Pripomienky k Tézam

Daniel Olejár

Tézy
vykonávacích právnych predpisov
k návrhu zákona o kybernetickej bezpečnosti
a o zmene a doplnení niektorých zákonov

Vykonávací predpis podľa podľa § 32 ods. 1 písm. a), ktorým sa ustanovujú podrobnosti o technickom, technologickom a personálnom vybavení jednotky CSIRT [§ 14 písm. a)]

Cieľom tohto vykonávacieho predpisu je stanoviť podrobnosti o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov a podmienky je akreditácie v zmysle požiadaviek a procesu preukazovania zhody podľa zákona.

Požiadavky na technické, technologické a personálne vybavenie jednotky CSIRT sa delia na:

a) Všeobecné požiadavky

Jednotka CSIRT v procese akreditácie preukazuje splnenie všeobecných požiadaviek na akreditáciu jednotky CSIRT, a to najmä:

- Oblastná pôsobnosť,
- Vecná pôsobnosť,
- Zakladateľské dokumenty,
- Vymedzenie poskytovaných služieb,
- Model financovania,
- Jednotka CSIRT ako organizačná jednotka,
- Vnútorná organizácia jednotky CSIRT.

- toto všetko by mal obsahovať štatút a organizačný poriadok CSIRT

b) Bezpečnostná politika

Jednotka CSIRT v procese akreditácie preukazuje existencie bezpečnostných politík na akreditáciu jednotky CSIRT, a to najmä:

- Politika klasifikácie informácií,
- Politika ochrany informácií,
- Politika uchovávania informácií,
- Politika likvidácie informácií,
- Politika šírenia informácií,
- Politika prístupu k informáciám,
- Politika správania sa v rámci sietí a informačných systémov jednotky CSIRT,
- Politika kybernetických bezpečnostných udalostí a kybernetických bezpečnostných incidentov,

- Politika riadenia kybernetických bezpečnostných incidentov,
- Politika pre spoluprácu a výmenu informácií.

- v podstate by stačilo, aby CSIRT mala zavedený ISMS podľa ISO/IEC 27001 a 2
- aký je rozdiel medzi Politikou kybernetických bezpečnostných udalostí a kybernetických bezpečnostných incidentov a Politikou riadenia kybernetických bezpečnostných incidentov?
- požiadavky na akreditáciu sú slabšie ako požiadavky na ISVS

c) Pracovisko a pracovné prostredie

Jednotka CSIRT v procese akreditácie preukazuje splnenie požiadaviek na pracovisko a pracovné prostredie jednotky CSIRT z dôvodu jej akreditácie, a to najmä:

- Fyzická a objektová bezpečnosť,
- Technické zabezpečenie a vybavenie,
- Úložisko,
- Vznik, založenie a sledovanie kybernetického bezpečnostného incidentu,
- Sieťová infraštruktúra,
- Šifrovacie prostriedky.

- spracovanie bezpečnostného incidentu je proces, ktorý do tohto bodu nepatrí (napokon, je v bodoch d a e)

d) Riadenie kybernetických bezpečnostných incidentov

Jednotka CSIRT má zavedený funkčný proces nahlasovania kybernetických bezpečnostných incidentov za účelom ich riadenia. Zriaďovateľ jednotky CSIRT, ako aj ostatné subjekty, ktorým jednotka CSIRT poskytuje služby, majú možnosť prostredníctvom systému nahlasovania kybernetického bezpečnostného incidentu nahlasovať kybernetické bezpečnostné incidenty a ďalšie relevantné informácie a skutočnosti a prijímať pokyny, otázky, spätnú väzbu a poradenstvo. Pokyny jednotky CSIRT týkajúce sa nahlasovania kybernetických bezpečnostných incidentov obsahujú najmä:

- Definícia a vymedzenie kybernetického bezpečnostného incidentu.
- Dôvody na nahlásenie kybernetického bezpečnostného incidentu.
- Označenie miesta, času a adresáta oznámenia o kybernetickom bezpečnostnom incidente.
- Určenie spôsobov nahlásenia kybernetického bezpečnostného incidentu.
- Stanovenie rozsahu hlásenia o kybernetickom bezpečnostnom incidente vymedzením jeho formálnych a obsahových náležitostí.

e) Reakcia na kybernetický bezpečnostný incident

Jednotka CSIRT má zadefinovaný proces reakcie na kybernetické bezpečnostné incidenty sprístupnený na oficiálnej webovej stránke jednotky CSIRT. Uvedené zahŕňa najmä spôsoby, akým je kybernetický bezpečnostný incident:

- prideľovaný,
- analyzovaný,
- eskalovaný,
- uzavretý,
- vyhodnotený na účely best practises.

f) Kontaktné informácie a ich dostupnosť

Jednotka CSIRT má zabezpečenú distribúciu svojich kontaktných informácií, a to ako internými procesmi v prospech zriaďovateľa, tak aj voči tretím stranám navonok takým spôsobom, aby bola zabezpečená nepretržitá dostupnosť kontaktných informácií o jednotke CSIRT a možnostiach jej kontaktovania. Jednotka CSIRT má na tieto účely zriadené verejne dostupné webové sídlo (portál), ktorý používateľom poskytuje aktuálne informácie ohľadom jednotky CSIRT (RFC 2350) v slovenskej a anglickej verzii, pravidelne aktualizované informácie z okruhov, súhrnné prehľady informácií z diskusných fór a iných informačných zdrojov z oblasti kybernetickej bezpečnosti s dôrazom na šírenie povedomia o kybernetickej bezpečnosti, prevenciu a riešenie kybernetických bezpečnostných incidentov.

g) Plán profesionálneho rozvoja

Jednotka CSIRT sa prostredníctvom svojich príslušníkov pravidelne zúčastňuje konferencií, školení, seminárov a ďalších vzdelávacích aktivít so zameraním na problematiku jednotiek CSIRT (napr. riadenie kybernetických bezpečnostných incidentov) tak, aby každý príslušník jednotky CSIRT preukázateľne absolvoval minimálne jednu takúto aktivitu ročne.

Vykonávací predpis podľa podľa § 32 ods. 1 písm. b), ktorým sa ustanovujú identifikačné kritériá prevádzkovanej služby CSIRT [§ 18]

Cieľom tohto vykonávacieho predpisu je stanoviť podrobnosti identifikačné kritériá a postup určovania prevádzkovateľa základnej služby.

Identifikačné kritériá základnej služby

(1) Prevádzkovateľ služby v sektore podľa osobitného predpisu[1]) posudzuje zhodu poskytovanej služby s identifikačnými kritériami základnej služby podľa ods. 2.

(2) Identifikačné kritéria poskytovanej služby na posúdenie zhody a identifikáciu prevádzkovateľov základných služieb sa delia na:

a) dopadové kritéria,
b) špecifické sektorové kritéria,

Prevádzkovateľ služby v sektore

(1) Prevádzkovateľ služby v sektore sa rozumie ten, kto spĺňa sektorové kritériá podľa ktorých sa posudzuje, či je tento prevádzkovateľom služby v sektore.

[1]) Príloha č. 1 zákona č. xx/2017 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

(2) Sektorové kritériá sú určené druhom služby a prevádzkovateľom služby.

Dopadové kritéria

Dopadovými kritériami sa rozumejú možné dôsledky kybernetického bezpečnostného incidentu v sieti alebo informačnom systéme a vymedzujú významnosť dopadu narušenia základnej služby na zabezpečenie spoločenských alebo ekonomických činností.

Špecifické sektorové kritériá

Špecifické sektorové kritériá sú naplnené, pokiaľ prevádzkovateľ služby spĺňa spolu s dopadovými kritériami zároveň aspoň jedno špecifické kritérium, ak je určené.

Ako prevádzkovateľ základnej služby bude určený ten, kto súčasne spĺňa sektorové kritériá, dopadové kritériá a špecifické sektorové kritériá, ak sú určené.

Vykonávacím predpisom sa nebudú žiadnym subjektom ukladať práva, povinnosti ani kompetencie.

Vykonávací predpis podľa podľa § 32 ods. 1 písm. c), ktorým sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúru bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení [§ 20 ods. 1 a 5]

Cieľom tohto vykonávacieho predpisu je stanoviť obsah a rozsah bezpečnostných opatrení nevyhnutných na zabezpečenie kybernetickej bezpečnosti, dostupnosti a spoľahlivosti základných služieb v kybernetickom priestore prostredníctvom primeraného zabezpečenia sietí a informačných systémov pred ich zneužitím, zničením, poškodením, odcudzením, neoprávneným prístupom, zmenou alebo pred stratou. Týmto vykonávacím predpisom sa ustanoví:

a) obsah a rozsah bezpečnostných opatrení prevádzkovateľa základnej služby,
b) obsah a štruktúra bezpečnostnej dokumentácie prevádzkovateľa základnej služby,
c) rozsah všeobecných bezpečnostných opatrení

Rozsah všeobecných bezpečnostných opatrení

Všeobecné bezpečnostné opatrenia sa týkajú celej organizácie, t. j. sú to spoločné opatrenia pre všetky informačné systémy prevádzkovateľa základnej služby

Fyzická bezpečnosť

a) informačné systémy sú umiestnené v priestoroch, ktoré im poskytujú dostatočnú ochranu pred vplyvmi prostredia,
b) informačné systémy sú chránené pred fyzickým prístupom nepovolaných osôb,
c) technologická podporná infraštruktúra je chránená pred zásahom nepovolaných osôb,
d) sieťová kabeláž je chránená pred zásahom nepovolaných osôb,
e) protipožiarna ochrana,

f) uzamykanie a kontrola technických vstupov do objektov,
g) opravy a vyraďovanie zariadení sa musia robiť takým spôsobom, aby nedochádzalo k úniku informácií alebo porušovaniu licenčných práv *(metodiku).*

Organizačná bezpečnosť

a) každý prevádzkovateľ základnej služby a poskytovateľ digitálnej služby má osobu poverenú funkciou manažéra kybernetickej bezpečnosti organizácie; organizácia môže mať aj viacero manažérov kybernetickej bezpečnosti,
b) bezpečnostná politika organizácie je prerokovaná a schválená vedením *(vzorová BP a k nej metodika),*
   1. informačné systémy sa môžu používať len na plnenie pracovných povinností,
   2. čo nie je povolené, je zakázané,
   3. okrem systémov, aplikácií s anonymným prístupom, zodpovednosť za činnosť v systéme,
c) pre jednotlivých pracovníkov/príslušníkov sú explicitne stanovené povinnosti v kybernetickej bezpečnosti uvedené aj v pracovnej náplni,
d) popísané postupy pri riešení kybernetických bezpečnostných incidentov,
e) popísané postupy pri haváriách,
f) pravidelné hodnotenie stavu kybernetickej bezpečnosti v organizácii (bezpečnostný manažér, nezávislý audítor - vedenie organizácie).

Personálna bezpečnosť

a) úvodné školenie: základné povinnosti pracovníka pri práci s informačnými systémami organizácie,
b) preškolenia zamestnancov,
c) identifikovať činnosti s vymedzením ich kumulácie s ohľadom na konflikt záujmov,
d) pravidlá pre zmenu pracovného zaradenia,
e) pravidlá pri ukončení pracovného pomeru, funkčného zaradenia,
f) poučenie a zmluva s externým pracovníkom vrátane vyhlásenia o mlčanlivosti.

Bezpečnosť informačných systémov

a) pre každý informačný systém, vrátane jeho programového vybavenia, vedie organizácia jeho technickú dokumentáciu,
b) pre každú časť programového vybavenia, ktoré organizácia obstarala, uchováva organizácia originálne pamäťové médiá,
c) ak si organizácia spravuje informačné systémy sama, tak sa nasledujúce opatrenia vzťahujú na jej zamestnancov; ak správu informačných systémov uskutočňuje externý dodávateľ, organizácia zabezpečí, aby uvedené zásady/opatrenia presadzovali ako externí, tak aj interní pracovníci,
d) každý informačný systém (HW, SW, OS, DB, AP) má explicitne stanoveného správcu informačného systému, ktorým môže byť len kvalifikovaná osoba vlastníka informačného systému (zamestnanca organizácie),
e) pre každý informačný systém je stanovená a zdokumentovaná jeho HW a SW konfigurácia, ktorú môže meniť len správca informačného systému (databázy, aplikácie),
f) v informačnom systéme je inštalovaný a používaný len legálny softvér,
g) správca informačného systému aktualizuje operačný systém bezodkladne po vydaní záplat,

h) záplaty, aktualizácie a nový softvér správca informačného systému inštaluje len z originálnych nosičov, alebo overených stránok dodávateľa (pred inštaláciou vykoná kontrolu autentickosti SW),
i) organizácia pravidelne zálohuje údaje a médiá so zálohovanými údajmi, ktoré uchováva mimo priestorov, v rámci ktorých sú umiestnené informačné systémy organizácie a tieto chráni v súlade s bezpečnostnou klasifikáciou a bezpečnostnými požiadavkami na zálohované údaje,
j) organizácia zabezpečí systém vyhotovenia upozornení o pokus o prístup na interné schránky organizácie už pri prihlasovaní,
k) organizácia zabezpečí implementáciu antivírových riešení na:
   1. mailovom serveri,
   2. pracovných staniciach,
   spolu s automatizovanou aktualizáciou databáz,
l) organizácia zabezpečí, že vzdialený prístup do informačného systému je:
   1. povolený len v odôvodnených prípadoch,
   2. zavedená silná identifikácia a autentizácia,
m) používateľ nemá v informačnom systéme správcovské právomoci, t.j. nemôže meniť konfiguráciu systému, inštalovať nové programy a iné,
n) používateľ sa pred začiatkom práce s informačným systémom úspešne identifikovať a autentizovať,
o) používateľ
   1. chráni svoje autentizačné prostriedky pred neoprávneným prístupom a manipuláciou a tieto pravidelne mení
   2. vyberá dostatočne silné heslá,
p) organizácia zabezpečí poučenie používateľov v rozsahu najmä:
   1. o prístupe k aktívnym prílohám elektronickej pošty,
   2. o prístupe na neznáme stránky,
   3. o zákaze sťahovania pochybného a neovereného obsahu,
   4. o spame a možnostiach jeho šírenia,
   5. o vytváraní kópie údajov a iné,
q) nepoužívať vlastné pamäťové médiá a zariadenia (USB, CD, notebook, tablet, mobil,...) na záznam a spracovanie údajov organizácie.

Všeobecné požiadavky na kybernetickú bezpečnosť informačných systémov pri ich vytváraní, implementácii, prevádzke a vyraďovaní

a) Všeobecné bezpečnostné požiadavky na informačný systém sú
- Organizácia zaistenia informačnej a kybernetickej bezpečnosti a zásady bezpečného vytvárania, implementácie, prevádzky, vyraďovania a zálohovania.
- Limity a podmienky bezpečnej prevádzky alebo bezpečného vyraďovania.
- Zásady bezpečného vyraďovania.
- Dokumentovanie vykonávaných činností a zmien.
- Ochrana proti požiarom.
- Požiadavky na nakladanie s informáciami.
- Prevádzkové predpisy.
- Požiadavky na pravidelnú údržbu, kontrolu, audit a skúšky.
- Vedenie záznamov a prevádzkovej dokumentácie.
- Zabezpečenie pravidelnej údržby, kontroly, auditov a skúšok.

b) Opatrenia na zaistenie dôvernosti

c) Opatrenia pre zaistenie dostupnosti

d) Opatrenia pre zaistenie integrity

Vykonávacím predpisom sa nebudú žiadnym subjektom ukladať práva, povinnosti ani kompetencie.

Vykonávací predpis podľa podľa § 32 ods. 1 písm. d), ktorým sa ustanovujú bezpečnostné štandardy a znalostné štandardy v oblasti kybernetickej bezpečnosti [§ 5 ods. 1 písm. w), § 20 ods. 1]

Cieľom tohto vykonávacieho predpisu je stanovenie bezpečnostných štandardov v oblasti kybernetickej bezpečnosti, ktorých cieľom je dosiahnuť adekvátnu úroveň bezpečnosti pre všetky typy sietí a informačných systémov v organizácii. Prostredníctvom aplikácie technických, organizačných a personálnych opatrení je možné dosiahnuť úroveň bezpečnosti, ktorá je organizáciou požadovaná a vhodná na ich zabezpečenie. Tieto štandardy obsahujú odporúčania ohľadom metód, procesov, postupov a opatrení, ktoré súvisia s informačnou bezpečnosťou a je možné ich použiť pri implementácii bezpečnosti a prispôsobiť ich podľa potreby.

Úrad v spolupráci s ústredným orgánov vypracuje minimálne bezpečnostné požiadavky vo forme mapovacích štandardov pre oblasť informačnej bezpečnosti v rámci jednotlivých sektorov, ktoré:

- definujú všeobecné požiadavky na systém riadenia informačnej bezpečnosti (ISMS) v súlade so štandardom ISO 27002 s prihliadnutím na odporúčania ďalších štandardov z tejto rodiny.
- popíšu spôsob ako vytvoriť, implementovať a prevádzkovať ISMS v praxi. Poskytne detailný návod ako iniciovať proces bezpečnosti, zostaviť bezpečnostný koncept, implementovať ho, udržiavať ho funkčným a neustále ho zlepšovať. Tento štandard

poskytne rozsiahle, detailné a prístupné návody na splnenie požiadaviek na ISMS spolu s mnohými poznámkami a príkladmi.
- zabezpečia vysoké bezpečnostné požiadavky na niektoré informačné systémy alebo prevádzka dôležitých komponentov.
- sú zamerané na vývoj, zavedenie a udržiavanie systému pre riadenie kontinuity činností, ktorého cieľom je zaistiť, aby dôležité procesy neboli prerušené, resp. aby boli prerušené len na krátky čas a to aj v kritických situáciách.

Návrh sa odvoláva na normy, ktoré boli zrušené. Zo 42 noriem je neplatných 26. Ďalšie relevantné normy boli rozšírené a tieto v zozname chýbajú. Tvorcovia zoznamu zrejme opisovali zo starého prehľadového materiálu. Zoznam noriem s vyznačením neplatných je uvedený v materiáli PrehladNoriemISO

Mapovací štandard bude vychádzať s noriem rady 27000, ktoré predstavujú medzinárodné štandardy v oblasti riadenia informačnej bezpečnosti:

ISO/IEC 27000:2014
Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
ISO/IEC 27000:2014 poskytuje prehľad systémov manažárstva informačnej bezpečnosti (SMIB) a termíny a definície bežne používané v štandardoch radu 27000. Je aplikovateľný na všetky typy a veľkosti organizácií (vládne, komerčné, neziskové).

ISO/IEC 27000:2016

ISO/IEC 27001:2013
Information technology -- Security techniques -- Information security management systems – Requirements
ISO/IEC 27001:2013 špecifikuje požiadavky na vytvorenie, implementáciu, udržiavanie a zlepšovanie SMIB v kontexte organizácie. Tiež obsahuje požiadavky na posudzovanie a narábanie s rizikami informačnej bezpečnosti. Požiadavky tejto normy sú generické a aplikovateľné na všetky organizácie nezávisle na ich type, veľkosti a charaktere.

ISO/IEC 27001:2013/Cor 2:2015

ISO/IEC 27002:2013
Information technology -- Security techniques -- Code of practice for information security controls
ISO/IEC 27002:2013 poskytuje pokyny pre štandardy informačnej bezpečnosti organizácie a praktiky riadenia informačnej bezpečnosti vrátane výberu, implementácie a riadenie opatrení berúc do úvahy rizikové prostredia informačnej bezpečnosti organizácie. Je navrhnutý pre organizácie, ktoré zamýšľajú:
- výber opatrení v rámci procesu implementácie SMIB založeného na ISO/IEC 27001,
- implementáciu všeobecne akceptovaných opatrení informačnej bezpečnosti,

- vývoj vlastných smerníc pre informačnú bezpečnosť.

SO/IEC 27002:2013/Cor 2:2015

ISO/IEC 27003:2010
Information technology -- Security techniques -- Information security management system implementation guidance
ISO/IEC 27003:2010 sa zameriava na kritické aspekty úspešného návrhu a implementácie SMIB v súlade s ISO/IEC 27001:2005. Popisuje proces špecifikácie a návrhu SMIB od počiatku až po vytvorenie plánu implementácie.

ISO/IEC 27003:2017

ISO/IEC 27004:2009
Information technology -- Security techniques -- Information security management – Measurement
ISO/IEC 27004:2009 poskytuje návod pre vývoj a používanie metrík a merania pre posúdenie efektivity implementovaného SMIB a opatrení špecifikovaných v ISO/IEC 27001.

ISO/IEC 27004:2016

ISO/IEC 27005:2011
Information technology -- Security techniques -- Information security risk management
ISO/IEC 27005:2011 poskytuje návod pre riadenie rizík informačnej bezpečnosti. Podporuje všeobecné koncepty špecifikované v ISO/IEC 27001 a je navrhnutý tak, aby podporoval implementáciu informačnej bezpečnosti založenej na riadení rizík.

ISO/IEC 27006:2011
Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27006:2011 špecifikuje požiadavky a poskytuje návod pre organizácie poskytujúce audit a certifikácie SMIB. Štandard je primárne zameraný na podporu akreditácie organizácií poskytujúcich certifikáciu SMIB.

ISO/IEC 27006:2015

ISO/IEC 27007:2011
Information technology -- Security techniques -- Guidelines for information security management systems auditing
ISO/IEC 27007:2011 poskytuje návod a požiadavky pre riadenie programu auditov SMIB, vykonávanie auditov a kompetencie audítorov SMIB.

ISO/IEC 27007:2017

ISO/IEC TR 27008:2011
Information technology -- Security techniques -- Guidelines for auditors on information security controls
ISO/IEC TR 27008:2011 poskytuje návod na preskúmavanie implementácie a prevádzky opatrení, vrátane technického súladu opatrení informačnej bezpečnosti.

ISO/IEC 27010:2012
Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications
ISO/IEC 27010:2012 poskytuje návod pre implementáciu riadenia informačnej bezpečnosti v rámci organizácií zdieľajúcich informácie. Je aplikovateľný na všetky formy výmeny a zdieľania citlivých informácií (verejné, súkromné, národné, medzinárodné, v rámci odvetvia, alebo medzi jednotlivými sektormi).

ISO/IEC 27010:2015

ISO/IEC 27011:2008
Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
Cieľom tohto návodu je podporiť implementáciu riadenia informačnej bezpečnosti v telekomunikačných organizáciach. Prijatie tohto štandardu umožní telekomunikačným organizáciam splniť základné požiadavky na dostupnosť, dôvernosť a integritu.

ISO/IEC 27011:2016

ISO/IEC 27013:2012
Information technology -- Security techniques -- Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
ISO/IEC 27013:2012 poskytuje návod pre integrovanú implementáciu ISO 27001 a ISO 20000-1 pre organizácie, ktoré zamýšľajú:
- implementovať ISO 27001 po predchádzajúcej implementácií ISO 20000-1 alebo opačne,
- implementovať súčasne ISO 27001 a ISO 20000-1,
- integrovať existujúce ISO 27001 a ISO 20000-1 manažérske systémy.

ISO/IEC 27013:2015

ISO/IEC 27014:2013
Information technology -- Security techniques -- Governance of information security

ISO/IEC 27014:2013 poskytuje koncepty a princípy strategického riadenia informačnej bezpečnosti (Governance) pomocou ktorých môžu organizácie vyhodnocovať, koordinovať, monitorovať a komunikovať aktivity súvisiace s informačnou bezpečnosťou.

ISO/IEC TR 27015:2012
Information technology -- Security techniques -- Information security management guidelines for financial services
ISO/IEC TR 27015:2012 poskytuje návod pre spustenie, implementáciu, udržiavanie a zlepšovanie informačnej bezpečnosti a opatrení z ISO/IEC 27002 pre organizácie poskytujúce finančné služby.

ISO/IEC TR 27016:2014
Information technology -- Security techniques -- Information security management -- Organizational economics
ISO/IEC TR 27016:2014 poskytuje návod pre organizácie pre tvorbu rozhodnutí o ochrane informácií a pochopenie ekonomických dôsledkov týchto rozhodnutí v kontexte konkurenčných požiadaviek na zdroje.

ISO/IEC CD 27017
Information technology -- Security techniques -- Code of practice for information security controls for cloud computing services based on ISO/IEC 27002

ISO/IEC 27017:2015

ISO/IEC 27018:2014
Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO/IEC 27018:2014 ustanovuje všeobecne prijaté ciele riadenia, opatrenia a návod pre implementáciu opatrení na ochranu osobných údajov (Personally Identifiable Information) v súlade s princípmi ochrany súkromia v ISO/IEC 29100 pre verejné cloudy.

ISO/IEC TR 27019:2013
Information technology -- Security techniques -- Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry
ISO/IEC TR 27019:2013 poskytuje návod založený na ISO/IEC 27002 na aplikáciu riadenia informačnej bezpečnosti na riadiace a kontrolné systémy používané v energetickom priemysle.

ISO/IEC DTR 27023
Security techniques -- Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002

ISO/IEC TR 27023:2015

ISO/IEC 27031:2011
Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity
ISO/IEC 27031:2011 popisuje koncepty a princípy pripravenosti IKT na kontinuitu činností a poskytuje rámec metód a procesov pre identifikáciu a špecifikáciu všetkých aspektov (kritérií výkonnosti, návrhu a implementácie) pre zlepšovanie pripravenosti IKT organizácie na zaistenie kontinuity činností.

ISO/IEC 27032:2012
Information technology -- Security techniques -- Guidelines for cybersecurity
ISO/IEC 27032:2012 poskytuje návod pre zlepšovanie stavu kybernetickej bezpečnosti popisujúc špecifické aspekty tejto aktivity a jej závislosti na ostatných oblastiach bezpečnosti, ako napr.:
- informačná bezpečnosť,
- sieťová bezpečnosť,
- bezpečnosť internetu,
- ochrana kritickej informačnej infraštruktúry (CIIP).

ISO/IEC 27033-1:2009
Information technology -- Security techniques -- Network security -- Part 1: Overview and concepts
ISO/IEC 27033-1:2009 poskytuje prehľad sieťovej bezpečnosti a súvisiacich definícií.

ISO/IEC 27033-1:2015

ISO/IEC 27033-2:2012
Information technology -- Security techniques -- Network security -- Part 2: Guidelines for the design and implementation of network security
ISO/IEC 27033-2:2012 poskytuje návod pre plánovanie, návrh, implementáciu a dokumentovanie sieťovej bezpečnosti v organizácii.

ISO/IEC 27033-2:2012

ISO/IEC 27033-3:2010
Information technology -- Security techniques -- Network security -- Part 3: Reference networking scenarios -- Threats, design techniques and control issues
ISO/IEC 27033-3:2010 popisuje hrozby, techniky návrhu a problémy súvisiace s opatreniami súvisiacimi s referenčnými sieťovými scenármi. Pre každý scenár poskytuje detailný návod pre narábanie s bezpečnostnými hrozbami, technikami návrhu opatrení a opatreniami na minimalizáciu súvisiacich rizík.

ISO/IEC 27033-4:2014
Information technology -- Security techniques -- Network security -- Part 4: Securing communications between networks using security gateways

ISO/IEC 27033-4:2014 poskytuje bávod pre zabezpečenie komunikácie medzi sieťami použitím bezpečnostných brán (firewall, aplikačný firewall, IPS) v súlade s dokumentovanou politikou informačnej bezpečnosti.

ISO/IEC 27033-5:2013
Information technology -- Security techniques -- Network security -- Part 5: Securing communications across networks using Virtual Private Networks (VPNs)
ISO/IEC 27033-5:2013 poskytuje návod pre výber, implementáciu a monitorovanie technických opatrení potrebných na zaistenie sieťovej bezpečnosti využitím pripojení virtuálnej súkromnej siete (VPN) na prepojenie sietí a pripojenie vzdialených používateľov do týchto sietí.

chýba

ISO/IEC 27033-6:2016

Information technology -- Security techniques -- Network security -- Part 6: Securing wireless IP network access

ISO/IEC 27033-6:2016 describes the threats, security requirements, security control and design techniques associated with wireless networks. It provides guidelines for the selection, implementation and monitoring of the technical controls necessary to provide secure communications using wireless networks. The information in this part of ISO/IEC 27033 is intended to be used when reviewing or selecting technical security architecture/design options that involve the use of wireless network in accordance with ISO/IEC 27033-2.

ISO/IEC 27034-1:2011
Information technology -- Security techniques -- Application security -- Part 1: Overview and concepts
ISO/IEC 27034 poskytuje organizáciám pomoc pri integrovaní bezpečnosti do procesov na riadenie aplikácií. Poskytuje prehľad aplikačnej bezpečnosti, oboznamuje s definíciami, konceptmi, princípmi a procesmi súvisiacimi s aplikačnou bezpečnosťou.

ISO/IEC 27034-1:2011/Cor 1:2014

norma má ďalších 5 častí

ISO/IEC 27035:2011
Information technology -- Security techniques -- Information security incident management
ISO/IEC 27035:2011 poskytuje štruktúrovaný a plánovitý prístup k:
- detekcii, nahlasovaniu a posudzovaniu incidentov informačnej bezpečnosti,
- reakcii a riadeniu incidentov informačnej bezpečnosti,
- detekcii, posudzovaniu a riadeniu zraniteľností informačnej bezpečnosti,
- neustálemu zlepšovaniu informačnej bezpečnosti a správy incidentov ako výsledku riadenia incidentov a zraniteľností informačnej bezpečnosti.

ISO/IEC 27035-1:2016

ISO/IEC 27035-1:2016
Information technology -- Security techniques -- Information security incident management -- Part 1: Principles of incident management

ISO/IEC 27035-2:2016
Information technology -- Security techniques -- Information security incident management -- Part 2: Guidelines to plan and prepare for incident response

ISO/IEC 27036-1:2014
Information technology -- Security techniques -- Information security for supplier relationships -- Part 1: Overview and concepts
ISO/IEC 27036-1:2014 poskytuje pomoc organizáciam pri zabezpečení ich informácií a informačných systémov v kontexte vzťahov s dodávateľmi.

ISO/IEC 27036-2:2014
Information technology -- Security techniques -- Information security for supplier relationships -- Part 2: Requirements
ISO/IEC 27036-2:2014 špecifikuje základné požiadavky informačnej bezpečnosti na definovanie, implementovanie, prevádzku, monitorovanie, preskúmavanie, udržiavanie a zlepšovanie vzťahov s dodávateľmi a nadobúdateľmi.

ISO/IEC 27036-3:2013
Information technology -- Security techniques -- Information security for supplier relationships -- Part 3: Guidelines for information and communication technology supply chain security
ISO/IEC 27036-3:2013 poskytuje návod pre dodávateľov a nadobúdateľov prostriedkov IKT na:
- získanie prehľadu a riadenie rizík informačnej bezpečnosti spôsobených fyzicky rozptýlenými a mnoho vrstvovými dodávateľkými reťazcami,
- reakciu na riziká vyplývajúce z globálneho dodávateľského reťazca prostriedkov IKT , ktoré môžu mať dopad na organizácie používajúcie tieto prostriedky IKT,
- integráciu procesov informačnej bezpečnosti do životného cyklu informačných systémov a softvéru.

ISO/IEC WD 27036-4
Information technology -- Information security for supplier relationships -- Part 4: Guidelines for security of Cloud services
V príprave.

ISO/IEC 27036-4:2016

ISO/IEC 27037:2012
Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence

ISO/IEC 27037:2012 poskytuje návod pre špecifické aktivity pri narábaní s digitálnymi dôkazmi, ktorými sú identifikácia, zber, získanie a uchovávanie potenciálnych digitálnych dôkazov, ktoré môžu mať dôkaznú hodnotu.

ISO/IEC 27038:2014
Information technology -- Security techniques -- Specification for digital redaction
ISO/IEC 27038:2014 špecifikuje techniky vykonávania digitálnej redakcie elektronických dokumentov. Tiež špecifikuje požiadavky na softvérové nástroje používané pri odstraňovaní citlivých informácií zo zverejňovaných elektronických dokumentov a metódy testovania bezpečného odstraňovania týchto informácií.

ISO/IEC FDIS 27039
Information technology -- Security techniques -- Selection, deployment and operations of intrusion detection systems (IDPS)

ISO/IEC 27039:2015

ISO/IEC FDIS 27040
Information technology -- Security techniques -- Storage security

ISO/IEC 27040:2015

ISO/IEC DIS 27041
Information technology -- Security techniques -- Guidance on assuring suitability and adequacy of incident investigative methods

ISO/IEC 27041:2015

ISO/IEC DIS 27042
Information technology -- Security techniques -- Guidelines for the analysis and interpretation of digital evidence

ISO/IEC 27042:2015

ISO/IEC FDIS 27043
Information technology -- Security techniques -- Incident investigation principles and processes

ISO/IEC 27043:2015

ISO/IEC WD 27044
Guidelines for Security Information and Event Management (SIEM)

ISO/IEC 27050
Information technology -- Security techniques -- Electronic discovery

ISO/IEC 27050-1:2016

Information technology -- Security techniques -- Electronic discovery -- Part 1: Overview and concepts

ISO/IEC 27050-3:2017

Information technology -- Security techniques -- Electronic discovery -- Part 3: Code of practice for electronic discovery

ISO 27799:2008

Health informatics -- Information security management in health using ISO/IEC 27002

ISO 27799:2008 poskytuje návod a podporu pri interpretácii a implementácii ISO 27002 do zdravotníckych organizácií.

Cieľom tohto vykonávacieho predpisu je aj stanovenie znalostných štandardov v oblasti kybernetickej bezpečnosti pre jednotlivé role kybernetickej bezpečnosti. Úrad vypracuje minimálne znalostné požiadavky vo forme štandardov pre oblasť informačnej bezpečnosti pre kategórie

a) laických používateľov informačných systémov,
b) riadiacich pracovníkov,
c) pracovníkov zodpovedných za prevádzku informačných systémov,
d) pracovníkov zodpovedných za ochranu informačných systémov,
e) audítorov informačnej bezpečnosti.

Znalostné štandardy budú vychádzať zo špecifikácie jednotlivých rolí a definujú záväzné znalostné požiadavky, ktorých naplnenie je nevyhnutné na to, aby mohol byť subjekt do danej roly zaradený.

Vykonávacím predpisom sa nebudú žiadnym subjektom ukladať práva, povinnosti ani kompetencie.

Vykonávací predpis podľa podľa § 32 ods. 1 písm. e), ktorým sa stanovujú identifikačné kritériá pre jednotlivé kategórie kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov [§ 24 ods. 1 a 4],

Kategórie závažných kybernetických bezpečnostných incidentov

(1) Závažným kybernetickým bezpečnostným incidentom je akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky subjektu negatívny vplyv na kybernetickú bezpečnosť.

- takto je v zákone definovaný kybernetický bezpečnostný incident
- znamená to, že kybernetický bezpečnostný incident = závažný kybernetický bezpečnostný incident?
- a výhrady k definícii uvedené v pripomienkach k zákonu

(2) Podľa príčiny sa závažné kybernetické bezpečnostné incidenty delia na incidenty spôsobené:

a) kybernetickým útokom alebo inou udalosťou ktorá spôsobila prienik do systému alebo obmedzenie dostupnosti služieb,
b) škodlivým kódom,
c) porušením alebo prekonaním bezpečnostných opatrení,
d) porušením záväzných metodík a politiky správania sa v kybernetickom priestore,
e) inými kybernetickými útokmi.

- toto delenie je nezmyselné, lebo na útok možno použiť škodlivý kód; porušenie bezpečnostných opatrení a záväzných metodík môže umožniť úspešný útok
- čo to je iný kybernetický útok?

(3) Podľa dopadov sa závažné kybernetické bezpečnostné incidenty delia na incidenty, ktorých následkom je:

a) strata dôvernosti dát, zničenie dát alebo narušenie integrity systému,
b) obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby,
c) vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby,
d) ohrozenie bezpečnosti informácií.

- toto delenie je nelogické, lebo: ohrozenie bezpečnosti informácií (d) zahŕňa aj stratu dôvernosti, dostupnosti údajov (a); z nedostupnosti potrebných údajov vyplýva aj strata alebo obmedzenie dostupnosti služieb (b) a kompromitácia (c)

Stupne závažných kybernetických bezpečnostných incidentov

(1) Závažný kybernetický bezpečnostný incident sa podľa stupňa závažnosti člení podľa kategórie na:

a) závažný kybernetický bezpečnostný incident (III) stupňa
b) závažný kybernetický bezpečnostný incident (II) stupňa
c) závažný kybernetický bezpečnostný incident (I) stupňa

Kritériá závažných kybernetických bezpečnostných incidentov

(1) Prevádzkovateľ základnej služby a poskytovateľ digitálnej služby pri kategorizácii jednotlivých závažných kybernetických bezpečnostných incidentov podľa § 3 zohľadní možné dôsledky kybernetického bezpečnostného incidentu na sieť alebo informačný systém najmä:

a) dôležitosť siete alebo informačného systému,
b) dopad incidentu na inú základnú alebo digitálnu službu,
c) predpokladané škody a iné dopady,
d) kritériá podľa odseku 2.

- text nie je delený na §, preto odkaz nemá zmysel

(2) Kritériá na identifikáciu závažných kybernetických bezpečnostných incidentov prevádzkovateľmi základných služieb a poskytovateľov digitálnych služieb sa určujú v závislosti od:

a) počtu používateľov základnej služby alebo digitálnej služby, postihnutých kybernetickým bezpečnostným incidentom,
b) dĺžky trvania kybernetického bezpečnostného incidentu,
c) geografického rozšírenia kybernetického bezpečnostného incidentu,
d) stupňa narušenia fungovania základnej služby alebo digitálnej služby, rozsahu vplyvu kybernetického bezpečnostného incidentu na hospodárske alebo spoločenské činnosti štátu,

Pri hlásení incidentu platia nasledujúce pravidlá:

1. Je nutné uvádzať korektnú e-mailovú adresu, ktorá je primárnym kontaktom.
2. Je nutné uviesť jednoznačný popis incidentu.
3. Pri popise incidentu uveďte čo najviac informácií, ktoré by mohli pomôcť pri jeho analýze a následnom spracovaní. Každá, aj zdanlivo na prvý pohľad neužitočná informácia, môže byť veľmi užitočná.

Popis incidentu by mal obsahovať tieto údaje:

1. Informácie o osobe v organizácii, ktorá hlási incident:

a) funkcia/pracovné zaradenie

b) názov organizácie, typ organizácie
c) ďalšie dotknuté organizácie

2. Informácie o incidente:

a) čas začiatku incidentu (ak je známy)
b) čas a spôsob zistenia
c) typ incidentu
d) kategória incidentu
e) ide o prebiehajúci incident
f) boli zneužité nejaké známe zraniteľnosti
g) aké protiopatrenia boli vykonané
h) detailný popis – popis priebehu incidentu, aké typy útokov boli použité, odkiaľ útok smeroval, aké boli bezpečnostné opatrenia, či boli prekonané, súčasný stav zvládania kybernetického bezpečnostného incidentu, rozsah škôd a prijaté opatrenia, počet zasiahnutých služieb, odhad dopadu incidentu na užívateľov apod.
i) ak ide o spam pripojte úplnú hlavičku a telo e-mailovej správy
j) ak ide o vírus, tak dotknutý súbor zabalený vo formáte ZIP zabezpečený heslom: „incident“
k) ak ide o phishing alebo pharming, pripojte prosím aj úplnú adresu URL.
l) ak ide o sieťové skenovanie alebo útok typu odopretia služieb (DoS), pripojte prosím časové známky, časovú zónu, zdrojové a cieľové IP (prípadne MAC) adresy a porty, typ protokolu (TCP, UDP, ICMP,…) – ak je možné vzorku zachytených paketov.

3. Informácie o zasiahnutých zariadeniach a dopadoch:

a) typ a funkcia zariadenia
b) IP adresa, hostname,
c) protokol a porty na ktoré útok smeroval,
d) popis hardwaru zariadenia,
e) operačný systém (typ, verzia)
f) zasiahnutý software alebo súbory
g) informácia či ide o kritické zariadenie z pohľadu pokračovania v činnosti
h) informácia či je zariadenie v prevádzke
i) kontaktná osoba pre získanie prístupu k zariadeniu
j) obsahuje neverejné informácie.

Typ	druh	Popis
Nežiaduci obsah	Spam Obťažovanie	Spam - nevyžiadaný hromadný e-mail - znamená, že používateľ nedal povolenie na jeho poslanie a správa je súčasťou väčšieho súboru správ s rovnakým obsahom. Ďalej do tejto skupiny patria e-maily alebo webové stránky s diskriminačným alebo diskreditačným obsahom, s obsahom pornografie, propagácie násilia a podobne.
Škodlivý kód	Vírus Červ Trójsky kôň Spyware	Softvér, ktorý je zámerne obsiahnutý alebo vložený do systému so škodlivým zámerom. Na aktiváciu kódu je väčšinou potrebná súčinnosť používateľa.

	Dialler	
Získavanie informácií	Skenovanie Odpočúvanie Sociálne inžinierstvo	Skenovanie znamená posielanie požiadaviek na systém s cieľom odhalenia jeho slabín. To zahŕňa niektoré testovacie procesy na zistenie informácií o zariadeniach, službách a účtoch, napr. fingerd, DNS požiadavky, ICMP, SMTP (EXPN, RCPT,...) apod. Odpočúvanie zahŕňa sledovanie a zaznamenávanie sieťovej prevádzky za týmto účelom. Sociálne inžinierstvo znamená získavanie informácií od ľudí netechnickým spôsobom (lži, triky, hrozby).
Pokus o prienik	Využitie známej zraniteľnosti Opakované pokusy o prihlásenie Útok s neznámymi znakmi	Pokus skompromitovať systém alebo narušiť službu využitím zraniteľnosti so štandardizovaným identifikátorom (napr. CVE), ako napr. pretečenie pamäte, zadné dvierka, XSS (cross side scripting) apod. Patria sem aj opakované neúspešné pokusy o prihlásenie (hádanie, útok hrubou silou), ako aj pokusy o prienik doposiaľ neznámym spôsobom.
Prienik	Skompromitovanie privilegovaného účtu Skompromitovanie obmedzeného účtu Skompromitovanie aplikácie Botnet	Úspešné skompromitovanie systému alebo aplikácie (služby). Môže k nemu dôjsť na diaľku využitím známej alebo novej zraniteľnosti, ale aj neautorizovaným lokálnym prístupom.
Nedostupnosť	DoS DDoS Sabotáž	Pri tomto type útokov je systém bombardovaný takým množstvom paketov, že operácie sú oneskorené, alebo systém skolabuje. Príklady vzdialeného útoku typu DoS sú SYN flooding, ping-flooding, E-mail bombing (DDoS: TFN, Trinity,...). Dostupnosť však môže byť obmedzená aj lokálnymi činnosťami (deštrukcia, prerušenie napájania,...).
Ohrozenie bezpečnosti informácií	Neoprávnený prístup k informáciám Neoprávnená zmena informácií	Okrem lokálneho zneužitia dát a systémov, bezpečnosť informácií môže byť ohrozená aj úspešným skompromitovaním aplikácie alebo účtu. Patria sem aj útoky, pri ktorých dochádza k zachytávaniu a pristupovaniu k informáciám počas prenosu.
Podvod, sprenevera	Neoprávnené využívanie zdrojov Porušenie autorských práv	Patrí sem využívanie zdrojov na neoprávnené účely vrátane neoprávneného zisku (napr. účasť na ilegálnych reťazových e-mailoch pre dosiahnutie zisku alebo

	Prevzatie identity Phishing	pyramídové schémy). Patrí sem aj predaj a inštalácia nelicencovaných kópií komerčného softvéru alebo iných materiálov chránených autorskými právami. Ďalej sem patria útoky, pri ktorých jedna entita nelegitímne predstiera identitu druhej, aby z toho mala úžitok, ako aj phishing.
Iné		

Kritériá na identifikáciu závažných kybernetických bezpečnostných incidentov prevádzkovateľmi základných služieb a poskytovateľov digitálnych služieb

Parameter		**Kritériá na identifikáciu závažných kybernetických bezpečnostných incidentov prevádzkovateľmi základných služieb a poskytovateľov digitálnych služieb**	
		Metrika	**Závažnosť vplyvu incidentu**
1.	Geografické rozšírenie kybernetického bezpečnostného incidentu,	Kybernetický bezpečnostný incident má rušivý vplyv na kontinuitu základnej služby v rámci celého územia SR, v rámci celého kraja SR alebo celého okresu SR	3. stupňa: celé územie SR 2. stupňa: celý kraj SR 1. stupňa: celý okres SR
2.	Stupeň narušenia fungovania základnej služby alebo digitálnej služby	Kybernetický bezpečnostný incident má rušivý vplyv na kontinuitu základnej služby z pohľadu narušenia jej integrity, dôvernosti, dostupnosti a autentickosti	3. stupňa: narušenie aspoň troch bezpečnostných požiadaviek 2. stupňa: narušenie aspoň dvoch bezpečnostných požiadaviek 1. stupňa: narušenie aspoň jednej bezpečnostnej požiadavky
3.	Počet používateľov základnej služby alebo digitálnej služby postihnutých kybernetickým bezpečnostným incidentom + dĺžka trvania kybernetického bezpečnostného incidentu	Kybernetický bezpečnostný incident má rušivý vplyv na kontinuitu základnej služby, pričom dosiahol intencií absolútnej hranice (A) vyjadrenej ako súčin počtu postihnutých používateľov (B) a dĺžky trvania incidentu v hodinách (C)	A= 10 tisíc používateľov/hodín B= 1000 používateľov C= 1 hodina
4.	Rozsah rušivého vplyvu incidentu na sociálne a ekonomické aktivity používateľov	Počet používateľov postihnutých kybernetickým bezpečnostným incidentom	3. stupňa: A: 30 tisíc používateľov/hodín B: 2000 používateľov C: 3 hodiny 2. stupňa: A: 20 tisíc používateľov/hodín B: 1500 používateľov C: 2 hodiny 1. stupňa: A: 10 tisíc používateľov/hodín B: 1000 používateľov C: 1 hodina

Vykonávacím predpisom sa nebudú žiadnym subjektom ukladať práva, povinnosti ani kompetencie.

Vykonávací predpis podľa podľa § 32 ods. 1 písm. f), ktorým sa ustanovujú 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].

Cieľom tohto vykonávacieho predpisu je stanovenie podrobnosti o požiadavkách na audit a rozsah auditu, na základe ktorého sa overuje a hodnotí kybernetická bezpečnosť sietí a informačných systémov prevádzkovateľa základnej služby, a to najmä v rozsahu súladu prijatých a implementovaných bezpečnostných opatrení a bezpečnostnej dokumentácie s požiadavkami podľa zákona.

Vykonávaci predpis bude vychádzať s noriem rady 27000, ktoré predstavujú medzinárodné štandardy v oblasti riadenia informačnej bezpečnosti:

ISO/IEC 27006:2011
Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27006:2011 špecifikuje požiadavky a poskytuje návod pre organizácie poskytujúce audit a certifikácie SMIB. Štandard je primárne zameraný na podporu akreditácie organizácií poskytujúcich certifikáciu SMIB.

ISO/IEC 27007:2011
Information technology -- Security techniques -- Guidelines for information security management systems auditing
ISO/IEC 27007:2011 poskytuje návod a požiadavky pre riadenie programu auditov SMIB, vykonávanie auditov a kompetencie audítorov SMIB.

ISO/IEC TR 27008:2011
Information technology -- Security techniques -- Guidelines for auditors on information security controls
ISO/IEC TR 27008:2011 poskytuje návod na preskúmavanie implementácie a prevádzky opatrení, vrátane technického súladu opatrení informačnej bezpečnosti.

Vykonávacím predpisom sa nebudú žiadnym subjektom ukladať práva, povinnosti ani kompetencie.

Označené normy sú neplatné

Vykonávací predpis podľa podľa § 32 ods. 2

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 štandardami v oblasti kybernetickej bezpečnosti.

Vykonávacím predpisom sa nebudú žiadnym subjektom ukladať práva, povinnosti ani kompetencie.