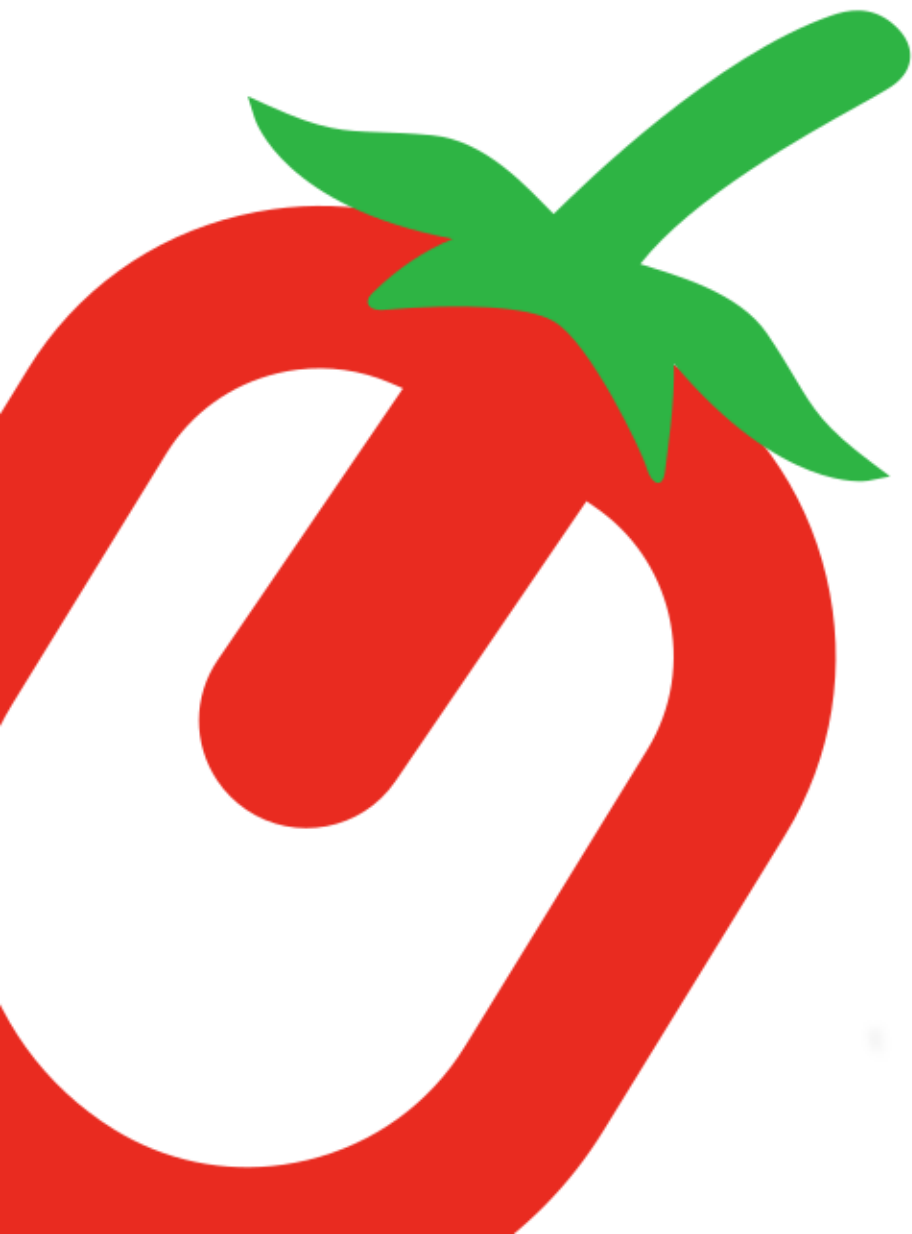


Kybernetická bezpečnost v kostce

Ostrava

Petr Šubert

02.12.2024



Rozdíl mezi stávajícím a připravovaným ZoKB

- Místo ochrany kritické infrastruktury a významných informačních systémů se regulace zaměřuje na **dostupnost tzv. regulovaných služeb.**

**Zavádí pohled shora dolů
– od businessu k počítačům.**



Váš business je postavený na **aktivech**

Co je/bylo aktivum podle zákona:

- a) aktivem **primární aktiva a podpůrná aktiva, relevantní pro zpracování informací** a dat v elektronické podobě, a to **včetně likvidace**
- b) primárním aktivem **informace a služby (původně i procesy)**
- c) podpůrným aktivem **zaměstnanci, dodavatelé, objekty a technická aktiva**
- d) technickým aktivem **technické a programové prostředky a vybavení, a to včetně průmyslových, řídicích nebo jiných obdobných specifických aktiv**



Aktiva (přehledně)

- Primární aktiva
 - Služby
 - Informace
- Podpůrná aktiva, **relevantní pro zpracování informací a dat v elektronické podobě**
 - Zaměstnanci
 - Dodavatelé
 - Objekty
 - Technická aktiva
 - *Technické prostředky a vybavení*
 - *Programové prostředky a vybavení*
 - *Komunikační prostředky*
 - *Sítě elektronických komunikací*
 - *Průmyslová, řídicí nebo jiná podobná aktiva*



Co je to primární aktivum?

- **Služby nebo produkty**, které dáváte na trh
- To, co je pro Vás a Vaši organizaci a její business nejdůležitější, prvořadé, hlavní – prostě **primární**
- To, za co Vám někdo platí, co směňujete za peníze
- To, co je (legitimním) zdrojem Vašeho bohatství

Úplně se oprostěte od IT, pokud IT samozřejmě není Váš business

Pomoc najdeme ve vyšších povinnostech

Při identifikaci primárních aktiv regulované služby je vhodné nejprve **identifikovat její účel**. Z účelu je možné odvodit **aktivum typu služba**. Následně je vhodné identifikovat, **s jakými informacemi daná služba pracuje (jaké informace ZNALOSTI potřebujete pro to, abyste mohli tuto služby poskytovat)** a odvodit primární aktiva typu informace.

Pomoc najdeme ve vyšších povinnostech - pokračování

Při identifikaci podpůrných aktiv je nutné vycházet z architektury systému regulované služby a zejména zohlednit **vazby na primární aktiva**.

Povinná osoba by měla **zvolit takový detail podpůrných aktiv (ale i primárních aktiv!!!)**, aby byla schopna adekvátně identifikovat a **řídit rizika** s aktivy spojená.

Primární aktiva - podle vzoru ORP

Regulovaná služba **výroba potravin a výroba elektrické energie**

- **Primární aktiva**

- Služby

- **Výkon svěřených pravomocí**

- Dle zákona 128/2000 Sb. - Zákon o obcích (obec pečuje o všestranný rozvoj svého území a o potřeby svých občanů; při plnění svých úkolů chrání též veřejný zájem)

- Zajištění tepla a teplé vody

- Provoz čistírný odpadních vod

- Svoz odpadů

- Rozvojové projekty

- Výkon přenesené působnosti dle zákona č. 114/1992 Sb., o ochraně přírody a krajiny

- Zákon č. 561/2004 Sb. - Školský zákon

- Zákon č. 240/2000 Sb. – Krizový zákon

- ...

- **Výroba elektrické energie**

- Informace (které potřebujete k poskytování služeb – informace o dotčených subjektech, data z registrů,)

02.12.2024



Podpůrná aktiva - podle vzoru ORP

Regulovaná služba **Výkon svěřených povinností**

- **Podpůrná aktiva**

- Zaměstnanci
- Dodavatelé
 - Externí dodavatelé
 - Inertní dodavatelé
 - Obchodní společnosti
 - Příspěvkové organizace
 - Organizační složky
 - Externí dodavatelé
- Objekty (čistírna odpadních vod, škola, infrastruktura ...)
- Technická aktiva
 - *Technické prostředky a vybavení*
 - *Programové prostředky a vybavení*
 - *Komunikační prostředky*
 - *Sítě elektronických komunikací*
 - *Průmyslová, řídicí nebo jiná podobná aktiva*



ICT - pokud nejsou váš chleba, patří sem:

- **Primární aktiva**
 - Informace
 - Služby
- **Podpůrná aktiva**
 - Zaměstnanci
 - Dodavatelé
 - Objekty
 - Technická aktiva
 - *Technické prostředky a vybavení*
 - *Programové prostředky a vybavení*
 - *Komunikační prostředky*
 - *Sítě elektronických komunikací*
 - *Průmyslová, řídicí nebo jiná podobná aktiva*



A máme zde první povinnost

§ 12 - Stanovení rozsahu řízení kybernetické bezpečnosti

(1) Součástí rozsahu řízení kybernetické bezpečnosti (dále jen „stanovený rozsah“) jsou aktiva související s poskytováním regulované služby.

(2) Za účelem vymezení stanoveného rozsahu poskytovatel regulované služby

- a) určí **všechna** svá primární aktiva,
- b) **posoudí**, zda primární aktiva souvisí s poskytováním regulované služby, a
- c) u primárních aktiv podle písmene b) **určí** podpůrná aktiva.

(3) Poskytovatel regulované služby **eviduje aktiva**, která jsou součástí stanoveného rozsahu, **a primární aktiva**, která byla ze stanoveného rozsahu vyjmuta, **včetně důvodů jejich vyjmutí**.

(4) Platí, že primární aktiva, která ještě nebyla posouzena podle odstavce 2 písm. b), a podpůrná aktiva, která ještě nebyla určena podle odstavce 2 písm. c), jsou součástí stanoveného rozsahu.

(5) Stanovený rozsah je poskytovatel regulované služby povinen **pravidelně přezkoumávat a aktualizovat**.



Potměšilost úředníků?

Function	Category	Category Identifier
<u>Govern (GV)</u>	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
<u>Identify (ID)</u>	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
<u>Protect (PR)</u>	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
<u>Detect (DE)</u>	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
<u>Respond (RS)</u>	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
<u>Recover (RC)</u>	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

NIST Cybersecurity Framework 2.0



Dává vám to takto smysl?

Je to úplně stejné jako řízení jiných (ne kybernetických) rizik.



Dopady aneb povinnost číslo 2.

§ 15 - Stanovení významnosti dopadu kybernetického bezpečnostního incidentu

(1) Povinná osoba pro potřeby vyhodnocení významnosti dopadu kybernetického bezpečnostního incidentu na poskytování regulované služby stanoví

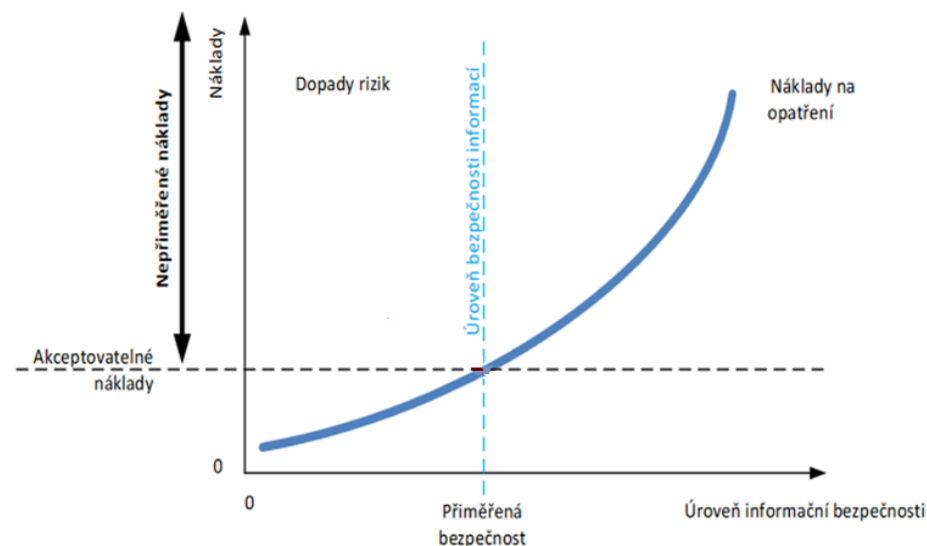
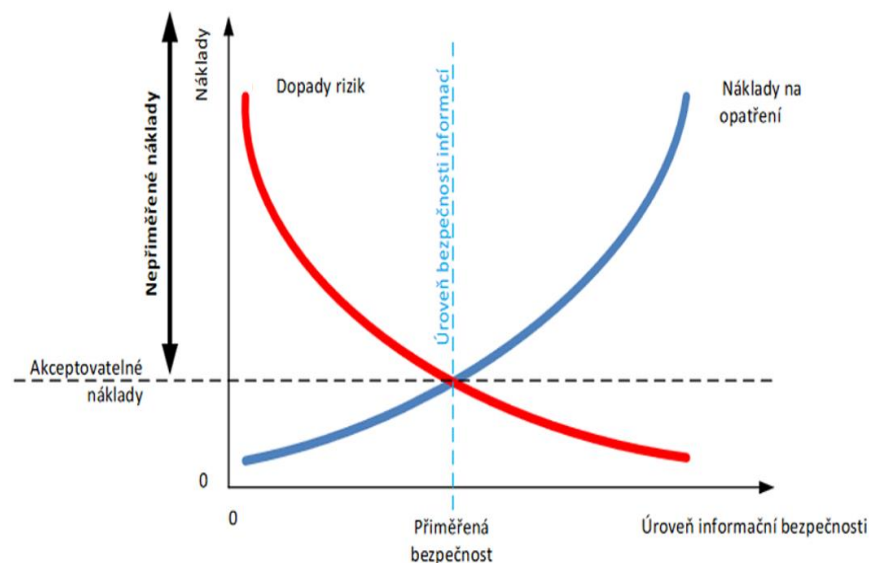
a) **únosnou míru újmy způsobené kybernetickým bezpečnostním incidentem** představující úhrn nejvyšší škody a nemajetkové újmy vzniklý v souvislosti s kybernetickým bezpečnostním incidentem, v jehož důsledku ještě nejsou ohroženy život či zdraví osob nebo schopnost poskytovatele regulované služby dostát svým závazkům,

Další lumpárna úředníků z Brna?

- Pomocí dopadů v podstatě řídíte implementaci systému řízení bezpečnosti informací.
- Je potřeba to mít někde popsána (pište si i proč jste to tak vyhodnotili – druhý den to zapomenete).
- Občas to zkontrolujte – určitě se to bude měnit.
- Nemyslím si, že to dáte na první dobrou, je potřeba změnit myšlení.
- **Je to srozumitelné pro management** – dokonce to už někde máte pro jiné oblasti řízení rizik.
- Omezí Vám to komunikaci s NÚKIBem 😊.
- Vědecky se tomu říká **BIA (Business Impact Analýza)**.

I BIA je bezesporu věda

- Ale je jen a jen na Vás, kterou cestou se vydáte.

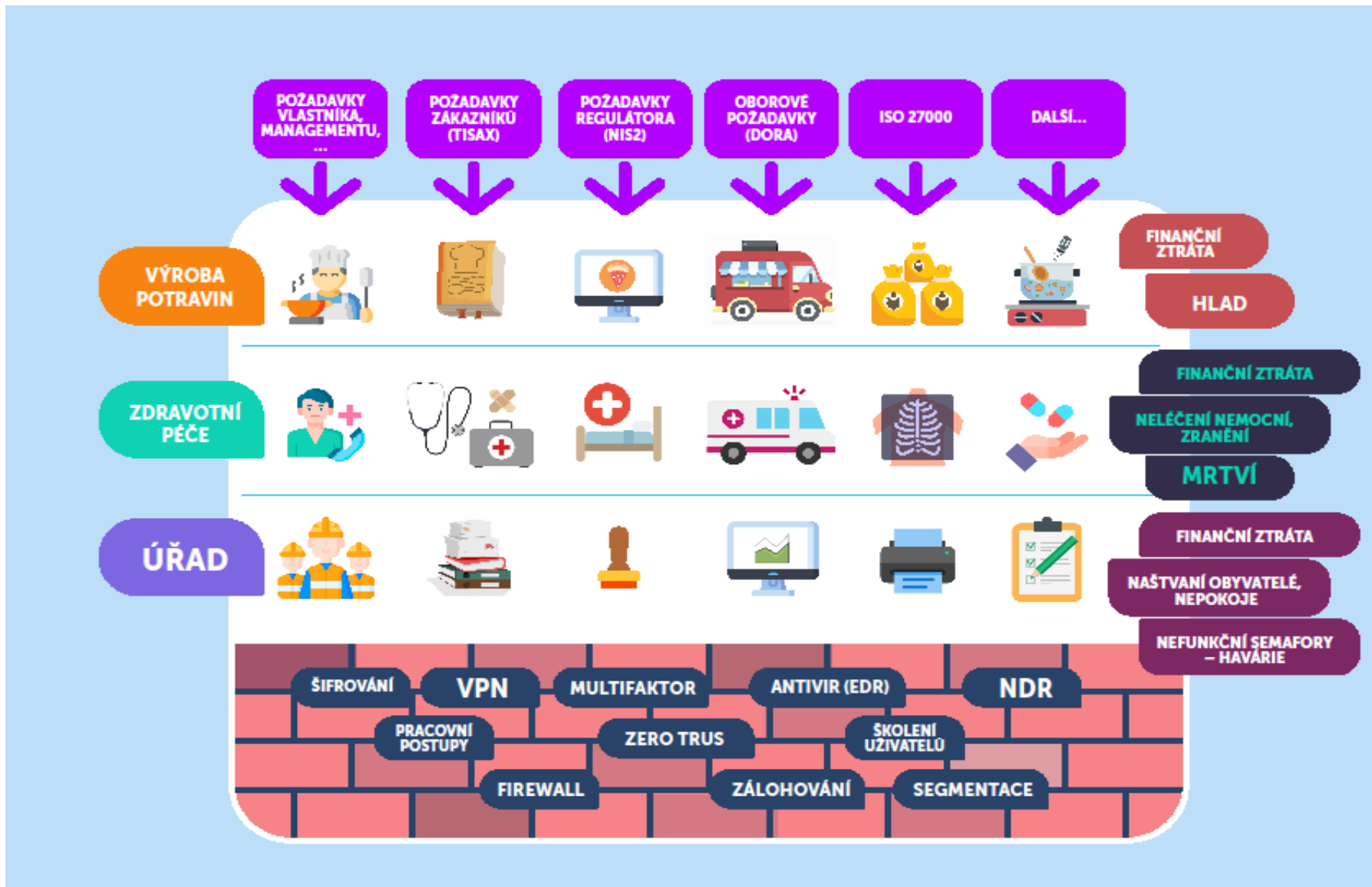


Ostrava

- Nezavrhujte věci pro jejich složitost, ale pracujte s myšlenkou/podstatou, kterou Vám přinášejí.



Jsme to nakreslili



Základní pojmy (osa zla)

- **Aktivum** – cokoli, co má hodnotu pro vaše podnikání.
- **Zranitelnost** – slabina nebo chyba v aktivu, kterou může útočník využít.
- **Hrozba** – potenciální nebezpečí, že někdo(něco) využije zranitelnost k provedení útoku.
- **Riziko** – pravděpodobnost, že hrozba využije zranitelnost a způsobí škodu.
- **Incident** – konkrétní případ, kdy došlo k využití zranitelnosti hrozbou, která způsobila škodu.
- **Dopad** – škoda, kterou incident způsobil organizaci nebo některým zájmovým skupinám.
- **Opatření** – krok/akce, které mají předcházet přeměně hrozby na incident.
- **Politiky** – soubor pravidel a opatření určených k řízení rizik.
- **Zralost** – úroveň vyspělosti procesů řízení rizik v organizaci.
- **Štěstí** – je to co budete potřebovat.

Opatření aneb povinnost No. 3.

- Jsou určeny Vyhláškami:
 - Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností
 - **Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností (dále jen Vyhláška)**
- Přichází čas pro **gap analýzu**
- **Popis stavu implementace povinných opatření, naplánování jejich implementace, implementace a pravidelný přezkum je jednou ze základních povinností (i pro nepovinné)**

Seznam bezpečnostních opatření (nižší povinnosti)

- §4 **systém zajišťování minimální kybernetické bezpečnosti,**
- §5 **požadavky na vrcholné vedení,**
řízení aktiv – není rozpracováno ve Vyhlášce, ale máme zde §12
řízení rizik – není rozpracováno ve Vyhlášce
- §6 **bezpečnost lidských zdrojů,**
- §7 řízení kontinuity činností,
- §8 řízení přístupu,
- §9 řízení identit a jejich oprávnění,
- §10 **detekce a zaznamenávání kybernetických bezpečnostních událostí,**
- §11 **řešení kybernetických bezpečnostních incidentů,**
- §12 bezpečnost komunikačních sítí,
- §13 aplikační bezpečnost a
- §14 kryptografické algoritmy



Seznam bezpečnostních opatření (vyšší povinnosti)

- **organizační opatření**

1. systém řízení bezpečnosti informací,
2. požadavky na vrcholné vedení,
3. bezpečnostní role,
4. řízení bezpečnostní politiky a bezpečnostní dokumentace,
5. řízení aktiv,
6. řízení rizik,
7. řízení dodavatelů,
8. bezpečnost lidských zdrojů,
9. řízení změn,
10. akvizice, vývoj a údržba,
11. řízení přístupu,
12. zvládání kybernetických bezpečnostních událostí a incidentů,
13. řízení kontinuity činností a
14. provádění auditu kybernetické bezpečnosti



Seznam bezpečnostních opatření (vyšší povinnosti)

- **technická opatření**

1. fyzická bezpečnost,
2. bezpečnost komunikačních sítí,
3. správa a ověřování identit,
4. řízení přístupových práv a oprávnění,
5. detekce kybernetických bezpečnostních událostí,
6. zaznamenávání událostí,
7. vyhodnocování kybernetických bezpečnostních událostí,
8. aplikační bezpečnost,
9. kryptografické algoritmy,
10. zajišťování dostupnosti regulované služby a
11. zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv.



Další zbytečnosti?

CYBERSECURITY BASICS

Cyber criminals target companies of all sizes.

Knowing some cybersecurity basics and putting them in practice will help you protect your business and reduce the risk of a cyber attack.

PROTECT ——— YOUR FILES & DEVICES



Update your software

This includes your apps, web browsers, and operating systems. Set updates to happen automatically.



Secure your files

Back up important files offline, on an external hard drive, or in the cloud. Make sure you store your paper files securely, too.



Require passwords

Use passwords for all laptops, tablets, and smartphones. Don't leave these devices unattended in public places.



Encrypt devices

Encrypt devices and other media that contain sensitive personal information. This includes laptops, tablets, smartphones, removable drives, backup tapes, and cloud storage solutions.



Use multi-factor authentication

Require multi-factor authentication to access areas of your network with sensitive information. This requires additional steps beyond logging in with a password — like a temporary code on a smartphone or a key that's inserted into a computer.

V případě zájmu pošlu
nebo stahujte

https://www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecurity_small_business_factsheets_all.pdf

Federal Trade
Commission (.gov)



Povinnosti číslo 4. (§ 59 – Přestupky)

- a) Nehlásí změnu regulované služby (175 MKč),
- b) nehlásí kontaktní nebo doplňující údaje nebo jejich změnu (50 MKč),
- c) neurčí za účelem vymezení stanoveného rozsahu všechna primární aktiva nebo podpůrná aktiva, nebo jejich určení pravidelně nepřezkoumává nebo neaktualizuje (175 MKč),
- d) neposoudí za účelem vymezení stanoveného rozsahu, zda primární souvisí s poskytováním regulované služby nebo toto posouzení pravidelně nepřezkoumává nebo neaktualizuje podle (175 MKč),
- e) neeviduje aktiva (175 MKč),
- f) nezavádí nebo neprovádí bezpečnostní opatření (175 MKč),
- g) nevybírá svého dodavatele v souladu s požadavky vyplývajícími z bezpečnostního opatření nebo nezahrnuje požadavky vyplývající z bezpečnostního opatření do smlouvy s dodavatelem (175 MKč),



Kontrolní seznam povinností (§ 59 – Přestupky) – pokračování

- h) nepředloží prvotní hlášení o nebo nedoplní některý z údajů o incidentu nebo nenahlásí kybernetický bezpečnostní incident (175 MKč),
- i) neposkytne informace nebo součinnost při zvládnutí incidentu (175 MKč),
- j) neplní povinnost nebo zákaz informovat uživatele regulované služby o kybernetickém bezpečnostním incidentu s významným dopadem stanovený rozhodnutím Úřadu (175 MKč),
- k) neinformuje uživatele regulované služby o významné hrozbě a krocích, které může uživatel služby učinit v reakci na ni (175 MKč),
- l) neplní povinnost uloženou rozhodnutím o výstraze (175 MKč),
- m) neplní reaktivní protiopatření uložené podle (175 MKč),
- n) neoznámí provedení reaktivního protiopatření a jeho výsledek (35 MKč)
- o) neplní povinnost uloženou nápravným opatřením (175 MKč).



Něco pro neregulované - (§ 60 – Přestupky dalších osob)

- a) **nesplní povinnost ohlásit službu (regulovanou) Úřadu,**
- b) neposkytne informace nebo součinnost při zvládnutí incidentu,
- c) neposkytne nezbytnou součinnost při zajišťování podkladů pro vydání protiopatření.
- d) nesplní povinnost uloženou rozhodnutím.
- e) neposkytne nezbytnou součinnost na základě žádosti řadu,
- f) v souvislosti se stavem kybernetického nebezpečí nesplní povinnost provést opatření k řešení značného ohrožení nebo narušení bezpečnosti informací v kybernetickém prostoru uloženou rozhodnutím nebo opatřením obecné povahy,
- g) nesplní povinnost uloženou nápravným opatřením,
- h) v rozporu s rozhodnutím o zákazu výkonu funkce tuto funkci dále vykonává, nebo
- i) neposkytne informace nebo jinou součinnost nezbytnou k posouzení splnění podmínek.



NÚKIB je vlastně taková kyberhygiiena.

Povinnosti číslo 5. – Papíre

- Bezpečnostní politiky a
- bezpečnostní dokumentace.

- Původně byly uvedeny výčtem v přílohách Vyhlášky o nižších povinnostech
- Nyní jsou **navázány na jednotlivá povinná opatření** (výborný počín NÚKIBu)

Pište papíre, které odpovídají skutečné implementaci ve Vaší organizaci.



Jak by mohl vypadat projekt implementace NIS2

- Proškolit vedení
- Stanovení rozsahu (§12 Zákona)
- Začít přemýšlet o dopadech (nedáte to na poprvé)
- Mrknout na povinná opatření, začít dělat tabulku a plánovat kdy se do čeho pustíte
- Začít přemýšlet o obsazení rolí a začít je obsazovat:
 - Osoba odpovědná za kybernetickou bezpečnost
 - Osoby určené pro komunikaci s NÚKIBem
 - **Garanti aktiv**
- Implementovat opatření
- Papíre psát až po implementaci (politiky lze psát trochu dříve)
- Sledovat jaké podpůrné materiály vydá NÚKIB a vhodně je použít

02.12.2024



Nezapomeňte – k diskuzi

- Regulovaná služba ORP se nazývá **Výkon svěřených pravomocí**
- Poskytovatel regulované služby je **obec s rozšířenou působností** nikoliv obecní úřad

Kde hledat primární aktiva pro orgány veřejné moci?

- Ideálně asi **Registr práv a povinností**
- Ale bude snazší se podívat do **organizačního řádu** případně statutu

Přenesené povinnosti

ORP je v podstatě dodavatel, pravidla by měl dát vlastník agendy

02.12.2024

„Nezáleží na tom, že se to nestalo až do důsledků. Důležitý je, že se to mohlo stát.“

(Jiří Sovák ve filmu Světáci)



Otázky?

Ostrava

02.12.2024



Rajské služby

- Školení vedení – prokazatelné seznámení.
- Stanovení rozsahu – katalog primárních aktiv.
- Gap na povinná opatření – popis aktuálního stavu.
- Školení osoby odpovědné za kybernetickou bezpečnost (ve spolupráci s partnery).
- Dohled na implementaci.
- S našimi skvělými partnery spoustu dalších věcí.



Děkuji za pozornost

E: petr@pribehrajske.cz

M: +420 703 404 004

W: www.pribehrajske.cz

IT PRO TY, CO UMÍ
HLAVNĚ JINÉ VĚCI

Myslím, že na světě je spousta lidí, kteří dovedou úžasné věci, ale my jim nučíme svou představu IT světa, ve kterém se necítí zrovna komfortně.