Národný bezpečnostný úrad

Zákon č. 95/2019 Z. z. o informačných systémoch verejnej správy

---

Povinnosti

Základné úlohy Národného bezpečnostného úradu v oblasti kybernetickej bezpečnosti

Odsek 1, Paragraf 5, Článok I

Úrad v oblasti kybernetickej bezpečnosti
a) riadi a koordinuje výkon štátnej správy,
b) určuje štandardy, operačné postupy, vydáva metodiku a politiku správania sa v kybernetickom priestore,
c) určuje zásady predchádzania kybernetickým bezpečnostným incidentom a zásady ich riešenia,
d) vypracúva národnú stratégiu kybernetickej bezpečnosti a ročnú správu o stave kybernetickej bezpečnosti v Slovenskej republike v spolupráci s príslušnými štátnymi orgánmi,
e) je národným kontaktným miestom pre kybernetickú bezpečnosť pre zahraničie a zabezpečuje spoluprácu s jednotnými kontaktnými miestami členských štátov Európskej únie a Organizácie Severoatlantickej zmluvy,
f) plní notifikačné a nahlasovacie povinnosti voči príslušným orgánom Európskej únie a Organizácie Severoatlantickej zmluvy a podieľa sa a podporuje vytváranie partnerstiev na národnej a medzinárodnej úrovni v oblasti kybernetickej bezpečnosti,
g) zabezpečuje členstvo Slovenskej republiky v skupine pre spoluprácu a v sieti jednotiek CSIRT,
h) v spolupráci s Ministerstvom zahraničných vecí a európskych záležitostí Slovenskej republiky rozvíja medzinárodnú spoluprácu a sleduje vplyvy aktivít v oblasti kybernetickej bezpečnosti na zahraničnopolitické záujmy Slovenskej republiky a partnerov v rámci Európskej únie a Organizácie Severoatlantickej zmluvy,
i) spolupracuje s ústrednými orgánmi, inými orgánmi štátnej správy a jednotkami CSIRT, prevádzkovateľmi základných služieb a poskytovateľmi digitálnych služieb pri plnení úloh podľa tohto zákona,
j) spravuje a prevádzkuje jednotný informačný systém kybernetickej bezpečnosti,
k) na základe oznámenia ústredného orgánu, prevádzkovateľa základnej služby, poskytovateľa digitálnej služby alebo z vlastnej iniciatívy určuje
1. základnú službu a zaraďuje ju do zoznamu základných služieb,
2. digitálnu službu a zaraďuje ju do zoznamu digitálnych služieb,
3. poskytovateľa digitálnej služby a zaraďuje ho do registra poskytovateľov digitálnych služieb,
4. prevádzkovateľa základnej služby a zaraďuje ho do registra prevádzkovateľov základných služieb,
l) vedie a spravuje
1. zoznam základných služieb,
2. register prevádzkovateľov základných služieb,
3. zoznam digitálnych služieb,
4. register poskytovateľov digitálnych služieb,
5. zoznam akreditovaných jednotiek CSIRT,
m) systematicky získava, sústreďuje, analyzuje a vyhodnocuje informácie o stave kybernetickej bezpečnosti v Slovenskej republike,
n) akredituje jednotky CSIRT okrem Národnej jednotky CSIRT a vládnej jednotky CSIRT a zaraďuje ich do zoznamu akreditovaných jednotiek CSIRT,
o) plní úlohy príslušného orgánu pre digitálne služby,
p) zabezpečuje a zodpovedá za koordinované riešenie kybernetických bezpečnostných incidentov na národnej úrovni,
q) rieši kybernetické bezpečnostné incidenty, vyhlasuje výstrahu a varovania pred závažným kybernetickým bezpečnostným incidentom, ukladá povinnosť vykonať reaktívne opatrenie a schvaľuje ochranné opatrenie,
r) zasiela včasné varovania,
s) prijíma vnútroštátne hlásenia o kybernetických bezpečnostných incidentoch,
t) prijíma hlásenia o kybernetických bezpečnostných incidentoch zo zahraničia a zabezpečuje spoluprácu s medzinárodnými organizáciami a orgánmi iných štátov pri riešení kybernetických bezpečnostných incidentov s cezhraničným charakterom,
u) vykonáva kontrolu, vydáva rozhodnutia o uložení opatrení na nápravu a ukladá pokutu za priestupok alebo iný správny delikt,
v) vykonáva audit alebo požiada orgán posudzovania zhody o vykonanie auditu u prevádzkovateľa základnej služby,
w) vydáva znalostné štandardy a v spolupráci s Ministerstvom školstva, vedy, výskumu a športu Slovenskej republiky vykonáva a zabezpečuje budovanie bezpečnostného povedomia,
x) koordinuje výskum a vývoj

Dohoda úradu o spolupráci s orgánmi verejnej moci alebo inými právnickými osobami na účely zabezpečenia plnenia úloh v zmysle zákona

(V roli Orgán verejnej moci) (V roli Právnická osoba)

Odsek 2, Paragraf 5, Článok I

Na účely zabezpečenia plnenia úloh podľa tohto zákona môže úrad na účel zabezpečenia kybernetickej bezpečnosti uzatvoriť písomnú dohodu o spolupráci a o výmene informácií a podkladov s orgánmi verejnej moci alebo s inou právnickou osobou. Pri poskytnutí informácií je prijímajúci subjekt povinný zabezpečiť najmenej rovnakú úroveň dôvernosti ako subjekt, ktorý informácie poskytol.

Postavenie a pôsobnosť Národného bezpečnostného úradu v rámci jednotky CSIRT

(V roli Národná jednotka CSIRT)

Odsek 1, Paragraf 6, Článok I

Úrad má postavenie národnej jednotky CSIRT s pôsobnosťou pre Slovenskú republiku, ktorá musí spĺňať podmienky akreditácie podľa § 14 a plniť úlohy jednotky CSIRT podľa § 15 pre všetky sektory a podsektory uvedené v prílohe č. 1 a digitálne služby okrem tých sektorov a podsektorov, pre ktoré plní úlohy jednotky CSIRT ústredný orgán. Národná jednotka CSIRT je zaradená v zozname akreditovaných jednotiek CSIRT.

Pôsobnosť národnej jednotky CSIRT

(V roli Národná jednotka CSIRT)

Odsek 2, Paragraf 6, Článok I

Národná jednotka CSIRT plní úlohu ústredného orgánu v rozsahu podľa § 9 ods. 1 písm. a), ak ústredný orgán túto úlohu nezabezpečí spôsobom podľa § 9 ods. 2.

Zodpovednostné vzťahy

(V roli Prevádzkovateľ základnej služby)

Odsek 4, Paragraf 6, Článok I

Plnenie úloh úradu podľa odsekov 1 a 2 nezbavuje prevádzkovateľa základnej služby ani ústredný orgán zodpovednosti za plnenie povinností podľa tohto zákona a ani za plnenie povinností vo vzťahu k sieťam a informačným systémom podľa osobitných predpisov.

Povinnosť poskytovať informácie, údaje a hlásenia prostredníctvom jednotného informačného systému kybernetickej bezpečnosti

(V roli Ten, kto je povinný podľa tohto zákona poskytovať informácie, údaje a hlásenia prostredníctvom jednotného informačného systému kybernetickej bezpečnosti)

Odsek 6, Paragraf 8, Článok I

Ten, kto je povinný podľa tohto zákona poskytovať informácie, údaje a hlásenia prostredníctvom jednotného informačného systému kybernetickej bezpečnosti, je povinný ich poskytovať bezodplatne a bezodkladne po tom, ako sa dozvie o skutočnosti zakladajúcej túto povinnosť. Informácie, údaje a hlásenia sa poskytujú spôsobom určeným funkcionalitou jednotného informačného systému kybernetickej bezpečnosti.

Povinnosť mlčanlivosti

(V roli Ten, kto plní alebo plnil úlohy na základe tohto zákona a v súvislosti s ním)

Odsek 1, Paragraf 12, Článok I

Kto plní alebo plnil úlohy na základe tohto zákona alebo v súvislosti s ním, je povinný zachovávať mlčanlivosť o skutočnostiach, o ktorých sa v súvislosti s plnením úloh podľa tohto zákona dozvedel a ktoré nie sú verejne známe. Povinnosť zachovávať mlčanlivosť trvá aj po skončení dohody o spolupráci podľa § 5 ods. 3, pracovnoprávneho vzťahu alebo obdobného pracovného vzťahu vrátane služobného pomeru. Ustanoveniami o povinnosti zachovávať mlčanlivosť podľa tohto zákona nie je dotknutá povinnosť mlčanlivosti alebo zachovania tajomstva podľa osobitných predpisov.

Zbavenie povinnosti mlčanlivosti

(V roli Riaditeľ Národného bezpečnostného úradu) (V roli Štatutárny orgán)

Odsek 2, Paragraf 12, Článok I

O zbavení povinnosti mlčanlivosti osoby podľa odseku 1 rozhodne v pôsobnosti
a) úradu riaditeľ úradu,
b) iného subjektu štatutárny orgán.

Zodpovednosť Národného bezpečnostného úradu za škodu, ktorá vznikla oznámením podľa § 12 odseku 4 tohto zákona

Odsek 5, Paragraf 12, Článok I

Za škodu spôsobenú prevádzkovateľom základnej služby, poskytovateľom digitálnej služby, ich zamestnancom alebo osobe oznamujúcej kybernetický bezpečnostný incident, ktorá vznikla oznámením podľa odseku 4, zodpovedá úrad.

Spracúvanie osobných údajov v jednotnom informačnom systéme kybernetickej bezpečnosti na nevyhnutne potrebný čas

Odsek 6, Paragraf 12, Článok I

Na účely riešenia kybernetického bezpečnostného incidentu v rozsahu potrebnom na jeho identifikáciu a zabezpečenia kybernetickej bezpečnosti úrad v záujme národnej bezpečnosti spracováva v jednotnom informačnom systéme kybernetickej bezpečnosti na čas nevyhnutne potrebný osobné údaje spôsobom podľa osobitného predpisu.

Povinnosť Národného bezpečnostného úradu zabezpečiť nepretržitú ochranu osobných údajov a informácií spracúvaných podľa tohto zákona

Odsek 7, Paragraf 12, Článok I

Úrad zabezpečí nepretržitú ochranu osobných údajov a informácií spracúvaných podľa tohto zákona pred nezákonným vyzradením, zneužitím, poškodením, neoprávneným zničením, odcudzením a stratou spôsobom podľa osobitného predpisu.

Posudzovanie zhody

Odsek 1, Paragraf 13, Článok I

Zhodu jednotky CSIRT s podmienkami akreditácie jednotky CSIRT posudzuje úrad na základe žiadosti.

Začatie konania podľa § 13 odseku 1 zákona

Odsek 3, Paragraf 13, Článok I

Konanie podľa odseku 1 sa začína dňom doručenia žiadosti úradu podľa odseku 2. Ak žiadosť nie je úplná, úrad vyzve žiadateľa na jej doplnenie v určenej lehote, ktorá nesmie byť kratšia ako desať dní. Ak žiadateľ žiadosť v stanovenej lehote nedoplní požadovaným spôsobom, úrad na žiadosť ďalej neprihliada.

Lehota na vydanie rozhodnutia vo veci akreditácie jednotky CSIRT

Odsek 4, Paragraf 13, Článok I

Úrad o akreditácii rozhodne do 90 dní odo dňa doručenia úplnej žiadosti, a ak posúdi splnenie zhody jednotky CSIRT s podmienkami akreditácie jednotky CSIRT, vydá rozhodnutie o akreditácii. Rozhodnutie o akreditácii sa vydáva na dobu určitú, najviac na päť rokov.

Prolongácia platného rozhodnutia o akreditácii

Odsek 5, Paragraf 13, Článok I

Úrad môže na základe žiadosti opakovane predĺžiť platné rozhodnutie o akreditácii, ak nenastala zmena podmienok, na základe ktorých bolo rozhodnutie o akreditácii vydané. Žiadosť podľa predchádzajúcej vety sa predkladá úradu najmenej šesť mesiacov pred uplynutím doby platnosti rozhodnutia o akreditácii, ktoré sa má predĺžiť. Na konanie a na podanie žiadosti sa primerane vzťahujú odseky 2 až 4. Ak úrad predĺženie akreditácie uzná, vydá o tom rozhodnutie podľa odseku 4 s doložkou „predĺženie“.

Uznávanie akreditácie jednotky CSIRT

Odsek 6, Paragraf 13, Článok I

Úrad na základe žiadosti ústredného orgánu, ktorý má plniť úlohy jednotky CSIRT, uzná aj akreditáciu jednotky CSIRT, ktorá bola akreditovaná podľa predpisov iného štátu alebo medzinárodnej organizácie, ak je preukázateľne zabezpečené splnenie podmienok akreditácie jednotky CSIRT; podmienka podľa § 14 písm. a) sa nepreukazuje. Na konanie a na podanie žiadosti sa primerane vzťahujú odseky 2 až 4. Úrad o akreditácii vydá rozhodnutie podľa odseku 4 s doložkou „uznanie“ najviac na dobu platnosti, na ktorú bola jednotka CSIRT akreditovaná podľa predpisov iného štátu alebo medzinárodnej organizácie.

Zaradenie jednotky CSIRT do zoznamu akreditovaných jednotiek CSIRT

Odsek 7, Paragraf 13, Článok I

Úrad jednotku CSIRT akreditovanú spôsobom podľa tohto zákona zaradí do zoznamu akreditovaných jednotiek CSIRT.

Podmienky akreditácie jednotky CSIRT

(V roli Žiadateľ o akreditáciu jednotky CSIRT)

Paragraf 14, Článok I

Žiadateľ o akreditáciu jednotky CSIRT podľa § 13 dokumentáciou preukazuje, že jednotka CSIRT

a) má požadované technické, technologické a personálne vybavenie podľa všeobecne záväzného právneho predpisu, ktorý vydá úrad,

b) má vytvorené podmienky umožňujúce chránený prenos a spracovanie údajov spôsobom podľa osobitného predpisu,

c) chráni informácie a údaje, ktoré v súvislosti s plnením povinností podľa tohto zákona získava a spracováva ich tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integrita,

d) má umiestnenú dokumentáciu, informačné systémy a ostatné informačno-komunikačné technológie v zabezpečenom priestore tak, aby nebola narušená ich dôvernosť, autentickosť a integrita.

Zodpovednosť za riešenie kybernetických bezpečnostných incidentov

(V roli Ten, kto plní úlohy jednotky CSIRT)

Odsek 1, Paragraf 15, Článok I

Ten, kto plní úlohy jednotky CSIRT v rozsahu svojej pôsobnosti určenej podľa prílohy č. 1, zodpovedá za riešenie kybernetických bezpečnostných incidentov a vykonáva preventívne služby a reaktívne služby.

Subjekty vykonávajúce reaktívne služby

(V roli Jednotka CSIRT)

Odsek 4, Paragraf 15, Článok I

Reaktívne služby vykonáva jednotka CSIRT za účasti prevádzkovateľa základnej služby alebo poskytovateľa digitálnej služby.

Povinnosti toho, kto plní úlohy jednotky CSIRT

(V roli Ten, kto plní úlohy jednotky CSIRT)

Odsek 1, Paragraf 16, Článok I

Ten, kto plní úlohy jednotky CSIRT,
a) musí zabezpečiť, aby jednotka CSIRT v jeho pôsobnosti, ktorá je zaradená v zozname akreditovaných jednotiek CSIRT, nepretržite počas celej doby svojej prevádzky spĺňala podmienky akreditácie jednotky CSIRT podľa § 14 a zároveň plnila všetky úlohy podľa § 15,
b) oznamuje úradu všetky zmeny, ktoré majú vplyv na akreditáciu jednotky CSIRT bezodkladne po tom, ako nastali,
c) si vyžiada vyjadrenie Národnej banky Slovenska alebo Európskej centrálnej banky k postupu ústredného orgánu pri plnení úloh podľa tohto zákona, ak prevádzkovateľom základnej služby je dohliadaný subjekt finančného trhu, nad ktorým vykonáva dohľad Národná banka Slovenska podľa osobitných predpisov22) alebo nad ktorým vykonáva dohľad Európska centrálna banka podľa osobitného predpisu.

Postup konania v prípade, ak akreditovaná jednotka CSIRT prestane spĺňať podmienky podľa § 14 alebo ak neplní úlohy podľa § 15 tohto zákona

(V roli Ten, kto plní úlohy jednotky CSIRT)

Odsek 2, Paragraf 16, Článok I

Ak akreditovaná jednotka CSIRT prestane spĺňať podmienky podľa § 14 alebo ak neplní úlohy podľa § 15, ten, kto plní úlohy jednotky CSIRT, to bezodkladne oznámi úradu; úrad na základe oznámenia podľa predchádzajúcej vety zruší rozhodnutie o akreditácii a jednotku CSIRT vyradí zo zoznamu akreditovaných jednotiek CSIRT.

Konanie Národného bezpečnostného úradu v situáciách podľa § 16, ods. 2 tohto zákona

Odsek 3, Paragraf 16, Článok I

Úrad môže na základe vlastného zistenia oboznámiť toho, kto plní úlohy jednotky CSIRT o nedostatkoch v plnení podmienok podľa § 14 alebo úloh podľa § 15 s uvedením lehoty na ich odstránenie. Ak nedostatky podľa prechádzajúcej vety na základe oznámenia úradu neodstráni v určenej lehote, úrad zruší rozhodnutie o akreditácii a jednotku CSIRT vyradí zo zoznamu akreditovaných jednotiek CSIRT.

Zaradenie základnej služby do zoznamu základných služieb podľa § 3 písm. k) prvého bodu tohto zákona

Odsek 2, Paragraf 17, Článok I

Úrad zaradí základnú službu podľa § 3 písm. k) prvého bodu do zoznamu základných služieb a jej prevádzkovateľa do registra prevádzkovateľov základných služieb:
a) na základe oznámenia prevádzkovateľom tejto služby podľa odseku 1,
b) na základe podnetu ústredného orgánu, ak došlo k prekročeniu identifikačných kritérií prevádzkovanej služby podľa § 18,
c) z vlastnej iniciatívy, ak sa úrad dozvedel o prekročení identifikačných kritérií prevádzkovanej služby podľa § 18 a nedošlo k postupu podľa písmena a) alebo písmena b).

Zaradenie základnej služby do zoznamu základných služieb podľa § 3 písm. k) druhého bodu tohto zákona

Odsek 3, Paragraf 17, Článok I

Úrad v spolupráci s príslušným ústredným orgánom zaradí základnú službu podľa § 3 písm. k) druhého bodu do zoznamu základných služieb a jej prevádzkovateľa do registra prevádzkovateľov základných služieb.

Zaradenie základnej služby podľa § 3 písm. k) tretieho bodu tohto zákona do zoznamu základných služieb

Odsek 4, Paragraf 17, Článok I

Úrad zaradí základnú službu podľa § 3 písm. k) tretieho bodu do zoznamu základných služieb a jej prevádzkovateľa do registra prevádzkovateľov základných služieb zo zákona.

Oznámenie o zaradení služby do zoznamu základných služieb a do registra prevádzkovateľ základných služieb

Odsek 6, Paragraf 17, Článok I

Zaradenie služby do zoznamu základných služieb a jej prevádzkovateľa do registra prevádzkovateľov základných služieb oznámi úrad prevádzkovateľovi tejto služby prostredníctvom informačného systému kybernetickej bezpečnosti.

Povinnosť prevádzkovateľa základnej služby prijať a dodržiavať všeobecné bezpečnostné opatrenia

(V roli Prevádzkovateľ základnej služby)

Odsek 1, Paragraf 19, Článok I

Prevádzkovateľ základnej služby je povinný do šiestich mesiacov odo dňa oznámenia o zaradení do registra prevádzkovateľov základných služieb prijať a dodržiavať všeobecné bezpečnostné opatrenia najmenej v rozsahu bezpečnostných opatrení podľa § 20 a sektorové bezpečnostné opatrenia, ak sú prijaté.

Povinnosť prevádzkovateľa základnej služby uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

(V roli Prevádzkovateľ základnej služby)

Odsek 2, Paragraf 19, Článok I

Prevádzkovateľ základnej služby je povinný pri uzatvorení zmluvy s dodávateľom na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa základnej služby (ďalej len „tretia strana“) uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa tohto zákona počas celej doby platnosti zmluvy.

Povinnosť prevádzkovateľa základnej služby informovať o zaradení do registra prevádzkovateľov základných služieb

(V roli Prevádzkovateľ základnej služby)

Odsek 3, Paragraf 19, Článok I

Prevádzkovateľ základnej služby je povinný dňom zaradenia do registra prevádzkovateľov základných služieb o tejto skutočnosti informovať podnik na poskytovanie elektronických komunikačných služieb alebo sietí podľa osobitného predpisu, ku ktorému je sieť alebo informačný systém základnej služby pripojená. Na základe informovania podľa predchádzajúcej vety uzatvára prevádzkovateľ základnej služby s podnikom zmluvu podľa odseku 2.

Povinnosť prevádzkovateľa základnej služby informovať o hlásenom kybernetickom bezpečnostnom incidente

(V roli Prevádzkovateľ základnej služby)

Odsek 4, Paragraf 19, Článok I

Prevádzkovateľ základnej služby je povinný informovať v nevyhnutnom rozsahu tretiu stranu o hlásenom kybernetickom bezpečnostnom incidente za predpokladu, že by sa plnenie zmluvy podľa odseku 2 stalo nemožným, ak úrad nerozhodne inak. Povinnosť zachovávať mlčanlivosť tým nie je dotknutá.

Povinnosti Národného bezpečnostného úradu v prípade, ak prevádzkovateľ základnej služby poskytuje službu aj v inom členskom štáte Európskej únie

Odsek 5, Paragraf 19, Článok I

Ak prevádzkovateľ základnej služby túto službu poskytuje aj v inom členskom štáte Európskej únie, úrad v súčinnosti s príslušným orgánom tohto členského štátu rozhodne o tom, podľa kritérií ktorého členského štátu bude prevádzkovateľ základnej služby identifikovaný tak, aby bol jednoznačne identifikovaný ako prevádzkovateľ základnej služby aspoň v jednom z týchto členských štátov.

Ďalšie povinnosti prevádzkovateľa základnej služby

(V roli Prevádzkovateľ základnej služby)

Odsek 6, Paragraf 19, Článok I

Prevádzkovateľ základnej služby je ďalej povinný
a) riešiť kybernetický bezpečnostný incident,
b) bezodkladne hlásiť závažný kybernetický bezpečnostný incident,
c) spolupracovať s úradom a ústredným orgánom pri riešení hláseného kybernetického bezpečnostného incidentu a na tento účel im poskytnúť potrebnú súčinnosť, ako aj informácie získané z vlastnej činnosti dôležité pre riešenie kybernetického bezpečnostného incidentu,
d) v čase kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní,
e) oznámiť orgánu činnému v trestnom konaní alebo Policajnému zboru skutočnosti, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka, ak sa o ňom hodnoverným spôsobom dozvie.

Povinnosť prevádzkovateľa základnej služby hlásiť zmeny v údajoch

(V roli Prevádzkovateľ základnej služby)

Odsek 7, Paragraf 19, Článok I

Prevádzkovateľ základnej služby je povinný hlásiť zmeny v údajoch podľa § 17 ods. 5 do 30 dní odo dňa ich vzniku prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.

Obmedzenie zodpovednosti prevádzkovateľa základnej služby za škodu, ktorá vznikne inému subjektu obmedzením kontinuity základnej služby

Odsek 8, Paragraf 19, Článok I

Prevádzkovateľ základnej služby nezodpovedá za škodu, ktorá vznikne inému subjektu obmedzením kontinuity základnej služby pri riešení kybernetického bezpečnostného incidentu spôsobom a postupom podľa § 27. Za škodu spôsobenú obmedzením kontinuity základnej služby kybernetickým bezpečnostným incidentom plnením povinnosti spôsobom podľa predchádzajúcej vety zodpovedá úrad.

Oznamovacia povinnosť poskytovateľa digitálnej služby

(V roli Poskytovateľ digitálnej služby)

Odsek 1, Paragraf 21, Článok I

Poskytovateľ digitálnej služby je povinný do 30 dní odo dňa začatia poskytovania digitálnej služby oznámiť úradu
a) názov a sídlo,
b) kontaktné údaje,
c) poskytovanú službu,
d) názov, sídlo a kontaktné údaje zástupcu podľa § 23.

Zaradenie služby do zoznamu digitálnych služieb na základe oznámenia

Odsek 2, Paragraf 21, Článok I

Na základe oznámenia podľa odseku 1 úrad zaradí službu do zoznamu digitálnych služieb a jej poskytovateľa do registra poskytovateľov digitálnych služieb.

Zaradenie služby do zoznamu digitálnych služieb na základe vlastného zistenia Národného bezpečnostného úradu

Odsek 3, Paragraf 21, Článok I

Úrad zaradí službu do zoznamu digitálnych služieb a jej poskytovateľa do registra poskytovateľov digitálnych služieb aj na základe vlastného zistenia.

Oznámenie o zaradení služby do zoznamu digitálnych služieb

Odsek 4, Paragraf 21, Článok I

Zaradenie služby do zoznamu digitálnych služieb a jej poskytovateľa do registra poskytovateľov digitálnych služieb oznámi úrad poskytovateľovi tejto služby.

Lehota na ohlásenie zmien v údajoch podľa § 21 odsek 1 tohto zákona

(V roli Poskytovateľ digitálnej služby)

Odsek 5, Paragraf 21, Článok I

Poskytovateľ digitálnej služby je povinný hlásiť zmeny v údajoch podľa odseku 1 do 30 dní odo dňa ich vzniku.

Povinnosť prijať a dodržiavať vhodné a primerané bezpečnostné opatrenia

(V roli Poskytovateľ digitálnej služby)

Odsek 1, Paragraf 22, Článok I

Poskytovateľ digitálnej služby je povinný do šiestich mesiacov odo dňa oznámenia o zaradení do registra poskytovateľov digitálnych služieb prijať a dodržiavať vhodné a primerané bezpečnostné opatrenia podľa osobitného predpisu na účely riadenia rizík súvisiacich s ohrozením kontinuity digitálnej služby a procesu riešenia kybernetických bezpečnostných incidentov. Na tento účel je poskytovateľ digitálnej služby povinný vyčleniť dostatočné personálne, materiálno-technické, časové a finančné zdroje s cieľom zabezpečenia kontinuity digitálnej služby.

Oblasti posúdenia za účelom splnenia povinností podľa § 22 ods. 1 tohto zákona - demonštratívny výpočet

(V roli Poskytovateľ digitálnej služby)

Odsek 2, Paragraf 22, Článok I

Poskytovateľ digitálnej služby na účely splnenia povinnosti podľa odseku 1 posudzuje najmä
a) bezpečnosť sietí a informačného systému a jeho schopnosť predchádzať a riešiť kybernetický bezpečnostný incident,
b) spôsob zachovania kontinuity digitálnej služby v prípade kybernetického bezpečnostného incidentu,
c) súlad sietí a informačného systému s bezpečnostnými štandardmi v oblasti kybernetickej bezpečnosti.

Ďalšie povinnosti poskytovateľa digitálnej služby

(V roli Poskytovateľ digitálnej služby)

Odsek 3, Paragraf 22, Článok I

Poskytovateľ digitálnej služby je povinný
a) hlásiť každý kybernetický bezpečnostný incident, ak disponuje informáciami, na základe ktorých je spôsobilý identifikovať, či má tento kybernetický bezpečnostný incident podstatný vplyv podľa osobitného predpisu, a to bezodkladne po jeho zistení,
b) riešiť hlásený kybernetický bezpečnostný incident,

c) spolupracovať s úradom pri riešení hláseného kybernetického bezpečnostného incidentu.

Povinnosť poskytovateľa digitálnej služby uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností

(V roli Poskytovateľ digitálnej služby)

Odsek 4, Paragraf 22, Článok I

Ak poskytovateľ digitálnej služby využíva na poskytovanie svojej digitálnej služby prevádzkovateľa základnej služby, je povinný uzatvoriť s prevádzkovateľom základnej služby zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa tohto zákona počas celej doby, keď poskytovateľ digitálnej služby využíva na poskytovanie svojej digitálnej služby prevádzkovateľa základnej služby.

Informačná povinnosť poskytovateľa digitálnej služby

(V roli Poskytovateľ digitálnej služby)

Odsek 5, Paragraf 22, Článok I

O hlásenom kybernetickom bezpečnostnom incidente v nevyhnutnom rozsahu informuje poskytovateľ digitálnej služby tretiu stranu, ak by sa plnenie zmluvy stalo nemožným, ak úrad nerozhodne inak. Povinnosť zachovávať mlčanlivosť tým nie je dotknutá.

Zástupca poskytovateľa digitálnej služby sídliaci mimo územia Európskej únie

(V roli Poskytovateľ digitálnej služby)

Odsek 2, Paragraf 23, Článok I

Ak poskytovateľ digitálnej služby, ktorý poskytuje digitálnu službu v Slovenskej republike, nemá sídlo v Európskej únii a neustanovil si svojho zástupcu v inom členskom štáte Európskej únie, je povinný si ustanoviť svojho zástupcu v Slovenskej republike.

Činnosť Národného bezpečnostného úradu pri výkone štátnej správy v prípade poskytovateľa digitálnej služby sídlom na území SR

Odsek 3, Paragraf 23, Článok I

Ak má poskytovateľ digitálnej služby sídlo v Slovenskej republike alebo tu má ustanoveného zástupcu, ale jeho siete a informačné systémy sa nachádzajú v inom členskom štáte Európskej únie, úrad pri výkone štátnej správy spolupracuje s príslušným orgánom členského štátu Európskej únie.

Povinnosť hlásiť všetky závažné kybernetické incidenty

(V roli Prevádzkovateľ základnej služby)

Odsek 1, Paragraf 24, Článok I

Prevádzkovateľ základnej služby je povinný hlásiť každý závažný kybernetický bezpečnostný incident, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov.

Povinnosť poskytovateľa digitálnej služby hlásiť každý závažný kybernetický bezpečnostný incident

(V roli Poskytovateľ digitálnej služby)

Odsek 3, Paragraf 24, Článok I

Ak prevádzkovateľ základnej služby využíva na poskytovanie základnej služby poskytovateľa digitálnej služby, je poskytovateľ digitálnej služby povinný hlásiť každý závažný kybernetický bezpečnostný incident, ktorý postihol poskytovateľa digitálnej služby.

Odosielanie neúplného hlásenia kybernetického bezpečnostného incidentu

(V roli Prevádzkovateľ základnej služby)

Odsek 5, Paragraf 24, Článok I

Ak do okamihu hlásenia kybernetického bezpečnostného incidentu nepominuli jeho účinky, prevádzkovateľ základnej služby je povinný odoslať neúplné hlásenie kybernetického bezpečnostného incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia, a bezodkladne po obnove riadnej prevádzky siete a informačného systému toto hlásenie doplní.

Povinnosť poskytovateľa digitálnej služby hlásiť kybernetický bezpečnostný incident

(V roli Poskytovateľ digitálnej služby)

Odsek 1, Paragraf 25, Článok I

Poskytovateľ digitálnej služby je povinný hlásiť kybernetický bezpečnostný incident podľa § 22 ods. 3 písm. a) spôsobom podľa § 24 ods. 4.

Neúplné hlásenie kybernetického bezpečnostného incidentu

(V roli Poskytovateľ digitálnej služby)

Odsek 2, Paragraf 25, Článok I

Ak do okamihu hlásenia kybernetického bezpečnostného incidentu nepominuli jeho účinky, poskytovateľ digitálnej služby je povinný odoslať neúplné hlásenie kybernetického bezpečnostného incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia, a

bezodkladne po obnove riadnej prevádzky siete a informačného systému toto hlásenie doplní.

Spracovanie a analýza dobrovoľných hlásení kybernetických bezpečnostných incidentov

Odsek 2, Paragraf 26, Článok I

Úrad spracováva a analyzuje dobrovoľné hlásenia kybernetických bezpečnostných incidentov v rozsahu, v akom to úradu umožňujú technické podmienky a kapacity tak, aby nedošlo k neprimeranému zaťažovaniu subjektov a neobmedzovala sa medzinárodná spolupráca.

Vyhlásenie výstrahy a varovania

Odsek 2, Paragraf 27, Článok I

Výstrahu a varovanie vyhlasuje úrad prostredníctvom jednotného informačného systému kybernetickej bezpečnosti. Ak ide o naliehavý verejný záujem, výstraha a varovanie sa vyhlási aj prostredníctvom hromadných oznamovacích prostriedkov a na ústrednom portáli verejnej správy.

Uloženie povinnosti riešiť kybernetický bezpečnostný incident

Odsek 3, Paragraf 27, Článok I

Povinnosť riešiť kybernetický bezpečnostný incident ukladá úrad rozhodnutím tomu, kto plní úlohy jednotky CSIRT, prevádzkovateľovi základnej služby a poskytovateľovi digitálnej služby.

Povinnosť vykonať reaktívne opatrenie

Odsek 5, Paragraf 27, Článok I

Povinnosť vykonať reaktívne opatrenie ukladá úrad rozhodnutím prevádzkovateľovi základnej služby alebo poskytovateľovi digitálnej služby, ktorí sú pri riešení závažného kybernetického bezpečnostného incidentu nečinní, alebo ak riešenie závažného kybernetického bezpečnostného incidentu je zjavne neúspešné. Poskytovateľovi digitálnej služby možno uložiť povinnosť vykonať reaktívne opatrenie iba počas krízovej situácie.

Oznamovacia povinnosť v súvislosti s vykonaním reaktívneho opatrenia

(V roli Poskytovateľ digitálnej služby) (V roli Prevádzkovateľ základnej služby)

Odsek 6, Paragraf 27, Článok I

Prevádzkovateľ základnej služby alebo poskytovateľ digitálnej služby je povinný bezodkladne oznámiť a preukázať úradu prostredníctvom jednotného informačného systému kybernetickej bezpečnosti vykonanie reaktívneho opatrenia a jeho výsledok.

Prijatie ochranného opatrenia prevádzkovateľom základnej služby

(V roli Prevádzkovateľ základnej služby)

Odsek 7, Paragraf 27, Článok I

Ochranné opatrenie prijíma prevádzkovateľ základnej služby na základe analýzy riešeného závažného kybernetického bezpečnostného incidentu.

Povinnosť prevádzkovateľa základnej služby predložiť navrhované ochranné opatrenie na schválenie Národnému bezpečnostnému úradu

(V roli Prevádzkovateľ základnej služby)

Odsek 8, Paragraf 27, Článok I

Prevádzkovateľ základnej služby je na výzvu úradu v určenej lehote povinný predložiť navrhované ochranné opatrenie na schválenie. Úrad rozhodnutím navrhované opatrenie schváli a určí lehotu na jeho vykonanie. V prípade, ak prevádzkovateľ základnej služby nenavrhne ochranné opatrenie v určenej lehote alebo ak je navrhované ochranné opatrenie zjavne neúspešné, je prevádzkovateľ základnej služby povinný spolupracovať s úradom, ústredným orgánom a s tým, kto prevádzkuje jednotku CSIRT, na jeho návrhu.

Ďalšie povinnosti Národného bezpečnostného úradu v prípade, keď boli vyčerpané všetky spôsoby riešenia závažného kybernetického bezpečnostného incidentu

Odsek 9, Paragraf 27, Článok I

Ak úrad na účely zaistenia kybernetickej bezpečnosti vyčerpá všetky spôsoby riešenia závažného kybernetického bezpečnostného incidentu podľa tohto zákona, predloží predsedovi Bezpečnostnej rady Slovenskej republiky informáciu o predpokladaných vplyvoch kybernetického bezpečnostného incidentu na bezpečnosť štátu ako podklad na riešenie krízovej situácie.

Povinnosť Národného bezpečnostného úradu informovať Vojenské spravodajstvo

(V roli Poskytovateľ digitálnej služby) (V roli Prevádzkovateľ základnej služby)

Odsek 10, Paragraf 27, Článok I

Z dôvodu neodkladnosti a naliehavosti riešenia závažného kybernetického bezpečnostného incidentu úrad na účely kybernetickej obrany informuje Vojenské spravodajstvo, že závažný kybernetický bezpečnostný incident je kategórie tretieho (III) stupňa, alebo o skutočnostiach, ktoré nasvedčujú, že závažný kybernetický bezpečnostný incident môže byť kybernetickým terorizmom. Prevádzkovateľ základnej služby a poskytovateľ digitálnej služby, ktorí hlásia tento kybernetický bezpečnostný incident, sú na účely zabezpečenia kybernetickej obrany povinní poskytnúť Vojenskému spravodajstvu informácie v potrebnom rozsahu. O postupe podľa prvej vety informuje úrad predsedu Bezpečnostnej rady Slovenskej republiky.

Postup Národného bezpečnostného úradu pri výkone kontroly

Odsek 1, Paragraf 28, Článok I

Pri výkone kontroly nad dodržiavaním ustanovení tohto zákona a jeho vykonávacích predpisov postupuje úrad podľa základných pravidiel kontrolnej činnosti ustanovených osobitným predpisom.

Práva a povinnosti prevádzkovateľa základnej služby a poskytovateľa digitálnej služby počas výkonu kontroly

(V roli Poskytovateľ digitálnej služby) (V roli Prevádzkovateľ základnej služby)

Odsek 2, Paragraf 28, Článok I

Na účely výkonu kontroly má prevádzkovateľ základnej služby a poskytovateľ digitálnej služby práva a povinnosti kontrolovaného subjektu podľa osobitného predpisu.

Vykonanie kontroly Národným bezpečnostným úradom

Odsek 3, Paragraf 28, Článok I

Úrad vykoná kontrolu u poskytovateľa digitálnej služby, ak je dôvodné podozrenie, že poskytovateľ digitálnej služby nespĺňa požiadavky ustanovené týmto zákonom.

Povinnosť prevádzkovateľa základnej služby preveriť účinnosť prijatých bezpečnostných opatrení

(V roli Prevádzkovateľ základnej služby)

Odsek 1, Paragraf 29, Článok I

Prevádzkovateľ základnej služby je povinný preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených týmto zákonom vykonaním auditu kybernetickej bezpečnosti do dvoch rokov odo dňa zaradenia prevádzkovateľa základnej služby do registra prevádzkovateľov základných služieb.

Rozsah preverovania účinnosti prijatých bezpečnostných opatrení

(V roli Prevádzkovateľ základnej služby)

Odsek 2, Paragraf 29, Článok I

Prevádzkovateľ základnej služby je povinný preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených týmto zákonom vykonaním auditu kybernetickej bezpečnosti v rozsahu stanovenom podľa všeobecne záväzného právneho predpisu, ktorý vydá úrad, a to v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov po každej zmene majúcej významný vplyv na realizované bezpečnostné opatrenia a v určenom časovom intervale.

Povinnosť prevádzkovateľa základnej služby predložiť Národnému bezpečnostnému úradu správu o audite

(V roli Prevádzkovateľ základnej služby)

Odsek 4, Paragraf 29, Článok I

Prevádzkovateľ základnej služby je povinný predložiť záverečnú správu o výsledkoch auditu úradu spolu s opatreniami na nápravu a s lehotami na ich odstránenie do 30 dní od ukončenia auditu.

Úhrada nákladov auditu kybernetickej bezpečnosti

(V roli Prevádzkovateľ základnej služby)

Odsek 6, Paragraf 29, Článok I

Náklady na audit kybernetickej bezpečnosti podľa odseku 1 znáša prevádzkovateľ základnej služby a náklady na audit kybernetickej bezpečnosti podľa odseku 5 znáša úrad.

Splnomocňovacie ustanovenia týkajúce sa jednotky CSIRT a kybernetickej bezpečnosti

Odsek 1, Paragraf 32, Článok I

Úrad ustanoví všeobecne záväzným právnym predpisom
a) podrobnosti o technickom, technologickom a personálnom vybavení jednotky CSIRT (§ 14 písm. a)),
b) identifikačné kritériá prevádzkovanej služby CSIRT (§ 18),
c) obsah bezpečnostných opatrení, obsah a štruktúru bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (§ 20 ods. 1 a 5),

d) bezpečnostné štandardy a znalostné štandardy v oblasti kybernetickej bezpečnosti (§ 5 ods. 1 písm. w), § 20 ods. 1),
e) identifikačné kritériá pre jednotlivé kategórie kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov (§ 24 ods. 1 a 4),
f) pravidlá a rozsah auditu kybernetickej bezpečnosti a podrobnosti o akreditácii orgánov posudzovania zhody a o obsahu záverečnej správy o výsledkoch auditu kybernetickej bezpečnosti podľa (§ 29 ods. 1 až 4).

Sprístupnenie jednotného informačného systému kybernetickej bezpečnosti

Odsek 1, Paragraf 34, Článok I

Úrad sprístupní jednotný informačný systém kybernetickej bezpečnosti spôsobom podľa § 8 do 18 mesiacov odo dňa účinnosti toho zákona.

Zaradenie do zoznamu služieb

Odsek 5, Paragraf 34, Článok I

Úrad do 9. novembra 2018 zaradí službu do zoznamu základných služieb a jej prevádzkovateľa do registra prevádzkovateľov základných služieb, ak ešte nie sú zaradení; na digitálnu službu a jej poskytovateľa sa to vzťahuje rovnako.

Povinnosť zosúladiť zmluvy prevádzkovateľa so zákonom

(V roli Prevádzkovateľ základnej služby)

Odsek 8, Paragraf 34, Článok I

Zmluvy uzatvorené na výkon činností podľa § 19 ods. 2 musí prevádzkovateľ základnej služby zosúladiť s týmto zákonom najneskôr do dvoch rokov od účinnosti tohto zákona.

Povinnosť prevádzkovateľa základnej služby podrobiť sa auditu kybernetickej bezpečnosti

(V roli Prevádzkovateľ základnej služby)

Odsek 9, Paragraf 34, Článok I

Prevádzkovateľ základnej služby je povinný podrobiť sa auditu kybernetickej bezpečnosti a predložiť záverečnú správu o výsledkoch auditu úradu najneskôr do troch rokov od uplynutia lehoty podľa odseku 5.

Práva

Dohoda úradu o spolupráci s orgánmi verejnej moci alebo inými právnickými osobami na účely zabezpečenia plnenia úloh v zmysle zákona

Odsek 2, Paragraf 5, Článok I

Na účely zabezpečenia plnenia úloh podľa tohto zákona môže úrad na účel zabezpečenia kybernetickej bezpečnosti uzatvoriť písomnú dohodu o spolupráci a o výmene informácií a podkladov s orgánmi verejnej moci alebo s inou právnickou osobou. Pri poskytnutí informácií je prijímajúci subjekt povinný zabezpečiť najmenej rovnakú úroveň dôvernosti ako subjekt, ktorý informácie poskytol.

Dohoda Národného bezpečnostného úradu o spolupráci s fyzickými osobami na účely zabezpečenia plnenia úloh

Odsek 3, Paragraf 5, Článok I

Na účely zabezpečenia plnenia úloh podľa tohto zákona môže úrad uzatvoriť písomnú dohodu o spolupráci s fyzickou osobou. Dohoda o spolupráci musí obsahovať konkrétnu formu a podmienky spolupráce a fyzická osoba musí byť oprávnená na oboznamovanie sa s utajovanými skutočnosťami príslušného stupňa utajenia, ak to plnenie úloh vyžaduje.

Subjekty s priamymi prístupovými právami do neverejnej časti jednotného informačného systému kybernetickej bezpečnosti

(V roli Orgán verejnej moci) (V roli Poskytovateľ digitálnej služby) (V roli Prevádzkovateľ základnej služby)

Odsek 5, Paragraf 8, Článok I

K neverejnej časti jednotného informačného systému kybernetickej bezpečnosti má priamy prístup v elektronickej forme v reálnom čase, v rozsahu určenom úradom alebo osobitným predpisom a na základe vecnej pôsobnosti
a) ústredný orgán,
b) jednotka CSIRT zaradená v zozname akreditovaných jednotiek CSIRT,
c) prevádzkovateľ základnej služby a poskytovateľ digitálnej služby,
d) Národná banka Slovenska,
e) Úrad na ochranu osobných údajov Slovenskej republiky,
f) iný orgán verejnej moci rozhodnutím úradu.

Právo Národného bezpečnostného úradu použiť osobné údaje a informácie, získané na základe tohto zákona

Odsek 8, Paragraf 12, Článok I

Informácie a osobné údaje získané na základe tohto zákona alebo v súvislosti s ním môže úrad použiť len na plnenie úloh podľa tohto zákona.

Prolongácia platného rozhodnutia o akreditácii

Odsek 5, Paragraf 13, Článok I

Úrad môže na základe žiadosti opakovane predĺžiť platné rozhodnutie o akreditácii, ak nenastala zmena podmienok, na základe ktorých bolo rozhodnutie o akreditácii vydané. Žiadosť podľa predchádzajúcej vety sa predkladá úradu najmenej šesť mesiacov pred uplynutím doby platnosti rozhodnutia o akreditácii, ktoré sa má predĺžiť. Na konanie a na podanie žiadosti sa primerane vzťahujú odseky 2 až 4. Ak úrad predĺženie akreditácie uzná, vydá o tom rozhodnutie podľa odseku 4 s doložkou „predĺženie“.

Konanie Národného bezpečnostného úradu v situáciách podľa § 16, ods. 2 tohto zákona

Odsek 3, Paragraf 16, Článok I

Úrad môže na základe vlastného zistenia oboznámiť toho, kto plní úlohy jednotky CSIRT o nedostatkoch v plnení podmienok podľa § 14 alebo úloh podľa § 15 s uvedením lehoty na ich odstránenie. Ak nedostatky podľa prechádzajúcej vety na základe oznámenia úradu neodstráni v určenej lehote, úrad zruší rozhodnutie o akreditácii a jednotku CSIRT vyradí zo zoznamu akreditovaných jednotiek CSIRT.

Zmluva o spôsobe a forme hlásenia kybernetických bezpečnostných incidentov

Odsek 6, Paragraf 24, Článok I

Na účely hlásenia kybernetických bezpečnostných incidentov a zaistenia funkcionality jednotného informačného systému kybernetickej bezpečnosti môže úrad namiesto postupu uvedeného v § 8 ods. 6 uzatvoriť písomnú zmluvu o spôsobe a forme hlásenia kybernetických bezpečnostných incidentov s prevádzkovateľom základnej služby.

Zmluva o spôsobe a forme hlásení kybernetických bezpečnostných incidentov

Odsek 3, Paragraf 25, Článok I

Na účely hlásenia kybernetických bezpečnostných incidentov a zaistenia funkcionality jednotného informačného systému kybernetickej bezpečnosti môže úrad namiesto postupu uvedeného v § 8 ods. 6 uzatvoriť písomnú zmluvu o spôsobe a forme hlásenia kybernetických bezpečnostných incidentov s poskytovateľom digitálnej služby.

Oprávnenia Národného bezpečnostného úradu v prípade závažného kybernetického bezpečnostného incidentu alebo hrozby

Odsek 1, Paragraf 27, Článok I

V prípade závažného kybernetického bezpečnostného incidentu alebo jeho hrozby môže úrad
a) vyhlásiť výstrahu a varovanie pred závažným kybernetickým bezpečnostným incidentom,
b) uložiť povinnosť riešiť kybernetický bezpečnostný incident,
c) uložiť povinnosť vykonať reaktívne opatrenie,
d) požadovať návrh opatrení a vykonanie opatrení určených na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu závažného kybernetického bezpečnostného incidentu (ďalej len „ochranné opatrenie“).

Práva a povinnosti prevádzkovateľa základnej služby a poskytovateľa digitálnej služby počas výkonu kontroly
(V roli Poskytovateľ digitálnej služby) (V roli Prevádzkovateľ základnej služby)

Odsek 2, Paragraf 28, Článok I

Na účely výkonu kontroly má prevádzkovateľ základnej služby a poskytovateľ digitálnej služby práva a povinnosti kontrolovaného subjektu podľa osobitného predpisu.

Oprávnenie Národného bezpečnostného úradu na výkon auditu kybernetickej bezpečnosti

Odsek 5, Paragraf 29, Článok I

Bez toho, aby bol dotknutý odsek 1, môže úrad kedykoľvek vykonať audit kybernetickej bezpečnosti u prevádzkovateľa základnej služby, alebo požiadať orgán posudzovania zhody, aby vykonal takýto audit u prevádzkovateľa základnej služby s cieľom potvrdiť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených týmto zákonom.

Splnomocňovacie ustanovenia pre sektorové bezpečnostné opatrenia

Odsek 2, Paragraf 32, Článok I

Ústredný orgán sa v spolupráci s úradom splnomocňuje na vydanie všeobecne záväzného právneho predpisu, ktorým ustanovia sektorové bezpečnostné opatrenia v rozsahu svojej pôsobnosti podľa prílohy č. 1 a v súlade s bezpečnostnými štandardmi v oblasti kybernetickej bezpečnosti.

Nepriame povinnosti

Uloženie povinnosti riešiť kybernetický bezpečnostný incident

(V roli Poskytovateľ digitálnej služby) (V roli Prevádzkovateľ základnej služby) (V roli Ten, kto plní úlohy jednotky CSIRT)

Odsek 3, Paragraf 27, Článok I

Povinnosť riešiť kybernetický bezpečnostný incident ukladá úrad rozhodnutím tomu, kto plní úlohy jednotky CSIRT, prevádzkovateľovi základnej služby a poskytovateľovi digitálnej služby.

Povinnosť vykonať reaktívne opatrenie

(V roli Poskytovateľ digitálnej služby) (V roli Prevádzkovateľ základnej služby)

Odsek 5, Paragraf 27, Článok I

Povinnosť vykonať reaktívne opatrenie ukladá úrad rozhodnutím prevádzkovateľovi základnej služby alebo poskytovateľovi digitálnej služby, ktorí sú pri riešení závažného kybernetického bezpečnostného incidentu nečinní, alebo ak riešenie závažného kybernetického bezpečnostného incidentu je zjavne neúspešné. Poskytovateľovi digitálnej služby možno uložiť povinnosť vykonať reaktívne opatrenie iba počas krízovej situácie.

Vykonanie kontroly Národným bezpečnostným úradom

(V roli Poskytovateľ digitálnej služby)

Odsek 3, Paragraf 28, Článok I

Úrad vykoná kontrolu u poskytovateľa digitálnej služby, ak je dôvodné podozrenie, že poskytovateľ digitálnej služby nespĺňa požiadavky ustanovené týmto zákonom.

Nepriame práva

Základné úlohy Národného bezpečnostného úradu v oblasti kybernetickej bezpečnosti

(V roli Jednotka CSIRT) (V roli Národná jednotka CSIRT) (V roli Poskytovateľ digitálnej služby) (V roli Prevádzkovateľ základnej služby)

Odsek 1, Paragraf 5, Článok I

Úrad v oblasti kybernetickej bezpečnosti
a) riadi a koordinuje výkon štátnej správy,
b) určuje štandardy, operačné postupy, vydáva metodiku a politiku správania sa v kybernetickom priestore,
c) určuje zásady predchádzania kybernetickým bezpečnostným incidentom a zásady ich riešenia,
d) vypracúva národnú stratégiu kybernetickej bezpečnosti a ročnú správu o stave kybernetickej bezpečnosti v Slovenskej republike v spolupráci s príslušnými štátnymi orgánmi,
e) je národným kontaktným miestom pre kybernetickú bezpečnosť pre zahraničie a zabezpečuje spoluprácu s jednotnými kontaktnými miestami členských štátov Európskej únie a Organizácie Severoatlantickej zmluvy,
f) plní notifikačné a nahlasovacie povinnosti voči príslušným orgánom Európskej únie a Organizácie Severoatlantickej zmluvy a podieľa sa a podporuje vytváranie partnerstiev na národnej a medzinárodnej úrovni v oblasti kybernetickej bezpečnosti,
g) zabezpečuje členstvo Slovenskej republiky v skupine pre spoluprácu a v sieti jednotiek CSIRT,
h) v spolupráci s Ministerstvom zahraničných vecí a európskych záležitostí Slovenskej republiky rozvíja medzinárodnú spoluprácu a sleduje vplyvy aktivít v oblasti kybernetickej bezpečnosti na zahraničnopolitické záujmy Slovenskej republiky a partnerov v rámci Európskej únie a Organizácie Severoatlantickej zmluvy,
i) spolupracuje s ústrednými orgánmi, inými orgánmi štátnej správy a jednotkami CSIRT, prevádzkovateľmi základných služieb a poskytovateľmi digitálnych služieb pri plnení úloh podľa tohto zákona,
j) spravuje a prevádzkuje jednotný informačný systém kybernetickej bezpečnosti,
k) na základe oznámenia ústredného orgánu, prevádzkovateľa základnej služby, poskytovateľa digitálnej služby alebo z vlastnej iniciatívy určuje
1. základnú službu a zaraďuje ju do zoznamu základných služieb,
2. digitálnu službu a zaraďuje ju do zoznamu digitálnych služieb,
3. poskytovateľa digitálnej služby a zaraďuje ho do registra poskytovateľov digitálnych služieb,
4. prevádzkovateľa základnej služby a zaraďuje ho do registra prevádzkovateľov základných služieb,

l) vedie a spravuje
1. zoznam základných služieb,
2. register prevádzkovateľov základných služieb,
3. zoznam digitálnych služieb,
4. register poskytovateľov digitálnych služieb,
5. zoznam akreditovaných jednotiek CSIRT,
m) systematicky získava, sústreďuje, analyzuje a vyhodnocuje informácie o stave kybernetickej bezpečnosti v Slovenskej republike,
n) akredituje jednotky CSIRT okrem Národnej jednotky CSIRT a vládnej jednotky CSIRT a zaraďuje ich do zoznamu akreditovaných jednotiek CSIRT,
o) plní úlohy príslušného orgánu pre digitálne služby,
p) zabezpečuje a zodpovedá za koordinované riešenie kybernetických bezpečnostných incidentov na národnej úrovni,
q) rieši kybernetické bezpečnostné incidenty, vyhlasuje výstrahu a varovania pred závažným kybernetickým bezpečnostným incidentom, ukladá povinnosť vykonať reaktívne opatrenie a schvaľuje ochranné opatrenie,
r) zasiela včasné varovania,
s) prijíma vnútroštátne hlásenia o kybernetických bezpečnostných incidentoch,
t) prijíma hlásenia o kybernetických bezpečnostných incidentoch zo zahraničia a zabezpečuje spoluprácu s medzinárodnými organizáciami a orgánmi iných štátov pri riešení kybernetických bezpečnostných incidentov s cezhraničným charakterom,
u) vykonáva kontrolu, vydáva rozhodnutia o uložení opatrení na nápravu a ukladá pokutu za priestupok alebo iný správny delikt,
v) vykonáva audit alebo požiada orgán posudzovania zhody o vykonanie auditu u prevádzkovateľa základnej služby,
w) vydáva znalostné štandardy a v spolupráci s Ministerstvom školstva, vedy, výskumu a športu Slovenskej republiky vykonáva a zabezpečuje budovanie bezpečnostného povedomia,
x) koordinuje výskum a vývoj

Spolupráca pri vypracovaní Národnej stratégie kybernetickej bezpečnosti

Odsek 3, Paragraf 7, Článok I

Ústredný orgán a iný orgán štátnej správy spolupracujú s úradom na vypracovaní národnej stratégie kybernetickej bezpečnosti a na tento účel sú povinné poskytnúť mu informácie v potrebnom rozsahu.

Základné úlohy ústredného orgánu v oblasti zabezpečenia kybernetickej bezpečnosti

(V roli Prevádzkovateľ základnej služby)

Odsek 1, Paragraf 9, Článok I

Ústredný orgán v rozsahu svojej pôsobnosti pre sektor alebo podsektor podľa prílohy č. 1, zodpovedá za zabezpečenie kybernetickej bezpečnosti tým, že
a) plní úlohy jednotky CSIRT spôsobom podľa odseku 2,
b) poskytuje úradu požadovanú súčinnosť a informácie získané z vlastnej činnosti dôležité na zabezpečenie kybernetickej bezpečnosti; informácie sa poskytujú len za podmienky, že ich poskytnutím nedôjde k ohrozeniu plnenia konkrétnej úlohy podľa osobitného predpisu alebo k odhaleniu jej zdrojov, prostriedkov, totožnosti osôb konajúcich v jej prospech alebo k ohrozeniu medzinárodnej spravodajskej spolupráce,
c) spolupracuje s ostatnými ústrednými orgánmi a prevádzkovateľmi základných služieb vo svojej pôsobnosti pri plnení úloh podľa tohto zákona,
d) buduje bezpečnostné povedomie, koordinovanú spoluprácu na všetkých stupňoch riadenia kybernetickej bezpečnosti a aplikuje bezpečnostné opatrenia a politiku správania sa v kybernetickom priestore,
e) v spolupráci s úradom určuje špecifické sektorové identifikačné kritériá podľa § 18 ods. 3,
f) identifikuje základnú službu a prevádzkovateľa základnej služby a ich aktuálny zoznam predkladá úradu na účely zaradenia do zoznamu základných služieb a registra prevádzkovateľov základných služieb,
g) spolupracuje so zahraničnou inštitúciou obdobného zamerania.

Poskytovanie súčinnosti a informácií

Odsek 2, Paragraf 10, Článok I

Iný orgán štátnej správy ďalej poskytuje úradu požadovanú súčinnosť a informácie získané z vlastnej činnosti dôležité na zabezpečenie kybernetickej bezpečnosti; informácie sa poskytujú len za podmienky, že ich poskytnutím nedôjde k ohrozeniu plnenia konkrétnej úlohy podľa osobitného predpisu alebo k odhaleniu jej zdrojov, prostriedkov, totožnosti osôb konajúcich v jej prospech, alebo k ohrozeniu medzinárodnej spravodajskej spolupráce.

Zodpovednosť Národného bezpečnostného úradu za škodu, ktorá vznikla oznámením podľa § 12 odseku 4 tohto zákona

(V roli Poskytovateľ digitálnej služby) (V roli Prevádzkovateľ základnej služby)

Odsek 5, Paragraf 12, Článok I

Za škodu spôsobenú prevádzkovateľom základnej služby, poskytovateľom digitálnej služby, ich zamestnancom alebo osobe oznamujúcej kybernetický bezpečnostný incident, ktorá vznikla oznámením podľa odseku 4, zodpovedá úrad.

Posudzovanie zhody

(V roli Jednotka CSIRT)

Odsek 1, Paragraf 13, Článok I

Zhodu jednotky CSIRT s podmienkami akreditácie jednotky CSIRT posudzuje úrad na základe žiadosti.

Podanie žiadosti v zmysle § 13 odseku 1 tohto zákona

Odsek 2, Paragraf 13, Článok I

Žiadosť podľa odseku 1 predkladá úradu v elektronickej podobe ústredný orgán, ktorý má plniť úlohy jednotky CSIRT; k žiadosti prikladá dokumentáciu preukazujúcu splnenie podmienok akreditácie jednotky CSIRT.

Začatie konania podľa § 13 odseku 1 zákona

(V roli Žiadateľ o akreditáciu jednotky CSIRT)

Odsek 3, Paragraf 13, Článok I

Konanie podľa odseku 1 sa začína dňom doručenia žiadosti úradu podľa odseku 2. Ak žiadosť nie je úplná, úrad vyzve žiadateľa na jej doplnenie v určenej lehote, ktorá nesmie byť kratšia ako desať dní. Ak žiadateľ žiadosť v stanovenej lehote nedoplní požadovaným spôsobom, úrad na žiadosť ďalej neprihliada.

Lehota na vydanie rozhodnutia vo veci akreditácie jednotky CSIRT

(V roli Žiadateľ o akreditáciu jednotky CSIRT)

Odsek 4, Paragraf 13, Článok I

Úrad o akreditácii rozhodne do 90 dní odo dňa doručenia úplnej žiadosti, a ak posúdi splnenie zhody jednotky CSIRT s podmienkami akreditácie jednotky CSIRT, vydá rozhodnutie o akreditácii. Rozhodnutie o akreditácii sa vydáva na dobu určitú, najviac na päť rokov.

Zaradenie jednotky CSIRT do zoznamu akreditovaných jednotiek CSIRT

(V roli Jednotka CSIRT)

Odsek 7, Paragraf 13, Článok I

Úrad jednotku CSIRT akreditovanú spôsobom podľa tohto zákona zaradí do zoznamu akreditovaných jednotiek CSIRT.

Povinnosti toho, kto plní úlohy jednotky CSIRT

Odsek 1, Paragraf 16, Článok I

Ten, kto plní úlohy jednotky CSIRT,
a) musí zabezpečiť, aby jednotka CSIRT v jeho pôsobnosti, ktorá je zaradená v zozname akreditovaných jednotiek CSIRT, nepretržite počas celej doby svojej prevádzky spĺňala podmienky akreditácie jednotky CSIRT podľa § 14 a zároveň plnila všetky úlohy podľa § 15,
b) oznamuje úradu všetky zmeny, ktoré majú vplyv na akreditáciu jednotky CSIRT bezodkladne po tom, ako nastali,
c) si vyžiada vyjadrenie Národnej banky Slovenska alebo Európskej centrálnej banky k postupu ústredného orgánu pri plnení úloh podľa tohto zákona, ak prevádzkovateľom základnej služby je dohliadaný subjekt finančného trhu, nad ktorým vykonáva dohľad Národná banka Slovenska podľa osobitných predpisov22) alebo nad ktorým vykonáva dohľad Európska centrálna banka podľa osobitného predpisu.

Postup konania v prípade, ak akreditovaná jednotka CSIRT prestane spĺňať podmienky podľa § 14 alebo ak neplní úlohy podľa § 15 tohto zákona

Odsek 2, Paragraf 16, Článok I

Ak akreditovaná jednotka CSIRT prestane spĺňať podmienky podľa § 14 alebo ak neplní úlohy podľa § 15, ten, kto plní úlohy jednotky CSIRT, to bezodkladne oznámi úradu; úrad na základe oznámenia podľa predchádzajúcej vety zruší rozhodnutie o akreditácii a jednotku CSIRT vyradí zo zoznamu akreditovaných jednotiek CSIRT.

Oznamovacia povinnosť v prípade prekročenia identifikačných kritérií prevádzkovanej služby podľa § 18 tohto zákona

Odsek 1, Paragraf 17, Článok I

Ak prevádzkovateľ služby v sektore podľa prílohy č. 1 zistí, že došlo k prekročeniu identifikačných kritérií prevádzkovanej služby podľa § 18, je povinný to oznámiť úradu do 30 dní odo dňa, keď prekročenie zistil.

Zaradenie základnej služby do zoznamu základných služieb podľa § 3 písm. k) prvého bodu tohto zákona

(V roli Prevádzkovateľ základnej služby)

Odsek 2, Paragraf 17, Článok I

Úrad zaradí základnú službu podľa § 3 písm. k) prvého bodu do zoznamu základných služieb a jej prevádzkovateľa do registra prevádzkovateľov základných služieb:
a) na základe oznámenia prevádzkovateľom tejto služby podľa odseku 1,
b) na základe podnetu ústredného orgánu, ak došlo k prekročeniu identifikačných kritérií prevádzkovanej služby podľa § 18,
c) z vlastnej iniciatívy, ak sa úrad dozvedel o prekročení identifikačných kritérií prevádzkovanej služby podľa § 18 a nedošlo k postupu podľa písmena a) alebo písmena b).

Zaradenie základnej služby do zoznamu základných služieb podľa § 3 písm. k) druhého bodu tohto zákona

(V roli Prevádzkovateľ základnej služby)

Odsek 3, Paragraf 17, Článok I

Úrad v spolupráci s príslušným ústredným orgánom zaradí základnú službu podľa § 3 písm. k) druhého bodu do zoznamu základných služieb a jej prevádzkovateľa do registra prevádzkovateľov základných služieb.

Zaradenie základnej služby podľa § 3 písm. k) tretieho bodu tohto zákona do zoznamu základných služieb

(V roli Prevádzkovateľ základnej služby)

Odsek 4, Paragraf 17, Článok I

Úrad zaradí základnú službu podľa § 3 písm. k) tretieho bodu do zoznamu základných služieb a jej prevádzkovateľa do registra prevádzkovateľov základných služieb zo zákona.

Oznámenie o zaradení služby do zoznamu základných služieb a do registra prevádzkovateľ základných služieb

(V roli Prevádzkovateľ základnej služby)

Odsek 6, Paragraf 17, Článok I

Zaradenie služby do zoznamu základných služieb a jej prevádzkovateľa do registra prevádzkovateľov základných služieb oznámi úrad prevádzkovateľovi tejto služby prostredníctvom informačného systému kybernetickej bezpečnosti.

Povinnosti prevádzkovateľa služby podľa prílohy č. 1 tohto zákona v prípade prekročenia špecifických sektorových kritérií

Odsek 4, Paragraf 18, Článok I

Ak prevádzkovateľ služby podľa prílohy č. 1 zistí, že došlo k prekročeniu špecifických sektorových kritérií, oznámi to úradu do 30 dní odo dňa, keď prekročenie zistil v rozsahu podľa § 17 ods. 5 aj v prípade, ak neprekročí dopadové kritériá.

Povinnosť prevádzkovateľa základnej služby informovať o zaradení do registra prevádzkovateľov základných služieb

(V roli Podnik na poskytovanie elektronických komunikačných služieb alebo sietí podľa osobitného predpisu)

Odsek 3, Paragraf 19, Článok I

Prevádzkovateľ základnej služby je povinný dňom zaradenia do registra prevádzkovateľov základných služieb o tejto skutočnosti informovať podnik na poskytovanie elektronických komunikačných služieb alebo sietí podľa osobitného predpisu, ku ktorému je sieť alebo informačný systém základnej služby pripojená. Na základe informovania podľa predchádzajúcej vety uzatvára prevádzkovateľ základnej služby s podnikom zmluvu podľa odseku 2.

Ďalšie povinnosti prevádzkovateľa základnej služby

Odsek 6, Paragraf 19, Článok I

Prevádzkovateľ základnej služby je ďalej povinný
a) riešiť kybernetický bezpečnostný incident,
b) bezodkladne hlásiť závažný kybernetický bezpečnostný incident,
c) spolupracovať s úradom a ústredným orgánom pri riešení hláseného kybernetického bezpečnostného incidentu a na tento účel im poskytnúť potrebnú súčinnosť, ako aj informácie získané z vlastnej činnosti dôležité pre riešenie kybernetického bezpečnostného incidentu,
d) v čase kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní,
e) oznámiť orgánu činnému v trestnom konaní alebo Policajnému zboru skutočnosti, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka, ak sa o ňom hodnoverným spôsobom dozvie.

Oznamovacia povinnosť poskytovateľa digitálnej služby

Odsek 1, Paragraf 21, Článok I

Poskytovateľ digitálnej služby je povinný do 30 dní odo dňa začatia poskytovania digitálnej služby oznámiť úradu
a) názov a sídlo,
b) kontaktné údaje,
c) poskytovanú službu,
d) názov, sídlo a kontaktné údaje zástupcu podľa § 23.

Zaradenie služby do zoznamu digitálnych služieb na základe oznámenia

(V roli Poskytovateľ digitálnej služby)

Odsek 2, Paragraf 21, Článok I

Na základe oznámenia podľa odseku 1 úrad zaradí službu do zoznamu digitálnych služieb a jej poskytovateľa do registra poskytovateľov digitálnych služieb.

Zaradenie služby do zoznamu digitálnych služieb na základe vlastného zistenia Národného bezpečnostného úradu

(V roli Poskytovateľ digitálnej služby)

Odsek 3, Paragraf 21, Článok I

Úrad zaradí službu do zoznamu digitálnych služieb a jej poskytovateľa do registra poskytovateľov digitálnych služieb aj na základe vlastného zistenia.

Oznámenie o zaradení služby do zoznamu digitálnych služieb

(V roli Poskytovateľ digitálnej služby)

Odsek 4, Paragraf 21, Článok I

Zaradenie služby do zoznamu digitálnych služieb a jej poskytovateľa do registra poskytovateľov digitálnych služieb oznámi úrad poskytovateľovi tejto služby.

Lehota na ohlásenie zmien v údajoch podľa § 21 odsek 1 tohto zákona

Odsek 5, Paragraf 21, Článok I

Poskytovateľ digitálnej služby je povinný hlásiť zmeny v údajoch podľa odseku 1 do 30 dní odo dňa ich vzniku.

Ďalšie povinnosti poskytovateľa digitálnej služby

Odsek 3, Paragraf 22, Článok I

Poskytovateľ digitálnej služby je povinný
a) hlásiť každý kybernetický bezpečnostný incident, ak disponuje informáciami, na základe ktorých je spôsobilý identifikovať, či má tento kybernetický bezpečnostný incident podstatný vplyv podľa osobitného predpisu, a to bezodkladne po jeho zistení,
b) riešiť hlásený kybernetický bezpečnostný incident,
c) spolupracovať s úradom pri riešení hláseného kybernetického bezpečnostného incidentu.

Povinnosť poskytovateľa digitálnej služby hlásiť každý závažný kybernetický bezpečnostný incident

(V roli Prevádzkovateľ základnej služby)

Odsek 3, Paragraf 24, Článok I

Ak prevádzkovateľ základnej služby využíva na poskytovanie základnej služby poskytovateľa digitálnej služby, je poskytovateľ digitálnej služby povinný hlásiť každý závažný kybernetický bezpečnostný incident, ktorý postihol poskytovateľa digitálnej služby.

Povinnosť poskytovateľa digitálnej služby hlásiť kybernetický bezpečnostný incident

Odsek 1, Paragraf 25, Článok I

Poskytovateľ digitálnej služby je povinný hlásiť kybernetický bezpečnostný incident podľa § 22 ods. 3 písm. a) spôsobom podľa § 24 ods. 4.

Oznamovacia povinnosť v súvislosti s vykonaním reaktívneho opatrenia

Odsek 6, Paragraf 27, Článok I

Prevádzkovateľ základnej služby alebo poskytovateľ digitálnej služby je povinný bezodkladne oznámiť a preukázať úradu prostredníctvom jednotného informačného systému kybernetickej bezpečnosti vykonanie reaktívneho opatrenia a jeho výsledok.

Povinnosť prevádzkovateľa základnej služby predložiť navrhované ochranné opatrenie na schválenie Národnému bezpečnostnému úradu

(V roli Ten, kto prevádzkuje jednotku CSIRT)

Odsek 8, Paragraf 27, Článok I

Prevádzkovateľ základnej služby je na výzvu úradu v určenej lehote povinný predložiť navrhované ochranné opatrenie na schválenie. Úrad rozhodnutím navrhované opatrenie schváli a určí lehotu na jeho vykonanie. V prípade, ak prevádzkovateľ základnej služby nenavrhne ochranné opatrenie v určenej lehote alebo ak je navrhované ochranné opatrenie zjavne neúspešné, je prevádzkovateľ základnej služby povinný spolupracovať s úradom, ústredným orgánom a s tým, kto prevádzkuje jednotku CSIRT, na jeho návrhu.

Povinnosť prevádzkovateľa základnej služby predložiť Národnému bezpečnostnému úradu správu o audite

Odsek 4, Paragraf 29, Článok I

Prevádzkovateľ základnej služby je povinný predložiť záverečnú správu o výsledkoch auditu úradu spolu s opatreniami na nápravu a s lehotami na ich odstránenie do 30 dní od ukončenia auditu.

Splnomocňovacie ustanovenia týkajúce sa jednotky CSIRT a kybernetickej bezpečnosti

(V roli Jednotka CSIRT)

Odsek 1, Paragraf 32, Článok I

Úrad ustanoví všeobecne záväzným právnym predpisom
a) podrobnosti o technickom, technologickom a personálnom vybavení jednotky CSIRT (§ 14 písm. a)),
b) identifikačné kritériá prevádzkovanej služby CSIRT (§ 18),
c) obsah bezpečnostných opatrení, obsah a štruktúru bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (§ 20 ods. 1 a 5),
d) bezpečnostné štandardy a znalostné štandardy v oblasti kybernetickej bezpečnosti (§ 5 ods. 1 písm. w), § 20 ods. 1),
e) identifikačné kritériá pre jednotlivé kategórie kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov (§ 24 ods. 1 a 4),
f) pravidlá a rozsah auditu kybernetickej bezpečnosti a podrobnosti o akreditácii orgánov posudzovania zhody a o obsahu záverečnej správy o výsledkoch auditu kybernetickej bezpečnosti podľa (§ 29 ods. 1 až 4).

Povinnosť podať oznámenie o prekročení kritérií podľa § 18 ods. 1 tohto zákona

Odsek 2, Paragraf 34, Článok I

Osoba existujúca ku dňu účinnosti tohto zákona je povinná odo dňa prekročenia identifikačných kritérií podľa § 18 ods. 1, najneskôr však do šiestich mesiacov odo dňa účinnosti tohto zákona, podať úradu oznámenie podľa § 18 ods. 1.

Povinnosť podať oznámenie pri začatí poskytovania digitálnej služby

Odsek 3, Paragraf 34, Článok I

Osoba existujúca ku dňu účinnosti tohto zákona je povinná do šiestich mesiacov odo dňa účinnosti tohto zákona oznámiť úradu informácie podľa § 21 ods. 1.

Doručenie zoznamu o prekročení identifikačných kritérií

Odsek 4, Paragraf 34, Článok I

Ústredný orgán je povinný do 30 dní odo dňa zistenia prekročenia identifikačných kritérií podľa § 18 ods. 1 prevádzkovateľom služby existujúcim ku dňu účinnosti tohto zákona, najneskôr však do šiestich mesiacov odo dňa účinnosti tohto zákona, doručiť úradu zoznam podľa § 9 ods. 1 písm. e).

Zaradenie do zoznamu služieb

(V roli Poskytovateľ digitálnej služby) (V roli Prevádzkovateľ základnej služby)

Odsek 5, Paragraf 34, Článok I

Úrad do 9. novembra 2018 zaradí službu do zoznamu základných služieb a jej prevádzkovateľa do registra prevádzkovateľov základných služieb, ak ešte nie sú zaradení; na digitálnu službu a jej poskytovateľa sa to vzťahuje rovnako.

Povinnosť prevádzkovateľa základnej služby podrobiť sa auditu kybernetickej bezpečnosti

Odsek 9, Paragraf 34, Článok I

Prevádzkovateľ základnej služby je povinný podrobiť sa auditu kybernetickej bezpečnosti a predložiť záverečnú správu o výsledkoch auditu úradu najneskôr do troch rokov od uplynutia lehoty podľa odseku 5.

Vymedzenia

Predmet zákona

(V roli Jednotka CSIRT) (V roli Orgán verejnej moci) (V roli Poskytovateľ digitálnej služby) (V roli Prevádzkovateľ základnej služby)

Paragraf 1, Článok I

Tento zákon upravuje
a) organizáciu, pôsobnosť a povinnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti,
b) národnú stratégiu kybernetickej bezpečnosti,
c) jednotný informačný systém kybernetickej bezpečnosti,
d) organizáciu a pôsobnosť jednotiek pre riešenie kybernetických bezpečnostných incidentov (ďalej len „jednotka CSIRT“) a ich akreditáciu,
e) postavenie a povinnosti prevádzkovateľa základnej služby a poskytovateľa digitálnej služby,

f) bezpečnostné opatrenia,
g) systém zabezpečenia kybernetickej bezpečnosti,
h) kontrolu nad dodržiavaním tohto zákona a audit.

Prevádzkovateľ základnej služby
(V roli Prevádzkovateľ základnej služby)
Článok I., Paragraf 3, písm. l)

Na účely tohto zákona sa rozumie:
l) prevádzkovateľom základnej služby orgán verejnej moci alebo osoba, ktorá prevádzkuje aspoň jednu službu podľa písmena k),

Poskytovateľ digitálnej služby
(V roli Poskytovateľ digitálnej služby)
Článok I., Paragraf 3, písm. n)

Na účely tohto zákona sa rozumie:
n) poskytovateľom digitálnej služby právnická osoba alebo fyzická osoba – podnikateľ, ktorá poskytuje digitálnu službu a zároveň zamestnáva aspoň 50 zamestnancov a má ročný obrat alebo celkovú ročnú bilanciu viac ako 10 000 000 eur,

Pôsobnosť orgánov verejnej moci

Paragraf 4, Článok I

Pôsobnosť v oblasti kybernetickej bezpečnosti vykonáva:
a) Národný bezpečnostný úrad (ďalej len „úrad“),
b) úrad, Ministerstvo dopravy a výstavby Slovenskej republiky, Ministerstvo financií Slovenskej republiky, Ministerstvo hospodárstva Slovenskej republiky, Ministerstvo obrany Slovenskej republiky, Ministerstvo vnútra Slovenskej republiky, Ministerstvo zdravotníctva Slovenskej republiky, Ministerstvo životného prostredia Slovenskej republiky, Slovenská informačná služba, Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky a Vojenské spravodajstvo (ďalej len „ústredný orgán“),
c) ministerstvá a ostatné ústredné orgány štátnej správy, ktoré nie sú ústredným orgánom, Generálna prokuratúra Slovenskej republiky, Najvyšší kontrolný úrad Slovenskej republiky, Úrad pre dohľad nad zdravotnou starostlivosťou, Úrad na ochranu osobných údajov Slovenskej republiky, Úrad pre reguláciu sieťových odvetví a iné štátne orgány v rozsahu svojej pôsobnosti (ďalej len „iný orgán štátnej správy“).

Centrálny systém včasného varovania
(V roli Orgán verejnej moci) (V roli Poskytovateľ digitálnej služby) (V roli Prevádzkovateľ základnej služby)
Odsek 4, Paragraf 8, Článok I

Centrálny systém včasného varovania je informačný systém, ktorý zaisťuje včasnú výmenu informácií o hrozbách, kybernetických bezpečnostných incidentoch a rizikách s nimi spojených medzi úradom a subjektmi podľa odseku 5.

Obligatórne náležitosti zmluvy o využívaní Akreditovanej jednotky CSIRT
(V roli Akreditovaná jednotka CSIRT)
Odsek 3, Paragraf 9, Článok I

Zmluva podľa odseku 2 musí obsahovať obdobie, počas ktorého sa akreditovaná jednotka CSIRT využíva, zoznam osôb v pôsobnosti ústredného orgánu, ktoré budú zodpovedné za poskytovanie údajov a informácií a ich rozsah, povinnosti o hlásení zmien ovplyvňujúcich riadne fungovanie akreditovanej jednotky CSIRT a vyčíslenie prevádzkových nákladov, ktoré je ústredný orgán povinný uhradiť.

Výnimka z povinnosti zachovávať mlčanlivosť
(V roli Poskytovateľ digitálnej služby) (V roli Prevádzkovateľ základnej služby)
Odsek 3, Paragraf 12, Článok I

Na účely konania pred orgánom verejnej moci, na účely trestného konania, oznamovania skutočnosti nasvedčujúcej tomu, že bol spáchaný trestný čin, alebo oznamovania kriminality alebo inej protispoločenskej činnosti sa povinnosť zachovávať mlčanlivosť podľa odseku 1 nevzťahuje na prevádzkovateľa základnej služby a poskytovateľa digitálnej služby a jeho zamestnancov.

Zástupca poskytovateľa digitálnej služby sídliaci na území Slovenskej republiky
(V roli Poskytovateľ digitálnej služby) (V roli Zástupca poskytovateľa digitálnej služby)
Odsek 1, Paragraf 23, Článok I

Zástupcom poskytovateľa digitálnej služby je právnická osoba, ktorá má sídlo v Slovenskej republike, alebo fyzická osoba – podnikateľ, ktorá má miesto podnikania v Slovenskej republike, ak odsek 2 neustanovuje inak, a ktorá je poskytovateľom digitálnej služby písomne poverená konať v jeho mene a na jeho zodpovednosť vo vzťahu k povinnostiam podľa tohto zákona.

Vylúčenie pôsobnosti správneho poriadku na konanie Národného bezpečnostného úradu podľa § 13 ods. 7, § 16 ods. 2 a 3, § 17 ods. 6, § 21 ods. 4 a § 27 tohto zákona

Odsek 1, Paragraf 33, Článok I

Na konanie úradu podľa § 13 ods. 7, § 16 ods. 2 a 3, § 17 ods. 6, § 21 ods. 4 a § 27 sa nevzťahuje správny poriadok.

Elektronický formulár hlásenia a jeho vzor

Odsek 2, Paragraf 33, Článok I

Informácie, údaje a hlásenia podľa tohto zákona sa predkladajú úradu v elektronickej podobe prostredníctvom elektronického formulára, ktorého vzor zverejní úrad prostredníctvom jednotného informačného systému kybernetickej bezpečnosti a na ústrednom portáli verejnej správy v module elektronických formulárov.

Zaraďovanie základnej a digitálnej služby do zoznamu základných služieb

(V roli Prevádzkovateľ základnej služby)

Odsek 3, Paragraf 33, Článok I

Ak služba spĺňa podmienky základnej služby a zároveň aj digitálnej služby, považuje sa za základnú službu a zaraďuje sa len do zoznamu základných služieb a jej prevádzkovateľ do registra prevádzkovateľov základných služieb.

Základná služba ktorá spadá do viacerých sektorov alebo podsektorov

Odsek 4, Paragraf 33, Článok I

Ak základná služba spadá do viacerých sektorov alebo podsektorov podľa prílohy č. 1, pôsobnosť podľa tohto zákona vykonáva ústredný orgán určený úradom.