Návrh vyhlášky
k zákonu o kybernetické bezpečnosti

Přemysl Pazderka
NCKB

Východiska

- ISO/IEC 27001:2005 – Systémy řízení bezpečnosti informací – Požadavky
- ISO/IEC 27002:2005 – Soubor postupů pro management bezpečnosti informací
- ISO/IEC 27001:2013 – Systémy řízení bezpečnosti informací – Požadavky
- ISO/IEC 27002:2013 – Soubor postupů pro opatření bezpečnosti informací
- ISO/IEC 20000-1:2011 – Řízení služeb – Požadavky na systém řízení služeb
- COBIT 5 for Information Security

Struktura vyhlášky

- Úvodní ustanovení
- Bezpečnostní opatření
  - Organizační opatření
  - Technická opatření
  - Bezpečnostní dokumentace
  - Certifikace ISMS
- Kybernetický bezpečnostní incident
- Protiopatření
- Kontaktní údaje
- Odborná kvalifikace osob
- Účinnost
- Přílohy

Přehled organizačních opatření

§ 3 Systém řízení bezpečnosti informací

§ 4 Řízení rizik

§ 5 Bezpečnostní politika

§ 6 Organizační bezpečnost

§ 7 Stanovení bezpečnostních požadavků pro dodavatele

§ 8 Řízení aktiv

§ 9 Bezpečnost lidských zdrojů

§ 10 Řízení provozu a komunikací

§ 11 Řízení přístupu a bezpečné chování uživatelů

§ 12 Akvizice, vývoj a údržba

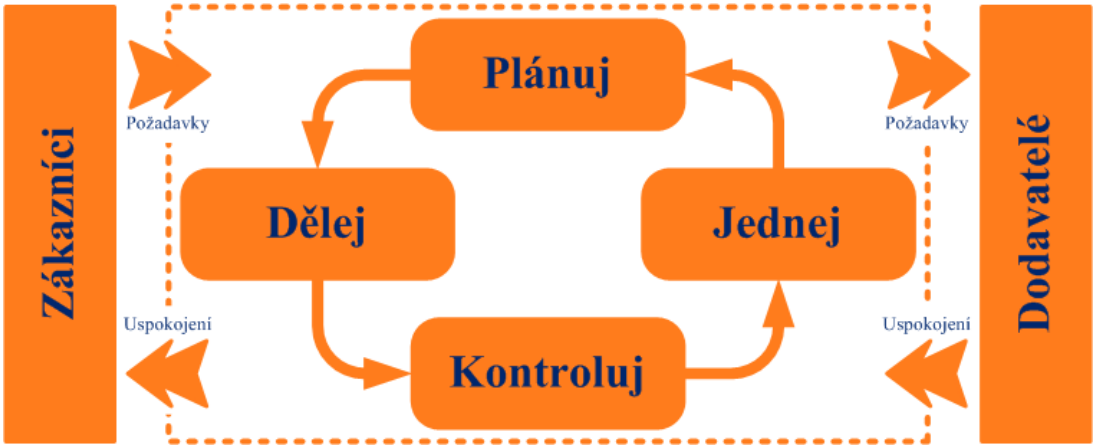
§ 13 Zvládání kybernetických bezpečnostních událostí a incidentů

§ 14 Řízení kontinuity činností

§ 15 Kontrola a audit

Systém řízení bezpečnosti informací

- Požadavky vychází z PDCA cyklu ISO/IEC 27001
- Pro KII požadován celý PDCA cyklus
- Pro VIS omezeny úkony v oblasti zpětné vazby
  - Pouze aktualizace existujících plánů



Řízení rizik

- KII - identifikace a hodnocení rizik aktiv KII
- VIS - identifikace a hodnocení rizik primárních aktiv VIS
- VIS+KII – určí a schválí zbytková rizika, vytvoří zprávu o hodnocení rizik a provádí její pravidelnou aktualizaci , vytvoří prohlášení o aplikovatelnosti , zpracuje a zavede plán zvládání rizik

Bezpečnostní politiky

- Výčet politik „není o“ počtu dokumentů, ale o počtu řešených oblastí kybernetické bezpečnosti
- VIS+KII - stanovení pravidel pro 10 základních oblastí kybernetické bezpečnosti (ISMS, aktiva, rizika, …)
- KII – rozšíření pravidel o dalších 11 oblastí kybernetické bezpečnosti (licencování SW, archivace, mobilní zařízení …)
- VIS+KII – hodnocení účinnosti politik a jejich aktualizace

Organizační bezpečnost

- VIS+KII – dokumentace o bezpečnostních rolích
- Pouze KII – předepsány následující role
  - Manažer bezpečnosti ICT
  - Architekt bezpečnosti ICT
  - Auditor bezpečnosti ICT
  - Garant aktiva
  - Výbor pro řízení bezpečnosti ICT
- Východisko COBIT 5

Stanovení bezpečnostních požadavků na dodavatele

- VIS+KII – využití dodavatelů při rozvoji, provozu ICT nebo zajištění bezpečnosti podmíněno smlouvou včetně ujednání o bezpečnosti informací
- Pouze KII – doplněno pravidelné hodnocení rizik dodavatelů, dohoda o úrovni bezpečnostních opatření a kontrola jejich realizace

Řízení aktiv

- VIS+KII – identifikování a ohodnocení primárních aktiv, určení garanta aktiva
- Pouze KII – identifikování podpůrných aktiv a vyhodnocení závislostí mezi primárními a podpůrnými aktivy, určení garanta podpůrných aktiv
- VIS+KII – stanovení a prosazení pravidel pro ochranu aktiv podle jejich klasifikace
- VIS+KII – spolehlivé mazání a likvidace

Bezpečnost lidských zdrojů

- VIS+KII – poučení o bezpečnosti informací, kontrola dodržování pravidel, plán rozvoje bezpečnostního povědomí, vrácení svěřených prostředků
- Pouze KII – zvýšená opatrnost při výběru zaměstnanců pro bezpečnostní role, hodnocení účinnosti rozvoje povědomí, disciplinární řízení, změna oprávnění při změně pracovní pozice

Řízení provozu a komunikací

- VIS+KII – detekce kybernetických bezpečnostních událostí a jejich vyhodnocení
- VIS+KII –zajištění bezpečného provozu, stanovení provozních pravidel a postupů
- Pouze KII – práva a povinnosti bezpečnostních rolí, spuštění, ukončení a obnově chodu, restart, chybové stavy, kontaktní osoby, schvalování provozních změn, řízení provozních kapacit, oddělení V,T,P prostředí, prověřování provedených záloh, řešení vydaných protiopatření
- Pouze KII – bezpečnost a integrita komunikačních služeb a sítí, určení pravidel pro ochranu informací , výměna informací doložena písemnými dohodami s ustanovením bezpečnosti

Řízení přístupu

- VIS + KII – povinnost řízení přístupu
- VIS + KII – závazek ochrany autorizačních údajů ze strany všech uživatelů
- Pouze KII – individuální identifikátor, princip minimalizace oprávnění, pravidelná přezkoumání, odebírání nepotřebných oprávnění, ochrana mobilních zařízení včetně BYOD

Akvizice, vývoj a údržba

- VIS+KII – stanovení bezpečnostních požadavků na systémy
- Pouze KII – identifikace, hodnocení a řízení rizik v daném projektu podle metodiky pro řízení rizik, zajištění bezpečnosti vývojového prostředí, provedení bezpečnostního testování nových nebo změněných systémů

Zvládání kybernetických bezpečnostních událostí a incidentů

- VIS+KII – zajistit hlášení kybernetických bezpečnostních incidentů
  - Připravit prostředí pro vyhodnocení kybernetických bezpečnostních událostí
  - Provést neprodlené hlášení kybernetického bezpečnostního incidentu
  - Dokumentuje systém zvládání kybernetických bezpečnostních incidentů

Řízení kontinuity činností

- VIS+KII – dokumentace strategie a cílů řízení kontinuity + postupy pro provedení protiopatření
- Pouze KII – vyhodnocení potenciálních dopadů a souvisejících rizik
  - Vytvoření a udržování plánů kontinuity včetně realizace bezpečnostních opatření
  - Pravidelné testování plánů kontinuity

Provádění kontrol a auditů

- VIS+KII – dokumentace požadavků relevantních právních a regulatorních předpisů a smluvních závazků
  - Provádění a dokumentování kontrol dodržování stanovených pravidel
- Pouze KII – provádění prověrek na technické úrovni (testy technických zranitelností, zátěžové testy, penetrační testy apod.) včetně reakce na nedostatky

Přehled technických opatření

§ 16 Fyzická bezpečnost

§ 17 Nástroj pro ochranu integrity komunikačních sítí

§ 18 Nástroj pro ověřování identity uživatelů

§ 19 Nástroj pro řízení přístupových oprávnění

§ 20 Nástroj pro ochranu před škodlivým kódem

§ 21 Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a správců

§ 22 Nástroj pro detekci kybernetických bezpečnostních událostí

§ 23 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí

§ 24 Aplikační bezpečnost

§ 25 Kryptografické prostředky

§ 26 Nástroje pro zajištění vysoké úrovně dostupnosti

§ 27 Bezpečnost průmyslových a řídicích systémů

Fyzická bezpečnost

- VIS + KII – ochrana neoprávněného vstupu, poškození, kompromitaci aktiv
- KII – ochrana objektů, ochrana vymezených prostor s technickými aktivy, ochrana jednotlivých technických aktiv
- Prostředky fyzické bezpečnosti – mechanické zábranné, EZS, vstupní systémy, kamerové systémy, UPS, klima …

Nástroj pro ochranu integrity komunikačních sítí

- VIS+KII – ochrana integrity rozhraní vnější a vnitřní sítě
  - bezpečné řízení komunikace mezi vnější a vnitřní sítí
  - segmentace pomocí DMZ k zamezení přímé komunikace mezi vnější a vnitřní sítí
  - šifrování pro vzdálený přístup a bezdrátové technologie
  - blokování informací které neodpovídají požadavkům
- KII - ochrana integrity vnitřní sítě její segmentací

Nástroje pro ověřování identity uživatelů

- VIS+KII – nástroje pro ověření identity musí zajistit
  - Ověření identity všech uživatelů
  - Minimální délku hesla 8 znaků
  - Minimální složitost – alespoň jedno velké písmeno, jedno malé písmeno, číslici a speciální znak
  - Maximální dobu platnosti hesla 100 dní

- Pouze KII – kontrola dříve použitých hesel + délka 15 znaků pro privilegované účty

Nástroje pro řízení přístupových oprávnění

- VIS+KII – nástroje pro řízení přístupových práv musí zajistit
  - Řízení oprávnění uživatelů k aplikacím a datovým entitám
  - Řízení oprávnění: čtení, zápis a změna oprávnění

- Pouze KII – zaznamenání využití přístupových oprávnění

Nástroj pro ochranu před škodlivým kódem

- VIS+KII – povinné použití nástrojů pro antivirovou ochranu
  - Ověření a kontrola komunikace mezi interní a veřejnou sítí
  - Ověření a kontrola serverů a sdílených prostředků
  - Ověření a kontrola pracovních stanic
  - Pravidelná aktualizace

Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a správců

- VIS+KII – povinné použití nástrojů pro zaznamenávání činností, které zajistí
  - Sběr informací o událostech a jejich ochranu
  - Zaznamenání následujících událostí – přihlášení a odhlášení, činnosti privilegovaných účtů, činnosti vedoucí k navýšení oprávnění neúspěšné činnosti, spuštění a ukončení práce systému, varování a chybová hlášení, přístupy a manipulace s logy, použití mechanismů autentizace, odmítnuté činnosti v důsledku nedostatku oprávnění
  - Synchronizace času

Nástroj pro detekci kybernetických bezpečnostních událostí

VIS+KII – povinné použití nástroje pro detekci KBU
- kontrola a případné blokování komunikace mezi vnitřní a vnější sítí

Pouze KII – kontrola a případné blokování komunikace v rámci vnitřní komunikační sítě
– kontrola a případné blokování komunikace v rámci určených serverů

Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí

Pouze KII
- povinné použití nástroje pro sběr vyhodnocení KBU
- poskytuje informace o KBU bezpečnostním rolím
- nepřetržité vyhodnocování KBU
- politika pro použití a údržbu nástroje
- pravidelná aktualizace nastavených pravidel
- využívání získaných informací o KBU k optimalizaci bezpečnostních vlastností ICT

Aplikační bezpečnost

- VIS + KII – provádí bezpečnostní testy aplikací přístupných z vnější sítě před uvedením do provozu
- Pouze KII – zajišťuje trvalou ochranu apl. přístupných z vnějších sítí
  - Neoprávněnou činnosti
  - Popřením provedených činností
  - Kompromitací nebo neautorizovanou změnou
  - Transakcí před nedokončením, nesprávným směrováním, neautorizovanou změnou, kompromitací …

Kryptografické prostředky

- VIS + KII – stanovení politiky kryptografické ochrany
  - Typ a síla kryptografického algoritmu
  - Ochrana přenosu po komunikačních sítích, uložení na mobilní zařízení nebo vyměnitelná média
- Pouze KII – stanovení požadavků na správu a kvalitu kryptografických klíčů
  - Symetrické algoritmy
  - Asymetrické algoritmy
  - Algoritmy hash funkcí

Nástroje pro zajištění vysoké úrovně dostupnosti

- Pouze KII – použití nástrojů pro vysokou úroveň dostupnosti, které zajistí
  - Prosazení potřebné úrovně kontinuity
  - Nezbytnou míru odolnosti vůči útokům na snížení dostupnosti
  - Redundanci důležitých prvků KII (automatizovaně, ručně)

Bezpečnost průmyslových a řídicích systémů

- Pouze KII
  - Omezení fyzického i logického přístupu k průmyslovým a řídícím systémům
  - Ochrana jednotlivých prvků před známými zranitelnostmi
  - Obnovení chodu po incidentu

Bezpečnostní dokumentace

- §28 – Obsahuje výčet dokumentace a vazeb na § vyhlášky jednotlivých bezpečnostních opatření
- Není cílem ale nástrojem k zajištění bezpečnosti ICT

Certifikace systému řízení bezpečnosti informací

- Výčet dokumentace pro uznatelnost schody formou certifikace ISMS
  - Rozsah ISMS
  - Politika ISMS
  - Metodika hodnocení rizik a zpráva o hodnocení rizik
  - Certifikát ISMS
  - Záznam z přezkoumání
  - Zprávy certifikačního orgánu

Kybernetický bezpečnostní incident

§ 30 Typy kybernetických bezpečnostních incidentů

fyzická poškození, škodlivý SW, útoky, porušením opatření, kompromitací informací …

§ 31 Kategorie kybernetických bezpečnostních incidentů

- **Kategorie III** – velmi závažný kybernetický bezpečnostní incident
- **Kategorie II** – závažný kybernetický bezpečnostní incident
- **Kategorie I** – méně závažný kybernetický bezpečnostní incident

§ 32 Forma a náležitosti hlášení kybernetických bezpečnostních incidentů

Protiopatření

§ 33 Protiopatření

- VIS+KII : oznámení o provedení protiopatření , poskytnutí dodatečných informací, poskytnutí důkazů souvisejícím s incidentem, změna či rozšíření stávajících bezpečnostních opatření s minimalizací negativních dopadů

§ 34 Kontaktní údaje

- Oznámení kontaktních údajů danou formou

Odborná kvalifikace osob

§ 35 Kvalifikace manažera a architekta bezpečnosti ICT

- Vyškolení a 3 roky praxe v oboru

§ 36 Kvalifikace osob provádějících interní audity ISMS

- Vyškolení a 3 roky praxe v oboru

Přílohy

Příloha 1:	Typy, způsoby hodnocení a úrovně aktiv
Příloha 2:	Hodnocení rizik
Příloha 3:	Minimální požadavky na kryptografické algoritmy
Příloha 4:	Struktura bezpečnostní dokumentace
Příloha 5:	Kategorie kybernetických bezpečnostních událostí a incidentů
Příloha 6:	Formulář pro hlášení KBI
Příloha 7:	Formulář oznámení o provedení protiopatření
Příloha 8:	Formulář pro hlášení

Účinnost

1. 1. 2015

Děkuji za pozornost