Certyfikacja NASK

Specyfikacja techniczna - Wymagania dla Programu certyfikacji Firma Bezpieczna Cyfrowo

(Egzemplarz dla Klienta)

Wersja **1.0** (data wydania 10.10.2023)

NASK-PIB
ul. Kolska 12
01–045 Warszawa

NIP: 521 04 17 157
Regon: 010464542
KRS: 0000012938

nask@nask.pl
+48 22 380 82 00
www.nask.pl

Certyfikacja NASK

Spis treści

I. Wymagania Organizacyjne 3
4 Zakres oceny 3
II. Wymagania Techniczne 3
5 Zabezpieczenie brzegowe (Firewall) 3
6 Bezpieczna konfiguracja 4
7 Zarządzanie aktualizacjami 5
8 Kontrola dostępu użytkowników 5
9 Ochrona przed złośliwym oprogramowaniem 6
10 Tworzenie kopii zapasowych danych 7
11 Usługi cyfrowe i identyfikacja w sieci 7

Certyfikacja NASK

UWAGA

Numeracja wymagań w tekście jest zgodna z numeracją określoną w dokumentach:

- Przewodnik do wymagań Programu certyfikacji Firma Bezpieczna Cyfrowo;
- Metodyka oceny dla Programu certyfikacji Firma Bezpieczna Cyfrowo.

I. Wymagania Organizacyjne

4 Zakres oceny

4.1

Organizacja powinna zidentyfikować swoją działalność w kontekście zakresu eksploatowanych technologii informacyjnych i komunikacyjnych (ICT).

4.2

Organizacja powinna zidentyfikować aktywa związane z informacjami i środkami przetwarzania informacji.

4.3

Organizacja powinna zidentyfikować wszystkie wykorzystywane usługi w chmurze, które są dostarczane przez stronę trzecią.

II. Wymagania Techniczne

5 Zabezpieczenie brzegowe (Firewall)

5.1

Organizacja powinna zapewnić ochronę informacji w sieciach. Sieci powinny być zarządzane i nadzorowane w celu zapewnienia bezpieczeństwa informacji w systemach i aplikacjach.

5.2

Organizacja powinna zapewnić dostęp uprawnionym użytkownikom i zapobiec nieuprawnionemu dostępowi do systemów i usług poprzez zdefiniowane konfiguracje zabezpieczeń dla sprzętu, oprogramowania, usług (np. usług w chmurze) i sieci, zarówno dla nowo zainstalowanych systemów, jak i dla eksploatowanych systemów przez cały okres ich użytkowania.

5.3

Organizacja powinna zapewnić bezpieczeństwo usług sieciowych gwarantując, iż wszystkie usługi sieciowe świadczone wewnętrznie lub zewnętrznie zawierają zidentyfikowane i właściwie skonfigurowane mechanizmy zabezpieczeń, określony

poziom świadczenia usług oraz udokumentowane wymagania dotyczące zarządzania.

5.4

Organizacja powinna zapewnić bezpieczeństwo usług sieciowych i zapobiec nieuprawnionemu dostępowi do systemów i usług poprzez zdefiniowane konfiguracje zabezpieczeń dla sprzętu, oprogramowania i sieci.

5.5

Organizacja powinna ustanowić, udokumentować, zatwierdzić, wdrożyć i nadzorować zasady konfiguracji zabezpieczeń dla sprzętu, oprogramowania i sieci zgodnie z wymaganiami biznesowymi i wymaganiami bezpieczeństwa informacji.

5.6

Organizacja powinna ustanowić, udokumentować, zatwierdzić, wdrożyć i nadzorować zasady zarządzania zmianami konfiguracji zabezpieczeń dla sprzętu, oprogramowania i sieci zgodnie z wymaganiami biznesowymi i wymaganiami bezpieczeństwa informacji.

6 Bezpieczna konfiguracja

6.1

Organizacja powinna ustanowić i udokumentować politykę kontroli dostępu zgodnie z wymaganiami biznesowymi i wymaganiami bezpieczeństwa informacji. Użytkownicy powinni mieć dostęp wyłącznie do tych sieci i usług sieciowych, do których otrzymali wyraźne uprawienia. Przyznane uprawnienia należy odbierać lub dostosowywać do zaistniałych zmian.

6.2

Organizacja powinna ustanowić proces przydzielania informacji uwierzytelniających i zarządzania dostępem użytkowników. Domyślne informacje uwierzytelniające, predefiniowane lub dostarczone przez dostawców są zmieniane natychmiast po instalacji systemów lub oprogramowania.

6.3

Organizacja powinna ustanowić zasady instalacji oprogramowania i usług, zapewniając wyłączenie lub usunięcie zbędnego, niewykorzystywanego oprogramowania i usług (w tym aplikacji, narzędzi systemowych i usług sieciowych).

6.4

Organizacja powinna wyłączyć wszelkie funkcje automatycznego uruchamiania plików podczas pobierania, które umożliwiają uruchomienie pliku bez autoryzacji użytkownika.

6.5

Organizacja powinna ustanowić i udokumentować politykę kontroli dostępu zgodnie z wymaganiami biznesowymi i wymaganiami bezpieczeństwa informacji oraz ustanowić politykę haseł, proces przydzielania informacji uwierzytelniających i zarządzania dostępem użytkowników.

6.6

Organizacja powinna zapewnić kontrolę dostępu i chronić urządzenia przed nieuprawnionym dostępem.

7 Zarządzanie aktualizacjami

7.1

Organizacja powinna określić istotne wymagania prawne, regulacyjne, umowne oraz dotyczące łańcucha dostaw produktów w celu wdrożenia procesu zarządzania oprogramowaniem i wsparciem technicznym.

7.2

Organizacja powinna określić istotne wymagania prawne, regulacyjne, umowne oraz dotyczące łańcucha dostaw produktów w celu wdrożenia procesu zarządzania oprogramowaniem i wsparciem technicznym. Zasady instalacji oprogramowania i usług powinny zapewnić wyłączenie lub usunięcie zbędnego, niewykorzystywanego lub niewspieranego oprogramowania i usług (w tym aplikacji, narzędzi systemowych i usług sieciowych).

7.3

Organizacja powinna określić zasady zarządzania podatnościami technicznymi i podejmować odpowiednie działania w celu przeciwdziałania związanemu z nimi ryzyku.

8 Kontrola dostępu użytkowników

8.1

Organizacja powinna ustanowić i udokumentować politykę kontroli dostępu zgodnie z wymaganiami biznesowymi i wymaganiami bezpieczeństwa informacji oraz ustanowić politykę haseł, proces przydzielania informacji uwierzytelniających i zarządzania dostępem użytkowników.

8.2

Organizacja powinna ustanowić i udokumentować politykę kontroli dostępu zgodnie z wymaganiami biznesowymi i wymaganiami bezpieczeństwa informacji oraz ustanowić politykę haseł, proces przydzielania informacji uwierzytelniających i zarządzania dostępem użytkowników. Użytkownicy powinni mieć dostęp wyłącznie

do tych sieci i usług sieciowych, do których otrzymali wyraźne uprawienia. Przyznane uprawnienia należy odbierać lub dostosowywać do zaistniałych zmian.

8.3

Organizacja powinna ustanowić i udokumentować politykę kontroli dostępu zgodnie z wymaganiami biznesowymi i wymaganiami bezpieczeństwa informacji oraz ustanowić politykę haseł, proces przydzielania informacji uwierzytelniających i zarządzania dostępem użytkowników. Organizacja powinna zapewnić kontrolę dostępu do urządzeń poprzez procedurę bezpiecznego logowania.

8.4

Organizacja powinna ustanowić i udokumentować politykę kontroli dostępu zgodnie z wymaganiami biznesowymi i wymaganiami bezpieczeństwa informacji oraz ustanowić politykę haseł, proces przydzielania informacji uwierzytelniających i zarządzania dostępem użytkowników. Organizacja powinna zapewnić zarządzanie prawami uprzywilejowanego dostępu.

8.5

Organizacja powinna ustanowić i udokumentować politykę kontroli dostępu zgodnie z wymaganiami biznesowymi i wymaganiami bezpieczeństwa informacji oraz ustanowić politykę haseł, proces przydzielania informacji uwierzytelniających i zarządzania dostępem użytkowników. Organizacja powinna zapewnić zarządzanie prawami uprzywilejowanego dostępu. Należy monitorować i regularnie przeglądać prawa uprzywilejowanego dostępu.

9 Ochrona przed złośliwym oprogramowaniem

9.1

Organizacja powinna wdrożyć ochronę przed złośliwym oprogramowaniem, w połączeniu z właściwym uświadamianiem użytkowników.

9.2

Organizacja powinna zapewnić regularne, zgodnie z zaleceniami dostawcy, aktualizowanie zainstalowanego oprogramowania antywirusowego w celu zachowania jego ciągłej skuteczności do wykrywania złośliwego oprogramowania.

9.3

Organizacja powinna wdrożyć listy dozwolonych aplikacji, zasad i mechanizmy kontrolne, które zapobiegają instalacji i uruchomieniu nieautoryzowanego oprogramowania, a także zapewnić konfigurację oprogramowania antywirusowego uniemożliwiającą uruchomienie złośliwego oprogramowania.

9.4

Organizacja powinna wdrożyć zasady i mechanizmy kontrolne, które chronią przed ryzykiem instalacji i uruchomienia złośliwego kodu dostarczanego poprzez sieć zewnętrzną lub na jakimkolwiek nośniku.

9.5

Organizacja powinna wdrożyć mechanizmy kontrolne, które zapobiegają lub wykrywają korzystanie ze znanych lub podejrzanych złośliwych stron internetowych (np. listy blokowania), a także zapewnić skanowanie stron internetowych w poszukiwaniu złośliwego kodu i oprogramowania, po uzyskaniu do nich dostępu, w celu ochrony użytkownika.

10 Tworzenie kopii zapasowych danych

10.1

Organizacja powinna chronić się przed utratą danych poprzez regularne wykonywanie kopii zapasowych informacji, zgodnie z ustaloną polityką wykonywania kopii zapasowych.

11 Usługi cyfrowe i identyfikacja w sieci

11.1

Organizacja powinna chronić dane podczas transmisji i spoczynku.

11.2

Organizacja powinna wykorzystywać mechanizmy identyfikacji (rozpoznawania i uwierzytelniania użytkowników) w sieci w celu bezpiecznego dostępu do usług cyfrowych.