VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

KYBERNETICKÁ BEZPEČNOST VE VEŘEJNÉ SPRÁVĚ

Autor práce: Daniel Strnad

Studijní program: Bezpečnostně právní činnost

Forma studia: kombinovaná

Vedoucí práce: RNDr. Růžena Ferebauerová

Katedra: Katedra právních oborů a bezpečnostních studií

2023

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 6, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Daniel Strnad

Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Kybernetická bezpečnost ve veřejné správě

Název bakalářské práce v anglickém jazyce: Cyber Security in Public Administration

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, titul):
RNDr. Růžena Ferebauerová

Datum zadání bakalářské práce (měsíc, rok): duben 2022

Cíl bakalářské práce:
Cílem bakalářské práce je analýza vybraných aspektů kybernetické bezpečnosti ve veřejné správě se zaměřením na kategorii významných informačních systémů a rozbor bezpečnostních opatření vedoucích k zabránění kybernetických útoků.

Student: Daniel Strnad	26.4.2022 *datum*	Strnad *podpis*
Vedoucí práce: RNDr. Růžena Ferebauerová	10.5.2022 *datum*	 *podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	31.5.2022 *datum*	 *podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	1.6.2022 *datum*	 *podpis*
Rektor: doc. Ing. Jiří Dušek, Ph.D.	10.6.2022 *datum*	 *podpis*

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z.ú. ČESKÉ BUDĚJOVICE

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucí a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucí bakalářské práce RNDr. Růženě Ferebauerové za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

STRNAD, D. *Kybernetická bezpečnost ve veřejné správě: bakalářská práce.* České Budějovice: Vysoká škola evropských a regionálních studií, 2023. 78 s. Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová

Klíčová slova: kybernetická bezpečnost, kybernetický bezpečnostní incident, zákon o kybernetické bezpečnosti, veřejná správa, hacker

Tato bakalářská práce se zabývá problematikou informačních systémů veřejné správy, informační a kybernetickou bezpečností, kybernetickými hrozbami a ochranou před nimi. Představuje právní předpisy, které tvoří právní rámec e-Governmentu a orgány působící v oblasti prevence a obrany proti kybernetickým útokům. Cílené útoky proti IT se staly celosvětovým fenoménem. Způsobují rozsáhlé škody v soukromém i veřejném sektoru. Právě orgány veřejné správy patří k významným subjektům kybernetické bezpečnosti. Práce obsahuje poznatky shromážděné ze vzdělávacích materiálů publikovaných státními orgány a autory zabývajícími se problematikou kybernetické bezpečnosti.

Klíčová slova: kybernetická bezpečnost, kybernetický bezpečnostní incident, zákon o kybernetické bezpečnosti, veřejná správa, hacker

ABSTRACT

STRNAD, D. *Cyber Security in Public Administration: bachelor´s thesis.* České Budějovice: University of European and Regional Studies, 2023. 78 pp. Supervisor: RNDr. Růžena Ferebauerová

Klíčová slova: cyber security, cyber security incident, cyber security law, public administration. a hacker

This bachelor's thesis deals with the issues of information systems in public administration, information and cyber security, cyber threats and protection against them. It presents the legal regulations that make up the legal framework of e-Government and the authorities operating in the field of prevention and defense against cyber attacks. Targeted attacks against IT have become a worldwide phenomenon. They cause widespread damage in both sectors - the private and the public sectors. It is the public administration authorities that belong to the significant subjects of cyber security. The work contains knowledge collected from educational materials published by state authorities and authors dealing with the issue of cyber security.

Klíčová slova: cyber security, cyber security incident, cyber security law, public administration, a hacker

Obsah

Úvod

Vývoj ve společnosti směřuje k postupné digitalizaci všech dat, a využití informačních technologií se tak stává součástí života každého člověka. Kromě zjevných benefitů, které s sebou neustálý vývoj moderních informačních a komunikačních technologií přináší, narůstá i riziko zneužití těchto technologií a útoků na informace, s kterými tyto technologie pracují. Informační a komunikačních technologie jsou využívány téměř ve všech odvětvích nejen soukromého, ale i veřejného sektoru a narušení jejich důvěrnosti, dostupnosti nebo integrity může ve svém důsledku zapříčinit rozsáhlé a závažné následky. Z těchto důvodů roste také důležitost kybernetické bezpečnosti, jejímž cílem je ochránit informační a komunikační technologie před zásahy vedoucími k ohrožení nebo omezení jejich chodu.

Jednou z klíčových oblastí z hlediska zajištění kybernetické bezpečnosti státu je sféra výkonu veřejné moci, jejíž aktivity se stále větší měrou přesouvají do kybernetického prostoru. Veřejná správa ze své podstaty pracuje s informacemi, které jsou postupně digitalizovány. Není proto pochyb o tom, že nedílnou součástí efektivní a moderní veřejné správy by měla být informační bezpečnost, jejíž systémový přístup by měl být reflektován na všech úrovních správního orgánu. Orgány veřejné správy se stávají správci nebo provozovateli různých komunikačních systémů, a tudíž musí plnit povinnosti, které vyplývají z právní úpravy kybernetické bezpečnosti. Veřejná správa by se měla přizpůsobovat společenskému vývoji, měnícím se podmínkám a potřebám společnosti a její činnost by se měla stát ve veřejném zájmu efektivní.

K dosažení tohoto cíle je nutné objasnit základní pojmy, které souvisí s problematikou kybernetické bezpečnosti, vztahy mezi informační a kybernetickou bezpečností a definovat její základní hrozby.

Následující kapitola bude věnována orgánům veřejné správy jakožto subjektům kyberbezpečnosti. V závěrečné kapitole přiblížím problematiku kybernetické bezpečnosti z hlediska právních nástrojů a bezpečnostních opatření.

1 Cíl a metodika bakalářské práce

Cílem mé bakalářské práce je analýza vybraných aspektů kybernetické bezpečnosti ve veřejné správě se zaměřením na kategorii významných informačních systémů a rozbor bezpečnostních opatření vedoucích k zabránění kybernetických útoků.

Pro dosažení cíle BP byla využita literární rešerše a její následná komparace a syntéza. Pro určení relevantní literatury byl využit způsob vyhledávání na klíčových slovech. Pomocí klíčových slov „kybernetická bezpečnost, kybernetický bezpečnostní incident, zákon o kybernetické bezpečnosti, veřejná správa, hacker“ byly vybrány publikované zdroje ne starší než 10 let.

Úvodní část BP se zabývá základní terminologií kybernetické bezpečnosti, přiblížil jsem otázku bezpečnostních hrozeb a kybernetické kriminality. Velmi významného postavení v tomto směru nabyla oblast práva, která ukládá povinnosti provozovatelům významných informačních systémů a rizikových infrastruktur, a proto jsem další část mé práce věnoval zákonům a vyhláškám týkajícím se kybernetické bezpečnosti a významných informačních systémů veřejné správy. Připomněl jsem úlohu Národního úřadu pro kybernetickou a informační bezpečnost a dalších orgánů činných v oblasti prevence a obrany proti kybernetickým útokům a okrajově se zmínil o institucích mezinárodních. Další část mé BP byla věnována popisu veřejné správy a e-Governmentu. Podrobněji jsem popsal základní informační systémy veřejné správy – Czech POINT, datové schránky a základní registry. V poslední části BP jsem se zabýval zabezpečením ISVS a předpoklady pro posílení jejich bezpečnosti. Rovněž jsem poukázal na nedostatky, které bývají častou příčinou kybernetických útoků. Závěrem musím konstatovat, že zajištění kybernetické bezpečnosti je nepochybně jednou z klíčových výzev současnosti.

2 Základní aspekty kybernetické bezpečnosti

Ve veřejnosprávní sféře stejně jako v mnoha dalších odvětvích roste množství vytvářených a ukládaných informací. Vývoj ve společnosti směřuje k postupné digitalizaci všech dat, a využití informačních technologií se tak stává součástí života každého člověka. Kybernetická bezpečnost se v současné době dostává do popředí zájmu různých subjektů, počínaje obchodními společnostmi působícími v oblasti informačních a komunikačních technologií až po orgány státní správy. V dnešní době s klíčovými informacemi disponují i orgány veřejné správy a jejich zneužití může mít nedozírné následky. Téměř veškerou činnost státní správy doprovází aktivity v kyberprostoru, proto se problémem v celostátním měřítku stává i nárůst kybernetických útoků.

2.1 Základní terminologie kybernetické bezpečnosti

Ačkoliv je pojem kybernetická bezpečnost aktuálně velmi používaný, neexistuje zcela přesná formulace, která by tento pojem 21. století definovala. Nejčastěji je termín uváděn jako bezpečnost informačních a komunikačních technologií, který je oborem informatiky, směřujícím k zajištění ochrany kybernetického prostoru. Zabývá se ochranou počítačových systémů a sítí před počítačovou kriminalitou (krádež nebo poškození elektronických údajů, hardwaru, softwaru, zneužitím nebo narušením poskytovaných služeb, kybernetickým útokem) a před neoprávněným přístupem k infor macím. Jeho hlavním cílem je ochránit soukromí údajů zavedených v systému a spolehlivost kyberprostoru[1].

Mezi nejpoužívanější základní pojmy kybernetické bezpečnosti patří:

Adware (Advertising Supported Software) – software, který cílí na uživatele nevyžádanou reklamou vyskakující na obrazovce během on-line práce s internetem.

Aktivní hrozba (Active Threat) – událost v kyberprostoru, která může být příčinou ztráty dostupnosti dat nebo narušení jejich důvěrnosti. Důsledkem toho může být vložení falešné zprávy, odmítnutí služby nebo krádež identity.

Analýza hrozeb (Threat Analysis) – zabývá se průzkumem událostí a činností, které by mohly negativně ovlivnit data nebo kvalitu služeb IT.

[1] Počítačová bezpečnost – Wikipedie. [online]. [cit. 2023-25-01]. Dostupné z: https://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_bezpe%C4%8Dnost

Analýza počítačového viru (Virus Analysis) – rozebírá chování viru v počítači nebo počítačové síti z hlediska jeho šíření, způsobených škod a chování. Tento vir zkoumá a posléze odstraní.

Antivirový program (Antivirus Program) – program, který vyhledá viry, léčí napadané soubory, provádí zálohu a obnovu systémových částí na disku a rovněž ukládá kontrolní data o souborech na disku.

Bezpečnost informací (Information Security) – zachování důvěrnosti, dostupnosti informací, jejich integrity při uplatnění základních bezpečnostních opatření vedoucích k ochraně informací před jejich ztrátou nebo kompromitací.

Bezpečnostní manažer (Security manager) – zaměstnanec, který je za bezpečnost systému odpovědný. Jeho pravomoce a odpovědnost jsou přesně definovány.

Bot – parazitní program nainstalovaný na počítači bez vědomí jeho uživatele. Hacker tento počítač může ovládat vzdáleným přístupem a zneužívat ho pro plnění různých příkazů.

Brána (Gateway) – označení vstupu do informačního systému vybaveného zvláštními bezpečnostními prvky (šifrováním vstupů a výstupů, firewallem, autentizací přístupu).

Certifikace (Certification) – třetí strana provádí ověřování způsobilosti informačního systému k nakládání s utajovanými informacemi, její schválení a vystavení certifikátu.

Cyberstalking – využití elektronického média, např. elektronické pošty k obtěžování s cílem vyvolat v oběti pocit strachu. Pachatel získává informace o oběti z chatu, diskuzních fór nebo webových stránek.

Červ (Worm) – druh programu, který vytváří své kopie a následně je přeposílá do dalších počítačových systémů nebo sítí, v nichž dále pracuje podle svého naprogramování. Používá se k vyhledávání bezpečnostních skulin např. v poštovních programech.

DDoS Distribuované odmítnutí služby – útok na internetové stránky nebo služby, při kterém dochází k přehlcení požadavků a nedostupnosti služby pro ostatní uživatele. Útok je v jednom časovém intervalu veden z několika počítačů najednou.

Hacking – zvnějšku provedený neoprávněný vstup do informačního systému. Pachatel se k objektu útoku (počítači) nepřipojuje přímo, ale přes internetový server, který se může nacházet v různých částech světa. Identifikace počítače, ze kterého byl útok veden je tím ztížena.

Kybernetický prostor (Cyber Space) – digitální prostředí, které tvoří informační a komunikační technologie, v nichž informace vznikají, jsou zde zpracovávány a dochází k jejich výměně. Lze si ho představit jako virtuální prostředí, které je vytvořené propojením počítačových systémů v síti. Probíhá zde komunikace mezi subjekty bez nutnosti fyzické aktivity.

Kybernetický terorismus (Cyber Terrorist) – nezákonný útok proti PC nebo počítačovým sítím a informacím, které obsahují, s cílem útočníka tyto informace získat, ovlivnit je nebo získat kontrolu nad prvky infrastruktury systému.

Management rizik (Risk management) – činnost, která slouží k analýze rizik, ať stávajících či budoucích a přijímání opatření k eliminování jejich výskytu a závažnosti jejich možných nežádoucích následků.

Malware – software, který negativně působí v systému při jeho spuštění. Projevuje se jako reakce na spouštěcí událost, např. otevření zprávy v elektronické poště.

Narušení (Breach) – v důsledku překonání bezpečnostních opatření dojde k narušení nebo prolomení důvěrnosti, dostupnosti nebo integrity informačního systému

Nevyžádaná pošta (Spam) – hromadné šíření nevyžádaného sdělení např. formou reklamy.

Ohrožení (Exposure) – možnost existence zranitelnosti, která může vést až ke zneužití hrozbou.

Phishing – způsob vedoucí ke zcizení digitální identity uživatele. Nejčastěji se jedná o podvodnou zprávu šířenou elektronickou poštou, která se snaží z uživatele vylákat přihlašovací jméno, hesla, čísla účtů a bankovních karet.

Spyware – program, jež skrytě sleduje chování uživatele PC a pomocí internetu odesílá data bez vědomí uživatele z jeho počítače jinému uživateli, který tyto informace dále zpracovává. Z hlediska bezpečnosti dat představuje spyware velkou hrozbu.

Trojský kůň (Trojan Horse) – program, který je implantován do IS uživatele bez jeho vědomí a který sleduje činnosti, o které má útočník zájem. Na jejich základě pak útočník získá přístupové údaje k bankovním účtům, kontaktům elektronické pošty či navštíveným webovým stránkám.

Útok (attack) – pokus o vystavení hrozbě, vyřazení z činnosti, zcizení nebo získání neautorizovaného přístupu do PC nebo počítačových sítí.

Vir (Virus) – škodlivý kód, který po připojení k určitému programu nebo systémové oblasti dokáže zahájit destrukční proces (stahování dalšího malware, poškození, změnu nebo zničení dat, narušení funkce operačního systému).

Zranitelnost (Vulnerability) – slabina v bezpečnosti (logické, fyzické, administrativní), která může být zneužita hrozbou[2].

2.2 Kybernetická, počítačová a informační bezpečnost

2.2.1 Kybernetická bezpečnost

Definice kybernetické bezpečnosti je často zaměňována s pojmem počítačová či informační bezpečnost. Toto pojetí je však mylné, neboť se jedná o rozdílné pojmy z hlediska odlišného předmětu ochrany[3].

Účelem kybernetické bezpečnosti je ochrana tzv. kyberprostoru, případně je možno hovořit o ochraně služeb informační společnosti. Tato ochrana zahrnuje tři základní složky, kterými jsou ochrana důvěrnosti, ochrana dostupnosti a ochrana integrity. Kybernetická bezpečnost není pouze oblastí, kterou se zabývají oddělení informačních a komunikačních technologií, ale týká se každého, kdo ve svém každodenním životě využívá jakékoli prvky informačních technologií. Nelze ji proto

[2] HRŮZA, P. *Kybernetická bezpečnost*. Brno: Univerzita obrany, 2012, s. 9-14.
[3] Důvodová zpráva. *Návrh zákona o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)* [online]. Úřad vlády České republiky, 2014, s. 72. [cit. 2023-12-01]. Dostupné z: https://apps.odok.cz/attachmen/-/down/KORN9F6H6BCH

bagatelizovat, neboť se stává klíčovou oblastí jak pro organizace, tak i pro každého jedince[4].

2.2.2 Počítačová bezpečnost

Počítačová bezpečnost zahrnuje na rozdíl od pojmu kybernetická bezpečnost užší pojem. Zahrnuje v zásadě technickou oblast. Lze ji definovat jako obor informatiky, zabývající se zabezpečením informací v počítačích. Jedná se především o zabezpečení ochrany před neoprávněnou manipulací s daty, neoprávněnou manipulací se zařízeními PC systému, chrání informace před jejich krádeží (např. nelegální kopírování dat) nebo poškozením, ochraňuje data z hlediska jejich přenosu, bezpečného uložení, dostupnosti, integrity a záměny[5].

Data s různými informacemi nejsou uložena pouze na počítačích a jejich systémech, ale mohou být zaznamenána i na jiných, tzv. analogových nosičích, proto je počítačová bezpečnost ochranou v nejužším smyslu.

2.2.3 Informační bezpečnost

Informační bezpečnost je v současné době běžně využívaným spojením. Představuje oblast, která zabezpečuje všechny informace, ať již se jedná o jejich fyzickou či virtuální podobu, po celou dobu jejich existence. Chrání informace před jejich únikem a zneužitím, což může vést k vážným následkům. Informace jsou v dnešní době uchovávány především v elektronické formě, proto je nutné chránit data na počítačích, serverech, ale rovněž na místech veřejně dostupných datových struktur, např. na online úložištích či veřejných fotogaleriích. Ochranou pracovních dat by se měli zabývat specializovaní odborníci, chránit svá osobní uživatelská data však musí každý z nás[6].

2.3 Bezpečnostní hrozby

2.3.1 Rozdělení hrozeb

S rozvojem informačních technologií vzrůstá i riziko nově narůstajících hrozeb, proto je nutné opakovaně, nejlépe v ročních intervalech, provádět analýzu rizik. U hrozeb se odhadne pravděpodobnost jejího naplnění a určí rozsah školy, včetně dopadů,

[4] POLČÁK, R. *Právní problémy kybernetické bezpečnosti*, 2016, s. 41.
[5] JIRÁSEK, P., NOVÁK, L., POŽÁR, J., *Výkladový slovník kybernetické bezpečnosti*, 2015, s. 72.
[6] INFORMAČNÍ BEZPEČNOST. *ŠKOLENÍ PROJEKTOVÉHO ŘÍZENÍ PRO FIRMY, VEŘEJNOU SPRÁVU A AKTIVNÍ STUDENTY* [online]. Copyright © [cit. 2023-25-01]. Dostupné z: https://www.acsa.cz/verejnost/sluzby/podle-temat/informacni-bezpecnost/

v případě jejího naplnění. Na základě odhadnutých rizik se navrhnou opatření k jejich odstranění, případně minimalizaci těch nepřijatelných. Některá rizika lze vyhodnotit jako přijatelná s tím, že se vytvoří postup v případě jejich naplnění. Takovým případem může být např. neoprávněné otevření dveří do datového centra (manipulace se zámkem, neoprávněné použití klíčů, útok hrubou silou). Měl by být stanoven postup, jak tuto událost řešit, kam a jak tento incident nahlásit, koho kontaktovat.

Hrozby můžeme rozdělit podle několika hledisek:

Podle úmyslu:

- náhodné hrozby (přerušení dodávky proudu, přírodní katastrofa),

- neúmyslné hrozby (neúmyslně vymazaný soubor),

- úmyslné hrozby (zcizení, útok v síti, úmyslné poškození).

Podle zdroje působení:

- hrozby vnější (zdroj hrozby je mimo aktivum),

- hrozby vnitřní (vycházejí ze samotného aktiva – výrobní vada).

Podle původu:

- hrozby způsobené člověkem (chyba uživatele, nezákonný odposlech),

- přírodní hrozby (zemětřesení, záplavy, blesk).

Podle motivace útočníka:

- hrozby za účelem msty,

- hrozby z důvodu neplnění povinností,

- hrozby za účelem získání konkurenční převahy,

- hrozby za účelem obohacení,

- hrozby za účelem prokázání svých schopností.

Podle působení na zdroje aktiva:

- hrozby pro informace,

- hrozby pro aplikace,

- hrozby pro hardware,

- hrozby pro uživatele,

- hrozby pro síť,

- hrozby pro operační systém.

Podle směrování na bezpečnostní atributy:

- hrozby integrity (chyba v transakci databáze),

- hrozby důvěrnosti (krádež tabletu),

- hrozby dostupnosti (požár, DDOS útok – odmítnutí služby)[7].

2.4 Kybernetická kriminalita, kybernetická válka, kyberterorismus

Kybernetická bezpečnost je neodmyslitelně spjata s oblastí kybernetické kriminality, kybernetických konfliktů a kyberterorismu.

2.4.1 Kybernetická kriminalita

Kybernetickou kriminalitu, někdy též zkráceně nazývánu jako kyberkriminalitu, definuje Policie ČR jako trestnou činnost, která je páchána v prostředí informačních a komunikačních technologií vč. počítačových sítí. Informační a komunikační technologie jsou buď přímo předmětem útoku nebo slouží jako prostředek k jejímu páchání[8].

Přestože se lze setkat s názory, které mezi kybernetickou a počítačovou kriminalitou nečiní rozdíl[9], převládá názor, že se jedná o pojmy zcela odlišné. Kybernetickou kriminalitu tak lze obecně definovat jako *„jednání namířené proti*

[7] Hrozby – KYBEZ. *KYBEZ – Platforma kybernetické bezpečnosti* [online]. Copyright © [cit. 2023-25-01]. Dostupné z: https://www.kybez.cz/hrozby/

[8] Rozcestník kyberkriminality – Prevence kriminality. *Prevence kriminality – Prevence kriminality v České republice* [online]. Copyright © 2023 Prevence kriminality v České republice. Všechna práva vyhrazena. Portál [cit. 2023-25-01]. Dostupné z: https://prevencekriminality.cz/prevence-kriminality/kyberkriminalita/rozcestnik-kyberkriminality/

[9] JIRÁSEK, P., NOVÁK, L., POŽÁR, J. Výkladový slovník kybernetické bezpečnosti, 2015, s. 73.

počítači, případně počítačové síti, nebo jako jednání, při němž je počítač použit jako nástroj pro spáchání trestného činu"[10]. Podle Polčáka se kyberkriminalitou rozumí protiprávní činnost, kdy je počítač nebo počítačová síť nástrojem, cílem nebo obojím"[11]. Zmínit lze i definici, která kybernetickou kriminalitu chápe jako činnost, kterou je porušován zákon, a která může být přímo proti počítačům namířena (proti datům, hardwaru nebo softwaru), nebo ve které počítač nebo počítačová síť jsou nástrojem nebo prostředím, ve které se tato činnost odehrává[12].

Z hlediska trestního práva se veškerá specifika kybernetické nebo jiné ICT kriminality dotýkají jenom hmotněprávní stránky. Stránka procesněprávní se v této oblasti neliší od postupů, které souvisejí s trestnými činy spáchanými v „off-line" prostředí[13].

Pro vymezení vztahu kybernetické kriminality a kybernetické bezpečnosti je vhodné zmínit členění kybernetické kriminality. Kyberkriminalitu lze podle kriminálních činů rozčlenit do tří základních skupin[14]:

1) Činy, u kterých jsou počítače či počítačové sítě cílem kriminálních aktivit (tzv. „cyber-dependent crimes")[15].

2) Činy, u kterých jsou počítače či počítačové sítě použity jako nástroje k páchání trestné činnosti (tzv. „cyber-enabled crimes")[16].

3) Činy, které sice byly spáchány v „off-line" světě, ale u kterých mohou počítače například obsahovat důkazy týkající se dané trestné činnosti (tzv. „computer-supported crimes")[17].

[10] KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC, s. 34.
[11] POLČÁK, R. *Právo informačních technologií.* Praha: Wolters Kluwer, 2018, s. 541.
[12] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, s. 19.
[13] DONÁT, J. a TOMÍŠEK, J. *Právo v síti: průvodce právem na internetu*. Praha: C.H. Beck, 2016, s. 248.
[14] CLOUGH, J. *Principles of Cybercrime.* New York: Cambridge University Press, 2010, s. 10.
[15] MCGIURE, M., DOWLING, S. *Cyber crime: A review of the evidence, Research Report 75, Chapter 1: Cyber-dependent crimes*. UK Home Office, 2013, s. 35.
[16] MCGIURE, M., DOWLING, S. *Cyber crime: A review of the evidence, Research Report 75, Chapter 2: Cyber-enabled crimes - fraud and theft*. UK Home Office, 2013, s. 27.
[17] POLČÁK, R. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018. Právní monografie (Wolters Kluwer ČR), s. 542.

2.4.2 Kybernetická válka

Pojem kybernetická válka zahrnuje veškeré aktivity zaměřené na poškození všech počítačových systémů. Akce prováděné kybernetickými zločineckými organizacemi nebo speciálními vojenskými aparáty jsou financovány vládními subjekty a jsou zaměřené na politicko-vojenské cíle prostřednictvím internetových páteřních sítí. Je nutno rozlišit kybernetickou válku od kybernetické špionáže, teroristického využívání sítí či kybernetické kriminality, neboť se liší především z hlediska vytyčených cílů a podílejících se subjektů[18].

2.4.3 Kyberterorismus

Kyberterorismus je úmyslný útok, který je vedený proti počítačům, jejich systémům, programům i uživatelům v oblasti kyberprostoru. Jedná se o politicky motivovaný útok, jehož účelem je napadení v kyberprostoru s cílem krádeže citlivých informací, zničení nebo pozměnění dat či vyřazení počítačových systémů za účelem nedostupnosti. Typickým příkladem kyberterorismu je napadení vojenské či státní infrastruktury nebo napadení bankovních sektorů. Kyberterorismus může zapříčinit i ztrátu na lidském životu ve chvíli, kdy spáchaná kyberkriminalita si v kybernetickém prostoru začíná vybírat svoji daň i mimo virtuální prostředí[19]. Kyberteroristické útoky můžeme dělit podle cíle a typu útoku na tyto možné varianty[20]:

Informace a komunikace – krádež identity, manipulace s volbami, získání vojenských informací, manipulace s průzkumem veřejného mínění.

Bankovnictví a finance – teroristé by po úspěšném útoku hackerů mohli ovlivnit ceny akcií a tím ovlivnit vývoj ekonomiky nebo zničit banku.

Doprava – útoky na systémy řízení dopravy, řízení letového provozu, dopravu a dopravní prostředky.

Vládní sektor – útoky na politiku, státní správu, vládní sektor.

---

[18] Co je to kybernetická válka – *Soubory*. [online]. [cit. 2023-27-01]. Dostupné z: https://soubory.info/info/co-je-to-kyberneticka-valka/

[19] Co je kyberterorismus? - Správa.sítě.eu. *Správa sítě - slovník pojmů: správa sítě, zabezpečení sítě, outsourcing IT* [online]. Copyright © [cit. 2023-27-01]. Dostupné z: https://www.sprava-site.eu/kyberterorismus/

[20] BRYAN, C. *Cyberterrorism, computer crime, and reality*. *Information Management & Computer Security* [online]. 2004, vol. 12, issue 2, s. 154-166. [cit. 2023-27-01]. Dostupné z: http://www.emeraldinsight.com/doi/abs/10.1108/09685220410530799

Všeobecná infrastruktura – sabotáž systémů souvisejících s plynem a palivem (např. systém pro distribuci pitné vody), sabotáž systémů vedení elektrické energie.

Záchranná služba – útoky na složky integrovaného záchranného systému.

Viry – útok vedený na počítačový systém v elektrárně může vyvolat ničivý výbuch.

Tabulka znázorňující typy počítačových trestných činů, motivace těch, kteří je páchají, cíle těchto zločinů a používané metody[21]:

Tab. 1 - Typy počítačových trestných činů

	Motivace	Cíl	Metoda
Kyberteror	Politická nebo sociální změna	Nevinní lidé	Násilí a destrukce založené na počítačích
Hacktivismus	Politická nebo sociální změna	Nevinní lidé, lidé rozhodující o určitých věcech	Protest pomocí změny designu webové stránky nebo DoS útoky
Black Hat hackování	Ego, osobní nenávist	Lidé, firmy, vlády	Malware, počítačové viry atd.
Kyberkriminalita	Ekonomický zisk	Lidé, firmy	Malware pro podvody a krádeže identity, DoS pro vydírání
Kybernetická špionáž	Ekonomický nebo politický zisk	Lidé, firmy, vlády	Všechny techniky
Informační válka	Politický nebo vojenský zisk	Infrastruktury, IT systémy a data (soukromá i veřejná)	Všechny techniky

Vzhledem k tomu, že závislost člověka na informačních technologiích, především na internetu je mnohem častější než tomu bylo v minulosti, dochází i k vyšší pravděpodobnosti rizika kybernetických útoků. Při plánování kyberteroristického útoku musí hacker nebo skupina vykonat několik navazujících kroků, aby počítačový útok úspěšně vykonala**,** ať se jedná o špionáž, běžný kybernetický zločin nebo masový kybernetický teror[22].

[21] LACHOW, I. *Cyber terrorism: Menace or myth. Cyberpower and national security*. 2009, [cit. 2023-27-01], s. 434-467.
[22] WILSON, C. *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress.* Washington: Congressional Research Service. 2003, [cit. 2023-27-01]. Dostupné z: http://www.fas.org/irp/crs/RL32114.pdf

Jedná se o následující úkony:

1. Analýza situace, její průzkum – první fáze je zaměřena na získání co nejvíce informací o předmětu útoku. Za tímto účelem se využívá především „sociálního inženýrství“ (manipulace lidí za účelem provedení určité akce). Běžně se využívá rovněž spywaru.

2. Skenování – útočník za pomoci získaných informací hledá nejlepší způsob, kterým by vnikl do systému. Zjišťuje způsob internetového připojení a druh využívaného počítačového softwaru.

3. Získání přístupu – útočník má počítačový program, který využije nedokonalosti v systému útoku a je schopen zaútočit na svůj cíl.

4. Udržení přístupu – útočník již získal přístup a vytváří způsob, kterým by se mohl vrátit, Využívá „backdoors“ neboli zadní vrátka (umožňuje obejít běžnou autenzitaci) nebo „rootkit“ (PC programy, které maskují přítomnost zákeřného softwaru v PC – trojských koní, spywaru, virů skrýváním adresářů, ve kterých jsou instalování).

5. Zahlazení stop - snaha útočníka o nastavení systému tak, aby se nedalo zjistit, že k nějakému útoku došlo. Mnohdy se provedený útok podaří utajit velmi dlouho[23].

[23] Kyberterorismus - Wikiwand. *Wikiwand – home* [online]. [cit. 2023-27-01]. Dostupné z: https://www.wikiwand.com/cs/Kyberterorismus

3 Právní základy kybernetické bezpečnosti

Mezi nástroje kybernetické bezpečnosti patří celá škála různých právních, procesních, organizačních, analytických a dalších nástrojů, které zahrnují tvorbu bezpečnostních politik na různých úrovních státu nebo konkrétních systémů či subjektů[24]. Právní úprava kyberbezpečnosti je poměrně specifickou oblastí právní regulace z hlediska předmětu, použitých přístupů i metodologie. Ačkoli kybernetická bezpečnost je úzce spjata s kybernetickou kriminalitou, z hlediska předmětu je jejich právní regulace odlišná. Hlavní rozdíl lze spatřovat v tom, že právní úprava kybernetické kriminality má trestněprávní charakter, zatímco úprava kybernetické bezpečnosti spadá do oblasti správněprávní. Obě tyto oblasti se od sebe odlišují svým předmětem, neboť cílem právní regulace kybernetické kriminality (nutno ji vnímat pouze jako specifickou část kriminality obecné) je trestněprávní postih pachatelů, účelem právní úpravy kybernetické bezpečnosti je ochrana kybernetického prostoru před kybernetickými hrozbami, resp. před důsledky kybernetických incidentů[25].

3.1 Kybernetická bezpečnost v českém právu

Koncepce kybernetické bezpečnosti v České republice byla poprvé souhrnněji definována ve Strategii pro oblast kybernetické bezpečnosti České republiky na období 2012 – 2015[26], resp. v Akčním plánu k této strategii, které Vláda České republiky schválila svým usnesením č. 364[27]. Tato Strategie se stala základem pro přijetí zákona č. 181/2014 Sb., o kybernetické bezpečnosti, který se stal hlavním pilířem právní úpravy české kybernetické bezpečnosti.

3.1.1 Zákon o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) vstoupil v platnost dnem 29.08.2014 s účinností od 01.01.2015. Předmětem tohoto zákona je úprava práv a povinností osob, jakož i stanovení pravomoci a působnosti orgánů veřejné moci v oblasti kybernetické bezpečnosti. Zapracovává příslušné předpisy Evropské unie a upravuje

[24] DONÁT, J. *Právo v síti: průvodce právem na internetu*, 2016, s. 236.
[25] POLČÁK, R. *Právo informačních technologií*, 2018, s. 589.
[26] ČESKO.*Strategie pro oblast kybernetické bezpečnosti České republiky na období 2012 - 2015* [online]. Vláda České republiky, 2012 [vid. 2023-28-01]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/
[27] ČESKO.*Akční plán ke Strategii pro oblast kybernetické bezpečnosti České republiky na období 2012 - 2015* [online]. Vláda České republiky, 2012 [vid. 2023-28-01]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/

zajišťování bezpečnosti informačních systémů a sítí elektronických komunikací. Co se týče informačních systémů jejichž součástí je práce s utajovanými informacemi, je nutno zdůraznit, že na tyto se zákon o kybernetické bezpečnosti nevztahuje. Pro pochopení zákona je třeba vymezit důležité pojmy, kterými se zabývá § 2 tohoto zákona. Jsou zde vysvětleny pojmy jako kritická informační infrastruktura, kybernetický prostor, provozovatel nebo správce informačního či komunikačního systému, digitální služba informační společnosti aj.

Zákon o kybernetické bezpečnosti není závazný pro všechny instituce a občany v ČR. Povinnost plnit požadavky určené zákonem a jeho vyhláškami mají pouze subjekty stanovené v § 3, kterými jsou:

a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací, pokud není orgánem nebo osobou podle písmene b),

b) orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem nebo provozovatelem komunikačního systému podle písmene d),

c) správce a provozovatel informačního systému kritické informační infrastruktury,

d) správce a provozovatel komunikačního systému kritické informační infrastruktury,

e) správce a provozovatel významného informačního systému,

f) správce a provozovatel informačního systému základní služby, pokud nejsou správcem nebo provozovatelem podle písmene c) nebo d),

g) provozovatel základní služby, pokud není správcem nebo provozovatelem podle písmene f),

h) poskytovatel digitální služby.

Zavádění bezpečnostních opatření v oblasti kybernetické bezpečnosti (§ 4 zákona) je nutností k zajištění ochrany informací a dostupnosti služeb a informačních sítí. Subjekty uvedené v § 3 písm. c) až f) jsou povinny tato opatření provést v nezbytně nutném rozsahu pro zajištění ochrany kritické informační a komunikační infrastruktury a významných informačních systémů. Jejich povinností je o nich vést bezpečnostní

dokumentaci. Tyto orgány musí při volbě dodavatelů zohledňovat požadavky vyplývající z bezpečnostních opatření, což ovlivňuje i konečný výběr smluvní strany.

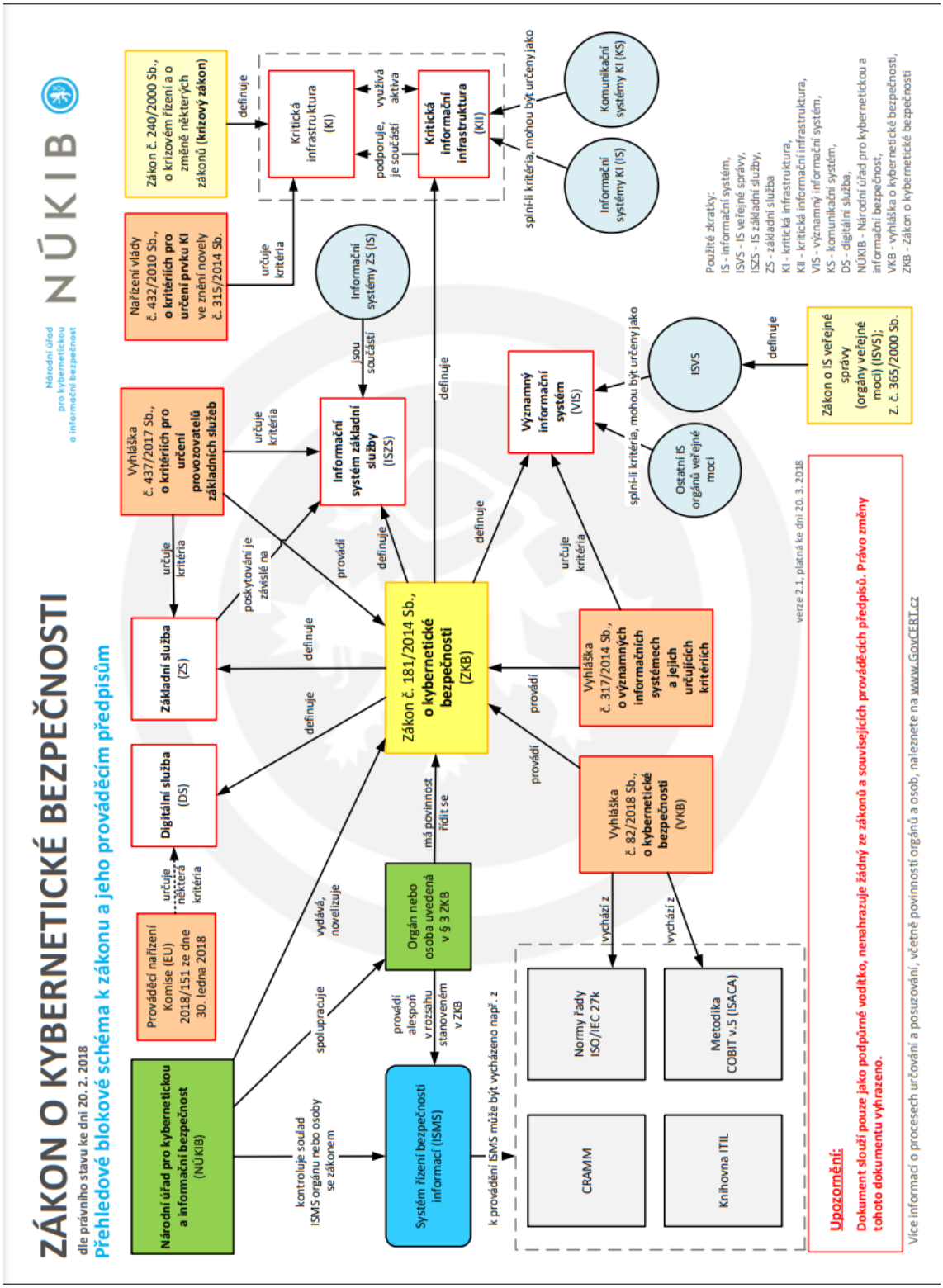
Bezpečnostní opatření jsou v zákoně rozčleněna na technická a organizační. § 5 stanoví jejich jednotlivé druhy a § 6 popisuje, co je obsahem prováděcího právního předpisu (obsah a struktura bezpečnostní dokumentace, obsah bezpečnostních opatření atd.).

Definicí pojmů kybernetická bezpečnostní událost a kybernetický bezpečnostní incident se zabývá § 7, který rovněž stanoví povinnost orgánů a osob uvedených v § 3 písm. c) až f) detekovat veškeré kybernetické bezpečnostní události. Komu mají být incidenty nahlášeny stanoví § 8. Rozlišení je dáno druhem orgánu nebo osoby. Detekované incidenty se hlásí provozovateli národního CERT nebo Národnímu bezpečnostnímu úřadu (orgány dle § 3 písm. c) až f).

Další paragrafy se zabývají evidencí kybernetických bezpečnostních incidentů (§ 9), opatřeními, která jsou nutná k ochraně informačních systémů nebo služeb a sítí před hrozbou v oblasti KB (§ 11), vyhlášením stavu kybernetického nebezpečí (§ 21), kontrolou plnění povinností ze strany dotčených subjektů (23) a aj[28].

[28] 181/2014 Sb. Zákon o kybernetické bezpečnosti. *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. Copyright © AION CS, s.r.o. 2010 [cit. 2023-28-01]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

Obr. 1. – Blokové schéma k zákonu o kybernetické bezpečnosti[29]



[29] Národní úřad pro kybernetickou a informační bezpečnost - Podpůrné materiály. *Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka* [online]. [cit. 2023-28-01]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/

3.1.2 Zákon č. 289/2005 Sb., o vojenském zpravodajství ve znění novelizace zákona č. 150/2021 Sb.

Zákon formuluje podíl Vojenského zpravodajství na zajišťování obrany ČR v kyberprostoru. Na základě podmínek stanovených v tomto zákoně jsou definovány tři oblasti, které vojenské zpravodajství provádí, a to, cituji:

a) cílenou detekci kybernetických útoků a hrozeb majících původ v zahraničí a směřujících proti důležitým zájmům státu, jejichž zajišťování je předmětem obrany České republiky podle zákona o zajišťování obrany České republiky (dále jen „detekce“),

b) identifikaci a vyhodnocování detekovaných kybernetických útoků a hrozeb a jejich dopadů (dále jen „vyhodnocování“),

c) opatření k odvracení detekovaných kybernetických útoků a hrozeb.

Vojenské zpravodajství zpracovává jednou ročně souhrnnou zprávu, kterou prostřednictvím ministerstva obrany předkládá prezidentu republiky a vládě a která informuje o činnostech a opatřeních, kterými se podílí na zajišťování obrany státu v kyberprostoru. Její nedílnou součástí je vyhodnocení jejich účinnosti[30].

3.1.3 Vyhláška č. 317/2014, o významných informačních systémech a jejich určujících kritériích

Předmětem této vyhlášky, která nabyla účinnosti dnem 1. ledna 2015 je stanovení významných informačních systémů a kritérií pro jejich určení[31].

Dle § 2 písm. d) této vyhlášky je významným informačním systémem takový, jehož správcem je orgán veřejné moci, který je součástí organizační složky státu, kraje nebo hlavního města Prahy. Jedná se o informační systémy, které slouží OVM k zajištění těchto agend:

- spisové služby,

- elektronické pošty, určené k použití při výkonu veřejné moci,

[30] 289/2005 Sb. Zákon o Vojenském zpravodajství. *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. Copyright © AION CS, s.r.o. 2010 [cit. 2023-29-01]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-289

[31] ČESKO.Národní úřad pro kybernetickou a informační bezpečnost - *Úvodní stránka* [online]. Copyright © [cit. 2023-29-01]. Dostupné z: https://nukib.cz/download/publikace/legislativa/2021-06-14_vyhlaska-o-VIS.pdf

- vedení úřední desky způsobem, který umožňuje dálkový přístup,

- státního dozoru, kontrolní nebo inspekční činnosti,

- příprav a řešení krizových situací při výkonu veřejné moci,

- mezinárodní spolupráce,

- zadávání VZ (veřejných zakázek).

§ 3 mimo určujících kritérií, která stanoví, jaké důsledky by mohly vzniknout narušením bezpečnosti informací v IS ukládá orgánům veřejné moci vést seznam informačních systémů, které spravuje a pokud tyto nejsou definovány v § 2 odst. 1, musí posoudit, zda splňují určující kritéria a o tomto vést písemný záznam[32].

Nutno podotknout, že vyhl. č. 317/2014. Sb., o významných informačních systémech a jejich určujících kritériích byla novelizována, a to vyhl. 205/2016 Sb., která nabyla účinnosti dnem 1. 7. 2016. V příloze č. 1 této vyhlášky jsou definovány VIS a jejich správci.

Pro názornost možno uvést:

- **Agendový systém pro pozemkové úpravy (ASPU – DMS)** – Státní pozemkový úřad

- **Centrální úložiště elektronických receptů** – Státní ústav pro kontrolu léčiv

- **Portál veřejné správy (PVS)** – Ministerstvo vnitra

- **ePasy** – Ministerstvo zahraničních věcí[33]

[32] 317/2014 Sb. Vyhláška o významných informačních systémech a jejich určujících kritériích. Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění [online]. Copyright © AION CS, s.r.o. 2010 [cit. 2023-15-03]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-317

[33]Novela vyhlášky č. 317/2014 Sb. Zakonycr.eu [online]. [cit. 2023-03-15]. Dostupné z: http://www.zakonycr.eu/clanek.asp?cl=10833/

3.1.4 Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)

Vyhláška zpracovává Směrnici NIS a pro informační a komunikační systémy kritických informačních infrastruktur, významné IS, informační systémy ZS a sítě elektronických komunikací, které využívá poskytovatel digitálních služeb, upravuje strukturu a obsah bezpečnostní dokumentace, obsah a šíři bezpečnostních opatření, určuje kybernetické bezpečnostní incidenty z hlediska jejich zařazení, hodnocení a způsobu ohlášení, definuje náležitosti a způsob ohlášení kybernetického bezpečnostního incidentu, náležitosti přijatých opatření a způsob likvidace informací a dat[34].

3.1.5 Vyhláška č. 437/2017 Sb.. o kritériích pro určení provozovatele základní služby, ve znění vyhlášky č. 573/2020 Sb.

Vyhlášku zpracoval Národní úřad pro kybernetickou a informační bezpečnost a dle § 28 odst. 2 písm. e) Zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů upravil kritéria pro určení provozovatele ZS, upravil odvětvová a dopadová kritéria a určil významnost dopadu narušení ZS na zabezpečení ekonomických činností (např. Energetika – Elektřina – Prodej elektřiny – Závažné omezení, narušení či nedostupnost druhu služby postihující více než 50 000 osob)[35].

Problematika kybernetické bezpečnosti je kromě Zákona o kybernetické bezpečnosti obsažena i v dalších právních předpisech, které souvisejí např. s regulací zdravotnické dokumentace, finančních a bankovních služeb, s ochranou osobních údajů nebo utajovaných informací[36].

[34] 82/2018 Sb. Vyhláška o kybernetické bezpečnosti. *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. Copyright © AION CS, s.r.o. 2010 [cit. 2023-29-01]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82?text=82%2F2018

[35] ČESKO.Viz 437-2017_Platne_zneni_2021.pdf. Národní úřad pro kybernetickou a informační bezpečnost - Legislativa ZKB. *Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka* [online]. [cit. 2023-29-01]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/legislativa-zkb/

[36] POLČÁK, R. *Právo informačních technologií*, 2018, s. 597.

4 Orgány činné v oblasti prevence a obrany proti kybernetickým útokům

Jak již bylo výše zmíněno, kybernetické útoky se netýkají pouze jednotlivců, ale rovněž organizací či jiných subjektů a v neposlední řadě i států. To stálo za potřebou vytvoření speciálních bezpečnostních týmů CSIRT (computer Security Incident Response Team a CERT (computer Emergency Response Team). První z nich řeší kybernetické incidenty, druhý se zabývá identifikací útoku a následným kontaktováním provozovatele sítě.

4.1 Instituce v České republice

4.1.1 Národní centrum kybernetické bezpečnosti (NCKB)

NCKB je výkonným odborem Národního úřadu pro kybernetickou a informační bezpečnost, který zejména zajišťuje:

- fungování Vládního CERT ČR (GovCERT.CZ),

- vzdělávání a osvětovou činnost v oblasti kyberbezpečnosti,

- vývoj a výzkum ve sféře kybernetické bezpečnosti,

- součinnost s organizacemi, které se podílejí na zajištění bezpečnosti kybernetického prostoru a to jak na úrovni národní, tak mezinárodní,

- prevenci před kybernetickými hrozbami, které jsou cíleny na kritickou informační infrastrukturu, významné, příp. vybrané informační systémy veřejné správy nebo informační systémy základní služby a podílí se na řešení a koordinaci bezpečnostních incidentů těchto subjektů,

- organizaci kybernetických cvičení na národní i mezinárodní úrovni,

- zhodnocení rizik ve sféře kybernetické bezpečnosti a stanovení příslušných preventivních a nápravných opatření,

- bezpečnostní politiku Úřadu v rámci své působnosti, plnění závazků, které vyplývají ze spolupráce na mezinárodní úrovni se státy NATO, EU, příp. jinými mezinárodními organizacemi,

- komunikační strategii v oblasti kyberbezpečnosti ve spolupráci s dalšími organizačními celky Úřadu[37].

4.1.2 Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)

Na vzniku tohoto úřadu dne 1. srpna 2017 měla zásadní podíl změna zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Tento zákon byl novelizován, a to zákonem č. 205/2017 Sb. V čele NÚKIB stojí ředitel Úřadu, který je členem Výboru pro kybernetickou bezpečnost a zasedá i při jednáních Bezpečnostní rady státu (BRS)[38].

NÚKIB, který je ústředním správním orgánem pro kybernetickou bezpečnost, zajišťuje nejen národní kybernetickou bezpečnost, ale i ochranu utajovaných informací ve sféře komunikačních a informačních systémů, kryptografickou ochranu a zabývá se otázkou neveřejných služeb v rámci družicového systému Galileo, jež představuje Evropský globální navigační družicový systém[39].

4.1.3 Bezpečnostní týmy

Posunem ve vnímání kyberkriminality je možno označit koncepci vzniku nových organizací zabývajících se ochranou kyberprostoru. Bezpečnostní týmy nazvané zkratkami CERT a CSIRT jsou toho příkladem. Oba týmy mají jasně definovánu oblast působnosti, v níž odpovídají za řešení bezpečnostních incidentů (komunikační pravidla, poskytované služby) Jsou rovněž definovány po stránce legislativní a jsou začleněny do struktur pro krizové řízení v případě hrozby ohrožení státu[40].

CERT – cílem odborníků složených z bezpečnostních analytiků, specialistů na digitalizaci dat a softwarových inženýrů je zlepšit kybernetickou bezpečnost v praxi.

[37] CO JE NCKB. Govcert [online]. [cit. 2023-29-01**]**. Dostupné z: https://www.govcert.cz/cs/
[38] Národní úřad pro kybernetickou a informační bezpečnost - O NÚKIB. *Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka* [online]. [cit. 2023-29-01]. Dostupné z: https://www.nukib.cz/cs/o-nukib/
[39] Téměř tajný Úřad pro kybernetickou bezpečnost odhalil svoji strukturu - Česká justice. *Homepage - Česká justice* [online]. [cit. 2023-29-01]. Dostupné z: https://www.ceska-justice.cz/2017/08/temer-tajny-urad-pro-kybernetickou-bezpecnost-odhalil-svoji-strukturu/
[40] CERT/CSIRT týmy a jejich role - Root.cz. *Root.cz - informace nejen ze světa Linuxu* [online]. Copyright © 1997 [cit. 2023-29-01]. Dostupné z: https://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/

Vzájemně spolupracují na vývoji špičkových informací vedoucích k zabezpečení síťových systémů a podílejí se na výzkumu bezpečnostních zranitelností v softwarových produktech[41].

Vládní CERT (GovCERT.cz) – je součástí NBÚ a zaměřuje se na kybernetické bezpečnostní incidenty v počítačových sítích státní správy a samosprávy a řeší incidenty, které ohrožují bezpečnost státu z hlediska napadení kritické informační infrastruktury a významných informačních systémů. Většinou se jedná o státní instituce, pro které jsou vytvořeny konkrétní zákony.

Národní CERT – bezpečnostní tým specialistů, který je od roku 2015 provozován právnickou osobou. Výběrem Národního bezpečnostního úřadu se jím stalo CZ.NIC, které již v minulosti bylo provozovatelem a správcem informačních systémů a elektronických komunikací. Na rozdíl od vládního CERT řeší národní CERT ostatní bezpečnostní incidenty v počítačových sítích v ČR[42].

CSIRT – bezpečnostní týmy CSIRT jsou vytvářeny v rámci jednotlivých organizací, které využívají ke své hlavní činnosti internet (např. banky), nebo které chod internetu přímo zprostředkovávají (ISP, poskytovatelé služeb a obsahu). Tito specialisté řeší problémy v rámci své působnosti, kterou je většinou síťová infrastruktura, v níž mají možnost reálně zasáhnout. Na rozdíl od běžného bezpečnostního týmu je tým tohoto typu zapojen do světové bezpečnostní infrastruktury, se kterou může sdílet informace a formální postupy. Každý z bezpečnostních týmů musí mít veřejně dostupné kontaktní údaje a pravidla činnosti. V praxi to znamená, že lze určit, kdo jsou členové týmu, jak se s nimi spojit, jaké služby nabízejí a především v jaké oblasti (domény, služby, síť) a na základě těchto informací je může napadený uživatel kontaktovat a iniciovat řešení příslušných incidentů. V závislosti na činnosti bezpečnostního týmu při řešení problému je možné tým rozdělit na interní a koordinační. Rozdíl mezi nimi je ten, že zatímco interní tým může zasáhnout přímo (např. zavést filtraci sítě, odpojit infikovaný zdroj), tým koordinační možnost přímého zásahu nemá. Jeho činnost spočívá v komunikaci a spolupráci při zprostředkování informací.

[41] The CERT Division | *Software Engineering Institute. Software Engineering Institute* [online]. Copyright © 1998 [cit. 2023-30-01]. Dostupné z: https://www.sei.cmu.edu/about/divisions/cert/

[42] NBÚ vybral provozovatele národního CERT (CSIRT.CZ), je jím CZ.NIC. *Úvodní stránka* [online]. [cit. 2023-30-01]. Dostupné z: https://www.nbu.cz/cs/aktualne/820-621-nbu-vybral-provozovatele-narodniho-cert-csirtcz-je-jim-cznic/

Národní CSIRT - jeho hlavním cílem je ve zprostředkování kontaktu mezi původcem problému a napadeným v rámci oblasti působnosti nebo v rámci státu. Jelikož tito odborníci nevládnou nad fyzickou infrastrukturou (kabelovody, rozvodné skříně aj.), nemohou přímo zasáhnout, pouze zprostředkovávají kontakty, nebo v případě rozsáhlejších problémů postupy jednotlivých řešitelů z více složek. Národní tým tak řeší incidenty velmi závažné, které se nedají řešit jinou cestou. Jeho snahou je působit k veřejnosti cestou osvěty a vzdělání a podpořit vznik dalších CSIRT týmů, kterým pomáhají při zavádění standardních postupů a vstupu na mezinárodní úroveň.

Vládní CSIRT – jeho činnost je dána legislativně, cílem bezpečnostních týmů je řešení incidentů na úrovni státní správy a samosprávy a incidentů ohrožujících služby a bezpečnost státu. Mívá podobu interního týmu, který má možnost v případě problému ihned zasáhnout.

Z hlediska komunikace, spolupráce či výměny informací jsou všechny týmy CERT nebo CSIRT sobě rovnocenné. Více pravomocí a tím i možnost jistého způsobu nadřazenosti může jednotlivým bezpečnostním týmům dát pouze legislativa, např. ve sféře reakce ze strany provozovatelů sítí[43].

4.2 Mezinárodní instituce

4.2.1 Speciální útvar kybernetických operací NATO

V souvislosti s útoky Ruska na infrastrukturu Estonska zřídila v roce 2009 NATO pro boj s kyberterorismem speciální útvar. Postupně došlo k její transformaci. Jako reakci na kybernetickou válku Ruska proti Ukrajině a provokaci Rusů během amerických voleb zařadila NATO v roce 2017 použití kybernetických zbraní jako nedílnou součást veškerých vojenských operací NATO a odklonila se pouze od postoje využívat kybernetiku jen k obranným účelům[44].

4.2.2 Computer Emergency Response Team EU

Tato instituce sídlící v Bruselu vznikla v roce 2011. Její odborníci na bezpečnost informačních technologií jsou členové různých institucí a orgánů EU. Zabývají se

[43] CERT/CSIRT týmy a jejich role - Root.cz. *Root.cz - informace nejen ze světa Linuxu* [online]. Copyright © 1997 [cit. 2023-31-01]. Dostupné z: https://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/

[44] NATO's Little Noticed but Important New Aggressive Stance on Cyber Weapons – *Foreign Policy. Foreign Policy – the Global Magazine of News and Ideas* [online]. Copyright © 2023, Graham Digital Holding Company [cit. 2023-31-01]. Dostupné z: https://foreignpolicy.com/2017/12/07/natos-little-noticed-but-important-new-aggressive-stance-on-cyber-weapons/

shromažďováním, správou a analýzou dat, které souvisí s hrozbami, zranitelnými místy nebo incidenty souvisejícími s neutajovanou infrastrukturou IKT a tyto informace sdílejí s dalšími subjekty převážně v rámci EU, ale i mezinárodními partnery mimo unii[45].

[45] CERT-EU – computer emergency response team | European *Union. Redirecting to /select-language?destination=/node/1* [online]. [cit. 2023-31-01]. Dostupné z: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/cert-eu_en

5 Veřejná správa

Vzhledem k názvu bakalářské práce, která se týká veřejné správy, je třeba definovat a vymezit tento pojem. Ohlédneme-li se do historie práva, zjistíme, že pojem „administratio res publika“ neboli „správa věcí veřejných“ používali již Římané po svržení krále. Vzniklé úřady a úředníci byli nazýváni latinsky Magistratus. Zde nalézáme počátek úřadů, úředníků a veřejné správy. Z výše uvedeného je vidno, že některé z termínů byly zachovány do dnešní doby[46].

Správa společnosti neboli správa věcí veřejných ve společnosti zorganizované ve stát je projevem realizace výkonné moci ve státě[47].

5.1 Vymezení pojmů

Pojem správa je obecně chápán jako záměrná činnost vedoucí k dosažení určitého cíle[48]. Správu můžeme v obecném smyslu rozdělit na soukromou a veřejnou. Veřejná správa, která je na rozdíl od soukromé vykonávána ve veřejném zájmu, je více vázána. Státní moc může být dle čl. 2 odst. 2 Listiny základních práv a svobod uplatňována pouze v případech, rozsahu a způsobem, které stanoví zákon. Uplatňování státní moci je upraveno Ústavou České republiky, a to v čl. 2 odst. 3. Veřejnou správu lze chápat jako druh činnosti (funkce) nebo instituce (orgánu), který tuto správu vykonává[49].

Veřejnou správou se rozumí:

- správa území (obce, kraje, státu),

- správa záležitostí (služby občanům, veřejnosti, veřejné záležitosti),

[46] Politické zřízení a úřední funkce v Římě. *Antika.avonet.cz* [online]. [cit. 2023-12-03]. Dostupné z: http://antika.avonet.cz/article.php?ID=1493

[47] PRŮCHA, P. *Správní právo: obecná část*. 7., dopl. a aktualiz. vyd., (V nakl. Doplněk 2.). Brno: Masarykova univerzita, 2007. ISBN 9788021042766, s. 48

[48] SLÁDEČEK, V. Obecné správní právo. 3., aktualiz. a upr. vyd. Praha: Wolters Kluwer Česká republika, 2013. ISBN 978-80-7478-002-8, s. 18

[49] Zkušební otázky a odborná literatura - Státní služba. Úvodní strana - Ministerstvo vnitra České republiky [online]. Copyright © 2023 Ministerstvo vnitra České republiky. Všechna práva vyhrazena. [cit. 12.03.2023]. Dostupné z: https://www.mvcr.cz/sluzba/clanek/zkusebni-otazky-a-odborna-literatura.aspx

- správa věci (veřejného sektoru, ke kterému má veřejnost vlastnická práva. Jedná se o nemovité věci, např. pozemky, budovy, komunikace nebo movité věci, např. dopravní prostředky),

- správa financí (správa veřejných rozpočtů, veřejných financí),

- správa objektů (přírodních zdrojů, veřejných zařízení a objektů).

5.2 Funkce veřejné správy

Funkce veřejné správy jsou mnohostranné a závisí na konkrétním cíli dané oblasti řídící činnosti,

Veřejnou správu charakterizují tyto její funkce:

- mocenská,

- ochranná,

- služby veřejnosti,

- regulační,

- organizační.

5.2.1 Mocenská funkce

Veřejná správa realizuje svou moc ve státě působením státního zřízení prostřednictvím právního řádu. Veřejná moc má schopnost ovlivňovat chování společnosti potřebným žádoucím směrem, jejím základem je formální autorita. Veřejnou moc lze rozdělit na centrální, kam patří moc výkonná, soudní a zákonodárná a necentrální, která je Ústavou ČR svěřena státní samosprávě.

5.2.2 Ochranná funkce

Tato funkce slouží k zajištění vnitřní a vnější bezpečnosti a veřejného pořádku. Orgány veřejné správy zajišťují obranu a bezpečnost státu, ochranu a bezpečnost občanů a ochranu veřejných záležitostí.

5.2.3 Služby veřejnosti

Pod pojmem služby veřejnosti rozumíme činnosti poskytované ve veřejném zájmu, např. sociální, finanční, pečovatelské, ekonomické a další, které jsou vymezeny veřejným právem a slouží k rozvoji společnosti.

5.2.4 Regulační funkce

Regulační funkce veřejné správy spočívá v prosazování systému, který je založen na solidaritě, toleranci a politickém pluralismu. Umožňuje shromažďování a sdružování občanů a podnikatelského sektoru nebo sdružování v neziskových, veřejně prospěšných organizacích.

5.2.5 Organizační funkce

Veřejná správa organizuje záležitosti občanů (vzdělávání, služby zdravotní a sociálního zabezpečení), institucí (správu katastru, soudů, obrany státu) a státní (člení území na obce, kraje, regiony…)[50].

5.3 Struktura veřejné správy

Velmi důležité je rozlišování dvou podsystémů veřejné správy, kterými jsou státní správa a samospráva a to z důvodu legislativní úpravy systému české veřejné správy a postavení a vztahů těchto prvků a rovněž s ohledem na způsob financování jednotlivých institucí, především těch, patřících do územní samosprávy[51].

Do tohoto členění lze uvést i ostatní veřejnou správu, považovanou za zbytkovou oblast VS, kterou vykonávají zčásti samosprávné a nesamosprávné instituce při plnění veřejných úkolů (např. veřejný ústav)[52].

5.3.1 Státní správa

Státní správou se rozumí činnost státu, kterou provádí přímo státní orgány, případně jiné, na které stát výkon této správy v daném rozsahu přenesl. Právní úprava státní správy a jejího působení v ČR je mimo ústavní zakotvení definováno zákonem č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy ČR. Tento

[50] KÁŇA, P. *Základy veřejné správy: [vybrané kapitoly veřejné správy pro studium žáků středních škol a maturitní témata k ústní maturitní zkoušce z předmětu Veřejná správa]*. 2., dopl., přeprac. vyd. Ostrava: Montanex, 2007. Varia (Montanex). [cit. 2023-12-03]. s. 12

[51] ESF:BPV_ZVFS Základy veřejných financí a veřejné správy. *Informační systém* [online]. [cit. 2023-12-03]. Dostupné z: https://is.muni.cz/el/econ/podzim2015/BPV_ZVFS/um/59151890/60414461/

[52] SLÁDEČEK, V. Obecné správní právo. 3., aktualiz. a upr. vyd. Praha: Wolters Kluwer Česká republika, 2013. [cit. 2023-12-03]. s. 309.

zákon upravuje působnost a strukturu centrální státní správy, tj. ministerstev a dalších ústředních orgánů státní správy a některých dalších správních úřadů s celostátní působností. Mezi přímé vykonavatele státní správy jménem a namísto státu patří

- vláda,

- prezident republiky,

- ministerstva a jiné ústřední orgány státní správy,

- další správní úřady s celostátní působností,

- bezpečnostní sbory,

- správní úřady.

Kromě orgánu státu se na výkonu státní správy mohou podílet i další subjekty veřejné správy odlišné od státu, případně také soukromé osoby v případě, že byl na ně výkon státní správy přenesen. Tyto orgány se nazývají nepřímí vykonavatelé státní správy a jsou jimi:

- právnické a fyzické osoby soukromého práva,

- orgány obcí (obecní úřady, úřady obcí s rozšířenou působností, rada obce, komise rady obce, zvláštní orgány obce),

- orgány krajů (krajské úřady, rada kraje, zvláštní orgány kraje).

Pro organizaci státní správy jsou příznačné principy výstavby a fungování. Základním principem členění státní správy je princip územní a věcný. Územní hledisko znamená, že vykonavatel státní správy je definován jako procesně příslušný pro dané území. U věcného principu jde o uplatnění výlučně nebo převážně obsahově stejnorodé nebo příbuzné agendy, jež je v působnosti orgánu státní správy.

Dalším hlediskem je princip centralizace a decentralizace. Centralizovaný systém se vyznačuje výkonem státní správy v jednom řídícím centru, které rozhoduje o všech otázkách a ovlivňuje rozhodování nižších orgánů. Decentralizovaný systém je založen na přenesení pravomoci a působnosti na jiné orgány státní správy než je stát, na tzv.

samosprávné orgány. V tomto případě jednotlivé jiné orgány státní správy pracují samostatně a s orgány státní správy nejsou ve vztahu nadřízenosti a podřízenosti. Jedním z dalších principů při organizaci státní správy jsou horizontální a vertikální koncentrace a dekoncentrace. Horizontální koncentrace soustřeďuje všechny funkce jedné úrovně do jednoho orgánu, dekoncentrace je opačný postup, tj. funkce na stejné úrovni jsou rozděleny do více orgánů. Vertikální koncentrace a dekoncentrace znamená, že funkce v rámci jedné organizační struktury jsou rozděleny mezi nižší (dekoncentrace) a vyšší úroveň (koncentrace). Ve státní správě se uplatňuje kolegiální a monokratický princip složení jednotlivých orgánů a způsobu rozhodování. Za kolegiální orgán je možno označit vládu, která je kolektivem osob pracujícím ve sboru. Typicky monokratickým orgánem je ministerstvo, v jehož čele stojí jedinec (ministr), který samostatně rozhoduje pouze v některých záležitostech a především přezkoumává rozhodnutí. V neposlední řadě je v rámci státní správy uplatňován princip nadřízenosti a podřízenosti. Princip nepodřízenosti je charakteristický pro orgány územní samosprávy, naopak oblast státní správy je charakteristická principem nadřízenosti vyšších a podřízeností nižších orgánů[53].

5.3.2 Samospráva

Samospráva je obdobně jako státní správa osobitým druhem společenského řízení. Veřejná správa je vykonávána jinou institucí, než je stát. Působí nezávisle na státu a ten vytváří podmínky pro její fungování[54].

Organizované společenství lidí, ať již územně či jinak, spravuje v mezích legislativy své záležitosti samo autonomním způsobem a hlavní rozhodnutí o svých věcech činí buď přímo (rozhodováním všech prostřednictvím přímé demokracie) nebo prostřednictvím volených orgánů (formou zastupitelské demokracie). Volené orgány jsou většinou ostatním orgánům společenství nadřazené. Autonomie ovlivňuje míru volnosti pro zavádění inovačních prvků v řízení samosprávy a její pojetí je tedy chápáno jako právo a schopnost řídit a uspořádat většinu veřejných záležitostí ve vlastním zájmu a na vlastní odpovědnost. Její výhodou je, že je spravovanému subjektu blíže, proto je při zabezpečování místních nebo zájmově vymezených záležitostí efektivnější a také levnější. Stát jako držitel státní moci zasahuje do samosprávy tvorbou a ochranou zákonů

[53] Zkušební otázky a odborná literatura - Státní služba. *Úvodní strana - Ministerstvo vnitra České republiky* [online]. Kapitola 1: Organizace a činnost veřejné správy. Copyright © 2023 Ministerstvo vnitra České republiky. Všechna práva vyhrazena. [cit. 2023-12-03]. Dostupné z: https://www.mvcr.cz/sluzba/clanek/zkusebni-otazky-a-odborna-literatura.aspx

[54] Co je Samospráva? *Definice pojmu*. Superia.cz [online]. [cit. 2023-12-03]. Dostupné z: https://cojeto.superia.cz/pravo/samosprava.php

a v případě mocenských rozhodnutí. Nestátní veřejnou správu vykonávají instituce s vlastní právní subjektivitou určenou k tomuto účelu a jimž byly ústavou a zákony svěřeny nástroje k jejímu výkonu. Cílem těchto veřejnoprávních korporací, které veřejnou správu vykonávají svým jménem a ve své působnosti, je reprezentovat veřejné zájmy. Samospráva není podřízena orgánům státní správy, tj. ústřední orgány se nemohou vměšovat do jejich činnosti ve smyslu ukládání pokynů či příkazů. Stát zasahuje do činnosti samosprávy pouze v případech, kdy to vyžaduje ochrana zákona a pouze způsobem, který zákon stanoví. Tímto způsobem je zajištěna kontrola fungování samosprávy. Příjmy a výdaje rozpočtu samospráv vyvolávají diskuze o jejich ekonomické soběstačnosti, případně o jejím ekonomickém omezení. Samosprávy jsou si formálně rovny po horizontále, znamená to např., že všechny obce mají rovné právo na samosprávy. Samospráva a státní správa mají být navzájem komplementární, tj. jejich činnost si nemá vzájemně konkurovat, ale vzájemně se doplňovat. Obě tyto části veřejné správy mají shodný cíl, a tím je služba občanům a společnosti. Samosprávu lze členit na územní a zájmovou[55].

Územní samospráva

Obecní samospráva byla v ČR obnovena počátkem 90. let 20. století a v roce 2000 proběhly první volby do krajských zastupitelstev nově vytvořených samosprávných krajů. Základními územními samosprávnými celky v České republice jsou obce, vyššími jsou kraje. Spolu tvoří dvoustupňový systém územní samosprávy. Územní celky sdružují územně příslušná společenství občanů, která mají právo na svoji samosprávu. Legislativně je činnost a působnost obcí, krajů a hlavního města Prahy upravena zákony č. 128/2000 Sb., o obcích, ve znění pozdějších předpisů, č. 129/2000 Sb., o krajích, ve znění pozdějších předpisů a č. 131/2000 Sb., o hlavním městě, ve znění pozdějších předpisů[56].

Zájmová samospráva

[55]Informační systém [online]. Copyright © [cit. 2023-26-02]. Dostupné z: https://is.muni.cz/el/1456/jaro2017/MKV_VES2/um/68159517/VEREJNA.SPRAVA.OCHRANA.PUCEK.SPACEK.pdf

[56] Zkušební otázky a odborná literatura - Státní služba. *Úvodní strana - Ministerstvo vnitra České republiky* [online]. Kapitola 1: Organizace a činnost veřejné správy. Copyright © 2023 Ministerstvo vnitra České republiky. Všechna práva vyhrazena. [cit. 2023-12-03]. Dostupné z: https://www.mvcr.cz/sluzba/clanek/zkusebni-otazky-a-odborna-literatura.aspx

Právo rozhodovat samostatně o vlastních záležitostech může být svěřeno i dílčím společenstvím, která vyjadřují určitý zájmový či profesní stav, např. lékaři, advokáti, notáři, architekti. Příkladem profesní samosprávy v ČR je Česká lékařská komora, Notářská komora ČR, Česká advokátní komora a další. Do zájmové samosprávy patří i školní samospráva, pomocí které se žáci a jejich zákonní zástupci podílejí na řízení školy[57].

Samospráva vysokých škol je zastupována členy akademické obce prostřednictvím voleného akademického senátu a dalších akademických orgánů.

Charakteristické znaky zájmové samosprávy:

- právní základ – subjekty mají právní subjektivitu, svými předpisy mohou regulovat jemu podřízené subjekty,

- zákonný základ – subjekty jsou zřízeny zákonem jako veřejnoprávní korporace s výjimkou soukromých VŠ, které jsou zřízeny na základě soukromé iniciativy se státním souhlasem,

- ekonomický základ - samosprávy disponují vlastním majetkem a vykazují vlastní hospodaření, přičemž převážný zdroj příjmů tvoří příspěvky jejích členů. U VŠ jsou zdrojem příjmů platby za studium získané od studentů nebo státu,

- osobní základ – vždy se vztahuje k osobám, především k fyzickým osobám[58].

Věcná samospráva

Zákon č. 128/2000 Sb. umožnil obcím, jakožto veřejnoprávním korporacím, tvořit svazek obcí. Činnost a hospodaření této právnické osoby jsou závislé na vůli svých zakladatelů, tj. obcích a rovněž na podmínkách, které vymezuje obcím zákon. Způsobilost k právním úkonům sdružených obcí je zakotveno v zakladatelské smlouvě a ve stanovách. Předmětem jeho činnosti je ochrana a prosazování společných zájmů obcí. Členské příspěvky obcí mají charakter prostředků veřejných rozpočtů. Majetek, který obec do svazku může vložit nadále zůstává jejím vlastnictvím. Členské obce se dle

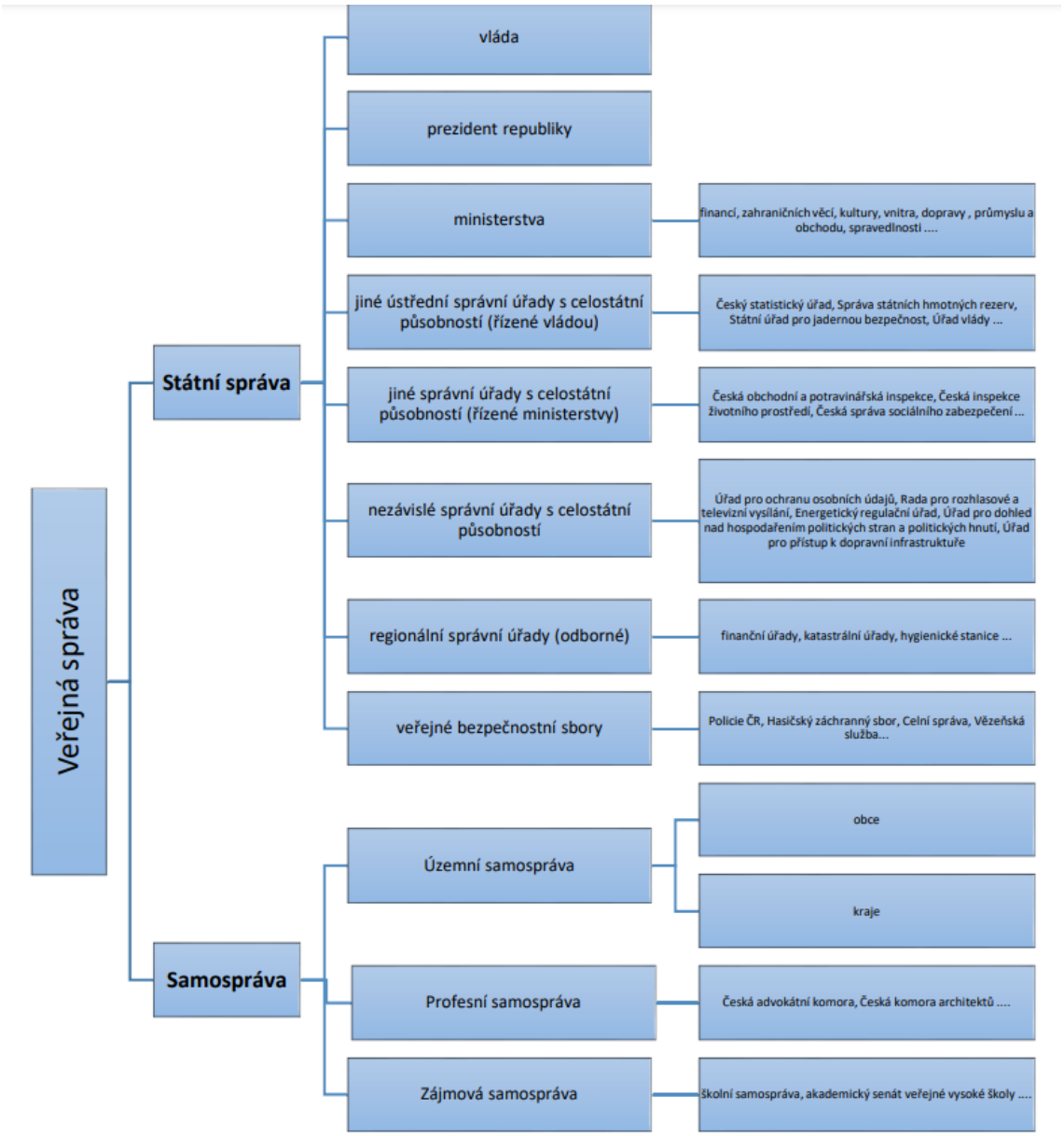
[57] Samospráva - *Iuridictum.* [online]. [cit. 2023-12-03]. Dostupné z: https://iuridictum.pecina.cz/w/Samospr%C3%A1va

[58] Několik poznámek k samosprávě a řízení vysokých | epravo.cz. *EPRAVO.CZ – Váš průvodce právem - Sbírka zákonů, judikatura, právo* [online]. Copyright © EPRAVO.CZ, a.s. 1999 [cit. 2023-12-03]. Dostupné z: https://www.epravo.cz/top/clanky/nekolik-poznamek-k-samosprave-a-rizeni-vysokych-skol-57865.html

podmínek uvedených ve stanovách podílejí na rozdělení zisku a na úhradě případné ztráty z podnikatelské doplňkové činnosti. S finančními prostředky a majetkem nakládá svazek jako správce cizího majetku. Právní způsobilost svazek nabývá zápisem do registru sdružení a zaniká jeho výmazem z registru[59].

[59] Základní pravidla pro svazky obcí | Moderní obec – odborný měsíčník . *Moderní obec – odborný měsíčník* [online]. Copyright © [cit. 2023-12-03]. Dostupné z: https://moderniobec.cz/zakladni-pravidla-pro-svazky-obci/

Obr. 2. – Schéma členění veřejné správy[60]



[60] Zkušební otázky a odborná literatura - Státní služba. *Úvodní strana - Ministerstvo vnitra České republiky* [online]. Kapitola 1: Organizace a činnost veřejné správy. Copyright © 2023 Ministerstvo vnitra České republiky. Všechna práva vyhrazena. [cit. 2023-12-03]. Dostupné z: https://www.mvcr.cz/sluzba/clanek/zkusebni-otazky-a-odborna-literatura.aspx

5.4 Orgány veřejné správy jako subjekty kybernetické bezpečnosti

Oblast ochrany informačních systémů veřejné správy a infrastruktury je jednou ze základních oblastí ochrany kybernetického prostoru. Její důležitost pramení především z neustále vzrůstající míry elektronizace veřejné správy, resp. procesů, které v ní probíhají. Drtivá většina orgánů veřejné správy má v současné době veřejně přístupné internetové stránky (od základních statistických informací až po komplexní aplikace s mnoha funkcemi), ke komunikaci běžně využívá elektronickou poštu (e-maily), zpracovává elektronická podání a pracuje s mnoha dalšími informačními systémy.

Trend elektronizace veřejné správy má i svá negativa v podobě rostoucího zájmu útočníků, kteří si informační systémy veřejné správy a infrastrukturu vybírají za cíle svých kybernetických útoků. Motivy těchto útoků bývají různé, jejich nejčastěji to bývá kybernetická špionáž[61].

Ochrana informačních systémů VS a informační infrastruktury má svá specifika. Jedním z nich je skutečnost, že tato informační infrastruktura se dělí dle kompetencí jednotlivých orgánů, v případě orgánů státních i dle ústavního principu dělby moci.

Dalším specifikem, které je nutno zohlednit v rámci právní regulace kyberbezpečnosti je to, že orgán veřejné správy plní roli správce i provozovatele pouze u části infrastruktury a informačních systémů. V ostatních případech pak orgány VS mají pouze roli správce, úloha provozovatelů je určena různým soukromoprávním subjektům. Z výše uvedeného je patrno, že orgány veřejné správy patří mezi významné subjekty kybernetické bezpečnosti, a tudíž mezi subjekty, kterým jsou za účelem ochrany kybernetického prostoru ukládány prostřednictvím právních předpisů povinnosti. Tento přístup se odráží v české právní úpravě prostřednictvím ZoKB, který zavádí kategorii tzv. významných informačních systémů[62].

[61] Výroční zpráva Bezpečnostní informační služby za rok 2017 [online]. Bezpečnostní informační služba, 2018, s. 15 a násl. [vid. 2023-27-02]. Dostupné z: https://www.bis.cz/public/site/bis.cz/content/vyrocnizpravy/2017-vz-cz.pdf

[62] POLČÁK, R. Internet a proměny práva. Praha: Auditorium, 2012. Téma (Auditorium), s. 350.

6 Elektronizace veřejné správy

Základním předpokladem pro optimalizaci činnosti veřejné správy je využívání moderních komunikačních a informačních technologií. Občanům i firmám tak veřejná správa může nabídnout služby, které jsou nejen profesionálnější, ale i rychlejší a srozumitelnější. Dosažení těchto cílů je možné pouze za předpokladu, že organizace VS budou dostatečně vybaveny informačními technologiemi, služby klientům budou zpřístupněny v on-line prostředí a úředníci budou schopni s náročnými informačními systémy pracovat[63].

6.1 Informační systémy veřejné správy

Informační systém tvoří programy (software), zařízení (hardware), organizační opatření a lidé, kteří společně působí na splnění vytyčených cílů. Uživatelům poskytuje informace prostřednictvím zpracování dat. Shromážděná data ukládá a pomocí různých analýz a procesů dochází k jejich třídění, vyhledávání relevantních dat a jejich zpracování do formátu, který je pro určený účel nejvýhodnější. Každý systém tvoří prvky, jež jsou jeho nedílnou součástí. Se svým okolím systém komunikuje pomocí vstupů a výstupů, podstatná je znalost vazeb na ostatní objekty a okolí. Tyto systémy mohou být otevřené, kdy alespoň jeden z jeho prvků komunikuje s okolím, nebo uzavřené. Každý ze systémů má svoji dynamickou a statickou část. U reálných systémů lze určit jejich strukturu, vazby a chování. ISVS v ČR tvoří soubor informačních systémů sloužících pro výkon veřejné správy nebo zajišťujících činnost dle zvláštních zákonů. Z právního hlediska zabezpečují systematickou a cílevědomou informační činnost. Optimalizací a budováním ISVS je snaha docílit zvýšení efektivity a autority veřejné správy, zvýšení transparentnosti a rozvoj ekonomického prostředí a posílení důvěry občanů ve veřejnou správu. Základní podmínkou funkčnosti ISVS jako celku je vytvoření organizačních, technických a právních aspektů vedoucích ke sdílení dat ve veřejné správě. V souvislosti s informačními systémy veřejné správy je vhodné stručně přiblížit pojmy provozovatele a správce informačního systému.

[63] Informační technologie ve veřejné správě. *Czso.cz* [online]. 2020 [cit. 2023-12-03]. Dostupné z: https://www.czso.cz/csu/czso/verejna_sprava

6.1.1 Správci a provozovatelé informačních systémů

Správcem IS veřejné správy je subjekt, který dle ZoKB odpovídá za provozování informačního systému a stanoví prostředky a účel zpracování informací. Z uvedeného tedy vyplývá, že aby byl subjekt považován za správce, musí současně splňovat oba výše uvedené znaky.

Správci ISVS jsou:

- ministerstva,

- další správní úřady,

- orgány územní samosprávy,

- jiné státní orgány[64].

Správce je ten, který má k dispozici informace o tom, jaký systém spadá do působnosti zákona o kybernetické bezpečnosti, čím je tvořen, zda-li je provozován jedním nebo více dodavateli a s ohledem na tyto poznatky je utvrzen v tom, zda daným dodavatelem poskytovaná činnost opravdu spočívá v zajišťování funkčnosti programových a technických prostředků vytvářejících systém[65].

Dalším významným pojmem je provozovatel informačního (komunikačního) systému, jehož definici lze nalézt v § 2 písm. g) ZoKB, ve kterém je formulován jako orgán nebo osoba, které zajišťují funkčnost prostředků technického a programového rázu tvořících komunikační či informační systém. Okruh povinných osob byl rozšířen o provozovatele až s novelizací zákona č. 104/2017 Sb., v období před touto právní úpravou se na provozovatele nebo subjekty v tomto postavení nevztahovaly přímé zákonné povinnosti. Vzhledem k tomu, že pouze malá část subjektů byla jak správci, tak zároveň provozovateli informačních systémů, došlo z hlediska ZoKB pouze k jejich omezenému dopadu[66].

[64] OPF:EVSNPEVS Ekonomika odvětví veřejného sektoru. Informační systém [online]. [cit. 2023-12-03]. Dostupné z: https://is.slu.cz/el/opf/leto2021/EVSNPEVS/um/9_informacni_systemy.pdf

[65] Provozovatel informačního nebo komunikačního systému v3.2. Nukib.cz [online]. [cit. 2023-12-03]. Dostupné z: https://nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/

[66] Důvodová zpráva. *Návrh zákona, kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, a některé další zákony* [online]. Úřad vlády České republiky, 2015, s. 36. [cit. 2023-26-02]. Dostupné z: https://apps.odok.cz/attachment/- /down/KORNAB7GCFCC

Správce může provozováním ISVS pověřit i jiný subjekt, pokud to některý ze zákonů nevylučuje[67].

Nutno poznamenat, že ZoKB vymezuje i další druhy povinných subjektů, které mají charakter provozovatele nebo správce, mimo již zmíněného provozovatele informačního systému a provozovatele informačního (komunikačního) systému se dále jedná o správce komunikačního systému a o provozovatele základní služby[68].

6.2 Digitalizace úřadu

Každý úřad, který chce úspěšně naplňovat cíle vedoucí k jeho digitalizaci, musí mít zpracován systém řízení kvality a informační koncepci úřadu. Ta stanovuje cíle a principy, jež vymezují povinnosti úřadu ve vztahu k optimalizaci fungování VS a k jeho digitalizaci, a to prostřednictvím architektury úřadu. Jednotlivé prvky architektury úřadu tvoří informační aktiva, agendy, procesy a jeho vnitřní organizace. Architektura popisuje strukturu a chování úřadu, jeho plánované změny a informatickou podporu. Úřad ji musí za pomoci nástrojů a metodik k tomu určených, které jsou publikovány v metodických pokynech Národní architektury eGovernmentu popsat, případně doplnit vazby jednotlivých prvků. Zpracovaná architektura může být využita např. při rozhodování o prioritách digitalizace úřadu, pro komunikaci s vedením úřadu a nastavením informačních vazeb s jinými úřady, k popisování toků dat, vazeb jednotlivých agend na informační systémy nebo komunikaci úřadu s veřejností[69].

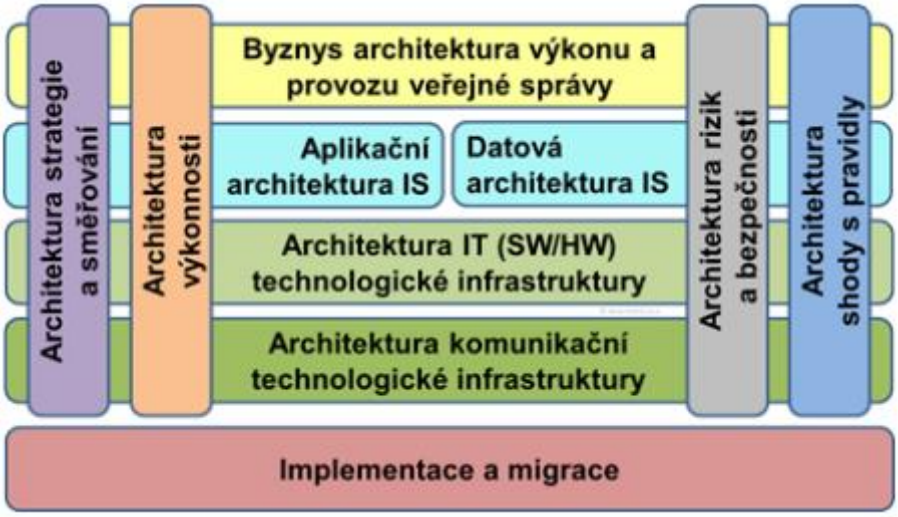
[67] OPF:EVSNPEVS Ekonomika odvětví veřejného sektoru. *Informační systém* [online]. [cit. 2023-13-03]. Dostupné z: https://is.slu.cz/el/opf/leto2021/EVSNPEVS/um/9_informacni_systemy.pdf

[68] 181/2014 Sb. Zákon o kybernetické bezpečnosti. *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. Copyright © AION CS, s.r.o. 2010 [cit. 2023-13-03]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

[69] Ministerstvo financí ČR [online]. Copyright © [cit. 2023-13-03]. Dostupné z: https://www.mfcr.cz/assets/cs/media/2022-11-08_MP-CHJ-24-Digitalizace-uradu.pdf

Architektura úřadu je členěna do jednotlivých domén viz obrázek:

Obr. 3. – Schéma členění veřejné správy[70]



Klíčovými doménami architektury úřadu jsou horizontální vrstvy, které zahrnují všechny základní prvky organizace, tj. její zdroje (převážně ICT) a její fungování. Do těchto konceptů patří:

Byznys architektura – popisuje jednotlivé služby a procesy, které v úřadu probíhají, jeho organizační uspořádání a odpovědnost jednotlivých útvarů.

Architektura informačních systémů – tvoří ji datová architektura (druh dat, jejich klasifikace, komu jsou poskytovány a v jakých informačních systémech) a aplikační architektura (druh spravovaných IS, jejich klasifikace, správce a provozovatel, funkce IS a systém jeho identifikace, druhy licencí, přístup a rozsah jednotlivých členů úřadu k IS).

Architektura technologická – zahrnuje architekturu IT technologií (popis jednotlivých platforem IT softwarového a hardwarového vybavení a jejich vazby na aplikace, služby platforem, jejich správce, provozovatel a umístění) a architekturu

[70]Ministerstvo financí ČR [online]. Copyright © [cit. 2023-13-03]. Dostupné z: https://www.mfcr.cz/assets/cs/media/2022-11-08_MP-CHJ-24-Digitalizace-uradu.pdf

komunikační infrastruktury (struktura a služby komunikačních sítí a technického vybavení, druh využívaných komunikačních služeb, provozovatel sítí, komunikační rozhraní, dostupnost komunikační infrastruktury).

Kromě horizontálních existují rovněž vertikální domény, které je doplňují a protínají. Patří sem:

Architektura rizik a bezpečnosti (popisuje rizika a způsob reakce na bezpečnostní události a incidenty).

Architektura výkonnosti (provozní efektivita, dosažená strategie a účelnost).

Architektura strategie a směřování, tzv. motivační architektura (důvod, omezení či potřeba změn, jejich cíle, zainteresované osoby).

Architektura shody s pravidly, standardizace a dlouhodobé udržitelnosti[71].

6.3 Data a jejich sdílení

Obsahem každého informačního systému jsou informace a data. Ve veřejné správě mají tato data cennou informační hodnotu. K dosažení co nejvyšší efektivity práce s daty musí každý úřad v pozici vlastníka informačního systému zajistit bez navýšení finančních prostředků k těmto datům přístup v otevřeném, strojově čitelném formátu a možností s nimi libovolně nakládat. Úřady data spravují v IS v rámci svých činností při výkonu agend a musí mít přehled, v jakých agendách vede jaká data a jaký je jejich význam. Nástrojem, který slouží pro evidenci dat je datový model úřadu, obsahující koncepty jednotlivých datových modelů pro různé agendy. Jeho vytvořením přispívá úřad k naplnění architektonických principů, mezi které patří např. připravenost na změny, propojování ISVS nebo interabilita jako standard. Veškerá agendová data jsou obsažena v Registru práv a povinností, který poskytuje informace o druhu dat ve veřejné správě, zda-li jsou veřejná či neveřejná, jak je lze získat, používaných číselnících apod.

Zásadními architektonickými principy pro sdílení a využívání sdílení dat jsou:

- otevřenost a transparentnost,

[71] Ministerstvo financí ČR [online]. Copyright © [cit. 2023-13-03]. Dostupné z: https://www.mfcr.cz/assets/cs/media/2022-11-08_MP-CHJ-24-Digitalizace-uradu.pdf

- zásada „pouze jednou“,

- sdílené služby veřejné správy,

- jeden stát.

Sdílené bezpečné referenční rozhraní ISVS, tzv. Referenční rozhraní VS umožňuje ke stejným datům současně přistupovat více subjektům ve stejném okamžiku. Jedná se o data ze základních registrů, jež tvoří nezbytný nástroj pro výkon většiny agend používaných ve veřejné správě v ČR. Získání údajů pro výkon agend umožňuje jednotlivým úřadům referenční rozhraní s Veřejným datovým fondem (VDF) a Propojeným datovým fondem (PPDF). Informační systémy úřadů si tak mohou vyměňovat jednotlivé údaje se zaručenou garancí. Neveřejná data získávají v PPDF, veřejná ve VDF. Tyto údaje mohou rovněž získat i osoby nebo subjekty s oprávněním k jejich využití dle právního předpisu. Jedná se například o zdravotní pojišťovny. Do budoucna se plánuje zavedení samostatného zákona o správě dat ve veřejném sektoru, který by umožnil přístup k neveřejným údajům přes tzv. řízený přístup komukoli, kdo splní stanovené podmínky, především prokáže svoji identitu. Maximum údajů by mělo být zveřejněno formou otevřených dat, která by mohla využívat veřejnost a komerční subjekty za účelem různých statistických výzkumů či šetření. V současné době jsou otevřená data k dispozici v Národním katalogu otevřených dat (NKOD).

IK České republiky vytyčila ve sféře strukturovaných dat informačních systémů a jejich sdílení např. tyto cíle:

- Zlepšení národního katalogu otevřených dat,

- Zkvalitnění, validace a aktualizace obsahu Registru práv a povinností,

- Vytvoření základních služeb,

- Podpora sdílení údajů agendových systémů pro výkon agendy státní správy v přenesené působnosti,

- Propojený datový fond,

- Veřejný datový fond,

- GeoInformace.

Předpokladem k úspěšnému sdílení dat v databázích je možnost k jejich přístupu v otevřeném a strojově čitelném formátu a to prostřednictvím rozhraní (API), k němuž musí mít úřad k dispozici aktuální a ucelenou dokumentaci popisující jeho datovou strukturu a způsob přístupu k jednotlivým operacím. Druhou možností je export kompletního obsahu databází na vyžádání dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím. Veškerá data, která informační systém úřadu spravuje, tvoří datový fond úřadu. Zahrnuje např. údaje o různých subjektech (zaměstnancích, dodavatelích, klientech) nebo o právních objektech (vlastní majetek úřadu, kulturní památky apod.). Tyto údaje úřady využívají při výkonu svých agend, kterými jsou např. agenda ochrany veřejného zdraví, agenda občanských průkazů a další) a musí být zapsány v RPP[72].

6.4 e-Goverment

Fungování systému správy věcí veřejných ovlivňuje nový způsob komunikace uvnitř systému úřadů v rámci státu a nový způsob poskytování veřejných služeb. OVM byly nuceny reagovat na flexibilitu změn v informačních a komunikačních technologiích a začít je využívat v rámci vládnutí pro zajištění výměny informací s občany, soukromými subjekty a jinými veřejnými orgány s cílem poskytování dostupných, rychlých a kvalitních služeb a zvyšování efektivity vnitřního fungování[73].

Otázka pojmu e-Government je poměrně složitá. Existuje mnoho odborných odkazů na definici, důležité je však vybrat tu, která nejlépe vyjadřuje podstatu. V dnešní době, kdy se anglické výrazy používají i v jiných jazycích, dochází k tomu, že se některé pojmy vůbec nepřekládají. e-Government tak vznikl spojením dvou anglických výrazů „electronic“ a „government“, což můžeme přeložit jako elektronická vláda. Mates se Smejkalem tento pojem definují jako *„různé úkoly, které se zabývají elektronizací výkonu činnosti veřejné správy nebo v širším pojetí spíše orgánů veřejné moci vůbec“*[74], David Špaček přibližuje tento pojem jako *„zapojování ICT do činnosti veřejné správy“*[75] a Ministerstvo vnitra uvádí, že *„samotný e-Government zahrnuje nejen samotné informační*

[72] Ministerstvo financí ČR [online]. Copyright © [cit. 2023-18-03]. Dostupné z: https://www.mfcr.cz/assets/cs/media/2022-11-08_MP-CHJ-24-Digitalizace-uradu.pdf

[73] STEJSKAL, J., KUVÍKOVÁ, H., MIKUŠOVÁ, B., MERIČKOVÁ, B., LINHARTOVÁ, V. *Teorie a praxe veřejných služeb*. Praha: Wolters Kluwer ČR, 2017. [cit. 2023-18-03], s. 129.

[74] MATES, P., SMEJKAL V. *E-government v českém právu*. Praha: Linde, 2006, [cit. 2023-18-03], s. 9.

[75] ŠPAČEK, D. *EGovernment: cíle, trendy a přístupy k jeho hodnocení*. V Praze: C.H. Beck, 2012. Beckova edice ekonomie, [cit. 2023-18-03], s. 1.

technologie, ale také optimalizaci a zjednodušování služeb veřejné správy vázané na legislativní prostředí"[76].

Vrátíme-li se k citaci Matese, eGovernment charakterizuje jako *„fenomén, který je označován poněkud technicistní, dnes však již všeobecně používanou zkratkou e-government, je produktem moderní doby, stejně tak jako jejím výrazem. Zahrnuje rozsáhlou škálu otázek od přístupu adresátů veřejné správy k informacím, přes elektronickou komunikaci s úřady, po vytváření potřebných organizačních a technických infrastruktur v rámci veřejné správy, jejichž společným jmenovatelem je zavádění a využívání elektronických informačních a komunikačních technologií"*[77].

Finanční prostředky získané ze strukturálních fondů EU napomohly k budování jednotlivých prvků e-Govermentu v souladu se strategií Efektivní veřejná správa a přátelské veřejné služby. Prvním z nich byl Czech Point, sdružující síť kontaktních míst veřejné správy, dalším byl systém datových schránek a rovněž došlo ke vzniku základních registrů. Aby mohly tyto složité systémy fungovat, bylo nutné zřídit i bezpečnou infrastrukturu. Nezbytným krokem k vyřízení veškerých agend z domova bez nutnosti občanů navštívit úřad bylo zřízení internetového připojení a zavedení elektronických formulářů, což umožnila elektronická identita. Není již nutné obíhat úřady a vyplňovat papírové formuláře, nýbrž elektronické podání učinit kdykoliv, zdarma a online[78].

ISVS netvoří uzavřený celek konkrétních IS, nýbrž lze předpokládat, že se s rozvojem dalších agend svěřených veřejné správě bude jejich počet měnit, v některých případech bude tento počet narůstat, ale může i klesat, např. z důvodu jejich transformování do jiných systémů. Jedním z ISVS je tzv. Portál veřejné správy, který poskytuje fyzickým a právnickým osobám dálkový přístup ke všem službám a informacím v oblasti VS, zpřístupňuje její záznamy, zvyšuje její autoritu a efektivnost a umožňuje státní správě vystupovat jako integrální organizace[79].

[76] MINISTERSTVO VNITRA. *Agenda odboru hlavního architekta eGovernmentu. Ministerstvo vnitra* [online]. [cit. 2023-18-03]. Dostupné na https://www.mvcr.cz/clanek/agenda-odboru-hlavniho-architekta-egovernmentu-agenda-odboru-hlavniho76architekta-egovernmentu.aspx

[77] MATES, P. *E-government v české veřejné správě*. Praha: Právní rozhledy, 2005, č. 8, [cit. 2023-18-03], s. 283–286.

[78] Co je eGovernment? - Ministerstvo vnitra České republiky. *Úvodní strana - Ministerstvo vnitra České republiky* [online]. Copyright © 2023 Ministerstvo vnitra České republiky, všechna práva vyhrazena [cit. 2023-18-03]. Dostupné z: https://www.mvcr.cz/clanek/co-je-egovernment.aspx

[79] MATES, P. E-government v české veřejné správě. Praha: Právní rozhledy, 2005, č. 8. ISSN: 1210-6410, str. 283-286.

ZoISVS kromě práv a povinností spojených se správou a provozem ISVS vymezuje i systémy, které nelze do ISVS zařadit z důvodu jejich nakládání s utajovanými informacemi. Jedná se o systémy zpravodajských služeb, NBÚ a NÚKIB. Na tyto systémy se právní rámec ZoISVS nevztahuje, jelikož by mohlo dojít k ohrožení bezpečnosti utajovaných informací, které jsou chráněny zvláštními předpisy vč. podmínek přístupu k těmto informacím[80].

6.4.1 Czech POINT

Czech POINT (Český podací ověřovací informační národní terminál) lze charakterizovat jako kontaktní místa veřejné správy, kterými jsou obecní, městské úřady, úřady městských obvodů, krajské úřady, notáři, velvyslanectví (v zahraničí). Rovněž jimi mohou být Hospodářská komora, Česká pošta a banky, kterým byla Ministerstvem vnitra udělena autorizace. Kontaktní místa jsou opatřena modrým logem Czech POINT[81].

Na těchto místech jsou zpracovávány požadavky klientů, většinou tzv. „na počkání“, v některých případech jsou zákonné lhůty delší. Výstupy ze zapsaných údajů vedených ve veřejných evidencích jsou převážně v listinné podobě, rovněž tak mohou být příslušným adresátům doručeny v podobě elektronické[82].

Czech POINT poskytuje veřejnosti tyto služby:

- založení a správu datové schránky,

- výpisy z ISVS,

- výpisy ze základních registrů,

- autorizovanou konverzi dokumentů v papírové podobě do dokumentu, který je obsažen v datovém souboru či datové zprávě a naopak[83].

---

[80] 412/2005 Sb. Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti. *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. Copyright © AION CS, s.r.o. 2010 [cit. 2023-18-03]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412?text=412%2F2005

[81] Služby pro veřejnost – Czech POINT. [online]. Copyright © 2023 Ministerstvo vnitra České republiky, všechna práva vyhrazena [cit. 2023-18-03]. Dostupné z: https://www.czechpoint.cz/public/verejnost/sluzby-pro-verejnost/

[82] FELIX, O., KAUCKÝ, J., KOLÁŘ, J., et al. *Jak se (z)rodil eGON: reforma a elektronizace veřejné správy*. Praha: CEVRO Institut, 2015, s. 24-26.

[83] Služby Czech POINT - Ministerstvo vnitra České republiky. *Úvodní strana - Ministerstvo vnitra České republiky* [online]. Copyright © 2023 Ministerstvo vnitra České republiky, všechna práva vyhrazena [cit. 2023-18-03]. Dostupné z: https://www.mvcr.cz/clanek/sluzby-czech-point.aspx

O veřejné informace z Czech POINTU může zažádat kdokoli, o konkrétní osobě však může získat data pouze tato osoba nebo jím pověřený zmocněnec na základě předložení ověřené plné moci. K vyřízení žádosti je třeba předložit platný doklad totožnosti, příp. ověřenou plnou moc. Výši poplatků stanovuje Sazebník správních poplatků[84].

6.4.2 Datové schránky

Povinnost zřídit elektronické podatelny byla OVM uložena již v roce 2001. Jejich princip spočíval na e-mailové komunikaci. Správní řád a další předpisy se však se způsobem takovéto komunikace zcela neslučovaly, neboť OVM neměl k dispozici reakci na doručení či nedoručení zprávy. Proto bylo nutno vytvořit jiný komunikační nástroj, který by z potřeb doručování orgánů veřejné moci vycházel. 1. 7. 2009 tak došlo ke zřízení významného nástroje českého e-Governmentu, kterým se staly datové schránky. Pod pojmem datová schránka je rozuměno elektronické úložiště, které slouží k doručování orgány veřejné moci, k úkonům vůči jiným OVM, k dodávání dokumentů právnických osob, podnikajících fyzických osob i samotných fyzických osob. Komunikaci s OVM hradí stát prostřednictvím Ministerstva vnitra ze svého rozpočtu, mezi soukromoprávními osobami je komerční služba poskytována Českou poštou[85].

V současné době se povinnost mít zřízenu datovou schránku nevztahuje pouze na fyzické osoby. K OVM, právnickým osobám zapsaným v obchodním rejstříku a právnickým osobám zřízeným zákonem, kterým byla uložena povinnost mít zřízenu DS již od počátku, byla DS zřízena i všem daňovým poradcům, insolventním správcům, advokátům a statutárním auditorům. Od 1. ledna 2023 stát tuto povinnost přenesl i na všechny právnické osoby, které ji dosud neměly (nadace, spolky, obecně prospěšné společnosti), na živnostníky a OSVČ. Elektronické dokumenty posílané prostřednictvím DS nejen usnadní a zrychlí tok informací, ale rovněž ušetří náklady, které byly vynakládány na listinnou komunikaci, a především slouží jako nástroj pro zpětné prokázání doručení dokumentu. Právní platnost těchto dokumentů je stejná jako je tomu u klasických dokumentů a jejich odeslání je na rozdíl od doporučených dopisů zdarma[86].

[84] Portál služeb - Moravskoslezský kraj - Krajský úřad. *Portál služeb - Moravskoslezský kraj - Krajský úřad* [online]. [cit. 2023-18-03]. Dostupné z: https://sluzby.msk.cz/sluzba/76-czech-point

[85] Deník veřejné správy - Deset let datových schránek. Deník veřejné správy [online]. Copyright © 2023 [cit. 2023-18-03]. Dostupné z: https://www.dvs.cz/clanek.asp?id=6783960

[86] Datová schránka je povinná nejen pro OSVČ. Kdo ji musí mít? | e15.cz. *e15.cz - Byznys, politika, ekonomika, finance, události* [online]. Copyright © 2001 [cit. 2023-18-03]. Dostupné

6.4.3 Základní registry

Vzrůstající počet informačních systémů naplnil cíl ZoISVS, kterým se stala bezpečná výměna informací a zajištění kvalitních dat. Z důvodu nejednotnosti, roztříštěnosti a duplicitnosti dat v databázích veřejné správy bylo nutné data sjednotit a zavést spolehlivý systém, který by umožnil k těmto údajům centrální přístup[87].

Dnem 1. července 2010 byl přijat Zákon č. 111/2009 Sb. o základních registrech, jehož cílem bylo výše uvedené problémy vyřešit. Vznikem registrů již nebylo nutné hlásit každou změnu údajů jednotlivým úřadům zvlášť. Zánikem tištěných formulářů tak odpadla byrokratická zátěž nejen na samotnou veřejnou správu, ale i na jednotlivého občana[88].

Obsahem těchto informačních systémů jsou referenční údaje, které jsou nejčastěji využívány při výkonu veřejné správy. Tato data slouží jako jedinečný datový zdroj pro OVM, jsou vždy aktuální a právně závazná. OVM tak nemusí získávat údaje z dalších zdrojů, ale pouze ze základních registrů, z nichž jsou propisována do určených agendových systémů, tzn. informačních systémů, které jsou zřizovány pro výkon konkrétní agendy u konkrétního OVM. Údaje z registrů je OVM povinen využívat v souladu s právními předpisy, aniž by ověřoval jejich správnost. Výjimku tvoří pouze údaje, které v ZR chybí, jsou označeny za nesprávné, případně jedná-li se o utajované informace podle zákona o utajovaných informacích. Za správnost referenčních údajů zodpovídají editoři, kterými jsou u občanů ČR Ministerstvo vnitra a u cizinců Policie ČR. Editorem provozních údajů je Správa základních registrů prostřednictví ISZS (informačního systému základních registrů).

Základní registry tvoří čtyři informační systémy:

a) základní registr obyvatel (dále jen „registr obyvatel“),

z: https://www.e15.cz/finexpert/vydelavame/datova-schranka-je-od-roku-2023-povinnost-nejen-pro-osvc-komu-a-proc-ji-stat-zrizuje-1394841

[87] FELIX, O., KAUCKÝ, J., KOLÁŘ, J., et al. *Jak se (z)rodil eGON: reforma a elektronizace veřejné správy*. Praha: CEVRO Institut, 2015, [cit. 2023-18-03], s. 137.

[88] 111/2009 Sb. Zákon o základních registrech. Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění [online]. Copyright © AION CS, s.r.o. 2010 [cit. 2023-18-03]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-111

b) základní registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci (dále jen „registr osob“),

c) základní registr územní identifikace, adres a nemovitostí (dále jen „registr územní identifikace“),

d) základní registr agend, orgánů veřejné moci, soukromoprávních uživatelů údajů a některých práv a povinností (dále jen „registr práv a povinností“).

Komunikace mezi základními registry probíhá pomocí vnitřního rozhraní[89]. Pro názornost popíši alespoň 2 ze základních registrů.

Registr obyvatel

Správou tohoto registru bylo pověřeno Ministerstvo vnitra. Údaje v něm obsažené jsou editovány prostřednictvím několika agendových systémů. Jedná se o Agendový informační systém evidence obyvatel (AISEO), Agendový informační systém cizinců (AISC), Agendový informační systém evidence občanských průkazů (AISEOP), Agendový informační systém evidence cestovních dokladů (AISECD) a Agendový informační systém datových schránek.

Registr vede údaje o všech fyzických osobách s konkrétním vztahem k ČR, kterými jsou:

- státních občané ČR,

- cizinci, pobývající na území ČR v rámci trvalého pobytu, příp. na základě dlouhodobého víza nebo povolení k dlouhodobému pobytu,

- občané a jejich rodinní příslušníci z členských států EU, států vázaných mezinárodní smlouvou uzavřenou s Evropským společenstvím či smlouvou o Evropském hospodářském prostoru, kteří v ČR pobývají v rámci trvalého nebo přechodného pobytu delšího než 3 měsíce,

89 Základní registry [Architektura eGovernmentu ČR]. Uvítání a obsah webu [Architektura eGovernmentu ČR] [online]. [cit. 2023-18-03]. Dostupné z: https://archi.gov.cz/nap:zakladni_registry

- cizinci, jimž byla na našem území udělena mezinárodní ochrana formou azylu nebo doplňkové ochrany,

- další fyzické osoby, u kterých jiný právní předpis vyžaduje AIFO a určuje, že budou vedeny v ROB.

Referenčními údaji u subjektů vedených v ROB jsou informace o jménu a příjmení, adrese místa pobytu, příp. adrese pro doručování písemností, o datu a místu narození, příp. i úmrtí, o státních občanstvích (pokud jich je více), druhu a čísle identifikačních dokladů vč. data ukončení jejich platnosti, typu a identifikátoru datové schránky a dat potřebných pro elektronickou identifikaci a autentizaci[90].

Registr územní identifikace, adres a nemovitostí (RÚIAN)

Smyslem tohoto registru je zprostředkování údajů o územně evidenčních jednotkách, územních prvcích a jejich vzájemných vazbách, přičemž jednotlivé prvky je možno dohledat na digitálních mapách veřejné správy a na mapách státního mapového díla. Data z tohoto registru jsou veřejně přístupná přes volně dostupnou internetovou aplikaci přes veřejný dálkový přístup v RÚIAN. Systém nevede žádné osobní údaje, pouze je zprostředkovatelem údajů z agendového systému katastru nemovitostí. Správcem registru je Český úřad zeměměřický a katastrální, editorem může být dle povahy údajů i příslušný stavební úřad, katastrální úřad nebo příslušná obec. Jako jediný registr vede i nereferenční údaje, např. technickoekonomické atributy stavebních objektů (připojení na kanalizaci, vodu, zdroj vytápění, počet podlaží)[91].

[90] REGISTR OBYVATEL. *Szrcr.cz* [online]. [cit. 2023-18-03]. Dostupné z: www.szrcr.cz/cs/registr-obyvatel

[91] REGISTR ÚZEMNÍ IDENTIFIKACE, ADRES A NEMOVITOSTÍ. *Szrcr.cz* [online]. [cit. 2023-18-03]. Dostupné z: www.szrcr.cz/cs/registr-uzemni-identifikace-adres-a-nemovitosti

7 Zabezpečení ISVS

Současná platná legislativa ukládá úřadům povinnost vést dokumenty, které se vztahují k používání, řízení a bezpečnosti informačních systémů veřejné správy. Především je nutno zmínit:

- zákon č. 365/2000 Sb, o ISVS, ve znění pozdějších předpisů,

- zákon č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů,

- zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů,

- vyhlášku č. 529/206 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality ISVS,

- vyhlášku č. 53/2007 Sb., o technických a funkčních náležitostech uskutečňování vazeb mezi ISVS prostřednictvím referenčního rozhraní[92].

Významný informační systém je informační systém, který spravuje OVM a u něhož narušení bezpečnosti informací může významně ohrozit nebo i omezit výkon působnosti orgánu veřejné moci. Zároveň tento IS nesmí být informačním systémem základní služby ani kritickou informační infrastrukturou. Zákon o kybernetické bezpečnosti nerozděluje VIS na komunikační a na informační systém, neboť pojem „informační systém“ zahrnuje vždy i jeho komunikační složku[93].

Orgány veřejné moci využívají VIS k zajišťování:

a) elektronické pošty, pokud je používána v rámci výkonu veřejné moci,

b) výkonu kontrolní nebo inspekční činnosti anebo státního dozoru,

c) výkonu veřejné moci, podílející se na přípravě na krizové situace a jejich řešení,

[92] Co je a co není ISVS [Architektura eGovernmentu ČR]. *Uvítání a obsah webu* [Architektura eGovernmentu ČR] [online]. [cit. 2023-18-03]. Dostupné z: https://archi.gov.cz/znalostni_baze:co_je_neni_isvs

[93] Národní úřad pro kybernetickou a informační bezpečnost - Podpůrné materiály. Národní úřad pro kybernetickou a informační bezpečnost - *Úvodní stránka* [online]. [cit. 2023-28-03]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/

d) výkonu spisové služby,

e) vedení úřední desky, která umožňuje dálkový přístup,

f) mezinárodní spolupráce,

g) zadávání veřejných zakázek,

přičemž úkony uvedené v bodech f) a g) nově od 1. ledna 2023.

Významným informačním systémem nemůže být dle § 2 písm. d) zákona o kybernetické bezpečnosti IS, jehož správcem není orgán veřejné moci[94].

Podle vyhlášky o ISVS sem patří informační systémy ministerstev a krajských úřadů.

Tab. 2 - Seznam vybraných IS[95]:

OVM, správce ISVS	**název ISVS**	**datum vzniku**
Ministerstvo práce a sociálních věcí	IS pro pojistné a nepojistné dávky	23.01.2023
Ministerstvo práce a sociálních věcí	Jednotný IS práce a sociálních věcí	07.06.2012
Ministerstvo průmyslu a obchodu	IS Registru živnostenského podnikání	12.01.2009
Městská část Praha 7	e-SPIS	20.03.2018
Ministerstvo vnitra	e-matrika	11.01.2023
Ministerstvo ŽP	ISPOP2	15.04.2020
Ministerstvo financí	Integrovaný IS Státní pokladny	23.11.2012

[94] Národní úřad pro kybernetickou a informační bezpečnost - Podpůrné materiály. *Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka* [online]. [cit. 2023-28-03]. Dostupné z: https://www.nukib.cz/cs/kyberneticka- bezpecnost/regulace-a-kontrola/podpurne-materialy/

[95] AIS RPP Působnostní. [online]. [cit. 2023-28-03]. Dostupné z: https://rpp-ais.egon.gov.cz/AISP/verejne/isvs/zobrazeni-isvs

Bezpečnost základních registrů

Mezi VIS patří i základní registry. Jedním z hlavních cílů ZR je mj. ochránit data v nich uložená proti zneužití. Nejdůležitější opatření spočívá ve striktním přístupu pouze oprávněných osob podle svých rolí a přidělených agend. Třetí osoby nemají k informacím o subjektech údajů přímý přístup, ale jsou jim zasílány prostřednictvím datových schránek. Zabezpečení dat v ZR spočívá v používání tzv. identifikátorů, kdy každá fyzická osoba má přidělen tzv. zdrojový identifikátor (ZIFO), z něhož jsou odvozeny další agendové identifikátory (AIFO) pro každou agendu, ve které je osoba uvedena. Toto opatření zajišťuje, že tatáž osoba má v každé agendě jiný identifikátor a je tak téměř nemožné neoprávněně sdílet údaje mezi agendami. Dalším, neméně důležitým opatřením je i nastavení rolí mezi jednotlivé úřady, kdy správcem registru je jeden úřad a provoz ISZR zajišťuje úřad jiný[96].

Svou roli hraje i Úřad pro ochranu osobních údajů, který má na starosti převodník identifikátorů fyzických osob, tzv. ORG převodník. Jeho činnost je v systému ZR klíčová. Generuje identifikátory FO pro jednotlivé agendy a je jedinou institucí, která dokáže přepočítat agendové identifikátory z jednoho registru pro druhý[97].

Zabezpečení Czech POINT

Systém Czech POINT je proti kybernetickým útokům chráněn na velmi vysoké úrovni. Šance na získání přihlašovacího hesla k tomuto systému nelegální cestou je prakticky nulová. V systému Czech POINT nezůstávají žádná data. Jeho prostřednictvím nelze listovat databázemi, pouze získat konkrétní výpis na základě konkrétních údajů. Zabezpečení systému je dle dostupných standardů. Hlavním cílem je ochrana osobních údajů osob, které tento systém prostřednictvím veřejné správy využívají. V současnosti se do registrů pro výpisy osobních údajů mohou přihlásit pouze úředníci VS na základě vydaných certifikátů[98].

---

[96] Základní registry veřejné správy | Přínosy a využití základních registrů | BusinessInfo.cz. *BusinessInfo.cz - Oficiální portál pro podnikání a export* [online]. Copyright © 1997 [cit. 2023-18-03]. Dostupné z: https://www.businessinfo.cz/navody/zakladni-registry-verejne-spravy-ppbi/4/

[97] ORG - PŘEVODNÍK. *Szrcr.cz* [online]. [cit. 2023-18-03]. Dostupné z: szrcr.cz/cs/?view=article&id=34:org-prevodnik&catid=2

[98] Novinky – 27. stránka – Czech POINT. [online]. Copyright © 2023 Ministerstvo vnitra České republiky, všechna práva vyhrazena [cit. 2023-18-03]. Dostupné z: https://www.czechpoint.cz/public/novinky/page/27/

Zabezpečení datových schránek

Datové schránky, které slouží jako digitální úložiště, přes které se předávají datové zprávy od nebo k orgánům veřejné moci, jsou nejkritičtějším z pohledu rozhraní uživatel – datová schránka. Lze předpokládat, že útočník může k systému provozovatele či správce (Česká pošta, Ministerstvo vnitra ČR) přijít zvenčí přes webovou službu. Hrozby zahrnují útoky na operační systémy, prohlížeče a další aplikace. Ochrana před kyberútoky spočívá nejen v zabezpečení každé jednotlivé stanice antivirem v kombinaci s firewallem, ale především v autentizaci. Tento problém je u DS řešen náhodně vygenerovaným uživatelským jménem, přísnými požadavky na přístupové heslo a přihlašováním komerčním certifikátem. Heslo by mělo být každé 3 měsíce obměňováno. Certifikát pro zaměstnance veřejné správy je vydáván akreditovanými certifikačními autoritami. Klíč k certifikátu musí být vygenerován na bezpečném elektronickém prostředku, kterými jsou čipové karty nebo USB tokeny, vyhovující podmínkám ve vyhlášce, která rovněž specifikuje přípustné šifrovací algoritmy. Autentizační token zvyšuje bezpečnost autentizace. Po registraci certifikátu v ISDS zůstávají certifikát a RSA klíč pouze v tokenu, odkud nejdou exportovat, a proto se do DS může dostat pouze ten, kdo vlastní token a zná k němu PIN. Certifikát v bezpečném úložišti je cestou, jak zvýšit bezpečnost autentizace do ISDS a chránit tak osobní data před útoky z vnějšku i zevnitř[99].

Shrnu-li způsoby, kterými se orgány veřejné správy mohou bránit před kyberkriminalitou, jsou to především:

- Aktualizovaný operační systém a bezpečnostní software (nejlépe automatické aktualizace). Internetový prohlížeč, který je mj. i hlavní branou k přístupu do DS nesmí mít žádné tzv. bezpečnostní díry, které by se mohly stát snadným terčem útoku.

- Hardwarový firewall používat na počítačové síti a softwarový na lokálním PC.

- Používat komplikovaná hesla, která obsahují malá i velká písmena, číslice a speciální znaky. Tato hesla často obměňovat, nenechávat je volně přístupná.

[99] Jak zajistit bezpečnost datových schránek? - Computerworld. *Computerworld* [online]. Copyright © 2020 [cit. 2023-18-03]. Dostupné z: https://www.computerworld.cz/clanky/jak-zajistit-bezpecnost-datovych-schranek/

- Nesdělovat nikomu přístupové údaje (jméno, heslo) do jakéhokoliv systému.

- Důvěryhodnost komunikace zajišťovat kontrolou držitelů, vydavatelů a platností bezpečnostních certifikátů.

- Používat pouze legální software, nestahovat software z neznámých zdrojů.

- Používat antivirové programy pro monitorování práce v PC, skenování obsahu paměťových médií, e-mailů apod.

- Neotvírat přílohy v e-mailových zprávách z neznámých zdrojů.

- Používat IDS systém pro odhalení průniku podezřelých aktivit vedoucích k narušení bezpečnosti operačního systému nebo PC sítě[100].

Předpokladem pro posílení bezpečnosti ISVS je povinnost orgánů veřejné správy implementovat a důsledně dodržovat normy a standardy vyplývající z výše citovaných zákonů a jejich následná kontrola. Zjištěná rizika týkající se ohrožení nebo napadení ISVS neprodleně hlásit NÚKIB který je na svém portále zveřejní. Většinu detekovaných incidentů dokážou eliminovat automatizované systémy jako firewally a antiviry, při vytvoření bezpečnostního incidentu je nutné učinit další opatření. Mohou se použít další detekční metody jako je mimořádné testování antiviry nebo podrobnější analýza. Magistrát hl. města Prahy a krajské úřady využívají při ochraně sítí dohledu specialistů na kyberbezpečnost[101].

Nedostatek spatřuji v tom, že IT oddělení městských úřadů řídí většinou správci sítí, kteří řeší běžnou agendu administrace sítí, ale ne bezpečnostní stránku provozu ICT infrastruktur. K úniku dat může dojít i roztříštěností městských sítí, kdy externí dodavatel spravuje pouze jejich část, chybí jednotnost a hlavní autorita, která ICT v obecní infrastruktuře hlídá a centrálně řídí. Bohužel největší hrozbou pro IS je stále lidský faktor, který může, většinou nevědomě, jeho bezpečnost poškodit. Pracovníci VS by se proto měli neustále v kybernetické bezpečnosti vzdělávat a být seznámeni s bezpečnostními

[100] Jak se chránit před kyberšikanou a jak se bránit kyberútočníkům - E-Bezpečí. *Projekt E-bezpečí - E-Bezpečí* [online]. [cit. 2023-18-03]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/kyberikana/102-27

[101] Deník veřejné správy - Kyberútoky se nevyhýbají ani městům a jejich úřadům. *Deník veřejné správy* [online]. Copyright © 2023 [cit. 2023-18-03]. Dostupné z: http://denik.obce.cz/clanek.asp?id=6816808

pravidly, která musí dodržovat. NÚKIB podpořil naplňování Národní strategie KB ČR na období let 2021-25 spuštěním on-line kurzu základů kybernetické bezpečnosti „Dávej kyber“, určeného především zaměstnancům státní správy a samosprávy. Kurz se skládá z osmi okruhů a po úspěšném absolvování závěrečného testu získá každý absolvent certifikát o jeho splnění[102].

Dalším z on-line kurzů, tentokrát určený manažerům KB, je kurz „Šéfuj kyber!“, který především seznamuje s obsahem Vyhlášky o kybernetické bezpečnosti. Je doplněn o komentáře, příklady a doporučení. Jeho obsahem je i praktická část, tzv. workshop, kde si účastníci kurzu mohou ověřit své znalosti v praxi. Rovněž tento kurz je zakončen testem a jeho úspěšnost dokladována certifikátem[103].

Dlouhodobým problémem je nedostatek finančních prostředků vynakládaných na zajišťování kybernetické bezpečnosti. Pro implementaci a rozvoj bezpečnostních systémů podporujících výkon státní správy je nutné, kromě finančních prostředků od státu, využít i dotačních prostředků. Integrovaný regionální operační program (IROP), který spravuje Ministerstvo pro místní rozvoj (MMR) by mělo na rozvoj českého eGovernmentu a kyberbezpečnosti rozdělit téměř 12,5 miliardy korun, jež by měly napomoci k rozšíření a urychlení elektronizace VS[104].

Orgány veřejné správy musí v souladu s novelou zákona o ISVS zajistit shodu smluvních vztahů v oblasti služeb cloud computingu. Požadavky vyplývající z těchto smluv musí obsahovat tyto nezbytné náležitosti:

- určení povinností poskytovatele služeb respektovat bezpečnostní politiku odběratele,

- podmínky, za kterých může být smluvní vztah z pohledu bezpečnosti ukončen,

---

[102] Národní úřad pro kybernetickou a informační bezpečnost - NÚKIB spouští aktualizovanou verzi on-line kurzu „Dávej kyber!“. *Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka* [online]. [cit. 2023-18-03]. Dostupné z: https://nukib.cz/cs/infoservis/aktuality/1841-nukib-spousti-aktualizovanou-verzi-on-line-kurzu-davej-kyber/

[103] Kurz pro manažery kybernetické bezpečnosti. [online]. Copyright © 2023 PragoData Consulting, s.r.o. [cit. 2023-18-03]. Dostupné z: https://osveta.nukib.cz/sefujkb

[104] MMR pro velký zájem po necelém týdnu uzavřelo jednu výzvu na kyberbezpečnost | ČeskéNoviny.cz. České noviny | *ČeskéNoviny.cz* [online]. Copyright © Copyright [cit. 2023-18-03]. Dostupné z: https://www.ceskenoviny.cz/zpravy/mmr-pro-velky-zajem-po-necelem-tydnu-uzavrelo-jednu-vyzvu-na-kyberbezpecnost/2246568

- určení úrovně poskytnutých služeb (SLA),

- způsob schvalování subdodavatelů služby cloud computingu,

- stanovení vlastníka uchovávaných dat,

- kontrolu kontinuity činností, které s cloud computingem souvisí,

- ujednání o důvěrnosti smluvního vztahu,

- statut zákaznického auditu,

- zakotvení úrovně, kterým budou data v cloud computingu chráněna z pohledu jejich dostupnosti, integrity a důvěrnosti,

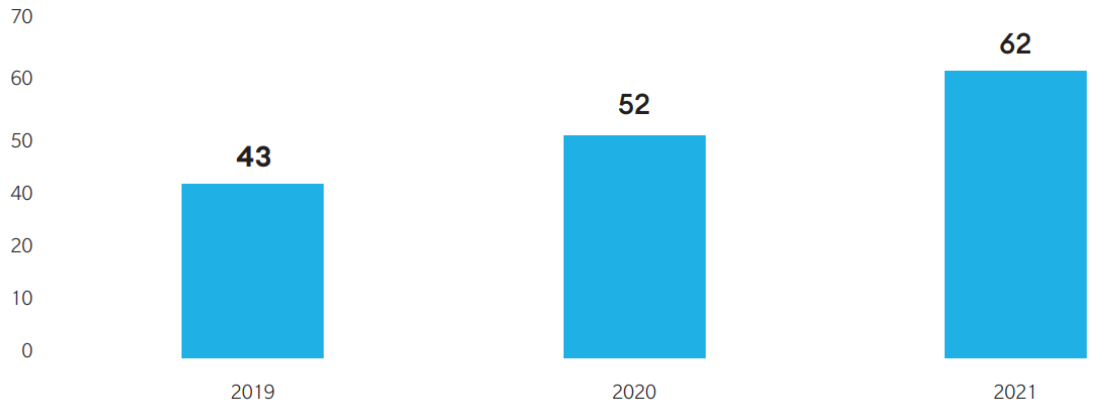
- nutnost poskytovatele služeb informovat odběratele o kybernetických bezpečnostních incidentech vyplývajících s plněním smlouvy[105].

NÚKIB vydává každoročně zprávu o stavu kybernetické bezpečnosti ČR. Nahlédneme-li do přehledu z roku 2021 (zpráva z roku 2022 ještě není k dispozici), zjistíme že v tomto roce NÚKIB evidoval 372 významných informačních systémů, 162 správců a provozovatelů VIS a 60 subjektů kritické informační infrastruktury. Mezi nejčastější typy kybernetických útoků patřily phishing, skenování sítě a podvodné maily. Veřejný sektor patřil v roce 2021 k nejvíce zasaženým, došlo v něm téměř ke 40 % všech kybernetických bezpečnostních incidentů[106].

[105] SEDLÁK, P., KONEČNÝ, M. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2. s. 313.

[106] Národní úřad pro kybernetickou a informační bezpečnost - Zveřejnili jsme Zprávu o stavu kybernetické bezpečnosti za rok 2021 . *Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka* [online]. [cit. 2023-18-03]. Dostupné z: https://nukib.cz/cs/infoservis/aktuality/1852-zverejnili-jsme-zpravu-o-stavu-kyberneticke-bezpecnosti-za-rok-2021/

Tab. 3 - Kybernetické incidenty ve veřejném sektoru v letech 2019 – 2021[107]



[107] Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka [online]. Copyright © [cit. 2023-25-03]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kybernetick_bezpenosti_2021.pdf

Závěr

Vzhledem k tomu, že dochází k neustálému nárůstu informačních technologií, mění se a vyvíjí i metody kybernetických útoků na tuto sféru. Jejich cíle však zůstávají stále tytéž. Ve veřejné sféře jsou to útoky na informační systémy obsahující citlivá data chráněná GDPR, útoky na finanční systémy a na zájmy národní bezpečnosti, tj. na krizovou infrastrukturu a státní instituce.

Většina lidí neznalých problému si kybernetickou bezpečnost představuje jako neustále se stupňující boj mezi bezpečnostními experty a hackery. Hrozby, které většinou přicházejí od technicky zdatných zločineckých útočníků však často vznikají kvůli nedostatečně zabezpečeným sítím, které se spoléhají na konvenční metody ochrany. Velkou měrou se však na kyberútoku podílí lidský faktor, kterým jsou nerozvážní zaměstnanci, jejichž práce se přesunula na home office, kde pracují s nezabezpečenými zařízeními. Čím více zařízení je do sítí propojeno, tím větší možnost se naskýtá útočníkům získat přístup k datům.

Naskýtá se otázka, jak ve veřejné správě kybernetický prostor zabezpečit. K tomu je zapotřebí zjistit, kdo a co je jeho součástí a jaké procesy jsou pro jeho chod zásadní. Orgánům státní správy v tom pomáhají sofistikované technické nástroje a systémy. Klíčem k bezpečným transakcím ve veřejné sféře je ověřování identity uživatelů pomocí autentizačních opatření a vícefaktorového ověřování. Každému uživateli musí být umožněn přístup jen do nezbytně využívané části systému. Pracovníkům ve veřejné sféře je tak např. z firemního počítače odepřen přístup do soukromého mailu. Důležitým se jeví osvěta pracovníků VS, kteří musí být v otázce kybernetické bezpečnosti proškoleni a musí si uvědomit, že otázka bezpečnosti není pouze záležitostí pracovníků IT, ale každého z nich. Kybernetická bezpečnost se z důvodu digitalizace informací stala součástí informační bezpečnosti. Důraz na vzdělávání a informovanost by měl vycházet z národních institucí, kterou je v České republice Národní úřad pro kybernetickou a informační bezpečnost. Oblast práva nabyla v tomto směru velmi významného postavení, neboť ukládá povinnosti provozovatelům IS a rizikových infrastruktur a nastavuje procesy, které v rámci subjektů i celého státu vedou k efektivnímu zvládání kybernetických incidentů.

Jedním z hlavních důvodů rozvoje ISVS se stala úspora veřejných prostředků, dostupnost a kvalita poskytovaných informací. Služby veřejné správy jsou poskytovány online, využití portálu veřejné správy a datové schránky je pro občany bezplatné. Žadatel o informace není vázán místní působností, na všech úrovních veřejné správy došlo ke sjednocení kontaktních míst. Pro efektivní využívání dat a zabezpečení ISVS, ve kterých jsou uložena, bylo nutno nejednotnou koncepci sjednotit. Nastavení pravidel pro jejich fungování byly definovány Zákonem č. 365/2005 Sb. o ISVS a Zákonem č.181/2014 o kybernetické bezpečnosti.

Cílem útočníků na ISVS bývá znevěrohodnění subjektů státu a destabilizace systému. V dnešní době globalizace, kdy dochází k propojení různých informačních systémů přes internetovou síť je nutné učinit veškerá možná opatření, která by kybernetická rizika snížila na minimum. Finanční prostředky územních samospráv jsou omezené, proto je nutné žádat o podporu u vyšších správních orgánů – krajů či státu. Neméně důležité je usilovat o možnost čerpání financí z nejrůznějších dotačních titulů, především z fondů Evropské unie. Budoucnost kybernetické bezpečnosti patří využívání umělé inteligence, kdy různé šifrovací algoritmy v síti indikují bezpečnostní hrozbu snáze než lidský faktor.

Ze závěru bakalářské práce vyplynulo, že zájem o kybernetickou bezpečnost stále narůstá, a to především vzhledem ke stále více se množícím a měnícím se druhům útoků, které bezpečnost v kyberprostoru narušují. Ochraně veřejných informačních systémů a systémů kritické infrastruktury musí být spolu s osvětou v budoucnu věnována klíčová pozornost.

Seznam použitých zdrojů

Literární zdroje

1. CLOUGH, J. *Principles of Cybercrime*. New York: Cambridge University Press, 2010, s. 504. ISBN 978-0-521-72812-6.
2. DONÁT, J. a TOMÍŠEK, J. *Právo v síti: průvodce právem na internetu*. Praha: C.H. Beck, 2016, s. 352. ISBN 978-80-7400-610-4.
3. FELIX, O., KAUCKÝ, J., KOLÁŘ, J. et al. *Jak se (z)rodil eGON: reforma a elektronizace veřejné správy*. Praha: CEVRO Institut, 2015, s. 313. ISBN 978-80-87125-28-1.
4. HRŮZA, Petr. *Kybernetická bezpečnost*. Brno: Univerzita obrany, 2012. 90 s. ISBN 978-80-7231-914-5.
5. JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti*, 2015, s. 240. ISBN 978-80-7251-436-6.
6. JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, s. 284. ISBN 978-80-247-1561-2.
7. KÁŇA, Pavel. *Základy veřejné správy: [vybrané kapitoly veřejné správy pro studium žáků středních škol a maturitní témata k ústní maturitní zkoušce z předmětu Veřejná správa]. 2., dopl., přeprac. vyd.* Ostrava: Montanex, 2007. Varia (Montanex). s. 12. ISBN 978-80-7225-244-2.
8. KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC., s. 522. ISBN 978-80-88168-15-7.
9. Lachow, I. 2009.: „Cyber Terrorism: Menace or Myth?“ In: Cyberpower and National Security (eds. Kramer). Washington: National Defense University Press, xxi, s. 664. ISBN-13 978-1597974233.
10. MATES, P. *E-government v české veřejné správě*. Praha: Právní rozhledy, 2005, č. 8, s.24. ISSN: 1210-6410.
11. MATES, P., SMEJKAL V. *E-government v českém právu*. Praha: Linde, 2006, s. 244. ISBN 80-7201-614-8.
12. MCGIURE, M. a DOWLING, S. *Cyber crime: A review of the evidence, Research Report 75, Chapter 1: Cyber-dependent crimes*. UK Home Office, 2013, s. 35. ISBN: 978-1-78246-245-3.
13. POLČÁK, R. *Internet a proměny práva*. Praha: Auditorium, 2012. Téma (Auditorium). s. 350. ISBN 978-80-87284-22-3.

14. POLČÁK, R. *Právní problémy kybernetické bezpečnosti*, 2016, s. 215. ISBN 978-80-210-8426-1.
15. POLČÁK, R. *Právo informačních technologií.* Praha: Wolters Kluwer, 2018, s. 656. ISBN 978-80-7598-045-8.
16. PRŮCHA, P. *Správní právo: obecná část. 7., dopl. a aktualiz. vyd., (V nakl. Doplněk 2.).* Brno: Masarykova univerzita, 2007. s. 48. ISBN 9788021042766.
17. SEDLÁK, P., KONEČNÝ, M. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021, s. 429. ISBN 978-80-7623-068-2.
18. SLÁDEČEK, V. *Obecné správní právo. 3., aktualiz. a upr. vyd*. Praha: Wolters Kluwer Česká republika, 2013. s. 500. ISBN 978-80-7478-002-8
19. STEJSKAL, J., KUVÍKOVÁ, H., MIKUŠOVÁ, B., MERIČKOVÁ, B., LINHARTOVÁ, V. *Teorie a praxe veřejných služeb*. Praha: Wolters Kluwer ČR, 2017, s. 280. ISBN 978-80-7552-726-4.
20. ŠPAČEK, D. *EGovernment: cíle, trendy a přístupy k jeho hodnocení*. V Praze: C.H. Beck, 2012. Beckova edice ekonomie, s. 288. ISBN 978-80-7400-261-8.

Elektronické zdroje

1. 111/2009 Sb. Zákon o základních registrech. Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění [online]. Copyright © AION CS, s.r.o. 2010 [cit. 2023-18-03]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-111
2. 181/2014 Sb. Zákon o kybernetické bezpečnosti. *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. Copyright © AION CS, s.r.o. 2010 [cit. 2023-28-01]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181
3. 181/2014 Sb. Zákon o kybernetické bezpečnosti. *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. Copyright © AION CS, s.r.o. 2010 [cit. 2023-13-03]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181
4. 289/2005 Sb. Zákon o Vojenském zpravodajství. *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. Copyright © AION CS, s.r.o. 2010 [cit. 2023-29-01]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-289
5. 412/2005 Sb. Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti. Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném

znění [online]. Copyright © AION CS, s.r.o. 2010 [cit. 2023-18-03]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412?text=412%2F2005

6. 82/2018 Sb. Vyhláška o kybernetické bezpečnosti. *Zákony pro lidi - Sbírka zákonů ČR v aktuálním konsolidovaném znění* [online]. Copyright © AION CS, s.r.o. 2010 [cit. 2023-29-01]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82?text=82%2F2018
7. AIS RPP Působnostní. [online]. [cit. 2023-28-03]. Dostupné z: https://rpp-ais.egon.gov.cz/AISP/verejne/isvs/zobrazeni-isvs
8. BRYAN, C. *Cyberterrorism, computer crime, and reality. Information Management & Computer Security* [online]. 2004, vol. 12, issue 2, s. 269, [cit. 2023-27-01]. Dostupné z: http://www.emeraldinsight.com/doi/abs/10.1108/09685220410530799
9. CERT/CSIRT týmy a jejich role - Root.cz. *Root.cz - informace nejen ze světa Linuxu* [online]. Copyright © 1997 [cit. 2023-29-01]. Dostupné z: https://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/
10. CERT-EU – computer emergency response team | European *Union. Redirecting to /select-language?destination=/node/1* [online]. [cit. 2023-31-01]. Dostupné z: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/cert-eu_en
11. Co je a co není ISVS [Architektura eGovernmentu ČR]. Uvítání a obsah webu [Architektura eGovernmentu ČR] [online]. [cit. 2023-18-03]. Dostupné z: https://archi.gov.cz/znalostni_baze:co_je_neni_isvs
12. Co je eGovernment? - Ministerstvo vnitra České republiky. *Úvodní strana - Ministerstvo vnitra České republiky* [online]. Copyright © 2023 Ministerstvo vnitra České republiky, všechna práva vyhrazena, [cit. 2023-18-03]. Dostupné z: https://www.mvcr.cz/clanek/co-je-egovernment.aspx
13. Co je kyberterorismus? - Správa.sítě.eu. *Správa sítě - slovník pojmů: správa sítě, zabezpečení sítě, outsourcing IT* [online]. Copyright © [cit. 2023-27-01]. Dostupné z: https://www.sprava-site.eu/kyberterorismus/
14. Co je Samospráva? *Definice pojmu*. Superia.cz [online]. [cit. 2023-12-03]. Dostupné z: https://cojeto.superia.cz/pravo/samosprava.php
15. Co je to kybernetická válka – Soubory. [online]. [cit. 2023-27-01]. Dostupné z: https://soubory.info/info/co-je-to-kyberneticka-valka/
16. CO JE NCKB. Govcert [online]. [cit. 2023-29-01]. Dostupné z: https://www.govcert.cz/cs/

17. Datová schránka je povinná nejen pro OSVČ. Kdo ji musí mít? | e15.cz. e15.cz - Byznys, politika, ekonomika, finance, události [online]. Copyright © 2001 [cit. 2023-18-03]. Dostupné z: https://www.e15.cz/finexpert/vydelavame/datova-schranka-je-od-roku-2023-povinnost-nejen-pro-osvc-komu-a-proc-ji-stat-zrizuje-1394841
18. Deník veřejné správy - Deset let datových schránek. *Deník veřejné správy* [online]. Copyright © 2023 [cit. 2023-18-03]. Dostupné z: https://www.dvs.cz/clanek.asp?id=6783960
19. Deník veřejné správy - Kyberútoky se nevyhýbají ani městům a jejich úřadům. Deník veřejné správy [online]. Copyright © 2023 [cit. 2023-18-03]. Dostupné z: http://denik.obce.cz/clanek.asp?id=6816808
20. Důvodová zpráva. *Návrh zákona o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)* [online]. Úřad vlády České republiky, 2014, s. 85. [cit. 2023-12-01]. Dostupné z: https://apps.odok.cz/attachmen/-/down/KORN9F6H6BCH
21. Důvodová zpráva. *Návrh zákona, kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, a některé další zákony* [online]. Úřad vlády České republiky, 2015, s. 36. [cit. 2023-26-02]. Dostupné z: https://apps.odok.cz/attachment/- /down/KORNAB7GCFCC
22. ESF:BPV_ZVFS Základy veřejných financí a veřejné správy. Informační systém [online]. [cit. 2023-12-03]. Dostupné z: https://is.muni.cz/el/econ/podzim2015/BPV_ZVFS/um/59151890/60414461/
23. Hrozby – KYBEZ. *KYBEZ – Platforma kybernetické bezpečnosti* [online]. Copyright © [cit. 2023-25-01]. Dostupné z: https://www.kybez.cz/hrozby/
24. INFORMAČNÍ BEZPEČNOST. *ŠKOLENÍ PROJEKTOVÉHO ŘÍZENÍ PRO FIRMY, VEŘEJNOU SPRÁVU A AKTIVNÍ STUDENTY* [online]. Copyright © [cit. 2023-25-01]. Dostupné z: https://www.acsa.cz/verejnost/sluzby/podle-temat/informacni-bezpecnost/
25. Informační systém [online]. Copyright © [cit. 2023-26-02]. Dostupné z: https://is.muni.cz/el/1456/jaro2017/MKV_VES2/um/68159517/VEREJNA.SPRAVA.OCHRANA.PUCEK.SPACEK.pdf
26. Informační technologie ve veřejné správě. Czso.cz [online]. 2020 [cit. 2023-12-03]. Dostupné z: https://www.czso.cz/csu/czso/verejna_sprava

27. Jak se chránit před kyberšikanou a jak se bránit kyberútočníkům - E-Bezpečí. *Projekt E-bezpečí - E-Bezpečí* [online]. [cit. 2023-18-03]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/kyberikana/102-27
28. Jak zajistit bezpečnost datových schránek? - Computerworld. *Computerworld* [online]. Copyright © 2020 [cit. 2023-18-03]. Dostupné z: https://www.computerworld.cz/clanky/jak-zajistit-bezpecnost-datovych-schranek/
29. Kurz pro manažery kybernetické bezpečnosti. [online]. Copyright © 2023 PragoData Consulting, s.r.o. [cit. 2023-18-03]. Dostupné z: https://osveta.nukib.cz/sefujkb
30. Kyberterorismus - Wikiwand. *Wikiwand – home* [online]. [cit. 2023-27-01]. Dostupné z: https://www.wikiwand.com/cs/Kyberterorismus
31. Ministerstvo financí ČR [online]. Copyright © [cit. 2023-13-03]. Dostupné z: https://www.mfcr.cz/assets/cs/media/2022-11-08_MP-CHJ-24-Digitalizace-uradu.pdf
32. MINISTERSTVO VNITRA. *Agenda odboru hlavního architekta eGovernmentu. Ministerstvo vnitra* [online]. [cit. 2023-18-03]. Dostupné na https://www.mvcr.cz/clanek/agenda-odboru-hlavniho-architekta-egovernmentu-agenda-odboru-hlavniho architekta-egovernmentu.aspx
33. MMR pro velký zájem po necelém týdnu uzavřelo jednu výzvu na kyberbezpečnost | ČeskéNoviny.cz. České noviny | ČeskéNoviny.cz [online]. Copyright © Copyright [cit. 2023-18-03]. Dostupné z: https://www.ceskenoviny.cz/zpravy/mmr-pro-velky-zajem-po-necelem-tydnu-uzavrelo-jednu-vyzvu-na-kyberbezpecnost/2246568
34. Národní úřad pro kybernetickou a informační bezpečnost - NÚKIB spouští aktualizovanou verzi on-line kurzu „Dávej kyber!“. *Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka* [online]. [cit. 2023-18-03]. Dostupné z: https://nukib.cz/cs/infoservis/aktuality/1841-nukib-spousti-aktualizovanou-verzi-on-line-kurzu-davej-kyber/
35. Národní úřad pro kybernetickou a informační bezpečnost - O NÚKIB. *Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka* [online]. [cit. 2023-29-01]. Dostupné z: https://www.nukib.cz/cs/o-nukib/
36. Národní úřad pro kybernetickou a informační bezpečnost - Podpůrné materiály. *Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka* [online]. [cit. 2023-28-

01]. Dostupné z: https://www.nukib.cz/cs/kyberneticka- bezpecnost/regulace-a-kontrola/podpurne-materialy/

37. Národní úřad pro kybernetickou a informační bezpečnost - Podpůrné materiály. *Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka* [online]. [cit. 2023-28-03]. Dostupné z: https://www.nukib.cz/cs/kyberneticka- bezpecnost/regulace-a-kontrola/podpurne-materialy/
38. Národní úřad pro kybernetickou a informační bezpečnost - Podpůrné materiály. Národní úřad pro kybernetickou a informační bezpečnost - *Úvodní stránka* [online]. [cit. 2023-28-03]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/
39. Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka [online]. Copyright © [cit. 2023-25-03]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kybernetick_bezpenosti_2021.pdf
40. Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka [online]. Copyright ©Rk [cit. 2023-28-03]. Dostupné z: https://www.nukib.cz/download/publikace/podpurne_materialy/Schema-VIS_nova_3.0.pdf
41. Národní úřad pro kybernetickou a informační bezpečnost - Zveřejnili jsme Zprávu o stavu kybernetické bezpečnosti za rok 2021 . *Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka* [online]. [cit. 2023-18-03]. Dostupné z: https://nukib.cz/cs/infoservis/aktuality/1852-zverejnili-jsme-zpravu-o-stavu-kyberneticke-bezpecnosti-za-rok-2021/
42. NATO's Little Noticed but Important New Aggressive Stance on Cyber Weapons – *Foreign Policy. Foreign Policy – the Global Magazine of News and Ideas* [online]. Copyright © 2023, Graham Digital Holding Company [cit. 2023-31-01]. Dostupné z: https://foreignpolicy.com/2017/12/07/natos-little-noticed-but-important-new-aggressive-stance-on-cyber-weapons/
43. NBÚ vybral provozovatele národního CERT (CSIRT.CZ), je jím CZ.NIC. *Úvodní stránka* [online]. [cit. 2023-30-01**]**. Dostupné z: https://www.nbu.cz/cs/aktualne/820-621-nbu-vybral-provozovatele-narodniho-cert-csirtcz-je-jim-cznic/

44. Několik poznámek k samosprávě a řízení vysokých | epravo.cz. *EPRAVO.CZ – Váš průvodce právem - Sbírka zákonů, judikatura, právo* [online]. Copyright © EPRAVO.CZ, a.s. 1999 [cit. 2023-12-03]. Dostupné z: https://www.epravo.cz/top/clanky/nekolik-poznamek-k-samosprave-a-rizeni-vysokych-skol-57865.html
45. Novinky – 27. stránka – Czech POINT. [online]. Copyright © 2023 Ministerstvo vnitra České republiky, všechna práva vyhrazena [cit. 2023-18-03]. Dostupné z: https://www.czechpoint.cz/public/novinky/page/27/
46. OPF:EVSNPEVS Ekonomika odvětví veřejného sektoru. *Informační systém* [online]. [cit. 2023-12-03]. Dostupné z: https://is.slu.cz/el/opf/leto2021/EVSNPEVS/um/9_informacni_systemy.pdf
47. ORG - PŘEVODNÍK. Szrcr.cz [online]. [cit. 2023-18-03]. Dostupné z: szrcr.cz/cs/?view=article&id=34:org-prevodnik&catid=2
48. Počítačová bezpečnost – Wikipedie. [online]. [cit. 2023-25-01]. Dostupné z: https://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_bezpe%C4%8Dnost
49. Politické zřízení a úřední funkce v Římě. *Antika.avonet.cz* [online]. [cit. 2023-12-03]. Dostupné z: http://antika.avonet.cz/article.php?ID=1493
50. Portál služeb - Moravskoslezský kraj - Krajský úřad. Portál služeb - Moravskoslezský kraj - Krajský úřad [online]. [cit. 2023-18-03]. Dostupné z: https://sluzby.msk.cz/sluzba/76-czech-point
51. Provozovatel informačního nebo komunikačního systému v3.2. Nukib.cz [online]. [cit. 2023-12-03]. Dostupné z: https://nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/
52. REGISTR OBYVATEL. Szrcr.cz [online]. [cit. 2023-18-03]. Dostupné z: www.szrcr.cz/cs/registr-obyvatel
53. REGISTR ÚZEMNÍ IDENTIFIKACE, ADRES A NEMOVITOSTÍ. Szrcr.cz [online]. [cit. 2023-18-03]. Dostupné z: www.szrcr.cz/cs/registr-uzemni-identifikace-adres-a-nemovitosti
54. Rozcestník kyberkriminality – Prevence kriminality. *Prevence kriminality – Prevence kriminality v České republice* [online]. Copyright © 2023 Prevence kriminality v České republice. Všechna práva vyhrazena. Portál [2023-25-01]. Dostupné z: https://prevencekriminality.cz/prevence-kriminality/kyberkriminalita/rozcestnik-kyberkriminality/

55. Samospráva - *Iuridictum*. [online]. [cit. 2023-12-03]. Dostupné z: https://iuridictum.pecina.cz/w/Samospr%C3%A1va
56. Služby Czech POINT - Ministerstvo vnitra České republiky. Úvodní strana - Ministerstvo vnitra České republiky [online]. Copyright © 2023 Ministerstvo vnitra České republiky, všechna práva vyhrazena [cit. 2023-18-03]. Dostupné z: https://www.mvcr.cz/clanek/sluzby-czech-point.aspx
57. Služby pro veřejnost – Czech POINT. [online]. Copyright © 2023 Ministerstvo vnitra České republiky, všechna práva vyhrazena [cit. 2023-18-03]. Dostupné z: https://www.czechpoint.cz/public/verejnost/sluzby-pro-verejnost/
58. Téměř tajný Úřad pro kybernetickou bezpečnost odhalil svoji strukturu - Česká justice. *Homepage - Česká justice* [online]. [cit. 2023-29-01]. Dostupné z: https://www.ceska-justice.cz/2017/08/temer-tajny-urad-pro-kybernetickou-bezpecnost-odhalil-svoji-strukturu/
59. The CERT Division | *Software Engineering Institute. Software Engineering Institute* [online]. Copyright © 1998 [cit. 2023-30-01]. Dostupné z: https://www.sei.cmu.edu/about/divisions/cert/
60. Výroční zpráva Bezpečnostní informační služby za rok 2017 [online]. *Bezpečnostní informační služba*, 2018, s. 25, [vid. 2023-27-02]. Dostupné z: https://www.bis.cz/public/site/bis.cz/content/vyrocnizpravy/2017-vz-cz.pdf
61. WILSON, C. *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress.* Washington: Congressional Research Service. 2003, [cit. 2023-27-01]. Dostupné z: http://www.fas.org/irp/crs/RL32114.pdf
62. Základní pravidla pro svazky obcí | *Moderní obec – odborný měsíčník* . Moderní obec – odborný měsíčník [online]. Copyright © [cit. 2023-12-03]. Dostupné z: https://moderniobec.cz/zakladni-pravidla-pro-svazky-obci/
63. Základní registry [Architektura eGovernmentu ČR]. Uvítání a obsah webu [Architektura eGovernmentu ČR] [online]. [cit. 2023-18-03]. Dostupné z: https://archi.gov.cz/nap:zakladni_registry
64. Základní registry veřejné správy | Přínosy a využití základních registrů | BusinessInfo.cz. BusinessInfo.cz - Oficiální portál pro podnikání a export [online]. Copyright © 1997 [cit. 2023-18-03]. Dostupné z: https://www.businessinfo.cz/navody/zakladni-registry-verejne-spravy-ppbi/4/
65. Zkušební otázky a odborná literatura - Státní služba. *Úvodní strana - Ministerstvo vnitra České republiky* [online]. Copyright © 2023 Ministerstvo vnitra České

republiky. Všechna práva vyhrazena. [cit. 2023-12-03]. Dostupné z: https://www.mvcr.cz/sluzba/clanek/zkusebni-otazky-a-odborna-literatura.aspx

66. Zkušební otázky a odborná literatura - Státní služba. *Úvodní strana - Ministerstvo vnitra České republiky [online]. Kapitola 1: Organizace a činnost veřejné správy.* Copyright © 2023 Ministerstvo vnitra České republiky. Všechna práva vyhrazena. [cit. 2023-12-03]. Dostupné z: https://www.mvcr.cz/sluzba/clanek/zkusebni-otazky-a-odborna-literatura.aspx

Legislativní dokumenty

1. ČESKO.*Akční plán ke Strategii pro oblast kybernetické bezpečnosti České republiky na období 2012 - 2015* [online]. Vláda České republiky, 2012 [vid. 2023-28-01]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/
2. ČESKO.Národní úřad pro kybernetickou a informační bezpečnost - *Úvodní stránka* [online]. Copyright ©4 [cit. 2023-29-01]. Dostupné z: https://nukib.cz/download/publikace/legislativa/2021-06-14_vyhlaska-o-VIS.pdf
3. ČESKO.*Strategie pro oblast kybernetické bezpečnosti České republiky na období 2012 – 2015* [online]. Vláda České republiky, 2012 [vid. 2023-28-01]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/
4. ČESKO.Viz 437-2017_Platne_zneni_2021.pdf. Národní úřad pro kybernetickou a informační bezpečnost – Legislativa ZKB. *Národní úřad pro kybernetick ou a informační bezpečnost - Úvodní stránka* [online]. [cit. 2023-29-01]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/legislativa-zkb/

Seznam tabulek a grafů

Seznam zkratek

AIFO - Agendový identifikátor

AIFO - Agendový identifikátor fyzických osob

AISC - Agendový informační systém cizinců

AISECD - Agendový informační systém cestovních dokladů

AISEO – Agendový informační systém evidence obyvatel

AISEOP – Agendový informační systém evidence občanských průkazu

BRS - Bezpečnostní rada státu

CERT – Computer Emergency Response Team

CSIRT – Computer Security Incident Response Team

DDoS – Distributed Denial of service

DS - Datová schránka

IK České republiky – Informační koncepce ČR

IROP – Integrovaný regionální operační program

IS – Informační systém

ISDS – Informační systém datových schránek

ISVS - Informační systémy veřejné správy

ISZR – Informační systém základních registrů

IT – Informační technika

MMR - Ministerstvo pro místní rozvoj

NBÚ - Národní bezpečnostní úřad

NCKB - Národní centrum kybernetické bezpečnosti

NKOD - Národní katalog otevřených dat

NÚKIB – Národního úřadu pro kybernetickou a informační bezpečnost

OVM – Orgán veřejné moci

PIN - Personal identification number

PPDF - Propojený datový fond

ROB - Výdejem údajů z Registru obyvatel

RSA - Šifra s veřejným klíčem

RÚIAN – Registr uzemni identifikace, adres a nemovitosti

VDF – Veřejný datový fond

VS - Veřejná správa

ZIFO - Zdrojový identifikátor

ZoISVS - Zákon o informačních systémech veřejné správy

ZoKB - Zákon o kybernetické bezpečnosti

ZR - Základní registr