**Kybernetická a informační bezpečnost**

**Úvod do problematiky a metodický rámec**

Dokument byl zpracován v rámci realizace projektu

„Efektivní řízení rozvoje obcí jako základní předpoklad efektivnosti výkonu veřejné správy

a poskytování veřejných služeb z úrovně obcí“,

registrační číslo projektu: č.CZ.03.4.74/0.0/0.0/15\_019/0010159

**Preambule**

Promořenost naší společnosti informačními a komunikačními technologiemi (ICT) a tím i naše závislost na nich neustále roste. Už je velmi těžké najít obor lidské činnosti, kde bychom se s těmito technologiemi nesetkali. To se týká i obcí, a to o to výrazněji, čím více se prosazuje elektronizace veřejné správy e-government. Zvykli jsme si na tyto technologie tak, že je za sebe necháme rozhodovat, řídit stroje, technologické procesy, auta, zdravotnickou techniku a mnoho dalšího. Jenže abychom se na ně mohli spolehnout, musíme technologie a procesy, ale také informace a systémy dobře zabezpečit. A k tomu slouží kybernetická a informační bezpečnost. V následujících odstavcích se na tuto disciplínu podíváme v širších souvislostech. Dozvíme se něco o legislativě a také o tom, jak se chovat bezpečně a obezřetně v kyberprostoru, který je zmíněnými technologiemi, systémy, procesy, informacemi a také lidmi tvořen.

**Úvod do kybernetické a informační bezpečnosti**

Nejdříve je nutno vyvrátit mýtus, že je kybernetická a informační bezpečnost (někdy také KIB) pouze záležitostí odborníků na informační a komunikační technologie (ICT) nebo specialistů na kybernetickou a informační bezpečnost. Opak je pravdou. Je to záležitost úplně všech, protože tyto technologie a jejich služby používáme všichni a je jedno, jestli doma nebo v práci. Vždy musíme mít na paměti, že kyberprostor (pro většinu běžných uživatelů představovaný internetem) není prostorem absolutního dobra a absolutní svobody. Ano, poskytuje nám pohodlí při rozhodování, poskytuje vzdělání, kulturu, zábavu, komunikaci napříč celým světem a mnoho dalších příjemných věcí. Je ale také rejdištěm kriminálních živlů, kyberšpionů, podvodníků, a zuří zde kybernetické války. Proto je nutné systémy a informace chránit a neustále se v tom zdokonalovat, protože druhá strana je vždy o krok napřed. Zlepšovat se musíme jak v úrovni technologií, tak hlavně v úrovni povědomí uživatelů o kybernetické a informační bezpečnosti. Což je s ohledem na medializované případy úspěšných kybernetický útoků téměř samozřejmostí.

Další rozšířený mýtus je ten, že kybernetickou a informační bezpečnost musí řešit jen ty instituce, které spadají pod zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Tak to ale není. Moje motto je „Kybernetická a informační bezpečnost není otázkou zákonů, je otázkou pudu sebezáchovy“. A je jedno, jestli se jedná o jednotlivce, firmu, úřad, stát nebo nebo společenství států postavené na jakémkoliv základě (NATO, EU apod.).

**Kybernetická a informační bezpečnost v souvislostech**

Považuji za velmi důležité uvést obecné souvislosti, protože bez nich si nelze uvědomit závažnost situace, a tím i nutnost se kybernetické a informační bezpečnosti věnovat a dostat ji do povědomí jako např. chování na silnici.

1. **Souvislost rozhodovací**

Nejprve si řekněme, co to jsou **informace**. Podle jedné z definic jsou to přesná a včasná data, která mají svojí specifikaci a jsou organizována za účelem prezentace v takovém kontextu, který dává smysl a význam. Jejich cílem je zvýšení porozumění a snížení nejistoty. Informace mají svoji důležitost, jelikož dokáží ovlivnit chování, rozhodování nebo výsledky. Co to v praxi znamená? Že informace sníží naši nejistotu (respektive zvýší naši jistotu) při rozhodování. Představte si, že chcete přejít na druhou stranu ulice, vyhodnotíte informaci, že na semaforu svítí zelená, a tedy se rozhodnete ulici přejít. Doporučuji se pro jistotu podívat, jestli se na vás neřítí auto s nezodpovědným řidičem. Takže jste se rozhodli na základě informací. A teď si představte, že ten semafor řídí počítač. A někdo, ať už úmyslně nebo neúmyslně, změnil nastavení tak, že vy i ten řidič máte zelenou. Oba jste se rozhodli správně, ale na základě špatných informací. Podívejme se na obrázek, který názorně ukáže cestu od dat k rozhodnutí (tento obrázek mimo jiné ilustruje, o čem celá informatika je).

Data

Informace

Rozhodnutí

Interpretace

Kontext

Obr. č.1 Od dat k rozhodnutí

Na obrázku vidíme znázorněnou cestu, kterou urazí data až k rozhodnutí. Představte si stroj, u kterého potřebujete řídit otáčky. Data, to je počet otáček za minutu. Data jsou ovšem ve tvaru nul a jedniček, takže nám nic neřeknout. Proto ty nuly a jedničky potřebujeme interpretovat (přeložit) tak, abychom z nich udělali smysluplnou informaci. Teď už víme, že se jedná o otáčky motoru s jakousi hodnotou, např. 1 000 otáček za minutu. Musíme je dát ovšem do nějakého kontextu. V zásadě to znamená vědět, jestli je počet otáček dobrý, nebo špatný a jestli je máme snížit, nebo zvýšit. Takže se musíme rozhodnout. A proč to dávám do souvislosti s kybernetickou a informační bezpečností? Protože v každé části zobrazeného řetězce se dají data zfalšovat nebo podvrhnout a tím fatálně ovlivnit rozhodnutí. A je jedno, jestli se rozhoduje člověk nebo počítač.

***Z praxe:*** *Zařízení pro obohacování uranu v Íránu bylo napadeno virem Stuxnet (zlí jazykové tvrdí, že to byl výsledek spolupráce USA a Izraele). Virus způsobil to, že dispečeři na řídicím pracovišti dostali na monitory informaci, že otáčky centrifug jsou v pořádku, a to i přes to, že je virus zvýšil nad kritickou mez. Na základě této falešné informace přijali fatální rozhodnutí – nedělat nic. Cca 1 000 centrifug bylo fyzicky zničeno a íránský jaderný program se v podstatě zastavil.*

V kybernetické a informační bezpečnosti je nutno zajistit tři základní parametry. Důvěrnost – to znamená, že do systému, k jeho službám, k informacím se dostane jen ten, kdo na to má oprávnění, kdo to potřebuje ke své legitimní práci. V případě Stuxnetu došlo jednoznačně k narušení důvěrnosti. Ten virus tam prostě neměl co dělat. Dalším parametrem je Integrita – ta znamená, že ten, kdo má oprávnění, se může na informace, služby a systémy spolehnout, že jsou správné. Což v případě Stuxnetu také splněno nebylo. A poslední parametr Dostupnost – ten, kdo má oprávnění, se k informacím dostane v čase, ve kterém je potřebuje ke své práci. Dispečeři se sice k informacím dostali, ale ty byly falešné.

***Z praxe:*** *V Benešovské nemocnici zaútočil Ransomware (program, který se dostane do počítačů a zašifruje všechna data; kybergangsteři, kteří to způsobili, potom požadují výkupné za obnovení provozu). Nemocnice byla totálně paralyzována a škody dosáhly výše kolem 70 milionů korun. Který z výše uvedených parametrů byl narušen? Nebudu vás napínat, všechny tři. Důvěrnost – ten virus tam neměl co dělat, integrita – data byla změněna, dostupnost – lékaři se nemohli dostat k dokumentaci pacientů a nemohli léčit.*

1. **Souvislost motivační**

Zde si vysvětlíme, proč to útočníci dělají. Co je vede k tomu, že páchají takové škody a ohrožují životy lidí? První a základní odpověď je, protože to jde a vyplatí se to. Je nasnadě, že se jednotlivé motivace můžou kombinovat, např. kybernetická špionáž za peníze apod.

**Peníze**

V kyberzločinu se ročně protočí více peněz než v obchodu s drogami. Současný odhad je kolem 3 bilionů dolarů ročně. A roste to. Kybergangsteři používají různé techniky, jak k penězům přijít. Nejvýnosnější jsou v současné době nelegální e-shopy, které tvoří zhruba 50 % z celkových výnosů. Bavíme se o těch e-shopech, kde si něco objednáte, zaplatíte a nic vám nepřijde, nebo přijde něco jiného. Na dalším místě žebříčku jsou krádeže informací, duševního vlastnictví, výsledků výzkumů apod. Na trhu s informacemi jsou jedněmi z nejdražších zdravotnické záznamy – až 5 000 USD za kus. Když si uvědomíme, že i celebrity a politici chodí k lékaři, je ta cena pochopitelná. Samozřejmě sem patří i již zmíněný ransomware.

***Z praxe:*** *V Singapuru došlo k odcizení 1 500 000 zdravotnických záznamů. Nakonec bylo zjištěno, že kyberzloději hledali informace o zdravotním stavu premiéra.*

**Hacktivismus**

Slovo hacktivismus je složeno ze slov hacking a aktivismus. Zde jde například o vyjádření politických postojů nebo nesouhlasu s nějakým jednáním cestou hackerského útoku na příslušnou instituci. V poslední době je asi nejznámější aktivita skupiny Anonymous v souvislosti s válkou na Ukrajině. Typické pro hacktivistické útoky je to, že se útočníci přiznají a svou motivaci vysvětlí. Nejčastějším používaným typem útoku je tzv. DDoS. Zde se jedná o zahlcení serverů oběti takovým množstvím dotazů, že se servery zhroutí. Je to, jako by vám 1 000 lidí položilo různé otázky ve stejnou vteřinu a všichni chtěli okamžitou odpověď.

**Konkurenční boj**

Ani konkurenční boj neopomíjí možnosti hackerských útoků. Jde zde o to zpochybnit kvalitu konkurenční firmy a tím zabrat její místo na trhu. Nejhorší je, že útoky lze koupit za pár dolarů, aniž byste byli odborníky. Stačí objednat a zaplatit.

***Z praxe:*** *Jedna nejmenovaná firma A poskytuje služby ve větším městě v rámci dopravní infrastruktury. Její konkurence, firma B, pomocí kybernetického útoku narušila funkčnost firmou A spravovaných zařízení s cílem znevěrohodnit firmu A, a dostat se na její místo na trhu.*

**Kybernetická špionáž**

Zde je v zásadě jedno, jestli se jedná o špionáž v rámci konkurenčního boje nebo stát versus stát. Často to provádějí tzv. státem podporovaní aktéři. To jsou hackerské skupiny, které řídí nebo podporuje stát. Techniky jsou stejné. Je nutno zmínit, že se tak děje ve spolupráci s „klasickými“ zpravodajskými službami. Zajímavý byl nárůst útoků s cílem získat zdravotnické informace, které vedl stát (nebo státem podporovaní aktéři) proti zdravotnickým zařízením jiného státu.

**Kybernetické války**

Kyberprostor se stal 5. válečným prostorem vedle země, vody, vzduchu a vesmíru. Tak to vnímá NATO. Nárůst kybernetických útoků na kritickou infrastrukturu v rámci války na Ukrajině to jen dokazuje. Armády už mají své jednotky kybernetické obrany. U nás je to Vojenské zpravodajství, které má i kompetenci kybernetického protiútoku.

Vyjmenoval jsem jen ty základní motivace kybernetických útočníků, protože rozsah kapitoly více nedovoluje.

1. **Legislativa**

Co se týká kybernetické a informační bezpečnosti, Česká republika disponuje speciální legislativou, reprezentovanou již zmíněným zákonem č. 181/2014 Sb.,[[1]](#footnote-1) o kybernetické bezpečnosti (ZoKB) a nejpodstatnější navazující vyhláškou č. 82/2018 Sb.,[[2]](#footnote-2) o kybernetické bezpečnosti (VoKB), která je k zákonu prováděcím předpisem. Na zákon navazují i další vyhlášky, ale pro obce je nejpodstatnější ta právě zmíněná, protože poskytuje návod, jak ke kybernetické a informační bezpečnosti přistoupit, jak ji zavést, řídit a rozvíjet. A to i přesto, že obce zatím pod zákon o kybernetické bezpečnosti nespadají. Neboť jak už bylo řečeno, spoléhat na to, že pod zákon nespadáme, je cestou do pekla. Hackerům je totiž úplně jedno, jestli oběť pod zákon spadá nebo ne. A vězte, že pro ně neexistují malé cíle. Regulátorem kybernetické a informační bezpečnosti je Národní úřad pro kybernetickou a informační bezpečnost [[3]](#footnote-3) (NÚKIB), který kromě toho, že kontroluje dodržování ZoKB ze strany osob povinných, tak vyvíjí intenzivní osvětovou činnost a vydává řadu metodických materiálů, které pomáhají všem institucím právě v zavádění, řízení a rozvíjení kybernetické a informační bezpečnosti, a to bez ohledu na jejich zákonnou povinnost v této oblasti. To, že obce pod ZoKB nespadají, už nebude mít dlouhého trvání. V souvislosti s novelou evropské směrnice o bezpečnosti sítí a informací (známá též jako NIS 2) je připravována i změna národní legislativy, která podle dosavadních diskusí zahrne pod ZoKB i obce s rozšířenou působností (ORP). To znamená, že dopad legislativy kybernetické bezpečnosti se výrazně zvětší. Co ale s menšími obcemi? Možná by stálo za to, aby kraje poskytovaly ORP i ostatním obcím kybernetickou a informační bezpečnost jako službu. To je ale varianta na zvážení. Jaké praktické dopady bude mít nutnost zavedení kybernetické a informační bezpečnosti na obce? Ať už bude zvolena kterákoliv varianta – každá obec sama za sebe, služba obcím ze strany ORP, z kraje nebo centrálně (zatím docela sci-fi představa), je zřejmé, že každá obec k této problematice bude muset zodpovědně přistoupit. NÚKIB vydal dokument Minimální bezpečnostní standard [[4]](#footnote-4), který popisuje v intencích VoKB, jaká opatření z pohledu kybernetické a informační bezpečnosti zavést. Jeho velkou nevýhodou je to, že je poměrně rozsáhlý (46 stran) a předpokládá, že řadu pojmů už čtenář zná. Zmíněný dokument lze využít tam, kde existuje vůle a tým odborníků, který jej dokáže uvést do praxe. A je jedno, jestli se jedná o zaměstnance nebo externí firmy, které tyto činnosti zajišťují jako službu.

1. **Praktická realizace z pohledu obce**

V první řadě bychom si měli přestat lhát, že se nás tato problematika netýká. Týká. Z této sebereflexe jasně vyplývá, že se kybernetickou a informační bezpečností obec bude chtít zabývat.

Dále je velmi důležité vytvořit vnitřní legislativní ráme pro zavedení opatření kybernetické a informační bezpečnosti .

* 1. **Zmapování situace**

To musí vycházet především z analýzy rizik. Není třeba se tohoto pojmu lekat. Tato analýza vychází z otázky „Co se stane když“. Je zřejmé, že výpadek evidence poplatků za psy reputaci obce výrazně neohrozí, výpadek komunikace s registrem vozidel nebo řidičů už generuje vysoké reputační riziko a pochybnosti občanů o důvěryhodnosti reprezentace obce. Proto je důležité vytvořit si katalog klíčových služeb, poskytovaných občanům, těch, které jsou určeny jako zákonná povinnost obce apod. V této souvislosti je velmi důležité mít jasno o vlastní informační a komunikační infrastruktuře a jejím zabezpečení, neboť na správném a bezpečném fungování informační a komunikační infrastruktury je závislé poskytování klíčových služeb. Co to znamená? Mít zdokumentováno (i graficky), jaké technologie jsou v obci používány, kde jsou umístěny a kdo je spravuje. Zde je podstatné mít vytvořenou i komunikační matici s kontakty na odborníky, kteří jsou správci technologií, ale i systémů. Dále je podstatné mít jakýsi katalog informačních systémů, které obec používá pro svoji činnost. A ten musí být vytvořen s velkou péčí. Nespoléhejte na to, co nosí „ajťáci“ v hlavách. Při tvorbě tohoto katalogu se bez nich neobejdete a je velmi těžké je k tomu přesvědčit, ale věřte mi, že v případě výpadků je to velmi důležitý podklad pro úspěšný návrat k normálnímu stavu. Do tohoto katalogu zahrňte všechny systémy (aplikace), které používáte a které vaše klíčové služby podporují. Od evidence poplatků za psy, přes ekonomické informační systémy až po komunikaci s centrálními registry. A stanovte si u nich priority, tzn. v jakém pořadí a v jakých časech má být jejich činnost po výpadku obnovena. Je zřejmé, že evidence poplatků za psy má nižší prioritu než matrika jako systém, kde jsou krátké zákonné lhůty.

***Z praxe:*** *Úřad městské části Praha 5 se stal cílem hackerského útoku. Díky tomu, že měl zpracován tzv. DRP (Disaster recovery plan – plán obnovy po výpadku), se s touto situací dokázal vyrovnat v téměř zázračně krátké době 9 dnů.*

* 1. **Bezpečnostní opatření**

Udělejte si jasno, jaká bezpečnostní opatření máte zavedena, a porovnejte to s tím, co o nich říká VoKB nebo Minimální bezpečnostní standard. VoKB hovoří o organizačních opatřeních a technických opatřeních. Jedním z organizačních opatření je vytvoření jasného obrazu o situaci. Aktuální opatření si přiměřeně popište, nemusí to ale být dokumenty o desítkách stran. Důležitá je jejich vypovídací hodnota a aby byl obraz jasný a zřetelný. Ruku v ruce s tím jde obraz o technických opatřeních, tedy o tom, jaké používáte bezpečnostní technologie (antiviry, firewally apod.). Pokud si vytvoříte pravdivý obraz o vašich aktuálních opatřeních, potom můžete vytvořit plán zavádění opatření, ve kterém si stanovíte postup, jak identifikované nedostatky odstranit. Doporučuji vaše zjištění porovnávat s požadavky VoKB nebo s Minimálním bezpečnostním standardem, který stejně z VoKB vychází.

Mějte také přehled o svých dodavatelích a mějte je zavázané smlouvou, ve které bude mít podchycenou i úroveň jimi poskytovaných služeb (SLA – servis level agreement). Taková smlouva např. říká, v jakých časech musí dodavatel reagovat na výpadek nějaké služby a do kdy musí být výpadek odstraněn. I to vzejde z analýzy rizik. Nespoléhejte na kamarády, kteří „umí s počítači“. I zde platí, že musíte mít komunikační matici s aktuálními kontakty.

Nezapomeňte vedle zavedení organizačních a technických opatření na vzdělávání uživatelů. Ti jsou největší hrozbou pro kybernetickou a informační bezpečnost každé instituce. A útočníci na to spoléhají. I ve zmíněné benešovské nemocnici došlo k tomu, že nepoučený uživatel kliknul na zavirovanou přílohu škodlivého e-mailu (tzv. phishing) a malér byl na světě. Na závěr uvádím jakési desatero (ono je těch bodů víc) toho, co by měl každý uživatel vědět o tom, jak se nechovat. Je to ten úplný základ, se kterým by se měl seznámit každý zaměstnanec hned při nástupu. Toto seznámení musí být prokazatelné stejně jako BOZP. Doporučuji typicky do tří měsíců doplnit a prohloubit e-learningovým kursem NÚKIB Dávej kyber[[5]](#footnote-5), který je zcela zdarma a pokrývá celou problematiku Kybernetické a informační bezpečnosti na uživatelské úrovni. O absolvování dostane uživatel certifikát, který je pro jeho zaměstnavatele důkazem o tom, že byl poučen, což může hrát svoji roli při řešení sporů po uživatelem způsobené škodě.

Velmi důležité je také vzdělávání IT specialistů a bezpečnostních specialistů. I tady lze využít e-learningový kurs z dílny NÚKIB Šéfuj kyber [[6]](#footnote-6) . Pokud jsou to externisté, požadujte od nich prokázání příslušné kvalifikace. To, že je to baví, nestačí.

Nelze v rozsahu tohoto dokumentu probrat detailně všechna bezpečnostní opatření, proto uvádím pro vaši orientaci jejich seznam s velmi stručnými komentáři. Detailní popis najdete zde na webových stránkách Zákony pro lidi.[[7]](#footnote-7) Při zavádění mějte vždy na paměti princip přiměřenosti, který by měl odpovídat velikosti obce a také rozsáhlosti její informační a komunikační infrastruktury. Je zřejmé, že obci I. typu stačí evidence základních informací o tom jaké, kde a kým mají spravované informační systémy, na této úrovni spíše aplikace. Často se jedná o jeden až dva počítače, které spravuje externí specialista v rámci správy takovýchto systémů pro více takovýchto obcí. To znamená, že investice do zajištění kybernetické a informační bezpečnosti jsou na odpovídající (minimální) úrovni s reflektováním faktu, že i přesto má být úroveň zabezpečení maximálně možná. Jiná situace je u větších obcí nebo měst. Zde se vedení obce může opřít o tým odborníků s technologickým zázemím na daleko vyšší úrovni. Přiměřenost vyplývá z analýzy rizik, kterou si každá obec musí vyhodnotit, byť i na úrovni mentálního cvičení, tedy zamyšlení. I úroveň a hloubka této analýzy se odvíjí od velikosti obce a velikosti její informační a komunikační infrastruktury. Je také dobré si uvědomit, že celá řada zmíněných opatření (někdy i všechna) se dá koupit jako služba. U každého opatření uvádím hypertextový odkaz na příslušný paragraf VoKB.

1. **Bezpečnostní opatření s komentáři**
   1. **Organizační opatření**

**Systém řízení bezpečnosti informací[[8]](#footnote-8)** - (někdy také ISMS – Information security management system)

Zavedením tohoto opatření si obec vytvoří dokumentaci ke své informační a komunikační infrastruktuře, zavede řízení rizik, stanoví si cíle bezpečnosti, vytvoří bezpečnostní dokumentaci apod**.**

**Řízení aktiv[[9]](#footnote-9)**

Aktivum je to, co má pro obec hodnotu. V oblasti informačních aktiv pracujeme s dvěma kategoriemi – primární aktiva (zde se jedná o služby a informace) a podpůrná (hardware, software, technologie, budovy, zaměstnanci, jejich znalosti atd.) Je tedy důležité vědět, které to jsou, a znát jejich důležitost s ohledem na chod obce. Zde je navýsost důležitá dokumentace.

Národní úřad pro kybernetickou a informační bezpečnost nedávno vydal dokument „Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti“, který je kvalitním návodem jak s aktivy a riziky pracovat. Nicméně e poměrně rozsáhlý (90 stran) a vyžaduje jistou míru teoretických znalostí zkušeností a jeho rozbor překračuje rámec tohoto dokumentu. V každém případě stojí za to se jím inspirovat hlavně co se týká např. formulářů pro evidenci aktiv a typových hodnocení hrozeb, zranitelností, dopadů a ztrát.[[10]](#footnote-10)

**Řízení rizik[[11]](#footnote-11)**

Jak už bylo řečeno, řízením rizik lze identifikovat problematická místa. Co se týká metodiky, doporučuji se řídit přílohou již zmíněné VoKB. Je velmi důležité s výstupy analýzy rizik pracovat a zavést opatření pro zmírnění jejich dopadu. V šuplíku jsou k ničemu. Řízení rizik je jediná cesta, jak opatření zavést efektivně bez zbytečně vysokých nákladů. Nemá cenu korunovou hodnotu chránit milionovým opatřením a naopak. S řízením rizik souvisí i příslušná dokumentace (viz VoKB).

Doporučuji se zaměřit na rizika:

* + ohrožení života a zdraví,
  + finanční ztráty (např. sankce za neplnění zákonných povinností, náklady na odstranění následků kybernetického útoku apod.)
  + ohrožení reputace obce a její reprezentace,
  + neplnění zákonných povinností apod.
  + rizika která souvisí s ochranou práv a svobod občanů obce (GDPR – téma, které je řešeno v předchozí kapitole)

To znamená vyhodnotit, že pokud dojde k výpadku některé služby, podporované správnou funkčností informační a komunikační infrastruktury, která rizika hrozí a jaký to bude mít dopad na chod obce, služby poskytované občanům, komunikaci s centrálními systémy atd.

**Organizační bezpečnost[[12]](#footnote-12)**

Zde je důležité zajistit integraci systému pro řízení bezpečnosti informací do všech procesů v obci, a to opět v přiměřené míře. Tento bod je také o identifikaci osob, které se budou kybernetickou a informační bezpečností zabývat z hlediska své funkce, a tím pádem se za její stav budou zodpovídat vedení obce. Nutno si však uvědomit, že za tuto oblast vždy zodpovídá statutár.

**Bezpečnostní role[[13]](#footnote-13)**

Tam, kde to dává smysl nebo to určuje ZoKB, jsou bezpečnostní role vytvořeny a jsou jim přiděleny odpovídající kompetence. Tento bod se týká spíše větších obcí. Bezpečnostní role jsou typicky manažer kybernetické bezpečnosti, architekt kybernetické bezpečnosti, garant aktiva a auditor kybernetické bezpečnosti. Tyto role lze zajistit externím subjektem jako službu.

**Řízení dodavatelů[[14]](#footnote-14)**

Toto je velmi důležitý bod, protože stále narážíme na to, že obce jsou v područí svých dodavatelů a smlouvy jsou postaveny tak, že vyhovují spíše jim než obcím. Proto doporučuji věnovat zvýšenou péči těmto smlouvám a při jejich tvorbě se inspirovat VoKB, kde naleznete i doporučený obsah takovéto smlouvy, a jak obecně k dodavatelům přistupovat.

**Bezpečnost lidských zdrojů[[15]](#footnote-15)**

Toto opatření už jsem částečně zmínil výše a týká se vzdělávání jak uživatelů, tak i IT administrátorů a bezpečnostních specialistů. Také hovoří o nutnosti kontrolovat dodržování pravidel kybernetické a informační bezpečnosti z jejich strany.

**Řízení provozu a komunikací (elektronických)[[16]](#footnote-16)**

Obsahem tohoto opatření jsou povinnosti, které obec plní při zajištění bezpečného a spolehlivého provozu informační a komunikační infrastruktury. Jsou to např. práva a povinnosti administrátorů, postupy pro obnovení chodu po výpadku, spojení na kontaktní osoby a další.

**Řízení změn[[17]](#footnote-17)**

Každá významná změna (např. instalace nové verze aplikace) by měla být plánována, měla by jí předcházet analýza rizik, měla by být testována (v testovacím prostředí) a samozřejmě dokumentována.

**Řízení přístupu[[18]](#footnote-18)**

Přístup ke všem prvkům informační a komunikační infrastruktury musí být řízen tak, aby byla zajištěna jejich ochrana. Důležité je nastavit přístupová oprávnění podle skupin a rolí, v žádném případě ne na základě známosti. Je zřejmé, že paní účetní bude mít přístup k jiným systémům a s jinou úrovní oprávnění než administrátor.

**Akvizice, vývoj a údržba[[19]](#footnote-19)**

V tomto opatření si obec stanoví požadavky na bezpečný vlastní vývoj aplikací, jejich testování a údržbu. Velmi problematické je tzv. šedé IT, kdy se v informační a komunikační infrastruktuře neřízeně provozují aplikace, které často bez jakýchkoliv pravidel přistupují k citlivým údajům. Zavedením těchto opatření by se měla minimalizovat rizika z toho plynoucí.

**Zvládání kybernetických bezpečnostních událostí a incidentů[[20]](#footnote-20)**

Tímto opatřením si definujete, jak postupovat v případě, že se děje něco, co by chod informační a komunikační infrastruktury mohlo ohrozit (událost), nebo už ohrozilo (incident). Tedy jak to poznat (detekce), vyhodnotit a zvládnout tuto situaci.

**Řízení kontinuity činností[[21]](#footnote-21)**

Tímto opatřením jsou definovány parametry a nastavení procesu, který se spustí po např. výpadku některého ze systémů. Souvisí s nastavením jejich priorit, definuje do kdy a v jakém pořadí má být chod systému obnoven a co je nutno vykonat pro to, aby tyto parametry byly dodrženy.

**Audit kybernetické bezpečnosti[[22]](#footnote-22)**

VoKB stanoví, kdo a v jakých intervalech provádí audit kybernetické bezpečnosti. Toto opatření se týká spíše větších obcí, nicméně i menší obec by měla mít aktuální přehled o tom, jak na tom s kybernetickou a informační bezpečností je.

1. **Technická opatření**

**Fyzická bezpečnost[[23]](#footnote-23)**

Fyzická bezpečnost je důležitým prvkem kybernetické a informační bezpečnosti, neboť se týká zabezpečení jejích prvků (hlavně technologií) před odcizením, fyzickým poškozením apod. I zde je důležité vycházet z analýzy rizik, aby byly prvky fyzické bezpečnosti nastaveny přiměřeně. Aby např. běžná místnost (např. kancelář) , nebyla zabezpečena stejně jako serverovna.

**Bezpečnost komunikačních sítí[[24]](#footnote-24)**

Toto opatření definuje, jaké principy a technologie mají být pro zabezpečení komunikačních sítí použity. Pozor, nejedná se o použití technologií konkrétních výrobců.

**Správa a ověřování identit[[25]](#footnote-25)**

Zde jsou uvedeny parametry, které má splňovat nástroj pro ověřování identit (tzv. IDM – Identity management).

**Řízení přístupových oprávnění[[26]](#footnote-26)**

I zde jde o definici parametrů nástroje pro řízení přístupových oprávnění, který zajistí to, že role mají různé úrovně oprávnění. Většino to technologicky řeší výše uvedený nástroj pro ověřování identit.

**Ochrana před škodlivým kódem[[27]](#footnote-27)**

Toto opatření říká, že musí být použit nástroj pro ochranu před škodlivým kódem. Ve velmi velkém zjednodušení si pod tímto nástrojem lze představit antivir. Toto opatření říká, kde všude má být nasazen, co všechno má chránit, že má být aktualizován apod.

**Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů[[28]](#footnote-28)**

Toto opatření popisuje parametry nástroje pro zaznamenávání událostí (tzv. logů), ze kterých lze vyhodnotit co, kdy, kdo a kde v informační a komunikační infrastruktuře dělal. Tyto záznamy jsou velmi důležité pro vyšetřování bezpečnostních událostí a incidentů.

**Detekce kybernetických bezpečnostních událostí[[29]](#footnote-29)**

Toto opatření popisuje parametry nástroje, který dokáže detekovat kybernetické bezpečnostní události (např. pokus o průnik), kde všude má být nasazen, co všechno má detekovat. Typicky se jedná o systém pro detekci průniku, resp. pokusu (IDS - Intrusion dection system) a systém pro prevenci průniku (IPS - Intrusion prevention system).

**Sběr a vyhodnocování kybernetických bezpečnostních událostí[[30]](#footnote-30)**

Opět se jedná o použití nástroje, jaké má splňovat parametry, co sbírat a vyhodnocovat, tak aby se dalo vyhodnotit, k jakým kybernetickým událostem došlo, v jakých časech, na kterých zařízeních apod. Až po možné zjištění příčiny události. Těch nástrojů je celá řada,

typicky se jedná o SIEM (Security Information and Event Management). Nelze je zde všechny vyjmenovat, protože se jedná o poměrně pokročilé technologie, jejichž podrobný popis přesahuje rámec této příručky

**Aplikační bezpečnost[[31]](#footnote-31)**

Toto opatření mimo jiné říká, kdy provádět penetrační testování důležitých prvků informační a komunikační infrastruktury. Jak zabezpečit aplikace atd.

**Kryptografické prostředky[[32]](#footnote-32)**

Toto opatření také definuje parametr kryptografických prostředků, kde je nasazovat a jak je spravovat.

**Zajišťování úrovně dostupnosti informací[[33]](#footnote-33)**

Zajištění dostupnost informačního a komunikačního systému pro splnění cílů kontinuity činností (viz výše) spočívá v zajištění odolnost informačního a komunikačního systému vůči kybernetickým bezpečnostním incidentům, které by mohly snížit jeho dostupnost, a to zabezpečením všech důležitých technických aktiv informačního a komunikačního systému, a to například redundancí těchto aktiv (například jejich zdvojením, vybudováním záložního datového centra). Způsob vyplyne z analýzy rizik

1. **Co nedělat**

Zde uvádím ty nejzákladnější zásady kybernetické a informační bezpečnosti, které by měl každý uživatel znát. Praxe ukázala, že je dobré, aby s těmito zásadami byl každý nový uživatel prokazatelně seznámen už při nástupu do zaměstnání (než poprvé položí ruce na klávesnici svěřené techniky)

1. Používejte služební zařízení (zejména PC a Notebook) pouze k plnění svých služebních nebo pracovních povinností, v souladu s účelem, ke kterému je zařízení určeno
2. Neprovádějte jakékoliv neoprávněné zásahy do operačního systému nebo software (např. instalaci vlastního SW, změna konfigurace)
3. U informací rozlišujte osoby nebo skupiny osob, komu jsou určeny nebo mohou být poskytovány s ohledem na jejich citlivost.
4. Pečlivě si chraňte svá zařízení před odcizením či zneužitím a přístupové údaje před jejich odhalením a zneužitím. Nepoužívejte služební emailovou adresu ani služební heslo pro externí webové služby. Přístupové údaje (zejména heslo nebo PIN) si nikam nepoznamenávejte (např. na papír, do diáře či telefonu). Nevyužívejte stejné přístupové údaje k více účtům, aplikacím či zařízením. Je nutné používat bezpečná hesla a pravidelně je měnit. Dodržovat zásadu, že hesla a PINy se nikomu nesdělují.
5. Neotvírejte neznámé emaily a zejména jejich přílohy, neotevírejte neznámé, neočekávané soubory. Soubory, které mají příponu typu exe, com, scr, pif a další mohou vést k ohrožení informačních systémů obce. Pokud se ve složce, kam se stahují soubory z webu, objeví neznámý soubor, neotevírejte ho. Může jít o infikovaný soubor, který byl bez vašeho vědomí stažen z nedůvěryhodné stránky. Oznamte tuto skutečnost prostřednictvím služby ServiceDesk.
6. Nenastavujte ani nepožadujte nastavení automatického přesměrování služebních e-mailů do soukromých e-mailových schránek.
7. Dodržujte zásadu uzamčené obrazovky stisknutím kláves Win+L či využití zkratky Ctrl+Alt+Del) a prázdného stolu (neponechávejte dokumenty bez dozoru volně na stole). Zamykejte zařízení (např. PC a notebook) pokud s ním nepracujete, a to zejména při odchodu z kanceláře.
8. Dbejte na zásady bezpečnosti při fyzickém přístupu do kanceláří a vyhrazených prostor. Neponechávejte v kanceláři jiné osoby bez dozoru a při odchodu kancelář vždy zamykejte. Dbejte na to, aby do vyhrazených prostor nevstupovaly neoprávněné osoby.
9. Používejte přidělená výměnná média (např. flash disk, CD, DVD) vždy zodpovědně a bezpečně. Nenechávejte je bez dozoru, a pokud je to možné tak je šifrujte. V případě nalezení neznámého výměnného média jej nepřipojujte ke svému zařízení bez předchozího prověření antivirem. Oznamte tuto skutečnost příslušným odborníkům.
10. Nesdílejte služební informace (dokumenty) cestou veřejných úložišť (Dropbox, Úschovna, Úložna apod.).
11. Nenavštěvujte nedůvěryhodné webové stránky a neklikejte na odkazy na neznámé či podezřelé webové stránky. Mezi typické znaky nedůvěryhodné webové stránky patří velké množství reklamy, vyskakovací okna, stránky měnící se bez akce uživatele, zahájení stahování bez vědomí uživatele apod. Preferujte webové stránky, které důvěrně znáte a jsou zabezpečeny protokolem https:// na začátku adresy.
12. V případě zjištění nestandardního chování aplikace, bezpečnostní události (zejména neoprávněného přístupu) nebo výskytu neznámých a nesrozumitelných jevů, nepodléhejte panice, ponechte vše, jak je, počítač nevypínejte a nahlaste tuto skutečnost příslušným odborníkům.
13. Neotevírejte neznámé soubory. Pokud se ve složce, kam se stahují soubory z webu, objeví neznámý soubor, neotevírejte ho. Může jít o infikovaný soubor, který byl bez vašeho vědomí stažen z nedůvěryhodné stránky. Oznamte tuto skutečnost vašemu přímému představenému a prostřednictvím služby ServiceDesk.
14. Nepožadujte po příslušných odbornících, aby vám zajistili výjimky z uvedených opatření. Jedna „vynucená“ výjimka může být právě tou útočníkem zneužitou „dírou“ do systému.
15. **Shrnutí**

Výčet výše uvedených opatření neznamená, že byste je měli aplikovat všechna. Navíc, jak už jsem uvedl, dají se zajistit jako nakupovaná služba. To, která opatření jak a kdy zavést vyplyne z analýzy rizik, tedy odpovědí na otázku „Co se stane když …?“ Jen je důležité se nad touto problematikou zamyslet a neignorovat ji. A neustále se ptát:

* **Chceme vůbec kybernetickou a informační bezpečnost řešit? (no musíme)**
* **Víme, kde co máme? (katalog informačních aktiv – služeb, serverů, systémů, aplikací atd.)**
* **Víme, co s čím komunikuje? (identifikované datové toky)**
* **Víme, jak jsme na tom se zabezpečením? (sebehodnocení – jaká opatření máme zavedena, jak jsou účinná)**
* **Známe rizika? (víme co hrozí, když se něco stane – co nebude fungovat, jaké služby nebudeme schopni poskytovat, jaké sankce za to hrozí, co na to řeknou občané atd.)**
* **Víme, kdo co spravuje? (Máme přehled o správcích našich technologií a systémů, a to i externích, kdo má od čeho klíče a to i ty fyzické)**
* **Máme kontaktní matici? (Víme, komu zavolat, když se něco stane)**
* **Víme jak z průšvihu? (Máme plán, jak průšvih zvládnout)**
* **Víme kde máme a jak máme použít zálohy ?**
* **Víme v jakém pořadí máme spouště po výpadku informační systémy (aplikace)?**
* **Víme, kdy a s jakým výsledkem jsme si obraz o stavu kontrolovali – testovali ?**
* **Víme, jak jsme na zjištění reagovali? (Přijali jsme nápravná opatření)**
* **Máme všechno dokumentováno? (A vytištěno – když nefungují počítače, tak je nám dokumentace v elektronické podobě k ničemu a spoléhat se na to, že to mají ajťáci v hlavách je cesta do pekla)**
* **Jsou naši uživatelé dostatečně obezřetní? (Prokazatelně a pravidelně proškolení)**
* **Co děláme pro to, aby byli? (máme na to plán)**
* **Máme pod kontrolou dodavatele? (řekli jsme jim, že po nich chceme bezpečné chování)**

1. **Zdroje**

* Zákon 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti
* Vyhláška 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
* Minimální bezpečnostní standard - podpůrný materiál pro subjekty, které nespadají pod zákon o kybernetické bezpečnosti
* Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti

1. <https://www.zakonyprolidi.cz/cs/2014-181> [↑](#footnote-ref-1)
2. <https://www.zakonyprolidi.cz/cs/2018-82> [↑](#footnote-ref-2)
3. [www.nukib.cz](http://www.nukib.cz) [↑](#footnote-ref-3)
4. <https://www.govcert.cz/cs/regulace-a-kontrola/podpurne-materialy/> [↑](#footnote-ref-4)
5. <https://osveta.nukib.cz/course/view.php?id=67> [↑](#footnote-ref-5)
6. <https://osveta.nukib.cz/course/view.php?id=92> [↑](#footnote-ref-6)
7. <https://www.zakonyprolidi.cz/cs/2018-82#cast2-hlava1> [↑](#footnote-ref-7)
8. <https://www.zakonyprolidi.cz/cs/2018-82#p3> [↑](#footnote-ref-8)
9. <https://www.zakonyprolidi.cz/cs/2018-82#p4> [↑](#footnote-ref-9)
10. <https://nukib.cz/cs/infoservis/aktuality/1868-nukib-zverejnil-pruvodce-rizenim-aktiv-a-rizik-dle-vyhlasky-o-kyberneticke-bezpecnosti/> [↑](#footnote-ref-10)
11. <https://www.zakonyprolidi.cz/cs/2018-82#p5> [↑](#footnote-ref-11)
12. <https://www.zakonyprolidi.cz/cs/2018-82#p6> [↑](#footnote-ref-12)
13. https://www.zakonyprolidi.cz/cs/2018-82#p7 [↑](#footnote-ref-13)
14. https://www.zakonyprolidi.cz/cs/2018-82#p8 [↑](#footnote-ref-14)
15. <https://www.zakonyprolidi.cz/cs/2018-82#p9> [↑](#footnote-ref-15)
16. https://www.zakonyprolidi.cz/cs/2018-82#p10 [↑](#footnote-ref-16)
17. https://www.zakonyprolidi.cz/cs/2018-82#p11 [↑](#footnote-ref-17)
18. <https://www.zakonyprolidi.cz/cs/2018-82#p12> [↑](#footnote-ref-18)
19. <https://www.zakonyprolidi.cz/cs/2018-82#p13> [↑](#footnote-ref-19)
20. <https://www.zakonyprolidi.cz/cs/2018-82#p14> [↑](#footnote-ref-20)
21. <https://www.zakonyprolidi.cz/cs/2018-82#p15> [↑](#footnote-ref-21)
22. <https://www.zakonyprolidi.cz/cs/2018-82#p16> [↑](#footnote-ref-22)
23. https://www.zakonyprolidi.cz/cs/2018-82#p17 [↑](#footnote-ref-23)
24. <https://www.zakonyprolidi.cz/cs/2018-82#p18> [↑](#footnote-ref-24)
25. <https://www.zakonyprolidi.cz/cs/2018-82#p19> [↑](#footnote-ref-25)
26. https://www.zakonyprolidi.cz/cs/2018-82#p20 [↑](#footnote-ref-26)
27. https://www.zakonyprolidi.cz/cs/2018-82#p21 [↑](#footnote-ref-27)
28. https://www.zakonyprolidi.cz/cs/2018-82#p22 [↑](#footnote-ref-28)
29. <https://www.zakonyprolidi.cz/cs/2018-82#p23> [↑](#footnote-ref-29)
30. https://www.zakonyprolidi.cz/cs/2018-82#p24 [↑](#footnote-ref-30)
31. https://www.zakonyprolidi.cz/cs/2018-82#p25 [↑](#footnote-ref-31)
32. <https://www.zakonyprolidi.cz/cs/2018-82#p26> [↑](#footnote-ref-32)
33. https://www.zakonyprolidi.cz/cs/2018-82#p27 [↑](#footnote-ref-33)