na konto?**

* Otrzymujesz wiadomość e-mail z informacją o zmianie danych logowania, która nie została przez Ciebie zainicjowana.
* Masz problem z zalogowaniem się do swoich kont.

*O)* Otrzymujesz mnóstwo reklam, które mają charakter spamu.

* Nagle zauważasz, że obserwujesz osoby, których nie znasz.
* Na Twoim koncie jest publikowana zawartość, która nie została przez Ciebie utworzona.

*W* Widzisz konto, które wykorzystuje Twoje imię i nazwisko i/lub Twoje zdjęcia.

**Co robić, kiedy podejrzewamy, że konto zostało zaatakowane?**

**Postaraj się zalogować i sprawdzić dane dotyczące konta (adres e-mail i telefon), aby podjąć próbę sprawdzenia, kto ma dostęp do Twoich informacji**

Gdy tylko zorientujesz się, że zabezpieczenia Twoich kanałów społecznościowych zostały złamane, sprawdź informacje dotyczące konta, aby przekonać się, czy żaden inny adres e-mail - poza Twoim adresem - nie ma dostępu do konta. Jeśli tak jest, natychmiast usuń ten adres.

Następnie sprawdź numer telefonu powiązany z Twoim kontem - jedynie Twój numer telefonu powinien być powiązany z kontem. Jeśli na koncie znajdują się jakiekolwiek nieznane numery, usuń je.

Często zdarza się, że po złamaniu zabezpieczeń konta atakujący dodaje do niego numer telefonu, którego może użyć w późniejszym czasie do zmiany hasła do konta.

**Natychmiast zmień hasło na nowe - silne i niepowtarzalne - i włącz uwierzytelnianie dwuskładnikowe.**

**Sprawdź swoje konta w innych serwisach społecznościowych i poszukaj zaleceń dotyczących czynności w przypadku ataku.**

W serwisach społecznościowych publikowane są zalecenia dotyczące działań, jakie należy podjąć, jeśli zabezpieczenia konta zostały złamane. Dzięki zawartym tam informacjom będziesz mieć pewność, że robisz wszystko, co możliwe, by zabezpieczać i chronić swoje konta.

Oto linki do wskazówek, co zrobić w przypadku ataków na konta w popularnych serwisach społecznościowych:

Facebook -<https://www.facebook.com/hacked>

Twitter -<https://help.twitter.com/pl/rules-and-policies/twitter-report-violation>

Instagram - <https://help.instagram.com/>



