OGÓLNE **ZASADY CYBERBEZPIECZEŃSTWA** DLA INSTYTUCJI RZĄDOWYCH

2024

Zalecenia i praktyki

FEDERACJA PRZEDSIĘBIORCÓW POLSKICH

I. Ogólne zasady cyberbezpieczeństwa dla instytucji rządowych

Zadbaj o kulturę cyberbezpieczeństwa

Świadomość pracowników, przykłady poprawnych zachowań, dbanie o szkolenia czy przejrzysta struktura organizacji cyberbezpieczeństwa są niezwykle istotne i stanowią podstawę dla zapewnienia skutecznego poziomu cyberbezpieczeństwa w organizacji.

Zdefiniuj osoby odpowiedzialne za zarządzanie – przypisz kluczową osobę odpowiedzialną za sprawy związane z cyberbezpieczeństwem na szczeblu rządowym, a także w kluczowych ministerstwach i agencjach.

Zdobądź zrozumienie, akceptację i uznanie pracowników urzędów wchodzących w skład administracji rządowej – prowadź skuteczną komunikację na tematy cyberbezpieczeństwa ze strony kompetentnych osób odpowiedzialnych za cyberbezpieczeństwo, organizuj specjalne szkolenia dla pracowników opisujące jasno i szczegółowo zasady określone w politykach cyberbezpieczeństwa.

Opracuj i opublikuj polityki cyberbezpieczeństwa – opracuj jasne i szczegółowe zasady dla wszystkich pracowników administracji państwowej dotyczące tego, jak mają się zachowywać podczas korzystania z rządowego środowiska teleinformatycznego, sprzętu i usług komunikacji elektronicznej.

Przeprowadzaj audyty cyberbezpieczeństwa – regularne audyty powinny być przeprowadzane przez osoby kompetentne posiadające odpowiednią wiedzę, umiejętności i doświadczenie.

Pamiętaj o ochronie danych – zgodnie z ogólnym rozporządzeniem Unii Europejskiej o ochronie danych osobowych każda organizacja musi zapewnić odpowiednie środki kontroli bezpieczeństwa w celu ochrony danych należących do mieszkańców UE / EOG.

Zapewnij odpowiednie szkolenia

W celu podwyższenia świadomości, zapewnij wszystkim pracownikom regularne szkolenia z zakresu cyberbezpieczeństwa, koncentrując się na sytuacjach z życia codziennego. Zapewnij również specjalistyczne szkolenia z zakresu cyberbezpieczeństwa dla personelu odpowiedzialnego za cyberbezpieczeństwo.

Współpracuj ze sprawdzonymi dostawcami

Upewnij się, że wszyscy dostawcy spełniają wymagane standardy cyberbezpieczeństwa i mają dobre i spełniają wymagany uzgodniony poziom bezpieczeństwa.

Opracuj skuteczny plan reagowania na incydenty

Plan reagowania na incydenty powinien zawierać udokumentowane przejrzyste instrukcje postępowania, wytyczne, podział ról oraz opis ich odpowiedzialności, by zapewnić odpowiednią i terminową reakcję na wszystkie zaistniałe incydenty związane z bezpieczeństwem oraz ich późniejszą profesjonalną obsługę.

Zapewnij bezpieczny dostęp do systemów i zasobów elektronicznych

Używaj haseł złożonych ze zbioru co najmniej trzech różnych słów połączonych we frazę łatwą do zapamiętania, a jednocześnie zapewniającą wysoki poziom bezpieczeństwa. Przy typowych hasłach stosuj poniższe zasady:

- Hasło powinno być długie (zalecane co najmniej 12 znaków), z małymi i dużymi literami, ewentualnie również z cyframi i znakami specjalnymi.
- Unikaj haseł oczywistych lub powszechnie znanych, których łatwo można się domyśleć, takich jak nazwa aktualnego miesiąca, aktualny rok, itp. lub sekwencji liter czy cyfr, takich jak „abc", czy „123".
- Przy tworzeniu haseł, unikaj używania swoich danych osobowych, które można wyszukać w Internecie.

Ponadto, niezależnie od tego, czy używasz fraz czy typowych haseł, stosuj poniższe zasady:

- Nie używaj tych samych haseł przy dostępach do różnych systemów lub kont.
- Nie udostępniaj haseł współpracownikom lub innym osobom.
- Włącz uwierzytelnianie wieloskładnikowe.
- Używaj specjalistycznego menedżera haseł.

Zabezpiecz urządzenia

1. **Aktualizuj oprogramowanie i regularnie wgrywaj poprawki** – dla wszystkich podmiotów publicznych wysoce zaleca się stosowanie następujących zasad:
   - Regularnie aktualizuj całe oprogramowanie.
   - Włącz funkcję automatycznej aktualizacji, gdzie tylko jest to możliwe.
   - Zidentyfikuj oprogramowanie i sprzęt, który wymaga ręcznych aktualizacji.
   - Pamiętaj o urządzeniach mobilnych i IoT oraz stosuj dla tych urządzeń te same zasady.

2. **Włącz oprogramowanie antywirusowe** – rozwiązania antywirusowe powinny być wdrożone na wszystkich typach urządzeń i regularnie aktualizowane w celu zapewnienia ich ciągłej skuteczności. Nigdy nie instaluj pirackiego oprogramowania, ponieważ może ono zawierać złośliwe oprogramowanie.

3. **Stosuj rozwiązania ochrony poczty elektronicznej i serwisów WWW** – pamiętaj o stosowaniu rozwiązań blokujących wiadomości e-mail typu spam, wiadomości e-mail zawierających linki do złośliwych stron internetowych lub/i zawierających złośliwe załączniki, takie jak wirusy, oraz wiadomości e-mail typu phishing.

4. **Stosuj szyfrowanie**
   - Chroń dane szyfrując je na urządzeniach mobilnych, takich jak laptopy, smartfony i tablety.
   - W przypadku przesyłania danych za pośrednictwem sieci publicznych, takich jak sieci hotelowe lub na lotniskach, upewnij się, że stosujesz szyfrowanie danych.
   - Upewnij się, że strona internetowa, z której korzystasz, wykorzystuje odpowiednią technologię szyfrowania.

5. **Wdróż zarządzanie urządzeniami mobilnymi** – zapewnij bezpieczeństwo biznesowych danych wrażliwych przechowywanych na urządzeniach mobilnych pracowników poprzez zastosowanie rozwiązania Mobile Device Management (MDM), które umożliwia:
   - kontrolowanie dostępu i definiuje, które urządzenia mogą uzyskać dostęp do danych, systemów i usług w organizacji.
   - zapewnienie, by urządzenia mobilne miały zainstalowane aktualne oprogramowanie antywirusowe z aktualną bazą wirusów.
   - weryfikację, czy urządzenie jest szyfrowane.
   - zarządzanie aktualizacjami i sprawdza, czy urządzenie ma zainstalowane aktualne poprawki oprogramowania.
   - wymuszanie ochrony urządzenia za pomocą kodu PIN i/lub hasła.
   - zdalne wyczyszczenie wszelkich danych z urządzenia, w przypadku jego zgubienia lub kradzieży, lub jeśli pracownik zakończył pracę w organizacji.

Zabezpiecz sieć teleinformatyczną

1. **Zapora ogniowa** jest kluczowym narzędziem w ochronie sieci i systemów organizacji. Filtruj ruch, który wchodzi i wychodzi z sieci. Zapory sieciowe powinny być stosowane w celu ochrony wszystkich krytycznych systemów, zwłaszcza połączonych z siecią Internet.
2. **Zabezpiecz rozwiązania zdalnego dostępu do sieci** – zapewnij bezpieczeństwo zdalnego dostępu do sieci z zewnątrz, w szczególności:
   - Upewnij się, że stosowane oprogramowanie do zdalnego dostępu jest aktualne, a najnowsze poprawki oprogramowania są zainstalowane.
   - Blokuj próby nawiązywania połączenia zdalnego dostępu z podejrzanych lokalizacji geograficznych lub podejrzanych adresów IP.
   - Pracownikom logującym się za pośrednictwem zdalnego dostępu ogranicz dostęp tylko do zasobów, systemów i komputerów, których potrzebują do pracy.
   - Wymuś używanie silnych haseł do zdalnego dostępu i w miarę możliwości włącz uwierzytelnianie wieloskładnikowe.
   - Upewnij się, że używanie zdalnego dostępu jest monitorowane, rejestrowane oraz włączone jest ostrzeganie o podejrzanych atakach lub nietypowej podejrzanej aktywności.

Zadbaj o bezpieczeństwo fizyczne

Zadbaj o zabezpieczanie fizyczne urządzeń i dokumentów oraz zastosuj odpowiednie kontrole dostępu fizycznego wszędzie tam, gdzie znajdują się istotne informacje.

- Laptop lub smartfon jednostki rządowej nie powinny być pozostawiane bez opieki, na przykład na tylnym siedzeniu samochodu lub w jego bagażniku.

- Za każdym razem, gdy pracownik odchodzi od komputera czy odkłada telefon, powinien go zablokować.
- Włącz funkcję automatycznej blokady na wszystkich urządzeniach używanych do celów biznesowych.
- Nie pozostawiaj bez opieki wszelkich drukowanych dokumentów zawierających istotne, wrażliwe czy poufne dane.
- Zapewnij bezpieczne przechowywanie papierowych dokumentów zawierających istotne, wrażliwe czy poufne dane.

Zabezpiecz kopie zapasowe

- Wykonuj kopie zapasowe regularnie i, w miarę możliwości, w sposób zautomatyzowany.
- Przechowuj kopie zapasowe odseparowane od środowiska i sieci teleinformatycznej organizacji.
- Szyfruj kopie zapasowe, zwłaszcza jeśli mają być przenoszone lub przesyłane między lokalizacjami.
- Regularnie testuj procedurę przywracania danych z kopii zapasowych (wykonuj regularne testy pełnego przywracania od początku do końca).
- Stosuj regułę 3-2-1 dla kopii zapasowych:
    a. 3 kopie – przechowuj trzy kopie wszystkich ważnych plików.
    b. 2 miejsca – przechowuj kopie na dwóch różnych nośnikach pamięci, najlepiej w dwóch różnych fizycznych lokalizacjach geograficznych, aby chronić je przed zagrożeniami związanymi z charakterystyką danej geolokalizacji,
    c. 1 off site – przechowuj co najmniej jedną kopię zapasową poza siedzibą firmy, poza środowiskiem teleinformatycznym organizacji, i dodatkowo lub w zdalnej lokalizacji w chmurze.

Zabezpiecz strony internetowe

Upewnij się, że strony internetowe są skonfigurowane i utrzymywane zgodnie z wytycznymi i zapewniają bezpieczeństwo użytkowania. Wszelkie dane osobowe lub dane finansowe, takie jak numery kart kredytowych, muszą być odpowiednio chronione. Przeprowadzaj regularne testy bezpieczeństwa stron internetowych, aby zidentyfikować potencjalne słabości bezpieczeństwa.

Szukaj informacji i dziel się doświadczeniami

Skutecznym narzędziem w walce z cyberprzestępczością jest stałe pogłębianie wiedzy, śledzenie najnowszych wiadomości oraz dzielenie się informacjami w zakresie cyberbezpieczeństwa. Dziel się z innymi swoim doświadczeniem, dobrymi praktykami oraz ostrzegaj innych o potencjalnych atakach.

II. Praktyki bezpiecznego zachowania dla pracownika jednostek rządowych

Nie musisz być ekspertem, aby zwiększyć bezpieczeństwo cyfrowe swojej organizacji. Znaczenie ma nie tylko specjalistyczna wiedza, wyrafinowane narzędzia i programy, ale także Twoje codzienne postępowanie zgodnie z podstawowymi zasadami cyberhigieny i prawidłowymi nawykami cyfrowymi.

Poczta elektroniczna, wiadomości, załączniki, linki

1. **Nie otwieraj załączników ani nie klikaj w linki**, które otrzymujesz w wiadomościach e-mail, jeśli nie jesteś pewien nadawcy wiadomości lub tego, co jest ich zawartością (tzw. „dziwne" wiadomości).
2. Korzystaj z rozwiązań i aplikacji, które **ograniczą** ilość wiadomości e-mail typu **spam i phishing**.
3. Zawsze zwracaj uwagę na nadawcę wiadomości – dokładnie i rzetelnie **weryfikuj adres e-mail nadawcy**.
4. Szczególnie uważnie sprawdzaj wiadomości, które **wywierają na Tobie presję, grożą Ci i wymuszają natychmiastowe działania** – takie jak informacje o niezapłaconych fakturach, mandatach, opóźnieniach w płatnościach, nieodebranych paczkach itp.
5. Zanim otworzysz załącznik lub dokonasz płatności, **sprawdź, czy wiadomość jest prawdziwa** – w razie wątpliwości skontaktuj się z nadawcą innym środkiem komunikacji (np. telefonicznie).
6. Te same zasady dotyczą również **wiadomości SMS, MMS** oraz wiadomości odbieranych za pośrednictwem aplikacji i **portali społecznościowych** (np. What's Up).
7. Zanim otworzysz plik dołączony do wiadomości, zwróć szczególną uwagę na

rozszerzenie pliku załącznika. Najbardziej podejrzane to: .com, .scr, .js, .jse, .rtf, .iso, .img, .htm, .html, .xlsx, .xlsm, .xlsm, .xlsm. Pamiętaj też, że zainfekowany plik może być spakowany do archiwum, np. zip/.rar/.iso.

8. Upewnij się, że link w otrzymanej wiadomości **prowadzi do znanej Tobie i zaufanej strony**. Najedź kursorem na link (nie klikaj!) i sprawdź u dołu przeglądarki lub programu pocztowego, który adres jest wyświetlany. Sprawdź i zweryfikuj adres linku.

Oprogramowanie i urządzenia

9. Korzystaj wyłącznie z **legalnego oprogramowania** i oprogramowania, które jest **autoryzowane lub dystrybuowane przez jednostkę odpowiedzialną za cyberbezpieczeństwo** w Twoim podmiocie. Oprogramowanie należy kupować bezpośrednio od producenta lub pobierać tylko z oficjalnych i zweryfikowanych stron internetowych i sklepów.
10. Pamiętaj, aby **aktualizować sprzęt, firmware, oprogramowanie i aplikacje**, z których korzystasz. Włącz **automatyczne aktualizacje** systemu operacyjnego, oprogramowania antywirusowego, przeglądarek internetowych i innego oprogramowania, gdzie tylko to możliwe.
11. Zawsze **blokuj lub wyłączaj urządzenia**, gdy opuszczasz stanowisko pracy lub przestajesz ich używać.
12. Nie używaj **sprzętu pracowniczego do celów prywatnych** i odwrotnie. Jeśli masz jeden komputer, utwórz dwa oddzielne konta dla każdej z ról.
13. Na urządzeniach pracowniczych **używaj wyłącznie oprogramowania zatwierdzonego** przez osobę odpowiedzialną za cyberbezpieczeństwo w Twoim podmiocie i nigdy nie używaj oprogramowania, które służy do użytku prywatnego (tj. prywatne wiadomości e-mail, komunikatory do prywatnego użytku, prywatne aplikacje, rozrywka itp.).

14. Używaj **oprogramowania antywirusowego z aktualnymi bazami** danych wirusów. Regularnie skanuj swój komputer opcją pełnego skanowania.
15. Nie podłączaj **niezaufanych lub nieznanych nośników pamięci USB** do swojego komputera.
16. Nie bądź 'uprzejmy' i **nie podłączaj ŻADNEGO nieznanego sprzętu do portu USB** Twojego komputera. Nie ładuj niezaufanego lub nieznanego sprzętu innych osób ze swojego portu komputera.
17. **Stwórz aktualną kopię zapasową danych** i zapisuj ją na dyskach zewnętrznych lub przechowuj w chmurze. Użyj reguły 3-2-1 dla kopii zapasowych: 3 kopie zapasowe, 2 kopie na różnych nośnikach i w różnych lokalizacjach geograficznych, oraz 1 kopia zapasowa odseparowana od sieci organizacji (offline).
18. Skonfiguruj, zgodnie z zaleceniami bezpieczeństwa Twojej organizacji, **ustawienia prywatności** w usługach online i aplikacjach, systemie operacyjnym, oprogramowaniu antywirusowym na wszystkich swoich urządzeniach.

Hasła

19. Silne i bezpieczne **hasło powinno być długie** (co najmniej 12-znakowe, ale zalecane jest dłuższe) i **łatwe do zapamiętania**. Powinno zawierać duże i małe litery, cyfry oraz znaki specjalne. Dobrym rozwiązaniem może być stworzenie frazy, np. cytat z piosenki, przysłowie, tytuł filmu/serialu – fraza, która zostanie zmodyfikowana w tylko Tobie znany sposób (np. Don'tWorryBeHungry!) oraz dodanie do niej znaków specjalnych oraz cyfr.
20. Silne hasło nie wymaga cyklicznych, częstych zmian. Jednakże, **zmień je natychmiast**, jeśli tylko istnieje podejrzenie, że wyciekło.
21. Hasła powinny być **unikalne dla każdej usługi** czy systemu – jedna usługa,

jedno hasło.

22. Rozważ skorzystanie z **rozwiązania jakim jest menedżer haseł**, które ułatwi zarządzanie różnymi hasłami do różnych systemów i usług.
23. Używaj **uwierzytelniania wieloskładnikowego** w usługach, z których korzystasz.
24. Rozważ **użycie sprzętowego klucza** w wyznaczonych aplikacjach jako metodę dwuskładniowego uwierzytelnienia, która znacznie podnosi bezpieczeństwo w cyberprzestrzeni.
25. Nie przyklejaj **notatek z zapisanymi hasłami** na ekranie komputera lub laptopa, ani nie pozostawiaj haseł dostępnych w formie pisemnej w innych miejscach (należy zachęcać do korzystania z menedżera haseł).

Bezpieczeństwo fizyczne

26. Każdy dokument powinien być **sklasyfikowany do określonego poziomu poufności** zgodnie z wagą zawartej informacji i wytycznymi organizacji (na przykład sklasyfikowany jako 'wewnętrzny', 'poufne', 'tajne' lub 'ściśle tajne').
27. Postępuj z dokumentami **zgodnie z ich przypisanym poziomem poufności**: zamykaj szafki, umieszczaj w strefie bezpieczeństwa, itp. Nie zostawiaj wydrukowanych wrażliwych dokumentów na biurku ani w pobliżu drukarki.
28. Nie drukuj dokumentów **zdalnie,** jeśli nie jesteś przy drukarce.
29. Nie udostępniaj, ani nie pożyczaj swojej **karty dostępu innym osobom**.
30. Karty dostępu i/lub klucze, które nie są już używane lub utraciły ważność, **zwróć personelowi** odpowiedzialnemu za zarządzanie obiektem.
31. Zgubione lub skradzione karty dostępu i/lub klucze jak najszybciej **zgłaszaj osobie odpowiedzialnej** za zarządzanie obiektem.

32. Zmniejsz **ryzyko kradzieży**, np. w razie potrzeby, przedmioty, takie jak laptopy, powinny być fizycznie przymocowane do biurka.
33. Nie bądź ‘uprzejmy’ i **nie pomagaj innym osobom wejść** do obszarów o ograniczonym dostępie (szczególnie osobom, których nie znasz).
34. W przypadku, gdy jakakolwiek nieznana osoba znajduje się w obszarze o ograniczonym dostępie, zapytaj ją o cel pobytu i **zweryfikuj jej identyfikator** pozwolenia. Zgłoś do odpowiedniego podmiotu, jeśli to konieczne.

Ataki socjotechniczne

35. Natychmiast **zakończ komunikację** z osobą, jeśli istnieje podejrzenie, że jesteś celem ataku socjotechnicznego. Najlepiej po prostu odłuż słuchawkę lub zignoruj wiadomość i natychmiast powiadom pomoc techniczną lub zespół ds. bezpieczeństwa.
36. Nie spiesz się i **nie podejmuj działań pod wpływem emocji**. Ataki socjotechniczne polegają bardzo często na wykreowaniu sytuacji, która potrzebuje niezwykle pilnego działania z Twojej strony. Cyberprzestępcy stwarzają napiętą sytuację i prowokują do popełnienia błędu. Jeśli ktoś naciska, aby ominąć lub zignorować procedury, prawdopodobnie jest to atak.
37. **Poznaj socjotechniczne sztuczki który coraz częściej używają cyberprzestępcy**. Wykorzystują oni emocje, takie jak strach, zastraszanie, ciekawość lub podekscytowanie, aby skłonić Cię do podjęcia działania i zrobienia czegoś, czego oczekują. Jeśli coś wydaje się zbyt piękne, aby mogło być prawdziwe, prawdopodobnie jest to atak.
38. **Zastanów się zanim w coś klikniesz.** Ataki socjotechniczne prowokują do nieumyślnego klikania linków i łączy, pobierania załączników oraz różnych plików (również dokumentów), które są zainfekowane złośliwym oprogramowaniem lub zawierają wirusy. Uważaj: jeden zły ruch może

spowodować, że Twoje urządzenie zostanie zainfekowane, a złośliwe oprogramowanie rozprzestrzeni się na inne urzadzenia w sieci organizacji.

39. Uważaj, co **pobierasz i podłączasz do komputera**. Cyberprzestępcy oczekują, że pod wpływem emocji (ciekawość, podekscytowanie) pobierzesz złośliwe oprogramowanie lub podłączysz zainfekowaną pamięć masową lub urządzenie. Używaj tylko zatwierdzonego sprzętu i oprogramowania.
40. **Nie wahaj się pytać**, a jeśli cokolwiek będzie wydawało się Tobie dziwne lub podejrzane, skontaktuj się z zespołem ds. bezpieczeństwa lub personelem ochrony. Jeśli uważasz, że doświadczasz ataku socjotechnicznego, odłóż słuchawkę (lub nie odpowiadaj na e-maila) i natychmiast skontaktuj się z pomocą techniczną lub zespołem ds. bezpieczeństwa.

Praca z domu

41. **Zabezpiecz swoją sieć domową.** Zmień domyślne hasło administratora na routerze. Skonfiguruj szyfrowanie transmisji w ustawieniach Wi-Fi i ustaw silne hasło. Udostępniaj hasło Wi-Fi tylko zaufanym osobom. Hasło Wi-Fi powinno być inne niż hasło administratora na routerze.
42. **Nie udostępniaj urządzeń** przeznaczonych do pracy członkom rodziny, dzieciom lub przyjaciołom. Nie używaj urzadzeń służbowych do celów prywatnych. Nie używaj urządzeń prywatnych do celów słuzbowych w innych przypadkach niż szczególnie uzasadnione i za zgodą osób odpowiedzialnych za cyberbezpieczeństwo w Twojej organizacji
43. Regularnie **aktualizuj swoje urządzenia domowe**, w tym prywatne laptopy, smartfony, routery, drukarki sieciowe i inne urządzenia IoT korzystające z sieci domowej Wi-Fi. Zainstaluj oprogramowanie z najnowszymi poprawkami oraz aktualizuj firmware urządzeń.
44. Zachowaj **ostrożność podczas korzystania z Hotspotu Wi-Fi**. Ogranicz korzystanie z publicznie dostępnych sieci Wi-Fi. Korzystając z kluczowych

usług (e-mail, bankowość online, portale społecznościowe) poza domową siecią prywatną, używaj własnego modemu LTE lub połączenia VPN. **Zawsze używaj szyfrowanej metody transmisji danych**.

45. Pamiętaj, aby **wyłączać moduł Wi-Fi i Bluetooth** na urządzeniach, gdy ich nie używasz.

Pozostałe zalecenia

46. **Zapoznaj się z zasadami i procedurami** bezpieczeństwa obowiązującymi w Twojej organizacji. W przypadku wystąpienia incydentu bezpieczeństwa, postępuj zgodnie z procedurami
47. Bierz aktywny **udział w szkoleniach i kursach** poszerzających wiedzę na temat cyberbezpieczeństwa.
48. **Sprawdzaj regularnie strony internetowe i profile** instytucji zajmujących się cyberbezpieczeństwem. Dzięki temu będziesz na bieżąco z różnymi zagrożeniami i kampaniami przeciwko użytkownikom Internetu.
49. Bądź na bieżąco z **aktualnościami i nowościami** dotyczącymi cyberbezpieczeństwa.
50. Wszelkie **podejrzane sytuacje oraz incydenty** związane z cyberbezpieczeństwem zgłaszaj zgodnie z instrukcją do zespołu ds. bezpieczeństwa lub personelowi ochrony.