PORADNIK CYBERBEZPIECZEŃSTWA

Realizując zadania wynikające z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa przekazujemy Państwu dostęp do informacji pozwalających na zrozumienie zagrożeń wynikających z cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami.

Co to jest cyberbezpieczeństwo?
Zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa, poprzez cyberbezpieczeństwo należy rozumieć „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy".

Cyberbezpieczeństwo (ang. cybersecurity) stanowi zespół zagadnień związanych z zapewnianiem ochrony w obszarze cyberprzestrzeni. Z pojęciem cyberbezpieczeństwa związana jest między innymi ochrona przestrzeni przetwarzania informacji oraz zachodzących interakcji w sieciach teleinformatycznych. **Cyberprzestrzeń** rozumiana jest natomiast jako przestrzeń przetwarzania i wymiany informacji, tworzona przez systemy teleinformatyczne, wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami (*Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego (2013), Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, Warszawa).*

Celem cyberprzestępców zwykle jest kradzież danych użytkowników. Kradzież odbywać się może podczas niewielkich, dyskretnych ataków na pojedyncze ofiary lub podczas masowych operacji cyberprzestępczych na dużą skalę z wykorzystaniem stron internetowych www. i włamań do baz danych. Metody mogą być różne, ale cel pozostaje ten sam. W większości przypadków napastnicy próbują w pierwszej kolejności dostarczyć na komputer ofiary rodzaj szkodliwego oprogramowania, jako że jest to najkrótsza droga pomiędzy nimi a danymi użytkownika. Zamiary cyberprzestępcy ukierunkowane mogą być również na dokonanie strat finansowych w atakowanej instytucji lub utraty reputacji konkurencji, która zostaje sparaliżowana przez niedostępność usług, bądź w celu uzyskania okupu.

Co to jest zagrożenie cyberbezpieczeństwa? jest to potencjalna przyczyna wystąpienia incydentu;
Co to jest incydent? jest to zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo.

Rodzaje zagrożeń cyberbezpieczeństwa m.in. jest to:
Phishing jest to metoda oszustwa, oznaczająca w tradycyjnym rozumieniu tego słowa podszywania się (przede wszystkim z wykorzystaniem poczty elektronicznej i stron internetowych www.) pod inną osobę, instytucję lub znane marki, w celu wyłudzenia określonych informacji takich jak numery oraz hasła PIN kart płatniczych, hasła logowania do urzędów czy też płatności internetowej banków lub szczegółów karty kredytowej w celu wyłudzenia danych.
Przestępcy tworzą fałszywe strony Internetowe, żeby wyłudzić dane (loginy i hasła). Najczęściej wysyłają maile zawierające odnośniki do tych stron.
Jak się chronić? Dokładnie weryfikuj adres witryny zanim się na niej zalogujesz. Nie należy wpisywać swojego loginu i hasła na podejrzanych stronach internetowych.

Malware- złośliwe oprogramowanie- to określenie opisuje całą gamę szkodliwych programów i aplikacji, które po uzyskaniu dostępu do sieci podmiotu lub instytucji może poczynić wiele szkód. Złośliwe oprogramowanie może przyjąć formę wirusów, robaków, koni trojańskich i innych.
Ransomware to rodzaj złośliwego oprogramowania, które infekując urządzenie lub komputer blokuje jego podstawowe funkcje i wymusza użytkownika do zapłacenia haraczu, w zamian za przywrócenie kontroli nad systemem operacyjnym i umożliwienia dostępu do danych zgromadzonych na komputerze. Zagrożenie może dostać się do komputera za pośrednictwem pobranego pliku, wykorzystując niespójności w strukturze ochrony lub nawet przez wiadomość tekstową. Czym się różni od typowego złośliwego oprogramowania?

- Nie kradnie danych użytkownika, lecz je szyfruje.
- Wymusza płatność okupu, zazwyczaj w dolarach lub Bitcoinach
- Jest relatywnie łatwy do stworzenia – istnieje wiele bardzo dobrze udokumentowanych cryptobibliotek

Często stosowane są ataki z użyciem szkodliwego oprogramowania (malware, ransomware itp.), hakerzy mogą wysyłać złośliwe oprogramowanie za pośrednictwem e-mail, dołączonego do e-mail załącznika itp.
Jak się chronić? *Nie otwieraj podejrzanych wiadomości oraz załączników, ponieważ w przypadku instalacji złośliwego oprogramowania na Twoim urządzeniu, hakerzy mogą przejąć dostęp np. do Twojego konta w banku.*

Atak Key Logger (ang. Key Logger Attack) – cyberprzestępcy używają programów, które mogą zapisywać naciśnięcie każdego klawisza na klawiaturze. Dzięki temu mogą poznać login i hasło użytkownika zainfekowanego komputera. Wystarczy raz zalogować się do danej usługi żeby dostarczyć przestępcom pełne dane.

Vishing przestępcy mogą do Ciebie zadzwonić i podawać się za pracownika instytucji np. SANEPID, Policji, ZUS, Twojego przełożonego i prosić Cię o przekazanie Twojego loginu, hasła, nr PESEL, nr dowodu osobistego. Podanie tych danych może skutkować kradzieżą Twojej tożsamości, umożliwieniem przestępcy zalogowania się do Systemu.
Jak się chronić? Nigdy nie podawaj swoich danych dopóki nie upewnisz się z kim rozmawiasz.

DOBRE PRAKTYKI W ZAKRESIE BEZPIECZEŃSTWA TELEINFORMATYCZNEGO

BEZPIECZNE KORZYSTANIE Z SIECI INTERNET

- Podstawowym elementem bezpieczeństwa w sieci Internet jest **zastosowanie zasady ograniczonego zaufania i podwyższonej ostrożności**
- Pamiętajmy o zainstalowaniu i aktualizowaniu programu ochrony przed złośliwym oprogramowaniem. **Program powinien chronić przed wirusami i phishingiem**
- Na bieżąco aktualizujemy system operacyjny i aplikacje użytkowe Nie odwiedzamy stron powszechnie uznawanych za niebezpieczne Nie klikamy na linki do nieznanych stron internetowych
- **Zwracamy uwagę na komunikaty programu antywirusowego i przeglądarek internetowych**
- **Ograniczamy do minimum podawanie swoich danych osobowych.** Nie podawaj swoich danych osobowych na stronach internetowych, co do których nie masz pewności, że nie są one

widoczne dla osób trzecich. Nie korzystaj ze stron, które nie mają ważnego certyfikatu (np. brak protokołu https)

- Nie zostawiaj swoich danych osobowych w niesprawdzonych serwisach i na stronach zawsze czytaj dokładnie Regulaminy i Polityki, weryfikuj na co wyrażasz zgodę
- Nie wysyłaj e-mailem poufnych danych/ danych osobowych bez ich szyfrowania. Pamiętaj, że inny Urząd, Szkoła czy bank, nie wysyła e-maili do swoich pacjentów/klientów/interesantów z prośbą o podanie hasła lub loginu do jakichkolwiek systemów w celu ich weryfikacji

BEZPIECZNE KORZYSTANIE Z POCZTY ELEKTRONICZNEJ

- Zwracamy szczególna uwagę na nadawcę wiadomości
- Zwracamy szczególną uwagę na poprawność adresata (adresatów) poczty elektronicznej
- Nie klikamy na podejrzane linki umieszczone w załączniku poczty
- Nie wysyłamy danych osobowych, logowania, karty kredytowej w niezabezpieczonej treści wiadomości e-mail; żaden bank czy urząd nie wysyła do swoich klientów e-maili z prośbą o podanie hasła czy loginu w celu ich weryfikacji
- W przypadku przesyłania ważnych (wrażliwych) wiadomości stosujemy mechanizmy szyfrowania

BEZPIECZNE KORZYSTANIE Z URZĄDZEŃ MOBILNYCH

- Zabezpieczamy bezpiecznym hasłem dostęp do urządzenia :
  ▪ Laptop – zakładamy hasło do BIOS/UEFI, oraz hasło do systemu operacyjnego
  ▪ Smartphone – hasło do PIN, drugi poziom zabezpieczeń (hasło obrazkowe, biometryka)
- Na bieżąco aktualizujemy system operacyjny urządzenia oraz aplikacje użytkowe
- Uruchamiany firewalla jeżeli jest wyłączony
- Instalujemy oprogramowanie antywirusowe, używamy i na bieżąco aktualizujemy
- Korzystamy z możliwości szyfrowania plików, katalogów lub całego dysku, dysków usb pendrive
- Skanujemy oprogramowaniem antywirusowym wszystkie urządzenia podłączane do komputera – pendrive, płyty, karty pamięci
- Wszystkie pobrane pliki należy skanować programem antywirusowym
- Nie otwieraj plików nieznanego pochodzenia
- Nie korzystaj ze stron banków, poczty elektronicznej, które nie mają ważnego certyfikatu bezpieczeństwa
- W przypadku aplikacji na smartphone sprawdzamy do jakich usług aplikacja będzie miała dostęp oraz jaka jest wiarygodność producenta aplikacji
- Regularnie tworzymy kopie zapasowe ważnych danych
- Zachowujemy szczególną ostrożność przy korzystaniu z otwartych, publicznych sieci WiFi
- Szczególna uwagę zwracamy na podejrzane SMS lub MMS
- Zwracaj uwagę na komunikaty wyświetlane na ekranie komputera
- Nie otwieraj plików nieznanego pochodzenia

Cyberbezpieczeństwo – jak chronić nasze informacje przed atakami w cyberprzestrzeni ?

W ramach realizacji Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, Ministerstwo Cyfryzacji opracowało poradnik pn:

„Cyberbezpieczeństwo – jak chronić nasze informacje przed atakami w cyberprzestrzeni ?”

Z Poradnika dowiecie się Państwo jakie są najpopularniejsze ataki w cyberprzestrzeni i jak skutecznie się przed nimi bronić m.in.:

Cyberbezpieczeństwo - czy mnie to dotyczy ?

Cyberbezpieczeństwo jest ważne, ponieważ smartfony, komputery i Internet są obecnie tak fundamentalną częścią współczesnego życia, że trudno sobie wyobrazić, jak moglibyśmy bez nich funkcjonować, w szczególności w stanie epidemii, gdy musimy ograniczyć swoje fizyczne kontakty. Dlatego też szczególnie dziś ważne jest, aby w ramach kilku kroków ograniczyć cyberprzestępcom zdobycie dostępu do zawartości naszych urządzeń – smartfonów i komputerów – za ich pośrednictwem do naszych kont bankowych, kont w portalach społecznościowych, skrzynek poczty elektronicznej – zarówno prywatnych jak i służbowych.

Niezależnie od wielkości i rodzaju organizacji, w której pracujesz, ważne jest, aby zrozumieć, dlaczego możesz być podatny na cyberataki i sposoby obrony przed nimi. Te podstawowe porady dotyczą zarówno Twojego życia zawodowego, jak i prywatnego.

Zabezpiecz swoje urządzenia

- Smartfony, tablety, laptopy lub komputery stacjonarne, których używasz, mogą być celem ataków w cyberprzestrzeni, a także ataków fizycznych – np. kradzieży. Jak się chronić przed takimi atakami na urządzenia:
- Nie ignoruj aktualizacji oprogramowania - zawierają poprawki i nowe funkcje, które chronią przed najnowszymi zagrożeniami. Jeśli pojawi się monit o zainstalowanie aktualizacji, upewnij się, czy faktycznie zostały one zaktualizowane.
- Zawsze blokuj urządzenie, gdy go nie używasz. Użyj kodu PIN, hasła lub odcisku palca. Utrudni to atakującemu wykorzystanie urządzenia, jeśli zostanie ono zgubione lub skradzione.
- Unikaj pobierania aplikacji, których reputacji nie jesteś pewien. Używaj tylko oficjalnych sklepów z aplikacjami (takich jak Google Play lub Apple App Store), które zapewniają większą ochronę przed złośliwym oprogramowaniem. Nie pobieraj aplikacji od przypadkowych źródeł, tylko dlatego, że ktoś do tego zachęca na mediach społecznościowych.

Używaj silnych haseł i używaj różnych haseł do różnych kont

- Atakujący wypróbują najpopularniejsze hasła (np. 12334, abcd. itp.) lub wykorzystają publicznie dostępne informacje, aby uzyskać dostęp do Twoich kont. Jeśli się im powiedzie, mogą użyć tego samego hasła, aby uzyskać dostęp do innych Twoich kont.
- Utwórz silne i łatwe do zapamiętania hasło do ważnych kont, na przykład używając trzech losowych słów. Unikaj używania przewidywalnych haseł, takich jak daty, nazwisko i imię czy imię Twojego zwierzaka.
- Używaj osobnego hasła do konta służbowego. Jeśli prywatne konto internetowe zostanie przejęte, nie chcesz, aby osoba atakująca znała również twoje hasło służbowe.
- Jeśli zapisujesz swoje hasła, przechowuj je bezpiecznie z dala od urządzenia. Nigdy nie ujawniaj nikomu swojego hasła.
- Użyj wieloskładnikowego uwierzytelniania (MFA – Multi-Factor Authentication) w ważnych usługach online, takich jak bankowość i poczta e-mail, jeśli masz taką opcję. MFA zapewnia sposób co najmniej „podwójnego sprawdzenia”, że naprawdę jesteś osobą, za którą się podajesz, gdy korzystasz z usług online.

W razie wątpliwości, zgłoś podejrzane działania do zespołu reagowania na incydenty bezpieczeństwa CSIRT NASK

Zgłaszanie informacji o podejrzanych działaniach w cyberprzestrzeni może znacznie zmniejszyć potencjalne szkody powodowane przez cyberataki.

Cyberataki mogą być trudne do wykrycia, więc nie wahaj się prosić o dalsze wskazówki lub wsparcie, gdy coś wydaje się podejrzane lub niezwykłe.

Zgłoś ataki jak najszybciej - nie zakładaj, że zrobi to ktoś inny – zgłoszenia możesz dokonać pod adresem (adres podmiotu zewnętrznego):

https://incydent.cert.pl/

Więcej informacji na temat cyberbezpieczeństwa Państwo uzyskają w Poradniku:

https://www.gov.pl/web/baza-wiedzy/poradnik--prcyber-01 Poradnik (Wydanie 1 - maj 2020 r.)

Państwowy Instytut Badawczy NASK opracował poradnik „ABC Cyberbezpieczeństwa".

Publikacja opracowana przez ekspertów NASK w ramach Ogólnopolskiej Sieci Edukacyjnej (OSE), to poradnik, który w przystępny dla każdego sposób przybliża szeroko pojęty świat internetu. Jest podzielony na cztery obszary kluczowe dla użytkownika sieci. Są to: cyberbezpieczeństwo, higiena cyfrowa, profilaktyka i wsparcie.

„ABC cyberbezpieczeństwa" został przygotowany w taki sposób by każdy, bez względu na wiek, zawód czy też stopień korzystania z internetowego świata, mógł zrozumieć i bronić się przed cyberzagrożeniem, a także zadbać o dobrostan cyfrowy swój oraz najbliższych. Zawarto w nim nie tylko techniczne definicje, ale przede wszystkim pigułkę wiedzy, dobrych praktyk i cyfrowych nawyków.

Zachęcamy Państwa do lektury (adres/link podmiotu zewnętrznego):

Poradnik ABC cyberbezpieczeństwa

Zachęcamy Państwa do śledzenia cyklicznego, bezpłatnego biuletynu zawierającego porady bezpieczeństwa dla użytkowników komputerów - OUCH!: https://www.cert.pl/ouch/

Poradniki informacyjne z zakresu cyberbezpieczeństwa:

https://www.gov.pl/web/baza-wiedzy/poradnik--prcyber-01 Poradnik (Wydanie 1 - maj 2020 r.)

Poradnik ABC cyberbezpieczeństwa

Cyberhigiena dla każdego - serwis RP

Ważne informacje z zakresu cyberbezpieczeństwa dostępne są m.in. na stronach:

https://www.cert.pl/ – strona internetowa zespołu reagowania na incydenty informatyczne CERT Polska

https://www.cert.pl/publikacje/ – publikacje CERT Polska

https://www.cert.pl/ouch/ – Biuletyn OUCH! Cykliczny, darmowy zestaw porad bezpieczeństwa dla użytkowników komputerów

https://dyzurnet.pl/ – strona internetowa zespołu ekspertów Naukowej i Akademickiej Sieci Komputerowej

https://www.saferinternet.pl/ – Polskie Centrum Programu Safer Internet (PCPSI) działające na rzecz bezpieczeństwa dzieci i młodzieży korzystających z internetu i nowych technologii.

Uwaga!: wskazane w Poradniku Cyberbezpieczeństwa adresy/linki https:// (...) dotyczą podmiotów zewnętrznych