Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti

Ing. Tomáš Krejčí
Odbor regulace, auditu a podpory

Národní úřad
pro kybernetickou
a informační bezpečnost

Nová VKB - průběh prací

- **Svolání expertního týmu (ET),**
  - 7. 6. – 3. 10. 2017,
  - celkem 11 schůzí ET, vždy na min. 4 hodiny,
  - souběžná spolupráce s vládním CERT.
- **06. 10. 2017 - Zpřístupnění nové (neoficiální) verze VKB veřejnosti.**
- **31. 10. 2017 - Zpracování připomínek finalizace VKB za RAP.**
- **20. 12. 2018 - Poslední jednání ET.**
- **15. 01. 2017 - Předání VKB právnímu oddělení NÚKIB, finalizace za NÚKIB.**
- **Legislativní proces,**
  - 16. 02. 2018 MPŘ,
  - 30. 4. 2018 komise LRV,
  - 14. 5. 2018 finalizace VKB na NÚKIB.
- **21. 05. 2018 - Nová VKB podepsána ředitelem úřadu.**
- **28. 05. 2018 - Účinnost nové vyhlášky.**

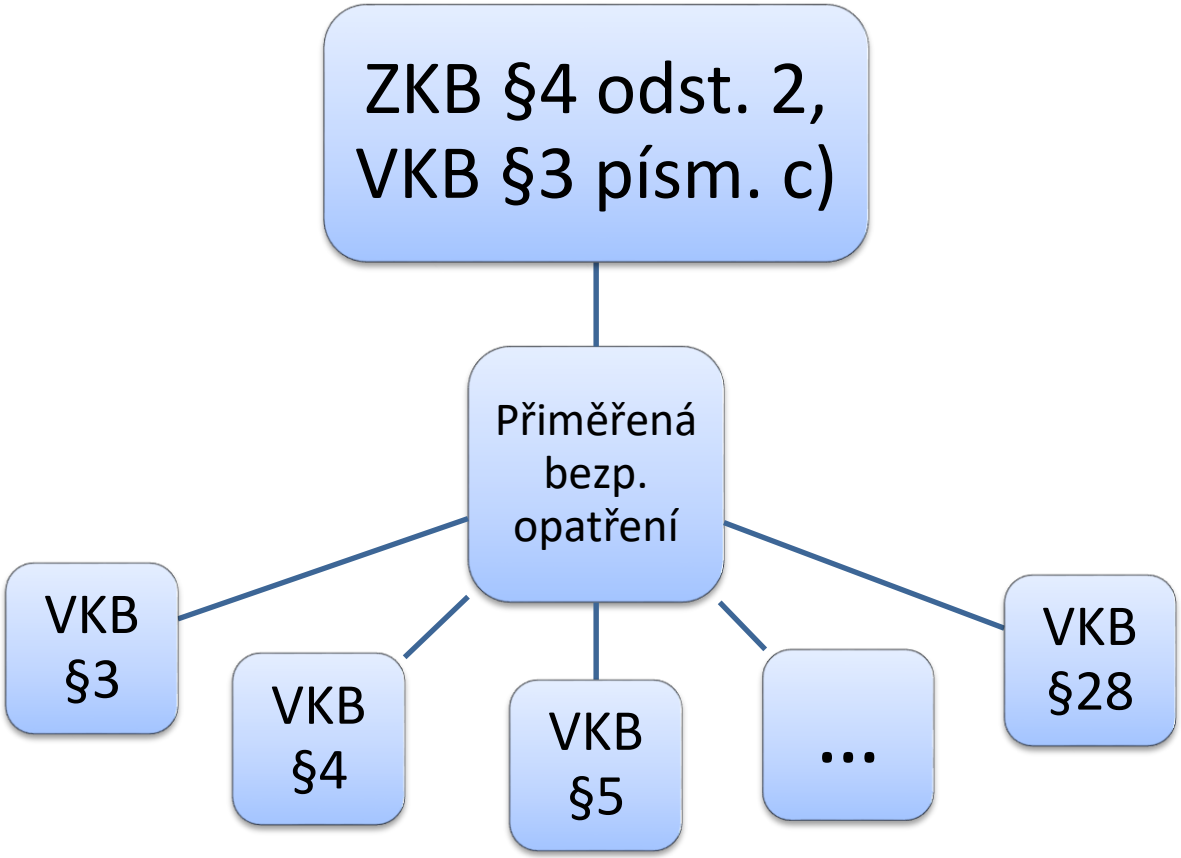
Nová VKB - co bude jinak?

- Pořadí některých paragrafů,
- úprava formulací,
  - odstranění duplicit,
  - přeformulování názvů některých paragrafů,
    - Nástroj pro ochranu před škodlivým kódem X Ochrana před škodlivým kódem,
  - změny povinností,
    - zejména zmenšení rozdílu mezi KII, PZS a VIS.
- logické úpravy některých povinností,
  - zjednodušení, odstranění, přidání,
- větší soulad s „best practice“
  - požadavky i terminologie.

Bezpečnostní opatření

- Co je bezpečnostní opatření?
  - **ZKB §4 odst. 1)** Bezpečnostním opatřením se rozumí **souhrn úkonů**, jejichž cílem je **zajištění bezpečnosti informací v informačních systémech** a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru.
- Implementace
  - **ZKB §4 odst. 2)** Orgány a osoby uvedené v § 3 písm. **c) až f)** jsou povinny **zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti** informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury, informačního systému základní služby a významného informačního systému a vést o nich bezpečnostní dokumentaci.
- Princip VKB (§3 ≈ ČSN ISO/IEC 27001 kap. 4 – 10)
  - **VKB §3 písm. a)** stanoví s ohledem na požadavky dotčených stran a organizační bezpečnost rozsah systému řízení bezpečnosti informací, ve kterém určí organizační části a aktiva, jichž se systém řízení bezpečnosti informací týká, (ČSN ISO/IEC 27001 kap. 4)
  - **VKB §3 písm. b)** stanoví cíle systému řízení bezpečnosti informací, (ČSN ISO/IEC 27001 kap. 6)
  - **VKB §3 písm. c)** pro stanovený rozsah systému řízení bezpečnosti informací na základě cílů systému řízení bezpečnosti informací, bezpečnostních potřeb a hodnocení rizik zavede přiměřená bezpečnostní opatření, (ČSN ISO/IEC 27001 kap. 6 a příloha A, ČSN ISO/IEC 27002 kap. 5 - 18)

Bezpečnostní opatření



Plán zvládání rizik, Prohlášení o aplikovatelnosti

- **Plán zvládání rizik (Risk Treatment Plan (RTP)) obsahuje:**
  - cíle a přínosy bezpečnostních opatření pro zvládání rizik,
  - osoby zajišťující prosazování bezpečnostních opatření pro zvládání rizik,
  - potřebné zdroje,
  - termíny zavedení bezpečnostních opatření,
  - popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními.
- **Prohlášení o aplikovatelnosti (Statement of Applicability (SoA)) obsahuje:**
  - přehled zavedených a nezavedených bezpečnostních opatření,
  - způsoby zavedení bezpečnostních opatření,
  - důvody nezavedení bezpečnostních opatření.

Nejvýznamnější změny

Organizační opatření

- §3 Systém řízení bezpečnosti informací,
  - doplněny cíle ISMS,
  - Zrušena certifikace ISMS (§29 stará VKB).
- §4 Řízení aktiv,
  - změna pořadí paragrafů,
  - formulační změny.
- §5 Řízení rizik,
  - hrozby a zranitelnosti v nové příloze,
  - stará VKB na tomto paragrafu obsahovala politiky,
  - nově politiky v příloze.
  - SoA zavedená i nezavedená bezp. opatření
- §6 Organizační bezpečnost,
  - Cílí na vrcholové vedení a deklaraci podpory,
  - stanovení bezpečnostních rolí,
  - zastupitelnost bezpečnostních rolí,
    - KII a PZS manažera a architekta,
    - VIS pouze MKB.
- **§7 Bezpečnostní role,**
  - **požadavky na bezpečnostní role,**
  - **provázáno s nepovinnou přílohou č. 6.**
- §8 Řízení dodavatelů,
  - významný dodavatel,
  - oblasti, které je nutné ošetřit ve smlouvě s význ. dodavateli příloha č. 7,
  - speciální požadavky pro významné dodavatele,
  - náležitosti prokazatelného informování významného dodavatele (provozovatele) správcem.

Nejvýznamnější změny

- §9 Bezpečnost lidských zdrojů,
  - předání odpovědností u administrátorů a bezpečnostních rolí,
  - větší důraz kladen i na praktická školení.
- §10 Řízení provozu a komunikací,
  - zjednodušení paragrafu,
  - v Současné VKB mírně roztříštěný paragraf.
- **§11 Řízení změn,**
  - **Nastavení procesu řízení změny,**
  - **významné změny,**
  - **u významné změny se o penetrační testování a testování zranitelností rozhoduje na základě AR.**
- §12 Řízení přístupu,
  - omezení přidělování privilegovaných účtů.
- §13 Akvizice vývoj a údržba,
  - požadován 2FA při tvorbě projektu na vývoj nástroje pro správu a ověřování identity
- §14 Zvládání kybernetických bezpečnostních událostí a incidentů
  - Bez významné změny
- §15 Řízení kontinuity činností,
  - změny ve formulaci nyní v souladu s normou BCM,
    - minimální úrovně poskytovaných služeb, která je přijatelná pro užívání, provoz a správu informačního a komunikačního systému,
    - doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb informačního a komunikačního systému, a
    - bodu obnovení dat jako časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání.

Nejvýznamnější změny

- §16 Audit kybernetické bezpečnosti,
  - nově i při významných změnách,
  - KII a PZS v intervalu alespoň po 2 letech,
  - v celém rozsahu nejpozději do 5 let,
  - provozovatel musí předat výsledky auditu správci.

Technická opatření

- §17 Fyzická bezpečnost,
  - Zjednodušení.
- §18 Bezpečnost komunikačních sítí,
  - segmentace,
  - řízení na perimetru,
  - již se nepoužívá vnitřní a vnější síť,
  - aktivně se blokuje nežádoucí komunikace.
- §19 Správa a ověřování identit,
  - 2 FA,
  - kryptografické klíče,
  - jméno heslo,
  - do doby implementace požadavků může využít i jiné varianty,
  - délky hesel: uživatel: 12, admin.: 17
  - využití frází,
  - komplexita již není požadována,
  - inspirace v NIST SP 800-63B,
  - změna nutná po 18 měsících,
  - výchozí hesla nutná změna,
  - hesla k obnovení přístupu pouze dočasná platnost.
- §20 Řízení přístupových oprávnění,
  - Místo aplikacím a dat jsou řízena přístupová oprávnění k aktivům.

Nejvýznamnější změny

- §21 Ochrana před škodlivým kódem,
  - rozšířený seznam pro ochranu před škodlivým kódem,
    - koncové stanice,
    - mobilních zařízení,
    - servery,
    - datová úložiště a výměnné datové nosiče,
    - komunikační sítě a prvků komunikační sítě a
    - obdobná zařízení.
- §22 Zaznamenávání událostí IS a KS jeho uživatelů a administrátorů,
  - bezpečnostní a potřebné provozní události důležitých aktiv,
  - aktualizuje rozsah aktiv,
  - co je nutné zaznamenávat,
    - datum a čas včetně specifikace časového pásma,
    - typ činnosti,
    - identifikaci technického aktiva, které činnost zaznamenalo,
    - jednoznačnou identifikaci účtu, pod kterým byla činnost provedena,
    - jednoznačnou síťovou identifikaci zařízení původce a
    - úspěšnost nebo neúspěšnost činnosti,
  - typ činnosti,
    - přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů,
    - činností provedených administrátory,
    - úspěšné i neúspěšné manipulace s účty, oprávněními a právy,
    - neprovedení činností v důsledku nedostatku přístupových práv a oprávnění,
    - činností uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému,
    - zahájení a ukončení činností technických aktiv,
    - kritických i chybových hlášení technických aktiv a
    - přístupů k záznamům o událostech, pokusy o manipulaci se záznamy o událostech a změny nastavení nástrojů pro zaznamenávání událostí a

Nejvýznamnější změny

- KII a PZS uchovává tyto záznamy 18 měsíců
- VIS uchovává tyto záznamy 12 měsíců

- §23 Detekce KBU
  - Více specifikované pro KII a PZS
    - koncových stanic,
    - mobilních zařízení,
    - serverů,
    - datových úložišť a výměnných datových nosičů,
    - síťových aktivních prvků a
    - obdobných aktiv.
- §24 Sběr a vyhodnocování KBU (SIEM),
  - pro KII, PZS a pouze formulační změny.
- §25 Aplikační bezpečnost,
  - přidáno navíc penetrační testování zaměřené na důležitá aktiva,
    - před jejich uvedením do provozu,
    - v souvislosti s významnou změnou.
- §26 Kryptografické prostředky,
  - používá aktuálně odolné kryptografické algoritmy a kryptografické klíče,
  - používá systém správy klíčů a certifikátů,
  - místo přílohy: zohledňuje doporučení v oblasti kryptografických prostředků vydaná Úřadem, zveřejněná na jeho internetových stránkách.
- §27 Zajišťování úrovně dostupnosti informací,
  - formulační změny povinnosti zůstávají stejné.
- §28 Průmyslové, řídící a obdobné specifické systémy,
  - použití technických a programových prostředků, které jsou určeny do specifického prostředí,
  - vyčlenění komunikační sítě určené pro tyto systémy od ostatní infrastruktury,

Nejvýznamnější změny

- §29 Digitální služby,
  - odkaz na prováděcí nařízení komise (EU) 2018/151.
- §30 Bezpečnostní politika a bezpečnostní dokumentace,
  - oblasti jsou v příloze č. 5.
- §31 Kategorizace KBI.
- §32 Forma a náležitosti hlášení KBI.
- §33 Reaktivní opatření,
  - prověří dopady reaktivního opatření,
  - stanoví způsob rychlého provedení,
  - minimalizuje možné negativní účinky,
  - určí časový harmonogram provedení.
- §34 Kontaktní údaje,
  - přidán národní CERT.
- §35 Přechodná ustanovení,
  - rok na implementaci nové vyhlášky pro subjekty které již spadají pod ZKB,
    - v přechodném období se použije stará vyhláška,
  - přechodné období pro subjekty, které naplní kritéria pro KII, PZS nebo VIS po účinnosti NVKB je 1 rok,
  - Přílohy,
    - hodnocení aktiv,
    - hodnocení rizik,
    - zranitelnosti a hrozby,
    - likvidace dat,
    - obsah bezpečnostní politiky a bezpečnostní dokumentace,
    - bezpečnostní role,
    - řízení dodavatelů – bezpečnostní opatření pro smluvní vztahy,

příloha č.3 Zranitelnosti a hrozby

- Zranitelnosti:
  - nedostatečná údržba informačního a komunikačního systému,
  - zastaralost informačního a komunikačního systému,
  - nedostatečná ochrana vnějšího perimetru,
  - .
  - .
  - .
  - nedostatečná míra nezávislé kontroly.
- Hrozby:
  - poškození nebo selhání technického anebo programového vybavení,
  - zneužití identity,
  - nedostatek zaměstnanců s potřebnou odbornou úrovní,
  - .
  - .
  - .
  - cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik.

příloha č.4 Likvidace dat

- Jednotliví správci informačního a komunikačního systému si stanoví pravidla pro mazání dat a likvidaci technických nosičů dat v souladu s touto přílohou.
- Pravidla pro likvidaci dat by měla být stanovena přiměřeně hodnotě a důležitosti aktiv a měla by zejména zohledňovat,
  - hodnotu aktiva (zejména z pohledu důvěrnosti),
  - technologii (typy a velikost nosičů informace),
  - …
- Způsoby likvidace technických nosičů informace, provozních údajů, informací a jejich kopií,
  - odstranění,
  - přepsání,
  - fyzická likvidace nosiče informace.
- Příklad možných způsobů likvidace podle úrovně důvěrnosti aktiva.

Příloha č. 6

Role:	Architekt kybernetické bezpečnosti
Klíčové činnosti:	a) Odpovědnost za návrh implementace bezpečnostních opatření b) Zajišťování architektury bezpečnosti
Znalosti:	a) Architektura informačních a komunikačních systémů a její navrhování b) Hardwarové komponenty, nástroje a architektury c) Operační systémy a software d) Podnikové procesy a jejich integrace a závislost na ICT e) Řízení bezpečnosti a rizik f) Bezpečnost komunikací a sítí g) Řízení identit a přístupů h) Hodnocení a testování bezpečnosti i) Bezpečnost provozu j) Základní principy bezpečného vývoje softwaru k) Integrace a závislosti ICT a obchodních procesů
Zkušenosti:	a) Navrhování implementace bezpečnostních opatření b) Navrhování architektury bezpečnosti se zaměřením na cíle a bezpečnost c) Bezpečnost vývoje softwaru
Vzdělání a praxe:	a) Alespoň 3 roky praxe v oboru informační nebo kybernetické bezpečnosti, nebo b) Absolvování studia ve studijním programu na vysoké škole a alespoň 1 rok praxe v oboru informační nebo kybernetické bezpečnosti
Relevantní certifikace*:	Certified Ethical Hacker (CEH), CompTIA Security +, Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), Certified Information Systems Security Professional (CISSP), Manažer BI (akreditační schéma ČIA)
Další podmínky:	Role není slučitelná s rolemi odpovědnými za provoz informačních a komunikačních systémů

příloha č.7 Řízení dodavatelů

- Obsah smlouvy uzavírané s významnými dodavateli:
  - ustanovení o bezpečnosti informací (z pohledu důvěrnosti, dostupnosti a integrity),
  - ustanovení o oprávnění užívat data,
  - ustanovení o autorství programového kódu, popřípadě o programových licencích,
  - ustanovení o kontrole a auditu dodavatele (pravidla zákaznického auditu),
  - ustanovení upravující řetězení dodavatelů, přičemž musí být zajištěno, že poddodavatelé se zaváží dodržovat v plném rozsahu ujednání mezi povinnou osobou a dodavatelem a nebudou v rozporu s požadavky povinné osoby na dodavatele,
  - ustanovení o povinnosti dodavatele dodržovat bezpečnostní politiky povinné osoby nebo ustanovení o odsouhlasení bezpečnostních politik dodavatele povinnou osobou,
  - ustanovení o řízení změn,
  - ustanovení o souladu smluv s obecně závaznými právními předpisy,
  - .
  - .
  - .
  - ustanovení o právu jednostranně odstoupit od smlouvy v případě významné změny kontroly nad dodavatelem nebo změny kontroly nad zásadními aktivy využívanými dodavatelem k plnění podle smlouvy a
  - ustanovení o sankcích za porušení povinností.

Děkuji za pozornost.

t.krejci@nukib.cz