Novela zákona o kybernetické bezpečnosti

Adam Kučínský

Národní bezpečnostní úřad

Národní centrum kybernetické bezpečnosti

4. dubna. 2017

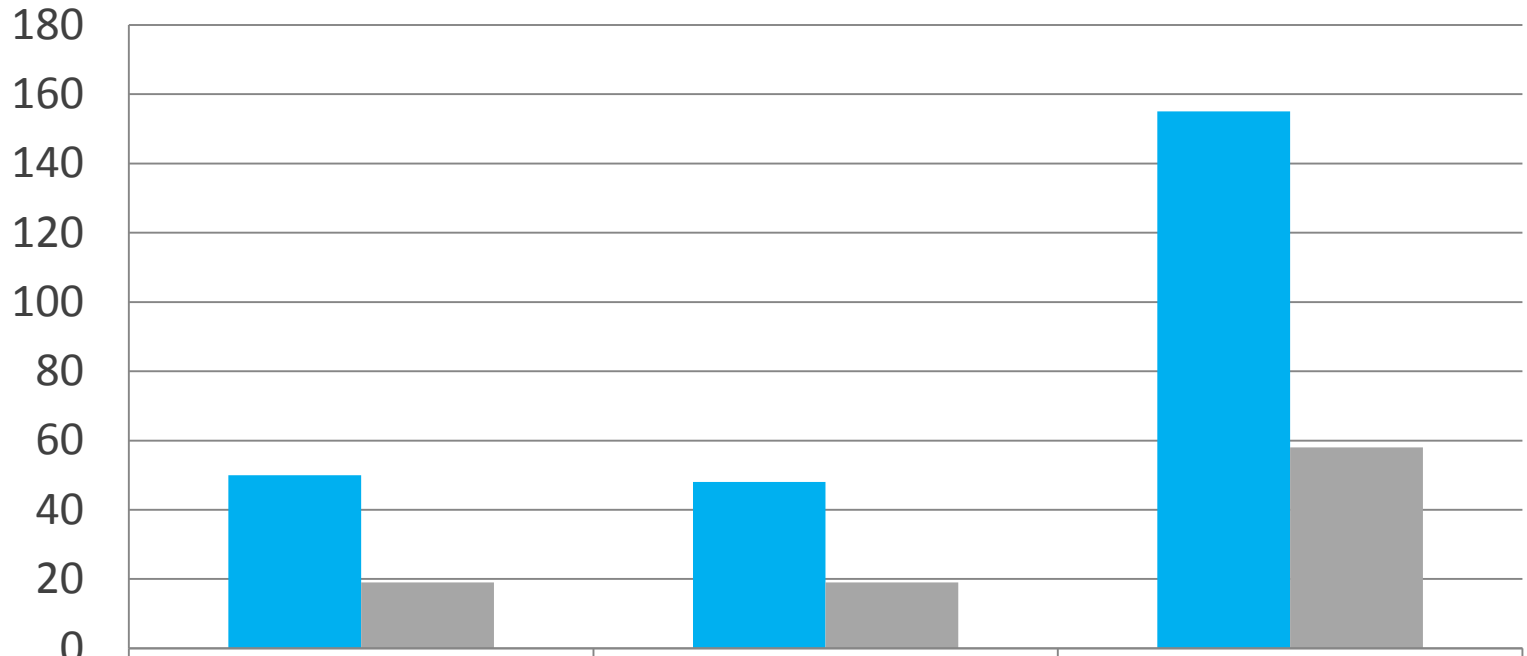
ZKB - cíle právní úpravy

- Stanovit základní úroveň bezpečnostních opatření
- Zlepšit detekci a zavést hlášení kybernetických bezpečnostních incidentů
- Zavést systém opatření k reakci na kybernetické bezpečnostní incidenty
- Upravit činnost dohledových pracovišť
- **Cíle „velké“ novely:**
  - Transpozice Směrnice Evropského parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, (směrnice NIS)
  - Odstranění některých nedostatků současné úpravy
- **Probíhá ještě „malá“ novela – zák. č. 365/2000 Sb.**
  - Nový pojem provozovatel IS/KS, ustanovení o vlastnictví a předávání dat, hlášení incidentů provozovatelem, změny správních deliktů

Jak se daří ZKB naplňovat?

- Kybernetické bezpečnostní incidenty
  - Měsíčně hlášeno cca 30 incidentů, dalších cca 50 identifikuje GovCERT sám
- Počet KII – 98 systémů u 38 subjektů
  - z toho 50 systémů v soukromém sektoru a 48 ve veřejném
- Počet VIS – 155 systémů u 50 subjektů
- Celkem pod ZKB spadá 253 systémů ve správě 84 subjektů
- Audity/Kontroly plnění povinností
  - Od roku 2016 provedeno 15 auditů/kontrol správců KII/VIS
- Mnoho dalších aktivit
  - Kybernetická cvičení, mezinárodní spolupráce, EU agendy, vzdělávání…

KII/VIS v číslech



	KII - soukromý sektor	KII - veřejný sektor	VIS
Počet systémů	50	48	155
Počet správců	19	19	58

Legislativa KB – současnost vs. budoucnost

- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti („ZKB“)
  - *Probíhá novelizace – třetí čtení*
  - *Předpokládaná účinnost srpen/září 2017*
- Vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti („VKB“)
  - *Bude novelizována (povinnosti rozšiřovány/měněny nebudou)*
  - *Termín předložení LRV – říjen 2017, předpoklad. účinnost - leden 2018*
- Vyhláška č. 317/2014 Sb., o významných informačních systémech
  - *Beze změny*
- Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku KI
  - *Beze změny*
- **Nová vyhláška o poskytovatelích základních služeb (určovací kritéria)**
  - *Termín předložení LRV – srpen 2017*
  - *předpokládaná účinnost – říjen 2018*

Struktura povinných podle ZKB – současnost

- §3 ZKB

a) Poskytovatel služeb el. komunikací, subjekt zajišťující síť el. komunikací,
   - ISP

b) Orgán nebo osoba zajišťující významnou síť
   - ISP pro KII, přímé zahraniční připojení

NÁRODNÍ CERT

c) Správce IS KII

d) Správce KS KII
   - Systémy důležité pro chod státu, bezpečnost, kritické služby

e) Správce VIS
   - Systémy státní správy - orgánů veřejné moci

VLÁDNÍ CERT

Struktura povinných podle ZKB – současnost vs. budoucnost

- §3 NZKB

a)	poskytovatelé služeb elektronických komunikací, subjekt zajišťující sít elektronických komunikací	NÁRODNÍ CERT
b)	orgán nebo osoba zajišťující významnou síť	
c)	**Poskytovatel digitálních služeb**	
d)	správce ***a provozovatel*** IS KII	VLÁDNÍ CERT
e)	správce ***a provozovatel*** KS KII	
f)	správce ***a provozovatel*** VIS	
g)	**správce a provozovatel IS základní služby**	
h)	**provozovatel základní služby**	

Co směrnice NIS reguluje a jaké povinnosti přináší

- Směrnice NIS byla přijata 6. července 2016, platná je od srpna 2016
- Směrnice stanovuje opatření pro bezpečnost sítí a informačních systémů v rámci Unie s cílem zlepšit fungování vnitřního trhu
- Státy musí přijmout národní strategii pro bezpečnost sítí a IS
- Státy musí určit vnitrostátní příslušné orgány pro oblast regulace, jednotná kontaktní místa a týmy CSIRT
- Státy musí určit **provozovatele základních služeb (PZS)** - do 9. 11 2018
- Směrnice přímo definuje **poskytovatele digitálních služeb (DSP)** – povinnost zapracovat do právního řádu
- PZS a DSP povinnost zavést bezpečnostní opatření a hlásit incidenty
- Směrnice dále ustavuje síť skupin pro reakci na incidenty (CSIRT) a skupinu pro spolupráci na úrovni EU

Průběh transpozice NIS na národní úrovni

- ČR musí přijmout úpravu do 21 měsíců od vstupu směrnice v platnost – tedy nejpozději do května 2018

Příprava novely

- Březen 2016 – svolána prac. skupina na úrovni resortů
- Duben 2016 - vytvořena prac. skupina na úrovni odborné veřejnosti

Legislativní proces

- MPŘ: od 18. 7. do 15. 8. 2016 – cca 300 připomínek
- 23. 11. schváleno vládou
- Nyní po druhém čtení (proběhlo 14. 3.)
- Následuje Garanční Výbor pro bezpečnost (od 4. dubna)

Platnost a účinnost

- Předpokládaná platnost červen/červenec
- Předpokládaná účinnost srpen/září

➢ **Sněmovní tisk č. 984**

www.psp.cz

Směrnice NIS – povinné subjekty

- Směrnice zavádí dva druhy povinných subjektů

I. Provozovatelé základních služeb (PZS)

- Klíčové subjekty pro fungování společenských a ekonomických činností
- Určováni členskými státy na základě stanovených kritérií
- Kritéria rámcově stanovena směrnicí – dopady a odvětví
- Podobné KII – jsou zde ale rozdíly (PZS orientovány na vnitřní trh x KII na bezpečnost státu, kritéria KII plně nepokryjí kritéria pro PZS,…)

II. Poskytovatelé digitálních služeb (DSP)

- Regulováni nově
- Typově se jedná o vyhledávače, on-line tržiště, cloud computing
- Povinnosti jsou mírnější než u PZS - princip maximální harmonizace

Provozovatel základní služby (PZS) - definice

- **Základní služba** = služba, jejíž poskytování **je závislé na sítích nebo informačních systémech** a jejíž narušení by mohlo mít významný dopad na zabezpečení činností v některém z těchto odvětví:

1. energetika
2. doprava
3. bankovnictví
4. infrastruktura finančních trhů
5. zdravotnictví
6. vodní hospodářství
7. digitální infrastruktura
8. chemický průmysl

- **Informační systém základní služby** = systém, na jehož fungování je závislé poskytování základní služby
- **Provozovatel základní služby** = orgán nebo osoba odpovědná za poskytování základní služby a určená NBÚ

Určování provozovatelů základních služeb (PZS)

- PZS budou určováni rozhodnutím (dle SŘ) vydaným NBÚ
- Určující kritéria stanoví prováděcí vyhláška k ZKB (účinnost říjen 2017)
  - Zveřejněny teze vyhlášky, na finální podobě se pracuje
  - Konkrétní nastavení kritérií – pracovní skupina z řad soukromé i státní sféry (13 podskupin dle odvětví a pododvětví)
- Pro určení bude nutné naplnit jak dopadová tak odvětvová kritéria
  - Odvětví budou kopírovat NIS (+ chemický průmysl)
  - Dopadová kritéria budou respektovat požadavky směrnice a zohledňovat národní podmínky
- Kritéria budou nastavena tak, aby regulace pokryla pouze systémy nezbytné pro zajištění služeb (ne fakturační, marketingové systémy ani např. bankomaty)

Určování PZS – dopadová kritéria

- Dopadová kritéria pro určování PZS by mohla vypadat následovně:

Narušení bezpečnosti informací a dat (C-I-A) v informačním systému nebo síti elektronických komunikací způsobí:	
a) omezení základní služby postihující více než 50 000 osob	e) oběti na životech s mezní hodnotou více než 100 mrtvých nebo 1000 zraněných osob
b) omezení či narušení jiné ZS, nebo omezení či narušení provozu prvku KI	f) mimořádnou událost ve smyslu zákona o integrovaném záchranném systému
c) hospodářskou ztrátu vyšší než 0,25 % HDP	g) kompromitaci citlivých údajů o 200 000 osobách
d) nedostupnost služby, která není nahraditelná jinou službou	

- Mnoho vitálních systémů již určeno jako KII – nepředpokládáme výrazné množství PZS (výjimky - např. zdravotnictví)
- V případě, že systém naplní kritéria pro PZS i KII – určí se jako KII

Odvětví PZS podle NIS: I. Energetika

- Pododvětví Elektřina
  - elektroenergetický podnik
  - provozovatel distribuční a přenosové soustavy
- Pododvětví Ropa
  - provozovatel ropovodů
  - provozovatelé zařízení na zpracování, rafinaci a úpravu ropy a skladovacích a přenosových zařízení
- Pododvětví Zemní plyn
  - fyzická nebo právnická osoba, která provádí dodávky
  - provozovatel distribuční a přepravní soustavy
  - provozovatel skladovacího zařízení
  - provozovatel zařízení LNG
  - plynárenský podnik a provozovatel zařízení na rafinaci a úpravu plynu

Odvětví PZS podle NIS: II. Doprava

- Pododvětví Letecká doprava
  - letečtí dopravci
  - letiště
  - řízení letového provozu
- Pododvětví Železniční doprava
  - provozovatelé infrastruktury
  - železniční podniky
- Pododvětví Vodní doprava
  - podniky vnitrozemské, námořní a pobřežní osobní a nákladní vodní dopravy
  - řídící orgány přístavů
- Pododvětví Silniční doprava
  - silniční orgány a provozovatelé inteligentních dopravních systémů

*Zde **KII** prozatím **neurčena***

*Zde **KII** prozatím **neurčena***

Odvětví PZS podle NIS:
III. Bankovnictví, IV. Infrastruktura finančních trhu

- Bankovnictví
  - úvěrové instituce (podnik, jehož činnost spočívá v přijímání vkladů nebo jiných splatných peněžních prostředků od veřejnosti a poskytování úvěrů na vlastní účet)
- Infrastruktura finančních trhů
  - provozovatelé obchodních systémů (regulovaný trh, mnohostranný obchodní systém nebo organizovaný obchodní systém)
  - ústřední protistrana (právnická osoba, která vstupuje mezi strany smluv uzavíraných na jednom či na několika finančních trzích, a stává se tak kupujícím pro každého prodávajícího a prodávajícím pro každého kupujícího)

*Zde **KII** prozatím **neurčena***

Odvětví PZS podle NIS:
V. Zdravotnictví, VI. Vodní hospodářství

- Zdravotnictví - poskytovatelé zdravotní péče
  - poskytovatel zdravotní péče = fyzická nebo právnická osoba nebo jiný subjekt, který zákonným způsobem poskytuje zdravotní péči na území členského státu

*Zde **KII** prozatím **neurčena***

- Vodní hospodářství
  - Výrobce, dodavatel a distributor pitné vody a subjekt zajišťující odvod a čištění odpadních vod

Odvětví PZS podle NIS:
VII. Digitální infrastruktura, VIII. Chemický průmysl

- Digitální infrastruktura
  - Výměnné uzly internetu
  - Poskytovatelé služeb systému doménových jmen
  - Rejstříky internetových domén nejvyšší úrovně

KII** prozatím **neurčena úplně

- Chemický průmysl
  - Na kritériích se pracuje
  - Podniky zpracovávající nebezpečné či strategické suroviny

Provozovatel základní služby (PZS) – povinnosti

- NIS stanovuje následující okruhy povinností pro PZS:
  - Přijmout technická a organizační opatření k řízení rizik
  - Přijmout opatření k předcházení incidentům narušujícím bezpečnost
  - Oznamovat incidenty včetně případných přeshraničních dopadů
  - Poskytovat regulační autoritě součinnost k posouzení bezpečnosti
  - Provádět nápravu zjištěných nedostatků
- Povinnosti budou stejné jako u KII (specifikuje vyhl. č. 316/2014)
- KII má navíc povinnosti vyplývající z krizového zákona
- PZS bude regulována jako samostatná kategorie - nebude zahrnuta pod krizový zákon

Poskytovatel digitálních služeb (DSP) - definice

- Poskytovatel digitální služby poskytuje službu:
  - **On-line tržiště** - umožňuje on-line uzavírat kupní smlouvu nebo smlouvu o poskytnutí služeb prostřednictvím internetové stránky on-line tržiště nebo prostřednictvím internetové stránky prodávajícího, která využívá službu on-line tržiště
  - **Internetového vyhledávače**
  - **Cloud computingu** - umožňuje přístup k rozšiřitelnému a přizpůsobitelnému úložišti výpočetních zdrojů, jež je možno sdílet
    - Tyto definice vycházejí přímo ze směrnice
- Regulace se <u>netýká malých a mikro podniků</u>
  - (>50 zaměstnanců a roční bilanční suma nebo obrat >10 mil. €)
- Funguje zde <u>princip samourčení</u> – naplnění definice = povinná osoba

Poskytovatel digitálních služeb (DSP) – povinnosti

- **§ 4 odst. 3 NZKB:** zavést a provádět vhodná a přiměřená bezpečnostní opatření pro sítě a IS, využívané k poskytování služby
- **§ 8 odst. 2 NZKB:** hlásit kybernetický bezpečnostní incident s významným dopadem na poskytování jeho služeb NCERTu
- **§ 16 odst. 2 písm. h) NZKB:** oznamovat kontaktní údaje NCERTu
- Uplatňuje se princip maximální harmonizace – povinnosti nad rámec NIS se neukládají, kontrola pouze při podezření neplnění požadavků
- Opatření musejí odpovídat „míře existujícího rizika“
  - **Minimální bezp. opatření pro DSP:** *Technical Guidelines for the implementation of minimum security measures for Digital Service Providers* (ENISA, prosinec 2016)

https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers

NIS x ZKB – srovnání požadavků z pohledu ČR

Směrnice NIS	Zákon o kybernetické bezpečnosti	
• Národní strategie bezpečnosti sítí a informací	• Národní strategie kybernetické bezpečnosti	✓
• Zavádí požadavky na bezpečnost a oznamování incidentů	• Povinnost zavést bezp. opatření a hlásit incidenty	✓
• Ustavuje síť skupin pro reakci na incidenty (CSIRT)	• Zakotvil činnosti Vládního a Národního CERT	✓
• Povinnost zřídit vnitrostátní orgány, které budou mít bezpečnost sítí a IS v gesci	• NBÚ gestorem Kybernetické bezpečnosti	✓
• Určit jednotné kontaktní místo v regulované oblasti	• NBÚ je kontaktním místem pro nár. i mezinár. spolupráci v oblasti KB	✓
• Určení PZS	• Částečně zavedeno (KII)	⚠
• Určení DSP	• Nezavedeno	✗

Přehled povinností podle novely ZKB

- Nahlášení kontaktních údajů (§16 ZKB)
  - Všechny povinné osoby, **nově i DSP a PZS**
- Hlášení kybernetických bezpečnostních incidentů (§8 ZKB)
  - KII, VIS, významné sítě, **nově i DSP a PZS**
- Zavedení bezpečnostních opatření (standardizace) (§4 ZKB)
  - KII, VIS, **nově i PZS, DSP pouze některá opatření**
- Činit opatření vydané NBÚ (§11 ZKB)
  - KII, VIS, **nově i PZS**
  - Významné sítě a poskytovatelé služby el. komunikací pouze za stavu kybernetického nebezpečí, pouze reaktivní opatření

Co dále přináší „velká“ novela ZKB – dodav. vztahy I.

- KII, VIS a PZS kteří jsou orgánem veřejné moci, jsou povinni si s poskytovatelem cloud computingu smluvně ošetřit vlastnictví dat a možnost jejich kontroly
- Budou nutné úpravy některých smluv – ustanovení o vlastnictví informací a dat + ustanovení ohledně kontroly informací a dat
- Důvod úpravy
  - Ve smlouvách často chybí ustanovení ohledně vlastnictví dat
  - Nemožnost kontrolovat data, informace a bezpečnostní opatření ze stany vlastníka/správce
- Dále zákon uvádí povinné náležitosti smluv orgánů veř. moci určených jako KII/VIS/PZS s poskytovateli cloud computing. služeb

Co dále přináší „velká“ novela ZKB – dodav. vztahy II.

- **§ 4 odst. 5 NZKB**: povinné náležitosti smluv OVM (KII/VIS/PZS) s CC:
  a) zakotvení povinnosti poskytovatele služeb respektovat bezpečnostní politiky odběratele služeb,
  b) stanovení úrovně poskytovaných služeb,
  c) systém schvalování subdodavatelů služby cloud computingu,
  d) specifikace podmínek ukončení smlouvy z pohledu bezpečnosti,
  e) řízení kontinuity činností v souvislosti s poskytovanou službou cloud computingu,
  f) určení vlastníka uchovávaných dat,
  g) dohoda o důvěrnosti,
  h) stanovení úrovně ochrany dat z pohledu důvěrnosti, dostupnosti a integrity,
  i) pravidla zákaznického auditu,
  j) informovat odběratele o incidentech souvisejících s plněním smlouvy.

Co dále přináší „velká“ novela ZKB

- **§ 3a**: pokud DSP nemá zástupce v členském státu EU musí jej zřídit
- **§4a odst. 2**: Pokud KII, VIS nebo PZS není provozovatelem svého systému, musí provozovatele informovat o tom, že IS/KS byl určen
- **§4a odst. 2**: KII musí informovat své ISP o tom, že se tito ISP stávají významnou sítí
- **§ 12 odst. 3**: Právo NBÚ informovat veřejnost o incidentu (veř. zájem)
- **§ 25**: Změna sankcí za správní delikty a zavedení nových deliktů
- **§ 10a**: Průlom zákona o svobodném přístupu k informacím

Co dále přináší „malá“ novela ZKB – exit strategie

- **§ 6a odst. 1:** možnost pověřit jiného provozem KII/VIS, pokud to nevylučuje jiný zákon
- **§ 6a odst. 2:** povinnost provozovatele KII/VIS předat správci data, provozní údaje a informace které má v souvislosti s provozem KII/VIS
- **§ 6a odst. 3**: úprava předání a ničení dat v mezi správcem a provozovatelem KII/VIS v případě ukončení spolupráce
  - Povinnost provozovatele předat v dohodnutém formátu data, provozní údaje a informace související s provozem KII/VIS
  - Povinnost provozovatele tato data a informace po předání zničit
  - Povinnost umožnit správci dohled nad ničením
- **§ 6a odst. 4:** právo provozovatele požadovat úhradu nákladů spojených s výše uvedeným a povinnost správce je uhradit

Co dále přináší novela ZKB – předávání dat

- **§ 15a:** Pravomoc Úřadu na návrh správce KII/VIS v případě hrozícího incidentu uložit provozovateli systému předat data, provozní údaje a informace spojené se systémem
  - Poměrně přesně stanoveny podmínky, za kterých je to možné

- **§ 17/1 písm. l a § 20 písm. l:** Národnímu i Vládnímu CERTU doplněna možnost přijímat hlášení o KBI i od jiných než povinných osob
  - Pokud budou mít kapacity – povinné osoby jsou upřednostněny
  - V zásadě se nic nemění – N i V CERT to činí již nyní

Co dále přináší novela ZKB - přestupky - § 25

- Změn poměrně dost – § 25 má nyní 3 odstavce, novela jich má 12
  - Zavedení nových přestupků
  - Změna výše sankcí za správní delikty – zvyšují se pokuty
    - z max. 100 000 Kč na max. 1 000 000/5 000 000, spodní hranice nestanovena

Povinnost	Sankce	Povinná osoba
Neplnění povinnosti při SKB, nápravných opatření, rozhodnutí, nepředání dat	1000 K	Síť el. komunikací, významná síť
Nebude mít smluvně ošetřené vlastnictví, ničení a předání dat	1000 K	KII, VIS
Nehlásí incidenty, neplnění rozhodnutí, nezveřejnění informací	1000 K	Významná síť, KII, VIS, PZS
Nezavede bezp. opatření	5000 K	KII,VIS, PZS
Neustaví si zástupce, neprovádí bezp. opatření, nehlásí incidenty, neplní uložené povinnosti NBÚ	1000 K	DSP
Hlášení kontaktních údajů	10 K	Všichni
Nepředá data, nezničí data/nespolupracuje při určování	200 K	Dodavatelé/PZS

Kontrola plnění povinností ZKB - průběh

- Kontroly zahájeny začátkem roku 2016
  - provedeno 15 kontrol, zkontrolováno 24 systémů
- Kritérium kontroly – ZKB a vyhláška č. 316/2014 Sb.
- Průběh kontroly
  - Subjekt obdrží oznámení o plánované kontrole a „Průvodce kontrolou“
  - Kontrole na místě může přecházet přezkoumání dokumentace (případně je provedeno na místě)
  - Délka kontroly na místě se pohybovala v rozmezí 2 až 4 dnů
  - Na konci kontroly je vypracován „Protokol o kontrole“ obsahující:
    - Základní informace o kontrole, manažerské shrnutí, kontrolní zjištění, termíny pro zavedení nápravných opatření, poučení, přílohy – program kontroly atd.
    - Protokol je standardně předán poslední den kontroly

Kontrola plnění povinností ZKB - nejčastější zjištění I.

- Systém řízení bezpečnosti informací
  - Chybějící podpora vedení
  - Nezpracované/neúplné/neschválené/neřízené/nedodržované bezp. politiky
- Řízení aktiv a rizik
  - Chybějící metodiky pro řízení aktiv a rizik
  - Nejednotný proces řízení rizik v rámci organizace
  - Chybějící prohlášení o aplikovatelnosti a plán zvládání rizik
- Organizační bezpečnost
  - Bezpečnostní role neustanoveny / nemají přiděleny dostatečné kompetence
- Aplikační bezpečnost
  - Neprováděny bezpečnostní testy zranitelnosti aplikací přístupných z vnějšku

Kontrola plnění povinností ZKB - nejčastější zjištění II.

- Řízení dodavatelů
  - Smlouvy nerespektují zákonné požadavky
  - Řízení přístupových oprávnění dodavatelů ke službám
  - Správa privilegovaných účtů
- Audit kybernetické bezpečnosti
  - Neprovádění auditu KB
- Řízení identit
  - Chybné/nedostatečné procesy správy uživatelských účtů (např. odebírání přístupů s souvislosti s životním cyklem zaměstnanců)
  - Síla hesel
- Řízení kontinuity činností
  - Plán kontinuity/havarijní plán neexistuje, je neúplný, není otestován

Děkuji za pozornost

Adam Kučínský

Národní bezpečnostní úřad

Národní centrum kybernetické bezpečnosti

nbu.cz

govcert.cz

Užitečné odkazy

- Blokové schéma k zákonu o kybernetické bezpečnosti: http://www.govcert.cz/cs/kii--vis/kii--vis/
- Proces určování kritické informační infrastruktury: http://www.govcert.cz/cs/kii--vis/kriticka-informacni-infrastruktura/
- Proces určování významných informačních systémů: http://www.govcert.cz/cs/kii--vis/vyznamne-informacni-systemy/
- Pomůcka k auditu/kontrole bezpečnostních opatření podle zákona: http://www.govcert.cz/cs/kii--vis/dalsi-materialy-ke-stazeni/
- Výkladový slovník kybernetické bezpečnosti - třetí vydání: http://www.govcert.cz/cs/informacni-servis/vykladovy-slovnik/
- **Návrh novely zákona o KB** (Sněmovní tisk č. 984): http://www.psp.cz/sqw/historie.sqw?o=7&t=984
- **Směrnice NIS v ČJ** (Úřední věstník EU, 19. 7. 2016, L194): http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=OJ:L:2016:194:FULL&from=EN