Wstęp

Zgodnie z art. 22 ust. 1 pkt 4 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (dalej jako „Ustawa") przekazujemy Państwu niezbędne informacje w przedmiocie zagadnienia jakim jest cyberbezpieczeństwo.

Cyberbezpieczeństwo jest to odporność systemów informacyjnych na wszelkie działania naruszające ich dostępność, integralność, poufność oraz autentyczność. Jest to jeden z kluczowych czynników zapewniających bezpieczeństwo i ciągłość działania zarówno osób prywatnych, jak i przedsiębiorstw.

Podstawowe zasady cyberbezpieczeństwa

Do podstawowych zasad cyberbezpieczeństwa należą:

- Kontrola dostępu - należy ograniczać dostęp do systemów informatycznych do osób uprawnionych.
- Ochrona danych osobowych - należy chronić dane osobowe przed nieuprawnionym dostępem, ujawnieniem, zmianą lub zniszczeniem.
- Ochrona przed złośliwym oprogramowaniem - należy stosować oprogramowanie antywirusowe i antymalware oraz regularnie aktualizować oprogramowanie.
- Ochrona przed phishingiem i innymi technikami socjotechnicznymi - należy uważać na podejrzane wiadomości e-mail i linki.
- Ochrona przed wyciekami danych - należy stosować bezpieczne hasła i szyfrować dane.

Instrukcje dla osób prywatnych

Oto kilka wskazówek dotyczących cyberbezpieczeństwa dla osób prywatnych:

- Stosuj silne hasła - hasła powinny składać się z co najmniej 12 znaków, zawierać duże i małe litery, cyfry oraz znaki specjalne.
- Nie używaj tego samego hasła do wielu serwisów - w przypadku wykradzenia jednego hasła, przestępcy będą mogli uzyskać dostęp do wszystkich serwisów, w których używasz tego samego hasła.

- Aktualizuj oprogramowanie - producenci oprogramowania regularnie publikują aktualizacje, które zawierają poprawki zabezpieczeń. Aktualizowanie oprogramowania jest ważne, aby chronić się przed najnowszymi zagrożeniami.
- Bądź ostrożny przy klikaniu w linki w wiadomościach e-mail - jeśli nie jesteś pewien, czy wiadomość e-mail jest prawdziwa, nie klikaj w żadne linki w niej zawarte.
- Nie otwieraj załączników w wiadomościach e-mail - załączniki w wiadomościach e-mail mogą zawierać złośliwe oprogramowanie. Jeśli nie jesteś pewien, czy załącznik jest bezpieczny, nie otwieraj go.
- Używaj bezpiecznego połączenia internetowego - podczas łączenia się z siecią publiczną, np. w kawiarni lub hotelu, korzystaj z bezpiecznego połączenia internetowego (HTTPS).
- Zabezpiecz swoje urządzenia mobilne - na urządzeniach mobilnych zainstaluj oprogramowanie antywirusowe i antymalware.

Instrukcje dla firm i instytucji

Oto kilka wskazówek dotyczących cyberbezpieczeństwa dla firm i instytucji:

- Zastosuj politykę bezpieczeństwa - polityka bezpieczeństwa powinna określać zasady i procedury dotyczące cyberbezpieczeństwa w przedsiębiorstwie.
- Stwórz zespół ds. cyberbezpieczeństwa - zespół ds. cyberbezpieczeństwa powinien być odpowiedzialny za monitorowanie bezpieczeństwa systemów informatycznych w przedsiębiorstwie.
- Wykonaj audyt bezpieczeństwa - audyt bezpieczeństwa pozwoli zidentyfikować i usunąć luki w zabezpieczeniach systemów informatycznych.
- Dowiedz się, jak reagować na incydenty bezpieczeństwa - przed wystąpieniem incydentu bezpieczeństwa należy opracować plan działania, który określi, jak przedsiębiorstwo będzie reagować na takie sytuacje.
- Informuj pracowników o cyberbezpieczeństwie - pracownicy powinni być świadomi zagrożeń związanych z cyberbezpieczeństwem i wiedzieć, jak się przed nimi chronić.

Podsumowanie

Cyberbezpieczeństwo jest ważną kwestią dla każdego. Stosując się do podstawowych zasad cyberbezpieczeństwa, można znacząco zmniejszyć ryzyko ataku.

Zalecamy również śledzenie na bieżąco stron internetowych organizacji wyspecjalizowanych w zakresie cyberbezpieczeństwa, takich jak:
https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo
https://www.cert.pl/publikacje/