POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostního managementu

Katedra krizového řízení

Hodnocení způsobů ochrany prvků kritické infrastruktury s důrazem na elektronickou ochranu a kyberbezpečnost

Bakalářská práce

Evaluation of methods of protection of critical infrastructure elements with emphasis on electronic protection and cybersecurity

Bachelor thesis

VEDOUCÍ PRÁCE
Ing. Lubomír POLÍVKA

AUTOR PRÁCE
Tomáš FOLLPRECHT

PRAHA

2024

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Novém Strašecí, dne 11.3. 2024

Tomáš Follprecht

Poděkování

Tímto bych rád poděkoval panu Ing. Lubomíru Polívkovi za cenné rady a věcné připomínky, které přispěly ke zpracování mé práce.

ANOTACE

Bakalářská práce se zabývá problematikou ochrany prvků kritické infrastruktury s důrazem na jejich elektronickou ochranu a kybernetickou bezpečnost. Teoretická část je zaměřena na charakteristiku kritické infrastruktury, prvků kritické infrastruktury a jejich ochranu. Je zde uvedena související legislativa a dokumenty. Dále je v teoretické části popsána kybernetická bezpečnost, související základní pojmy v oblasti kybernetické bezpečnosti a jsou zde charakterizovány typy kybernetických útoků, legislativní rámec, aktéři působící v kyberbezpečnosti a dokumenty řešící kyberbezpečnost. Praktická část se věnuje způsobu zajištění kyberbezpečnosti prvku v rámci organizace a návrhu na zdokonalení kybernetické bezpečnosti. Na závěr je uvedeno zhodnocení na základě získaných poznatků.

KLÍČOVÁ SLOVA

kritická infrastruktura * prvek kritické infrastruktury * ochrana prvků kritické infrastruktury * kybernetická bezpečnost * kybernetický útok * elektronická ochrana

ANOTATION

The bachelor thesis deals with protection of critical infrastructure elements with emphasis on their electronic protection and cyber security. The theoretical part is focused on the characteristics of critical infrastructure, critical infrastructure elements and their protection. Related legislation and documents are presented. Furthermore, the theoretical part describes cybersecurity, the related basic concepts in the field of cybersecurity and characterises the types of cyber attacks, the legislative framework, the actors involved in cybersecurity and documents addressing cybersecurity. The practical part focuses on how to ensure the cybersecurity elements to cybersecurity. Finally, an evaluation based on the lessons learned is presented.

KEYWORDS

critical infrastructure * critical infrastructure * critical infrastructure element * protection of critical infrastructure elements * cybersecurity * cyber attack * electronic protection

Obsah

Úvod

Kritická infrastruktura představuje základní služby, které jsou zásadní pro celou společnost a její fungování. Zahrnuje klíčová odvětví jako je energetika, doprava, zdravotní péče, digitální infrastruktura a další.

V dnešní době, kdy je společnost z velké části závislá na informačních a komunikačních technologiích, se problematika kybernetické bezpečnosti stala nedílnou součástí ochrany kritické infrastruktury. S neustále se zvyšující vzájemnou propojeností s digitálním světem čelí kritická infrastruktura kybernetickým hrozbám, které mohou ohrozit nejen její plynulý provoz, ale i způsobit zkázu v celé společnosti.

Tato bakalářská práce se zaměřuje na hodnocení způsobů ochrany prvků kritické infrastruktury s důrazem na elektronickou ochranu a kyberbezpečnost. Cílem práce je zhodnotit, jakým způsobem jsou chráněny prvky kritické infrastruktury z pohledu kybernetické bezpečnosti.

1. Kritická infrastruktura

Pojem infrastruktura obecně označuje množinu strukturálních prvků, které jsou navzájem propojené a zachovávají potom celou strukturu jako takovou pospolu. Většinou se tento pojem využívá výhradně pro struktury, které vznikají uměle. Výraz infrastruktura má různé významy v závislosti na kontextu a oboru, ve kterém se používá; pravděpodobně nejvíce se využívá v oblasti ekonomie ve smyslu popisu fyzické infrastruktury, kam se řadí např. silnice nebo budovy. Infrastruktura se zřizuje buďto státem nebo v rámci soukromého sektoru.[1] V každé společnosti je část infrastruktury, která je zásadní pro její správný chod. „*Tato infrastruktura se označuje jako životně důležitá, resp. kritická*.“[2]

Definic, které popisují kritickou infrastrukturu, je více a během let se postupně vyvíjely. V České republice byl v minulosti roku 2003 usnesením Výboru pro civilní nouzové plánování stanoven pojem kritické infrastruktury jako „*vybraná výrobní, nevýrobní, telekomunikační a dopravní zařízení a objekty, bez ohledu na vlastnický vztah, pomocí kterých jsou za krizových stavů naplňovány základní funkce státu*.“[3] V zahraničí v období přelomu století byla KI popsána jako „*fyzické a kybernetické systémy, které jsou nutné pro zajištění minimálního chodu ekonomiky a správy státu“*, a to především v odvětvích telekomunikace, energetiky, bankovnictví a financí, dopravy, systémů zásobování vodou a nouzových složek v rámci státního a soukromého sektoru.[4]

Zatím stále aktuální a platná definice na národní úrovni vychází ze zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon). Tento zákon konkrétně „*stanoví působnost a pravomoc státních orgánů a orgánů územních samosprávných celků a práva a povinnosti právnických a fyzických*

[1] ŠENOVSKÝ, Michal, Pavel ŠENOVSKÝ a Vilém ADAMEC. *Ochrana kritické infrastruktury*. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2007. 5 s. ISBN 978-80-735-025-8.
[2] ŠENOVSKÝ, Michal, Pavel ŠENOVSKÝ a Vilém ADAMEC. *Ochrana kritické infrastruktury.* Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2007. 46 s. ISBN 978-80-735-025-8.
[3] *Modul G – vnitřní bezpečnost a veřejný pořádek a vybrané kapitoly krizového řízení: studijní text k problematice bezpečnosti zpracované dle Koncepce z roku 2004* [online]. Ministerstvo vnitra: odbor bezpečnosti, Praha – aktualizace 2014 [cit. 5.3.2024]. Dostupné z: https://www.hzscr.cz/clanek/moduly-studijni-texty-k-problematice-bezpecnosti-zpracovane-dle-koncepce-z-roku-2004.aspx
[4] ŠENOVSKÝ, Michal, Pavel ŠENOVSKÝ a Vilém ADAMEC. *Ochrana kritické infrastruktury.* Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2007. 47 s. ISBN 978-80-735-025-8.

osob při přípravě na krizové situace, které nesouvisejí se zajišťováním obrany České republiky před vnějším napadením, a při jejich řešení a při ochraně kritické infrastruktury a odpovědnost za porušení těchto povinností." Dle krizového zákona se kritickou infrastrukturou rozumí „*prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, jehož narušení by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu*." [5]

V krizovém zákoně jsou uvedeny definice základních pojmů v kritické infrastruktuře. V tomto smyslu se rozumí:

- „***Evropskou kritickou infrastrukturou*** *kritická infrastruktura na území České republiky, jejíž narušení by mělo závažný dopad i na další členské státy Evropské unie;*
- ***Prvkem kritické infrastruktury*** *zejména stavba, zařízení, prostředek nebo veřejná infrastruktura, určené podle průřezových a odvětvových kritérií; je-li prvek kritické infrastruktury součástí evropské kritické infrastruktury, považuje se za prvek evropské kritické infrastruktury;*
- ***Subjektem kritické infrastruktury*** *provozovatel prvku kritické infrastruktury; je-li prvek kritické infrastruktury součástí evropské kritické infrastruktury, považuje se tento za subjekt evropské kritické infrastruktury;*
- ***Ochranou kritické infrastruktury*** *opatření zaměřená na snížení funkce prvku kritické infrastruktury."* [6]

1.1 Prvky kritické infrastruktury

Pod pojmem prvek KI je zahrnuta kromě stavby, zařízení nebo prostředku rovněž veřejná infrastruktura, která je popsána ve stavebním zákoně č. 183/2006 Sb., o územním plánování a stavebním řádu. Na základě tohoto zákona veřejná infrastruktura představuje dopravní infrastrukturu, technickou infrastrukturu, občanské vybavení a veřejné prostranství. [7]

[5] Zákon č. 240/2000 Sb., *o krizovém řízení v posledním znění*
[6] Zákon č. 240/2000 Sb., *o krizovém řízení v posledním znění*
[7] Zákon č. 183/2006 Sb., *o územním plánování a stavebním řádu ve znění k 31.12.2023*

Prvky kritické infrastruktury se určují podle nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, a to na základě průřezových a odvětvových kritérií, která musí být splněna k tomu, aby se daný prvek mohl zařadit mezi kritickou infrastrukturu.

Průřezová kritéria jsou navrhovány Ministerstvem vnitra ČR a označují „*soubor hledisek pro posuzování závažnosti vlivu narušení funkce prvku kritické infrastruktury s mezními hodnotami*." Průřezovým kritériem pro určení prvku KI je hledisko:

- *„obětí s mezní hodnotou více než 250 mrtvých nebo více než 2500 osob s následnou hospitalizací po dobu delší než 24 hodin,*
- *ekonomického dopadu s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu, nebo*
- *dopadu na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125000 osob*." [8]

Odvětvová kritéria jsou „*technické nebo provozní hodnoty k určování prvků kritické infrastruktury*." Navrhují je ministerstva a jiné ústřední správní úřady a tyto návrhy pak předkládají Ministerstvu vnitra.[9] Nařízení vlády č. 315/2014 Sb., nařízení vlády, kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvků kritické infrastruktury definuje odvětvová kritéria v následujících odvětvích a pododvětvích:

- **Energetika** – elektřina, zemní plyn, ropa a ropné produkty, centrální zásobování teplem;
- **Vodní hospodářství**;
- **Potravinářství a zemědělství** – rostlinná výroba, živočišná výroba, potravinářská výroba;
- **Zdravotnictví** – zdravotnické zařízení, jehož celkový počet akutních lůžek je nejméně 2500;

[8] Nařízení vlády č. 432/2010 Sb., *o kritériích pro určení prvku kritické infrastruktury v posledním znění*
[9] Zákon č. 240/2000 Sb., *o krizovém řízení v posledním znění*

- **Doprava** – silniční doprava, železniční doprava, letecká doprava, vnitrozemská vodní doprava;
- **Komunikační a informační systémy** – technologické prvky pevné sítě elektronických komunikací, technologické prvky mobilní sítě a elektronických komunikací, technologické prvky sítí pro rozhlasové a televizní vysílání, technologické prvky pro satelitní komunikaci, pro poštovní služby, technologické prvky informačních systémů, oblast kybernetické bezpečnosti;
- **Finanční trh a měna**;
- **Nouzové služby** – integrovaný záchranný systém, radiační monitorování, předpovědní, varovná a hlásná služba, vnitřní bezpečnost;
- **Veřejná správa** – veřejné finance, sociální ochrana a zaměstnanost, zpravodajské služby, ostatní státní správa. [10]

U procesu určování prvků KI se rozlišuje jejich provozovatel. Tím jsou státní instituce nebo soukromé subjekty.[11]

[10] Nařízení vlády č. 315/2014 Sb., *kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury v posledním znění*

[11] *Mvcr.cz: Ochrana kritické infrastruktury* [online]. [cit.6.2.2024]. Dostupné z: https://www.mvcr.cz/chh/clanek/ochrana-kriticke-infrastruktury-ochrana-kriticke-infrastruktury.aspx

2. Ochrana kritické infrastruktury

Subjekt KI, tedy provozovatel KI, je odpovědný za ochranu KI. Na základě účelu ochrany je dle krizového zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) tento subjekt povinen:

- *„vypracovat plán krizové připravenosti subjektu kritické infrastruktury do jednoho roku od rozhodnutí vlády nebo ode dne nabytí právní moci, kterým byl prvek kritické infrastruktury určen*;
- *umožnit příslušnému ministerstvu nebo jinému ústřednímu správnímu úřadu vykonání kontroly plánu krizové připravenosti subjektu kritické infrastruktury a ochrany prvku kritické infrastruktury včetně umožnění vstupů a vjezdů na pozemky a do prostorů, ve kterých se tento prvek nachází;*
- *oznámit příslušnému ministerstvu nebo jinému ústřednímu správnímu úřadu bez zbytečného odkladu informace o trvalém zastavení provozu, ukončení činnosti, nebo restrukturalizaci.“* [12]

Plán krizové připravenosti subjektu KI vychází ze zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon). V tomto plánu je popsána identifikace možných ohrožení funkce prvku KI a jsou zde stanoveny opatření týkající se jeho ochrany. Je složen ze tří částí – základní, operativní a pomocné. [13]

Do ochrany KI je krizovým zákonem zařazena rovněž Česká národní banka, která v rámci ochrany KI zajišťuje tyto činnosti:

- *„navrhuje odvětvová kritéria a předkládá je Ministerstvu vnitra,*
- *vyžaduje od právnické nebo podnikající fyzické osoby informace nezbytné k určení prvku kritické infrastruktury včetně údajů, u kterých je nutné zachovat mlčenlivost, pokud požadované informace nelze zajistit jiným způsobem,*

[12] Zákon č. 240/2000 Sb., *o krizovém řízení v posledním znění*

[13] *Mvcr.cz: Ochrana kritické infrastruktury* [online]. [cit.6.2.2024]. Dostupné z: https://www.mvcr.cz/chh/clanek/ochrana-kriticke-infrastruktury-ochrana-kriticke-infrastruktury.aspx

- *určí opatřením obecné povahy prvky kritické infrastruktury a prvky evropské kritické infrastruktury a o tomto určení informuje bez zbytečného odkladu Ministerstvo vnitra včetně uvedení údaje o počtu členských státům, které jsou závislé na určených prvcích evropské kritické infrastruktury, nebo zašle návrhy prvků kritické infrastruktury a prvků evropské kritické infrastruktury Ministerstvu vnitra k zařazení do seznamu podle § 10 odst. 1 písm. f); návrhy prvků evropské kritické infrastruktury obsahují též informaci o počtu členských států, které jsou závislé na jednotlivých prvcích evropské kritické infrastruktury,*
- *kontroluje plány krizové připravenosti subjektů kritické infrastruktury a ochranu prvků kritické infrastruktury a ukládá opatření k nápravě nedostatků zjištěných při kontrole.“* [14]

2.2 Vývoj ochrany kritické infrastruktury v EU

V červnu roku 2004 Evropská rada projevila žádost vůči Evropské komisi, aby navrhla souhrnnou strategii zaměřenou na ochranu evropských kritických infrastruktur. Na to Komise zareagovala „*Sdělením o ochraně kritické infrastruktury v boji proti terorismu.“* V tomto sdělení byly obsaženy návrhy týkající se zvýšení evropské prevence, připravenosti a odezvy v souvislosti s teroristickými útoky, jež zahrnovaly KI.

Následovala komplexní přípravná fáze, ve které došlo k vydání Zelené knihy o Evropském programu na ochranu kritické infrastruktury a proběhla porada mezi subjekty z veřejného a soukromého sektoru.

Poté byly uvedené návrhy přeměněny do souhrnu strategických opatření s názvem Evropský program na ochranu kritické infrastruktury (EPCIP). Roku 2006 došlo k jeho schválení komisí.

Prvotní záměr směrovaný na prevenci, připravenost a odezvu na teroristické útoky se zformuloval na komplexní přístup k rizikům. Primární cíl programu obecně spočíval ve zdokonalení ochrany KI v EU tak, aby byl zajištěn odpovídající

[14] Zákon č. 240/2000 Sb., *o krizovém řízení v posledním znění*

a shodný stupeň ochrany KI a aby došlo k minimalizaci jednotlivých bodů výpadků a k zajištění pohotových a osvědčených opatření obnovy napříč EU. Evropský program na ochranu kritické infrastruktury posloužil jako základ pro vznik Směrnice Rady č. 2008/114/ES, která zavedla postup pro „*určování a označování evropských kritických infrastruktur a o posouzení zvýšit jejich ochranu*.“[15]

Směrnice byla implementována do vnitrostátního práva ČR, konkrétně došlo ke změně zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), která vstoupila v platnost v roce 2011.

Následující rok proběhlo přezkoumání této směrnice, na jejíž základě došlo ke zjištění několika nedokonalostí a vzhledem k úsudku komplexního posouzení bezpečnostní politiky EU z roku 2017 Evropská komise rozhodla o zahájení vyhodnocení směrnice, které mělo vzít v úvahu tehdejší hrozby, u nichž mohlo dojít k ohrožení ochrany KI v EU. Ve spojitosti s tímto stanoviskem došlo ke konci roku 2018 k zahájení tzv. veřejné konzultace.

Prostřednictvím konzultace získala Evropská komise pohled na uvedenou problematiku od veřejných, nevládních a soukromých subjektů a organizací, kterých se tato oblast dotýkala nebo byla v jejich zájmu. V souvislosti s výsledkem zmíněné konzultace došlo dne 18. prosince 2020 k návrhu směrnice o posílení kritických subjektů (tzv. směrnice CER).[16]

Tato směrnice byla následně vydána Evropským parlamentem a Radou Evropské unie dne 14. prosince 2022 a souhrnným názvem je označována jako Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a zrušení směrnice Rady 2008/114/ES. Směrnice tak nahradila výše zmíněnou původní Směrnici Rady 2008/114 ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu. K nabytí účinku směrnice 2022/2557 došlo dne 16.

[15] BLAŽKOVÁ, Kateřina a kol. *Ochrana obyvatelstva a krizové řízení* [online]. 1. vydání. Praha: MV – generální ředitelství Hasičského záchranného sboru ČR, 2015. ISBN 978-80-86466-62-0.
[16] *Hzscr.cz: Evropský program na ochranu kritické infrastruktury* [online]. [cit.6.2.2024]. Dostupné z: https://www.hzscr.cz/clanek/evropsky-program-na-ochranu-kriticke-infrasruktury.aspx

ledna 2024 a zavádí nová závazná pravidla za účelem zvýšení ochrany kritické infrastruktury pro státy, které jsou součástí EU. [17]

Směrnice CER

V kapitole I této směrnice jsou uvedena obecná ustanovení, ve kterých je v článku 1 vymezen předmět a oblast působnosti, na jehož základě směrnice:

- *„Stanovuje členským státům povinnosti přijmout konkrétní opatření, jejichž cílem je zajistit, aby služby nezbytné pro zachování nejdůležitějších společenských funkcí nebo hospodářských činností v rámci působnosti článku 114 Smlouvy o fungování EU byly na vnitřním trhu poskytovány neomezeně, zejména povinnosti určit kritické subjekty při plnění povinností, které jim byly uloženy;*
- *Stanovuje povinnosti pro kritické subjekty zaměřené na posílení jejich odolnosti a schopnosti poskytovat služby podle písmena a) na vnitřním trhu;*
- *Stanovuje pravidla pro:*
    - *dohled nad kritickými subjekty;*
    - *vymáhání;*
    - *určení kritických subjektů zvláštního evropského významu a poradní komise za účelem posouzení opatření, která takové subjekty zavedly za účelem splnění jejich povinností podle kapitoly III;*
- *Stanovuje společné postupy pro spolupráci a podávání zpráv o uplatňování této směrnice;“* [18]

Směrnicí zároveň „*není dotčena odpovědnost členských států za ochranu národní bezpečnosti a obranu, ani jejich pravomoc chránit jiné základní funkce státu, včetně zajištění územní celistvosti státu a zachování veřejného pořádku a nevztahuje se na subjekty veřejné správy, které vykonávají své činnosti v oblasti*

[17] Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022, *o odolnosti kritických subjektů a zrušení směrnice Rady 2008/114/ES*.
[18] Směrnice Evropského parlamentu a Rady (EU) 2022/2557, *o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES*

národní bezpečnosti, veřejné bezpečnosti, obrany nebo prosazování práva, včetně odhalování a stíhání trestných činů.“[19]

V článku 2 jsou obsaženy definice pojmů, se kterými směrnice pracuje. Pro tyto účely se rozumí:

- „***kritickým subjektem*** *veřejný nebo soukromý subjekt, který byl členským státem určen v souladu s článkem 6 jako subjekt náležející do jedné z kategorií stanovených ve třetím sloupci tabulky v příloze*;
- ***odolností*** *schopnost kritického subjektu předcházet incidentům, chránit se před těmito incidenty, reagovat na ně, odolávat jim, zmírňovat a absorbovat je, přizpůsobovat se jim a zotavit se z nich*;
- ***incidentem*** *událost, která může významně narušit nebo která narušuje poskytování základní služby, včetně případů, kdy ovlivňuje vnitrostátní systémy chránící právní stát*;
- ***kritickou infrastrukturou*** *aktivum, zařízení, vybavení, síť nebo systém či část aktiva, zařízení, vybaven, sítě nebo systému, které jsou nezbytné pro poskytování základní služby*;
- ***základní službou*** *služba, která je zásadní pro zachování nejdůležitějších společenských funkcí, hospodářských činností, veřejného zdraví a bezpečnosti nebo životního prostředí*;
- ***rizikem*** *možnost ztráty nebo narušení v důsledku incidentu, přičemž toto riziko má být vyjádřeno jako kombinace rozsahu takové ztráty nebo takového narušení a pravděpodobnosti vzniku incidentu*;
- ***posouzením rizik*** *celkový postup určení povahy a rozsahu rizika identifikací a analýzou možných relevantních hrozeb, zranitelných míst a nebezpečí, které by mohly vést k incidentu, a hodnocením možné ztráty nebo narušení poskytování základní služby způsobené tímto incidentem.“* [20]

[19] Směrnice Evropského parlamentu a Rady (EU) 2022/2557, *o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES*
[20] Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince, *o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES*

Kritické subjekty mají členské státy určovat na základě těchto odvětví, pododvětví a dále jednotlivých kategorií, která jsou uvedena v příloze směrnice:

- Energetika
    - elektřina
    - dálkové vytápění a chlazení
    - ropa
    - zemní plyn
    - vodík
- Doprava
    - letecká doprava
    - železniční doprava
    - vodní doprava
    - silniční doprava
    - veřejná přeprava
- Bankovnictví
- Infrastruktura finančních trhů
- Zdraví
- Pitná voda
- Odpadní voda
- Digitální infrastruktura
- Subjekty veřejné správy
- Vesmír
- Výroba, zpracování a distribuce potravin[21]

Členské státy jsou povinny určit kritické subjekty pro uvedená odvětví a pododvětví konkrétně do 17. července 2026. V rámci určení kritických subjektů „*každý členský stát vytvoří seznam určených kritických subjektů a zajistí, aby tyto kritické subjekty byly informovány o tom, že byly určeny jakožto kritické subjekty do jednoho měsíce od tohoto určení.*“[22] Tento seznam mají státy v případě potřeby

[21] Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022, *o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES*
[22] Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022, *o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES*

a vždy alespoň každé čtyři roky přezkoumat a případně aktualizovat. Kritické subjekty, které jsou v odvětvích bankovnictví, infrastruktury finančních trhů a digitální infrastruktury, „*mohou členské státy přijmout nebo ponechat v platnosti ustanovení vnitrostátního práva s cílem dosáhnout vyšší úrovně odolnosti těchto kritických subjektů za předpokladu, že jsou tyto předpisy v souladu s platným právem Unie*.“[23]

Ve směrnici je rovněž popsána strategie, která je určena pro posílení odolnosti kritických subjektů. „*Tato strategie stanoví na základě relevantních stávajících vnitrostátních a odvětvových strategií, plánů nebo obdobných dokumentů strategické cíle a opatření politik s cílem dosáhnout vysoké úrovně odolnosti kritických subjektů a zachovat ji a pokrýt alespoň odvětví,“*[24] která jsou stanovena výše. V každé takové strategii musí být v souladu se směrnicí obsaženy alespoň určité prvky, které se týkají např. strategických cílů a priorit za účelem posílení celkové odolnosti kritických subjektů s ohledem na přeshraniční závislost, popisu opatření nutných k posílení odolnosti kritických subjektů jako celku nebo popisu určování těchto subjektů. Všechny členské státy jsou povinny tuto strategii přijmout do 17. ledna roku 2026.

Dalším úkolem členských států je posouzení rizik. V tomto případě pro tento účel příslušné orgány využijí seznam základních služeb, které vychází z uvedených odvětví a pododvětví. Posouzení rizik slouží pro účely určení kritických subjektů a má zohlednit *„všechna relevantní přírodní a člověkem způsobená rizika, včetně rizik meziodvětvové nebo přeshraniční povahy, havárií, přírodních katastrof, mimořádných událostí v oblasti veřejného zdraví a hybridních hrozeb či jiných antagonistických hrozeb, včetně teroristických trestných činů, jak je stanoveno ve směrnici Evropského parlamentu a Rady (EU) 2017/541*.“[25] Členské státy mají zajistit, aby *„kritické subjekty na základě relevantních informací poskytnutých členskými státy v posouzení rizik členského státu a na základě výsledku*

[23] Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022, *o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES*
[24] Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022, *o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES*
[25] Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022, *o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES*

posouzení rizik kritického subjektu, přijaly vhodná a přiměřená technická, bezpečnostní a organizační opatření k zajištění své odolnosti, *včetně opatření nezbytných za účelem předcházení vzniku incidentů, zajištění přiměřené fyzické ochrany jejich prostor a kritické infrastruktury, odezvy na incidenty, odolávání důsledkům incidentů a jejich zmírňování, zotavení se z incidentů, zajištění přiměřeného řízení bezpečnosti zaměstnanců a zvyšování povědomí příslušných pracovníků o opatřeních.“*[26] V souvislosti s opatřením za účelem zajištění odolnosti kritických subjektů *„členské státy zajistí, aby kritické subjekty zavedly a používaly plán odolnosti nebo rovnocenný dokument či dokumenty, které popisují opatření přijatá podle odstavce 1“*[27] v čl. 13 a rovněž „*zajistí, aby každý kritický subjekt určil pro účely kontaktu s příslušnými orgány styčnou osobu nebo její ekvivalent*.“[28]

V rámci příslušných orgánů „*každý členský stát určí nebo zřídí jeden nebo více příslušných orgánů odpovědných za správné uplatňování této směrnice na vnitrostátní úrovni a v případě potřeby vymáhání pravidel stanovených v této směrnici*.“[29]

Další stanovisko směrnice se týká zřízení jednotného kontaktního místa každým členským státem, které má být určeno pro *„výkon styčné funkce k zajištění přeshraniční spolupráce s jednotnými místy jiných členských států a skupinou pro odolnost kritických subjektů*.“[30]

Za účelem posilování odolnosti kritických subjektů má být zajištěna podpora prostřednictvím jednotlivých členských států pro tyto subjekty. Podpora zahrnuje např. „*vypracování poradenských manuálů a metodik, podporu organizace cvičení sloužících k prověření jejich odolnosti nebo poskytování poradenství a školení*

[26] Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022, *o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES*
[27] Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022, *o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES*
[28] Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022, *o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES*
[29] Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022, *o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES*
[30] Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022, *o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES*

pracovníkům kritických subjektů"[31] *a* je založena na vzájemné spolupráci a výměně informací a osvědčených postupů mezi kritickými subjekty, které spadají do jednotlivých odvětví. V případě potřeby mezi sebou mají spolupracovat rovněž členské státy, a to ve formě vzájemných konzultací. Ve spojitosti se spoluprací a předkládáním zpráv má být také zřízena *skupina pro odolnost kritických subjektů.*[32] Tato skupina „*podporuje Komisi a usnadňuje spolupráci mezi členskými státy a výměnu informací o otázkách týkajících se této směrnice*." [33]

Pozornost je dále věnována kritickým subjektům, které mají zvláštní evropský význam. Podle směrnice se „*subjekt považuje za kritický subjekt zvláštního evropského významu, pokud:*

- *byl určen jako kritický subjekt podle čl. 6 odst. 1;*
- *poskytuje stejné nebo podobné základní služby v šesti nebo více členských státech nebo do těchto států; a*
- *byl jako takový vyrozuměn podle odstavce 3 článku 17."*[34]

V souladu se směrnicí „*členské státy zajistí, aby kritický subjekt po vyrozumění podle čl. 6 odst. 3 informoval příslušný orgán, pokud poskytuje základní služby v šesti nebo více členských státech nebo do těchto států."*[35]

Směrnice se rovněž zaměřuje na dohled a vymáhání, a to "*za účelem posouzení, zda subjekty, které členské státy určily jakožto kritické subjekty podle čl. 6 odst. 1, dodržují povinnosti stanovené v této směrnici*."[36] V případě nedodržení stanovených pravidel budou hrozit sankce. Na základě směrnice *„členské státy stanoví pravidla pro sankce za porušení vnitrostátních opatření přijatých na základě této směrnice a přijmou veškerá opatření nezbytná k zajištění jejich*

[31] Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022, *o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES*
[32] Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022, *o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES*
[33] Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022, *o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES*
[34] Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022, *o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES*
[35] Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022, *o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES*
[36] Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022, *o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES*

uplatňování. Stanovené sankce musí být účinné, přiměřené a odrazující. Členské státy uvědomí o těchto pravidlech a opatřeních Komisi do 17. října 2024 a neprodleně ji uvědomí o veškerých pozdějších změnách, které se jich dotýkají.“[37]

V závěrečném ustanovení směrnice jsou obsaženy informace, které se týkají předkládání zpráv a přezkumu, kde směrnice uvádí, že „*do 17. července 2027 Komise předloží Evropskému parlamentu a Radě zprávu, v níž posoudí, do jaké míry každý členský stát přijal opatření nezbytná pro dosažení souladu s touto směrnicí.“*[38] Dále jsou v tomto ustanovení uvedeny informace o provedení stanovených pravidel směrnicí ve vnitrostátním právu členských států. Ve směrnici je uvedeno, že: „*Členské státy do 17. října 2024 přijmou a zveřejní opatření nezbytná pro dosažení souladu s touto směrnicí. Neprodleně o nich uvědomí Komisi a použijí tato opatření od 18. října 2024.“* [39]

V České republice na implementaci směrnice CER zareagovalo Ministerstvo vnitra a 9. února 2024 předložilo návrh zákona o odolnosti subjektů kritické infrastruktury a o změně dalších zákonů (zákon o kritické infrastruktuře), který je zatím ve fázi připomínkového řízení. Tento návrh nového zákona je vyjmut z krizového zákona a vytvořen samostatně. Kromě požadavků týkajících se směrnice CER má návrh nového zákona o kritické infrastruktuře vycházet i z praktických zkušeností získaných prostřednictvím doposud platného krizového zákona v rámci ochrany KI. [40]

V návrhu nového zákona jsou představeny definice pojmů postavených na základu směrnice CER, kterými jsou základní služba, poskytovatel základní služby, subjekt kritické infrastruktury, subjekt evropské kritické infrastruktury, odolnost subjektu kritické infrastruktury, incident, kritická infrastruktura, u které jsou zatím uvedeny dvě varianty definic, dále pracovník a kritický pracovník, ověřování spolehlivosti a významný dodavatel. Mimoto jsou zde vymezeny

[37] Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022, *o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES*
[38] Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022, *o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES*
[39] Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022, *o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES*
[40] *Zakonyprolidi.cz: Důvodová zpráva k návrhu zákona o odolnosti subjektů kritické infrastruktury a o změně některých zákonů* [online]. [cit.27.2.2024]. Dostupné z: https://www.zakonyprolidi.cz/monitor/7855524.htm

jednotlivé úkoly Ministerstva vnitra, ostatních ministerstev a jiných ústředních správních úřadů a České národní banky. [41]

Ministerstvo vnitra podle důvodové zprávy k návrhu zákona „*bude nadále zastávat ústřední a koordinační roli v oblasti kritické infrastruktury a pro účely plnění této role zřídí a bude provozovat Portál kritické infrastruktury, který bude stěžejním nástrojem pro komunikaci a sdílení informací mezi poskytovateli základní služby, subjekty kritické infrastruktury, věcně příslušnými ministerstvy a jinými ústředními správními úřady a Českou národní bankou, Ministerstvem vnitra, v oblasti kritické infrastruktury*.“[42] Ministerstvo vnitra bude mít podle návrhu také dominantní pozici při určování subjektů KI, jelikož má mít jako jediný orgán pravomoc tyto subjekty určovat bez ohledu na to, zda půjde o státní subjekty nebo jiné. Zároveň bude udržovat seznam určených subjektů KI, které do tohoto seznamu zařadí.[43] Kromě toho má mít na starosti v rámci povinností směrnice CER zpracování strategie pro posilování odolnosti subjektů KI, bude plnit funkci jednotného kontaktního místa ČR a má poskytovat část posouzení rizik ČR subjektům KI, a to podle krizového zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů, aby tyto subjekty mohly vypracovat vlastní posouzení rizik. Další činností Ministerstva vnitra má být nařízení a koordinování cvičení k ověření odolnosti subjektů KI v působnosti více ministerstev nebo jiných ústředních správních úřadů a na základě toho má Ministerstvo vnitra zpracovat plán cvičení. Kromě toho bude také zajišťovat výměnu informací na mezinárodní úrovni a pravidelně předkládat informace pro Evropskou komisi o seznamu základních služeb, zprávu o incidentech, strategii pro posílení odolnosti subjektů KI a o posouzení rizik ČR,

[41] *Zakonyprolidi.cz: Návrh zákona o odolnosti subjektů kritické infrastruktury a o změně dalších zákonů (zákon o kritické infrastruktuře*) [online]. [cit.27.2.2024]. Dostupné z: https://www.zakonyprolidi.cz/monitor/7855524.htm

[42] *Zakonyprolidi.cz: Důvodová zpráva k návrhu zákona o odolnosti subjektů kritické infrastruktury a o změně některých zákonů* [online]. [cit.27.2.2024]. Dostupné z: https://www.zakonyprolidi.cz/monitor/7855524.htm

[43] *Zakonyprolidi.cz: Důvodová zpráva k návrhu zákona o odolnosti subjektů kritické infrastruktury a o změně některých zákonů* [online]. [cit.27.2.2024]. Dostupné z: https://www.zakonyprolidi.cz/monitor/7855524.htm

informace o subjektu evropské kritické infrastruktury a další povinnosti související se směrnicí CER. [44]

Ostatní ministerstva a jiné ústřední správní úřady mají být trvale významnou složkou v oblasti KI jako tomu bylo doposud. Jejich hlavní role bude spočívat v určování subjektů KI. V této souvislosti mají mít právo v okruhu své působnosti požadovat od poskytovatelů základních služeb informace, které by jim umožnily doporučit Ministerstvu vnitra jejich možné zařazení mezi subjekty KI. Kromě toho mají spolupracovat s Ministerstvem vnitra v rámci jeho činností uvedených výše a dalších, které jsou obsaženy v návrhu zákona. [45]

Role České národní banky má být ve srovnání s ministerstvy a jinými správními úřady omezenější. ČNB bude podle návrhu zákona mít v gesci odvětví bankovnictví a infrastrukturu finančních trhů.[46] V rámci těchto odvětví má stejně tak jako jednotlivá ministerstva, spolupracovat s Ministerstvem vnitra při zpracování strategie pro posílení odolnosti subjektů KI a souhrnné zprávy o incidentech, dále má mít právo požadovat od poskytovatelů v rámci své působnosti potřebné informace pro navržení k zařazení subjektu mezi KI a další činnosti uvedené v návrhu zákona.[47]

Novým pojmem, který se objevuje v návrhu zákona, je „manažer kritické infrastruktury.“ Ten má nahradit dosavadní termín, kterým je „styčný bezpečnostní zaměstnanec‘‘. Pro výkon této role mají být současně upraveny nároky na odbornou kvalifikaci. [48]

---

[44] *Zakonyprolidi.cz: Návrh zákona o odolnosti subjektů kritické infrastruktury a o změně dalších zákonů (zákon o kritické infrastruktuře*) [online]. [cit.27.2.2024]. Dostupné z: https://www.zakonyprolidi.cz/monitor/7855524.htm

[45] *Zakonyprolidi.cz: Důvodová zpráva k návrhu zákona o odolnosti subjektů kritické infrastruktury a o změně některých zákonů* [online]. [cit.27.2.2024]. Dostupné z: https://www.zakonyprolidi.cz/monitor/7855524.htm

[46] *Zakonyprolidi.cz: Důvodová zpráva k návrhu zákona o odolnosti subjektů kritické infrastruktury a o změně některých zákonů* [online]. [cit.27.2.2024]. Dostupné z: https://www.zakonyprolidi.cz/monitor/7855524.htm

[47] *Zakonyprolidi.cz: Návrh zákona o odolnosti subjektů kritické infrastruktury a o změně dalších zákonů (zákon o kritické infrastruktuře*) [online]. [cit.27.2.2024]. Dostupné z: https://www.zakonyprolidi.cz/monitor/7855524.htm

[48] *Zakonyprolidi.cz: Důvodová zpráva k návrhu zákona o odolnosti subjektů kritické infrastruktury a o změně některých zákonů* [online]. [cit.27.2.2024]. Dostupné z: https://www.zakonyprolidi.cz/monitor/7855524.htm

Kromě těchto důležitých informací jsou v návrhu nového zákona obsaženy informace týkající se kritéria významnosti, kterým se bude identifikovat poskytovatel základní služby a rozhodnutí, zda bude považován nebo nepovažován za subjekt KI. Dále jsou zde popsány povinnosti poskytovatele základní služby, změny v poskytování základní služby, práva a povinnosti subjektu KI, zvláštní ustanovení o bezpečnosti dodavatelského řetězce, opatření k zajištění odolnosti KI, ověřování spolehlivosti, hlášení incidentu a informace o kontrole a sankcích.[49]

2.3 Nelegislativní dokumenty související s ochranou kritické infrastruktury

Mimo normativní stránky se ochranou kritické infrastruktury v ČR zabývají také některé dokumenty, které mají nelegislativní povahu.

2.3.1 Bezpečnostní strategie České republiky 2023

Jedná se o základní vládní dokument v oblasti bezpečnostní politiky ČR, který slouží jako zdroj pro další strategie a záměry. Určuje základní principy a orientování bezpečnostní politiky, kterými jsou vázány činnosti všech státních orgánů a veřejné správy. Bezpečnostní strategie je zpracována v rámci konzultace Kanceláře prezidenta republiky a Parlamentu ČR za účelem nalezení různých přístupů k zajištění bezpečnosti, a kromě toho vychází ze zásadních mezinárodních dokumentů, kterými jsou Strategické koncepce NATO a strategický kompas EU. Strategie svým obsahem přitom dodržuje soulad se Strategickým rámcem České republiky 2030, který se soustředí na strategickou vizi a dlouhodobé cíle ČR. V Bezpečnostní strategii z roku 2023 je směrována pozornost na několik oblastí, které jsou považovány za důležité, konkrétně se

[49] *Zakonyprolidi.cz: Návrh zákona o odolnosti subjektů kritické infrastruktury a o změně dalších zákonů (zákon o kritické infrastruktuře*) [online]. [cit.27.2.2024]. Dostupné z: https://www.zakonyprolidi.cz/monitor/7855524.htm

jedná např. o vnitřní, ekonomickou a kybernetickou bezpečnost nebo o postavení Česka v mezinárodních vztazích. [50]

2.3.2 Komplexní strategie ČR k řešení problematiky kritické infrastruktury

Tato strategie byla vydána usnesením vlády v roce 2010 a obsahuje souhrn konzultovaných, schválených a budoucích opatření, jež jsou dále rozvedeny v Národním programu ochrany kritické infrastruktury do jednotlivých úkolů pro odpovědné subjekty jejich realizace. Hlavní princip této strategie spočívá v zabezpečení fungování zásadních a strategických infrastruktur s cílem zajistit ochranu obyvatelstva. Strategie rovněž zahrnuje řešení problematiky KI v EU a NATO.[51]

[50] Kolektiv autorů pod vedením Ministerstva zahraničních věcí. *Bezpečnostní strategie České republiky 2023* [online]. Praha: Ministerstvo zahraničních věcí České republiky, 2023. [cit.6.2.2024]. ISBN 978-7441-099-4.

[51] *Databaze-strategie.cz: Komplexní strategie ČR k řešení problematiky kritické infrastruktury (2010)* [online]. [cit.6.2.2024]. Dostupné z: https://www.dataplan.info/img_upload/7bdb1584e3b8a53d337518d988763f8d/komplexni-strategie-ki.pdf

3. Kybernetická bezpečnost

Pojem bezpečnost obecně představuje ochranu *„něčeho před zničením, poškozením nebo zcizením*.“[52] K tomu připojená předpona kyber (cyber), která původně vychází z angličtiny, je běžně využívána ve spojitosti s počítači nebo počítačovými sítěmi. [53]

Kybernetická bezpečnost je neustále se měnícím výrazem a význam tohoto pojmu může být stejně tak jako u pojmu bezpečnosti různý, poněvadž v kybernetické bezpečnosti dochází k postupnému vývoji v souvislosti s technologickými, společenskými nebo politickými změnami ve společnosti.[54] Z tohoto důvodu tedy existuje mnoho definic, které kybernetickou bezpečnost popisují.

Kybernetickou bezpečnost lze například definovat jako „*souhrn právních, technických a vzdělávacích prostředků směrujících k zajištění ochrany kybernetického prostoru.“* [55]

Kybernetický prostor může být popsán jako „*digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, službami a sítěmi elektronických komunikací*.“ [56]

3.1 Důležité pojmy v oblasti kybernetické bezpečnosti

S kybernetickou bezpečností a kyberprostorem souvisí několik dalších základních pojmů, které je zapotřebí zmínit.

[52] ŠULC Vladimír. *Kybernetická bezpečnost.* Plzeň: Aleš Čeněk, 2018. 9 s. ISBN 978-80-7380-737-5.
[53] ŠULC Vladimír. *Kybernetická bezpečnost.* Plzeň: Aleš Čeněk, 2018. 9 s. ISBN 978-80-7380-737-5.
[54] RAMEŠOVÁ Kristina. *Právní regulace kybernetické bezpečnosti a její meze.* 1. vydání. Praha: C. H. Beck, 2023, 80 s. ISBN 978-80-7400-931-0.
[55] SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* 1. vydání. Brno: Akademické nakladatelství CERM, 2021. 13 s. ISBN 978-80-7623-068–2.
[56]SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* 1. vydání. Brno: Akademické nakladatelství CERM, 2021. 12 s. ISBN 978-80-7623-068–2.

Kybernetická kriminalita

Je definována jako „*trestná činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsána zařízení jako movité), nebo jako nástroj trestné činnosti*."[57] Kybernetickou kriminalitu popisuje také přímo Policie ČR, kterou je definována jako „*trestná činnost, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí*."[58]

Kybernetický útok

Jedná se o „*útok na ICT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace*."[59] Nejčastěji je tento pojem využit v souvislosti s útoky, které jsou politicky nebo vojensky podnícené.[60]

Kybernetická obrana

Je charakterizována jako „*obrana proti kybernetickému útoku a zmírňování jeho následků nebo rezistence subjektu na útok a schopnost se účinně bránit*." [61]

Kybernetická strategie

Tato strategie je popsána jako „*obecný postup k rozvoji využití schopností pracovat v kybernetickém prostoru, integrovaný a koordinovaný přístup s ostatními operačními oblastmi k dosažení nebo podpoře dosažení stanovených*

[57]SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* 1. vydání. Brno: Akademické nakladatelství CERM, 2021. 13 s. ISBN 978-80-7623-068-2.

[58] *Policie.cz: Kyberkriminalita* [online]. [cit.6.2.2024]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

[59] SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* 1. vydání. Brno: Akademické nakladatelství CERM, 2021. 13 s. ISBN 978-80-7623-068–2.

[60] SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* 1. vydání. Brno: Akademické nakladatelství CERM, 2021. 13 s. ISBN 978-80-7623-068–2.

[61] SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* 1. vydání. Brno: Akademické nakladatelství CERM, 2021. 13 s. ISBN 978-80-7623-068–2.

cílů pomocí identifikovaných prostředků, metod a nástrojů v určitém časovém rozvrhu.“ [62]

Kybernetický (bezpečnostní) incident

„Je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.“ [63]

Kyberterorismus

Je definován jako „*trestná činnost páchaná za primárního využití či cílení prostředků IT s cílem vyvolat strach či neadekvátní reakci*.“[64] Pojem kyberterorismus je využíván ve spojitosti s extrémistickými, nacionalistickými a politickými útoky.[65]

Kybernetická špionáž

Je „*získávání strategicky citlivých či strategicky důležitých informací od jednotlivců nebo organizací za použití či cílení prostředků IT*.“ [66] Kybernetická špionáž je často spojena s dosahováním politické, ekonomické či vojenské nadvlády.[67]

[62] SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* 1. vydání. Brno: Akademické nakladatelství CERM, 2021. 13 s. ISBN 978-80-7623-068–2.
[63] SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* 1. vydání. Brno: Akademické nakladatelství CERM, 2021. 13 s. ISBN 978-80-7623-068–2.
[64] SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* 1. vydání. Brno: Akademické nakladatelství CERM, 2021. 13 s. ISBN 978-80-7623-068–2.
[65] SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* 1. vydání. Brno: Akademické nakladatelství CERM, 2021. 13 s. ISBN 978-80-7623-068–2.
[66] SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* 1. vydání. Brno: Akademické nakladatelství CERM, 2021. 13 s. ISBN 978-80-7623-068–2.
[67] SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* 1. vydání. Brno: Akademické nakladatelství CERM, 2021. 13 s. ISBN 978-80-7623-068–2.

Kybernetická válka

Jedná se o „*použití počítačů a internetu k vedení války v kybernetickém prostoru*.“[68] Tento pojem představuje široký souhrn kybernetických útoků a protiútoků, které jsou vzájemně propojeny a vyvolány. Tyto útoky bývají obvykle politicky nebo strategicky ovlivněné. [69]

Sociální inženýrství

Je „*snaha podvodem vylákat od důvěřivých uživatelů jejich osobní informace, jako jsou hesla nebo bankovní údaje, případně získat přístup k jejich počítači, za účelem instalace škodlivých programů*.“ [70]

Bezpečnost informací

„Bezpečností informací se rozumí zajištění důvěrnosti, integrity a dostupnosti informací a dat.“ [71]

Software

„Je programové vybavení počítače – tedy programy a aplikace v počítači.“ [72]

Hardware

Je *„veškeré technické vybavení počítače.“* [73]

[68] SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* 1. vydání. Brno: Akademické nakladatelství CERM, 2021. 14 s. ISBN 978-80-7623-068–2.

[69]SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* 1. vydání. Brno: Akademické nakladatelství CERM, 2021. 14 s. ISBN 978-80-7623-068-2.

[70] *Avast.com: Sociální inženýrství* [online]. [cit.7.2.2024]. Dostupné z: https://www.avast.com/cs-cz/c-social-engineering

[71]SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti.* Plzeň: Aleš Čeněk, 2019. 66 s. ISBN 978-80-7380-765-8.

[72] *It-slovnik.cz: Co je to Software?* [online]. [cit.7.2.2024]. Dostupné z: https://it-slovnik.cz/pojem/software

[73] *It-slovnik.cz: Co je to Hardware?* [online]. [cit.7.2.2024]. Dostupné z: https://it-slovnik.cz/pojem/hardware

3.2 Typy kybernetických útoků

Typů kybernetických útoků je mnoho. Mezi útoky, které jsou v této době nejrozšířenější, se řadí phishing, malware, ransomware, spyware, DDoS útoky, trojské koně a počítačové viry. [74]

Phishing

Phishing je podvodný způsob, který je útočníkem používán ve smyslu vylákání důvěrných informací, jako jsou např. hesla nebo údaje o kreditních kartách.[75] Phishingový útok probíhá ve formě emailu, ve kterém útočník zašle dané oběti odkaz, který má přitáhnout její pozornost tak, aby odkaz rozklikla.[76] To následně útočníkovi poskytne možnost získání přístupu k citlivým informacím anebo stažení škodlivého softwaru přímo do zařízení oběti. Přitom se útoky vydávají za věrohodné organizace, kterými mohou být např. banky, pojišťovny nebo mobilní operátoři.[77] Při phishingu je využívána forma manipulace, která je označována jako sociální inženýrství.[78]

Malware

Malwarem je všeobecně označován software, který danému útočníkovi poskytuje možnost zneužít, zničit či kompromitovat jeden nebo více počítačů a počítačových sítí.[79] Jedná se o obvyklý druh kyberútoku, který má formu škodlivého softwaru.[80] Malware umožňuje např. krádež, šifrování a smazání dat, přeměnu základních funkcí počítače nebo sledování aktivity na cizím počítači.[81] Běžně je využíván pro

---

[74] *Legislativa.cz: Kybernetický útok: definice, typy, následky a prevence* [online]. [cit.6.2.2024]. Dostupné z: https://legislativa.cz/zdroje/kyberneticka-bezpecnost/kyberneticky-utok
[75] *Legislativa.cz: Kybernetický útok: definice, typy, následky a prevence* [online]. [cit.6.2.2024]. Dostupné z: https://legislativa.cz/zdroje/kyberneticka-bezpecnost/kyberneticky-utok
[76] ŠULC Vladimír. *Kybernetická bezpečnost.* Plzeň: Aleš Čeněk, 2018. 68 s. ISBN 978-80-7380-737-5.
[77] *Legislativa.cz: Kybernetický útok: definice, typy, následky a prevence* [online]. [cit.6.2.2024]. Dostupné z: https://legislativa.cz/zdroje/kyberneticka-bezpecnost/kyberneticky-utok
[78] ŠULC Vladimír. *Kybernetická bezpečnost.* Plzeň: Aleš Čeněk, 2018. 68 s. ISBN 978-80-7380-737-5.
[79] *Legislativa.cz: Kybernetický útok: definice, typy, následky a prevence* [online]. [cit.6.2.2024]. Dostupné z: https://legislativa.cz/zdroje/kyberneticka-bezpecnost/kyberneticky-utok
[80]SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* 1. vydání. Brno: Akademické nakladatelství CERM, 2021. 109 s. ISBN 978-80-7623-068-2.
[81] *Legislativa.cz: Kybernetický útok: definice, typy, následky a prevence* [online]. [cit.6.2.2024]. Dostupné z: https://legislativa.cz/zdroje/kyberneticka-bezpecnost/kyberneticky-utok

získání určitých informací, krádeže identity, narušení služeb nebo špionáž.[82] Malware se dále rozděluje na několik druhů, kterými jsou ransomware, spyware, DDoS útoky, počítačové viry a trojské koně.[83]

Ramsomware

Ransomware je škodlivý kód malwaru, který útočník zneužívá buďto k šifrování souborů na zařízení oběti nebo k znemožnění přístupu tomuto uživateli k danému zařízení. Za znovuuvedení takového zařízení do prvotního stavu útočník vyžaduje určitou peněžní částku. [84]

Spyware

Jedná o software, jenž poskytuje útočníkovi možnost monitorovat činnosti jiného uživatele na počítačových, mobilních a dalších zařízeních, a to za pomocí tajného přenosu dat vedených ze zařízení uživatele do malwaru. Tento software může být použit i legální cestou, např. pro reklamní účely, ale obecně je především zneužíván k dosažení zisku prostřednictvím zcizených údajů. [85]

DDoS útoky

DDos (anglicky Distributed Denial of Service) jsou útoky, které se soustřeďují na weby a servery, oslabují služby sítí a usilují o vyčerpání prostředků aplikací. Kyberzločinci se úmyslně snaží za pomocí těchto útoků zahltit weby za účelem způsobit nefunkčnost webů nebo jejich kompletní vyřazení z provozu. DDoS útoky jsou často mířené na oblasti jako jsou např. telekomunikace, elektronické obchody nebo herní průmysl. Jedná o útoky, kterých v posledních letech neustále přibývá a řadí se mezi ty nejrozšířenější.[86]

---

[82]SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* 1. vydání. Brno: Akademické nakladatelství CERM, 2021. 109 s. ISBN 978-80-7623-068-2.

[83] *Legislativa.cz: Kybernetický útok: definice, typy, následky a prevence* [online]. [cit.6.2.2024]. Dostupné z: https://legislativa.cz/zdroje/kyberneticka-bezpecnost/kyberneticky-utok

[84] ŠULC, Vladimír. *Kybernetická bezpečnost.* Plzeň: Aleš Čeněk, 2018. 49-50 s. ISBN 978-80-7380-737-5.

[85] *Legislativa.cz: Kybernetický útok: definice, typy, následky a prevence* [online]. [cit.7.2.2024]. Dostupné z: https://legislativa.cz/zdroje/kyberneticka-bezpecnost/kyberneticky-utok

[86] *Microsoft.com: Definice útoků DDoS* [online]. [cit.7.2.2024]. Dostupné z: https://www.microsoft.com/cs-cz/security/business/security-101/what-is-a-ddos-attack

Trojské koně

Trojský kůň je název pro škodlivý kód, který je skrytou součástí v softwaru a na první pohled může vypadat důvěryhodně.[87] Jeho skutečnou funkcí je však proniknout do zařízení uživatele, a to na principu podvodných metod sociálního inženýrství. Může se tedy jednat např. o důvěryhodnou emailovou přílohu nebo o program, který se na první pohled jeví jako užitečný. Hned poté, co se tento škodlivý kód dostane do určitého zařízení a dojde k jeho infikaci, započne trojský kůň poškozovat zařízení způsobem, kterým je naprogramován. Trojský kůň je kyberzločinci využíván např. k získání kontroly nad infikovaným zařízením nebo k vylákání dat uživatele. [88]

Počítačové viry

Počítačový vir je škodlivý program, jenž je šířen samostatně bez toho, aniž by o tom napadený uživatel věděl. K tomu dochází prostřednictvím zkopírování viru do dalšího programu nebo dokumentu. Záměrem použití virů je infikování systémů, které jsou nedostatečně zabezpečené, ovládnout tato zařízení a odcizit soukromá data uživatele. Kyberútočníci tyto viry programují za účelem podvést uživatele.[89]

[87] *It-slovnik.cz*: *Co je to Trojský kůň?* [online]. [cit.7.2.2024]. Dostupné z: https://it-slovnik.cz/pojem/trojsky-kun

[88] *Eset.com: Trojský kůň* [online]. [cit.7.2.2024]. Dostupné z: https://www.eset.com/cz/trojsky-kun/

[89] *Eset.com: Co je počítačový vir + druhy virů* [online]. [cit.7.2.2024]. Dostupné z: https://www.eset.com/cz/virus/

4. Legislativní rámec kybernetické bezpečnosti

4.1 Právní úprava v ČR

Stěžejním zákonem, který řeší problematiku kybernetické bezpečnosti v ČR, je zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). *„Tento zákon upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti*.“[90] V rámci své působnosti rovněž implementuje příslušné právní předpisy vydané Evropskou unií a zajišťuje bezpečnost elektronických komunikačních sítí a informačních systémů. [91]

Zákon o kybernetické bezpečnosti je účinný od 1. ledna 2015 a za dobu svého trvání byl několikrát legislativně upraven. Významná novelizace zákona proběhla v rámci implementace evropské směrnice NIS o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů.[92] Na tuto směrnici navazuje směrnice Evropského parlamentu a Rady s označením NIS 2 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii, která bude nově upravovat tento zákon.

4.1.1 Související právní předpisy

- 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 č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.

Obě tyto vyhlášky jsou nyní ve fázi přípravy na implementaci směrnice NIS 2. [93]

[90] Zákon č. 181/2014 Sb., *o kybernetické bezpečnosti v posledním znění*
[91] Zákon č. 181/2014 Sb., *o kybernetické bezpečnosti v posledním znění*
[92] SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* 1. vydání. Brno: Akademické nakladatelství CERM, 2021. 69 s. ISBN 978-80-7623-068-2.
[93] *Osveta.nukib.cz: Návrh nového zákona o kybernetické bezpečnosti a dalších předpisů* [online]. [cit.7.3.2024]. Dostupné z: https://osveta.nukib.cz/course/view.php?id=145#section-3

4.2 Právní úprava v rámci EU

Směrnice NIS 2

V roce 2016 byla Evropskou unii přijata směrnice NIS o bezpečnosti sítí a informací, v oficiálním znění Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Tato směrnice posloužila jako podklad pro bezpečnost sítí a informačních systémů poskytujících nezbytné služby v rámci všech členských států EU. V České republice již v tomto okamžiku byl platný zákon č. 181/2014 Sb., o kybernetické bezpečnosti, a na základě směrnice NIS, která musela být povinně implementována do právního prostředí ČR, byl tento zákon novelizován. Česká republika se v tu dobu nacházela ve výhodě z toho důvodu, že byla do této chvíle kybernetická bezpečnost v ČR již nějakou dobu regulována tímto zákonem a ČR tak získala v tomto směru určitou praxi.

V současné době Evropská unie přišla s novou směrnicí řešící kybernetickou bezpečnost, která tímto způsobem nahrazuje původní směrnici NIS a je označena pod názvem NIS 2[94], oficiálně je tato směrnice nazývána jako Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2).[95] K platnosti směrnice došlo dne 16. ledna 2023 a tím vznikla povinnost přenést text směrnice do vnitrostátního práva státu. Transpoziční lhůta, která stanovuje časový rámec pro převzetí této směrnice do národního práva, je vymezena na 21 měsíců, a to od okamžiku, kdy směrnice vstoupila v platnost. Z toho vyplývá, že by Česká republika měla implementovat nové právní povinnosti v rámci kybernetické bezpečnosti a souvisejících právních předpisů do národní legislativy konkrétně do 18. října 2024. Do této úpravy se

[94] *Osveta.nukib.cz: Obecné informace o směrnici NIS2 a budoucí národní úpravě* [online]. [cit.8.2.2024]. Dostupné z: https://osveta.nukib.cz/mod/page/view.php?id=2582

[95] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022, *o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)*

pustil Národní úřad pro kybernetickou a informační bezpečnost prostřednictvím návrhu nového zákona o kybernetické bezpečnosti a jeho vyhlášek. Dále by měla být určena další lhůta pro zahájení procesu implementace nových pravidel u organizací, které do této doby nebyly zahrnuty do regulace kybernetické bezpečnosti.

Směrnice NIS 2 stanovuje společnou legislativní strukturu kybernetické bezpečnosti za účelem zvýšení úrovně kybernetické bezpečnosti v členských státech EU a zároveň požaduje, aby u těchto států došlo k posílení jejich schopností v této oblasti. Jsou zde obsaženy pokyny pro kritické subjekty, které se týkají opatření k řízení kybernetických bezpečnostních rizik a oznamovací povinnosti, kybernetické spolupráce na unijní a mezinárodní úrovni, sdílení informací a dohledu a vymáhání pro tyto subjekty. [96]

Směrnice je současně vzájemně propojena se Směrnicí Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a zrušení směrnice Rady 2008/114/ES a vztahuje se na subjekty, jenž působí v 11 odvětvích, která jsou označena jako vysoce kritická a dále na subjekty působící v 6 odvětvích, považovaných za další kritická odvětví.

Mezi vysoce kritická odvětví se řadí:[97]

- **Energetika**
    - elektřina – elektroenergetické podniky, provozovatelé distribuční a přenosové soustavy;
    - dálkové vytápění a chlazení;
    - ropa – provozovatelé ropovodů, provozovatelé zařízení na těžbu, rafinaci a zpracování ropy a skladovacích a přenosových zařízení, ústřední správci zásob;

[96] *Osveta.nukib.cz*: *Obecné informace o směrnici NIS2 a budoucí národní úpravě* [online]. [cit.9.2.2024]. Dostupné z: https://osveta.nukib.cz/mod/page/view.php?id=2582

[97] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022, *o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)*

    - zemní plyn – dodavatelské podniky, provozovatelé distribuční a přepravní soustavy, provozovatelé skladovacího zařízení, provozovatelé LNG, plynárenské podniky, provozovatelé zařízení na rafinaci a zpracování zemního plynu;
    - vodík – provozovatelé výroby, skladování a přepravy vodíku.
- **Doprava**
    - letecká doprava – letečtí dopravci, řídící orgány letiště;
    - železniční doprava –provozovatelé infrastruktury, železniční podniky;
    - vodní doprava – společnosti vnitrozemské, námořní a pobřežní osobní a nákladní vodní dopravy, řídící orgány přístavů a provozovatelé služeb lodní dopravy;
    - silniční doprava – silniční orgány odpovědné za kontrolu řízení provozu, s výjimkou veřejných subjektů, pro něž je řízení provozu nebo provoz inteligentních dopravních systémů nepodstatnou částí jejich obecné činnosti, provozovatelé inteligentních dopravních systémů.
- **Bankovnictví** – úvěrové instituce.
- **Infrastruktura finančních trhů** – provozovatelé obchodních systémů a ústřední protistrany.
- **Zdravotnictví** – poskytovatelé zdravotní péče, referenční laboratoře EU, subjekty provádějící výzkum a vývoj týkající se léčivých přípravků, subjekty vyrábějící základní farmaceutické výrobky a farmaceutické přípravky, subjekty vyrábějící zdravotnické prostředky považované za kriticky důležité v případě mimořádné situace v oblasti veřejného zdraví.
- **Pitná voda** – dodavatelé a distributoři vody určené k lidské spotřebě.
- **Odpadní voda** – podniky zajišťující odvádění, vypouštění nebo čištění městských odpadních vod, splašek nebo průmyslových odpadních vod.
- **Digitální infrastruktura** – provozovatelé výměnných uzlů internetu, provozovatelé DNS, registry domén nejvyšší úrovně (TLD), poskytovatelé služeb cloud computingu, datových center, sítí pro doručování obsahu a vytvářejících důvěru.

- **Řízení služeb IKT** (mezi podniky) – poskytovatelé řízených služeb a řízených bezpečnostních služeb.
- **Veřejná správa –** ústřední subjekty veřejné správy vymezené členským státem v souladu s vnitrostátním právem, subjekty regionální veřejné správy vymezené členským státem v souladu s vnitrostátním právem.
- **Vesmír** – provozovatelé pozemních infrastruktur vlastněných, spravovaných a provozovaných členskými státy nebo soukromými subjekty a podporujících poskytování služeb využívajících kosmického prostoru, s výjimkou poskytovatelů veřejných sítí elektronických komunikací.

Další kritická odvětví zahrnují:

- **Poštovní a kurýrní služby;**
- **Nakládání s odpady;**
- **Výroba, zpracování a distribuce potravin;**
- **Výroba** zahrnující např. zdravotnické prostředky, počítače, elektrická zařízení nebo motorová vozidla;
- **Digitální poskytovatelé;**
- **Výzkum.**

V souvislosti se vzájemnou propojeností této směrnice se Směrnicí Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a zrušení směrnice Rady 2008/114/ES je ve směrnici NIS 2 obsažen text s významem pro Evropský hospodářský prostor, kde je v odstavci č. 30 tato propojenost charakterizována takovýmto způsobem: [98]

- *„Vzhledem ke vzájemným vazbám mezi kybernetickou bezpečností a fyzickou bezpečností subjektů by měl být zajištěn soudržný přístup ke směrnici Evropského parlamentu a Rady (EU) 2022/2557 a k této směrnici. Za tímto účelem by subjekty, které jsou určeny jakožto kritické subjekty*

[98] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022, *o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)*

podle směrnice (EU) 2022/2557, měly být považovány za základní subjekty podle této směrnice. Mimoto by každý členský stát měl zajistit, aby jeho národní strategie kybernetické bezpečnosti stanovila rámec politik pro posílení koordinace uvnitř uvedeného členského státu mezi jeho příslušnými orgány podle této směrnice a podle směrnice (EU) 2022/2557 v souvislosti se sdílením informací o rizicích, kybernetických hrozbách a incidentech a o jiných než kybernetických rizicích, hrozbách a incidentech a při výkonu úkolů dohledu. Příslušné orgány podle této směrnice a orgány příslušné podle směrnice (EU) 2022/2557 by měly spolupracovat a vyměňovat si informace bez zbytečného odkladu, zejména ve vztahu k určení kritických subjektů, rizik, kybernetických hrozeb a incidentů, jakož i ohledně jiných než kybernetických rizik, hrozeb nebo incidentů dotýkajících se kritických subjektů, včetně opatření v oblasti kybernetické bezpečnosti a fyzických opatření přijatých kritickými subjekty a výsledků činností v oblasti dohledu prováděných s ohledem na tyto subjekty."[99]

- *„V zájmu zefektivnění činností v oblasti dohledu mezi příslušnými orgány podle této směrnice a podle směrnice (EU) 2022/2557 a v zájmu minimalizace administrativní zátěže pro dotčené subjekty by uvedené příslušné orgány dále měly usilovat o harmonizaci šablon pro oznamování incidentů a postupů v oblasti dohledu. Příslušné orgány podle směrnice (EU) 2022/2557 by případně měly mít možnost požádat příslušné orgány podle této směrnice, aby vykonávaly své dohledové a vymáhací pravomoci ve vztahu k subjektu, který je určen jakožto kritický subjekt podle směrnice (EU) 2022/2557. Příslušné orgány podle této směrnice a podle směrnice (EU) 2022/2022/2557 by za tímto účelem měly, pokud možno v reálném čase, spolupracovat a vyměňovat si informace."*[100]

[99] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022, *o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)*

[100] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022, *o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)*

- V čl. 1, ve kterém je obsažen předmět směrnice je uvedeno, že: Za účelem opatření, „*jejichž cílem je dosáhnout vysoké společné úrovně kybernetické bezpečnosti v rámci Unie s cílem zlepšit fungování trhu tato směrnice stanoví v odst. 2 písm. b) opatření k řízení kybernetických bezpečnostních rizik a oznamovací povinnosti pro subjekty, jejichž druhy jsou uvedeny v příloze I nebo II, jakož i pro subjekty, jež jsou určeny jakožto kritické subjekty podle směrnice (EU) 2022/2022/2557.“*[101]
- V čl. 2, který popisuje oblast působnosti směrnice se podle odst. 3 „*tato směrnice použije na subjekty určené jakožto kritické subjekty podle směrnice (EU) 2022/2557*.“ [102]
- V čl. 3, kde jsou uvedeny základní a důležité subjekty podle odst. 1 písm. f) „*se pro účely této směrnice za základní subjekty považují subjekty určené jakožto kritické subjekty podle směrnice (EU) 2022/2557, jež jsou uvedeny v čl. odst. 3 směrnice.“*[103]
- V čl. 7 je popsána Národní strategie kybernetické bezpečnosti takto: „*Každý členský stát přijme národní strategii kybernetické bezpečnosti, která stanovuje strategické cíle, zdroje potřebné k dosažení těchto cílů a příslušné politiky a regulační opatření s cílem dosáhnout vysoké úrovně kybernetické bezpečnosti a udržovat ji. Národní strategie kybernetické bezpečnosti zahrnuje podle písm. g) rámce politiky lepší koordinaci mezi příslušnými orgány podle této směrnice a příslušnými orgány podle směrnice (EU) 2022/2557 pro účely sdílení informací o rizicích, kybernetických hrozbách a incidentech a o jiných než kybernetických*

[101] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022, *o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)*

[102] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022, *o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)*

[103] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022, *o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)*

rizicích, hrozbách a incidentech, případně pro výkon úkolů v oblasti dohledu.“[104]

- Čl. 13 je zaměřen na spolupráci členských států na vnitrostátní úrovni. Podle odst. 5 „*členské státy zajistí, aby jejich příslušné orgány podle této směrnice a jejich příslušné orgány podle směrnice (EU) 2022/2557 spolupracovaly a pravidelně si vyměňovaly informace o určení kritických subjektů, o rizicích, kybernetických hrozbách a incidentech, jakož i o jiných než kybernetických rizicích, hrozbách a incidentech postihujících základní subjekty určené jakožto kritické podle směrnice (EU) 2022/2557, jakož i o opatřeních přijatých v reakci na tato rizika, hrozby a incidenty. Členské státy rovněž zajistí, aby si jejich příslušné orgány podle této směrnice a jejich příslušné orgány podle nařízení (EU) č. 910/2014, nařízení (EU) 2022/2554a směrnice (EU) 2018/1972 pravidelně vyměňovaly relevantní informace, včetně informací o příslušných incidentech a kybernetických hrozbách*.“[105]
- Vzájemná spolupráce mezi členskými státy má být rovněž zajištěna na unijní a mezinárodní úrovni. Podle čl. 14 mají v rámci této spolupráce členské státy zřídit skupinu pro spolupráci, která má „*podporovat a usnadňovat strategickou spolupráci a výměnu informací mezi členskými státy a posilovat důvěru*.“ Podle odst. 9 tohoto článku se má skupina pro spolupráci scházet pravidelně, „*a vždy alespoň jednou ročně, se skupinou pro odolnost kritických subjektů zřízenou podle směrnice (EU) 2022/2557 za účelem podpory a usnadnění strategické spolupráce a výměny informací.“* [106]

[104] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022, *o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)*

[105] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022, *o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)*

[106] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022, *o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)*

- V čl. 32 jsou specifikována opatření v oblasti dohledu a vymáhání týkajících se základních subjektů. Podle odst. 1 „*členské státy zajistí, aby byla opatření v oblasti dohledu nebo vymáhání uložená základním subjektům v souvislosti s povinnostmi stanovenými v této směrnici účinná, přiměřená a odrazující, přičemž zohlední okolnosti každého jednotlivého případu.*“ Podle směrnice „*členské státy zajistí, aby jejich příslušné orgány podle této směrnice informovaly relevantní příslušné orgány ve stejném členském státě podle směrnice (EU) 2022/2557, když plní své pravomoci v oblasti dohledu a vymáhání zaměřené na zajištění toho, aby subjekt určený jakožto kritický subjekt podle směrnice (EU) 2022/2557 dodržoval tuto směrnici. Příslušné orgány podle směrnice (EU) 2022/2557 mohou případně požádat příslušné orgány podle této směrnice, aby vykonávaly své dohledové a vymáhací pravomoci ve vztahu k subjektu, který je určen jakožto kritický subjekt podle směrnice (EU) 2022/2557*.“ [107]

[107] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022, *o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)*

5. Aktéři působící v kybernetické bezpečnosti

5.1 Národní úřad pro kybernetickou a informační bezpečnost

„Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany.“[108] Kromě toho působí v oblasti problematiky veřejně regulovaných služeb v souvislosti s družicovým systémem Galileo. Ke vzniku úřadu došlo 1. srpna 2017 v kontextu se zákonem č. 205/2017, kterým byl změněn zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). [109]

NÚKIB je podle konkrétních činností rozdělen do několik sekcí; sekce personalistiky, práva a provozu, sekce strategických agend a spolupráce (SSAS), sekce informačních systémů a sekce Národního centra kybernetické bezpečnosti (NCKB). Tyto sekce jsou dále rozčleněny na jednotlivé odbory a oddělení. [110]

Národní centrum kybernetické bezpečnosti a sekce strategických agend a spolupráce v rámci úřadu slouží jako výkonné celky kybernetické a informační bezpečnosti. V mezích své působnosti zajišťují tyto důležité činnosti:

- *„činnost Vládního CERT České republiky (GovCERT.CZ);*
- *prevenci před kybernetickými hrozbami proti prvkům kritické informační infrastruktury, informačním systémům základní služby, proti významným informačním systémům a vybraným informačním systémům veřejné správy;*
- *řešení a koordinaci řešení kybernetických bezpečnostních incidentů u subjektů kritické infrastruktury, provozovatelů základní služby a orgánů veřejné správy;*
- *osvětovou a vzdělávací činnost v oblasti kybernetické bezpečnosti;*

[108] *Nukib.gov.cz: NÚKIB* [online]. [cit.10.2.2024]. Dostupné z: https://nukib.gov.cz/cs/o-nukib/
[109] *Nukib.gov.cz: NÚKIB* [online]. [cit.10.2.2024]. Dostupné z: https://nukib.gov.cz/cs/o-nukib/
[110] *Nukib.gov.cz*: *Organizační struktura úřadu [*online]. [cit.10.2.2024]. Dostupné z: https://nukib.gov.cz/cs/o-nukib/organizacni-struktura-uradu/

- *spolupráci s národními i mezinárodními organizacemi podílejícími se na zajišťování bezpečnosti kybernetického prostoru;*
- *pořádání a účast na kybernetických cvičeních na národní a mezinárodní úrovni;*
- *výzkum a vývoj v oblasti kybernetické bezpečnosti;*
- *ve spolupráci s kabinetem ředitele zastupování České republiky v orgánech mezinárodních organizací působících v oblasti kybernetické bezpečnosti;*
- *vyhodnocování rizik v oblasti kybernetické bezpečnosti a přijímaní příslušných nápravných a preventivních opatření;*
- *v rozsahu své působnosti bezpečnostní politiku Úřadu, plnění mezinárodních závazků a spolupráci na mezinárodní úrovni při realizaci předpisů vyplývajících z členství České republiky v NATO a členství v EU a členství v jiných mezinárodních organizacích;*
- *stanovují komunikační strategii Úřadu v oblasti kybernetické bezpečnosti ve spolupráci s ostatními organizačními celky Úřadu.“* [111]

5.2 Rada pro kybernetickou bezpečnost

Rada byla zřízena na základě usnesení vlády č. 781 ze dne 19. října 2011 a „*je poradním orgánem předsedy vlády pro oblast kybernetické bezpečnosti*.“ [112]

5.3 Výbor pro kybernetickou bezpečnost

„Výbor pro kybernetickou bezpečnost je stálým pracovním orgánem Bezpečnostní rady státu pro koordinaci plánování opatření k zajišťování kybernetické bezpečnosti ČR.“[113] K jeho vzniku došlo usnesením vlády ze dne 10. května 2017 č. 360. Mezi úkoly výboru patří především:

[111] *Nukib.gov.cz: Kybernetická bezpečnost* [online]. [cit.10.2.2024]. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/
[112] *Govcert.cz: Rada pro kybernetickou bezpečnost* [online]. [cit.7.3.2024]. Dostupné z: https://www.govcert.cz/cs/rkb/rada-pro-kybernetickou-bezpecnost/
[113] *Vlada.gov.cz: Statut Výboru pro kybernetickou bezpečnost* [online]. [cit.7.3.2024]. Dostupné z: https://vlada.gov.cz/assets/ppov/brs/pracovni-vybory/Kyberneticka_bezpecnost/statut-vkb-2024.pdf

- zajišťování meziresortní spolupráce, projednávání plánovacích záměrů a koncepčních dokumentů souvisejících s kybernetickou bezpečností,
- zajišťování meziresortní koordinace plánování a přípravy postupů k zabezpečení kyberbezpečnosti, hodnocení a prodiskutování žádostí od orgánů státní správy,
- posuzování a projednávání materiálů usnesených Bezpečnostní radou státu,
- analyzování, hodnocení a koordinování významných činností zástupců ČR v rámci mezinárodních spojenectví jako jsou EU, NATO a další. [114]

5.4 Bezpečnostní týmy CERT a CSIRT

Bezpečnostní týmy typu CERT (Computer Emergency Response Team) nebo CSIRT (Computer Security Incident Response Team) jsou týmy, které se zaměřují na řešení spojená s bezpečnostními incidenty v oblasti státu, odvětví, komunity, organizace nebo sítě. Jejich pracovní náplň je v rámci těchto incidentů rozsáhlá a představuje spoustu funkcí, které se týkají např. předcházení, osvěty nebo zhodnocení zkušeností z těchto incidentů. Tyto bezpečnostní týmy se vytvářejí především s cílem zajistit účinnou odezvu v kontextu kybernetických bezpečnostních incidentů. Významným aspektem týmů je obzvláště jejich účast v mezinárodním bezpečnostním společenství a infrastruktuře ostatních bezpečnostních týmů na mezinárodní úrovni, ve kterých dochází k vzájemné výměně informací a postupů. [115]

V České republice jsou podle zákona č. 181/2014 Sb. o kybernetické bezpečnosti stanoveny dva bezpečnostní týmy tohoto typu – Vládní CERT (GovCERT.CZ) a Národní CERT (CSIRT.CZ). Vládní CERT je provozován Národním úřadem pro kybernetickou a informační bezpečnost. Národní CERT spravuje sdružení

[114] *Vlada.gov.cz: Statut Výboru pro kybernetickou bezpečnost* [online]. [cit.7.3.2024]. Dostupné z: https://vlada.gov.cz/assets/ppov/brs/pracovni-vybory/Kyberneticka_bezpecnost/statut-vkb-2024.pdf

[115] SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* 1. vydání. Brno: Akademické nakladatelství CERM, 2021. 84 s. ISBN 978-80-7623-068-2.

CZ.NIC.[116] Tyto týmy mají na základě zákona o kybernetické bezpečnosti zásadní význam pro ochranu kritické informační infrastruktury a důležitých informačních systémů a vzájemně spolu spolupracují[117]. Vládní CERT v rámci NÚKIBU plní tyto úkoly:

- *„přijímá oznámení kontaktních údajů od orgánů a osob uvedených v § 3 písm. c) až g);*
- *přijímá hlášení o kybernetických bezpečnostních incidentech od orgánů a osob uvedených v § 3 písm. c) až g);*
- *vyhodnocuje údaje o kybernetických bezpečnostních událostech a kybernetických bezpečnostních incidentech z kritické informační infrastruktury, informačního systému základní služby, významných informačních systémů a dalších informačních systémů veřejné správy;*
- *poskytuje orgánům a osobám uvedeným v § 3 písm. c) až g) metodickou podporu a pomoc;*
- *poskytuje součinnost orgánům a osobám uvedeným v § 3 písm. c) až g) při výskytu kybernetického bezpečnostního incidentu a kybernetické bezpečnostní události;*
- *přijímá podněty a údaje od orgánů a osob uvedených v § 3 a od jiných orgánů a osob a tyto podněty a údaje vyhodnocuje;*
- *přijímá údaje od provozovatele národního CERT a tyto údaje vyhodnocuje;*
- *přijímá údaje od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí, a tyto údaje vyhodnocuje;*
- *poskytuje podle § 9 odst. 4 provozovateli národního CERT, orgánům vykonávajícím působnost v oblasti kybernetické bezpečnosti v zahraničí a jiným osobám působícím v oblasti kybernetické bezpečnosti údaje z evidence incidentů;*
- *provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti;*
- *informuje bez uvedení identifikačních údajů ohlašovatele příslušný orgán jiného členského státu o kybernetickém bezpečnostním incidentu, který má*

[116]SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* 1. vydání. Brno: Akademické nakladatelství CERM, 2021. 85 s. ISBN 978-80-7623-068-2.

[117] *Nukib.gov.cz: Vládní CERT* [online]. [cit.11.2.2024]. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vladni-cert/

významný dopad na kontinuitu poskytování základních služeb v tomto členském státě nebo se dotýká poskytování digitálních služeb v tomto členském státě, přičemž zachovává bezpečnost a obchodní zájmy ohlašovatele;

- *přijímá hlášení o kybernetickém bezpečnostním incidentu od orgánů a osob neuvedených v §3;* Vládní CERT hlášení *zpracovává, a pokud to jeho kapacity umožňují a jedná se o kybernetický bezpečnostní incident s významným dopadem, poskytuje orgánům nebo osobám dotčeným kybernetickým bezpečnostním incidentem metodickou podporu, pomoc a součinnost;*
- *plní roli týmu CSIRT podle příslušného předpisu Evropské unie a spolupracuje s týmy CSIRT jiných členských států.“* [118]

Provozovatel národního CERT podle zákona č. 181/2014 Sb., má tyto povinnosti:

- *„přijímá oznámení kontaktních údajů od orgánů a osob uvedených v § 3 písm. a), b) a h) a tyto údaje eviduje a uchovává;*
- *přijímá hlášení o kybernetických bezpečnostních incidentech od orgánů a osob uvedených v § 3 písm. b) a h) a tyto údaje eviduje, uchovává a chrání;*
- *vyhodnocuje kybernetické bezpečnostní incidenty u orgánů a osob uvedených v § 3 písm. b) a h);*
- *poskytuje orgánům a osobám uvedeným v § 3 písm. a), b) a h) metodickou podporu, pomoc a součinnost při výskytu kybernetického bezpečnostního incidentu;*
- *působí jako kontaktní místo pro orgány a osoby uvedené v § 3 písm. a), b) a h);*
- *provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti;*
- *předává Úřadu údaje o kybernetických bezpečnostních incidentech ohlášených podle § 8 odst. 3, bez uvedení ohlašovatele;*
- *předává Úřadu na vyžádání údaje podle § 16 odst. 5 a 6;*

[118] Zákon č. 181/2014 Sb., *o kybernetické bezpečnosti v posledním znění*

- *plní roli týmu CSIRT podle příslušného předpisu Evropské unie;*
- *informuje bez uvedení identifikačních údajů ohlašovatele příslušný orgán jiného členského státu o kybernetickém bezpečnostním incidentu s významným dopadem na kontinuitu poskytování základní nebo digitální služby v tomto členském státě a zároveň o tom informuje Úřad, přičemž zachovává bezpečnost a obchodní zájmy ohlašovatele;*
- *spolupracuje s týmy CSIRT jiných členských států;*
- *přijímá hlášení o kybernetických bezpečnostních incidentech od orgánů a osob neuvedených v § 3, a pokud to jeho kapacity umožňují, zpracovává je a poskytuje orgánům nebo osobám dotčeným kybernetickým bezpečnostním incidentem metodickou podporu, pomoc a součinnost.“* [119]

5.5 Agentura ENISA

Agentura ENISA (European Union Network and Information Security Agency) je organizací Evropské unie, která vznikla v roce 2004. Primárním cílem této agentury je zajistit vysoký stupeň kybernetické bezpečnosti napříč celou Evropou. Agentura ENISA aktivně podporuje politiku EU ve sféře kybernetické bezpečnosti, rozvíjí důvěryhodnost IKT produktů, služeb a procesů pomocí certifikačních systémů pro kybernetickou bezpečnost, navazuje spolupráci s členskými státy a orgány EU a přispívá k připravenosti Evropy s ohledem na budoucí kybernetické výzvy. V oblasti spolupráce se Agentura ENISA zapojuje do součinnosti s hlavními aktéry a v této spolupráci rozšiřuje znalosti, rozvíjí schopnosti a zvyšuje informovanost s cílem zaručit digitální bezpečnost pro všechny občany EU. [120]

5.6 NATO CCDCOE

CCDCOE (Cooperative Cyber Defence Centre of Excellence) je centrum kybernetické obrany, které bylo vytvořené Severoatlantickou aliancí NATO. Toto centrum se snaží podpořit a posílit své členské státy a NATO v oblasti

[119] Zákon č. 181/2014 Sb., *o kybernetické bezpečnosti v posledním znění*
[120] *Enisa.europa.eu: About ENISA* [online]. [cit.11.2.2024]. Dostupné z: https://www.enisa.europa.eu/about-enisa

kybernetické bezpečnosti na mezinárodní úrovni, a to prostřednictvím činností zahrnujících výzkum, výcvik a každoročně pořádaná cvičení zaměřená na kybernetickou obranu proti kybernetickým bezpečnostním incidentům mířeným na běžné IT prostředky, vojenské systémy a kritickou infrastrukturu. Kromě toho centrum iniciovalo veřejně známý a mezinárodně uznávaný dokument s názvem Tallinnský manuál 2.0, který pojednává o použití mezinárodního práva v rámci kybernetických operací. Centrum má své sídlo ve městě Tallinn v Estonsku a v současné době pojímá 30 členských států, které jsou součástí NATO a jsou označeny jako „sponzorské národy", a dále 9 států nepatřících mezi NATO, které jsou označeny jako „přispívající účastníci".[121]

[121] *Ccdcoe.org: About us* [online]. [cit.19.2.2024]. Dostupné z: https://ccdcoe.org/about-us/

6. Dokumenty řešící kybernetickou bezpečnost v ČR

6.1 Audit národní bezpečnosti

Audit národní bezpečnosti je dokument z roku 2016, jenž byl vypracován Ministerstvem vnitra a je zaměřen na deset oblastí hrozeb, které ohrožují nejen ČR, ale i celou Evropu. Dokument je kromě bezpečnostních hrozeb jako je extremismus zaměřen rovněž na ty aktuální, které se týkají hrozeb v kyberprostoru. V této oblasti byla auditem analyzována rizika související s kybernetickou špionáží, kyberterorismem, odolností IT infrastruktury nebo ochranou eGovernmentu.[122]

6.2 Národní strategie kybernetické bezpečnosti ČR 2021–2025

Jedná se o strategii, která byla vytvořena Národním úřadem pro kybernetickou a informační bezpečnost a je zaměřena na tři hlavní cíle, ve kterých jsou popsány jednotlivé vize pro celkové zajištění kybernetické bezpečnosti v ČR:

- *„Sebevědomě v prostoru*
    - *Společný přístup ke kybernetické bezpečnosti;*
    - *Bezpečná infrastruktura;*
    - *Účinná strategická komunikace.*

- *Silná a spolehlivá spojenectví*
    - *Efektivní mezinárodní spolupráce;*
    - *Prohlubování a tvorba aktivních spojenectví;*
    - *Mezinárodní právní rámec;*
    - *Schopnosti a expertíza.*

- *Odolná společnost 4.0*
    - *Zabezpečení digitální společnosti a veřejné správy;*

[122] *Databaze-strategie.cz: Audit národní bezpečnosti (2016)* [online]. [cit.12.2.2024]. Dostupné z: https://www.databaze-strategie.cz/cz/mv/strategie/audit-narodni-bezpecnosti

- *Vzdělávání a osvěta;*
- *Rozšiřování expertní základny.“* [123]

[123]SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* 1. vydání. Brno: Akademické nakladatelství CERM, 2021. 44 s. ISBN 978-80-7623-068-2.

7. Zajištění kyberbezpečnosti prvku KI v rámci organizace

Tato kapitola se zaměřuje na praktický příklad způsobu zajišťování kybernetické bezpečnosti proti kybernetickým hrozbám v dané organizaci, která je součástí kritické informační infrastruktury. V tomto ohledu bude popsán princip řízení ISMS.

ISMS je anglická zkratka pro Information Security Management System a představuje řízení bezpečnosti informací na základě účinného dokumentovaného systému řízení a správy informačních aktiv zaměřeného na minimalizaci rizika jejich ztráty či poškození.

Tento systém identifikuje, chrání a řídí aktiva, analyzuje možná rizika, implementuje opatření s odpovídající úrovní zabezpečení a pravidelně je kontroluje.[124] Aktiva jsou v tomto smyslu rozdělena na primární a podpůrná.

Primární aktiva představují ty nejvýznamnější informace nebo data, které se v organizaci nachází. Organizace mají svůj jedinečný seznam těchto hlavních aktiv, které se odvíjejí od oboru, ve kterém působí.[125]

Mezi podpůrná aktiva patří lidské zdroje, hardware, software, objekty, dodavatelé (provozovatelé), externí systémy apod.[126]

V tomto procesu hrají zásadní roli tři velmi důležité prvky, kterými jsou důvěrnost, integrita a dostupnost.

Důvěrnost znamená, že ke konkrétní informaci mají přístup pouze osoby, které k tomu jsou oprávněny.[127] Integrita označuje, že je určitá informace příslušné osobě dodána v původním stavu a neobsahuje žádné úpravy či změny.[128]

---

[124] *Cybersecurity.cz: Systém řízení informační bezpečnosti* [online]. [cit.8.3. 2024]. Dostupné z: https://www.cybersecurity.cz/data/SRIB.pdf

[125] *Aptien.com: Jak identifikovat primární aktiva* [online]. [cit.8.3. 2024]. Dostupné z: https://aptien.com/cs/kb/articles/how-to-identify-primary-information-assets

[126] *Aptien.com: Co jsou podpůrná informační aktiva* [online]. [cit.8.3. 2024]. Dostupné z: https://aptien.com/cs/kb/articles/what-are-primary-information-assets

[127] *Aptien.com: Co je důvěrnost (Confidentiality)* [online]. [cit.8.3. 2024]. Dostupné z: https://aptien.com/cs/kb/articles/what-is-confidentiality

[128] *Aptien.com: Co je integrita (Integrity)* [online]. [cit.8.3. 2024]. Dostupné z: https://aptien.com/cs/kb/articles/what-is-data-integrity

Dostupnost je charakterizována tak, že příslušný uživatel má schopnost obdržet data ze systému vždy, když je to potřeba.[129]

Bezpečnost těchto informací je v organizaci řízená přes rizika. Riziko představuje potenciál výskytu nežádoucí události. S rizikem souvisí hrozba, což je určitá nejistá událost, která může mít nežádoucí dopad. S hrozbou je spojena zranitelnost, která představuje slabé místo systému, které umožní působení hrozby. S tím související dopad charakterizuje velikost ztrát způsobených hrozbou, která zneužila zranitelnost. Platí tedy tento vzorec: Riziko = dopad x hrozba x zranitelnost.

Působnost organizace je současně regulována příslušným zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a souvisejícími vyhláškami. V souladu s tím musí být určeny povinné osoby a bezpečnostní opatření, která se rozdělují na technická a organizační.

Organizační opatření zahrnují systém řízení bezpečnosti informací, řízení rizik, bezpečnostní politiku, organizační bezpečnost, stanovení bezpečnostních požadavků pro dodavatele, řízení aktiv, bezpečnost lidských zdrojů, řízení provozu a komunikací, řízení přístupu osob, akvizicí, vývoj a údržbu, zvládání kybernetických bezpečnostních incidentů, řízení kontinuity činností, kontrolu a audit.

Technická opatření obsahují fyzickou bezpečnost, nástroj pro ochranu integrity komunikačních sítí, nástroj pro ověřování identity uživatelů, nástroj pro řízení přístupových oprávnění, nástroj pro ochranu před škodlivým kódem, nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů, nástroj pro detekci kybernetických bezpečnostních událostí, aplikační bezpečnost, kryptografické prostředky, nástroj pro zajišťování úrovně dostupnosti informací a bezpečnost průmyslových a řídících systémů.[130]

Nutná je rovněž aplikace zákonných požadavků v prostředí organizace, která se týká lidí, procesů a technologií operujících v organizaci. Lidé působící v organizaci

[129] *Aptien.com: Co je dostupnost (Availability)* [online]. [cit.8.3. 2024]. Dostupné z: https://aptien.com/cs/kb/articles/what-is-availability
[130] Zákon č. 181/2014 Sb., *o kybernetické bezpečnosti v posledním znění*

musí být pravidelně školeni, aby měli bezpečnostní povědomí o daných hrozbách a jsou povinni provádět testy sociální odolnosti.

V rámci procesů v organizaci se klade důraz na řídící dokumentace, chování uživatelů informačních systémů a na zajištění dobré praxe. Tyto procesy jsou současně kontrolovány. Management dohlíží na dodržování stanovených pravidel a interní audit kontroluje efektivitu ISMS v organizaci a provádí penetrační testy, pomocí kterých identifikuje zranitelnosti, které by mohly být součástí aktiva. Dále je organizace kontrolována Národním úřadem pro kybernetickou a informační bezpečnost, který kontroluje dodržováni kybernetického zákona a jeho vyhlášek a provádí Externí audit informační bezpečnosti.

Nedílnou součástí organizace jsou jednotlivé technologie a procesy, které zabezpečují organizaci proti kybernetickým hrozbám:

- Antivirus – bezpečnostní program sloužící k vyhledávání, detekování, blokování a eliminaci kybernetických hrozeb; [131]
- EDR (Endpoint Detection and Response) – bezpečnostní technologie soustředící se na identifikaci a odpověď na rizika na koncových zařízeních;[132]
- NDR (Network Detection and Response) – technologie, která využívá strojového učení a odstraňuje nedostatky v infrastruktuře a umožňuje IT týmu monitorovat infrastrukturu v okamžitém čase; [133]
- XDR (Extended Detection and Response) – software rozšířené detekce a reakce; [134]
- Log Management – nepřetržitý proces centrálního shromažďování, uchovávání, vyhodnocování a odstraňování dat, který přináší užitečné

[131] *Eset.com*: *Antivirus* [online]. [cit.8.3. 2024]. Dostupné z: https://www.eset.com/cz/antivirus-software/
[132] *Comguard.cz: Služby v oblasti Endpoint Detection and Response* [online]. [cit.8.3. 2024]. Dostupné z: https://www.comguard.cz/endpoint-detection-and-response-edr
[133] *Comguard.cz: LogRhythm Network Detection and Response (NDR)* [online]. [cit.8.3. 2024]. Dostupné z: https://www.comguard.cz/logrhythm-ndr
[134] *Microsoft.com: Co je rozšířená detekce a reakce (XDR)?* [online]. [cit.8.3. 2024]. Dostupné z: https://www.microsoft.com/cs-cz/security/business/security-101/what-is-xdr

informace k podpoře řešení problémů, posílení výkonu nebo sledování zabezpečení; [135]

- SIEM (Security Information and Event Management) – technologie, která umožňuje organizacím identifikovat potencionální nebezpečí, provést jejich analýzu a podniknout kroky k odvrácení škody ještě předtím, než by mohla ohrozit běžný chod firmy; [136]
- SOAR (Security Orchestration, Automation and Response) – technologie nabízející plně integrovaný systém, který automaticky rozpoznává bezpečnostní hrozby a bez potřeby lidského zásahu na ně reaguje; [137]
- IDM (Identity management) – Sjednocená správa identit v IT systémech, která poskytuje oprávněným uživatelům přístup k vhodným prostředkům v pravou chvíli a za správných podmínek, přičemž jsou veškeré aktivity dokumentovány; [138]
- Firewall – bezpečnostní opatření v počítačové síti, které pečlivě vyhodnocuje a reguluje tok dat podle stanovených pravidel, v IT prostředí představuje software či hardware, který filtrováním řídí komunikaci mezi důvěryhodnými a nedůvěryhodnými sítěmi; [139]
- IDS (Intrusion Prevention System), IPS (Intrusion Detection System) – systémy určeny pro detekci a prevenci průniku, kterými je sledována síť nebo činnost operačního systému v rámci škodlivého působení; [140]
- Honeypot – aplikace umožňující simulovat reálná zařízení zahrnující jejich vlastnosti a prvky, která funguje jako léčka pro útočníky, kteří se pokoušejí vniknout do určité sítě či nějakého zařízení v rámci této sítě;[141]

[135] *Solarwinds.com: What is Log Management?* [online]. [cit.8.3. 2024]. Dostupné z: https://www.solarwinds.com/resources/it-glossary/log-management
[136] *Microsoft.com: Co je SIEM?* [online]. [cit.8.3. 2024]. Dostupné z: https://www.microsoft.com/cs-cz/security/business/security-101/what-is-siem
[137] *Microsoft.com: Co je SOAR?* [online]. [cit.8.3. 2024]. Dostupné z: https://www.microsoft.com/cs-cz/security/business/security-101/what-is-soar
[138] *Blog.bcvsolutions.eu: Co je to Identity Management* [online]. [cit.8.3. 2024]. Dostupné z: https://blog.bcvsolutions.eu/co-je-to-identity-management/
[139] *Eset.com: Firewall* [online]. [cit.8.3. 2024]. Dostupné z: https://www.eset.com/cz/firewall/
[140] *Ict.nwt.cz: Systémy detekce a prevence průniku* [online]. [cit.8.3. 2024]. Dostupné z: https://ict.nwt.cz/blog/systemy-detekce-a-prevence-pruniku/
[141] *It-slovnik.cz: Co je to Honeypot?* [online]. [cit.8.3. 2024]. Dostupné z: https://it-slovnik.cz/pojem/honeypot

- MFA (Multi-Factor Authentication) – postup ověření totožnosti, při kterém je kromě prostého zadání přihlašovacích údajů nutné tuto identitu prokázat dalšími metodami (např. jednorázovým kódem skrze SMS);[142]

[142] *Upce.cz: Multifaktorová autentizace* [online]. [cit.8.3. 2024]. Dostupné z: https://www.upce.cz/multifaktorova-autentizace

8. Hodnocení ochrany prvků KI s důrazem na kyberbezpečnost

Zásadní význam v rámci zvýšení ochrany prvků KI má nyní evropská směrnice CER, která je zaměřena na zvýšení odolnosti těchto kritických subjektů a směrnice NIS 2, která se soustředí na celkové zesílení kybernetické bezpečnosti v rámci všech členských států EU.

Tyto směrnice vycházejí z dosavadních zkušeností jednotlivých států EU a snaží se reagovat na aktuální hrozby a předcházet jim.

Důležitým aspektem v případě kybernetických hrozeb je národní strategie kybernetické bezpečnosti, kterou má v rámci posílení vysoké úrovně kybernetické bezpečnosti každý členský stát přijmout a která má sloužit pro vzájemnou koordinaci a spolupráci ve sdílení informací o rizicích, kybernetických incidentech.

Dalším kladným bodem je spolupráce členského státu prostřednictvím jeho orgánů, které mezi sebou mají spolupracovat a pravidelně si mezi sebou vyměňovat informace o těchto rizicích a kybernetických bezpečnostních incidentech a následných opatřeních, které orgány přijmou.

Velkým kladem je rovněž spolupráce členských států na unijní a mezinárodní úrovni, která má být zajištěna prostřednictvím skupiny pro spolupráci, díky které mohou jednotlivé státy získat praxi a zavést účinná opatření ke zvýšení ochrany proti kybernetickým hrozbám.

Celkově lze tedy obě směrnice hodnotit velmi kladně. Určitě však záleží na tom, jak se tyto směrnice projeví v praxi potom, co dojde k promítnutí směrnic do vnitrostátního práva jednotlivých členských států.

9. Návrh na zdokonalení kybernetické bezpečnosti

Zvyšování povědomí o kybernetické bezpečnosti – je důležité, aby docházelo k pravidelné osvětě a vzdělávání v rámci kybernetické bezpečnosti se zaměřením na aktuální kybernetické hrozby, a to především v rámci státních orgánů zajišťujících kybernetickou bezpečnost a u organizací, které jsou nebo se v budoucnu stanou součástí kritické informační infrastruktury.

Posilování legislativní stránky – stejně tak jako je tomu nyní, tak i nadále bude zapotřebí revidovat a aktualizovat právní úpravu s ohledem na nově vznikající hrozby v kyberprostoru.

Rozvoj pokročilých technologií – kybernetické útoky se stávají čím dál důmyslnějšími a propracovanějšími a v souladu s tím bude nezbytné využívat moderní technologie, které budou schopny na tyto útoky efektivně reagovat.

Investování v rámci kybernetické bezpečnosti – podpora prostřednictvím finančních prostředků do moderních technologií, vzdělávání a výzkumu by mohla celkově zlepšit úroveň kybernetické bezpečnosti.

Zvýšení počtu kvalifikovaných odborníků – počet expertů přes kybernetickou bezpečnost v současné době není dostatečný a tento problém se neustále zvětšuje. V tomto případě by bylo vhodné zahrnout vzdělávací metody a školení pro rozvoj odborné kvalifikace a praxe v tomto oboru.

Závěr

Cílem této bakalářské práce bylo popsat, jakým způsobem jsou chráněny prvky kritické infrastruktury s důrazem na elektronickou ochranu a kyberbezpečnost a tyto způsoby zhodnotit.

Z pohledu kybernetické bezpečnosti je vidět, že se této oblasti věnuje celá řada státních orgánů, právních předpisů a dokumentů.

Nejen Česká republika, ale i ostatní státy v rámci Evropské unie jsou si vědomy neustále přibývajících a čím dál tím více rafinovanějších kybernetických hrozeb, které mohou významně ohrozit vysoce kritická odvětví a tím způsobit rozsáhlé škody i ztráty na lidských životech.

To se projevilo do evropských směrnic CER a NIS 2, které by měly posílit celkovou odolnost kritických subjektů a zajistit vysokou společnou úroveň kybernetické bezpečnosti.

Národní strategie kybernetické bezpečnosti, spolupráce členského státu prostřednictvím jeho orgánů a vzájemná spolupráce těchto států na unijní a mezinárodní úrovni jsou významnými aspekty, které by měly přispět k posílení kybernetické bezpečnosti. V tomto ohledu je důležité, aby členské státy přijaly tyto směrnice co nejefektivněji do vnitrostátní legislativy. Vzhledem k neustále vyvíjejícím se kybernetickým hrozbám bude zapotřebí, aby k takovýmto legislativním změnám a aktualizacím docházelo i nadále.

Kromě toho by bylo vhodné pravidelně zvyšovat povědomí o kybernetické bezpečnosti systematickým vzděláváním a osvětou, rozvíjet pokročilé technologie, které budou schopny účinně reagovat na sofistikované kybernetické útoky, zvyšovat počet kvalifikovaných odborníků přes kybernetickou bezpečnost a podpořit investování v této oblasti. Všechny tyto faktory by zcela jistě přispěly k celkovému zajištění kybernetické bezpečnosti.

Seznam použité literatury

Monografie

1. RAMEŠOVÁ, Kristina. *Právní regulace kybernetické bezpečnosti a její meze.* 1. vydání. Praha: C. H. Beck, 2023. ISBN 978-80-7400-931-0.
2. SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* 1. vydání. Brno: Akademické nakladatelství CERM, 2021. ISBN 978-80-7623-068-2.
3. SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti.* Plzeň: Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.
4. ŠULC, Vladimír. *Kybernetická bezpečnost.* Plzeň: Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.
5. ŠENOVSKÝ, Michal, Pavel ŠENOVSKÝ a Vilém ADAMEC. *Ochrana kritické infrastruktury*. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2007. ISBN 978-80-735-025-8.

Právní předpisy

1. Nařízení vlády č. 432/2010 Sb., *o kritériích pro určení prvku kritické infrastruktury v posledním znění*
2. Nařízení vlády č. 315/2014 Sb., *kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury v posledním znění*
3. Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022, *o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES*
4. Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022, *o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)*
5. Zákon č. 240/2000 Sb., *o krizovém řízení v posledním znění*
6. Zákon č. 181/2014 Sb., *o kybernetické bezpečnosti v posledním znění*

7. Zákon č. 183/2006 Sb., *o územním plánování a stavebním řádu ve znění k 31.12.2023*

Webové stránky a elektronické zdroje

1. *Aptien.com: Co je dostupnost (Availability)* [online]. [cit.8.3. 2024]. Dostupné z: https://aptien.com/cs/kb/articles/what-is-availability
2. *Aptien.com: Co je důvěrnost (Confidentiality)* [online]. [cit.8.3. 2024]. Dostupné z: https://aptien.com/cs/kb/articles/what-is-confidentiality
3. *Aptien.com: Co je integrita (Integrity)* [online]. [cit.8.3. 2024]. Dostupné z: https://aptien.com/cs/kb/articles/what-is-data-integrity
4. *Aptien.com: Co jsou podpůrná informační aktiva* [online]. [cit.8.3. 2024]. Dostupné z: https://aptien.com/cs/kb/articles/what-are-primary-information-assets
5. *Aptien.com: Jak identifikovat primární aktiva* [online]. [cit.8.3. 2024]. Dostupné z: https://aptien.com/cs/kb/articles/how-to-identify-primary-information-assets
6. *Avast.com: Sociální inženýrství* [online]. [cit.7.2.2024]. Dostupné z: https://www.avast.com/cs-cz/c-social-engineering
7. BLAŽKOVÁ, Kateřina a kol. *Ochrana obyvatelstva a krizové řízení* [online]. 1. vydání. Praha: MV – generální ředitelství Hasičského záchranného sboru ČR, 2015. ISBN 978-80-86466-62-0.
8. *Blog.bcvsolutions.eu: Co je to Identity Management* [online]. [cit.8.3. 2024]. Dostupné z: https://blog.bcvsolutions.eu/co-je-to-identity-management/
9. *Ccdcoe.org: About us* [online]. [cit.19.2.2024]. Dostupné z: https://ccdcoe.org/about-us/
10. *Comguard.cz: LogRhythm Network Detection and Response (NDR)* [online]. [cit.8.3. 2024]. Dostupné z: https://www.comguard.cz/logrhythm-ndr
11. *Comguard.cz: Služby v oblasti Endpoint Detection and Response* [online]. [cit.8.3. 2024]. Dostupné z: https://www.comguard.cz/endpoint-detection-and-response-edr
12. *Cybersecurity.cz: Systém řízení informační bezpečnosti* [online]. [cit.8.3. 2024]. Dostupné z: https://www.cybersecurity.cz/data/SRIB.pdf

13. *Databaze-strategie.cz: Audit národní bezpečnosti (2016)* [online]. [cit.12.2.2024]. Dostupné z: https://www.databaze-strategie.cz/cz/mv/strategie/audit-narodni-bezpecnosti
14. *Databaze-strategie.cz: Komplexní strategie ČR k řešení problematiky kritické infrastruktury (2010)* [online]. [cit.6.2.2024]. Dostupné z: https://www.dataplan.info/img_upload/7bdb1584e3b8a53d337518d988763f8d/komplexni-strategie-ki.pdf
15. *Enisa.europa.eu: About ENISA* [online].[cit.11.2.2024]. Dostupné z: https://www.enisa.europa.eu/about-enisa
16. *Eset.com*: *Antivirus* [online]. [cit.8.3. 2024]. Dostupné z: https://www.eset.com/cz/antivirus-software/
17. *Eset.com: Co je počítačový vir + druhy virů* [online]. [cit.7.2.2024]. Dostupné z: https://www.eset.com/cz/virus/
18. *Eset.com: Firewall* [online]. [cit.8.3. 2024]. Dostupné z: https://www.eset.com/cz/firewall/
19. *Eset.com: Trojský kůň* [online]. [cit.7.2.2024]. Dostupné z: https://www.eset.com/cz/trojsky-kun/
20. *Govcert.cz: Rada pro kybernetickou bezpečnost* [online]. [cit.7.3.2024]. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/
21. *Hzscr.cz: Evropský program na ochranu kritické infrastruktury* [online]. [cit.6.2.2024]. Dostupné z: https://www.hzscr.cz/clanek/evropsky-program-na-ochranu-kriticke-infrasruktury.aspx
22. *Ict.nwt.cz: Systémy detekce a prevence průniku* [online]. [cit.8.3. 2024]. Dostupné z: https://ict.nwt.cz/blog/systemy-detekce-a-prevence-pruniku/
23. *It-slovnik.cz: Co je to Hardware?* [online]. [cit.7.2.2024]. Dostupné z: https://it-slovnik.cz/pojem/hardware
24. *It-slovnik.cz: Co je to Honeypot?* [online]. [cit.8.3. 2024]. Dostupné z: https://it-slovnik.cz/pojem/honeypot
25. *It-slovnik.cz: Co je to Software?* [online]. [cit.7.2.2024]. Dostupné z: https://it-slovnik.cz/pojem/software
26. *It-slovnik.cz*: *Co je to Trojský kůň?* [online]. [cit.7.2.2024]. Dostupné z: https://it-slovnik.cz/pojem/trojsky-kun

27. *Legislativa.cz: Kybernetický útok: definice, typy, následky a prevence* [online]. [cit.6.2.2024]. Dostupné z: https://legislativa.cz/zdroje/kyberneticka-bezpecnost/kyberneticky-utok
28. *Microsoft.com: Co je rozšířená detekce a reakce (XDR)?* [online]. [cit.8.3. 2024]. Dostupné z: https://www.microsoft.com/cs-cz/security/business/security-101/what-is-xdr
29. *Microsoft.com: Co je SIEM?* [online]. [cit.8.3. 2024]. Dostupné z: https://www.microsoft.com/cs-cz/security/business/security-101/what-is-siem
30. *Microsoft.com: Co je SOAR?* [online]. [cit.8.3. 2024]. Dostupné z: https://www.microsoft.com/cs-cz/security/business/security-101/what-is-soar
31. *Microsoft.com: Definice útoků DDoS.* [online]. [cit.7.2.2024]. Dostupné z: https://www.microsoft.com/cs-cz/security/business/security-101/what-is-a-ddos-attack
32. *Modul G – vnitřní bezpečnost a veřejný pořádek a vybrané kapitoly krizového řízení: studijní text k problematice bezpečnosti zpracované dle Koncepce z roku 2004* [online]. Ministerstvo vnitra: odbor bezpečnosti, Praha – aktualizace 2014 [cit. 5.3.2024]. Dostupné z: https://www.hzscr.cz/clanek/moduly-studijni-texty-k-problematice-bezpecnosti-zpracovane-dle-koncepce-z-roku-2004.aspx
33. *Mvcr.cz: Ochrana kritické infrastruktury* [online]. [cit.6.2.2024]. Dostupné z: https://www.mvcr.cz/chh/clanek/ochrana-kriticke-infrastruktury-ochrana-kriticke-infrastruktury.aspx
34. *Nukib.gov.cz: Kybernetická bezpečnost* [online]. [cit.10.2.2024]. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/
35. *Nukib.gov.cz: NÚKIB* [online]. [cit.10.2.2024]. Dostupné z: https://nukib.gov.cz/cs/o-nukib/
36. *Nukib.gov.cz*: *Organizační struktura úřadu* [online]. [cit.10.2.2024]. Dostupné z: https://nukib.gov.cz/cs/o-nukib/organizacni-struktura-uradu/
37. *Nukib.gov.cz: Vládní CERT* [online]. [cit.11.2.2024]. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vladni-cert/

38. *Osveta.nukib.cz: Návrh nového zákona o kybernetické bezpečnosti a dalších předpisů* [online]. [cit.7.3.2024]. Dostupné z: https://osveta.nukib.cz/course/view.php?id=145#section-3
39. *Osveta.nukib.cz: Obecné informace o směrnici NIS2 a budoucí národní úpravě* [online]. [cit.8.2.2024]. Dostupné z: https://osveta.nukib.cz/mod/page/view.php?id=2582
40. *Policie.cz: Kyberkriminalita* [online]. [cit.6.2.2024]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx
41. *Solarwinds.com: What is Log Management?* [online]. [cit.8.3. 2024]. Dostupné z: https://www.solarwinds.com/resources/it-glossary/log-management
42. *Upce.cz: Multifaktorová autentizace* [online]. [cit.8.3. 2024]. Dostupné z: https://www.upce.cz/multifaktorova-autentizace
43. *Vlada.gov.cz: Statut Výboru pro kybernetickou bezpečnost* [online]. [cit.7.3.2024]. Dostupné z: https://vlada.gov.cz/assets/ppov/brs/pracovni-vybory/Kyberneticka_bezpecnost/statut-vkb-2024.pdf
44. *Zakonyprolidi.cz: Důvodová zpráva k návrhu zákona o odolnosti subjektů kritické infrastruktury a o změně některých zákonů* [online]. [cit.27.2.2024]. Dostupné z: https://www.zakonyprolidi.cz/monitor/7855524.htm
45. *Zakonyprolidi.cz: Návrh zákona o odolnosti subjektů kritické infrastruktury a o změně dalších zákonů (zákon o kritické infrastruktuře)* [online]. [cit.27.2.2024]. Dostupné z: https://www.zakonyprolidi.cz/monitor/7855524.htm

Seznam použitých zkratek

CER	Critical Entities Resilience
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
ČNB	Česká národní banka
ČR	Česká republika
DNS	Domain Name System
DDoS	Distributed Denial of Service
EDR	Endpoint Detection and Response
EU	Evropská unie
ICT	Infomation and Communication Technologies
IDM	Identity Management
IDS	Intrusion Prevention System
IKT	informační a komunikační technologie
IPS	Intrusion Detection System
ISMS	Information Security Management System
IT	Information Technology
KI	kritická infrastruktura
LNG	Liquefied Natural Gas
MFA	Multi-Factor Authentication
NATO	Severoatlantická aliance
NCKB	Národní centrum kybernetické bezpečnosti
NDR	Network Detection and Response
NIS	Network and Information Security
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
SIEM	Security Infomation and Event Management
SOAR	Security Orchestration, Automation and Response
SSAS	Sekce strategických agend a spolupráce
TLD	Top Level Domain
XDR	Extended Detection and Response