Nabídka služeb kybernetické bezpečnosti

Z hlediska zákona o kybernetické bezpečnosti

(Implementační scénáře a metodiky aktualizovány dle BSI - IT Grundschutz)

Ing. Michal Vymazal
Ing. Jiří Richter

Červenec 2018

Obsah

Nabídka služeb v oblasti kybernetické bezpečnosti

Naše sdružení sestává z těchto subjektů

- **Ing. Jiří Richter - TURBO 2000, IČO: 15648427**,
  nezávislý Architekt kybernetické bezpečnosti se zápisem v obchodním rejstříku
  www.turbo2000.cz

- **Ing. Michal Vymazal - Linux Services, IČO: 12627721**,
  nezávislý Architekt kybernetické bezpečnosti se zápisem v obchodním rejstříku
  www.linuxservices.cz

Sídlíme v Praze. Máme více než 20 letou historii. Nabízíme řešení v oblasti informačních systémů a zabezpečení, zcela nezávislá na dodavatelích, odpovídající zákonným normám ČR a EU, na bázi otevřených standardů a platných technických norem.

Jsme způsobilí ke školení kybernetické bezpečnosti pro role dle §7 Vyhlášky k ZKB, písmena a, b a c. (tj. role manažer kybernetické bezpečnosti, architekt kybernetické bezpečnosti, auditor kybernetické bezpečnosti).

Dále jsme způsobilí k činnosti dle rolí §7 Vyhlášky k ZKB (82/2018 Sb.), písmena a, b a c. (tj. role manažer kybernetické bezpečnost, architekt kybernetické bezpečnosti, auditor kybernetické bezpečnosti).

Nabízíme tyto služby v souladu s požadavky zákona o kybernetické bezpečnosti

- Výkon role manažer kybernetické bezpečnosti
- Výkon role architekt kybernetické bezpečnosti
- Výkon role auditor kybernetické bezpečnosti
- Audit bezpečnostních opatření, dle metodik NÚKIB
- Audit bezpečnostních opatření, dle metodik BSI (IS audits based on IT-Grundschutz)
- Business Impact Analysis (dle metodik BSI)
- Disaster Recovery Plan (dle metodik BSI, NIST)
- Analýza rizik (dle metodik BSI)
- Penetrační testy (dle metodik BSI)
- Statická analýza zdrojového kódu (SAST)
- Technická opatření (Hlava II, Vyhlášky 82/2018 Sb.)

Pro jednotlivé implementační scénáře využíváme metodiky a doporučení BSI (BSI – Německá národní bezpečnostní autorita, *Bundesamt für Sicherheit in der Informationstechnik*). Vycházíme tedy ze scénářů **IT-Grundschutz**.

Legislativa

Gestorem oblasti kybernetické bezpečnosti je v ČR **Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB).** Tento úřad je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Dále má na starosti problematiku neveřejné služby v rámci družicového systému Galileo. Vznikl 1. srpna 2017 na základě zákona číslo 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

Prováděcí právní předpisy k zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) jsou následující:

- Zákon o kybernetické bezpečnosti
- Směrnice NIS
- Vyhláška o kybernetické bezpečnosti
- Vyhláška o významných informačních systémech
- Nařízení vlády o kritériích pro určení prvku kritické infrastruktury (vč. kritické informační infrastruktury)
- Vyhláška o kritériích pro určení provozovatele základní služby

Viz.
https://www.nukib.cz/cs/kyberneticky-zakon/legislativa/

V této souvislosti je dobré připomenout, že i Trestní zákoník zná trestné činy související s neoprávněnými přístupy do informačních systémů, konkrétně **§ 230** nazvaný "Neoprávněný přístup k počítačovému systému a nosiči informací".

Nový občanský zákoník pak pamatuje na škodu způsobenou informací nebo radou (§ 2950 NOZ).

Metodika / Národní autority

Vlastní Zákon o kybernetické bezpečnosti obsahuje odkazy na související normy a metodiky (např. ISO 27032, Cybersecurity). Národní bezpečnostní autorita dále respektuje metodiky relevantní (např. metodiky národních autorit členských zemí EU, NIST atp.)

Implementační scénáře

Tato otázka zatím není řešena ani legislativně, ani metodicky. Předpokládáme, že zde se situace začne rychle měnit a implementační scénáře budou jednak veřejně dostupné, jednak budou navazovat na metodiku. K dnešnímu dni můžeme odkázat na vzorové implementační scénáře volně dostupné na stránkách německé národní autority (BSI).

Bezpečnostní dokumentace / popis procesů

Vzhledem k faktu, že licence ISO dokumentů neumožňuje jejich „volnou“ distribuci a dále vzhledem k faktu, že ISO dokumenty nezahrnují tzv. „best practice“, rozhodli jsme se (v souladu s Č.j.: 1649/2013-NBÚ/41) využít pro jednotlivá doporučení metodik a dokumentů národních bezpečnostních autorit EU (BSI – Německá národní bezpečnostní autorita, *Bundesamt für Sicherheit in der Informationstechnik*) a NIST (National Institute of Standards and Technology, USA).

Audit bezpečnostních opatření

Vlastním auditem bezpečnostních opatření rozumíme proces jehož výstupem je zdokumentování jednotlivých opatření, popis vazeb na okolní informační systémy a prostředí, dekompozice aktiv, řízení kontinuity činností.

Výstupem auditu jsou zejména tyto dokumenty (dle metodiky NÚKIB):

- Bezpečnostní opatření
- **Organizační opatření**
- Systém řízení bezpečnosti informací (VKB § 3)
- Řízení rizik (VKB § 4)
- Bezpečnostní politika (VKB § 5)
- Organizační bezpečnost (VKB §
- Stanovení bezpečnostních požadavků pro dodavatele (VKB § 7) .
- Řízení aktiv (VKB § 8)
- Bezpečnost lidských zdrojů (VKB § 9) .
- Řízení provozu a komunikací (VKB § 10)
- Řízení přístupu a bezpečné chování uživatelů (VKB § 11)
- Akvizice, vývoj a údržba (VKB § 12)
- Zvládání kybernetických bezpečnostních událostí a incidentů (VKB § 13)
- Řízení kontinuity činností (VKB § 14)
- Kontrola a audit kybernetické bezpečnosti (VKB § 15)
- **Technická opatření**
- Fyzická bezpečnost (VKB § 16)
- Nástroj pro ochranu integrity komunikačních sítí (VKB § 17)
- Nástroj pro ověřování identity uživatelů (VKB § 18)
- Nástroj pro řízení přístupových oprávnění (VKB § 19)
- Nástroj pro ochranu před škodlivým kódem (VKB § 20)
- Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů (VKB § 21)
- Nástroj pro detekci kybernetických bezpečnostních událostí (VKB § 22)
- Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí (VKB § 23)
- Aplikační bezpečnost (VKB § 24)
- Kryptografické prostředky (VKB § 25)
- Nástroj pro zajišťování úrovně dostupnosti (VKB § 26)
- Bezpečnost průmyslových a řídících systémů (VKB § 27)

Veškerá dokumentace by pak měla ctít zásadu zvanou „**platform, vendor and architecture independent**“. To znamená, že je kladen důraz na dodržování veškerých souvisejících norem a standardů, nejsou zde uvedeny komerční názvy aplikací, výrobců nebo dodavatelů.

Výstupy z auditu pak slouží jako podklady (vstupy) pro BIA, DRP, Analýzu rizik, bezpečnostní směrnice a bezpečnostní politiky.

Metodika NÚKIB
https://www.govcert.cz/download/kii-vis/container-nodeid-580/vkbchecklistfinalv21rev.pdf

Metodika BSI pro audit bezpečnostních opatření
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/ISRevision/guideline-isrevision_pdf.pdf?__blob=publicationFile

Role auditora je dána §7, písm. c vyhlášky k ZKB (82/2018 Sb.)
Vlastní audit je vyžadován v §16 vyhlášky k ZKB.

Business Impact Analysis – BIA

Analýza dopadů (BIA) je základem celého procesu řízení kontinuity činností organizace (Business Continuity Plan, BCP). Sestává z technik a metod, pomocí kterých se hodnotí jaké dopady by na organizaci a další zainteresované strany mělo narušení dodávek klíčových produktů nebo služeb organizace a jejich podpůrných kritických činností. Součástí BIA je stanovení minimálních úrovní zdrojů potřebných pro obnovení kritických činností ve stanovených časech a na stanovených úrovních.

Analýza dopadů by měla být přezkoumávána v pravidelných intervalech nebo při podstatných změnách v organizaci a prostředí, v němž organizace působí.

Využíváme metodiky BSI a NIST.

Disaster Recovery Plan – DRP

Jedná se o metodiky a postupy sloužící k obnově funkčnosti informačního systému po živelných pohromách a jiných zásadních událostech. Obnova funkčnosti a provozuschopnosti informačního systému by měla proběhnout v co nejkratším čase a s minimem výdajů a rizik. V prvé řadě je třeba obnovit chod kritických modulů (podsystémů) a aplikací (tzv. Nouzový režim).
Vlastní DRP pak vychází z výstupů BIA.

Využíváme metodiky NIST.

Penetrační testy

Cílem penetračních testů je odhalení zranitelností cílového informačního systému, stanovení způsobu jejich možného využití a doporučení vedoucí k jejich nápravě.
Mezi nejčastější příčiny zranitelností IS řadíme zejména:

- Nedodržování platných standardů (RFC, W3C, ISO)
- Nedůsledná konfigurace zařízení (povoleny zbytečné/nevyužité síťové služby, slabé šifrování)
- Nevyhovující topologie systému
- Neznalost managementu/odborné obsluhy
- Neprovádění kontrol (auditů) zdrojových kódů jednotlivých aplikací
- Nepořádek

Možné důsledky zranitelnosti informačního systému
Zde se skutečně může jednat o velmi vážné škody mající dopad zejména na:

- Důvěryhodnost firmy
- Právní postih v případě zneužití/znehodnocení údajů dalších subjektů (osobní údaje, obchodní data, čísla kreditních karet apod.)
- Ztráta zakázky
- Finanční ztráty spojené s neefektivním využíváním informačního systému

Druhy penetračních testů
Obecně vzato, můžeme penetrační testy rozdělit na:

- Destruktivní a nedestruktivní
- Externí a interní

Kvalitní posouzení úrovně informační bezpečnosti nelze provést pouze auditem či pouze penetračními testy. Samotný audit nemůže dost dobře posoudit konfiguraci systémů a jejich schopnost odolat venkovním a vnitřním maligním útokům. Stejně tak provedení samotných penetračních testů, bez zasazení jejich výsledků do celkového kontextu úrovně zajištění bezpečnosti, nemá vypovídající hodnotu. Penetrační testy sice odhalí chyby v konfiguraci a nastavení HW, neukáží však na chyby v organizačním a procesním zajištění bezpečnosti. Je možné, že penetrační testy potvrdí dokonalé nastavení systému, nicméně systém sám bude vykazovat vážné závady, které mohou mít fatální dopad na jeho provoz. Je tedy jednoznačně výhodné využít synergického efektu.

Základní rozdělení je z hlediska provádění testů. Externí testy jsou vykonány z prostředí internetu (měřící bod Zhotovitele), interní pak přímo z prostředí informačního systému zákazníka.

Pro vlastní scénáře penetračních testů využíváme tyto metodiky:

- BSI (Penetration testing model)
- OWASP Application Security Verification Standard
- OWASP Testing Guide
- NIST Recommended Security Controls for Federal Information Systems and Organizations

Výstupy penetračního testování

Výstupem je zpráva, kterou lze rozdělit na dvě části a sice:

- Podrobný rozpis penetračních testů včetně technických detailů a výsledných doporučení
- Manažerský souhrn

Statická analýza zdrojového kódu (SAST)

Statická analýza kódu je sada metod pro analýzu počítačových programů, které jsou aplikovány bez jejich spuštění (softwarová analýza, která je aplikována na spuštěné programy, se nazývá dynamická softwarová analýza).

V nejběžnějších případech je analýza prováděna právě na zdrojovém kódu, nebo nějaké formě objektových kódů.

Blíže viz.
https://www.linuxservices.cz/sonarqube

Analýza rizik

Stupnice pro hodnocení a úrovně důležitosti aktiv je obsažena v Příloze 1 Vyhlášky k Zákonu o kybernetické bezpečnosti

Pravidla pro hodnocení dopadů, hrozeb, zranitelností a rizik jsou uvedena v Příloze 2 Vyhlášky k Zákonu o kybernetické bezpečnosti
https://www.govcert.cz/cs/zkb/legislativa/

Jedná se o metodiku/proces sloužící k rozpoznání, předpovězení a vyhodnocení jednotlivých hrozeb a jejich dopadů na daný informační systém. Analýza rizik navazuje na vlastní bezpečnostní proces a představuje zpětnou vazbu pro daný informační systém a oblasti tímto informačním systémem dotčené. Výstupní dokument je třeba periodicky aktualizovat.

Vlastní analýzu rizik je možné provést dle metodik BSI

Technická opatření

Zabýváme se návrhy, výrobou, testováním a provozováním bezpečnostních zařízení dle Hlavy II, §22 - §24, Vyhlášky 82/2018 (Vyhláška k zákonu o kybernetické bezpečnosti). Konkrétně se jedná o tato zařízení:

- §22 Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů
- §23 Nástroj pro detekci kybernetických bezpečnostních událostí
- §24 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí

Bezpečnostní parametry IS (Politika bezpečnosti sítě)

Vyžadováno v §6 Vyhlášky k ZKB.

Jedná se o soubor nastavení parametrů jednotlivých zařízení, která jsou součástí daného informačního systému. Dále jsou zde popsány bezpečnostní mechanismy, jejich význam a zaměření. Součástí dokumentu je popis jednotlivých uživatelských rolí, jejich oprávnění, pravomoce a přenositelnost práv (delegování pravomocí a zodpovědnosti).

Bezpečnostní směrnice IS

Vyžadováno v §6 Vyhlášky k ZKB.

Jde o soubor směrnic, jež jsou závazné pro všechny uživatele informačního systému. Tyto směrnice musejí být v souladu s judikaturou ČR.

- Začlenění bezpečnostních mechanismů do provozu IS, vysvětlení těchto mechanismů (procesy, postupy, nastavení parametrů).
- Chování uživatelů v IS.
- Práva a povinnosti uživatelů IS. Jejich zodpovědnost.
- Vysvětlení pojmu „Bezpečnostní incident“. Odstupňování bezpečnostních incidentů.
- Postupy pro řešení bezpečnostních incidentů.
- Klasifikace a řízení aktiv.

GDPR

Legislativa a standardy

Obecné nařízení o ochraně osobních údajů (GDPR) (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

Směrnice Evropského parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, (**směrnice NIS**) platná od 8. srpna 2016

ISMS řady ISO/IEC 27xxx u nás ČSN ISO/IEC 27001:2014
Metodiky NÚKIB
Metodiky a standardy Německého bezpečnostního úřadu (BSI)

Poznámka:
Směrnice NIS je plně integrována v zákonu o kybernetické bezpečnosti (181/2014 Sb.)

Regulátoři

ÚOOÚ – narušení bezpečnosti osobních údajů pro oblast elektronických komunikací podle zákona č. 127/2005 Sb. GDPR rozšiřuje i na další odvětví (bankovnictví, doprava, zdravotnictví, veřejná správa…).

NÚKIB - narušení bezpečnosti sítí a informací pro všechna odvětví závisející na bezpečnosti sítí podle EU směrnice NIS (zákon 181/2014 Sb. o kybernetické bezpečnosti).

ČTÚ – narušení bezpečnosti sítě (tzv. security breach) pro oblast elektronických komunikací podle e-privacy směrnice.

Vztah GDPR a informační bezpečnosti

Osobní údaj je jedním z typů informací, tedy **AKTIVEM organizace**, které musí být chráněno podle principů informační bezpečnosti

Pokud je osobní údaj v digitální podobě, musí být chráněno podle principů kybernetické bezpečnosti

GDPR podle článku 24. a 32. přímo předpokládá bezpečnostní opatření informační a kybernetické bezpečnosti v podobě organizačních i technických opatření.

Poznámka:
Bude-li proveden audit bezpečnostních opatření + organizační opatření + technická opatření + bezpečnostní dokumentace dle ZKB, pak certifikovaný (komerční) audit dle ISO 27000 nebo GDPR se může zaměřit pouze na ověření shody (veškerá příprava je již hotova dle ZKB).

Slovníček pojmů

Zkratka	Vysvětlení zkratky
Audit IS	Vlastním auditem informačního systému rozumíme proces jehož výstupem je zdokumentování informačního systému, popis jeho vazeb na okolní informační systémy a prostředí.
	Metodika BSI pro audit informačního systému https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/ISRevision/guideline-isrevision_pdf.pdf?__blob=publicationFile
Analýza rizik	Metodika sloužící k rozpoznání, předpovězení a vyhodnocení jednotlivých hrozeb a jejich dopadů na daný informační systém. Analýza rizik navazuje na vlastní bezpečnostní proces a představuje zpětnou vazbu pro daný informační systém a oblasti tímto informačním systémem dotčené.
	Výstupní dokument je třeba periodicky aktualizovat https://www.bsi.bund.de/EN/Publications/BSIStandards/standards.html
BIA	Business Impact Analysis
	Analýza dopadů (BIA) je základem celého procesu řízení kontinuity činností organizace (Business Continuity Plan, BCP). http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-4_e_pdf.html
BSI	*Bundesamt für Sicherheit in der Informationstechnik*
	Německá národní bezpečnostní autorita (obdoba českého NÚKIB). www.bsi.bund.de
DRP	Disaster Recovery Plan
	Jedná se o metodiky a postupy sloužící k obnově funkčnosti informačního systému po živelných pohromách a jiných zásadních událostech.
ISO	International Organization for Standardization
	Označení mezinárodní normy http://www.iso.org/iso/home.html
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
	www.nukib.cz
NIST	National Institute of Standards and Technology, USA
	http://www.nist.gov/
Penetrační testy	Cílem penetračních testů je odhalení zranitelností cílového informačního systému, stanovení způsobu jejich možného využití a doporučení vedoucí k jejich nápravě.
	http://www.linuxservices.cz/penetracni-testy