Jak jsme na tom s Kybernetickou bezpečností?

Jan Dienstbier

Situace se zlepšuje

- Rozdíl v přístupu mezi povinnými osobami a ostatními organizacemi
  - Místy stále převládá názor, nejsem-li osobou povinnou nemusím řešit
- Omyl!!!!!
  - Správa organizace péčí řádného hospodáře , …

Kde je tedy prostor ke zlepšení?

Dnes je již samozřejmostí?!

- Zálohování
- Pravidelné testování obnovy ze záloh
- Testovací prostředí
- Šifrování dat/přenosů

- Bezpečnost má podopru nejvyššího vedení

Kde je tedy prostor ke zlepšení?

Security by design

- Bezpečnost promítáme již do zadávacích řízení (soutěžíme na cenu😍)
  - § 4 Zákona (3) Orgány a osoby uvedené v § 3 písm. c) až e) jsou povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatelů pro informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém.

- Pravidelné školení (hands-on) s **následným vyhodnocením**!
- Prezenční či elearning nestačí
- Kontrola bezpečnosti - PEN testy
  - Spoléhat NUKIB nestačí

Kde je tedy prostor ke zlepšení?

- Zodpovědně zavádět organizační a technická opaření
  - Kdo má dnes oceněná aktiva a zpracovanou analýzu rizik?
  - Bez toho však následná technická opatření nemusejí být zaváděna v optimálním pořadí a navzájem se doplňovat

- Na systém je třeba nahlížet jako na celek, nestačí jen řešit bezpečnost jednotlivých aplikací/agend

- Řízení dodavatelů – **nejen těch významných**
- Naše zkušenost s vyjímkou oznámení o tom, že jsme významným dodavelem - 0

Řízení dodavatelů

§ 2 vyhlášky **Vymezení pojmů**

f) podpůrným aktivem technické aktivum, zaměstnanci a **dodavatelé** podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému

§ 8 **Řízení dodavatelů**

(1) Povinná osoba

a) stanoví pravidla pro dodavatele, která zohledňují požadavky systému řízení bezpečnosti informací,

d) seznamuje své dodavatele s pravidly podle písmene

a) a vyžaduje plnění těchto pravidel,

e) řídí rizika spojená s dodavateli,

f) v souvislosti s řízením rizik spojených s významnými dodavateli zajistí, aby smlouvy uzavírané s významnými dodavateli obsahovaly relevantní oblasti uvedené v příloze č. 7 k této vyhlášce, a

g) pravidelně přezkoumává plnění smluv s významnými dodavateli z hlediska systému řízení bezpečnosti informací.

Řízení dodavatelů - pokračování

(2) Povinná osoba u významných dodavatelů

dále

a) v rámci výběrového řízení a před uzavřením smlouvy provádí hodnocení rizik souvisejících

s plněním předmětu výběrového řízení přiměřeně podle přílohy č. 2 k této vyhlášce,

b) v rámci uzavíraných smluvních vztahů stanoví způsoby a úrovně realizace bezpečnostních

opatření a určí obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních

opatření,

c) provádí pravidelné hodnocení rizik a pravidelnou kontrolu zavedených bezpečnostních opatření u poskytovaných plnění pomocí vlastních zdrojů nebo pomocí třetí strany a

d) v reakci na rizika a zjištěné nedostatky zajistí jejich řešení.

Řízení dodavatelů - pokračování

§ 9 **Bezpečnost lidských zdrojů**

(1) Povinná osoba v rámci řízení bezpečnosti lidských zdrojů

a) s ohledem na stav a potřeby systému řízení bezpečnosti informací stanoví plán rozvoje bezpečnostního povědomí, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí a který obsahuje formu, obsah a rozsah

1. poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a **dodavatelů** o jejich povinnostech a o bezpečnostní politice a

2. potřebných teoretických i praktických školení

c) v souladu s plánem rozvoje bezpečnostního povědomí zajistí poučení uživatelů, administrátorů, osob zastávajících bezpečnostní **role a dodavatelů** o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení

Příloha č. 7 k vyhlášce č. 82/2018 Sb.

Řízení dodavatelů - bezpečnostní opatření pro smluvní vztahy

Obsah smlouvy uzavírané s významnými dodavateli:

a) ustanovení o bezpečnosti informací (z pohledu důvěrnosti, dostupnosti a integrity),

b) ustanovení o oprávnění užívat data,

c) ustanovení o autorství programového kódu, popřípadě o programových licencích,

d) ustanovení o kontrole a auditu dodavatele (pravidla zákaznického auditu),

e) 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,

f) ustanovení o povinnosti dodavatele dodržovat bezpečnostní politiky povinné osoby nebo ustanovení o odsouhlasení bezpečnostních politik dodavatele povinnou osobou,

g) ustanovení o řízení změn,

h) ustanovení o souladu smluv s obecně závaznými právními předpisy,

i) ustanovení o povinnosti dodavatele informovat povinnou osobu o

1. kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy,

2. způsobu řízení rizik na straně dodavatele a o zbytkových rizicích souvisejících s plněním smlouvy,

3. významné změně ovládání tohoto dodavatele podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných tímto dodavatelem k plnění podle smlouvy se správcem,

j) specifikace podmínek z pohledu bezpečnosti při ukončení smlouvy (například přechodné období při ukončení spolupráce, kdy je třeba ještě udržovat službu před nasazením nového řešení, migrace dat a podobně),

k) specifikace podmínek pro řízení kontinuity činností v souvislosti s dodavateli (například zahrnutí dodavatelů do havarijních plánů, úkoly dodavatelů při aktivaci řízení kontinuity činností),

l) specifikace podmínek pro formát předání dat, provozních údajů a informací po vyžádání správcem,

m) pravidla pro likvidaci dat,

n) 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

o) ustanovení o sankcích za porušení povinností.

Na co si dát dále pozor

Weby

Rozvoj portálový služeb

- Začít revizí procesů
- Umístění serveru
- Bezpečná komunikace
- Kontrola bezpečnosti implementace

Děkuji za pozornost.

Jan Dienstbier

jan_dienstbier@gordic.cz

+420 602 382 812