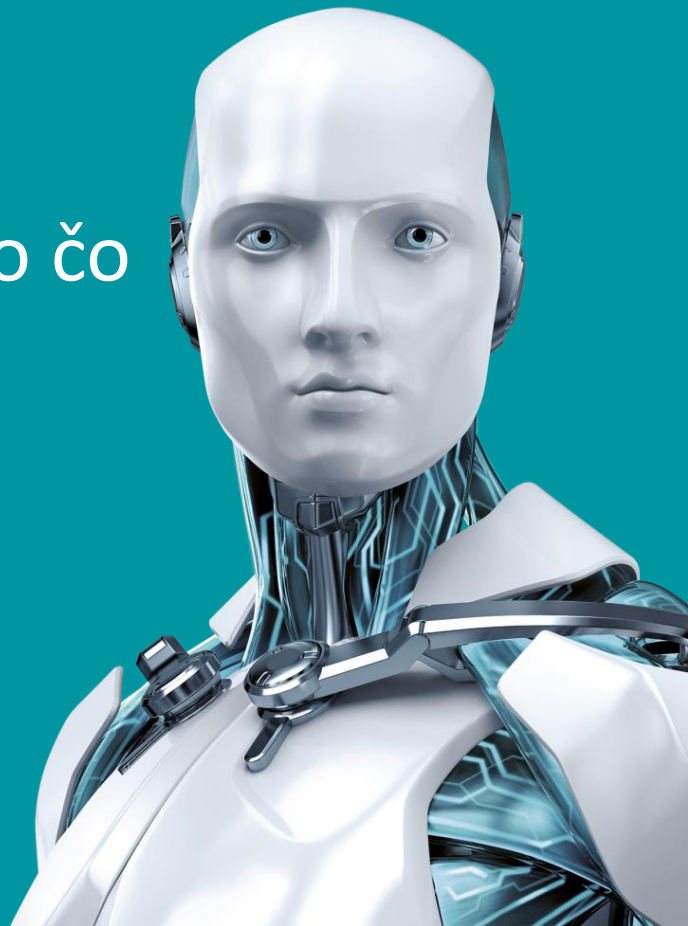
Audit súladu so Zákonom o kybernetickej bezpečnosti alebo čo potrebujeme na jeho úspešné absolvovanie

Peter Dekýš, PhD, CISA, CISM

ENJOY SAFER TECHNOLOGY™



Dôvody presadzovania kybernetickej bezpečnosti

Slovensko čelí masívnym útokom hackerov: Budú sa opakovať, takto sa môžete chrániť

POŠLITE NÁM TIP

Ilustračné foto
Zdroj: thinkstock.com

01.07.2018 10:17

BRATISLAVA - Slo
v posledných mesia
DDOS útokom hac
Okrem iných slover
adries útočníci v po
napadli stránky Slo
hydrometeorologick
ale aj portál slovens

Aluminum manufacturing giant Norsk Hydro shut down by ransomware

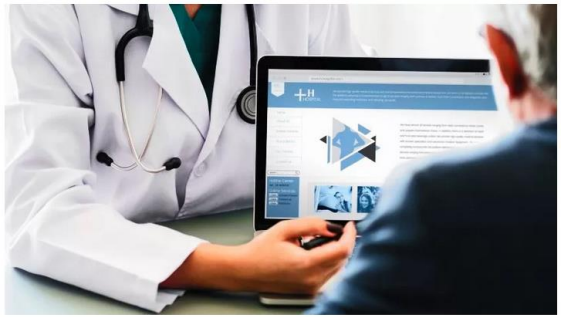
Zack Whittaker @zackwhittaker / 4:07 pm CET • March 19, 2019

Image Credits: Getty Images

Norsk Hydro, one of the largest global aluminum manufacturers, has confirmed its operations have been disrupted by a ransomware attack.

13.3.2020 09:15 | Bezpečnosť

AKTUALIZOVANÉ Hackeri napadli nemocnicu v Brne. Vypla všetky PC, odkladá operácie



Martin Hodás

Zdravotnícke zariadenie analyzuje aj vzorky ľudí, ktorí by mohli mať koronavírus.

Fakultná nemocnica v Brne je od dnešného rána paralyzovaná. Kvôli hackerskému útoku totiž lekári nemajú prístup k počítačom, informoval server iDnes.cz. Detaily ohľadom samotného útoku nie sú známe.

Právny základ a normatívne kritéria

- **Zákon č. 69/2018 Z.z.** o kybernetickej bezpečnosti (**ďalej len „Zákon“**)
- Vyhláška NBÚ č. 164/2018, ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby)
- Vyhláška NBÚ č. 165/2018, ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov
- **Vyhláška NBÚ č. 362/2018 Z.z.,** ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (**ďalej len „Vyhláška“**)
- Vyhláška NBÚ č. 436/2019 Z.z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora
- Zákon č. 56/2018 Z.z. o posudzovaní zhody výrobku, sprístupňovaní určeného výrobku na trhu
- STN EN ISO/IEC 17024:2012 Posudzovanie zhody - Všeobecné požiadavky na orgány vykonávajúce certifikáciu osôb

Vyhláška Národného bezpečnostného úradu č. 362/2018 Z.z.

- vyhláška upravuje
  - **obsah bezpečnostných opatrení**,
  - **obsah a štruktúru bezpečnostnej dokumentácie (§2)** a
  - **rozsah všeobecných bezpečnostných opatrení (§5- §17)**,

  ktoré prijíma prevádzkovateľ základnej služby podľa Zákona pre informačné systémy a siete, prostredníctvom ktorých zabezpečuje základnú službu a pre informačné systémy a siete, ktorých výpadok alebo poškodenie môže spôsobiť poškodenie alebo znemožnenie poskytovania základnej služby.

Krok #1: Prijatie stratégie kybernetickej bezpečnosti

- Stratégia kybernetickej bezpecnosti je **povinnou súčasťou bezpečnostnej dokumentácie** podľa §2 Vyhlášky
- Záväzný dokument organizácie, aby vedeniu a zamestnancom boli jasné:
  - ciele, základné princípy na ich dosiahnutie,
  - právomoci a zodpovednosti za riadenie kybernetickej bezpečnosti, riadenie rizík kybernetickej bezpečnoti a aktualizáciu bezpečnostnej dokumentácie.
- Štruktúra bezpečnostnej stratégie je definovaná v Prílohe č.1 k Vyhláške

Krok #2: Identifikácia informácií a sietí a informačných systémov

- **Informácie -** dáta, fakty alebo materiály, ktoré vznikajú pri činnosti organizácie.
- **Sieť a informačný systém -** zoznam vybraných komponentov sietí a informačných systémov, ktoré tvoria jednotlivú sieť a informačný systém.
- Pri identifikácii dochádza k vytváraniu **katalógu aktív**, ktorý je tvorený identifikovanými informáciami, sieťami a informačnými systémami.
- Pri jednotlivých aktívach je potrebná evidencia **vlastníka**, ktorý vie stanoviť alebo potvrdiť hodnotu aktíva pre organizáciu z pohľadu dôvernosti, integrity a dostupnosti.

Krok #3: Určenie klasifikácie informácií a kategorizácie sietí a informačných systémov

- Klasifikácia a kategorizácia je **povinnou súčasťou bezpečnostnej dokumentácie** podľa §2 Vyhlášky
- Pre určenie klasifikacie je dôležité **stanovisko** vlastníka aktíva
- **Klasifikáca informácií** je vykonávaná z pohľadu **dôvernosti** (4 stupne), **integrity a dostupnosti** (po 3 stupne).
- Klasifikácia informácii je nevyhnutná pre následnú kategorizáciu sietí a informacných systémov.
- **Kategorizácia sietí a informačných systémov** (I, II a III kategórie) je následne podkladom pre určenie minimálnych požiadviek na bezpečnostné opatrenia.
- A nezabudnime, ze klasifikácia a kategorizácia sú nevyhnutné pre vykonanie analýzy rizík, ich použitie však závisi od aplikovanej metodiky.

Dopad vykonanej kategrizácie sietí a informačných systémov

Tabuľka zobrazuje minimálne požiadavky na bezpečnostné opatrenia jednotlivých kategórií sietí a informačných systémov, ktoré môže prevádzkovateľ základnej služby pre individuálne aktíva sprísniť.

Bezpečnostné opatrenie pre	**Kategória I**	**Kategória II**	**Kategória III**
Oblasť podľa § 20 ods. 3 písm. a) zákona	Odporúčané	Odporúčané	Povinné
Oblasť podľa § 20 ods. 3 písm. b) zákona	Odporúčané	Povinné	Povinné
Oblasť podľa § 20 ods. 3 písm. c) zákona	Odporúčané	Povinné	Povinné
Oblasť podľa § 20 ods. 3 písm. d) zákona	Odporúčané	Povinné	Povinné
Oblasť podľa § 20 ods. 3 písm. e) zákona	Odporúčané	Povinné	Povinné
Oblasť podľa § 20 ods. 3 písm. f) zákona	Odporúčané	Povinné	Povinné
Oblasť podľa § 20 ods. 3 písm. g) zákona	Odporúčané	Povinné	Povinné
Oblasť podľa § 20 ods. 3 písm. h) zákona	Odporúčané	Povinné	Povinné
Oblasť podľa § 20 ods. 3 písm. i) zákona	Odporúčané	Odporúčané	Povinné
Oblasť podľa § 20 ods. 3 písm. j) zákona	Povinné	Povinné	Povinné
Oblasť podľa § 20 ods. 3 písm. k) zákona	Odporúčané	Povinné	Povinné
Oblasť podľa § 20 ods. 3 písm. l) zákona	Odporúčané	Odporúčané	Povinné
Oblasť podľa § 20 ods. 3 písm. m) zákona	Odporúčané	Povinné	Povinné

Dopad vykonanej kategrizácie sietí a informačných systémov na minimálne

Tabuľka zobrazuje minimálne požiadavky na bezpečnostné opatrenia jednotlivých kategórií sietí a informačných systémov, ktoré môže prevádzkovateľ základnej služby pre individuálne aktíva sprísniť.

Bezpečnostné opatrenie pre	**Kategória I**	**Kategória II**	**Kategória III**
Oblasť podľa § 20 ods. 3 písm. a) zákona	Odporúčané	Odporúčané	Povinné
Oblasť podľa § 20 ods. 3 písm. b) zákona	Odporúčané	Povinné	Povinné
Oblasť podľa § 20 ods. 3 písm. c) zákona	Odporúčané	Povinné	Povinné
Oblasť podľa § 20 ods. 3 písm. d) zákona	Odporúčané	Povinné	Povinné
Oblasť podľa § 20 ods. 3 písm. e) zákona	Odporúčané	Povinné	Povinné
Oblasť podľa § 20 ods. 3 písm. f) zákona	Odporúčané	Povinné	Povinné
Oblasť podľa § 20 ods. 3 písm. g) zákona	Odporúčané	Povinné	Povinné
Oblasť podľa § 20 ods. 3 písm. h) zákona	Odporúčané	Povinné	Povinné
Oblasť podľa § 20 ods. 3 písm. i) zákona	Odporúčané	Odporúčané	Povinné
Oblasť podľa § 20 ods. 3 písm. j) zákona	Povinné	Povinné	Povinné
Oblasť podľa § 20 ods. 3 písm. k) zákona	Odporúčané	Povinné	Povinné
Oblasť podľa § 20 ods. 3 písm. l) zákona	Odporúčané	Odporúčané	Povinné
Oblasť podľa § 20 ods. 3 písm. m) zákona	Odporúčané	Povinné	Povinné

Krok #4: Vykonanie analýzy rizík a riadenie rizík

- **Analýza rizík je povinnou súčasťou povinnej bezpečnostnej dokumentácie** podľa §2 Vyhlášky, ktorú prijíma prevádzkovateľ základnej služby.
- Pre kategóriu II a III sietí a informačných systémov sa postupuje minimálne podľa § 6 Vyhlášky (Riadenie aktív, hrozieb a rizík).
- Metodicky pre výpočet rizika je možné postupovať napr. podľa ISO/IEC 27005.
- **Vykonanie analýzy rizík je súčasťou riadenia rizík** nad identifikovanými aktívami. Proces riadenia sa realizuje v krokoch:
  - Identifikácia zraniteľností a hrozieb
  - Určenia rizika
  - **Určenie a implementácia opatrení**
  - Pravidelné opätovné preskúmanie rizík

Krok #5: Zadokumentovanie bezpečnostných opatrení

- zadokumentované vymedzenie rozsahu a spôsobu plnenia všetkých bezpečnostných opatrení je **povinnou súčasťou bezpečnostnej dokumentácie** podľa §2 Vyhlášky
- Východiská:
  - výsledky vykonanej analýzy rizík
  - niektorý z rámcov riadenia bezpečnostnej architektúry (štandardy ISO/IEC 27000 napr. ISO/IEC 27002, štandardy FIPS/NIST napr. NIST SP 800-37 alebo napr. výnos č. 55/2014 Z.z. o štandardoch pre informačné systémy verejnej správy)
  - minimálne požiadavky na bezpečnostné opatrenia v závislosti od kategorizácie podľa prílohy č.3 Vyhlášky

Krok #6 Spracovanie bezpečnostných politík kybernetickej bezpečnosti

B: Štruktúra bezpečnostnej politiky kybernetickej bezpečnosti

Bezpečnostné politiky	Súvisiace bezpečnostné štandardy
1. Organizácia bezpečnosti	– Riadenie bezpečnostnej architektúry – Systém riadenia kybernetickej bezpečnosti – Riadenie identít a prístupových práv – Riadenie privilegovaných prístupov – Bezpečnostný monitoring a správa bezpečnostných záznamov
2. Riadenie bezpečnostných rizík	– Testovanie a bezpečnostná certifikácia systémov – Metodika posudzovania vplyvu na ochranu osobných údajov – Metodika posudzovania rizík – Fyzická bezpečnosť a bezpečnosť prostredia – Riešenie bezpečnostných incidentov
3. Riadenie informačných aktív	– Klasifikácia informácií a kategorizácia sietí – Registratúrny poriadok a registratúrny plán
4. Pravidlá správania a dobrej praxe	– Práca na diaľku a používanie mobilných zariadení – Riadenie personálnej bezpečnosti – Pravidlá komunikácie
5. Riadenie dodávateľských vzťahov	– Riadenie dodávateľských služieb – Akvizícia informačných systémov
6. Riadenie vývoja a údržby v oblasti informačno-komunikačných technológií	– Vývoj a testovanie informačných systémov – Postupy údržby informačných systémov – Riadenie technických zraniteľností a manažment záplat
7. Riadenie a prevádzka informačno-komunikačných technológií	– Pravidlá prepájania systémov a prenosu elektronických informácií – Riadenie bezpečnosti sietí – Riadenie zmien infraštruktúry – Riadenie kapacity systémov a služieb – Riadenie kryptografických opatrení
8. Riadenie súladu	– Audit kybernetickej bezpečnosti – Spracúvanie osobných údajov a klasifikovaných informácií – Poskytovanie súčinnosti tretím stranám
9. Riadenie kontinuity procesov a činností	– Plány kontinuity prevádzkových činností – Plány havarijnej obnovy prevádzky – Metodika zálohovania a obnovy informácií

#7 Presadzovanie stratégie kybernetickej bezpečnosti

- Kontinuálny proces:
  - riadenia aktív
  - riadenia rizík
  - prevádzky a presadzovania bezpečnostných opatrení
  - overovania stavu kybernetickej bezpečnosti
  - revízie bezpečnostnej dokumentácie

Úloha a cieľ “certifikačného” auditu podľa Zákona o kybernetickej bezpečnosti

Posúdenie

- plnenia povinností **prevádzkovateľa základnej služby** podľa Zákona
- zhody prijatých bezpečnostných opatrení podľa Zákona a osobitných predpisov (najmä Vyhláška) **pre siete a informačné systémy základnej služby a pre tie, ktoré podporujú základné služby**

Cieľ auditu

- Identifikácia nedostatkov pri zabezpečovaní kybernetickej bezpečnosti prevádzkovateľom základnej služby pre prijatie opatrení na ich odstránenie a nápravu a na predchádzanie kybernetickým bezpečnostným incidentom.


ESET Services

Bezpečnostné služby pre zabezpečenie súladu so Zákonom

- **Interný audit kybernetickej bezpečnosti v organizácii:**
  - poskytnutie výkonu interného auditu pre overovanie stavu kybernetickej bezpečnosti a prítomnosti kontrolnej role pri riadení kybernetickej bezpečnosti podľa požiadavky Zákona.
- **Posúdenie súladu organizácie so Zákonom na identifikáciu a odstránenie nedostatkov.** Posúdenie vykonávame službami**:**
  - vstupná analýza a overenie súladu bezpečnostnej dokumentácie, procesov a opatrení so Zákonom;
  - detailná analýza presadzovania prijatej stratégie kybernetickej bezpečnosti.

Ďakujem za pozornosť

Kontakt pre vaše otázky a požiadavky

e-mail: services@eset.sk
https://www.eset.com/sk/firemna-it-bezpecnost/bezpecnostne-sluzby/services/kontakt/