Tézy
vykonávacích právnych predpisov

k návrhu zákona, ktorým sa mení a dopĺňa zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony

Podľa návrhu zákona, ktorým sa mení a dopĺňa zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony (ďalej len „návrh zákona“) sa na základe súčasného znenia § 31 písm. l) zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe predpokladá vydať štandardy podľa § 24 ods. 1 písm. k) a l):

1. k) štandard pre dizajnový manuál,
2. l) štandard pre kritériá prioritnej elektronickej služby a

taktiež sa návrhom zákona rozširuje splnomocňovacie ustanovenie § 31 písm. j) o rozsah údajov zasielaných orgánu vedenia a vládnej jednotke CSIRT podľa § 18 až 23a, ktoré znie:

3. „j) na úseku bezpečnosti informačných technológií verejnej správy
    1. podrobnosti o bezpečnosti informačných technológií verejnej správy,
    2. bezpečnostné opatrenia,
    3. rozsah a spôsob prijímania a realizácie bezpečnostných opatrení v závislosti od klasifikácie informácií a od kategorizácie sietí a informačných systémov,
    4. obsah a štruktúru bezpečnostného projektu,
    5. rozsah údajov zasielaných orgánu vedenia a vládnej jednotke CSIRT podľa § 18 až 23a,“.

Ad 1 – štandard pre dizajnový manuál

V oblasti štandardov je právny predpis už účinný, je ním vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu o štandardoch pre informačné technológie verejnej správy (ďalej len „vyhláška o štandardoch“). Štandard pre dizajn manuál sa navrhuje upraviť v samostatnom ustanovení vyhlášky o štandardoch vzhľadom na skutočnosť, že v aktuálnom platnom a účinnom znení je tento štandard upravený na viacerých miestach (§ 17 a § 35a a príloha č. 12 vyhlášky o štandardoch). Úprava tejto vyhlášky sa pripravuje s predpokladanou účinnosťou 1. augusta 2023 tak, ako je navrhovaná účinnosť návrhu zákona.

Ad 2 – štandard pre kritériá prioritnej elektronickej služby

V oblasti štandardov tak, ako je uvedené aj vyššie, je účinná vyhláška o štandardoch. Štandard pre kritéria prioritnej elektronickej služby má za cieľ definovať identifikačné kritériá (napríklad z hľadiska významu pre prostredie informačných technológií verejnej správy alebo početnosti využívania elektronickej služby občanom) na určenie prioritnej elektronickej služby pre orgán riadenia. Orgán riadenia podľa § 13a ods. 1 písm. c) návrhu zákona na základe týchto kritérií určuje prioritnú elektronickú službu. Cieľom priorizácie elektronických služieb je dosiahnutie lepších služieb pre občana z používateľského hľadiska. Úprava tejto vyhlášky sa pripravuje s predpokladanou účinnosťou 1. augusta 2023 tak, ako je navrhovaná účinnosť návrhu zákona.

Ad 3 – rozšírenie splnomocňovacieho ustanovenia § 31 písm. j) návrhu zákona

V oblasti bezpečnosti informačných technológií verejnej správy sa v nadväznosti na § 23 ods. 1 navrhuje upraviť účinný vykonávací právny predpis, ktorým je vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 z. z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy. Predpokladaný obsah nového vykonávacieho právneho predpisu, ktorým sa mení a dopĺňa vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z. je nasledovný:

Do § 2 sa vkladá nový odsek 5, ktorý znie:
„Systémové informácie z informačných technológií verejnej správy, ktoré sa zasielajú orgánu vedenia podľa § 23 ods. 3 písm. g) a § 23a ods. 4 písm. c) v spojení s § 23 ods. 4 písm. e) zákona [x)] v oblasti bezpečnosti informačných technológií verejnej správy sú upravené v prílohe č. 4.“

Poznámka pod čiarou:
x) návrh zákona č...., ktorým sa mení a dopĺňa zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony

Príloha č. 4
Systémové informácie z informačných technológií verejnej správy zasielané orgánu vedenia pre účely riadenia kybernetickej bezpečnosti.

(1) Základné údaje o správcovi:
názov správcu,
adresa správcu,
typ správcu.

(2) Kontaktné údaje na správcu:
Meno a priezvisko kontaktnej osoby,
e-mailový kontakt,
telefónny kontakt,
role osoby,
dostupnosť kontaktu (8x5, 24x7, ...).

(3) IPv4 adresy:
IPv4 adresa alebo rozsah IPv4 adries (adresa siete/dĺžka masky),
účel použitia danej adresy (adries).

(4) IPv6 adresy:
IPv6 adresa alebo rozsah IPv6 adries (prefix/dĺžka),
účel použitia danej adresy (adries).

(5) Doménové mená:
doménové meno,
priradená IPv4 adresa,
priradená IPv6 adresa,
účel použitia doménového mena.

(6) Sieťové služby:
názov služby,
doménové meno služby,
IPv4 a IPv6 adresa služby,

URL služby (pre služby na báze HTTP(S)),
čísla portov a transportné protokoly,
siete, z ktorých je služba prístupná (Internet, GOVNET, ...),
popis služby,
ID služby / príslušného informačného systému v MetaIS,
klasifikácia služby podľa dôvernosti, integrita a autentickosti, dostupnosti (číselníkové položky),
identifikácia, či je služba základnou službou podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti.

(7) Informácie o softvérovom vybavení správcu:
typ softvéru (operačný systém, aplikačný softvér, firmvér hardvéru, ... - číselníková položka),
názov softvéru,
verzia softvéru,
ID softvéru (podľa číselníka softvéru),
počet inštancií softvéru,
informácia, či je daný softvér použitý aj na systémoch prístupných z externých sietí,
informácia, či je daný softvér použitý aj na systémoch slúžiacich pre poskytovanie základnej služby.

(8) Informácie aktívach správcu:
ID aktíva
Názov aktíva
Typ aktíva
Popis aktíva
IP adresa
MAC adresa
Správca
Prevádzkovateľ

(9) Klasifikácia a kategorizácia informačných systémov správcu podľa tohto aj osobitného predpisu:1

(10) Parametre a výsledky realizácie:
analýzy rizík, alebo
analýza vplyvov na prevádzkovanie (business impact assessment „BIA“)

(11) Riziká definované podľa katalógu rizík vrátane previazania rizika na jednotlivé aktíva, spôsobov riadenia rizika aktuálneho stavu implementácie prijatých opatrení, termínov a zodpovedných osôb a pod. (komplexný manažment
ID rizika,
Názov rizika,
Popis rizika,
ID aktíva, ktorého sa riziko týka,
oblasť riadenia informačnej bezpečnosti, ktorej sa riziko týka,
dátum identifikovaného rizika
implementované opatrenia na zníženie alebo odstránenie rizika,
previazanie na politiky pokrývajúce jednotlivé riziká formou uvedenia alebo výberu názvu konkrétnej politiky alebo politík a ak je to možné odkazu na konkrétnu politiku,
hodnota reziduálneho rizika,
vlastník rizika,
plánované opatrenia na zníženie reziduálneho rizika,
termín realizácie plánovaných opatrení,
dátum poslednej aktualizácie.

(12) Evidenciu kybernetických bezpečnostných incidentov podľa osobitného predpisu:2)
dátum zistenia, aspoň predpokladaný dátum vzniku, časové údaje priebehu, dĺžke trvania,
geografické rozšírenie,
počet zasiahnutých používateľov,
stupeň narušenia
detailný opis priebehu,
rozsah vzniknutých škôd (aspoň odhad),
zasiahnuté služby, informačné systémy a informačné technológie verejnej správy,
konkrétny popis všetkých zasiahnutých aktív,
popis vplyvu na písm. d) a e),
stav riešenia,
vykonané nápravné opatrenia,
opis následkov
správa o riešení incidentu, a
prijaté bezpečnostné opatrenia
kybernetického bezpečnostného incidentu

(13) Odpovede na otázky v dotazníkoch:
identifikácia dotazníka,
identifikácia otázky,
kód odpovede,
hodnota odpovede.