Deloitte.

Kybernetická bezpečnosť (#NIS)

Jesenný seminár pre farmaceutické spoločnosti 2018

október 2018

Risk


Aký IT incident ste naposledy zaznamenali
a riešili vo vašej spoločnosti?

IT Bezpečnostné incidenty v 2017 - 2018

Mall.cz – údaje na Ulož.to – 730 000 zákazníkov a ich mená, heslá a emaily – pokuta 60 000 Eur

British Airways – únik osobných údajov - 380 000 osobných a platobných údajov o zákazníkoch

Facebook – únik osobných údajov – 29 miliónov profilov a informácií

Anthem – únik zdravotných záznamov 79 mil. pacientov (meno, č. soc. poistenia, ...) – pokuta 16 mil. USD

Ransomware (**WannaCry, NotPetya)** – zablokované IT v nemocniciach v UK (ale napr. aj v Nitre)

© 2018 Deloitte na Slovensku

Top 5 faktov kybernetickej bezpečnosti vo farma priemysle pre rok 2018

60 %

spoločností má vo firme funkciu **CISO**

61 %

spoločností má **bezpečnostnú stratégiu**

13 %

je zvýšenie rozpočtov pre účely **informačnej bezpečnosti**

- 30 %

je zníženie detegovaných **incidentov**

- 94 %

je celkové zníženie **finančných strát** kvôli incidentom

Ginni Rometty, IBM CEO:

“Cyber crime is the greatest threat to every company in the world.”

© 2018 Deloitte na Slovensku

Nová regulácia ...

Legislatíva

- SMERNICA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/1148 zo 6. júla 2016 **o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov** v Únii (#NIS)

- ZÁKON č. 69/2018 Z.z., o **kybernetickej bezpečnosti** a o zmene a doplnení niektorých zákonov

© 2018 Deloitte na Slovensku

Definície

Sieť a informačný systém

Kybernetický priestor

Kybernetická bezpečnosť

Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov / https://www.slov-lex.sk/static/pdf/2018/69/ZZ_2018_69.pdf

© 2018 Deloitte na Slovensku

Kybernetická vs Informačná bezpečnosť

Informačná bezpečnosť sa zaoberá otázkou zaručenia dôvernosti, integrity, dostupnosti a sledovateľnosti informačných aktív.

Kybernetická bezpečnosť sa venuje bezpečnosti informačných aktív, ktoré sú spracúvané kybernetickom priestore.

© 2018 Deloitte na Slovensku

Úrad a ústredné orgány

Národný Bezpečnostný Úrad

Ministerstvo Hospodárstva SR

Ministerstvo Zdravotníctva SR

© 2018 Deloitte na Slovensku

A platí to aj pre mňa?

Základná služba a jej prevádzkovateľ

Základná služba je služba, ktorá je zaradená v zozname základných služieb a závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č.1, je informačným systémom verejnej správy, je prvkom kritickej infraštruktúry.

Prevádzkovateľom základnej služby je orgán verejnej moci alebo osoba, ktorá prevádzkuje aspoň jednu službu podľa vyššieho odseku.

Bankovníctvo	Cestná doprava	Letecká doprava	Vodná doprava	Železničná doprava	Poskytovatelia vybraných internetových služieb	Satelitná komunikácia	Siete a služby pevných a mobilných komunikácií
Baníctvo	Elektroenergetika	Plynárenstvo	Ropa a ropné produkty	Tepelná energia	Prevádzkovatelia obchodných miest	Poštový podnik	Farmaceutický priemysel
Hutnícky priemysel	Chemický priemysel	Meteorologická služba	Vlastník vodnej stavby	Zabezpečovanie pitnej vody	IS verejnej správy	Spravodajské služby	Zdravotnícke zariadenia

© 2018 Deloitte na Slovensku

Identifikačné kritéria

Identifikačné kritériá prevádzkovanej služby sú dopadové kritériá a špecifické sektorové kritériá.

Dopadové kritéria zohľadňujú najmä:

- Počet používateľov využívajúcich základnú službu
- Závislosť ostatných sektorov podľa prílohy č.1 od základnej služby
- Vplyv, ktorý by mohli mať kybernetické bezpečnostné incidenty z hľadiska rozsahu a trvania na hospodárske a spoločenské činnosti a záujmy štátu alebo na bezpečnosť štátu
- Trhový podiel prevádzkovateľa služby
- Geografické rozšírenie z hľadiska oblasti, ktorú by kybernetický bezpečnostný incident mohol postihnúť
- Význam prevádzkovateľa základnej služby z hľadiska zachovania kontinuity poskytovania služby

Vyhláška č. 164 Národného bezpečnostného úradu, ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby) /
https://www.slov-lex.sk/static/pdf/2018/164/ZZ_2018_164_20180615.pdf

© 2018 Deloitte na Slovensku

Identifikačné kritéria – Zdravotníctvo

Prevádzkovateľ služieb (príloha č. 1 k zákonu)	Špecifické sektorové kritéria (jednotlivo)	Dopadové kritéria (jednotlivo)
Výrobca liekov podľa osobitného predpisu. (Zákon č. 362/2011 Z.z. o liekoch a zdravotníckych pomôckach)	-	1. Ohrozenie dostupnosti, pravosti, integrity alebo dôvernosti uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov, ktoré postihuje viac ako 25 000 osôb. 2. Obmedzenie či narušenie prevádzky inej základnej služby alebo prvku kritickej infraštruktúry. 3. Hospodársku stratu vyššiu ako 0,1 % HDP. 4. Hospodársku stratu alebo hmotnú škodu najmenej jednému užívateľovi viac ako 250 000 EUR. 5. Viac ako 100 zranených osôb vyžadujúcich lekárske ošetrenie alebo stratu jedného života 6. Narušenie verejného poriadku, verejnej bezpečnosti, mimoriadnu udalosť alebo tieseň, ktorá môže vyžadovať vykonanie záchranných prác, alebo výkon činností a opatrení súvisiacich s poskytovaním pomoci v tiesni.

© 2018 Deloitte na Slovensku

Identifikačné kritéria – Zdravotníctvo

Prevádzkovateľ služieb (príloha č. 1 k zákonu)	Špecifické sektorové kritéria (jednotlivo)	Dopadové kritéria (jednotlivo)
Poskytovateľ zdravotnej Starostlivosti fyzická osoba, právnická osoba alebo iný subjekt, ktorý poskytuje zdravotnú starostlivosť na území členského štátu Európskej únie.	a) Celkový počet akútnych lôžok v posledných troch kalendárnych rokoch najmenej 500. b) Štatút centra vysokošpecializovanej traumatologickej starostlivosti podľa osobitného predpisu. c) Laboratórne služby.	1. Ohrozenie dostupnosti, pravosti, integrity alebo dôvernosti uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov, ktoré postihuje viac ako 25 000 osôb. 2. Obmedzenie či narušenie prevádzky inej základnej služby, alebo prvku kritickej infraštruktúry. 3. Hospodársku stratu vyššiu ako 0,1 % HDP. 4. Hospodársku stratu alebo hmotnú škodu najmenej jednému užívateľovi viac ako 250 000 eur. 5. Viac ako 100 zranených osôb vyžadujúcich lekárske ošetrenie alebo stratu jedného života. 6. Narušenie verejného poriadku, verejnej bezpečnosti, mimoriadnu udalosť alebo tieseň, ktorá môže vyžadovať vykonanie záchranných prác, alebo výkon činností a opatrení súvisiacich s poskytovaním pomoci v tiesni.

© 2018 Deloitte na Slovensku

Oznámenie úradu

Ak prevádzkovateľ služby zistí, že došlo k prekročeniu identifikačných kritérií prevádzkovanej služby, je povinný to **oznámiť úradu** do 30 dní odo dňa, keď prekročenie zistil.

© 2018 Deloitte na Slovensku


Už ste oznámili úradu prekročenie
identifikačných kritérií?

Register prevádzkovateľov základnej služby (18.10.2018)

1. Prevádzkovatelia základnej služby podľa § 3 písm. k) prvý bod zákona o kybernetickej bezpečnosti

dátum poslednej aktualizácie: 18.10.2018

Prevádzkovateľ základnej služby	Základná služba	IČO	Sektor	Podsektor	Ústredný orgán
Prevádzkovateľ základnej služby zaradený v zozname prvkov kritickej infraštruktúry schváleného uznesením vlády Slovenskej republiky č. 347/2018 alebo informačné systémy k nemu priamo pripojené	Služba, ktorá je prvkom kritickej infraštruktúry alebo je k nemu priamo pripojená				
BENESTRA, s.r.o.	IP - Transit- poskytovateľ služby výmenného uzla internetu na účel prepájania sietí, ktoré sú z technického a organizačného pohľadu oddelené, DNS - poskytovateľ služieb systému doménových mien na internete	46 303 502	Digitálna infraštruktúra		Národný bezpečnostný úrad
Energotel, a.s.	Poskytovateľ služby výmenného uzla internetu na účel prepájania sietí, ktoré sú z technického a organizačného pohľadu oddelené; poskytovateľ služieb systému doménových mien na internete	35 785 217	Digitálna infraštruktúra		Národný bezpečnostný úrad
Komerční banka, a.s., pobočka zahraničnej banky	Poskytovanie bankových produktov a služieb - platobný styk	47 231 564	Bankovníctvo		Ministerstvo financií SR
Letové prevádzkové služby Slovenskej republiky, štátny podnik	ATC služba riadenia letovej prevádzky EUROCAT 2000	35 778 458	Doprava	Letecká doprava	Ministerstvo dopravy a výstavby SR
MBS spol. s r.o.	Poskytovanie služieb systému doménových mien na internete	30 228 018	Digitálna infraštruktúra		Národný bezpečnostný úrad
Národná diaľničná spoločnosť, a.s.	Služba elektronického výberu mýta, služba elektronická diaľničná známka, centrálny riadiaci systém tunelov; informačný systém diaľnic a rýchlostných ciest	35 919 001	Doprava	Cestná doprava	Ministerstvo dopravy a výstavby SR
O2 Slovakia	Siete a služby pevných a mobilných elektronických komunikácií; poskytovateľ služby výmenného uzla internetu; poskytovateľ služieb systému doménových mien na internete	35 848 863	Digitálna infraštruktúra		Národný bezpečnostný úrad
Orange Slovensko, a.s.	Služba výmenného uzla internetu na prepájanie sietí (IXP); služba systému doménových mien na internete	35 697 270	Digitálna infraštruktúra		Národný bezpečnostný úrad
OTP Banka Slovensko, a.s.	Poskytovanie bankových produktov a služieb	31 318 916	Bankovníctvo		Ministerstvo financií SR
Popradská energetická spoločnosť, s.r.o.	Výroba a dodávka tepla	50 339 729	Energetika	Tepelná energetika	Ministerstvo hospodárstva SR

http://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/prevadzkovatelia-ZS.htm

© 2018 Deloitte na Slovensku

Povinnosti prevádzkovateľa

Prijať a dodržiavať všeobecné **bezpečnostné opatrenia** najmenej v rozsahu bezpečnostných opatrení podľa § 20 a sektorové bezpečnostné opatrenia.

Uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností s dodávateľom zodpovedným za prevádzku sietí a informačných systémov

Povinný **riešiť incident**, **hlásiť závažný incident**, spolupracovať s úradom pri riešení hláseného incidentu, zabezpečiť dôkazy a určiť kontaktnú osobu pre hlásenia.

© 2018 Deloitte na Slovensku

Kontrola, audit, pokuty

Úrad v oblasti kybernetickej bezpečnosti:

- Vykonáva kontrolu, vydáva rozhodnutia o uložení opatrení na nápravu a ukladá pokutu za priestupok alebo iný správny delikt
- Vykonáva audit alebo požiada orgán posudzovania zhody o vykonanie auditu u prevádzkovateľa základnej služby
- Ustanoví pravidlá a rozsah auditu kybernetickej bezpečnosti a podrobnosti o akreditácii orgánov posudzovania zhody a o obsahu záverečnej správy o výsledkoch auditu kybernetickej bezpečnosti

Prevádzkovateľ základnej služby je povinný preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených týmto zákonom vykonaním **auditu kybernetickej bezpečnosti**.

Úrad uloží **pokutu od 300 EUR až do výšky 1 % celkového ročného obratu** za predchádzajúci účtovný rok, najviac však 300 000 EUR.

© 2018 Deloitte na Slovensku

Bezpečnostné opatrenia

© 2018 Deloitte na Slovensku

LSHC bezpečnostné opatrenia (as-is)

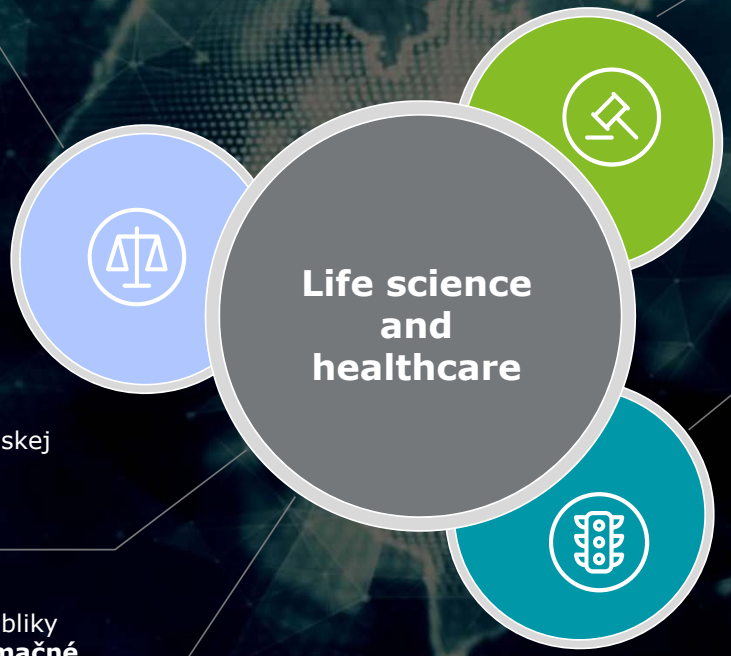
Zákon č. 362/2012 Z. z. o liekoch a zdravotníckych pomôckach

§ 60 Povinnosti držiteľa registrácie humánneho lieku

- **z)** zabezpečiť vytvorenie a prevádzkovanie informačného systému na mimoriadne objednávanie liekov, ...
- **aa)** technicky zabezpečiť udržiavanie informačného systému na mimoriadne objednávanie liekov podľa písmena z) v **nepretržitej prevádzke**,

Vyhláška Ministerstva zdravotníctva Slovenskej republiky č. 107/2015 Z. z., ktorou sa ustanovujú **štandardy zdravotníckej informatiky** a lehoty poskytovania údajov

Výnos Ministerstva financií Slovenskej republiky č. 55/2014 Z. z o **štandardoch pre informačné systémy verejnej správy**



Zákon č. 576/2004 Z. z. o zdravotnej starostlivosti

§20 Formy vedenia zdravotnej dokumentácie

- (3) Zdravotnú dokumentáciu možno viesť v elektronickej forme s elektronickým podpisom, len ak **bezpečnostné kópie dátových súborov** sa vyhotovujú podľa štandardov zdravotníckej informatiky[21a)] najmenej jedenkrát za každý pracovný deň,

Zákon č. 153/2013 Z. z. o národnom zdravotníckom informačnom systéme

§ 9 Štandardy zdravotníckej informatiky

- Štandardy zdravotníckej informatiky zabezpečujú jednotnosť, bezpečnosť a integrovateľnosť v oblasti informačno-komunikačných technológií v zdravotníctve.

§ 11 Overenie zhody informačného systému poskytovateľa zdravotnej starostlivosti

- (3) Informačný systém poskytovateľa zdravotnej starostlivosti musí
- **d)** spĺňať pri spracúvaní údajov **štandardy zdravotníckej informatiky,**
- g) zabezpečiť, aby údaje medzi národným zdravotníckym informačným systémom a informačným systémom poskytovateľa zdravotnej starostlivosti boli **prenášané bez narušenia ich integrity**.

© 2018 Deloitte na Slovensku

Bezpečnostné opatrenia

- **Bezpečnostné opatrenia** sú úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov.

- **Klasifikácia** informácií a **kategorizácia** sietí a informačných systémov.

- Bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej **bezpečnostnej dokumentácie**, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu.

Vyhláška XXX Národného bezpečnostného úradu, **obsah bezpečnostných opatrení, obsah a štruktúru bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.**

© 2018 Deloitte na Slovensku

Kategórie bezpečnostných opatrení

1. **Organizácia bezpečnosti**
2. **Riadenie aktív, hrozieb a rizík**
3. **Personálna bezpečnosť**
4. **Riadenie dodávateľských služieb, akvizície, vývoja a Údržba informačných systémov**
5. **Technické zraniteľností systémov a zariadení**
6. **Riadenie bezpečnosti sietí a informačných systémov**
7. **Riadenie prístupov**
8. **Riadenie prevádzky**
9. **Kryptografické opatrenia**
10. **Riešenie kybernetických bezpečnostných incidentov**
11. **Monitorovanie, testovanie bezpečnosti a bezpečnostných auditov**
12. **Fyzická bezpečnosť a bezpečnosť prostredia**
13. **Riadenie kontinuity procesov**

© 2018 Deloitte na Slovensku

Bezpečnostná dokumentácia

1. **Organizácia bezpečnosti**
2. **Riadenie bezpečnostných rizík**
3. **Riadenie informačných aktív**
4. **Pravidlá správania a dobrej praxe**
5. **Riadenie dodávateľských vzťahov**
6. **Riadenie vývoja a údržby v oblasti IKT**
7. **Riadenie IT služieb a prevádzky IKT**
8. **Riadenie súladu**
9. **Riadenie kontinuity činností**

© 2018 Deloitte na Slovensku

Bezpečnostné incidenty

Kybernetickým bezpečnostným incidentom je akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je

1. **Strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému,**
2. **Obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby,**
3. **Vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo**
4. **Ohrozenie bezpečnosti informácií.**

Vyhláška č. 165 Národného bezpečnostného úradu, ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov / https://www.slov-lex.sk/static/pdf/2018/165/ZZ_2018_165_20180615.pdf

© 2018 Deloitte na Slovensku

Závažný kybernetický bezpečnostný incident

Dopad kybernetického bezpečnostného incidentu v závislosti:	Závažný kybernetický bezpečnostný incident		
	Kategória I.	**Kategória II.**	**Kategória III.**
Počet zasiahnutých používateľov základnej služby	Postihuje viac ako 25 000 osôb	Postihuje viac ako 50 000 osôb	Postihuje viac ako 100 000 osôb
Dĺžka trvania incidentu a geografické rozšírenie	V rozsahu viac ako 15 000 používateľských hodín na území najmenej jedného okresu počas 60 min.	V rozsahu viac ako 100 000 používateľských hodín na území najmenej jedného kraja počas 60 min.	V rozsahu viac ako 500 000 používateľských hodín na celom území SR počas 60 min.
Stupeň narušenia fungovania základnej služby	-	Úplná nedostupnosť druhu služby, s možnosťou zabezpečiť náhradné riešenie	Úplná nedostupnosť druhu služby, bez možnosti zabezpečiť náhradné riešenie
Rozsah na hospodárske alebo spoločenské činnosti štátu	• Stratu alebo škodu viac ako 250 000 EUR pre jednotlivca • Viac ako 1 000 zranených alebo stratu 1 života • Narušenie verejného poriadku v okrese	• Stratu alebo škodu viac ako 500 000 EUR pre jednotlivca • Viac ako 3 500 zranených alebo stratu 100 životov • Narušenie verejného poriadku v kraji	• Stratu alebo škodu viac ako 1 000 000 EUR pre jednotlivca • Viac ako 5 000 zranených alebo stratu 500 životov • Narušenie verejného poriadku v SR

© 2018 Deloitte na Slovensku

A čo teraz ...

Ako na to

Identifikoval som sa ako prevádzkovateľ základnej služby?
(ak áno) Oznámil som túto skutočnosť na NBÚ?

december 2018

Spĺňam všetky požiadavky novej legislatívy?
(ak nie) Prijal som nové bezpečnostné opatrenia?

6 mesiacov

Viem preukázať dodržiavanie bezpečnostné opatrenia?
(ak áno) Vykonal som audit kybernetickej bezpečnosti?

2 roky

© 2018 Deloitte na Slovensku

Michal Ďorda
Cyber Security Senior Consultant

M: +421 905 915 660
mdorda@deloitteCE.com

© 2018 Deloitte na Slovensku

Deloitte.

Deloitte označuje jednu, resp. viacero spoločností Deloitte Touche Tohmatsu Limited, britskej súkromnej spoločnosti s ručením obmedzeným zárukou (UK private company limited by guarantee), a jej členských firiem. Každá z týchto firiem predstavuje samostatný a nezávislý právny subjekt. Podrobný opis právnej štruktúry združenia Deloitte Touche Tohmatsu Limited a jeho členských firiem sa uvádza na adrese www.deloitte.com/sk/o-nas.

Spoločnosť Deloitte poskytuje služby v oblasti auditu, daní, práva, podnikového a transakčného poradenstva klientom v mnohých odvetviach verejného a súkromného sektora. Vďaka globálne prepojenej sieti členských firiem vo viac ako 150 krajinách má Deloitte svetové možnosti a dôkladnú znalosť miestneho prostredia, a tak môže pomáhať svojim klientom dosahovať úspechy na všetkých miestach ich pôsobnosti. Približne 245 000 odborníkov spoločnosti Deloitte sa usiluje konať tak, aby vytvárali hodnoty, na ktorých záleží.

© 2018 Deloitte na Slovensku