NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Samohodnotenie v zmysle zákona o kybernetickej bezpečnosti

Vážený prevádzkovateľ základnej služby (PZS),

tento formulár samohodnotenia je určený pre tých PZS, ktorí:

1. majú v období od 1. augusta 2021 do 31. decembra 2023 povinnosť auditu podľa zákona č. 69/2018 Z.z. vo kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 69/2018 Z. z.“),
2. majú len informačné systémy kategórie I. a II. podľa vyhlášky Národného bezpečnostného úradu č. 362/2018 Z.z.z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „vyhláška č. 362/2018 Z. z.“) a
3. majú určeného manažéra kybernetickej bezpečnosti.

Tento formulár vypĺňa za PZS určený manažér kybernetickej bezpečnosti na základe aktuálneho stavu v prostredí PZS pravdivo a tak aby uvedené odpovede bolo možné v prípade potreby preveriť.
K jednotlivým otázkam je odporúčané pripojiť dokumenty podporujúce vyplnené tvrdenia.

K vyplnenému formuláru je potrebné priložiť plán implementácie opatrení kybernetickej bezpečnosti na nasledujúce obdobie schválené štatutárom.

Vyplnený formulár s plánom implementácie opatrení je potrebné elektronicky podpísať kvalifikovaným elektronickým podpisom štatutára a zaslať e-mailom na podatelna@nbu.gov.sk, prípadne zaslať do elektronickej schránky Národného bezpečnostného úradu (NBÚ) prostredníctvom ÚPVS (slovensko.sk).

Časť A: Identifikácia PZS

Identifikácia prevádzkovateľa základných služieb.

A.1 Názov PZS

A.2 Sídlo PZS

Ulica

Číslo ulice

Mesto

PSČ

A.3 IČO PZS

A.4 Meno a priezvisko štatutára

A.5 Dátum zaradenia PZS do registra PZS

Časť B: Základná služba

Zaregistrované základné služby.

Základná služba 1

B.1 Názov základnej služby

B.2 Sektor

Bankovníctvo

B.3 Podsektor

B.4 Dátum zápisu základnej služby

Základná služba 2 (voliteľné)

B.1 Názov základnej služby

B.2 Sektor

Bankovníctvo

B.3 Podsektor

B.4 Dátum zápisu základnej služby

Základná služba 3 (voliteľné)

B.1 Názov základnej služby

B.2 Sektor

Bankovníctvo

B.3 Podsektor

B.4 Dátum zápisu základnej služby

Časť C: Manažér KB

Identifikácia určeného manažéra kybernetickej bezpečnosti a vyjadrenie sa k popisu jeho právomocí, povinností a zodpovedností, ktoré sú súčasťou jeho pracovnej náplne alebo obdobného opisu jeho pracovných činností.

C.1 Meno určeného manažéra KB

C.2 Dátum určenia do funkcie manažéra KB

C.3

Vyplýva z pozície Vami určeného manažéra KB jeho možnosť predkladať návrhy a oznamovať informácie v oblasti KB priamo štatutárnemu orgánu danej PZS a jeho nezávislosť od riadenia prevádzky a vývoja služieb informačných technológií?

- ◯ Áno
- ◯ Nie

Časť D: Informačné systémy

Identifikácia centrálnych informačných systémov, popis ich funkčnosti a ich kategória v zmysle vyhlášky č. 362/2018 Z.z.
V prípade, že má Vaša organizácia viac ako 5 informačných systémov, použite prosím priloženú prílohu "Formulár pre dodatočné informačné systémy".

Informačný systém 1

D.1 Názov centrálneho IS podporujúceho ZS

D.2 Základný popis funkčnosti centrálneho IS

D.3 Názov ZS, ktorú podporuje

D.4 Kategória IS

Informačný systém 2 (voliteľné)

D.1 Názov centrálneho IS podporujúceho ZS

D.2 Základný popis funkčnosti centrálneho IS

D.3 Názov ZS, ktorú podporuje

D.4 Kategória IS

Informačný systém 3 (voliteľné)

D.1 Názov centrálneho IS podporujúceho ZS

D.2 Základný popis funkčnosti centrálneho IS

D.3 Názov ZS, ktorú podporuje

D.4 Kategória IS

Informačný systém 4 (voliteľné)

D.1 Názov centrálneho IS podporujúceho ZS

D.2 Základný popis funkčnosti centrálneho IS

D.3 Názov ZS, ktorú podporuje

D.4 Kategória IS

Informačný systém 5 (voliteľné)

D.1 Názov centrálneho IS podporujúceho ZS

D.2 Základný popis funkčnosti centrálneho IS

D.3 Názov ZS, ktorú podporuje

D.4 Kategória IS

Časť E: Stratégia KB

Informácia o tom, či je vedením prijatá stratégia kybernetickej bezpečnosti ako dokument určujúci hlavné ciele prevádzkovateľa základnej služby v oblasti ďalšieho rozvoja kybernetickej bezpečnosti.

E.1 Máte manažmentom prijatú stratégiu kybernetickej bezpečnosti a jej príslušné ciele?

○ Áno ○ Nie ○ Čiastočne

Príslušný dokument (voliteľné):

Časť F: Správa aktív

Popis toho ako má prevádzkovateľ identifikované svoje aktíva (informácie, procesy, HW, SW, služby, sieťové komponenty a dodávateľov) ako základný stavebný prvok základných služieb a ako je prevádzkovateľ ZS schopný spravovať ich počas prevádzky základnej služby.

F.1 Máte identifikované všetky informačné aktíva, ktoré podporujú niektorú z identifikovaných ZS?

◯ Áno ◯ Nie ◯ Čiastočne

Príslušný dokument (voliteľné):

F.2 Máte určenú ich klasifikáciu pre dôvernosť, integritu a dostupnosť?

◯ Áno ◯ Nie ◯ Čiastočne

Príslušný dokument (voliteľné):

F.3 Máte identifikované všetky podporné aktíva, ktoré podporujú niektorú z identifikovaných ZS?

◯ Áno ◯ Nie ◯ Čiastočne

Príslušný dokument (voliteľné):

F.4 Máte identifikovaných všetkých dodávateľov, ktorí Vám svojím poskytovaním služieb podporujú prevádzku ZS?

◯ Áno ◯ Nie ◯ Čiastočne

Príslušný dokument (voliteľné):

F.5 Máte identifikovaných vlastníkov ku všetkým identifikovaným aktívam?

◯ Áno ◯ Nie ◯ Čiastočne

Príslušný dokument (voliteľné):

F.6 Vediete si evidenciu všetkých aktív podieľajúcich sa na prevádzke ZS?

◯ Áno ◯ Nie ◯ Čiastočne

Príslušný dokument (voliteľné):

F.7 Máte zavedený proces na aktualizáciu evidencie aktív?

◯ Áno ◯ Nie ◯ Čiastočne

Príslušný dokument (voliteľné):

Časť G: Manažment konfigurácií

Popis toho aký má prevádzkovateľ prehľad o nastaveniach svojich aktív a o evidencii zmien týchto nastavení.

G.1 Vediete si evidenciu o konfiguračných nastaveniach identifikovaných aktív a služieb?

○ Áno ○ Nie ○ Čiastočne

Príslušný dokument (voliteľné):

G.2 Mate zavedený proces pravidelného aktualizovania záznamov v evidencii konfigurácií aktív a služieb?

○ Áno ○ Nie ○ Čiastočne

Príslušný dokument (voliteľné):

Časť H: Technické zraniteľnosti

Popis toho ako je prevádzkovateľ schopný identifikovať či sa publikované známe zraniteľnosti týkajú jeho aktív a schopnosť vyhodnocovať riziko potenciálneho prieniku zneužitím týchto zraniteľnosti.

H.1 Získavate informácie o známych zraniteľnostiach od dodávateľov Vašich aktív, SK-CERT, CSIRT-SK, pripadne iných?

○ Áno ○ Nie ○ Čiastočne

Príslušný dokument (voliteľné):

H.2 Vyhodnocujete dopad známych zraniteľností na Vaše aktíva a vyhodnocujete riziko spojené s týmito zraniteľnosťami?

○ Áno ○ Nie ○ Čiastočne

Príslušný dokument (voliteľné):

Časť I: Prevádzkový monitoring

Schopnosť prevádzkovateľa identifikovať a vyhodnocovať stavové veličiny svojich aktív tak, aby bol schopný odhaliť potenciálne zlyhanie konkrétneho prvku alebo celej služby.

I.1 Máte určené, pre ktoré aktíva a komponenty vo Vašom prostredí potrebujete mať nastavený prevádzkový monitoring?

○ Áno ○ Nie ○ Čiastočne

Príslušný dokument (voliteľné):

I.2 Vykonávate monitoring týchto parametrov tak aby ste mali nepretržitý prehľad o vašom prostredí?

○ Áno ○ Nie ○ Čiastočne

Príslušný dokument (voliteľné):

Časť J: Bezpečnostný monitoring

Schopnosť prevádzkovateľa identifikovať také udalosti (za normálnej prevádzky bežné) alebo kombináciu udalostí v jeho infraštruktúre, ktoré môžu znamenať prítomnosť škodlivého kódu alebo hackera.

J.1 Máte implementovaný nástroj na výkon bezpečnostného monitoringu nad aktívami, ktoré sa podieľajú na základnej službe?

○ Áno ○ Nie ○ Čiastočne

Príslušný dokument (voliteľné):

J.2 Máte nastavený proces, ktorým budete vedieť reagovať na kybernetický bezpečnostný incident?

○ Áno ○ Nie ○ Čiastočne

Príslušný dokument (voliteľné):

Časť K: Personálna bezpečnosť

Popis toho ako vykonáva prevádzkovateľ kontrolu dodržiavania svojich politík vlastnými zamestnancami alebo zamestnancami dodávateľov.

K.1 Vykonávate kontrolu dodržiavania bezpečnostných politík zo strany vlastných zamestnancov a zamestnancov dodávateľov?

◯ Áno ◯ Nie ◯ Čiastočne

Príslušný dokument (voliteľné):

Časť L: Riadenie rizík

Schopnosť prevádzkovateľa identifikovať riziká kybernetickej bezpečnosti, vyhodnotiť ich veľkosť a navrhnúť k nim opatrenia na zníženie rizika.

L.1 Identifikujete a vyhodnocujete riziká kybernetickej bezpečnosti?

◯ Áno ◯ Nie ◯ Čiastočne

Príslušný dokument (voliteľné):

L.2 Navrhujete a implementujete bezpečnostné opatrenia kybernetickej bezpečnosti, ktorými znížite neakceptovateľne veľké zvyškové riziká?

◯ Áno ◯ Nie ◯ Čiastočne

Príslušný dokument (voliteľné):

Časť M: Riadenie bezpečnosti sietí

Popis toho aký je stav a spôsob správy sieťovej segmentácie a zariadení, ktoré segmentáciu zabezpečujú v prostredí prevádzkovateľa.

M.1 Máte implementovanú bezpečnostnú sieťovú segmentáciu?

◯ Áno ◯ Nie ◯ Čiastočne

Príslušný dokument (voliteľné):

M.2 Vykonávate aktívnu a priebežnú správu pravidiel na zariadeniach oddeľujúcich jednotlivé sieťové segmenty?

◯ Áno ◯ Nie ◯ Čiastočne

Príslušný dokument (voliteľné):

Časť N: Riadenie prístupov

Popis toho ako prevádzkovateľ riadi prístupy vlastných používateľov a používateľov dodávateľov ku svojim informáciám, zariadeniam a sieťam.

N.1 Máte definované rozsahy logických a aj fyzických prístupových oprávnení vlastných zamestnancov a zamestnancov dodávateľov ku všetkým svojim aktívam?

◯ Áno ◯ Nie ◯ Čiastočne

Príslušný dokument (voliteľné):

N.2 Vykonávate pravidelnú kontrolu nad nastavenými rozsahmi prístupových oprávnení na vašich aktívach?

◯ Áno ◯ Nie ◯ Čiastočne

Príslušný dokument (voliteľné):

Časť O: Riadenie procesov pre správu a údržbu IS

Popis toho ako prevádzkovateľ vykonáva správu svojich zariadení a systémov v prevádzke a ako je schopný udržať ich v riadnom chode.

O.1 Máte zavedený proces zmenového konania (Change management)?

○ Áno ○ Nie ○ Čiastočne

Príslušný dokument (voliteľné):

O.2 Máte zavedený proces incident manažmentu?

○ Áno ○ Nie ○ Čiastočne

Príslušný dokument (voliteľné):

O.3 Máte zavedený proces zálohovania?

○ Áno ○ Nie ○ Čiastočne

Príslušný dokument (voliteľné):

O.4 Máte zavedený proces kontinuity procesov a služieb a obnovu po havárii?

○ Áno ○ Nie ○ Čiastočne

Príslušný dokument (voliteľné):

Časť P: Riadenie dodávateľských vzťahov

Schopnosť prevádzkovateľa zadefinovať požiadavky na dodávateľa pred zmluvným vzťahom a aj schopnosť ich merať a vyhodnocovať počas prevádzky.

P.1 Monitorujete na pravidelnej báze parametre služieb, ktoré Vám poskytujú dodávatelia?

○ Áno ○ Nie ○ Čiastočne

Príslušný dokument (voliteľné):

Podpis štatutára:

Dátum vyplnenia samohodnotenia: