Krajowy System Cyberbezpieczeństwa

Realizując zadania wynikające z Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1560 ze zm.) przekazujemy Państwu informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady jak przeciwdziałać tymi zagrożeniom.

Cyberbezpieczeństwo - zgodnie z obowiązującymi przepisami (art. 2 pkt. 4 ww. ustawy) to „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy"

I. Najpopularniejsze zagrożenia w cyberprzestrzeni:

1. Ataki z użyciem szkodliwego oprogramowania (tzw. malware, wirusy, robaki, itp.),
2. Kradzieże tożsamości, kradzieże (wyłudzenia), modyfikacje bądź niszczenie danych, blokowanie dostępu do usług, spam (niechciane lub niepotrzebne wiadomości elektroniczne), ataki socjotechniczne (np. phishing czyli wyłudzanie poufnych informacji przez podszywanie się pod godną zaufania osobę lub instytucję.

II. Sposoby zabezpieczenia się przed zagrożeniami:

1. Stosuj zasadę ograniczonego zaufania do odbieranych wiadomości email, sms, stron internetowych nakłaniających do podania danych osobowych, osób podających się za przedstawicieli firm, instytucji, którzy żądają podania danych autoryzacyjnych lub nakłaniających do instalowania aplikacji zdalnego dostępu.
2. Nie ujawniaj danych osobowych w tym danych autoryzacyjnych dopóki nie ustalisz czy rozmawiasz z osobą uprawnioną do przetwarzania Twoich danych.
3. Instaluj aplikacje tylko ze znanych i zaufanych źródeł.
4. Nie otwieraj wiadomości e-mail i nie korzystaj z przesłanych linków od nadawców, których nie znasz.
5. Każdy email można sfałszować, sprawdź w nagłówku wiadomości pole Received: from (ang. otrzymane od) w tym polu znajdziesz rzeczywisty adres serwera nadawcy.
6. Porównaj adres konta email nadawcy adresem w polu *„From" oraz „Reply to"* – różne adresy w tych polach mogą wskazywać na próbę oszustwa.
7. Szyfruj dane poufne wysyłane pocztą elektroniczną.
8. Bezpieczeństwo wiadomości tekstowych (SMS).
   - sprawdź adres url z którego domyślnie dany podmiot/instytucja wysyła do Ciebie smsy, cyberprzestępca może podszyć się pod dowolną tożsamość (odpowiednio definiując numer lub nazwę), otrzymując smsa, w którym cyberprzestępca podszywa się pod numer zapisany w książce adresowej, telefon zidentyfikuje go jako nadawcę wiadomości sms.
9. Jeśli na podejrzanej stronie podałeś swoje dane do logowania lub jeżeli włamano się na Twoje konto email – jak najszybciej zmień hasło.
10. Chroń swój komputer, urządzenie mobilne programem antywirusowym zabezpieczającym przez zagrożeniami typu; wirusy, robaki, trojany, robakami,

niebezpiecznymi aplikacjami typu ransomware, adware, keylogger, spyware, dialer, phishing, narzędziami hakerskimi, backdoorami. rootkitami, bootkitami i exploitami.

11. Aktualizuj system operacyjny, aplikacje użytkowe, programy antywirusowe, brak aktualizacji zwiększa podatność na cyberzagrożenia hakerzy, którzy znają słabości systemu/aplikacji , mają otwartą furtkę do korzystania z luk w oprogramowaniu.
12. Logowanie do e-usług publicznych, bankowości elektronicznej bez aktualnego (wspieranego przez producenta) systemu operacyjnego to duże ryzyko.
13. Korzystaj z różnych haseł do różnych usług elektronicznych.
14. Tam gdzie to możliwe (konta społecznościowe, konto email, usługi e-administracji, usługi finansowe) stosuj dwuetapowe uwierzytelnienie za pomocą np. sms, pin, aplikacji generującej jednorazowe kody autoryzujące, tokenów, klucza fizycznego.
15. Regularnie zmieniaj hasła.
16. Nie udostępniaj nikomu swoich haseł.
17. Pracuj na najniższych możliwych uprawnieniach użytkownika.
18. Wykonuj kopie bezpieczeństwa.
19. Skanuj podłączane urządzenia zewnętrzne.
20. Skanuj regularnie wszystkie dyski twarde zainstalowane na Twoim komputerze.
21. Kontroluj uprawnienia instalowanych aplikacji.
22. Unikaj z korzystania otwartych sieci Wi-Fi.
23. Podając poufne dane sprawdź czy strona internetowa posiada certyfikat SSL. Protokół SSL to standard kodowania (zabezpieczania) przesyłanych danych pomiędzy przeglądarka a serwerem.
24. Zadbaj o bezpieczeństwo routera (ustal silne hasło do sieci WI-FI, zmień nazwę sieci WI-Fi zmień hasło do panelu administratora, ustaw poziom zabezpieczeń połączenia z siecią Wi-FI np. WPA2 i wyższe, aktualizuj oprogramowanie routera, wyłącz funkcję WPS, aktywuj funkcję Gościnna Sieć Wi-Fi „Guest Network”.
25. Szyfruj dyski twarde komputera, przenośne.
26. Zapoznaj się z poradnikiem dotyczącym bezpieczeństwa skrzynek pocztowych i kont w mediach społecznościowych oraz zastosuj się do jego rekomendacji.
27. Bądź wyczulony na sensacyjne informacje, w szczególności zachęcające do natychmiastowego podjęcia jakiegoś działania. Weryfikuj informacje w kilku źródłach. **Upewnij się, że informacja jest prawdziwa przed podaniem jej dalej w mediach społecznościowych. Jeśli masz jakieś wątpliwości, wstrzymaj się.**
28. Uważaj na wszelkie linki w wiadomościach mailowych i SMS-ach, zwłaszcza te sugerujące podjęcie jakiegoś działania, np. konieczność zmiany hasła, albo podejrzaną aktywność na koncie. Obserwowaliśmy w przeszłości tego typu celowane ataki na prywatne konta, gdzie celem było zdobycie informacji zawodowych.
29. Upewnij się, że posiadasz kopię zapasową wszystkich ważnych dla siebie plików i potrafisz je przywrócić w przypadku takiej potrzeby.
30. Śledź ostrzeżenia o nowych scenariuszach ataków na naszych mediach społecznościowych: Twitter, Facebook.
31. Zgłaszaj każdą podejrzaną aktywność przez formularz na stronie incydent.cert.pl lub mailem na cert@cert.pl. Podejrzane SMS-y prześlij bezpośrednio na numer 799 448 084. Rekomendujemy zapisanie go w kontaktach.

Krajowy System Cyberbezpieczeństwa

III. Rekomendacje dla firm:

1. Przetestować przywracanie infrastruktury z kopii zapasowych. **Kluczowe jest, żeby zostało to wykonane w praktyce na wybranych systemach, nie tylko proceduralnie.**
2. Upewnić się, że posiadane **kopie zapasowe są odizolowane i nie ucierpią w przypadku ataku na resztę infrastruktury**.
3. Upewnić się, że dokonywane są aktualizacje oprogramowania, **w szczególności dla systemów dostępnych z internetu**. Należy zacząć od podatności, które są na liście obecnie aktywnie wykorzystywanych w atakach.
4. Upewnić się, że wszelki dostęp zdalny do zasobów firmowych wymaga uwierzytelniania dwuskładnikowego.
5. Przejrzeć usługi w adresacji firmowej dostępne z internetu i ograniczyć je do niezbędnego minimum. Można w tym celu wykorzystać np. portal Shodan. W szczególności nie powinny być bezpośrednio dostępne usługi pozwalające na zdalny dostęp jak RDP czy VNC.
6. Aktualizować w sposób automatyczny sygnatury posiadanych systemów bezpieczeństwa typu AV, EDR, IDS, IPS, itd.
7. Wdrożyć filtrowanie domen w sieci firmowej na bazie publikowanej przez nas listy ostrzeżeń. Dzięki temu w szybki sposób zablokowane zostaną zaobserwowane przez nas złośliwe domeny.
8. Zapoznać się z przygotowanym przez CSIRT KNF poradnikiem dotyczącym obrony przed atakami DDoS i wdrożyć jego rekomendacje.
9. Zapoznać się z naszym poradnikiem omawiającym sposoby wzmocnienia ochrony przed ransomware i wdrożyć jego rekomendacje.
10. Zapoznać się z naszymi materiałami dotyczącymi bezpieczeństwa haseł.
11. Zapoznać się z naszym artykułem dotyczącym mechanizmów weryfikacji nadawcy wiadomości i wdrożyć je dla domen wykorzystywanych do wysyłki poczty.
12. W przypadku posiadania własnego zakresu adresów IP zalecamy dołączenie do platformy N6. Za jej pośrednictwem udostępniamy na bieżąco informacje o podatnościach i podejrzanej aktywności obserwowanej przez nas w podanym zakresie adresowym.
13. Wyznaczyć osobę odpowiedzialną za koordynację działań w przypadku wystąpienia incydentu i przećwiczyć procedury reagowania.
14. Uczulić pracowników na obserwację podejrzanej aktywności oraz poinformowanie o sposobie jej zgłaszania do wyznaczonej w firmie osoby.
15. Zgłosić do nas osobę kontaktową, nawet jeśli nie zobowiązuje do tego ustawa. Dzięki temu będziemy w stanie szybko skontaktować się z właściwą osobą w celu przesłania ostrzeżenia.
16. Zgłaszać każdą podejrzaną aktywność do właściwego CSIRT-u, tj.:
    - CSIRT GOV — administracja rządowa i infrastruktura krytyczna,
    - CSIRT MON — instytucje wojskowe,
    - CSIRT NASK — wszystkie pozostałe.

Uwaga! Jeśli Twoja firma współpracuje z podmiotami na Ukrainie lub ma tam oddziały, dodatkowo:

Krajowy System Cyberbezpieczeństwa

- Sprawdź reguły dla dostępu sieciowego, ogranicz dozwolony ruch do minimum.
- Monitoruj ruch sieciowy, w szczególności na styku sieci z tymi firmami/oddziałami.
- Obejmij szczególnym monitoringiem hosty, na których jest zainstalowane oprogramowanie, które otrzymuje automatyczne aktualizacje od podmiotów na Ukrainie.
- Ostrzeż pracowników, aby byli szczególnie wyczuleni na informacje nakłaniające ich do podjęcia jakiegoś działania.

IV. Zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie sposobów zabezpieczania się przed zagrożeniami to wiedza niezbędna każdemu użytkownikowi komputera, smartphona czy też usług internetowych. Wszelkie porady bezpieczeństwa dla użytkowników tych urządzeń dostępne są na:

1. Witrynie internetowej CSIRT NASK – Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym pod adresem: https://www.cert.pl
2. Witrynie internetowej Ministerstwa Cyfryzacji pod adresem: https://www.gov.pl/web/cyfryzacja/cyberbezpieczenstwo
3. Stronie internetowej kampanii STÓJ-POMYŚL-POŁĄCZ po adresem: https://stojpomyslpolacz.pl
4. Kampania ma na celu zwiększanie poziomu świadomości społecznej i promowanie bezpieczeństwa w cyberprzestrzeni https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo https://akademia.nask.pl/publikacje/ https://dyzurnet.pl/

V. Zgłaszanie incydentów bezpieczeństwa: https://incydent.cert.pl/

Na osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami Krajowego Systemu Cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, wyznaczony został Pan Tomasz Więckowski, który pełni również funkcję Inspektora Ochrony Danych Osobowych, dane kontaktowe poczta e-mail: iod2@synergiaconsuting.pl

Podstawa prawna:

Ustawa z dnia 5 lipca 2018 r. o krajowym cyberbezpieczeństwa (Dz.U. z 2018r. poz.1560 ze zm.).