Cyberbezpieczeństwo

CYBERBEZPIECZEŃSTWO

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 definiuje się jako ogół procesów, mających na celu chronienie danych osobowych, a także systemów przedsiębiorstwa przed zagrożeniami związanymi z cyberatakami w sieci. Ofiarą takich ataków mogą być bowiem nie tylko silne korporacje o ugruntowanej pozycji, ale też nieco mniejsze firmy, w przypadku których luki systemowe są niestety częstsze.
Poruszając to pojęcie koniecznie trzeba wspomnieć również o rodzajach cyberbezpieczeństwa. Tutaj wyróżnia się wiele różnych obszarów, które mogą mu podlegać, wśród których wskazuje się m.in. na:

- sieć oraz aplikacje,
- dane przechowywane w chmurze,
- ochronę baz danych,
- ochronę dostępu do firmowej sieci,
- odzyskiwanie danych po awarii,
- ochronę danych osobowych.

Cyberbezpieczeństwo (ang. cybersecurity) stanowi zespół zagadnień związanych z zapewnianiem ochrony w obszarze cyberprzestrzeni. 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.

Rodzaje zagrożeń:

Malware, czyli złośliwe oprogramowanie, to ogólny termin opisujący każdy złośliwy program lub kod, który jest szkodliwy dla systemów.
Ransomware to forma złośliwego oprogramowania, które blokuje użytkownikowi dostęp do

plików lub urządzenia, a następnie żąda zapłaty za przywrócenie dostępu.
Keylogger to szkodliwe oprogramowanie, które odczytuje i zapisuje wszystkie naciśnięcia klawiszy bez wiedzy użytkownika danego sprzętu.
Vishing to przestępstwo oparte na inżynierii społecznej. Sprytni rozmówcy podający się za pracowników banków, doradców inwestycyjnych czy instytucje zaufania publicznego, są w stanie tak zmanipulować rozmówcę, że ten jest skłonny przelać środki finansowe na wskazane konto, czy też ujawni swoje szczegółowe dane poufnych.

Phishing - to jeden z najpopularniejszych typów ataków opartych o wiadomości e-mail lub SMS. Wykorzystuje inżynierię społeczną, czyli technikę polegającą na tym, że przestępcy internetowi próbują Cię oszukać i spowodować, abyś podjął działanie zgodnie z ich zamierzeniami

BEZPIECZNE KORZYSTANIE Z POCZTY ELEKTRONICZNEJ

- zwróć uwagę na nadawcę wiadomości,
- zwróć uwagę na poprawność adresata (adresatów) poczty elektronicznej
- nie klikaj na podejrzane linki umieszczone w załączniku poczty
- nie wysyłaj danych osobowych, logowani,
- nie podawaj danych z karty kredytowej
- jeżeli przysyłasz ważne (wrażliwe) wiadomości stosuj mechanizmy szyfrowania
- zabezpiecz sowje konto pocztowe złożonym hasłem i zmieniaj je systematycznie - https://www.gov.pl/web/baza-wiedzy/jak-tworzyc-bezpieczne-hasla

BEZPIECZNE KORZYSTANIE Z SIECI INTERNET

- miej zawsze zainstalowany i aktualizowany programu ochrony przed złośliwym oprogramowaniem
- na bieżąco aktualizuj system operacyjny i aplikacje użytkowe
- zwróć uwagę na komunikaty programu antywirusowego i przeglądarek internetowych
- nie podawaj swoich danych osobowych na stronach internetowych,
- niie zostawiaj swoich danych osobowych w niesprawdzonych serwisach
- zawsze czytaj dokładnie Regulaminy i Polityki, weryfikuj na co wyrażasz zgod
- nie wysyłaj e-mailem poufnych danych/danych osobowych bez ich szyfrowania.

BEZPIECZNY SPRZĘT

- nie pobierania aplikacji, których nie jesteś pewien
- używaj tylko oficjalnych sklepów z aplikacjami (takich jak Google Play lub Apple App Store)
- laptopy, komputery, smartfony: aktualizuj oprogramowania, blokuj urządzenie, gdy go nie używasz, użyj hasła, PIN-u, odcisku palca do odblokowania
- używywaj oprogramowania zabezpieczającego
- używaj silnych haseł i używaj różnych haseł do różnych kont

BEZPIECZNA SZKOŁA

Ministerstwo Edukacji Narodowej, we współpracy z organizacjami pozarządowymi, innymi

resortami i instytucjami odpowiedzialnymi za bezpieczeństwo, przygotowało poradnik „Bezpieczna szkoła. Zagrożenia i zalecane działania profilaktyczne w zakresie bezpieczeństwa fizycznego i cyfrowego uczniów”. Materiał to kompendium wiedzy na temat rozpoznawania sytuacji zagrożeń i reagowania na nie. Poradnik jest przeznaczony dla dyrektorów szkół, nauczycieli, rodziców i uczniów. Zachęcamy do zapoznania się z materiałem.

Bezpieczna szkoła. Zagrożenia i zalecane działania profilaktyczne w zakresie bezpieczeństwa fizycznego i cyfrowego uczniów – poradnik MEN - Ministerstwo Edukacji Narodowej - Portal Gov.pl (www.gov.pl)

https://www.gov.pl/web/baza-wiedzy/poradnik–prcyber-01

ABC CYBERBEZPIECZEŃSTWO

Publikacja opracowana przez ekspertów Naukowej i Akademickiej Sieci Komputerowej Państwowego Instytutu Badawczego (NASK-PIB) w ramach Ogólnopolskiej Sieci Edukacyjnej (OSE) to poradnik, który w przystępny dla każdego sposób przybliża terminologię szeroko pojętego świata internetu. Jest podzielony na cztery kluczowe dla użytkownika sieci obszary: cyberbezpieczeństwo; higiena cyfrowa; profilaktyka; wsparcie.

https://www.gov.pl/web/baza-wiedzy/abc-cyberbezpieczenstwa---nowy-poradnik-przygotowany-przez-nask-pib

KURSY E-LEARNINGOWE DLA UCZNIÓW I NAUCZYCIELI - CYBERBEZPIECZEŃSTWO

Kursy składają się z różnorodnych treści – mogą to być nagrane wykłady, filmy instruktażowe, pigułki wiedzy, a także zeszyty dydaktyczne i prezentacje w formacie PDF oraz inne materiały dodatkowe. Zestaw materiałów zależy od tematyki oraz zaawansowania kursu. Czas na pracę własną z materiałami nie jest ograniczony.

https://it-szkola.edu.pl/

ZGŁOSZENIE DO CSIRT NASK - INCYDENTU

Informujemy, że od dnia 28 sierpnia 2018 r. zespołowi CERT Polska zostały powierzone obowiązki CSIRT NASK wynikające z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560).

https://incydent.cert.pl/

Zgłoszenia do CSIRT NASK

Informujemy, że od dnia 28 sierpnia 2018 r. zespołowi CERT Polska zostały powierzone obowiązki **CSIRT NASK** wynikające z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560).

Jeżeli chcą Państwo zgłosić osobę kontaktową do CSIRT NASK proszę użyć poniższego odnośnika:
Zgłaszanie osoby kontaktowej do CSIRT NASK.

Jeżeli chcą Państwo zgłosić złośliwą domenę, proszę użyć poniższego odnośnika:
Zgłaszanie domeny internetowej służącej do wyłudzeń danych i środków finansowych.

Zgłaszanie podejrzanych wiadomości SMS

Wszystkie podejrzane wiadomości SMS z linkami można zgłosić używając funkcji "Przekaż", bezpośrednio na numer:

8080

Zgłoszenie incydentu – Jaki podmiot Państwo reprezentują?

- Osoba fizyczna / inne podmioty
- Operator usług kluczowych
- Dostawca usługi cyfrowej
- Podmiot publiczny