Organizace a subjekty kybernetické bezpečnosti v České republice a ve světě

Klára Jeřábková

Bakalářská práce
2022

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva

Akademický rok: 2021/2022

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Klára Jeřábková**
Osobní číslo:	**L19682**
Studijní program:	**B2825 Ochrana obyvatelstva**
Studijní obor:	**Ochrana obyvatelstva**
Forma studia:	**Prezenční**
Téma práce:	**Organizace a subjekty kybernetické bezpečnosti v České republice a ve světě**

Zásady pro vypracování

1. Proveďte rešerši současného stavu předmětné oblasti.
2. Seznamte se s teoretickými východisky a legislativním rámcem oblasti kybernetické bezpečnosti v České republice.
3. Identifikujte primární organizace a subjekty zabývající se kybernetickou bezpečností České republiky a vybraných států.
4. Vytvořte model struktury vybraných subjektů kybernetické bezpečnosti.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK. *Řízení kybernetické bezpečnosti a bezpečnosti informací.* Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.
2. SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.
3. ŠULC, Vladimír. *Kybernetická bezpečnost.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 9788073807375.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Petr Svoboda, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **1. prosince 2021**
Termín odevzdání bakalářské práce: **13. května 2022**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 1. prosince 2021

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 11.4.2022

Jméno a příjmení studenta: Klára Jeřábková

.....
podpis studenta

ABSTRAKT

Bakalářská práce je zaměřena na výčet organizací a subjektů kybernetické bezpečnosti v České republice a ve vybraných státech. Teoretická část vymezuje základní teoretická východiska předmětné oblasti, legislativní rámec ovlivňující kybernetickou bezpečnost v České republice, současný stav předmětné oblast jejíž součástí je i popis vybraných institucí. Praktická část se zabývá vytvořením modelů struktury organizací a subjektů kybernetické bezpečnosti pro Českou republiku i pro vybrané státy na základě zjištěných poznatků z teoretické části. Při zjišťování informací byl za vnímán jistý chaos mezi bezpečnostními týmy CSIRT a CERT a z tohoto důvodu se praktická část taktéž zaměřuje na vymezení rozdílů mezi těmito týmy a pro lepší pochopení je vytvořen model, který přehledně znázorňuje rozdíly mezi bezpečnostními týmy.

Klíčová slova: bezpečnost, kybernetická bezpečnost, kybernetický zákon, modelování, model struktury, organizace.

ABSTRACT

The bachelor thesis is focused on the list of organizations and subjects of cyber security in the Czech Republic and in selected countries. The theoretical part defines the basic theoretical background of the subject area, the legislative framework affecting cyber security in the Czech Republic, the current state of the subject area, which includes a description of selected institutions. The practical part deals with the creation of models of the structure of organizations and entities of cyber security for the Czech Republic and for selected countries on the basis of findings from the theoretical part. A certain chaos between the CSIRT and CERT security teams was perceived as gathering information, and for this reason the practical part also focuses on defining the differences between these teams and for a better understanding a model is created that clearly shows the differences between the security teams.

Keywords: cyber law, cyber security, modeling, organization, security, structure model.

Tímto bych ráda poděkovala svému vedoucímu Ing. Petru Svobodovi, Ph.D. za poskytnuté konzultace, rady a případné připomínky, které mi pomohli při zpracovávání bakalářské práce. Dále bych chtěla poděkovat svému otci, který mě ve studiu maximálně podporoval a byl mou oporou.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Jelikož čím dál tím víc zasahují informační technologie do běžného života, znamená to také daleko víc nových kybernetických hrozeb. V dnešní době už snad každý používá chytrý telefon, notebook či chytrou televizi, která je už ve většině případů taktéž připojena k internetu tzn. větší pravděpodobnost kybernetického útoku. Proto kybernetická bezpečnost je velmi aktuálním tématem a jelikož vznikají nové a pokročilé technologie jako například umělá inteligence dá se v budoucnu očekávat ještě větší nárust kybernetických hrozeb. Stále častěji je slýcháno o kybernetickém útoku například na nemocniční zařízení, banky ale i menší firmy či jednotlivce, proto je důležité, aby každý věděl, jak se chránit nebo alespoň minimálně na koho se obrátit v případě nějakého problému, zneužití či napadení kybernetickým útokem.

Jak je zmíněno výše problematika kybernetické bezpečnosti je velmi aktuální i z budoucího hlediska a zmíněné úřady a bezpečnostní týmy, které jsou uvedeny v bakalářské práci značně nabývají důležitosti a z tohoto důvodu byl jednoznačný výběr bakalářské práce, aby alespoň z nějaké části pomohl v přehledu organizací a subjektů, které se zabývají předmětnou oblastí.

Hlavním cílem bakalářské práce je vytvoření modelů struktury organizací a subjektů zabývající se kybernetickou bezpečností jak pro Českou republiku, tak i pro vybrané státy. Hlavní cíl bude naplňován za pomoci 6 dílčích cílů. Prvním dílčím cílem je provedení rešerše současného stavu předmětné oblasti v České republice zahrnující základní názvosloví, legislativní rámec a popis současného stavu. Druhým dílčím cílem je seznámení se s organizacemi a subjekty kybernetické bezpečnosti v České republice. Třetí dílčí cíl navazuje na dílčí cíl předešlý, kdy bude provedena sumarizace organizací a subjektů v České republice sloužící jako podklad pro realizaci modelu. Čtvrtým dílčím cílem je seznámení se s organizacemi a subjekty kybernetické bezpečnosti ve vybraných státech. Pátý dílčí cíl je opět založen na cíli předešlém, kdy bude provedena sumarizace organizací a subjektů kybernetické bezpečnosti vybraných států sloužící jako podklad pro realizaci modelu. Posledním dílčím cílem je pak vlastní realizace modelů v rámci České republiky i vybraných států.

I. TEORETICKÁ ČÁST

1 TEORETICKÁ VÝCHODISKA KYBERNETICKÉ BEZPEČNOSTI

V dnešní době se stále častěji vyskytují případy napadení počítačových sítí, při kterých dochází buď ke krádeži, částečnému narušení dat, které způsobuje nefunkčnost či k úplnému zničení. Je to i z toho důvodu, že je značně široké množství informačních technologií a s nimi souvisejícími službami, proto je kybernetická bezpečnost velmi důležitá oblast, jelikož se týká všech uživatelů, kteří běžně používají internet (Lukáš, 2019).

Tato kapitola bakalářské práce vychází z názvosloví, které je mezinárodně definováno.

Kybernetická bezpečnost

Účelem bezpečnosti je všeobecně ochrana něčeho před zcizením, poškozením anebo úplným zničením. Kybernetická bezpečnost pak obecně slouží k ochraně počítačových systémů a uživatelských dat před nedovolenou manipulací tzn. před odcizením, poškozením nebo znepřístupněním dat, prostřednictvím technologií, kde hlavním cílem je eliminovat riziko kybernetických útoků a zajistit ochranu před bezpečnostními hrozbami, které se začínají vyvíjet. Kybernetická bezpečnost je souhrn právních, technických, organizačních a vzdělávacích prostředků, které zajišťují ochranu kyberprostoru (Doucek, Konečný, Novák, 2019; Jirásek, Novák, Požár, 2015; Lukáš, 2019; Šulc, 2018).

Specifika kybernetické bezpečnosti

Nejvíce specifickým odvětvím je jednoznačně kybernetická bezpečnost, kde hlavním faktorem je její působnost. Působí totiž, jak v reálném světě, tak také v kyberprostoru (Lukáš, 2019).

Základní vlastnosti:

- Ohraničenost – místo, které je připojeno na internet, může být obětí útoku, zde nehraje žádnou roli vzdálenost ani hranice.
- Čas – jde o interpretaci digitálních dat, které jdou změnit (jako příklad lze uvést zkušební licence, kde je omezena doba užívání, jak licence skončí stačí změnit systémové datum a uživatel může pokračovat v používání).
- Motivovanost útočníka – v této oblasti jsou dva poměrně specifické motivy a těmi jsou nuda (existuje spoustu návodů, jak cracknout apod.) a potřeba si dokázat, že zvládne překonat překážky, které stanovil výrobce pro ochranu produktu => vzniká rádoby soutěž, kdo ochranu prolomí první.

- Anonymita – v kyberprostoru je možné se vyhnout osobnímu kontaktu, a proto je jednoduché se vydávat za někoho jiného, a tak skrýt svou pravou identitu (Lukáš, 2019).

Stav kybernetického nebezpečí

Je stav, ve kterém je ohrožena bezpečnost sítí elektronických komunikací či služeb a bezpečnost informací uvedené v informačních systémech (Jirásek, Novák, Požár, 2015).

Informační bezpečnost

Metody a strategie informační bezpečnosti jsou často odlišné od většiny výpočetních technologií, protože jejich hlavním cílem je zamezit nežádoucímu chování počítačů. Bezpečnostní informační systémy jsou kolektivní mechanismy a postupy, které mají chráněny cenné a citlivé informace a služby před poškozením, zveřejněním či kolapsem, činností nedůvěryhodné osoby nebo neoprávněnou činností a neplánované události. Tuto ochranu řeší během celého životního cyklu, tj. vznik, zpracování, ukládání, přenos a likvidace (Lukáš, 2019).

Bezpečnostní událost

Bezpečnostní událost může narušit informační technologie a systémy a také pravidla, které jsou vymezeny k jeho ochraně (Jirásek, Novák, Požár, 2015).

Kyberprostor

Pro kyberprostor není zcela jednoznačná definice, ale setkáváme se s ním jako s virtuálním počítačovým světem v internetu, který je tvořený informacemi a daty. Tím nabízí globální infrastrukturu pro vzájemné propojení jak osobních, podnikatelských tak i správních aktivit tzn. že se zde může komunikovat například přes e-mail, Viber, Skype nebo také lze nakupovat v internetových obchodech. Na druhou stranu, jelikož je to prostředí, které propojuje celosvětovou síť internetu žádná z organizací a subjektů nemá tento prostor pod kontrolou (Doucek, Konečný, Novák, 2019; Lukáš, 2019; Šulc, 2018).

Kybernetický incident

Je to kybernetická příhoda, která má dopad na procesní aktivity organizace nebo má za příčinu ztrátu informační bezpečnosti. O kybernetický incident se jedná v případě, že dojde k narušení kybernetické bezpečnosti (Doucek, Konečný, Novák, 2019).

Kybernetická kriminalita

Kybernetickou kriminalitou se rozumí trestný čin nebo také zločin, který se provádí prostřednictvím počítačové sítě či systému zpracování dat nebo částmi, které jsou s nimi spojeny, jako jsou krádeže osobních údajů a identity, kreditní karty nebo podvody. Tyto útoky jsou z větší části prováděny za účelem získání finančních prostředků (Jirásek, Novák, Požár, 2015; Lukáš, 2019).

Kybernetický terorismus

Kybernetický terorismus se stává nejčastěji přes internet a může být prováděn na velkou vzdálenost a bez vědomí uživatele (příkladem může být napadení státní infrastruktury nebo bank). Účelem je krádež informací, poškození nebo znepřístupnění dat anebo zneužití technologie, ale také vyvolání strachu nebo neadekvátní reakci. Útoky jsou nejčastěji nacionalisticky, extremisticky nebo politicky motivované (Jirásek, Novák, Požár, 2015; Lukáš, 2019).

Kybernetická špionáž

Jde o formu kybernetického útoku, kde cílem je získat strategicky citlivé nebo strategicky důležité údaje. Účelem kybernetické špionáže je získat například vojenskou, politickou či ekonomickou převahu (Jirásek, Novák, Požár, 2015; Lukáš, 2019).

Kybernetická válka

Bere se jako konflikt v oblasti informačních technologií tzn. vedení války v kyberprostoru použitím počítačů a internetu. Útoky zahrnují například politický či strategický motiv. Do kybernetické války se také řadí útoky teroristických skupin nebo skupin hackerů (Jirásek, Novák, Požár, 2015; Lukáš, 2019).

Kritická informační infrastruktura

V prostředí, kde je vytvářena kritická infrastruktura státu je taktéž zařazena kybernetická bezpečnost. Kritickou infrastrukturou je prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, kterým se bere například zařízení, stavba, veřejná infrastruktura nebo prostředek, kterým jsou určeny dle odvětvových a řezových kritérií, kdy v případě narušení jejich funkcí by to znamenalo ohrožení bezpečnosti státu, ekonomiky, zdraví osob a zabezpečení základních životních potřeb obyvatelstva (Jirásek, Novák, Požár, 2015; Sedlák, Konečný, 2021).

Kybernetické riziko

Kybernetické riziko je souhrn možností zranitelnosti aktiva či skupiny aktiv, kterou využije určitá hrozba, a to zapříčiní škodu organizaci. Je to způsobeno kybernetickou hrozbou (Doucek, Konečný, Novák, 2019; Sedlák, Konečný, 2021).

Kybernetická hrozba

Je vnímána jako možná příčina nechtěné události, která se týká kyberprostoru a která může způsobit poškození systému nebo organizace. Je to hrozba, který se vyskytuje v kyberprostoru (Doucek, Konečný, Novák, 2019; Sedlák, Konečný, 2021).

Kybernetický útok

Jedná se o pokus vystavení hrozbě, vyřazení z činnosti, zničení, změnu, získání neoprávněnému přístupu, a tak získat citlivé nebo strategicky důležité údajů, použití či také odcizení aktiva. Nejčastějším motivem jsou vojenské či politické útoky (Jirásek, Novák, Požár, 2015; Sedlák, Konečný, 2021).

Kybernetický protiútok

Je to odpověď na předchozí kybernetický útok. Útoky jsou nejčastěji vojensky či politicky motivované (Jirásek, Novák, Požár, 2015).

Datové modelování

Jelikož se praktická část bude zabývat modelováním je na místě popsat, co to modelování je. V tomto případě se bude jednat o datové modelování, které představuje proces analýzy a definování požadavků, které jsou kladeny na strukturu dat, s kterými pracují informační systémy. Jedná se o proces datového uspořádání a návrhu struktury, kde je cílem popsat reálný objekt (Rak, 2017).

2 LEGISLATIVNÍ RÁMEC KYBERNETICKÉ BEZPEČNOSTI V ČESKÉ REPUBLICE

Zákon číslo 181/2014 o kybernetické bezpečnosti a o změně souvisejících zákonů upravuje práva a povinnosti osob, pravomoc a působnost orgánů veřejné moci, které se věnují kybernetické bezpečnosti. Hlavním cílem zákona je vylepšit detekci kybernetických bezpečnostních incidentů, stanovit základní úroveň bezpečnostních opatření, upravit činnost dohledových pracovišť, zavést hlášení a systém opatření k reakci na kybernetické bezpečnostní incidenty. Avšak tento zákon se nevztahuje na komunikační či informační systémy, které zacházejí s utajovanými informacemi (Doucek, Konečný, Novák, 2019; Maisner, Vlachová, 2015; Národní úřad pro kybernetickou a informační bezpečnost; Sedlák, Konečný, 2021).

Kybernetický zákon upravuje typy povinných subjektů, kterými jsou:

- Osoby nebo orgány, které zajišťují významnou síť.
- Provozovatelé a správci informačního a komunikačního systému kritické informační infrastruktury.
- Provozovatelé základní služby, správci a provozovatelé významného informačního systému a informačního systému základní služby.
- Poskytovatelé digitálních služeb, služeb elektronických komunikací a subjekty zajišťující sítě elektronických komunikací (Doucek, Konečný, Novák, 2019; Sedlák, Konečný, 2021).

Zákon číslo 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti upravuje zásady pro stanovení utajovaných informací, jejich ochranu a přístup k nim, citlivé činnosti a podmínky pro výkon státní správy (Zákon č. 412/2005 Sb.).

Zákon číslo 110/2019 Sb., o zpracování osobních údajů upravuje práva a povinnosti při zpracování osobních údajů, kdy každý má právo na ochranu soukromí. Zároveň tento zákon zpracovává a navazuje na předpisy Evropské unie (Zákon č. 110/2019 Sb.).

Vyhláška číslo 82/2018 Sb., o kybernetické bezpečnosti pojednává o bezpečnostních a reaktivních opatření, kybernetických bezpečnostních incidentech, likvidaci dat a náležitostech podaní v kybernetické bezpečnosti, kde v základu obsahuje převážně požadavky na organizace a technická opatření, která musí některé typy povinných subjektů uskutečňovat (Doucek, Konečný, Novák, 2019; Sedlák, Konečný, 2021).

Vyhláška o kybernetické bezpečnosti upravuje:

- Strukturu a obsah bezpečnostní dokumentace.
- Rozsah a obsah bezpečnostních opatření.
- Formu a vzor oznámení kontaktních údajů.
- Náležitosti oznámení o provedení reaktivního opatření a jeho výsledku.
- Kategorie, typy a hodnocení významnosti kybernetických bezpečnostních incidentů.
- Způsob hlášení a náležitosti týkající se kybernetického bezpečnostního incidentu.
- Způsob likvidace dat, informací, kopií a provozních údajů (Národní úřad pro kybernetickou a informační bezpečnost).

Vyhláška číslo 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. Obsahem jsou typy informačních systémů, převážně veřejné správy, které upravuje zákon o kybernetické bezpečnosti a určující kritéria, které musí naplnit (Sedlák, Konečný, 2021).

Nařízení vlády číslo 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. Obsahem jsou dopadová a odvětvová kritéria, dle kterých se určuje prvek kritické infrastruktury (Doucek, Konečný, Novák, 2019; Sedlák, Konečný, 2021).

Vyhláška číslo 437/2017 Sb., o kritériích pro určení provozovatele základní služby. Obsahem jsou odvětvová a dopadová kritéria, která slouží k určení provozovatele základní služby a dále reguluje vymezení významnosti dopadu narušení základní služby na zabezpečení ekonomických nebo společenských činností. Vyhláška je upravována kybernetickým zákonem (Doucek, Konečný, Novák, 2019; Národní úřad pro kybernetickou a informační bezpečnost; Sedlák, Konečný, 2021).

Vyhláška číslo 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu. Vyhláška stanovuje vybrané soubory vstupních kritérií, které jsou důležité pro zápis poskytovatelů služeb cloud computingu a služeb cloud computingu do stejnojmenného katalogu, který vede Ministerstvo vnitra ČR. Aby se zefektivnil provoz při výkonu jejich působnosti je orgánům veřejné správy ze zmíněného katalogu umožněno pořizování služeb. Pro vstup jsou stanovena kritéria, které jsou rozdělena do čtyř bezpečnostních úrovní. Jakou má orgán veřejné správy požadovat bezpečnostní úroveň je uvedeno v následující vyhlášce (Národní úřad pro kybernetickou a informační bezpečnost).

Cloud computing = ukládání dat, provoz programů a přístup k nim skrze internetové připojení (Cloud Computing: Co to je a komu se vyplatí, 2020).

Vyhláška číslo 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci. Umožňuje ohodnotit významnost komunikačního a informačního systému orgánům veřejné moci, dle toho, který chce provozovat pomocí cloud computingu. Hodnocení se provádí s ohledem na nejhorší možný dopad v případě narušení dostupnosti, integrity nebo důvěrnosti daného systému nebo jeho části. Orgán veřejné moci na základě toho zařadí systém do určité bezpečnostní úrovně a následně poptá službu cloud computingu, která mu umožní splnit bezpečnostní pravidla, která jsou stanovena pro konkrétní úroveň (Národní úřad pro kybernetickou a informační bezpečnost).

Směrnice Evropského parlamentu a Rady Evropské Unie 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Směrnice NIS). Cílem je, aby právní úpravy členských států ladily v oblasti informačních systémů a bezpečnosti sítí a aby se zlepšovalo fungování vnitřního trhu, a to tak aby byl zaveden jednotný standard úrovně kybernetické bezpečnosti (Národní úřad pro kybernetickou a informační bezpečnost). K této směrnici bylo vydáno **nařízení Evropské komise 2018/151,** díky kterému jsou stanoveny bezpečnostní opatření a parametry významnosti dopadu incidentu pro poskytovatele digitálních služeb (Národní úřad pro kybernetickou a informační bezpečnost).

Národní strategie kybernetické bezpečnosti České republiky na období let 2021-2025 popisuje základní principy, které jsou velmi důležité pro kybernetickou bezpečnost České republiky, budoucí výzvy, základní představu a budoucí strategické směřování v kybernetické bezpečnosti. Dokument vychází ze zákona o kybernetické bezpečnosti a je aktualizován nejméně každých pět let (Národní strategie kybernetické bezpečnosti české republiky na období let 2021-2025).

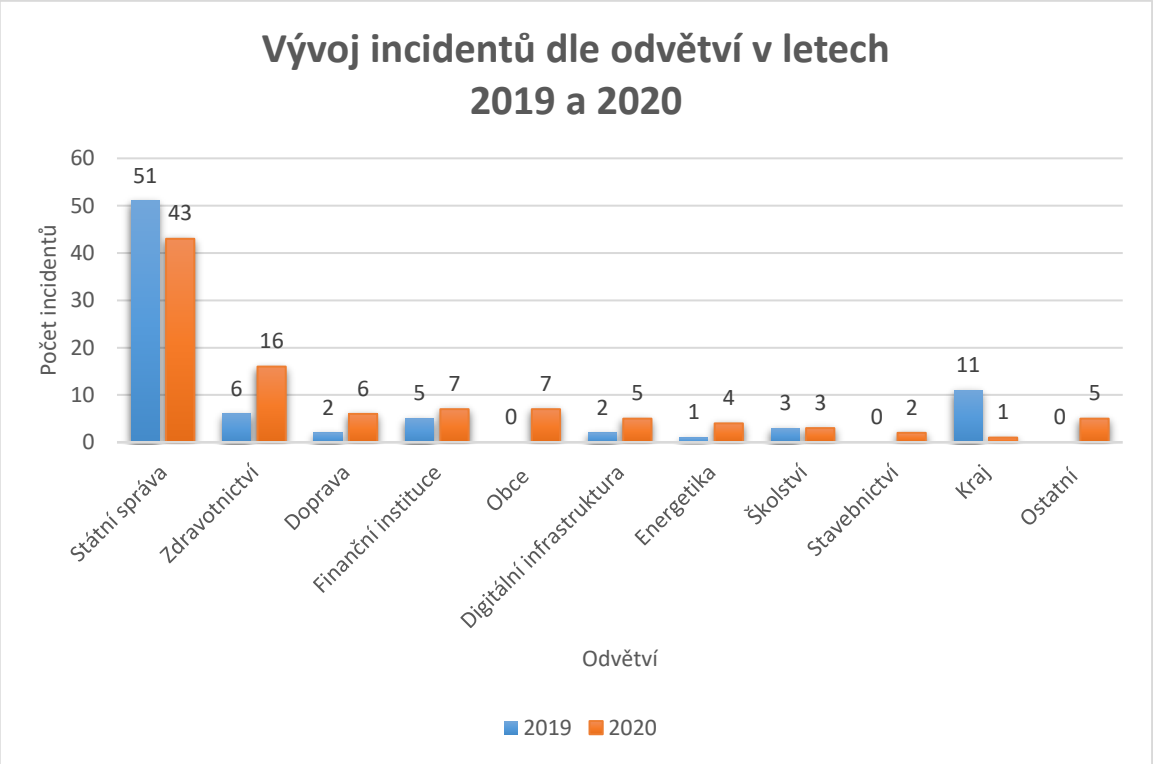
Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2021-2025, který podrobněji rozpracovává konkrétní úkoly a cíle Národní strategie kybernetické bezpečnosti ČR. Pomocí dokumentu Národní úřad pro kybernetickou a informační bezpečnost průběžně sleduje, koordinuje, hodnotí a diskutuje plnění jednotlivých cílů, které jsou stanoveny. Vychází z kybernetického zákona. Je aktualizován nejméně každých pět let v návaznosti na Národní strategii kybernetické bezpečnosti ČR (Akční plán k Národní strategii kybernetické bezpečnosti české republiky na období let 2021 až 2025).

3 REŠERŠE SOUČASNÉHO STAVU PŘEDMĚTNÉ OBLASTI

Kapitola rozebírá současný stav kybernetické bezpečnosti jak v České republice, tak i ve vybraných státech jimiž jsou Rusko, Německo, Francie a Spojené státy americké včetně výčtu a popisu organizací a subjektů, které se zabývají předmětnou oblastí. Jelikož Rusko je pověstné kybernetickými útoky apod. byl výběr téhle země jednoznačný. Následující Německo, Francie a Spojené státy americké byly vybrány, jelikož se řadí mezi státy, které mají dobře zajištěnou kybernetickou bezpečnost. Dalším z důvodu výběru těchto států byl, zda je rozdíl, když stát patří do Evropské unie či nikoli.

3.1 Současný stav kybernetické bezpečnosti v České republice

V dnešní době daleko víc vznikají kybernetické útoky než v předchozích letech. Například v roce 2019 uvedl Národní úřad pro kybernetickou a informační bezpečnost 217 incidentů, ale o rok později počet incidentů markantně vzrostl, a to přesně na 468 incidentů z nichž přímo řešil 99 což je největší počet za poslední čtyři roky. Nejvíce kybernetických útoků bylo zaznamenáno v oblasti státní správy poté následuje zdravotnictví. Přesné počty a oblasti jsou uvedeny ve grafu níže (Zpráva o stavu kybernetické bezpečnosti české republiky za rok 2020).



Obrázek 1 Vývoj incidentů dle odvětví v letech 2019 a 2020
(Zdroj: Zpráva o stavu kybernetické bezpečnosti české republiky za rok 2020 – upraveno)

Spousta organizací, spíše menšího rozsahu kybernetickou bezpečnost zanedbávají, jelikož jsou přesvědčeni, že jejich firma nemůže být cílem nějakého útoku například z důvodu, že jsou málo zajímaví pro útočníka, avšak si neuvědomují, že cílem nemusí být ona firma, ale útok může být plošný. Skrz tohle přesvědčení firmy málo financují tuto oblast (Šulc, 2018).

V grafu níže je uveden vývoj rozpočtů organizací na kybernetickou bezpečnost, který ze 39 % zůstal stejný jako v roce 2019 a dokonce ze 43 % se ještě snížil (Zpráva o stavu kybernetické bezpečnosti české republiky za rok 2020).

Obrázek 2 Vývoj rozpočtů na kybernetickou bezpečnost oproti roku 2019
(Zdroj: Zpráva o stavu kybernetické bezpečnosti české republiky za rok 2020 – upraveno)

Jelikož Národní úřad pro kybernetickou a informační bezpečnost si je vědom, že financovaní určitých organizací v předmětné oblasti je nedostatečný, proto se snaží alespoň vzdělávat zaměstnance státní správy aj. V roce 2020 proškolil více než 18 209 zaměstnanců státní správy, 2 000 pracovníků Fakultní nemocnice Na Bulovce, 214 pracovníků Armády ČR a 1 690 pracovníků prevence (Zpráva o stavu kybernetické bezpečnosti české republiky za rok 2020).

Organizace a subjekty kybernetické bezpečnosti v České republice

Kybernetické bezpečnosti v ČR je zástupcem Národní úřad pro kybernetickou a informační bezpečnost. Dalším poradním a koordinačním orgánem předsedy vlády je také Rada pro kybernetickou bezpečnost, která podporuje a koordinuje činnosti státních institucí, které se zabývají kybernetickou bezpečností (Doucek, Konečný, Novák, 2019; Sedlák, Konečný, 2021).

Národní úřad pro kybernetickou a informační bezpečnost, který je ústředním správním orgánem, který se zabývá kybernetickou bezpečností, kryptografickou ochranou a také ochranou utajovaných informací, která souvisí s informačním a komunikačním systémem (Národní úřad pro kybernetickou a informační bezpečnost).

Pod Národní úřad pro kybernetickou a informační bezpečnost spadá **Národní centrum kybernetické bezpečnosti**, které zajišťuje:

- Prevenci před kybernetickými hrozbami proti prvkům kritické informační infrastruktury, významným a vybraným informačním systémům veřejné správy, proti informačním systémům základní služby.
- Vyhodnocování rizik kybernetické bezpečnosti a přijímání preventivních a popřípadě nápravných opatření.
- Činnost Vládního CERT České republiky.
- Vzdělávací a osvětovou činnost v kybernetické bezpečnosti.
- Koordinaci a řešení kybernetických bezpečnostních incidentů u provozovatelů základní služby, subjektů kritické infrastruktury a orgánů veřejné správy.
- Účast a pořádání na cvičeních v oblasti kybernetiky na mezinárodní a národní úrovni.
- Spolupráci s mezinárodními a národními organizacemi, které zajišťují bezpečnost kyberprostoru.
- Vývoj a výzkum kybernetické bezpečnosti.
- Stanovuje komunikační strategii Úřadu kybernetické bezpečnosti ve spolupráci s ostatními organizačními celky Úřadu.
- Zastupování České republiky ve spolupráci s kabinetem ředitele v orgánech mezinárodních organizací, které zajišťují kybernetickou bezpečnost.

- Spolupráci na mezinárodní úrovni a plnění mezinárodních závazků při realizaci předpisů, které vyplívají z členství v NATO a EU a také v jiných mezinárodních organizacích (Národní úřad pro kybernetickou a informační bezpečnost).

Bezpečnostní rada státu je stálým pracovním orgánem vlády, který připravuje návrhy opatření k zajištění bezpečnosti a také koordinuje bezpečnost České republiky (Bezpečnostní rada státu).

Výbor pro kybernetickou bezpečnost je stálým pracovním orgánem Bezpečnostní rady státu, který má na starosti koordinaci plánování opatření, aby byla zajištěna kybernetická bezpečnost v České republice (Výbor pro kybernetickou bezpečnost).

Národní bezpečnostní úřad, který má oprávnění vést nezbytné evidence a zpracovávat osobní údaje, vyžadovat opis z Rejstříku trestů a nahlížet do něj, bezplatně požadovat poskytnutí informací u orgánů státu, podnikající fyzická a právnická osoba, spolupracovat s bezpečnostním úřadem cizí moci a požadovat od nich informace k účastníku řízení, požadovat od zpravodajských služeb a také od policie informace, které byly získány postupy dle zvláštního právního předpisu opět pro účely řízení apod. Všechny zmíněné a i další oprávnění může Národní bezpečnostní úřad provádět pouze pro plnění svých úkolů v rozporu se zákonem číslo 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti (Národní bezpečnostní úřad).

Vládní CERT (Computer Emergency Response Team = Skupina pro reakci na nouzové situace) je profesionální tým, který řeší kybernetické hrozby a zranitelná místa v organizaci. Mezi další úlohy patří prvotní zdroj bezpečnostních informací a pomoci pro orgány státu, organizace, ale i občany, jelikož jsou kompetentní zveřejňovat informace veřejnosti, aby pomohli posílit bezpečnostní infrastrukturu. V poslední řadě se tým taktéž věnuje zvyšování vzdělanosti v oblasti bezpečnosti na internetu (Národní úřad pro kybernetickou a informační bezpečnost; Sedlák, Konečný, 2021).

Národní CSIRT České republiky (Computer Security Incident Response Team = Skupina pro reakci na počítačové bezpečnostní události) je skupina, která řeší bezpečnostní incidenty v počítačových sítích, které jsou provozované na celém území ČR. Cílem je:

- Udržovat zahraniční vztahy prostřednictvím světových komunit CERT/CSIRT týmů a také organizací, které tyto komunity podporují.
- Spolupracovat se subjekty v rámci ČR => bezpečnostními složkami, úřady státní správy, bankami a dalšími.

- Poskytování služeb v oblasti bezpečnosti => koordinace a řešení bezpečnostních incidentů, proaktivní služby, školní a osvětová činnost (CZ.NIC: správce domény cz; Sedlák, Konečný, 2021).

Národní CSIRT ČR je provozován sdružením **CZ.NIC**, které je provozovatelem registru domén registrovaných pod doménou CZ, zabezpečuje provoz domén nejvyšší úrovně .CZ a osvětu v oblasti jmen domén. V neposlední řadě se sdružení zabývá rozšiřování a podpoře nových technologií a projektů, které jsou prospěšné pro internetovou infrastrukturu v ČR (CZ.NIC: správce domény cz).

Český institut manažerů informační bezpečnosti je sdružením pro informační a kybernetickou bezpečnost. Cílem je sdružovat odborníky ve zmíněné oblasti, vzdělávat, pořádat konference, workshopy apod. (Český institut manažerů informační bezpečnosti).

KYBEZ – Platforma kybernetické bezpečnosti, která zajišťuje technologie a služby v odvětví informační a kybernetické bezpečnosti, obrany, systematické vzdělání apod. (O nás: KYBEZ je platforma pro efektivní spolupráci akademických institucí a komerčních firem)

Asociace elektronických a informačních systémů v ozbrojených silách, která se zabývá rozvojem komunikačních a informačních technologií ozbrojených sil (Česká pobočka AFCEA).

Bezpečnostní tým Masarykovy univerzity cílem je mít bezpečný kybernetický prostor. Proto si Masarykova univerzita vytvořila vlastní bezpečnostní tým, který zajišťuje kybernetickou bezpečnost, informovanost, vzdělávání, zabývá se výzkumem a vývojem apod. (Kyberbezpečnostní tým Masarykovy univerzity).

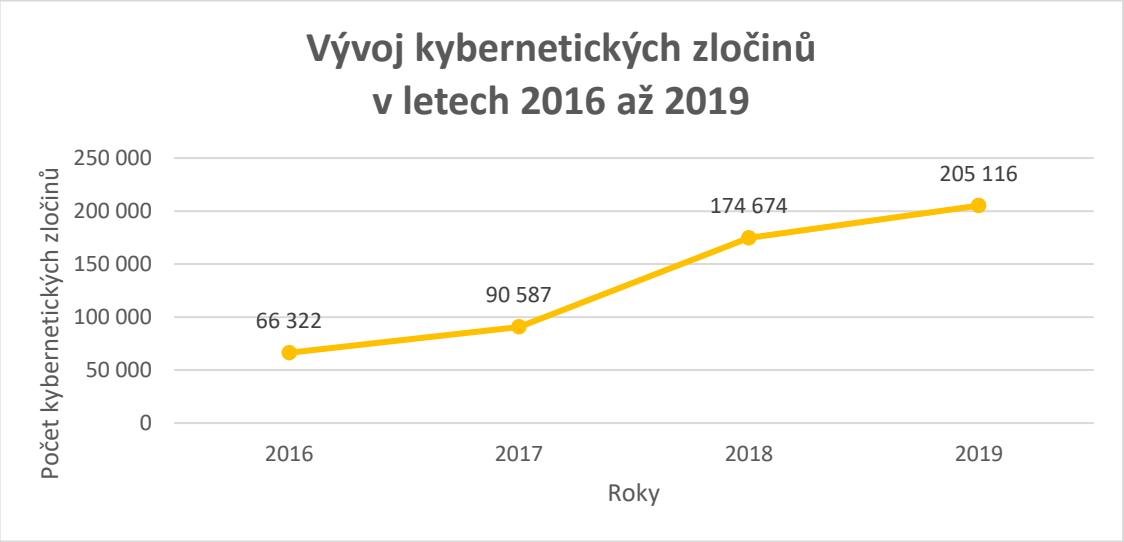
SOC (Security Operations Center = Bezpečnostní operační centrum) je centralizovaná jednotka, kde účelem je ochrana před kybernetickými útoky a to tak, že zajišťuje nepřetržitou analýzu a monitorování bezpečnostních incidentů a událostí s cílem minimalizovat reakční dobu a škody plynoucích z události (Sedlák, Konečný, 2021).

Mezi Mezinárodní organizace patří **ENISA** (European Union Network and Information Security Agency), která taktéž ovlivňuje chod kybernetické bezpečnosti v České republice. ENISA je agentura Evropské unie, která se zabývá kybernetickou bezpečností a dosažením vysoké a společné úrovně kybernetické bezpečnosti v celé Evropě. Mezi její činnosti se například řadí: zvyšování důvěryhodnosti produktů, služeb a procesů zabývající se hardwarem i softwarem pomocí certifikačních schémat kybernetické bezpečnosti dále

přispívá ke kybernetické politice EU, spolupracuje s členskými státy a orgány EU, pomáhá připravit Evropu na kybernetické výzvy, které mohou nastat. Jednou z možností je školení, vzdělávání v dané oblasti, sdílení informací o zranitelnostech a hrozbách, hlášení incidentů apod. (Doucek, Konečný, Novák, 2019; ENISA: European Union Agency For Cybersecurity).

3.2 Současný stav kybernetické bezpečnosti v Rusku

Stejně jako v České republice tak i v Rusku rok od roku roste počet kybernetických útoků. Ministerstvo vnitra Ruské federace uvedlo, že v roce 2016 bylo registrováno 66 322 trestných činů, při kterých byly použity komunikační a informační technologie oproti tomu v roce 2019 vzrostl počet trestných činů až o 138 794. V grafu níže jsou uvedeny přesné vzrůstající hodnoty kybernetických zločinů za poslední roky (Лобач, Смирнова, 2019).



Obrázek 3 Vývoj kybernetických zločinů v letech 2016 až 2019
(Zdroj: Лобач, Смирнова, 2019 – upraveno)

Kybernetickou kriminalitou netrpí jen stát jako celek, ale samozřejmě i jednotlivý občané. V roce 2020 Rusové kvůli kybernetickým podvodům přišli o asi 9 miliard rublů což je v přepočtu 2 520 000 000 českých korun. Tato částka oproti roku 2019 se podle Centrální banky zvýšila až o 34 % (Поздеева, 2021).

V roce 2021 ruský prezident Vladimir Putin schválil **Strategii národní bezpečnosti Ruské federace**, která obsahuje seznam činností jako například zvýšení bezpečnosti ruské informační infrastruktury, boj proti využívání informační infrastruktury státu extremistickými a teroristickými organizacemi, zajištění ochrany ústavních práv a svobod

občana při zpracování osobních údajů, včetně využívání informačních technologií, zvýšení bezpečnosti a stability fungování jednotné telekomunikační sítě v zemi, ruský Internet aj. (Утверждена Стратегия национальной безопасности России, 2021).

Organizace a subjekty kybernetické bezpečnosti v Rusku

V současné době v Rusku neexistuje žádný centralizovaný státní orgán, který by byl odpovědný za kybernetickou bezpečnost. Generální prokuratura Ruské federace vytvořila v roce 2020 mezirezortní pracovní skupinu pro boj s kybernetickou kriminalitou, která zahrnovala:

- Státní zástupce.
- Zástupce ministerstva zahraničních věcí.
- Zástupce ministerstva vnitra.
- Zástupce Federální bezpečnostní služby.
- Zástupce vyšetřovacího výboru.
- Zástupce ministerstva spravedlnosti Ruské federace (Поздеева, 2021).

Níže jsou zmíněné Ruské útvary, které se alespoň okrajově zabývají bezpečností informací apod.

Centrum pro udělování licencí, certifikaci a ochranu státních tajemství Federální bezpečnostní služby Ruska je hlavní jednotkou oprávněnou organizovat a provádět povolování činností podniků, institucí a organizací. Dále se podílí na regulaci dovozu na území Ruské federace a vývozu mimo něj šifrovacích prostředků a speciálních technických prostředků určených k tajnému získávání informací. Federální bezpečnostní služba Ruska má certifikát Státního standardu Ruska pro právo certifikovat nástroje bezpečnosti informací podle bezpečnostních požadavků na informace představující státní tajemství (Общая информация).

Vláda Ruské federace rozhoduje o schválení nařízení o **Federální službě pro dohled v oblasti komunikací, informačních technologií a hromadných komunikací** a umožňuje ji, aby měla čtyři zástupce v oblasti komunikací, informačních technologií a masových komunikací, dále ji přiřazuje do pravomoci federální státní jednotný podnik **Hlavní středisko rádiových frekvencí** a **Vědeckotechnické středisko**, kterým je federální rozpočtová instituce (Путин, 2009).

Federální služba pro technickou a exportní kontrolu je výkonný orgán, který zajišťuje bezpečnost kritické informační infrastruktury, ochranu informací obsahujících státní tajemství, jiné informace s omezeným přístupem, zabránění jejich úniku, neoprávněnému přístupu k nim, zvláštním vlivům na informace za účelem získat je, zničit je, zkreslit a zablokovat přístup k nim na území Ruské federace. Dále Organizuje a řídí činnost státního systému pro boj s technickým zpravodajstvím a ochranou informací (Указ Президента РФ от 16.08.2004 N 1085 (ред. от 08.12.2021) "Вопросы Федеральной службы по техническому и экспортному контролю" (Выписка), 2021).

3.3 Současný stav kybernetické bezpečnosti v Německu

Spolkový úřad pro informační bezpečnost uvedl, že situace v Německu začíná být znepokojivá, jelikož technologie jdou stále dopředu a tím pádem vznikají i daleko složitější kybernetické útoky. Například od června 2020 do konce května 2021 úřad identifikoval 144 milionů nových variant malwaru, což odpovídá nárůstu o 22 % v průběhu roku poté v únoru 2021 bylo objeveno rekordní počet 553 000 variant malwaru za jediný den. Proto celková úroveň hrozeb kybernetických útoků se zvýšila ze „závažné“ na „závažnou až kritickou“. Avšak co se týče celosvětového měřítka, tak Německo se řadí na třetí místo kyberneticky nejbezpečnější země (Balsiger, 2021; Chang).

Vzhledem k rostoucí hrozbě kybernetických útoků přijala německá federální vláda **Strategii kybernetické bezpečnosti pro Německo 2021**, která obsahuje čtyři základní pokyny:

- Stanovit kybernetickou bezpečnost jako společný úkol pro stát, byznys, společnost a vědu.
- Posílit digitální suverenitu státu, ekonomiky, vědy a společnosti.
- Bezpečně navrhnout digitalizaci.
- Měřitelné a transparentní cíle (Ziele für die Cybersicherheit beschlossen, 2021).

Organizace a subjekty kybernetické bezpečnosti v Německu

Evropská rada a Evropský parlament rozhodly o zřízení Evropského kompetenčního centra pro kybernetickou bezpečnost v průmyslu, technologii a výzkumu a každý členský stát si určí své národní koordinační centrum. V Německu je to tedy **Národní koordinační centrum pro kybernetickou bezpečnost v průmyslu, technologii a výzkumu.** Cílem Evropského centra kybernetické kompetence je zvýšit evropské kapacity

a konkurenceschopnost v oblasti kybernetické bezpečnosti. Evropské kompetenční centrum zajistí větší koordinaci výzkumu, vývoje a inovací i implementačních strategií (včetně začlenění, implementace a integrace produktů, služeb a procesů kybernetické bezpečnosti) na evropské a národní úrovni. Z členského státu a Evropské komise bude stanovena správní rada. Německo v tomto orgánu zastupuje **Spolkový úřad pro informační bezpečnost.** Ten je federálním úřadem pro kybernetickou bezpečnost a tvůrcem bezpečné digitalizace v Německu, kde cílem je preventivní podpora informační a kybernetické bezpečnosti s cílem podporovat a umožnit bezpečné používání informačních a komunikačních technologií. Mezi úkoly například patří ochrana federálních sítí, detekce a obrana proti útokům na vládní sítě, testování, certifikace a akreditace IT produktů a služeb, varování před škodlivými programy nebo bezpečnostními mezerami v produktech a službách IT, informování a zvyšování povědomí veřejnosti o tématu IT a internetové bezpečnosti apod. (Bundesamt für Sicherheit in der Informationstechnik; Das Europäische Kompetenzzentrum für Cybersicherheit).

Federální ministerstvo vnitra a vlasti a jeho útvary pokrývají širokou škálu úkolů a činností. Rozsah sahá od civilní ochrany přes integraci a propagaci sportu až po bezpečnostní úkoly. Je koordinátorem Národního koordinačního centra pro kybernetickou bezpečnost v průmyslu, technologii a výzkumu (Bundesamt für Sicherheit in der Informationstechnik; Das Europäische Kompetenzzentrum für Cybersicherheit; Ministerium).

Národní centrum pro kybernetickou odezvu je společná, meziagenturní a meziinstitucionální platforma, která má za cíl rychle vyměňovat relevantní informace mezi zúčastněnými orgány a partnery a koordinovat ochranná opatření k zajištění kybernetické bezpečnosti v Německu (Das Nationales Cyber-Abwehrzentrum).

Aliance pro kybernetickou bezpečnost poskytuje společnostem, sdružením, úřadům a organizacím platformu pro spolupráci, jejímž prostřednictvím lze vyměňovat informace o aktuálních hrozbách a praktických opatřeních v oblasti kybernetické bezpečnosti (Allianz für Cyber-Sicherheit: Viele Teilnehmer – ein starkes Netzwerk – ein Ziel).

DCSO: Inženýrské zabezpečení spolu spojuje společnosti, vládní agentury, instituce a vytváří prostor pro důvěryhodnou výměnu mezi nimi. Na základě těchto sdílených zkušeností a jejich odborných znalostí vyvíjejí nejmodernější služby pro efektivní obranu, ze kterých mohou mít prospěch všichni členové (Engineering Security).

Stejně jako v České republice i v Německu kybernetickou bezpečnost ovlivňuje agentura **ENISA**, která je rozebraná na konci kapitoly „Organizace a subjekty kybernetické bezpečnosti v České republice“.

3.4 Současný stav kybernetické bezpečnosti ve Francii

Ve Francii se počty kybernetických útoků velice zvýšily než v předchozích letech. V roce 2020 bylo terčem útoků 159 francouzských úřadů což je o 50 % více než v roce 2019. V téže roce se také staly obětí kybernetických útoků 119 francouzských společností. V letech 2020 a 2021 bylo napadeno i zdravotnictví, přesněji 135 francouzských nemocnic, z několika desítek lékařských laboratoří uniklo přes 500 tisíc zdravotních údajů pacientů jako jsou například rodná čísla, datum narození, adresa, krevní skupina a telefonní číslo apod. Z ostatních evropských zemí se Francie řadí na první místo, co se týče financování firem do oblasti kybernetické bezpečnosti (Chang; 7 statistiques sur la cybersécurité en France).

V roce 2015 přijala Francie **Národní strategii pro digitální bezpečnost**, která je určena na podporu digitální transformace francouzské společnosti a reaguje na nové výzvy vyplývající ze změn digitálního využití a hrozeb s nimi spojených. Zdůrazňuje pět cílů:

- Zaručit národní suverenitu.
- Poskytnout důraznou reakci na kybernetické zlomyslnosti.
- Informovat širokou veřejnost.
- Udělit z digitální bezpečnosti konkurenční výhodu pro francouzské společnosti.
- Posílit hlas Francie na mezinárodní úrovni (La France et la cybersécurité).

Tato strategie byla následně rozšířena o **Francouzskou mezinárodní digitální strategii**, která shrnuje všechny strategické směry, které Francie prosazuje v digitálním světě kolem tří pilířů a ty jsou správa veřejných věcí, ekonomika a bezpečnost. Druhým dokumentem, o který byla strategie rozšířena je **Strategický přezkum kybernetické obrany**, který objasňuje cíle národní strategie kybernetické obrany a potvrzuje relevanci francouzského modelu a primární odpovědnosti státu v této oblasti (La France et la cybersécurité).

Organizace a subjekty kybernetické bezpečnosti ve Francii

Národní agentura pro bezpečnost informačních systémů, která je národním orgánem pro kybernetickou bezpečnost a je zodpovědná za prevenci (včetně norem) a reakci na počítačové incidenty zaměřené na citlivé instituce dále také organizuje cvičení krizového řízení na národní úrovni (La France et la cybersécurité).

Ministerstvo ozbrojených sil má v tomto případě dvojí poslání, a to zajišťovat ochranu sítí, které podporují jeho činnost a integrovat digitální boj do středu vojenských operací. Za účelem upevnění činnosti ministerstva v této oblasti bylo počátkem roku 2017 vytvořeno **velitelství kybernetické obrany**, které je přímo podřízeno příkazům náčelníka štábu obrany, je operačním velením, které sdružuje všechny síly kybernetické obrany tedy i ministerstva pod stejnou stálou a společnou pravomoc. Jeho posláním je ochrana informačních systémů armád a také projektování, plánování a vedení vojenských operací v kyberprostoru (La France et la cybersécurité; Le commandement de la cyberdéfense).

Dalším ministerstvem, který se věnuje předmětné oblasti je **Ministerstvo vnitra**, které bojuje proti všem formám kybernetické kriminality zaměřené na národní instituce a zájmy, ekonomické subjekty a orgány veřejné moci a také na jednotlivce. Za tímto účelem může povolat **specializované ústřední služby, národní policii, národní četnictvo**, kteří jsou odpovědní za vyšetřování zaměřené na identifikaci pachatelů kybernetických útoků a jejich postavení před soud. Tyto služby rovněž přispívají k prevenci a zvyšování informovanosti veřejnosti (La France et la cybersécurité).

GCA: Skupina kybernetické obrany ozbrojených sil toto seskupení má za cíl upevnit kontinuitu mezi kybernetickou ochranou a obranou podporou spolupráce mezi těmito oblastmi a přenosem souvisejících dovedností, které byly dříve distribuovány v rámci samostatných jednotek (Le commandement de la cyberdéfense).

CALID: Centrum pro analýzu v obranném počítačovém boji je střediskem sledování, detekce a varování ministerstva ozbrojených sil v oblasti kybernetické obrany (Le commandement de la cyberdéfense).

CASSI: Centrum pro audit bezpečnosti informačních systémů je národní centrum, které pokrývá dvě oblasti: bezpečnost informačních systémů a kompromitace falešných signálů (Le commandement de la cyberdéfense).

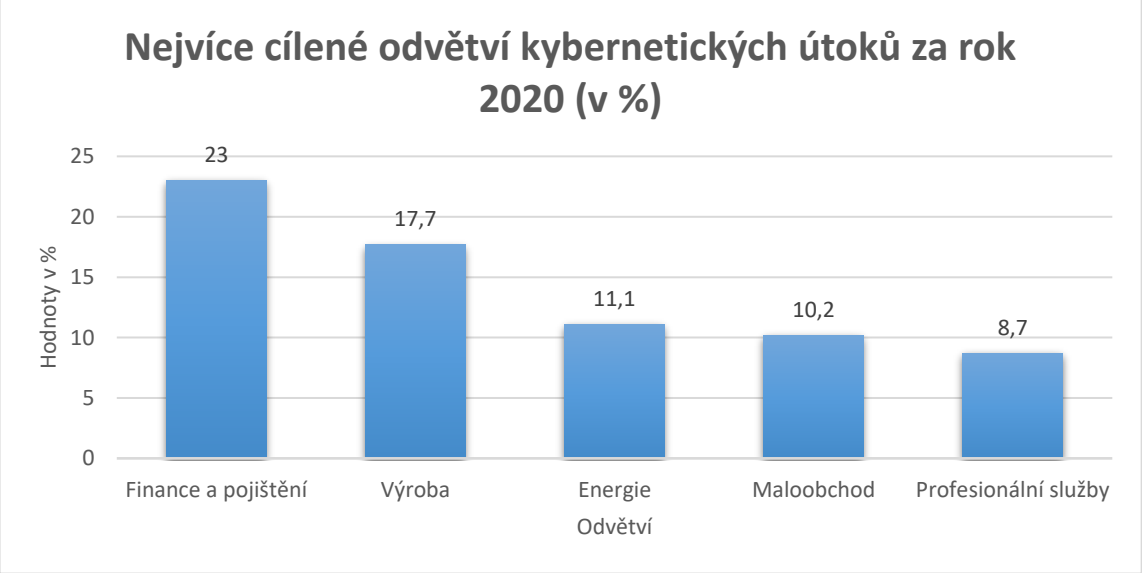
CRPOC: Centrum pro zálohu a operační připravenost na kybernetickou obranu, které stanovuje potřeby záložníků armád, ředitelství a služeb kybernetické obrany. Zajišťuje jejich nábor, výběr a přidělení na celém území státu (Le commandement de la cyberdéfense).

CHPI: Společné hlavní certifikační centrum, které provádí bezpečnostní studie, které vedou ke schválení nových informačních systémů ministerstva před jejich uvedením do provozu (Le commandement de la cyberdéfense).

Jelikož je Francie také v Evropské unii tak stejně jako v České republice i v Německu je ovlivněna kybernetická bezpečnost agenturou **ENISA**, která je rozebraná na konci kapitoly „Organizace a subjekty kybernetické bezpečnosti v České republice“.

3.5 Současný stav kybernetické bezpečnosti ve Spojených státech amerických

Jako v ostatních státech tak i ve Spojených státech amerických narůstá počet kybernetických útoků. Více než 50 % všech kybernetických útoků se zaměřuje na malé a střední podniky. Jedna ze studií Marylandské univerzity uvedla, že každých 39 sekund dochází k pokusu o kybernetický útok. V grafu níže je uvedeno pět odvětví, na které byly nejvíce cílené kybernetické útoky za rok 2020 (Chang; Watters, 2022).



Obrázek 4 Nejvíce cílené odvětví kybernetických útoků za rok 2020
(Zdroj: Watters, 2022 – upraveno)

Aby Spojené státy americké udrželi krok s vyvíjejícím se prostředím kybernetických rizik, snižováním zranitelností, budováním odolnosti, bojem proti zlovolným aktérům v kyberprostoru a učinili kyberprostor bezpečnější a odolnější, proto v roce 2018 přijali

Strategii kybernetické bezpečnosti, která poskytuje ministerstvu rámec pro plnění povinností v oblasti kybernetické bezpečnosti během příštích pěti let (DHS Cybersecurity Strategy).

Organizace a subjekty kybernetické bezpečnosti ve Spojených státech amerických

Agentura pro kybernetickou bezpečnost a bezpečnost infrastruktury je národním koordinátorem pro bezpečnost a odolnost kritické infrastruktury. Zajišťuje kritickou infrastrukturu země a dohlíží na celkový obraz hrozeb, koordinuje provádění národní kybernetické obrany a zajišťuje, aby byly včasné a použitelné informace sdíleny mezi federálními a nefederálními partnery a partnery ze soukromého sektoru. Spolupracuje s partnery napříč vládou a průmyslem. Jedním z úřadů, s kterým úzce spolupracuje je **Úřad pro správu a rozpočet**, který je celkově odpovědný za federální kybernetickou bezpečnost (About CISA).

Národní bezpečnostní agentura vede vládu USA v kryptologii, která zahrnuje jak poznatky signálového zpravodajství, tak produkty a služby kybernetické bezpečnosti (About NSA/CSS).

Centrální bezpečnostní služba poskytuje včasnou a přesnou kryptologickou podporu, znalosti a pomoc vojenské kryptologické komunitě a zároveň podporuje partnerství mezi Národní bezpečnostní agenturou a kryptologickými prvky ozbrojených sil (About NSA/CSS).

Národní centrum kybernetické bezpečnosti je nezisková organizace pro kybernetické inovace a povědomí. Pomáhá veřejným i soukromým organizacím a jednotlivcům prostřednictvím školení, vzdělávání a výzkumu (NCC).

Národní společnost pro kybernetickou bezpečnost je nezisková organizace zaměřená na poskytování vzdělávání, informovanosti a prosazování kybernetické bezpečnosti malým podnikům. Poskytuje vzdělávání v oblasti kybernetické bezpečnosti přizpůsobené potřebám vlastníků malých podniků, pomáhá malým podnikům vyhodnotit jejich kybernetická bezpečnostní rizika, distribuuje informace o hrozbách majitelům podniků, aby byli lépe informováni o hrozbách, kterým jejich podnikání čelí a poskytuje rady ohledně typu služeb potřebných k udržení bezpečí online (Who We Are).

Ministerstvo pro vnitřní bezpečnost zásadním posláním je chránit národ před mnoha hrozbami, kterým čelí. Pravomoci sahají od letectví a bezpečnosti hranic až po řešení nouzových událostí, od analytiky kybernetické bezpečnosti po inspektora chemických zařízení (About DHS, 2022).

Federálně financované výzkumné a vývojové centrum funguje jako prostředek pro speciální výzkum a vývoj smluv v rámci federální vlády, poskytuje Ministerstvu pro vnitřní bezpečnost nezávislé a objektivní rady a rychlou reakci na kritické problémy. Je výkonným zástupcem dvou federálně financovaných výzkumných a vývojových center a těmi jsou Centrum operační analýzy vnitřní bezpečnosti a Ústav pro inženýrství a vývoj systémů vnitřní bezpečnosti (Federally Funded Research and Development Centers, 2022).

Centrum operační analýzy vnitřní bezpečnosti působí v oblasti akviziční studie, studie hrozeb a příležitostí pro vnitřní bezpečnost, organizační a operační studie, regulační, doktrínové a politické studie, studie výzkumu a vývoje, inovace a technologického zrychlení (Homeland Security Operational Analysis Center, 2022).

Ústav pro inženýrství a vývoj systémů vnitřní bezpečnosti působí v oblasti plánování a rozvoje akvizice, vznikající hrozby, zkoumání konceptů, experimentování a hodnocení, informační technologie a komunikace, kybernetického řešení/operace, systémového inženýrství, systémové architektury a integrace, technické kvality a výkonu, nezávislého testování a hodnocení (Homeland Security Systems Engineering and Development Institute, 2022).

3.6 Dílčí závěr

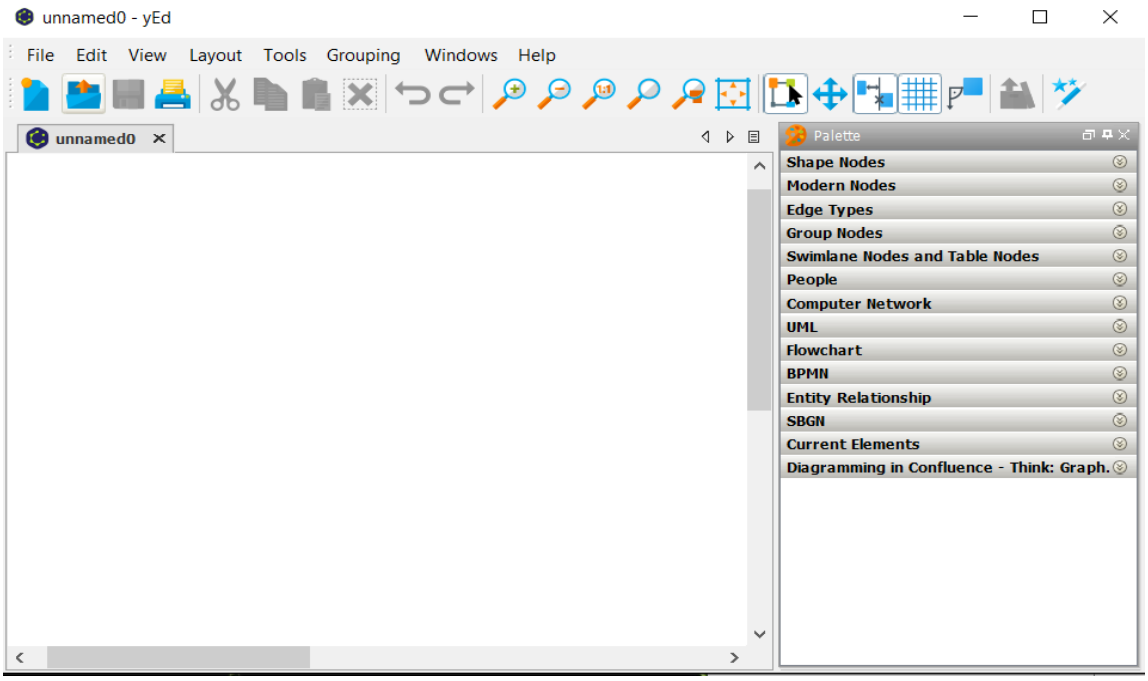
Na základě statistik jde jednoznačně vidět, že z vybraných státu, co se týče kybernetické bezpečnosti je na tom nejlépe Německo, které nemá zas tolik institucí, které spadají pod stát. Proto to že má nějaký stát několik desítek organizací vždy neznamená, že mají nejlépe zajištěnou kybernetickou bezpečnost. I při pohledu na Francii, která má jednu vrcholovou organizaci tak se řadí na dobré umístění kybernetického zabezpečení. Na druhou stranu Rusko, které je proslulé kybernetickými útoky apod. tím, jak nemá žádnou určitou organizaci vyloženě pro kybernetickou bezpečnost si taktéž moc nepřilepšuje. Avšak otázkou je, zda výše uvedené informace jsou kompletní a zda nějaké podrobnější informace nejsou pro okolní státy nepřípustné. Už jen to, že v Rusku mají vlastní internet a mají upravený přístup k informacím značí značnou nejistotu.

II. PRAKTICKÁ ČÁST

4 ANALÝZA FUNKCIONALITY MODELOVACÍHO NÁSTROJE YED GRAPH EDITOR

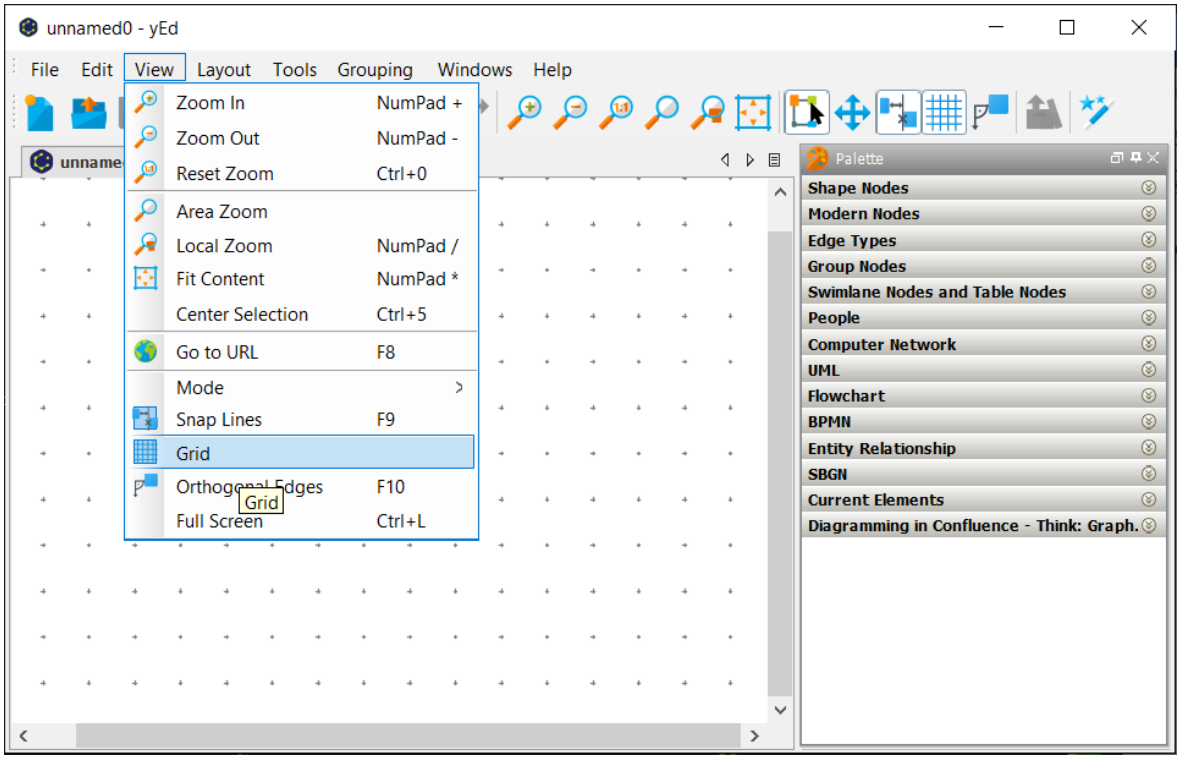
Praktická část bakalářské práce se bude zabývat vytvořením modelu struktury vybraných organizací a subjektů pro každý výše zmíněný stát. Pro vytvoření modelů je použita jednoduchá a zároveň výkonná aplikace yEd Graph Editor, která je volně dostupná ke stažení na všechny platformy: Windows, macOS a Unix/Linux. Aplikace je v anglickém jazyku a slouží k rychlému a efektivnímu generování či vytvoření různých diagramů či zmíněných modelů. Modely jdou vytvářet ručně nebo když se vlastní data importují do aplikace jdou snadno a přehledně uspořádat do nějaké struktury apod. například pro analýzu či pro lepší chápání.

V tomto případě bylo děláno vše ručně na základě poznatků o vybraných organizacích a subjektů, které jsou uvedeny v teoretické části. Ovládání je velmi jednoduché. Po otevření aplikace vyskočí prázdná stránka s horní lištou a s již otevřenou kolonkou Palette na pravé straně, kde jsou k dispozici různé obrazce, šipky, před vytvořené jednoduché tabulky a diagramy, postavičky lidí apod.



Obrázek 5 Aplikace yEd Graph Editor po otevření (Zdroj: vlastní)

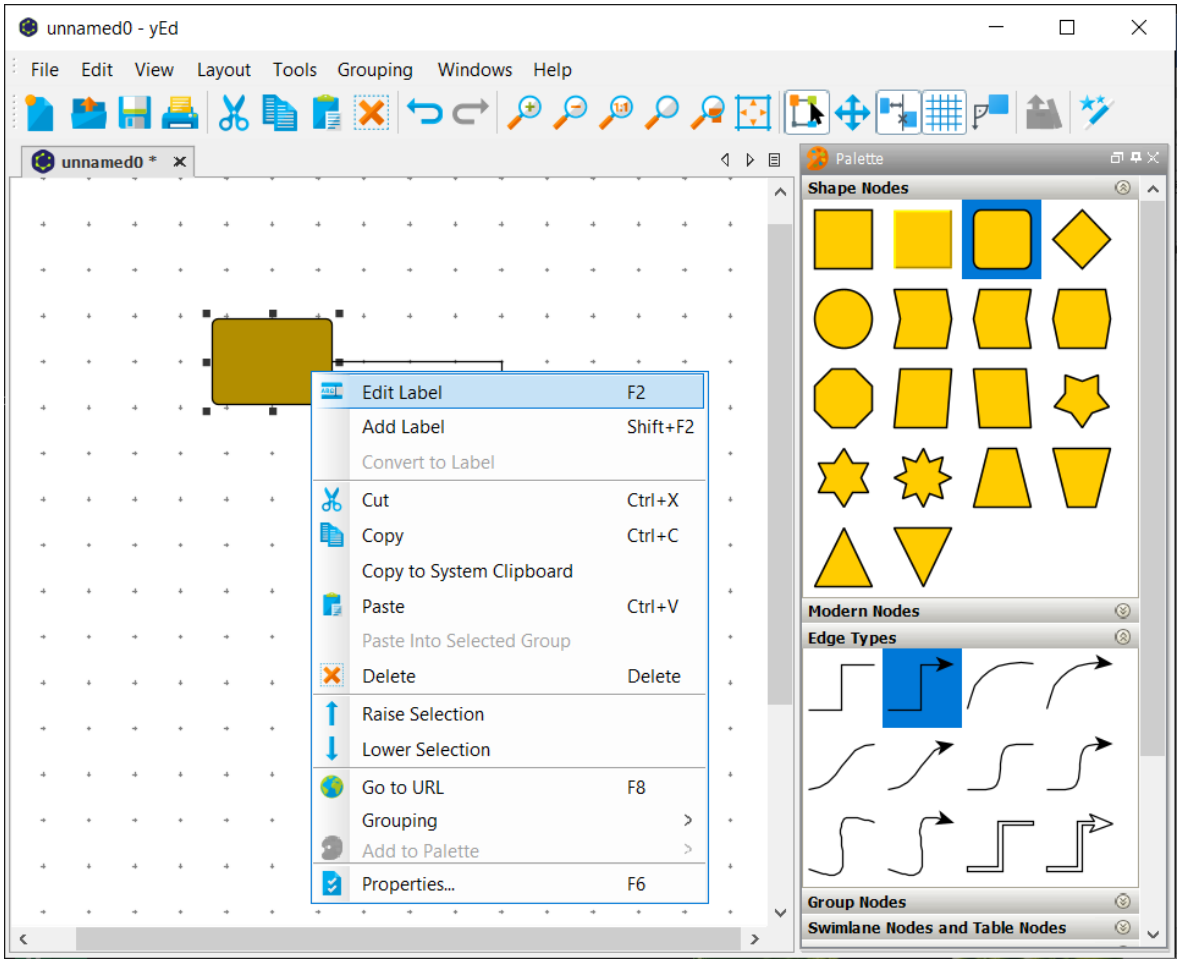
V horní liště jde zapnout pomocí tlačítka Grid pro mřížkové pozadí, aby se lépe a přesněji umisťovali obrazce, šipky apod. Tlačítko jde naleznout buď pod složkou View třetí od konce anebo to je už předvolené v liště tlačítko značící mřížku čtvrté od konce.



Obrázek 6 Grid – možnost zapnutí mřížkovaného pozadí (Zdroj: vlastní)

Po zapnutí mřížkového pozadí lze začít umisťovat obrazce, šipky apod. dle vlastního uvážení. Vybraný obrazec se umisťuje kliknutím a stálým držením tlačítka na myši či touchpadu a potáhnutím na dané místo. Pro uvolnění obrazce se tlačítko myši či touchpadu pustí. V případě propojení dvou obrazců jsou k dispozici různé šipky. Umístění šipek je stejné jako u obrazce, kliknutím a se stálým držením šipky se najede na zvolený obrazec, který se bude propojovat. Puštěním tlačítka na myši či touchpadu se šipka uvolní a následně se bez zmáčknutí tlačítka na myši či touchpadu najede na druhý obrazec, který bude propojen s tím prvním.

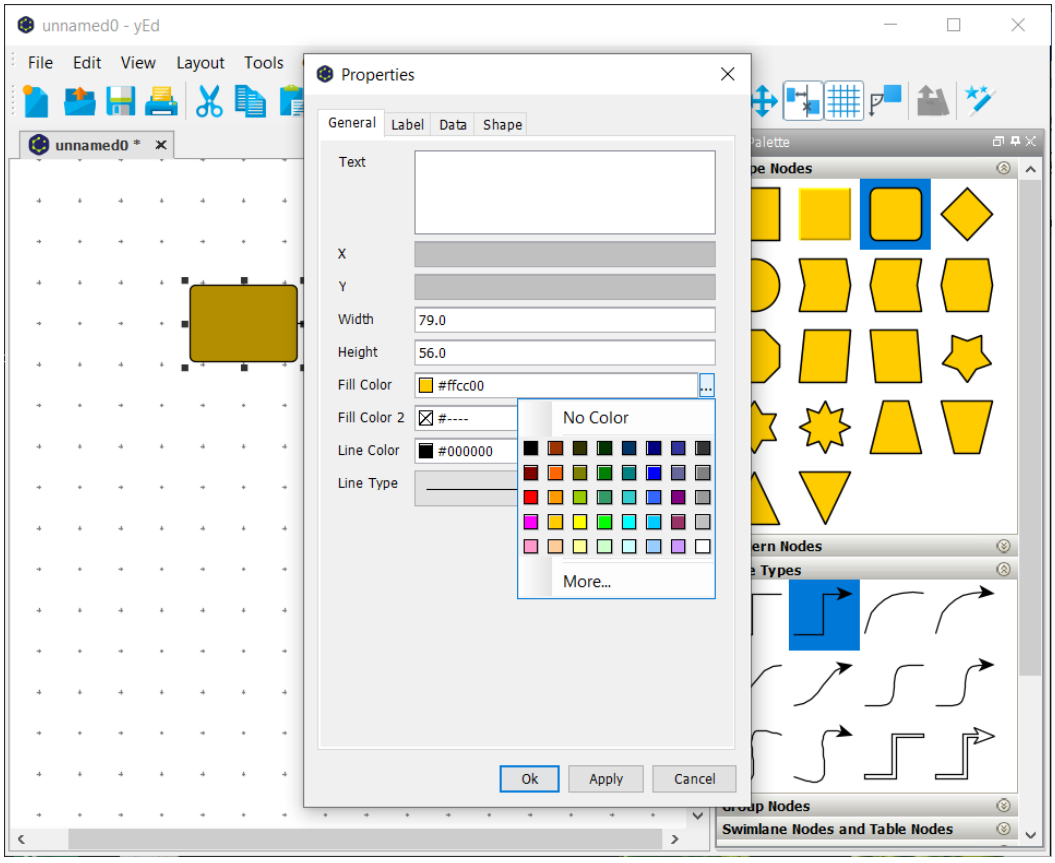
V aplikaci yEd Graph Editor lze také obrazce libovolně popisovat, měnit barvy obrazců apod. Popisu obrazce se docílí namířením a kliknutím myši na zvolený obrazec, zmáčknutím pravého tlačítka na myši či touchpadu a zvolením Edit Label, poté už lze libovolně psát text do obrazce.



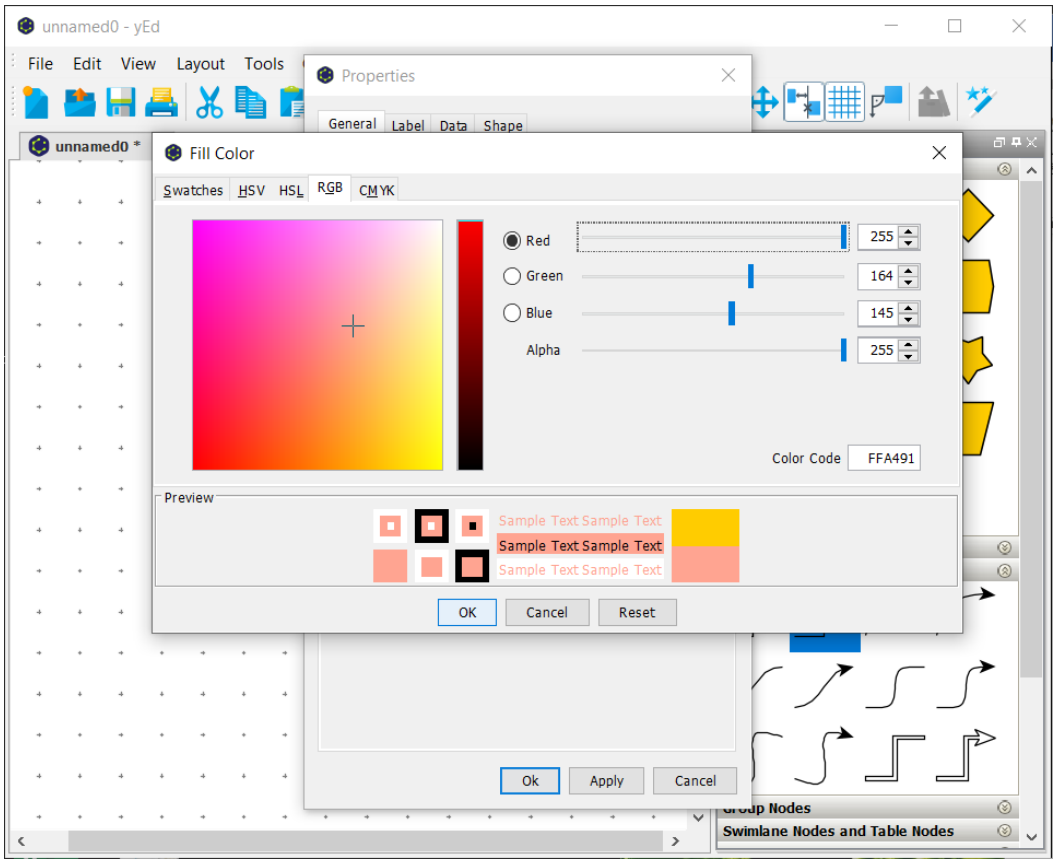
Obrázek 7 Umožnění psaní do obrazce (Zdroj: vlastní)

Pro změnu barev obrazců se na začátek postupuje stejně jako u zvolení možnosti psaní textu. Musí se označit kliknutím libovolný obrazec, popřípadě všechny obrazce a zmáčknutím pravého tlačítka na myši či na touchpadu vyjede kolonka, která je ukázaná v předchozím obrázku „Umožnění psaní do obrazce“. V tomto případě se zvolí složka poslední od konce Properties. Následně vyskočí kolonka, kde jsou informace o obrazci, textu v obrazci apod. Pro změnu barvy obrazce slouží kolonka Fill Color. Za kolonkou jsou uvedeny tři tečky, na které když se klikne vyjede paletka s barvami.

Pro větší množství barev lze kliknout na kolonku More, která se nachází pod paletkou s barvami. Po stisknutí kolonky More vyjede větší paletka s více odstíny barev. V případě stále nedostačujícímu množství barev lze ve složce v horní liště překliknout na následující kolonky, kde je možnost si libovolný odstín barvy namíchat viz. obrázek „Možnost vlastního odstínu barvy“. Následně se výběr potvrdí tlačítkem OK.

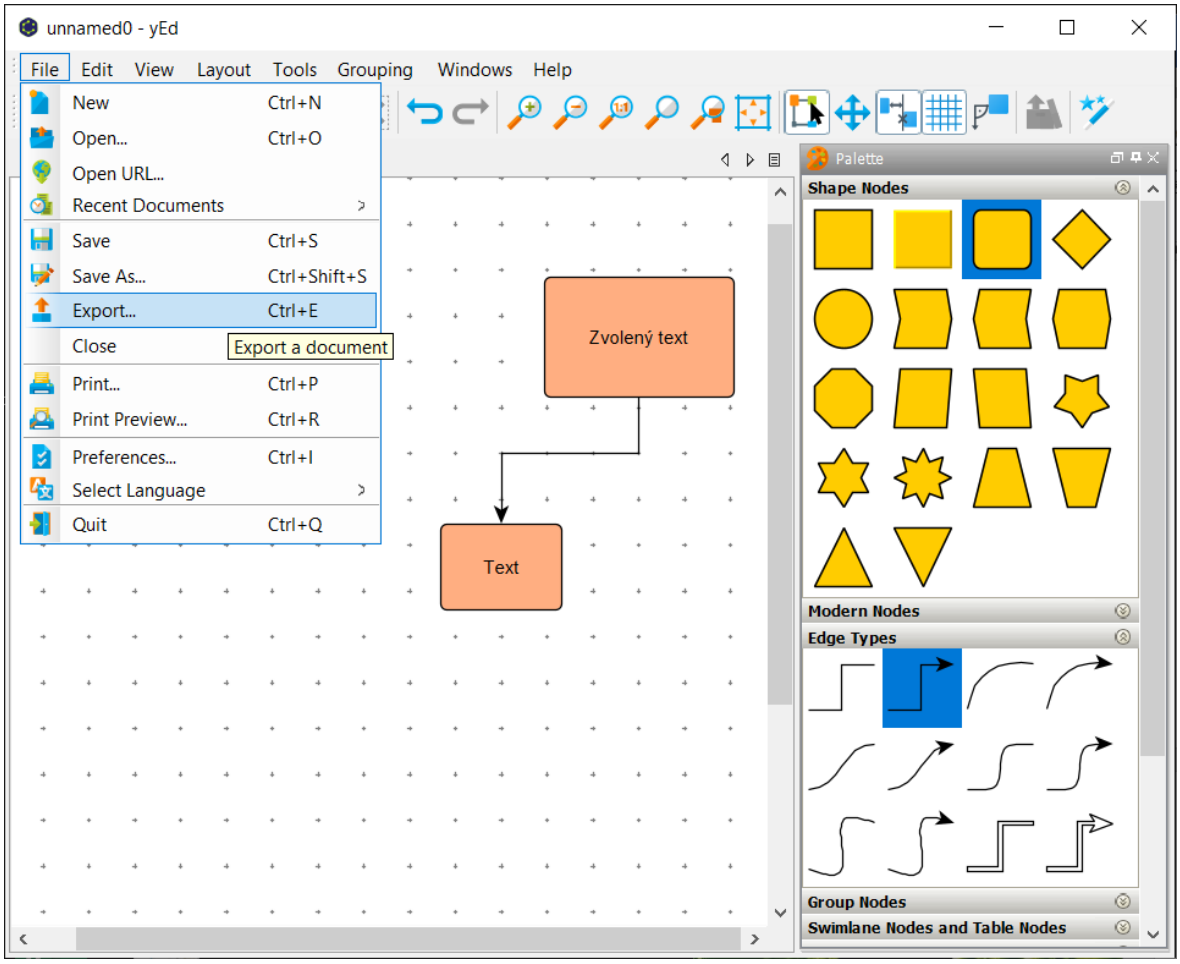


Obrázek 8 Možnost změny barvy obrazců (Zdroj: vlastní)



Obrázek 9 Možnost vlastního odstínu barvy (Zdroj: vlastní)

Jakmile je vše hotové soubor se uloží kliknutím na Save nebo Save As, který lze naleznout v horní liště pod složkou File. Vytvořený model či diagram apod. lze exportovat do obrázku. Opět, když se rozklikne složka File, vyjede výběr, kde stačí kliknout na Export.



Obrázek 10 Možnost dokument exportovat (Zdroj: vlastní)

5 MODELOVÁNÍ STRUKTURY KYBERNETICKÉ BEZPEČNOSTI

Model struktury organizací a subjektů se zaměřuje na hierarchii řízení tzn. kdo je komu nadřazený. Samotná struktura znamená vztahy mezi organizacemi či subjekty (Organization Structure).

5.1 Organizace a subjekty

Model struktury organizací a subjektů v České republice

V následujícím modelu je znázorněna struktura, kde jsou zakreslené vztahy dle zjištěných informací ohledně vybraných organizací a subjektů kybernetické bezpečnosti v ČR. Hlavičkou celé struktury je agentura ENISA, která je zařazena v sekci mezinárodní, protože je to agentura Evropské unie a v oblasti kybernetické bezpečnosti ovlivňuje celou Evropu, udává určitá stanoviska, které musí splňovat všechny země v EU, proto se řadí jako vrcholová organizace.

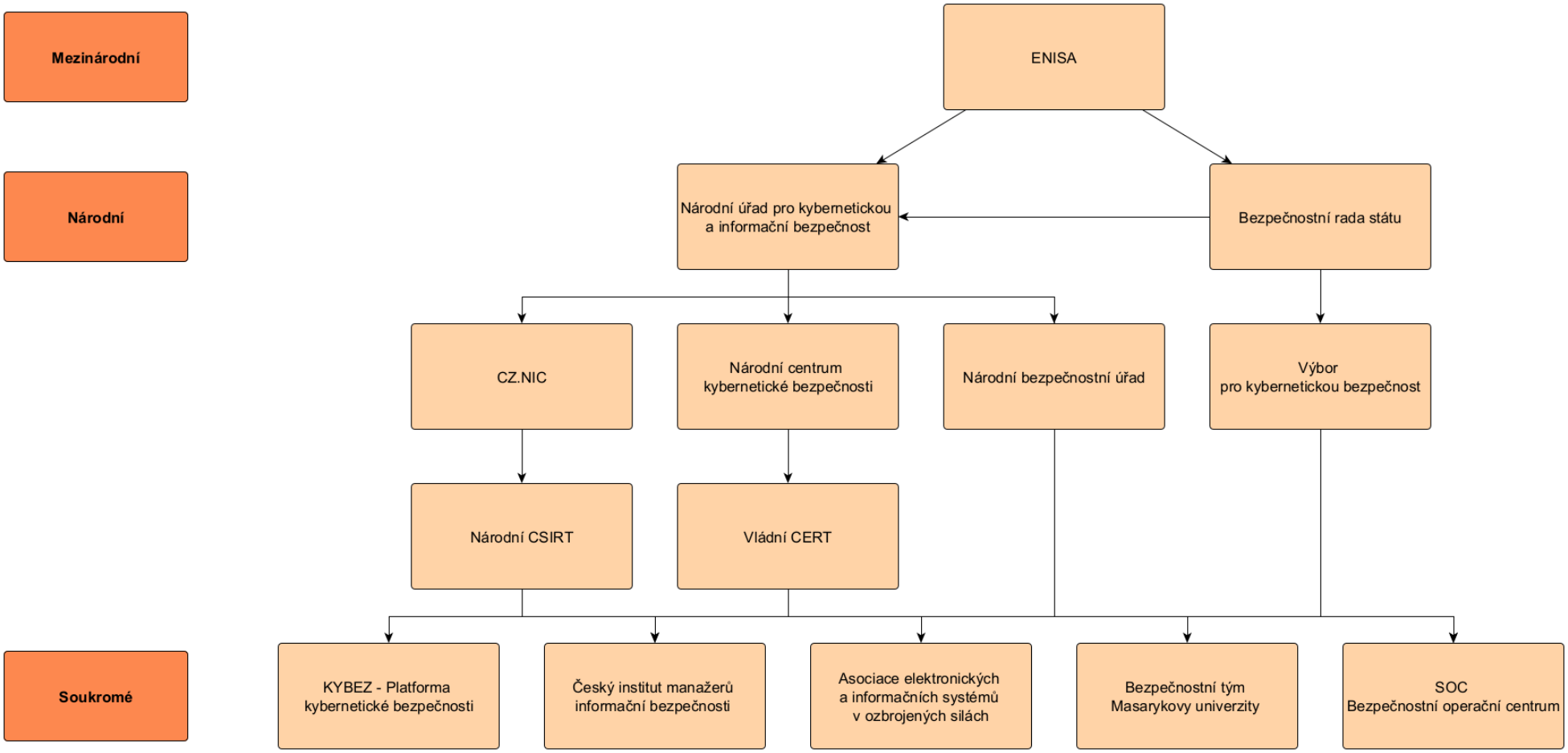
Poté následuje sekce národní, kde jsou organizace, které spadají pod stát. Vrcholovým orgánem, který zajišťuje kybernetickou bezpečnost pro ČR je Národní úřad pro kybernetickou a informační bezpečnost, který se zabývá kybernetickou bezpečností, kryptografickou ochranou a také ochranou utajovaných informací, ale i přes to, že je dalo by se říci hlavním orgánem v předmětné oblasti je v určitých mezích ovlivněn Bezpečnostní radou státu, která připravuje návrhy opatření k zajištění bezpečnosti a také koordinuje bezpečnost České republiky. Pod bezpečnostní radu státu spadá Výbor pro kybernetickou bezpečnost, který je jejím stálým pracovním orgánem a který koordinuje plánování opatření v předmětné oblasti.

Dále následují organizace, které spadají pod Národní úřad pro kybernetickou a informační bezpečnost a těmi jsou CZ.NIC, Národní centrum kybernetické bezpečnosti a Národní bezpečnostní úřad. I přesto, že CZ.NIC není vyloženě státní organizací, ale je sdružením právnických osob, které zabezpečují provoz domén nejvyšší úrovně .cz tak je zařazena do sekce národní, jelikož má také na starosti Národní CSIRT. Vládní CERT zajišťuje Národní centrum kybernetické bezpečnosti.

Poslední sekcí je sekce soukromá, kde jsou vybrané organizace, které nezřizuje stát, avšak stále jsou tyto organizace podřízené všem výše uvedeným organizacím.

Do této sekce spadají:

- Český institut manažerů informační bezpečnosti, který je sdružením pro informační a kybernetickou bezpečnost.
- KYBEZ – Platforma kybernetické bezpečnosti, která zajišťuje technologie a služby v odvětví informační a kybernetické bezpečnosti, obrany, systematické vzdělání apod.
- Asociace elektronických a informačních systémů v ozbrojených silách, která se zabývá rozvojem komunikačních a informačních technologií ozbrojených sil.
- Bezpečnostní tým Masarykovy univerzity, který si vytvořila sama Masarykova univerzita, aby si zajistila bezpečný kyberprostor.
- Poslední organizací, která je v modelu je SOC Bezpečnostní operační centrum, kterou je centralizovaná jednotka, která zajišťuje nepřetržitou analýzu a monitorování bezpečnostních incidentů a událostí.

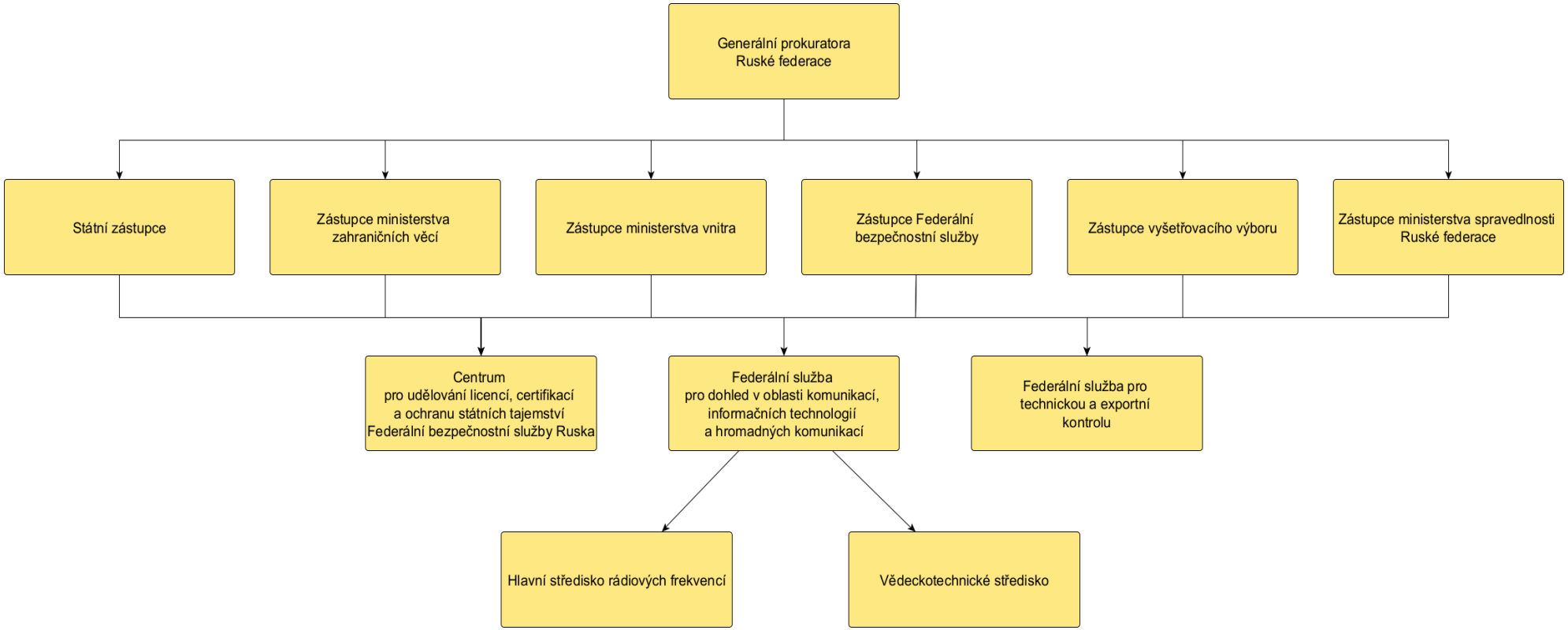


Obrázek 11 Struktura organizací a subjektů kybernetické bezpečnosti v České republice (Zdroj: vlastní)

Model struktury organizací a subjektů v Rusku

V Rusku to mají velmi odlišně zřízené oproti České republice. Jak je zmíněno v teoretické části Rusko nemá žádnou instituci, která by se vyloženě orientovala na kybernetickou bezpečnost. Generální prokuratura Ruské federace, která je v modelu struktury nadřazená všem, zřídila mezirezortní pracovní skupinu, do které spadají: Státní zástupce, Zástupce ministerstva zahraničních věcí, Zástupce ministerstva vnitra, Zástupce Federální bezpečnostní služby a Zástupce ministerstva spravedlnosti Ruské federace. Pod tyto všechny zástupce spadá:

- Centrum pro udělování licencí, certifikací a ochranu státních tajemství Federální bezpečnostní služby Ruska, které je hlavní jednotkou oprávněnou organizovat a provádět povolování činností podniků, institucí a organizací a podílí se na regulaci dovozu na území Ruska a vývozu mimo něj šifrovacích prostředků a speciálních technických prostředků určených k tajnému získávání informací.
- Federální služba pro dohled v oblasti komunikací, informačních technologií a hromadných komunikací, která má v pravomoci Hlavní středisko rádiových frekvencí a Vědeckotechnické středisko.
- Federální služba pro technickou a exportní kontrolu, která je výkonným orgánem, který zajišťuje bezpečnost kritické informační infrastruktury, ochranu informací obsahujících státní tajemství, jiné informace s omezeným přístupem, zabránění jejich úniku, neoprávněnému přístupu k nim, zvláštním vlivům na informace za účelem získat je, zničit je, zkreslit a zablokovat přístup k nim na území Ruské federace.



Obrázek 12 Struktura organizací a subjektů kybernetické bezpečnosti v Rusku (Zdroj: vlastní)

Model struktury organizací a subjektů v Německu

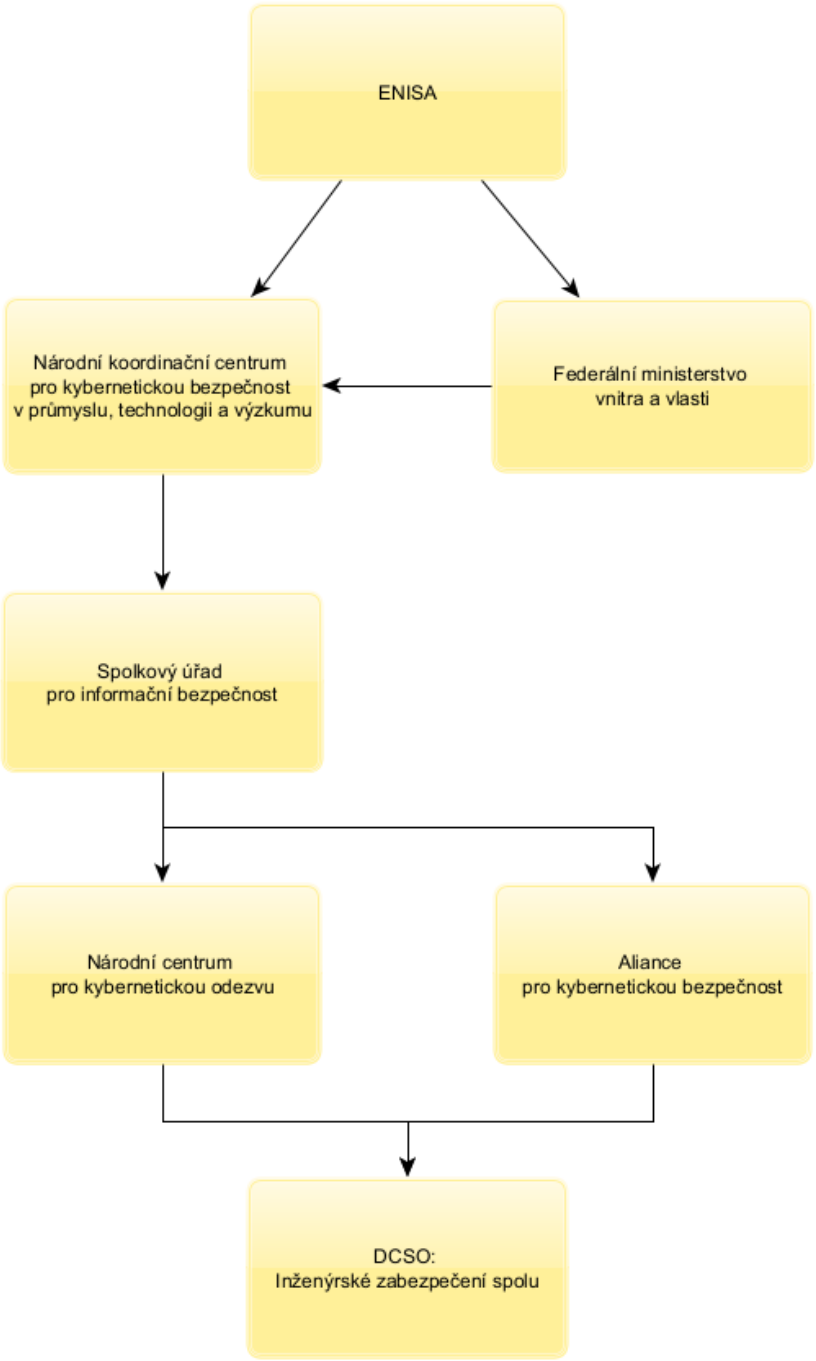
Německo to má podobně uzpůsobené jako Česká republika. Jelikož je Německo také v Evropské unii, proto je hlavičkou opět agentura ENISA, která v určitých mezí ovlivňuje Federální ministerstvo vnitra a vlasti. Na popud Evropské rady a Evropského parlamentu si Německo zvolilo vrcholovým orgánem pro kybernetickou bezpečnost Národní koordinační centrum pro kybernetickou bezpečnost v průmyslu, technologií a výzkumu. Jelikož toto centrum je ovlivněno Evropskou unií, je v modelu znázorněno přímo pod agenturou ENISA a současně je Národní koordinační centrum koordinováno Federálním ministerstvem vnitra a vlasti jehož rozsah sahá od civilní ochrany přes integraci a propagaci sportu až po bezpečnostní úkoly.

Poté následuje Spolkový úřad pro informační bezpečnost, který je federálním úřadem pro kybernetickou bezpečnost a tvůrcem bezpečné digitalizace v Německu, kde cílem je preventivní podpora informační a kybernetické bezpečnosti s cílem podporovat a umožnit bezpečné používání informačních a komunikačních technologií a ten spadá pod již zmíněné Národní koordinační centrum pro kybernetickou bezpečnost v průmyslu, technologií a výzkumu.

Pod všechny zmíněné organizace dále spadá:

- Národní centrum pro kybernetickou odezvu, které je meziagenturní a meziinstitucionální platformou, která má za cíl rychle vyměňovat relevantní informace mezi zúčastněnými orgány a partnery a koordinovat ochranná opatření k zajištění kybernetické bezpečnosti v Německu.
- Aliance pro kybernetickou bezpečnost, která poskytuje společnostem, sdružením, úřadům a organizacím platformu pro spolupráci a mohou tak vyměňovat informace o aktuálních hrozbách a praktických opatřeních v předmětné oblasti.

Všechny zmíněné organizace spadají pod stát, popřípadě pod Evropskou unii. Poslední organizací DCSO: Inženýrské zabezpečení spolu, které spojuje společnosti, vládní agentury, instituce a vytváří prostor pro důvěryhodnou výměnu mezi nimi, je soukromého charakteru, a právě proto je podřízená všem výše uvedeným institucím.



Obrázek 13 Struktura organizací a subjektů kybernetické bezpečnosti v Německu (Zdroj: vlastní)

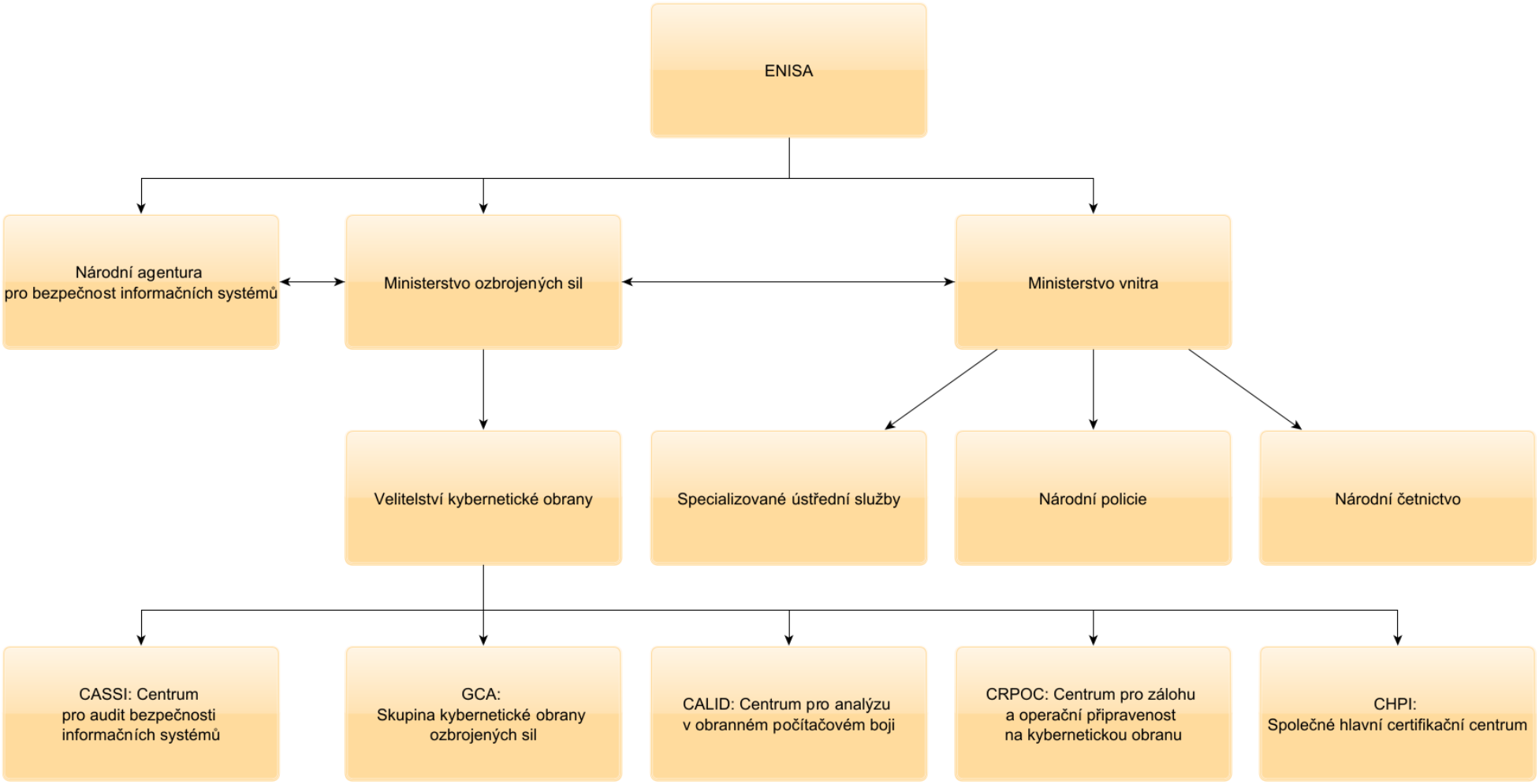
Model struktury organizací a subjektů ve Francii

Stejně jako u České republiky a Německa je hlavičkou modelu agentura ENISA. Vrcholovým orgánem pro kybernetickou bezpečnost je Národní agentura pro bezpečnost informačních systémů, která je národním orgánem pro kybernetickou bezpečnost a je zodpovědná za prevenci (včetně norem) a reakci na počítačové incidenty zaměřené na citlivé instituce. Ministerstvo ozbrojených sil, které zajišťuje ochranu sítí a integruje digitální boj do středu vojenských operací a ministerstvo vnitra, které bojuje proti všem formám kybernetické kriminality zaměřené na národní instituce. Tyto instituce taktéž ovlivňuje kybernetickou bezpečnost ve Francii, a právě proto jsou všechny tři instituce navzájem propojené, jelikož se navzájem doplňují a ovlivňují.

Pod ministerstvo ozbrojených sil spadá Velitelství kybernetické obrany, který chrání informační systémy armád a také se věnuje projektování, plánování a vedení vojenských operací v kyberprostoru. Ministerstvo vnitra, jelikož za účelem zjištění pachatele kybernetických útoků, prevenci či ke zvyšování informovanosti veřejnosti povolává specializované ústřední služby, národní policii nebo národní četnictvo, jsou taktéž uvedeny v modelu.

Pod Velitelství kybernetické obrany spadají subjekty či centra, které byly vytvořeny pro rozvoj v oblasti kybernetické obrany a těmi jsou:

- GCA: Skupina kybernetické obrany ozbrojených sil, jejíž cílem je upevnit kontinuitu mezi kybernetickou ochranou a obranou a podporuje spolupráce mezi těmito oblastmi.
- CALID: Centrum pro analýzu v obranném počítačovém boji, kterým je středisko sledování, detekce a varování ministerstva ozbrojených sil v oblasti kybernetické obrany.
- CASSI: Centrum pro audit bezpečnosti informačních systémů, které pokrývá dvě oblasti: bezpečnost informačních systémů a kompromitace falešných signálů.
- CRPOC: Centrum pro zálohu a operační připravenost na kybernetickou obranu, které stanovuje potřeby záložníků armád, ředitelství a služeb kybernetické obrany.
- CHPI: Společné hlavní certifikační centrum, které provádí bezpečnostní studie.



Obrázek 14 Struktura organizací a subjektů kybernetické bezpečnosti ve Francii (Zdroj: vlastní)

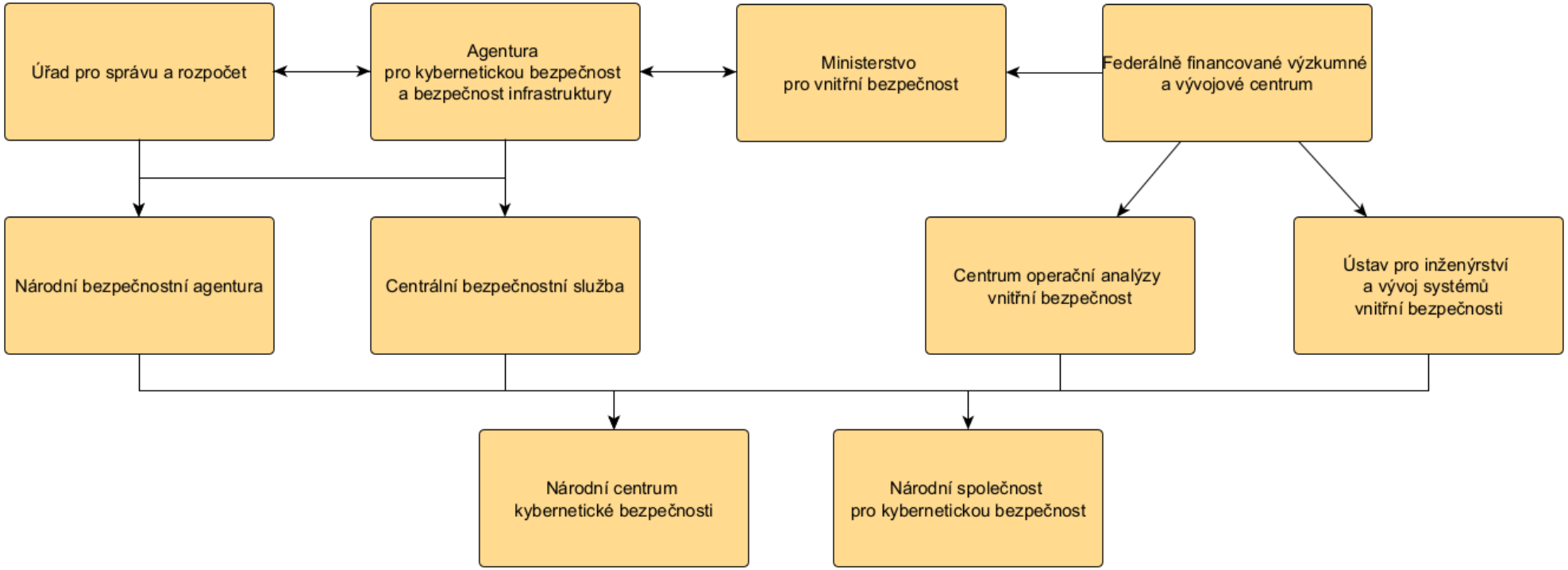
Model struktury organizací a subjektů ve Spojených státech amerických

Ve Spojených státech amerických se trošku liší zabezpečení kybernetické bezpečnosti od předchozích zemí. I z hlediska, že USA nepatří do Evropské unie, tak si veškeré ustanovení, organizace atd. řídí sama. Nejvíce významnými institucemi v předmětné oblasti je Agentura pro kybernetickou bezpečnost a bezpečnost infrastruktury, která je národním koordinátorem pro bezpečnost a odolnost kritické infrastruktury a také Úřad pro správu a rozpočet, které spolu úzce spolupracují. Další instituce, s kterou Agentura pro kybernetickou bezpečnost a bezpečnost infrastruktury spolupracuje je Ministerstvo pro vnitřní bezpečnost, které chrání národ před mnoha hrozbami, kterým čelí a kterému je zase napomáháno Federálně financovaným výzkumným a vývojovým centrem.

Centrum operační analýzy vnitřní bezpečnosti, které se zabývá různými studiemi o hrozbách, příležitostí pro vnitřní bezpečnost apod. a Ústav pro inženýrství a vývoj systémů vnitřní bezpečnosti, který působí v oblasti plánování a rozvoje vznikající hrozby, zkoumání konceptů, experimentování a hodnocení apod. Tyto dvě instituce spadají, pod již zmíněné Federálně financované výzkumné a vývojové centrum.

Pod Agenturu pro kybernetickou bezpečnost a bezpečnost infrastruktury a Úřad pro správu a rozpočet se řadí Národní bezpečnostní agentura, která primárně vede vládu USA v kryptologii a Centrální bezpečnostní služba, která poskytuje včasnou a přesnou kryptologickou podporu, znalosti a pomoc vojenské kryptologické komunitě.

Následující organizace, kterými jsou Národní centrum kybernetické bezpečnosti, které pomáhá veřejným i soukromým organizacím a jednotlivcům prostřednictvím školení, výzkumu a Národní společnost pro kybernetickou bezpečnost, která je zaměřená na poskytování vzdělávání, informovanosti a prosazování kybernetické bezpečnosti malým podnikům. Tyto dvě organizace jsou již neziskové a z tohoto důvodu podléhají všem výše uvedeným institucím.



Obrázek 15 Struktura organizací a subjektů kybernetické bezpečnosti ve Spojených státech amerických (Zdroj: vlastní)

5.2 CSIRT a CERT

Při zjišťování informací ohledně organizacích a subjektů kybernetické bezpečnosti bylo za vnímáno jisté nedorozumění až by se dalo říct jistý chaos mezi pojetím bezpečnostních týmů CSIRT a CERT. Někde bylo uvedeno, že to jsou totožné týmy jinde zas, že každý má na starosti něco jiného. Tato část praktické části bakalářské práce se bude zabývat rozdíly a ujasněním, jak to mezi týmy CSIRT a CERT je.

Ačkoli se termíny CERT a CIRT často zaměňují jako synonyma, existuje mezi nimi výrazný rozdíl, který je především v šíři a rozsahu povinností a odpovědnosti.

CERT

Působí v širším měřítku, a proto se obvykle skládá z vyhrazeného týmu zaměstnanců na plný úvazek. Působí jako partner s vládou, průmyslem a akademickou obcí s cílem zlepšit bezpečnost a odolnost počítačových systémů a sítí. CERT není určen pouze pro reakci na incidenty. Studuje problémy, které mají rozsáhlé důsledky pro kybernetickou bezpečnost, vyvíjí pokročilé metody a nástroje včetně nepřetržitého dohledu a analýzy sítě, ochrany perimetru a také zahrnuje různé disciplíny zajišťování informací v rámci týmu, které mohou, ale nemusí být nalezeny v omezeném CSIRT pomocí detekce narušení, analýza zranitelnosti, formulace zásad (Kabay; Moyle, 2021).

CERT upevňuje počítačovou bezpečnost, jelikož úzce spolupracuje s internetovou komunitou, aby usnadnila její reakci na události zabezpečení počítačů zahrnujících internetové hostitele, podnikla proaktivní kroky ke zvýšení povědomí komunity o problémech počítačové bezpečnosti například sdílením informací o identifikaci zranitelnosti, útoku a provedla výzkum zaměřený na zlepšení bezpečnosti stávajících systémů (Kabay).

CSIRT

Na rozdíl CSIRT ne vždy funguje v tak grandiózním měřítku, je používán mnoha externími organizacemi, malými někdy i velkými. Jelikož CSIRT je spíše menšího měřítka její provoz dobře funguje pro model malého podnikání, kde organizace nemá pracovní sílu ani zdroje potřebné k založení a financování rozsáhlého CERT. CSIRT se může skládat z omezených zaměstnanců na částečný úvazek nebo zaměstnanců s dodatečnou povinností, kteří plní své povinnosti CSIRT mimo své běžné pracovní povinnosti, a často pouze v případě incidentu (Kabay).

Ve srovnání s CERT je CSIRT mnohem obecnější. Je servisní organizace, která je zodpovědná za přijímání, kontrolu a reagování na hlášení a aktivity počítačových bezpečnostních incidentů. CSIRT často zaplňuje mezeru v mnoha menších, středních a decentralizovaných organizacích v oblasti reakce na incidenty a poskytuje informovanost, odborné znalosti a dohled nad obnovou. Jak je výše zmíněné CSIRT může v menší části doplňovat CERT v reakci na incidenty a v procesu zmírňování. Dalším úkolem CSIRT je udržovat zahraniční vztahy prostřednictvím světových komunit CERT/CSIRT týmů a také organizací, které tyto komunity podporují (Kabay).

Shrnutí rozdílů CERT a CIRT

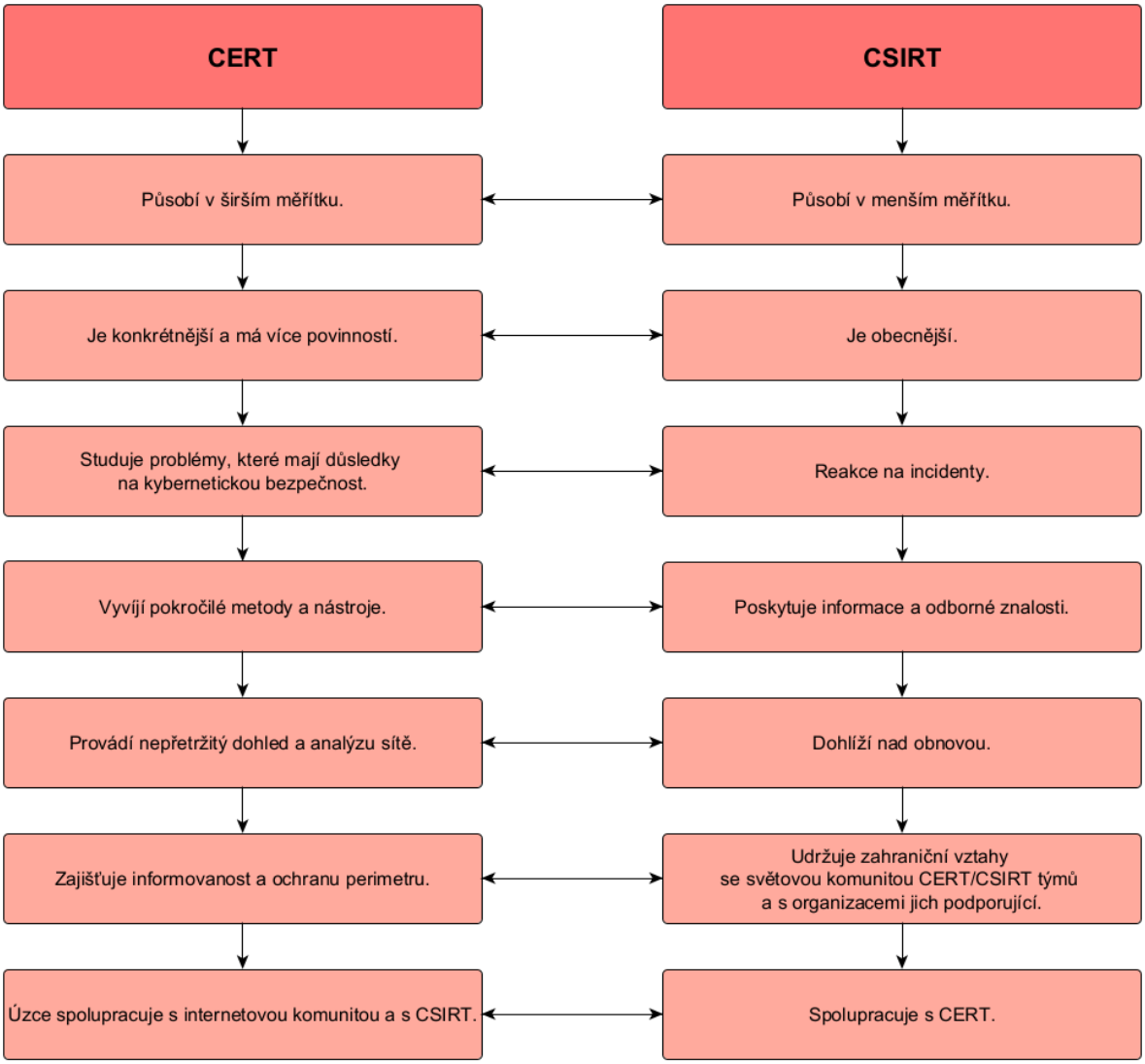
CERT

Působí v širším měřítku a je daleko konkrétnější. Má více povinností jako například studium problémů, které mají rozsáhlé důsledky pro kybernetickou bezpečnost, vyvíjení pokročilých metod a nástrojů, provádění nepřetržitého dohledu a analýzy sítě, zajišťování informovanosti a ochrany perimetru. Úzce spolupracuje s internetovou komunitou a s CSIRT.

CSIRT

Působí v menším měřítku a je obecnější. Mezi její povinnosti patří reakce na incidenty, poskytnutí informací a odborné znalosti, dohled nad obnovou. Udržuje zahraniční vztahy se světovou komunitou CERT/CSIRT týmů a s organizacemi jich podporující. Spolupráce s CERT.

V následujícím modelu jsou rozdíly přehledně zaznačeny.



Obrázek 16 Model s rozdíly mezi bezpečnostními týmy CERT a CSIRT
(Zdroj: Kabay; Moyle, 2021 – upraveno)

ZÁVĚR

Česká republika a zabezpečení kybernetické bezpečnosti je dalo by se říct ve středu. Není na tom nejhůř, ale určitě je co zlepšovat a důležitým krokem je se posunovat dopředu. V tomto případě je dobře, že je Česká republika součástí Evropské unie, která taktéž klade důraz na kybernetickou bezpečnost a udává různá ustanovení, které musí dodržovat všechny země, které do ní patří a tím zajišťuje, aby měly alespoň určité kybernetické zabezpečení. Na to navazuje Francie a Německo, které taktéž patří do Evropské unie a tím pádem mají strukturu organizací z určité části podobnou. Co se týče kybernetického zabezpečení v těchto dvou státech tak jsou na tom velmi dobře. S porovnáním Spojených států amerických a výše zmíněných zemí je z vlastního pohledu nejpřínosnější, když stát má jednu vrcholovou organizaci, která zaštiťuje kybernetickou bezpečnost a dodatečně ji doplňují další instituce.

U Ruska se nedá jednoznačně říct, jak na tom opravdu je, jelikož tím, jak je proslulé kybernetickými útoky z vlastního pohledu je nepravděpodobné, že by neměli organizace zajišťující vyloženě kybernetickou bezpečnost. I na základě toho, že bylo zjištěno že Rusko má vlastní internet, kde je značně hlídán obsah a upravuje se přístup k informacím dalo by se předpokládat, že upravují i informace, které jdou ven do světa, co se týče kybernetického zabezpečení.

Co se týče vlastního přínosu, tak je jednoznačně ve všeobecném přehledu současného stavu kybernetické bezpečnosti nejen v České republice, ale i v celosvětovém měřítku, výčtem jednotlivých organizací a která co zajišťuje a čím se zabývá, popřípadě na kterou organizaci se člověk může obrátit v případě problému apod. Dalším přínosem bakalářské práce je vymezení vztahů bezpečnostních týmů CSIRT a CERT, které jsou často zaměňovány a u kterých často není znám rozdíl.

SEZNAM POUŽITÉ LITERATURY

ABOUT CISA. CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY [online]. [cit. 2022-04-23]. Dostupné z: https://www.cisa.gov/about-cisa

About DHS. Homeland Security [online]. 2022, 04.05.2022 [cit. 2022-04-23]. Dostupné z: https://www.dhs.gov/about-dhs

About NSA/CSS. National Security Agency/Central Security Service [online]. [cit. 2022-04-23]. Dostupné z: https://www.nsa.gov/about/

AKČNÍ PLÁN NÁRODNÍ STRATEGIE KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY NA OBDOBÍ LET 2021-2025. Z: Národní úřad pro kybernetickou a informační bezpečnost, 2021, třetí. Dostupné také z: https://www.nukib.cz/download/publikace/strategie_akcni_plany/akcni_plan_2021-2025.pdf

Allianz für Cyber-Sicherheit: Viele Teilnehmer - ein starkes Netzwerk - ein Ziel. Bundesamt für Sicherheit in der Informationstechnik [online]. [cit. 2022-04-23]. Dostupné z: https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/home_node.html

BALSIGER, Jeannine. Stand der Cybersicherheit in Deutschland 2021. The State of Security: NEWS. TRENDS. INSIGHTS. [online]. 2021, 7. prosince 2021 [cit. 2022-04-20]. Dostupné z: https://www.tripwire.com/state-of-security/german/stand-der-cybersicherheit-in-deutschland-2021/

Bezpečnostní rada státu. VLÁDA ČESKÉ REPUBLIKY [online]. © 2009-2022 [cit. 2022-04-26]. Dostupné z: https://www.vlada.cz/cz/pracovni-a-poradni-organy-vlady/brs/brs-uvod-3851/

Bundesamt für Sicherheit in der Informationstechnik [online]. [cit. 2022-04-20]. Dostupné z: https://www.bsi.bund.de/DE/Home/home_node.html

Cloud Computing: Co to je a komu se vyplatí. Algotech [online]. 2020, 21. 04. 2020 [cit. 2022-04-07]. Dostupné z: https://www.algotech.cz/novinky/2020-04-21-cloud-computing-co-to-je-a-komu-se-vyplati

Computer modelling. Cambridge Business English Dictionary [online]. [cit. 2022-04-27]. Dostupné z: https://dictionary.cambridge.org/dictionary/english/computer-modelling

CZ.NIC: SPRÁVCE DOMÉNY CZ [online]. © 2022 [cit. 2022-04-07]. Dostupné z: https://www.nic.cz/

Česká pobočka AFCEA [online]. [cit. 2022-04-22]. Dostupné z: https://www.afcea.cz/

Český institut manažerů informační bezpečnosti. ČIMIB [online]. © 2022 [cit. 2022-04-22]. Dostupné z: https://www.cimib.cz/

Das Europäische Kompetenzzentrum für Cybersicherheit. Eine offizielle Website der Europäischen Union [online]. [cit. 2022-04-20]. Dostupné z: https://cybersecurity-centre.europa.eu/index_de

Das Nationales Cyber-Abwehrzentrum. Bundeskriminalamt [online]. © 2022 [cit. 2022-04-23]. Dostupné z: https://www.bka.de/DE/UnsereAufgaben/Kooperationen/NCAZ/ncaz_node.html

DHS Cybersecurity Strategy. Homeland Security [online]. [cit. 2022-04-25]. Dostupné z: https://www.dhs.gov/publication/dhs-cybersecurity-strategy

DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK. *ŘÍZENÍ KYBERNETICKÉ BEZPEČNOSTI A BEZPEČNOSTI INFORMACÍ*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.

Engineering Security. Together. DCSO [online]. [cit. 2022-04-23]. Dostupné z: https://www.dcso.de/en/

ENISA: EUROPEAN UNION AGENCY FOR CYBERSECURITY [online]. © 2005-2022 [cit. 2022-04-09]. Dostupné z: https://www.enisa.europa.eu/

Federally Funded Research and Development Centers. Science and Technology [online]. 2022, 10.02.2022 [cit. 2022-04-23]. Dostupné z: https://www.dhs.gov/science-and-technology/ffrdcs

Homeland Security Operational Analysis Center. Science and Technology [online]. 2022, 18.01.2022 [cit. 2022-04-23]. Dostupné z: https://www.dhs.gov/science-and-technology/hsoac

Homeland Security Systems Engineering and Development Institute. Science and Technology [online]. 2022, 18.01.2022 [cit. 2022-04-23]. Dostupné z: https://www.dhs.gov/science-and-technology/hssedi

CHANG, Jenny. 119 Impressive Cybersecurity Statistics: 2021/2022 Data & Market Analysis. FinancesOnline: REVIEWS FOR BUSINESS [online]. [cit. 2022-04-23]. Dostupné z: https://financesonline.com/cybersecurity-statistics/

Ing. SEDLÁK, Petr, Ing. Martin KONEČNÝ a a kolektiv. *KYBERNETICKÁ (NE)BEZPEČNOST: Problematika bezpečnosti v kyberprostoru*. Brno: CERM AKADEMICKÉ NAKLADATELSTVÍ, 2021. ISBN 978-80-7623-068-2.

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník Kybernetické bezpečnosti: Cyber Security Glossary [online]. Praha: Policejní akademie ČR v Praze a Česká pobočka AFCEA pod záštitou Národního centra kybernetické bezpečnosti České republiky, Národního bezpečnostního úřadu České republiky, 2015, Třetí aktualizované vydání, 242 [cit. 2022-04-17]. Dostupné z: https://www.nukib.cz/download/publikace/podpurne_materialy/vykladovy_slovnik_KB_3_vydani.pdf

KABAY, M.E. CERTs and CIRTs: homonyms but not synonyms, Part 1: The difference between CERTs and CIRTs. NETWORKWORLD [online]. [cit. 2022-05-05]. Dostupné z: https://www.networkworld.com/article/2328305/certs-and-cirts--homonyms-but-not-synonyms--part-1.html

KABAY, M.E. CERTs and CIRTs: homonyms but not synonyms, Part 2: Details on the differences between CERTs and CIRTs. NETWORKWORLD [online]. [cit. 2022-05-05]. Dostupné z: https://www.networkworld.com/article/2317581/certs-and-cirts--homonyms-but-not-synonyms--part-2.html

Kyberbezpečnostní tým Masarykovy univerzity [online]. Masarykova univerzita, © 2022 [cit. 2022-04-22]. Dostupné z: https://csirt.muni.cz/

La France et la cybersécurité. MINISTÈRE DES ARMÉES [online]. 2022, leden 2022 [cit. 2022-04-20]. Dostupné z: https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/lutter-contre-la-criminalite-organisee/la-france-et-la-cybersecurite/

Le commandement de la cyberdéfense: (COMCYBER). MINISTÈRE DES ARMÉES [online]. [cit. 2022-04-20]. Dostupné z: https://www.defense.gouv.fr/ema/commandement-cyberdefense-comcyber

ЛОБАЧ, Д.В. a Е.А. СМИРНОВА. Состояние кибербезопасности в России на современном этапе цифровой трансформации общества и становление национальной системы противодействия киберугрозам [online]. 2019, 29. listopadu 2019 [cit. 2022-04-20]. Dostupné z: doi:dx.doi.org/10.24866/VVSU/2073-3984/2019-4/023-032

LUKÁŠ, Luďěk a kolektiv. Konvergovaná bezpečnost. Zlín: Radim Bačuvčík-VeRBuM, 2019. ISBN 978-80-87500-99-6.

MAISNER, Martin a Barbora VLACHOVÁ. Zákon o kybernetické bezpečnosti: Komentář. Praha: Wolters Kluwer, 2015. ISBN 978-80-7478-817-8.

Ministerium. Bundesministerium des Innern und für Heimat [online]. © 2022 [cit. 2022-04-26]. Dostupné z: https://www.bmi.bund.de/DE/ministerium/ministerium-node.html

MOYLE, Ed. CERT vs. CSIRT vs. SOC: What's the difference?. TechTarget: SearchSecurity [online]. 2021, v březnu 2021 [cit. 2022-05-05]. Dostupné z: https://www.techtarget.com/searchsecurity/tip/CERT-vs-CSIRT-vs-SOC-Whats-the-difference

Národní bezpečnostní úřad [online]. Praha 5 [cit. 2022-04-18]. Dostupné z: https://www.nbu.cz/cs/

Národní úřad pro kybernetickou a informační bezpečnost [online]. [cit. 2022-04-05]. Dostupné z: https://nukib.cz/cs/

NÁRODNÍ STRATEGIE KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY NA OBDOBÍ LET 2021-2025. z: Národní úřad pro kybernetickou a informační bezpečnost, 2020, třetí. Dostupné také z: https://nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

NCC [online]. [cit. 2022-04-23]. Dostupné z: https://cyber-center.org/

ОБЩАЯ ИНФОРМАЦИЯ. ЦЕНТР ПО ЛИЦЕНЗИРОВАНИЮ, СЕРТИФИКАЦИИ И ЗАЩИТЕ ГОСУДАРСТВЕННОЙ ТАЙНЫ ФСБ РОССИИ [online]. © 1999–2022 [cit. 2022-04-25]. Dostupné z: http://clsz.fsb.ru/

O nás: KYBEZ je platforma pro efektivní spolupráci akademických institucí a komerčních firem. KYBEZ [online]. [cit. 2022-04-22]. Dostupné z: https://www.kybez.cz/o-nas/

Organization Structure. ScienceDirect [online]. © 2022 [cit. 2022-04-27]. Dostupné z: https://www.sciencedirect.com/topics/computer-science/organization-structure

ПОЗДЕЕВА, Екатерина. Кибербезопасность в России. ФИНАМ [online]. 2021, 15. září 2021 [cit. 2022-04-20]. Dostupné z: https://www.finam.ru/analysis/newsitem/kiberbezopasnost-v-rossii-20210915-183242/

ПУТИН, Владимир. Положение о Роскомнадзоре. ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ [online]. 2009, 16. března 2009 [cit. 2022-04-25]. Dostupné z: https://rkn.gov.ru/about/

RAK, Jakub. Informační podpora ukrytí obyvatelstva: Information support of population sheltering. Zlín, 2017. Disertační práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky. Vedoucí práce Prof. Ing. Dušan Vičar, CSc.

ŠULC, Vladimír. KYBERNETICKÁ BEZPEČNOST. Plzeň: Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

Указ Президента РФ от 16.08.2004 N 1085 (ред. от 08.12.2021) "Вопросы Федеральной службы по техническому и экспортному контролю" (Выписка). КонсультантПлюс: надежная правовая поддержка [online]. Moskva, 2021, 8. prosince 2021 [cit. 2022-04-25]. Dostupné z: http://www.consultant.ru/document/cons_doc_LAW_14031/9b13a25cec35f1d26a1331611204f68c696b5c53/

Утверждена Стратегия национальной безопасности России. RUБЕЖ: Информационно-аналитический журнал [online]. 5. července 2021 [cit. 2022-04-25]. Dostupné z: https://ru-bezh.ru/gossektor/news/21/07/05/utverzhdena-strategiya-naczionalnoj-bezopasnosti-rossii

Virtuální privátní síť. *LANPROCOM: Local Area Network Professional Communication* [online]. Brno, © 2022 [cit. 2022-03-31]. Dostupné z: http://www.lanpro.cz/sofistikovana-reseni/virtualni-privatni-sit/

Výbor pro kybernetickou bezpečnost. *VLÁDA ČESKÉ REPUBLIKY* [online]. © 2009-2022 [cit. 2022-04-07]. Dostupné z: https://www.vlada.cz/cz/ppov/brs/pracovni-vybory/kyberneticka_bezpecnost/vybor-pro-kybernetickou-bezpecnost-159932/

WATTERS, Ashley. Top 50 Cybersecurity Statistics, Figures and Facts. CompTIA [online]. 2022, 11. ledna 2022 [cit. 2022-04-23]. Dostupné z: https://connect.comptia.org/blog/cyber-security-stats-facts

Who We Are. The National Cybersecurity Society [online]. © 2022 [cit. 2022-04-23]. Dostupné z: https://nationalcybersecuritysociety.org/who-we-are/

Zákon č. 110/2019 Sb.: Zákon o zpracování osobních údajů. Z: 2019. Dostupné také z: https://www.zakonyprolidi.cz/cs/2019-110

Zákon č. 412/2005 Sb.: Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti. Z: 2005. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-412/zneni-20220201

Ziele für die Cybersicherheit beschlossen. Die Bundesregierung [online]. 2021, 8. září 2021 [cit. 2022-04-20]. Dostupné z: https://www.bundesregierung.de/breg-de/aktuelles/neue-cybersicherheitsstrategie-1958144

ZPRÁVA O STAVU KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY ZA ROK 2020 [online]. Národní úřad pro kybernetickou a informační bezpečnost, 2021, 26.07.2021 [cit. 2022-04-17]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf

7 statistiques sur la cybersécurité en France. Ndnm [online]. 2021, 21. února 2021 [cit. 2022-04-21]. Dostupné z: https://www.ndnm.fr/statistiques-cybersecurite/

SEZNAM OBRÁZKŮ