https://doi.org/10.5817/RPT2019-2-5

CERTIFIKACE KYBERBEZPEČNOSTNÍCH TECHNOLOGIÍ[1]

JAKUB VOSTOUPAL[2]

ABSTRAKT

Tento článek pojednává o certifikaci jako o jednom z nástrojů posuzování shody v oblasti technologií kybernetické bezpečnosti. V článku je vysvětlena problematika compliance a jejích výhod oproti obecnému odpovědnostnímu režimu, vysvětlena funkce posuzování shody a certifikace jak obecně, tak v kyberbezpečnostním prostředí, shrnutý stav současné úpravy certifikace kyberbezpečnostních technologií v ČR a EU a představení nadcházející úpravy jednotného evropského certifikačního rámce. V druhé části příspěvku autor představuje konkrétní certifikační systémy včetně institucionálního, organizačního a procesního zabezpečení. Pozornost je přitom zaměřena na systém Common Criteria a chystanou evropskou úpravu podle Aktu o kybernetické bezpečnosti. Pro úplnost jsou stručně rozebrány i vnitrostátní certifikační schémata z vybraných evropských států.

[1] Tento článek vznikl za podpory projektu "Centrum excelence pro kyberkriminalitu, kyberbezpečnost a ochranu kritických informačních infrastruktur" reg.č.: CZ.02.1.01/0.0/0.0/16_019/0000822 financovaného z EFRR. Článek vychází z autorovy diplomové práce "Certifikace kyberbezpečnostních technologií" (dostupná z: https://is.muni.cz/th/ggumu/). Autor děkuje za podnětné připomínky anonymním recenzentům článku.

[2] Mgr. Jakub Vostoupal je doktorandem na Ústavu práva a technologií Právnické fakulty Masarykovy univerzity a studentem bakalářského studia psychologie na Fakultě sociálních studií Masarykovy univerzity. Vedle toho působí v rámci několika projektů pod Právnickou fakultou a Fakultou informatiky Masarykovy univerzity, e-mail: Jakvost@gmail.com.

KLÍČOVÁ SLOVA:

Kybernetická bezpečnost, posuzování shody, certifikace, compliance, Common Criteria, Akt o kybernetické bezpečnosti

ABSTRACT

This article deals with certification as one of the instruments of conformity assessment in the area of cybersecurity technologies. The article explains the issue of compliance and its advantages over general liability regime. The text continues with an explanation of conformity assessment and certification both in general and in cybersecurity environment, followed by a summarization of the current state of regulation of certification of cybersecurity technologies in the Czech Republic and the EU and by an introduction of the forthcoming regulation of the unified European certification framework. In the second part of the article, the author presents specific certification systems including their institutional, organizational and procedural aspects. Attention is primarily given to the system of Common Criteria and the European regulation – the Cyber-Security Act. The author completes the comparison by introducing national certification schemes from selected European countries.

KEYWORDS:

Cyber-security, conformance assessment, certification, compliance, Common Criteria, the Cybersecurity Act

SEZNAM NEJDŮLEŽITĚJŠÍCH POJMŮ A ZKRATEK

Agentura	Evropská agentura pro bezpečnost sítí a informací, také jako „*ENISA*“
Akt	Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („*Agentuře Evropské unie pro kybernetickou bezpečnost*“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013
ANSSI	Agence nationale de la sécurité des systémes d’information

BSPA	Baseline Security Product Assessment
CAB	Conformance Assessment Body
CC	Common Criteria for Information Technology Security Evaluation
CCRA	Common Criteria Recognition Agreement
CEM	Common Evaluation Methodology
CPA	Commercial Product Assurance
CSPN	Certification Sécuritaure de Premier Niveau
ČIA	Český institut pro akreditaci, o.p.s.
EAL	Evaluation Assurance Level
eIDAS	Nařízení Evropského parlamentu a Rady o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu
GDPR	General Data Protection Regulation, Obecné nařízení o ochraně osobních údajů
ICT	Informační a komunikační technologie
ISMS	Information Security Management System (Systém řízení bezpečnosti informací)
ISO	International Standards Organization (Mezinárodní organizace pro standardizaci)
MRA	Mutual Recognition Agreement/Arrangement (Dohoda o vzájemném uznávání)
NBÚ	Národní bezpečnostní úřad
NCCA	National Cybersecurity Certification Authority (Národní autorita pro certifikaci kybernetické bezpečnosti)
NIS	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
NLCSA	Nationaal Bureau voor Verbindingsbeveiliging
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PP	Protection Profile, Profil ochrany

Program	Průběžný pracovní program Unie pro evropskou certifikaci kybernetické bezpečnosti
SFEU	Smlouva o fungování EU
Skupina	Evropská skupina pro certifikaci kybernetické bezpečnosti
SOG-IS	Senior Officials Group Information Systems Security
SOG-IS MRA	Senior Officials Group Information Systems Security Mutual Recognition Agreement
ST	Security Target, Bezpečnostní cíl
TOE	Target of Evaluation, Předmět posuzování
ÚNMZ	Úřad pro technickou normalizaci, metrologii a státní zkušebnictví

1. ÚVOD

S příchodem internetu věcí se každým rokem rapidně zvyšuje počet zařízení, která jsou připojena k internetu.[3] V rámci kyberprostoru je však již delší dobu patrný trend oslabení bezpečnosti, a přestože dle Europolu byl v roce 2019 zaznamenán určitý pokles v množství útoků provedených online, ekonomický dopad kyberkriminality se dále zvyšuje.[4] Připojování nezabezpečených technologií pozici útočníků jenom zjednodušuje.

Ke zvýšení důvěry uživatelů v nové technologie je v takovém prostředí nutné začít řešit kybernetickou bezpečnost, a to i v případě jednotlivých „stavebních kamenů“ informačních systémů. Jednou z cest jak posílit důvěru i bezpečnost je pak právě certifikace.

Na téma kybernetické bezpečnosti bylo již napsáno mnoho vědeckých prací, přesto však zůstává problematika certifikace kyberbezpečnostních

[3] Dle předběžných odhadů Komise z roku 2016 se počet zařízení připojených k internetu měl zvýšit z přibližně 1,8 milionu v roce 2013 na téměř šest miliard v roce 2020. Více viz Commission Staff Working Document: Advancing the Internet of Things in Europe [online]. B.m.: European Commission. 2016. Tento trend bude pravděpodobně ještě dále umocněn nástupem 5G sítí, které dané připojování značně zjednoduší. Více viz např. Report: EU coordinated risk assessment of the cybersecurity of 5G networks [online]. B.m.: NIS Cooperation Group. 2019.

[4] To je způsobeno zejména tím, že útočníci se začínají soustředit na ekonomicky výnosnější cíle než třeba na plošný dopad ransomwaru. Více viz IOCTA: Internet Organised Crime Threat Assessment 2019 [online]. B.m.: Europol – European Cybercrime Centre. 2019.

technologií tématem nepříliš známým. Cílem tohoto článku je tak úkol zmapovat tuto problematiku a představit ji čtenáři. K naplnění tohoto cíle si kladu dvě výzkumné otázky:

Jak fungují stávající certifikační systémy?

Jak tuto funkci zlepší Akt o kybernetické bezpečnosti[5]?

Pozornost přitom věnuji srovnání certifikačního systému Common Criteria[6] a připravovaného evropského certifikačního rámce podle Aktu o kybernetické bezpečnosti. Dílčím cílem článku bude i vyhodnocení slabin obou zmíněných systémů.

Vzhledem k tomu, že téma je nesmírně živé a část Aktu o kybernetické bezpečnosti věnující se certifikaci stále není účinná, byla teoretická (statická) materie zakonzervována ke dni 25. 12. 2018 a části, u kterých došlo k výraznějším změnám, byly aktualizovány ke dni 12. 10. 2019.

K tomu, abych dokázal odpovědět na výše zmíněné otázky, přistoupím v obecné části článku nejdříve k představení pojmu compliance a certifikace, která je jedním z typů posuzování shody (tedy compliance). Dále se budu věnovat druhům regulatorních požadavků, neboť je nutné pochopit, jakým způsobem se pravidla, se kterými se shoda posuzuje, formulují a kdy je certifikace vůbec třeba.

V další kapitole budou představena bezpečnostní opatření, jejichž implementace se v rámci procesu certifikace posuzuje, popíšu stávající úpravu certifikace v ČR a pokusím se o její teoretické zasazení do systému kybernetické bezpečnosti v České republice. Na závěr kapitoly rozeberu stav, který panuje v Evropské unii.

---

[5] Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost"), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 (dále také jako „*Akt o kybernetické bezpečnosti*" nebo „*Akt*")

[6] Přestože Výkladový slovník kybernetické bezpečnosti zná Common Criteria pod oficiálním českým překladem „*Společná kritéria*" (viz JIRÁSEK, Petr; NOVÁK, Luděk; POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti*. 3., aktualiz. vyd. Praha, Česká republika: Policejní akademie ČR v Praze: Česká pobočka AFCEA, 2015, s. 155), je v českém prostředí možné používat i originální anglickou verzi (činí tak např. Národní bezpečnostní úřad v níže citovaném informačním materiálu o Common Criteria), čehož v celém příspěvku využívám.

Ve čtvrté kapitole věnuji pozornost teoretické stránce a vývoji Aktu, přičemž se soustředím na jeho nejvíce problematické aspekty v průběhu vyjednávání. Touto kapitolou končí obecná část, která ve svém celku má sloužit jako teoretický základ pro pochopení, jak fungují certifikační systémy a rámcově i jaký typ změny s sebou přináší Akt o kybernetické bezpečnosti.

Článek ve zvláštní části přechází ke konkrétnímu popisu a analýze organizační, institucionální a procesní struktury aktuálních certifikačních schémat v prostředí mezinárodních iniciativ, národních úprav v prostředí vybraných evropských států a nakonec i v rámci Aktu samotného. V páté kapitole se věnuji aktivitě Mezinárodní společnosti pro standardizaci, rodině standardů ISO 27K a největšímu stávajícímu certifikačnímu systému – Common Criteria. Standardy ISO 27K sice nedopadají na certifikaci kyberbezpečnostních technologií, ale Akt vtahuje do své úpravy i materii upravenou těmito standardy, a tak je vhodné se s nimi seznámit, aby byla lépe pochopena povaha Aktu.

V šesté kapitole rozebírám národní schémata čtyř evropských certifikačních velikánů – Velké Británie, Francie, Nizozemí a Německa.[7,8] Jejich schémata jsou nejpokročilejší reakcí na slabiny systému Common Criteria a je tak možné je využít ke kritickému zhodnocení jak CC, tak Aktu (což je provedeno v kapitole sedmé).

Článek čerpá zejména z článků zahraničních odborných časopisů a monografií, a to hlavně pro značný nedostatek českých zdrojů[9] (díla českých autorů jsou využita hlavně v teoretické části). Neméně důležitou

[7] Toto je patrné z výzkumů a pracovních dokumentů Komise doplňujících prvotní návrh Aktu o kybernetické bezpečnosti (viz State of the Union 2017: Cybersecurity - EU Agency and Certification Framework. B.m.: European Commission). Explicitně byly tyto státy takto označeny na worshopu o budoucnosti ICT certifikace v Evropě, viz Joint EC/ENISA SOG-IS and ICT certification workshop – Minutes of the workshop [online]. 6. říjen 2014 [vid. 24. srpen 2018].

[8] Více viz DROGKARIS, Prokopios. *Considerations on ICT security certification in EU - Survey Report* [online]. B.m.: European Union Agency for Network and Information Security. 2017 [vid. 9. září 2018]; Pracovní dokument útvarů komise - Souhrn posouzení dopadů k návrhu *aktu o kybernetické bezpečnosti* [online]. B.m.: Evropská komise. 2017 [vid. 12. červenec 2018].

roli zastávají prezentace z odborných konferencí, zprávy a výzkumy unijních orgánů, znění normativních předpisů a konzultace s odborníky.

2. COMPLIANCE A CERTIFIKACE

Vysoká představitelka Unie pro zahraniční věci a bezpečnostní politiku upozornila[10] dne 13. 9. 2017 na studie,[11] ze kterých vyplývá, že hospodářský dopad kyberkriminality se mezi lety 2013 až 2017 zvýšil pětinásobně a do roku 2019 by se mohl ještě dále zčtyřnásobit.[12] Mezi kybernetickou kriminalitou a kybernetickou bezpečností existuje úzká vazba a provázanost,[13] a s narůstající kyberkriminalitou se tak zhoršuje bezpečnostní situace kyberprostoru celé Unie, přičemž rizika rostou téměř exponenciálně. To zároveň snižuje důvěru uživatelů v nové technologie a zpomaluje technologický postup (včetně negativního dopadu na zavádění internetu věcí).[14]

Aby byla bezpečnost v kyberprostoru posílena a tento znepokojivý trend zastaven (nebo přinejmenším zpomalen), politické reprezentace mnohých zemí se začaly kybernetickou bezpečností zabývat důkladněji. Příkladem

---

[9] Tuto skutečnost si autor příspěvku potvrdil nejen při samotném hledání pramenů, ale i konzultacemi s odborníky. O problematice kyberbezpečnostní certifikace je stručně pojednáno např. v POLČÁK, Radim; HARAŠTA, Jakub; STUPKA, Václav. *Právní problémy kybernetické bezpečnosti* [online]. 1. vydání. Brno: Masarykova univerzita, 2016 [vid. 10. srpen 2018].

[10] Učinila tak ve Společném sdělení Evropskému parlamentu a Radě ze dne 13. 9. 2017 „*Odolnost, odrazování a obrana: Budování silné kybernetické bezpečnosti pro EU*"

[11] V prohlášení citují jako jednu z použitých studií například „*Net losses: Estimating the Global Cost of Cybercrime*" (Čisté ztráty: Odhad globálních nákladů způsobených kyberkriminalitou), McAfee & Centre for Strategic and International Studies, 2014.

[12] To ve výsledku potvrzuje i zmiňovaná studie IOCTA. Více viz IOCTA: Internet Organised Crime Threat Assessment 2019 [online]. B.m.: Europol – European Cybercrime Centre. 2019.

[13] Boj proti kyberkriminalitě je součástí strategie národní kybernetické bezpečnosti na období let 2015-2020, a jako taková předpokládá mimo jiné přijímání legislativních kroků, které by vedly k minimalizaci škodlivého zneužívání ICT technologií. Více viz POLČÁK; HARAŠTA; STUPKA, op. cit., s. 125.

[14] V i z VYSOKÁ PŘEDSTAVITELKA UNIE PRO ZAHRANIČNÍ VĚCI A BEZPEČNOSTNÍ POLITIKU. *Společné sdělení Evropskému parlamentu a Radě ze dne 13. 9. 2017: Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU* [online]. 2017 [vid. 11. říjen 2018].

může být Česká republika se svým zákonem o kybernetické bezpečnosti, Unie a směrnice NIS, Spojené státy americké, které se obdobnými otázkami zabývají již od roku 1991, nebo Ruská federace, jejíž hlavní kyberbezpečnostní regulace byla vytvořena mezi roky 2006 a 2014 a která do roku 2020 plánuje kapacity v této oblasti dále významně rozvíjet.[15,16]

Regulatorní zátěž povinných subjektů, stanovená jednotlivými národními úpravami kybernetické bezpečnosti, se pro mnohé z nich může ukázat jako prakticky nezvladatelná, a to nejen kvůli náročné orientaci v pravidlech samotných, ale též kvůli např. „*risk-managementu*“,[17] ke kterému je nutná značná orientace v praxi. Analýza rizik, jakožto základní kámen „*risk-managementu*“, může být v praxi lidově řečeno kámen úrazu. Přitom je nezbytnou i pro vyhovění dalším regulatorním požadavkům, jako je tomu např. u institutu varování podle českého zákona o kybernetické bezpečnosti.[18]

2.1 OBECNĚ O COMPLIANCE

Pokud povinné subjekty nechtějí riskovat pokutu či trest, musí se regulatorními požadavky, které na ně klade normotvůrce, řídit a být s nimi v souladu, tedy dosáhnout stavu compliance. Compliance je v takové situaci určitým zvláštním druhem povinnosti, která může stát samostatně, bez závislosti na splnění či nesplnění jiných povinností. Za porušení compliance povinností tak může hrozit sankce, aniž by předtím došlo k reálnému ohrožení chráněných zájmů.[19,20]

---

[15] V i z TSAKANYAN, V.T. The role of cybersecurity in world politics. *Vestnik Rudn. International Relations* [online]. 2017, roč. 17, č. 2, s. 4–8 [vid. 25. únor 2019].

[16] Naopak třeba v Německu byl s přijetím kybernetické bezpečnosti jako politické priority po dlouhou dobu problém. Viz tamtéž.

[17] Zvládání rizik. Jedná se o proces, při kterém povinný subjekt musí vyhodnotit rizika, která mu hrozí, a stanovit ta, která jsou neakceptovatelná, a to buď podle interních předpisů a metodiky, nebo podle vnější regulace.

[18] Aféra Huawei mimo jiné ukázala, že mnoho subjektů není vůbec schopno varování zapracovat, neboť žádnou analýzu rizik nemají.

[19] Čímž se liší od standardní odpovědnosti. Podrobnější porovnání compliance povinností a obecného odpovědnostního modelu je provedeno v kapitole 2.2.

[20] Získáno na základě konzultací s doc. JUDr. Radimem Polčákem, Ph.D.

Základ anglického pojmu „*compliance*“ je ve slově „*to comply*“, což znamená podřídit se, být v souladu či ve shodě. Tento pojem vzešel z angloamerické právní a ekonomické terminologie (přesněji řečeno vzešel tento pojem ze Spojených států amerických). Nejedná se sice o pojem čistě právní, spíše korporátní, ale s tímto pojmem pracuje jak odborná literatura, tak judikatura (případně se vyskytuje i v právních předpisech). Doposud pro něj však nebyl nalezen dostatečně vhodný český ekvivalent.[21] Pro účely tohoto článku tedy budu používat jak pojem „*compliance*“, tak i „*shoda*“ nebo „*soulad*“.

Hurychová a Sýkora dále uvádějí, že „*za podstatu compliance je považováno zajištění souladu mezi společností vykonávanou (podnikatelskou) činností a obecně závaznými právními i jinými předpisy (včetně předpisů interních) a etickými standardy.*“[22] Tyto předpisy mohou být různé povahy a úrovně (úprava evropská, národní atd.), což podnikatelům a investorům situaci nezjednodušuje.

Compliance je kontinuální stav, povinný subjekt se musí regulatorními požadavky řídit neustále. Není tak dostačující konstatovat, že shody bylo dosaženo v určitém časovém bodě, ale je naopak nezbytné neustále monitorovat naplňování požadavků a činit příslušná opatření k zachování takového stavu.[23]

Dodržování stavu compliance představuje z pohledu společnosti určitý typ podnikatelského rizika, se kterým musí kalkulovat. Při vytváření regulatorních požadavků je tak nutné počítat s tím, že pokud budou celkové náklady na zavedení a udržení shody podstatně vyšší než případné postihy, je naivní očekávat od společností, že by pravidla hromadně dodržovaly. Nesmí se ovšem zapomenout, že do následků non-compliance se nezapočítávají pouze případné veřejnoprávní pokuty či tresty (od zavedení trestní odpovědnosti právnických osob je toto plně relevantní

[21] Viz HURYCHOVÁ, Klára; SÝKORA, Michal. *Compliance programy (nejen) v České republice*. Praha, Česká republika: Wolters Kluwer, 2018, s. 4–7.

[22] Viz tamtéž, s. 7.

[23] Viz tamtéž.

i pro právnické osoby), ale stejně tak i poškození pověsti, omezení pojistného plnění či soukromoprávní nároky na náhradu škody.[24]

K dosažení shody nestačí formalistická implementace jakýchsi prázdných pokynů, kterými se nikdo nebude řídit. Je nezbytné, aby společnost, na kterou dopadá regulatorní požadavek (dále také jako „*povinný subjekt*"), skutečně přijala nezbytná opatření, která budou mít potenciál k naplnění kýženého pozitivního stavu. Jen takové řešení totiž dokáže v případě kontroly nebo soudního sporu aktivovat pozitivní účinky stavu compliance (viz níže).[25] Tento aspekt je jedním z nejdůležitějších a zároveň nejzrádnějších. Jak bude níže popsáno, míra potenciálu, která je pro zmíněnou aktivaci dostatečná, nemusí být vždy explicitně a přesně stanovená, a působí tak nejistotu.

2.2 COMPLIANCE VS. STANDARDNÍ MODEL ODPOVĚDNOSTI (LIABILITY)

Standardní odpovědnostní model je, zjednodušeně řečeno, založen na vzniku sekundární povinnosti při porušení povinnosti primární. Pokud tedy povinný subjekt nesplní ať už komisivně nebo omisivně určitý regulatorní požadavek, vzniká mu sekundární povinnost, obvykle v podobě povinnosti nahradit škodu nebo strpět jiný druh trestu. Odpovědnostní sekundární povinnosti jsou tak úzce a neoddělitelně navázány na povinnosti primární a nemohou stát samy o sobě. Na stav naplnění primární povinnosti se pohlíží ex post, tedy až poté, co dojde k nějakému incidentu zasahujícího do právem chráněného objektu.

V momentě, kdy je pravidlo regulující chování povinného subjektu nastaveno obecněji (zvláště performativní pravidla, viz níže), způsobuje tento režim značné snížení právní jistoty povinných subjektů, neboť z důvodu absence oficiálních implementačních postupů a návodů neví, jestli mohou považovat svůj způsob naplnění povinnosti za dostatečný.

[24] Viz ČERMÁK, Miroslav. Regulatorní požadavky představují jen další riziko, a tak je s nimi třeba i zacházet. *CleverAndSmart* [online]. 20. říjen 2018 [vid. 8. listopad 2018]; POLČÁK; HARAŠTA; STUPKA, op. cit., s. 77.

[25] Srov. HURYCHOVÁ; SÝKORA, op. cit., s. 7–13.

Tyto informace mají možnost získat až z činnosti regulátora, kontrolora nebo soudu v jejich případě. Takto nejistě nastavené pravidlo jim nedovoluje funkčně plánovat, nemohou předvídat kroky správních orgánů ani soudů. Těm naopak tato nejistota neúnosně zvětšuje vlastní míru diskrece.[26] Toto představuje značné podnikatelské riziko a je problémem zvláště pro střední a velké podniky i pro veřejnoprávní společnosti. Jsou totiž nuceny fungovat v nejistotě a své podnikatelské chování zakládat na a priori neznámé výši nákladů. Velikost sekundární povinnosti se dá v komplexních situacích jen stěží odhadnout do všech možných důsledků.[27]

Paradoxně největším *„strašákem“* pro společnosti nejsou veřejnoprávní sankce, ale zmíněné soukromoprávní nároky na náhradu škody a omezení pojistného plnění (což jim v případě porušení primární povinnosti hrozí). S veřejnoprávní sankcí se dá dopředu kalkulovat, neboť je alespoň rámcově předepsaná v právních předpisech. Kvůli této skutečnosti může být v určitých situacích pro společnost i výhodnější porušit primární povinnost, pokud bude zisk vyšší než sankce. Ovšem s rozsahem poškozených zájmů a způsobené škody se už ve všech případech dobře kalkulovat nedá. Škoda může dosáhnout až několikanásobně větší výše než veřejnoprávní sankce.[28] Zvláště pak je tento dosah citelný, pokud by škodlivé jednání společnosti vedlo k odepření pojistného plnění.[29]

Když je pro určitý regulatorní požadavek zavedena oficiální compliance procedura (a priori aprobování určitého postupu), tak se tento tradiční odpovědnostní model v případě compliance povinností nemusí uplatnit. Místo něj se nabízí možnost, aby splnění primární povinnosti posoudil oficiální certifikační subjekt ex ante, tedy předtím, než k nějakému incidentu vůbec dojde. Pokud je povinný subjekt shledán v souladu s regulatorním požadavkem, předpokládá se, že učinil všechna rozumná

[26] Viz D'AMATO, Anthony. Legal Uncertainty. *California Law Review* [online]. 1983, roč. 71, č. 1, s. 1–4 [vid. 25. únor 2019].

[27] Viz POLČÁK; HARAŠTA; STUPKA, op. cit., s. 76–77.

[28] Příkladem může být situace, kdy provozovatel celosvětově využívané služby bude odpovědným za škodu na majetku uživatelů způsobenou právě provozem této služby – tedy kdyby např. návštěva internetové stránky www.google.com způsobovala zničení pevného disku počítače.

[29] Viz tamtéž, s. 34 až 37 a 76.

opatření, aby předešel porušení primární compliance povinnosti. Může tak být zaštítěn před právní odpovědností za naplnění stavu compliance.[30]

V takovém režimu pak odpadá podstatná část z výše zmíněných nebezpečí, která hrozí povinným subjektům. Je tím pádem zřejmé, že po takových procedurách bude velká poptávka, zvláště pak ze strany veřejnoprávních společností a velkých podniků. Střední a malé podniky sice mohou žít a fungovat při využívání compliance procedur ve větší jistotě, ale v jejich případě je rizikovost spojená s uplatněním odpovědnosti podstatně nižší, než je tomu u podniků velkých, a kvůli tomu se může stát, že náklady na zajištění stavu shody mohou být pro malé a střední společnosti i podstatně vyšší než ty, vzniklé z povinnosti nahradit škodu.

Oficiální compliance procedury mají oproti odpovědnosti i několik faktických nevýhod. Zvlášť v bezpečnostních odvětvích dávají vzniknout stavu, kdy si povinné subjekty (i spotřebitelé) přijdou „*falešně v bezpečí*“[31] a značně to snižuje jejich touhu starat se o bezpečí nad rámec stavu compliance. Snižuje to pak míru investic věnovaných vývoji nových ochranných opatření. Ty se tak mohou postupně stát nedostatečnými a neaktuálními. Způsob, jakým by se dal dosah tohoto negativního důsledku compliance částečně minimalizovat, je dostatečná aktualizace regulatorních požadavků tak, aby úroveň ochrany a zabezpečení byla stále objektivně dostačující.[32] Nevyžadovala by pak inovaci od povinných subjektů. Takové řešení by se ale mohlo ukázat jako neunesitelné pro regulátora.[33]

Se zavedením compliance procedur souvisí i opačný problém, který se též týká neefektivity, tentokrát však způsobené nadužíváním povinnosti inovovat a zavádět bezpečnostní opatření. Vzhledem k tomu, že compliance

[30] Při splnění compliance povinností se ovšem subjekt nemusí zbavit odpovědnosti za incident.

[31] Tedy kdy se mylně domnívají, že implementace compliance procedury je uchrání před jakoukoliv hrozbou.

[32] Regulátor by např. jedenkrát za měsíc vydával aktualizované předpisy, se kterými by se posuzovala compliance. Tyto předpisy by počítaly s vývojem nových technologií, zranitelností a předepisovaly by modifikované bezpečnější chování. Tento přístup však dle mého názoru nemůže prakticky fungovat, a to zejména kvůli značné rigiditě a kauzálnosti.

[33] Viz POLČÁK; HARAŠTA; STUPKA, op. cit., s. 36–37.

procedura nemůže dopadnout na všechny případy stejně, neodvratně dojde k tomu, že prevence bude muset být prováděna i v situacích, kdy jí nebude reálně potřeba.[34]

Je zároveň možné, že naplnění compliance procedury by v případě její zjevné nedostatečnosti a zastaralosti již nemuselo vést k uplatnění domněnky *„naplnění všech rozumných opatření proti vzniku újmy“* a neochránilo by tak povinný subjekt před vznikem sekundární povinnosti úplně. V takové situaci by část škody možná mohla být požadována i po regulátorovi, např. státu, v případě, že by svým jednáním, případně zjevným opomenutím způsobil ohrožení či poškození cizích zájmů. Ovšem posuzování dostatečnosti compliance procedur je nebezpečná myšlenka vedoucí opět k velké právní nejistotě.

Obecně vzato budou mít compliance procedury tendence zvyšovat byrokratickou zátěž pro povinné subjekty, neboť oproti standardnímu režimu posuzování splnění primární odpovědnosti ex post (tedy posuzují se jenom ty, u kterých došlo k nějakému incidentu) budou posuzována úplně všechna konkrétní řešení povinných subjektů, na které pravidlo dopadne, ex ante. Takové zvýšení byrokratické zátěže v sobě skýtá i nebezpečí vysokého korupčního potenciálu a zvýšení korupčního tlaku na subjekty shodu posuzující.[35]

2.3 STANDARD

Vzhledem k tomu, že bezpečnostní požadavky byly málokdy nadefinovány přesně, vzniklo za dlouholeté absence oficiálních compliance procedur velké množství tzv. standardů, které obsahovaly specifickou úpravu toho,

[34] Příklad: Povinný subjekt A se pohybuje ve vysoce rizikovém prostředí, denně čelí několika incidentům a útoky vedené proti němu jsou vedeny za použití nejmodernějších technologií. Potřeba inovovat a zavádět nejmodernější bezpečnostní opatření tak, jak by si žádala hypotetická compliance povinnost, je tedy v souladu s jeho vlastním zájmem. Povinný subjekt B se pobyhuje v málo rizikovém prostředí a s útoky se musí vypořádávat pouze ojediněle. Pokud by měl tedy povinnost inovovat a investovat do bezpečnostních opatření na stejné úrovni jako povinný subjekt A, dosažení compliance pro něj bude představovat až zbytečnou zátěž.

[35] Viz POLČÁK; HARAŠTA; STUPKA, op. cit., s. 77–78.

jak dosáhnout shody. Tyto standardy byly vytvářeny různými tělesy, ať už národními, mezinárodními, obecnými nebo speciálními odvětvovými.[36]

Mezinárodní organizace pro standardizaci (dále jen jako „ISO"), která zaštiťuje standardizační instituty celkem ze 162 zemí a je tak jednou z nejvýznamnějších institucí v oboru (podrobněji bude představena ve čtvrté kapitole), vyložila pojem standard následovně: „*Zdokumentované dohody obsahující technické specifikace či jiná konkrétní kritéria, kterých má být soustavně užíváno jako pravidel, vodítek nebo definic charakteristik, a to k zajištění toho, aby materiály, produkty, procesy a služby byly vhodné pro daný účel.*"[37]

Standardy nebývají založeny na využití specifických technologií, neboť by tak byly značně neohebné z pohledu schopnosti reakce na technologický vývoj, častěji se tak definuje styl a smysl implementačních postupů. S množstvím organizací a jiných subjektů pracujících na vytváření standardů (a to i v oblasti kybernetické bezpečnosti) však vznikl problém nesourodého názvosloví. Každá organizace si do standardu nadefinovala určité pojmy, a bohužel ne vždy v souladu s ostatními. Odborné debaty jsou pak zatížené více slovíčkařením než přínosnou rozpravou.[38]

Jakmile povinný subjekt naplní kritéria, která standard stanoví, může prohlásit compliance s tímto standardem. Ovšem vzhledem k tomu, že takové prohlášení učiní sám, bez jakéhokoliv dohledu či kontroly, neponese takové prohlášení samo o sobě u informovaných účastníků trhu velkou váhu.[39]

ISO samotné varuje, že dosažení shody s mezinárodním standardem nemůže sloužit k zaštítění povinného subjektu před právní odpovědností.

---

[36] Pro příklad, jak se vytvářejí standardy, viz https://www.iso.org/developing-standards.html.

[37] Autorův překlad z anglického originálu: „*Documented agreements containing technical specification or other precise criteria to be used consistently as rules, guidelines, or definitions of characteristics, to ensure that materials, products, processes and services are fit for their purpose*". Více viz MEHAN, Julie E. *CyberWar, CyberTerror, CyberCrime.* [online]. 2nd ed. Ely, Cambridge, UK: IT Governance Publishing, 2014, s. 162 [vid. 19. srpen 2018].

[38] Viz MEHAN, op. cit., s.162.

[39] Viz ALKALBANI, Ahmed et al. Information Security Compliance in Organizations: An Institutional Perspective. *Data and Information Management* [online]. 2017, roč. 1, č. 2, s. 106 [vid. 23. červenec 2018].

Takovou schopnost získá standard až při oficiálním uznání státem a pouze ve vztahu ke compliance povinnostem (např. Japonsko ve vztahu ke standardu ISO 27001).[40] Některé standardy či certifikační řešení umožňují postup, který stojí mezi prohlášením compliance a oficiální certifikační procedurou → tzv. sebe-certifikaci (angl. self-certification) použitelnou většinou v nízko-rizikovém prostředí. V tomto případě si regulovaný subjekt samotný vyhodnotí, zdali určená kritéria splňuje. Může pak vydat prohlášení o souladu, kterým informuje potenciální zákazníky, že dodržování regulatorního požadavku bylo v souladu s určitou metodikou zkontrolováno. Povinný subjekt ale většinou přebírá plnou odpovědnost za řádné provedení kontroly, nebo rovnou za celý proces.[41] Vlastní posouzení je tak sice rychlejší a podstatně levnější variantou k certifikaci, ale zároveň tak podnikatel přichází o mnoho výhod spojených s certifikovaným stavem compliance.[42]

Snaha o dosažení shody se standardy je obecně založena na dobrovolné bázi. Povinný subjekt se může svobodně rozhodnout, jestli standard využije a získá tak určitou výhodu, či nikoliv a dosáhne souladu s pravidly po své vlastní ose. To samozřejmě značně snižuje harmonizační (a v bezpečnostních odvětvích i zabezpečovací) účinky takového řešení, ale zase nedochází k ohýbání trhu, které by při vysokých nákladech na dosažení shody mohlo menší společnosti ze soutěže úplně vyloučit. Snahy o vytvoření závazných standardů narážejí opakovaně jak na nedostatek mezinárodní vůle (státy mají stále v některých odvětvích, zvláště týkajících se národní bezpečnosti, tendence preferovat protekcionismus), tak i na mnoho praktických komplikací, jako přílišná obecnost formulací (na těch je sice možné dosáhnout konsensu, ale zase takový standard nic neřeší) nebo absence vymahatelnosti a kontroly. Vedle toho některé státy vypracovaly

[40] Viz SMEDINGHOFF, Thomas J. *Information Security Law* [online]. Ely, Cambridge, UK: IT Governance Publishing, 2008, s. 129 [vid. 11. říjen 2018].

[41] Sebe-certifikace tak v tomto bodě nepředstavuje pouze limitaci odpovědnosti, ale zároveň i prohlášení, přijímající odpovědnost za určité typizované škody. Povinný subjekt totiž zaručuje, že určitá skutečnost nenastane.

[42] Viz AXELROD, C. Warren. The creation and certification of software cybersecurity standards. In: *2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT)* [online]. Farmingdale, NY, USA: IEEE, 2016, s. 1–2 [vid. 22. červenec 2018].

národní řešení, která jsou sice konkrétní, ale naprosto nevhodná k širší, či dokonce celosvětové aplikaci, neboť pochopitelně vůbec nereflektují specifika úpravy v dalších státech, a úprava je tak kompletně rozdrobená.[43] Na tyto problémy narazila i Common Criteria, která představují nejrozsáhleji akceptovaný mezinárodně uznávaný standard pro kyberbezpečnostní technologie. V jejich případě se ani po mnoha letech vyjednávání a úprav nepodařilo upravit tento model natolik, aby byl vhodný pro certifikaci služeb (např. služby typu Software as a Service, primárně z důvodu, že testovat jednotlivé části systému nepostačuje k tomu, aby bylo možné prohlásit bezpečnost celku).[44] O tom svědčí i fakt, že přestože bylo v roce 2013 certifikováno podle Common Criteria více jak 1500 produktů, nebyla certifikována ani jedna služba.[45] Do dne 12. 10. 2019 prošlo certifikačním procesem (včetně archivovaných) 4059 produktů, a služba stále žádná.[46]

Vzhledem k tomu, že standardizace vzniká nejčastěji díky spolupráci v rámci určitého odvětví, dochází tím mezi podniky k šíření tzv. best practice (společnosti se dělí o postupy, které se jim nejvíce osvědčily), což pozitivně ovlivňuje trh, vývoj i spotřebitele.[47] Se standardy často souvisí ještě různé pomocné dokumenty (angl. „*guidelines*“, tedy vodítka, návody, manuály, které demonstrují, jak mohou být standardy splněny). Ty jsou obvykle vydávány orgánem, který spravuje daný standard, za účelem výkladu problematických či neurčitých pojmů v praxi a fungují jako určitá forma soft law.[48]

---

[43] Viz AXELROD, op. cit., s. 1–3.

[44] Viz Joint EC/ENISA SOG-IS and ICT certification workshop – Minutes of the workshop [online]. 6. říjen 2014 [vid. 24. srpen 2018].

[45] Viz KALUVURI, Samuel Paul; BEZZI, Michele; ROUDIER, Yves. Bringing Common Criteria Certification to Web Services. In: *2013 IEEE Ninth World Congress on Services (SERVICES)* [online]. Santa Clara, CA, USA: IEEE, 2013, s. 1 [vid. 22. červenec 2018].

[46] Jedná se o součet 1401 certifikovaných produktů a 2658 archivovaných. Více viz Certified Products List - Statistics. *New CC Portal* [online]. [vid. 12. říjen 2019]. Získáno z: https://www.commoncriteriaportal.org/products/stats/.

[47] Viz HURYCHOVÁ; SÝKORA, op. cit., s. 8–14.

[48] Srovnej s HARAŠTA, Jakub. *Princip technologické neutrality v kybernetické bezpečnosti* [online]. Brno, 2017, s. 36 [vid. 26. únor 2019]. Disertační práce. Masarykova univerzita, Právnická fakulta.

2.4 CERTIFIKACE

Shodu s určitým regulatorním požadavkem, případně se standardem, pokud ten k naplnění takového požadavku směřuje (v odborné literatuře se vyskytuje i pojem „*conformance*“, který je svým významem compliance podobný, ač není úplně totožný[49]), může prohlásit subjekt sám o sobě. Vyšší úroveň důvěry však zakládá proces označovaný jako „*certifikace*“. Ten značí, že produkt, služba, proces (či obecně cokoliv, co by mohlo být předmětem regulačních aktivit a certifikace) výrobce byl otestován subjektem akreditovaným k udílení certifikací. V obecném certifikačním režimu je nezbytné, aby mezi hodnoceným a akreditovaným subjektem neexistoval žádný vztah (jako např. mateřská – dceřiná společnost), aby bylo posuzování skutečně nestranné a objektivní.[50] Jedná se o formalizované posouzení naplnění určitého setu požadavků (označovaných obvykle jako certifikační schéma) hodnotitelem, který se označuje jako certifikační autorita. Na konci certifikačního procesu bude povinnému subjektu vydán oficiální certifikát (do nějž by nemělo být možné zasáhnout, ani ho zfalšovat), který potvrzuje naplnění požadavků do určité úrovně. Certifikační autorita se tak zaručuje za naplnění požadavků standardu nebo práva a propůjčuje důvěru, kterou mají zákazníci v její jméno, prostřednictvím certifikátu produktu povinného subjektu.[51]

K tomu, aby mohlo k hodnocení vůbec dojít, je nezbytné, aby byla certifikační autorita spojena s dostatečně vyspělými testovacími laboratořemi. V nich je produkt (služba atd.) otestován, zdali splňuje veškeré compliance požadavky, a to podstoupením rozličné materie testů. Vybavení takových laboratoří představuje enormní finanční zátěž, a proto před vznikem podobné laboratoře investoři zevrubně mapují trh

[49] Srovnej s SCORM Compliant, SCORM Conformant, SCORM Certified. *SCORM.com* [online]. [vid. 27. říjen 2018]. Získáno z: https://scorm.com/scorm-explained/scorm-resources/conformance-vs-compliance/.

[50] Vyskytují se i compliance modely, ve kterých není naplnění této podmínky zapotřebí. Příkladem může být metoda vlastního posouzení, kterou upravuje Akt (viz kapitola 7.4.3), kdy se subjekt certifikuje sám.

[51] Viz What's the Difference Series: Compliance vs. Certification. *Mireaux Management Solutions* [online]. 14. leden 2013 [vid. 27. říjen 2018]; AXELROD, op. cit., s. 1–3.

a vyhodnocují, jaká bude po certifikačních službách poptávka (návratnost investice). V případě kybernetické bezpečnosti mnohé z menších evropských států zatím nepředstavují dostatečně zajímavý trh, a tak na jejich území certifikační laboratoře a autority zatím vůbec nevznikly (tomuto trendu napomáhá i mnohdy chybějící vnitrostátní právní úprava kyberbezpečnostní certifikace). Z právě uvedeného je patrné, že neexistuje a ani prakticky nemůže existovat laboratoř, která by byla schopna testovat univerzálně všechno. Z ekonomických důvodů dochází vždy k určité profilaci.[52]

Úprava možnosti vytvářet nová certifikační schémata může být buď rigidní (např. ISO 27001) nebo uvolněná (např. Common Criteria, kde si povinný subjekt může schéma nadefinovat i sám). Se schopností adaptace certifikačního schématu však rostou i náklady na výbavu laboratoří jak z pohledu technologického, tak personálního. Proto je výhodou, když i nově vytvářená schémata jsou založena na univerzálně přijímaných základech, díky čemu je snadnější najít laboratoř schopnou provedení testů. Certifikační proces může být zároveň i různě přísný podle toho, jak důkladnému testování bude produkt podroben před udělením certifikátu.

U testování obecně nastává problém prostředí, ve kterém k testování dochází. Pokud totiž dojde k aplikaci testovaného objektu v jiném prostředí, než v jakém byl testován, bude certifikát de facto (mnohdy i de iure) k ničemu, neboť v takovém prostředí se můžou vyskytovat úplně jiné hrozby. Zároveň je u certifikace velký problém s životním cyklem produktu/služby atd. Mezi teoretiky nepanuje shoda, jestli úpravy a aktualizace činí certifikát neplatným v celém jeho rozsahu a je tak nutné provést plnou recertifikaci, jestli se mají testovat jenom samotné úpravy, či jestli je správná jakási verze kompromisu mezi zmíněnými.[53]

U certifikace je důležité rozlišovat, zdali se jedná o certifikaci komerční, o certifikaci státem uznávanou nebo přímo o certifikaci státní. S povahou certifikace může právotvůrce spojit různé právní následky. Státní certifikace je prováděna státním orgánem a stát tak nad ní má kompletní

[52] Viz AXELROD, op. cit., s. 5.

[53] Viz AXELROD, op. cit., s. 5.

dohled a moc, tudíž bude získání takového certifikátu podmínkou pro splnění nějakého ze zákonných požadavků. Státem uznaná certifikace je vykonávaná sice samostatným subjektem, ale stát s takovouto procedurou pojí určité pozitivní následky. Poněkud na pomezí zmíněných modelů stojí certifikace prováděná sice samostatným subjektem, ovšem akreditovaným k takové činnosti akreditačním orgánem. Čistě komerční systém je prováděn toliko na podnikatelské bázi soukromým subjektem, kdy stát certifikaci nepřiznává žádné účinky. Posledně zmíněný model je pro podnikatele nevýhodný (i přes pozitiva, která spolupráce a šíření nejlepších praktik přináší), a proto jsou tendence zvrátit čistě komerční certifikace alespoň do modelu certifikace uznávané státem.[54]

Pokud povinný subjekt získá státem uznávaný certifikát, může žít a priori v jistotě, že dosáhl compliance se všemi jejími pozitivními efekty (nebo by se compliance alespoň předpokládala a bylo by nutné ji vyvrátit). S náklady na získání certifikátu se dá dopředu kalkulovat a taková situace je tak pro povinné subjekty podstatně jednodušší a výhodnější. Mimo jiné je tím odstraněna podnikatelská nejistota spojená s neurčitou úrovní dostatečnosti příslušné implementace compliance procedur a s výší nákladů.[55]

2.5 DRUHY REGULATORNÍCH PRAVIDEL

Složitost procesu k dosažení shody je základní otázkou, která určuje, zda je pro určitou regulaci potřebný specificky upravený compliance proces. Složitost je ovlivňována jak specifickou povahou regulace technologií, tak i samotným způsobem stanovení regulačního požadavku. V případě naprosto konkrétní úpravy požadavku bude potřeba compliance procedur minimální, s rostoucí obecností pak poroste i potřeba zjistit, jak shody uspokojivě dosáhnout. V této podkapitole tak rozeberu tři druhy regulatorních pravidel, kterých může být využito v certifikačních schématech, o nichž bude řeč v dalších kapitolách. Smyslem této

[54] Viz POLČÁK; HARAŠTA; STUPKA, op. cit., s. 80.

[55] Viz tamtéž, s. 30.

podkapitoly je objasnit, „*jak*“ mohou být formulovány požadavky, proti kterým má být shoda certifikována.

Normotvůrce stojí při rozhodování o metodě formulování regulatorního požadavku před problematikou poměřování čtyř důležitých principů – konzistence a jistoty proti flexibilitě a inovaci.[56] Nadměrná a nepragmatická obliba konzistence a rigidních úprav má dnes již mnoho kritiků, přestože se v minulosti jednalo o přístup víceméně jediný. Tito kritici poukazují na fakt, že mnohé regulace jsou tak úzce nadefinované a tak silně preskriptivní, že jejich účinky jsou po čase nedostatečně a až nelogicky zbytečně zatěžující společnosti, které musí na dosažení shody vynaložit příliš mnoho prostředků s minimální efektivitou výstupu (toto se děje zvláště v některých odvětvích, např. ochrana životního prostředí).[57]

Podle toho, na jakou fázi aktivit společnosti regulace dopadá,[58] rozlišujeme tři režimy pravidel – technologická pravidla (která můžou být též řazena jako podkategorie pravidel deskriptivních či behaviorálních,[59] z angl. Technology-based, resp. Descriptive rules) dopadající na fázi realizační, performativní pravidla (z angl. Performance-based rules) dopadající na fázi výslednou a pravidla řízení (z angl. Management-based rules) dopadající na fázi plánování.[60]

---

[56] Viz MAY, Peter J. Performance-Based Regulation and Regulatory Regimes: The Saga of Leaky Buildings. *Law & Policy* [online]. 2003, roč. 25, č. 4, s. 382–383 [vid. 22. září 2018].

[57] Viz HARAŠTA, Jakub. *Princip technologické neutrality v kybernetické bezpečnosti* [online]. Brno, 2017, s. 52–54 [vid. 26. únor 2019]. Disertační práce. Masarykova univerzita, Právnická fakulta; MAY, op. cit., s. 382-383.

[58] Rozlišujeme celkem tři fáze každé regulované aktivity a tři způsoby, jak na ně mohou pravidla dopadnout: plánovací fáze (pravidla zde regulují, jakým způsobem se má plánovat a jak se má chovat společnost od počátku projektu, aby směřovala k určitému cíli), realizační fázi (regulují konkrétně, jakým způsobem a za použití jakých prostředků má být činnost vykonávána) a na fázi výslednou či fázi výsledků, z ang. Output stage (pravidla regulující tuto fázi stanoví, k čemu má chování společnosti směřovat).

[59] Viz KNEEPKENS, Jules. Performance Based Regulation. In: *EASA Safety Conference* [online]. B.m. 10. říjen 2012 [vid. 20. září 2018].

[60] Viz COGLIANESE, Cary; LAZER, David. Management-Based Regulation: Prescribing Private Management to Achieve Public Goals. *Law & Society Review* [online]. 2003, roč. 37, č. 4, s. 694 [vid. 12. září 2018].

2.5.1 DESKRIPTIVNÍ PRAVIDLA

Pravidla, která jsou vystavěna na deskriptivním principu, jsou pravidla nejstarší. Stanovují konkrétně definované povinnosti subjektům. Jedná se např. stanovení výše daní nebo nejvyšší dovolené rychlosti na silnici. Tato pravidla nezmiňují přímo, k jakému cíli se má dospět (přestože je to z nich často pochopitelné), ale předepisují konkrétní chování, které má tento cíl naplnit. Normotvůrce tak přebírá povinnost vyhodnotit, jaké chování je v dané situaci žádoucí. V minulosti byl tento model používán nejvíce, nyní se ovšem ukazuje, že v mnohých oblastech úpravy (zvláště těch, ve kterých dochází ke střetu technologií a práva) má značné slabiny.[61]

Deskriptivní pravidla nejvíce trpí slabinou, která v různé míře postihuje všechny druhy regulatorních požadavků. Tato slabina se v angličtině označuje jako problém „*One size to fit them all*“.[62] Nabízí se sice řešení v podobě větší míry obecnosti, ale ani toto není žádoucí, neboť obecnost nevyhnutelně snižuje právní jistotu a způsobuje nutnost extenzivního výkladu normy, případně i vytvoření compliance procedur.[63]

Zůstává tedy faktem, že není možné zohlednit okolnosti každého určitého případu při vytváření normy, a tudíž může v mnoha případech dojít k tomu, že výsledný stav je buď nesmyslně přeregulován či podregulován. Tím myslím, že v takové situaci je po povinném subjektu pravidlem vyžadováno buď daleko víc, nebo podstatně méně, než je nezbytně nutné. Tím narůstají investice společností na dosažení shody s regulací či se naopak zvyšuje míra rizika, že se projeví negativní následek, kterému chce regulace zabránit. Buď tedy dochází k nesmyslnému ohýbání trhu, nebo regulace nepostačuje ani ke splnění svého vlastního cíle, čímž se stává de facto zbytečnou.[64]

Dalším negativem deskriptivních pravidel je skutečnost, že mohou efektivně vyřadit touhu společností inovovat „*žádoucím*“ způsobem. Oproti

[61] Viz tamtéž, s. 701.

[62] Po regulaci se chce, aby dopadla na všechny unikátní případy, a to s optimálními účinky.

[63] V i z COGLIANESE, Cary. The Limits of Performance-Based Regulation. *University of Michigan Journal of Law Reform* [online]. 2016, roč. 50, č. 3, s. 527 [vid. 12. září 2018].

[64] Viz tamtéž.

tomu se u společností může rozvinout touha inovací směřujících k úniku z dosahu regulace. Pokud je pevně stanoveno, jaké technologie má provozovatel služby používat, nemá pak tento provozovatel důvod nacházet efektivnější řešení, kromě lepšího poměru cena/výkon. Chybějící inovativnost subjektů musí nahrazovat normotvůrce, což samozřejmě vede ke zvýšení nákladů normotvorného procesu. Je možné tento „*aktualizační proces*“ provést buď neustálou novelizací textu zákona, nebo využitím neurčitých pojmů, které následně definuje správní cestou regulátor k tomu určený.[65] V českém prostředí vystupuje jako takový regulátor např. Český telekomunikační úřad.[66]

2.5.2 PERFORMATIVNÍ PRAVIDLA

Performativní pravidla jsou relativně novým konceptem regulace (přestože pravděpodobně první pravidlo tohoto druhu se vyskytlo již v Chamurappiho zákoníku[67]) a bude jim zde věnována větší pozornost kvůli jejich vhodnosti k použití regulace technologií. Performativní pravidlo je takové, které vymezí určitý cíl, určitý chtěný stav a nechá na regulovaném subjektu, jakým způsobem tohoto stavu dosáhne.[68] Pro příklad – „*Řidič motorového vozidla je povinen jet pouze tak rychle, aby jeho jízda byla bezpečná*“. Pro regulovaný subjekt není předepsané, jakým konkrétním způsobem se má zachovat, důležité je, aby naplnil stav požadovaný normou. Pravidlo tak přizpůsobí své individuální potřebě a do značné míry tím limituje dosah již zmíněného problému „*One size to fit them all*“, neboť si každý regulovaný subjekt své chování reguluje sám ad hoc.[69]

---

[65] Viz HARAŠTA, Jakub. *Princip technologické neutrality v kybernetické bezpečnosti* [online]. Brno, 2017, s. 33 [vid. 26. únor 2019]. Disertační práce. Masarykova univerzita, Právnická fakulta.

[66] Jako regulátor, alespoň v určitém smyslu slova, může vystupovat i NÚKIB v oblasti kybernetické bezpečnosti. Povaha jeho aktivit je ovšem v tomto ohledu méně jednoznačná, a je tak spíše „*kvaziregulátorem*“.

[67] Viz MAY, op. cit., s. 390.

[68] Viz COGLIANESE, Cary; NASH, Jennifer; OLMSTEAD, Todd. Performance-Based Regulation: Prospects and Limitations in Health, Safety and Environmental Protection. *Administrative Law Review* [online]. 2003, roč. 55, č. 4, s. 14 [vid. 20. září 2018].

[69] Viz tamtéž, s. 14–15.

Performativní pravidla se tak stávají, spíše než pravidly o chování, pravidly o vytváření pravidel chování. Nabízejí flexibilitu a mohou rozproudit touhu po „*dobré*“ inovaci a nacházení nových řešení, jak efektivněji plnit povinnost.[70] V praxi pak jeden subjekt, který se bude řídit výše zmíněným performativně-konstruovaným rychlostním limitem, může bez problémů jet rychlostí 150 km/h, protože se jedná o zkušeného řidiče na bezproblémovém úseku, a druhý subjekt pojede rychlostí 30 km/h, neboť se jedná o začátečníka a na více si nevěří. Oba dva jsou v souladu s pravidly, přesto každý jiným způsobem.

Performativní pravidla nabízejí velkou svobodu normotvůrci. Je možné je nadefinovat úzce či široce (určuje míru diskrece, která je ponechána subjektu, pokud regulace naformuluje, jakého výkonu má dosáhnout motor, tak je možnost diskrece očividně nízká).[71]

Tato pravidla operují s velkou mírou obecnosti, případně až volnosti povinných subjektů.[72] Pozitiva těchto pravidel, plynoucí z využívání velké volnosti subjektů, jsou velká, mají však i své slabiny. Ty vychází z téměř absolutní absence empirického výzkumu, který by jakkoliv vyhodnotil jejich reálné účinky. Přestože nad povahou performativních pravidel byly vedeny rozsáhlé vědecké debaty, mnohé vědění o těchto pravidlech zůstává na čistě teoretické úrovni. Problémem pak je i otázka vymáhání – většina států tuto otázku ignoruje nebo se jí z důvodu nedostatku zkušeností či prostředků věnuje naprosto nedostatečně a pravidla pak nefungují (jak ukázal i debakl Volkswagenu ohledně dodržování emisních limitů[73]).[74]

Performativní pravidla mají na první pohled velkou ekonomickou výhodu pro stát, neboť pro jejich vývoj není nutné vynaložit tolik prostředků, ani není nutné tak hluboké pochopení problematiky jako pro

[70] Viz COGLIANESE, 2016, op. cit., s. 543.

[71] Viz COGLIANESE; NASH; OLMSTEAD, op. cit., s. 14–15.

[72] Ale zvláště menší a začínající subjekty často nemají prostředky, kapacity nebo zkušenosti na to, aby mohly svobodu poskytovanou performativními pravidly efektivně využívat. To vytváří potřebu alespoň rámcových návodů, jak shody dosáhnout.

[73] Tento skandál vypukl v roce 2015, kdy vyšlo najevo, že Volkswagen více jak 7 let ignoroval performativně nastavená pravidla na limitaci vypouštěných emisí.

[74] Viz COGLIANESE, 2016, op. cit., s. 529–531.

zkonstruování funkčního pravidla deskriptivního. Ve skutečnosti se však jedná o částečné přesunutí finanční zátěže do oblasti vynucování pravidel. Svoboda v dosahování shody pro stát představuje daleko náročnější vyhodnocování, jestli subjekty dodržují právo.[75,76]

Snížení ekonomické zátěže státu se zároveň pojí se zvýšením nákladů pro povinné subjekty. Regulátor využívající tohoto modelu spoléhá na fakt, že regulované subjekty samotné ví nejlépe, co a jak mají dělat. Tak tomu bude často v případě velkých konglomerátů, ale pro malé podniky tato situace platit nebude. Ty budou muset vynaložit velké prostředky, aby zjistily, který z postupů je pro dosažení shody nejlepší. Tyto náklady mohou být dokonce tak vysoké, že ve spojení s absencí dostatečné jistoty, že tento postup bude pro dosažení shody dostatečný (tedy v případě absence oficiálních compliance procedur), povede taková situace k vytvoření blokády na trhu proti malým podnikům. Pro velké podniky dojde ke značné finanční úlevě, protože si budou moci stanovit limity a pravidla efektivněji a náklady na výzkum a inovace u nich nebudou tak znatelně zvýšeny.

Performativní pravidla mohou plně fungovat pouze tehdy, pokud se zájmy regulátora a regulovaných subjektů alespoň rámcově shodují. Pokud jsou v přímém rozporu, jako je tomu např. u daní, není prakticky možné, aby byla výše daní upravena performativně. Je jasné, že příkaz ve stylu „*Platte daně v takové výši, aby to státu vystačilo*“ by regulované subjekty k placení moc nemotivoval.

2.5.3 PRAVIDLA ŘÍZENÍ

Management-based rules, tedy pravidla řízení, regulují fázi plánování, procesů a operací, a to tak, že předepíšou, jak by plánování a celkově chování řídících orgánů společnosti mělo vypadat, aby mělo potenciál naplnit cílový stav. Mohou tedy stanovit, že součástí plánování musí být

[75] Nadále se totiž nevyskytuje jednoduchý stav „*splňuje/nesplňuje konkrétní normu*“, ale je nutné vyhodnotit celý proces i s jeho dopady, tedy – „*Byl tímto cíl naplněn?*“. I pro stát samotný tak může být výhodné vytvořit oficiální compliance proceduru, která sice nemusí být závazná pro všechny, ale mnohé subjekty by jí mohly využít a navíc poskytne i rámcový návod pro postup při kontrolách.

[76] Viz MAY, op. cit., s. 388.

hodnocení rizik, procedury pro monitorování problémů či zavedení jiných typů procesu do chování subjektu.[77] Procesy implementované do plánovací fáze pak ovlivňují celý život projektu, často v něm i celou dobu vystupují. Tyto procesy se musí dobře dokumentovat a zanést i do plánů, které v počátečních fázích života projektu vznikají, aby bylo možné kontrolovat a posuzovat shodu.[78] I tato pravidla má však smysl využívat pouze v případě, že stát dokáže dohlížet na jejich naplňování a případně shodu vynucovat, stejně jako u pravidel performativních.[79]

Ani pravidla řídící, ani pravidla performativní se v praxi téměř nevyskytují v čisté podobě. Je často nutné, aby byla zkombinována s modelem deskriptivním.

2.5.4 CHARAKTER PRAVIDEL KYBERNETICKÉ BEZPEČNOSTI

V oblasti kybernetické bezpečnosti je většina pravidel vystavěna na principu povinnosti subjektu provést rozumná či přiměřená opatření k ochraně dat. Cíle těchto regulací bývají většinou vyjádřeny pozitivním stavem, kterého je zapotřebí dosáhnout, např. zajištění dostupnosti. Vhodné by tak mohlo být použít performativní pravidla. Ta by byla vhodná i z jiného důvodu. Zákonodárci často pravidla o kybernetické bezpečnosti formulují s užitím neurčitých pojmů pro lepší flexibilitu pravidla. Občas je to však způsobené i tím, že nemají k dispozici dostatečné informace či vědomosti o problematice kybernetické bezpečnosti, a pravidla jsou tak konstruována ve stylu povinné implementace „*dostatečných procedu*r“ či „r*ozumných pojistek*“ kvůli tomu, že zákonodárce správné řešení nezná a bylo by pro něj jednodušší toto břímě přesunout na povinný subjekt.[80] I to ukazuje na větší vhodnost performativních pravidel, v některých případech i pravidel řízení. Tím však nechci bagatelizovat výhody využití neurčitých pojmů, pouze podotýkám, že je zapotřebí skutečně odborného regulátora.[81]

---

[77] Viz COGLIANESE; LAZER, op. cit., s. 694.

[78] Viz COGLIANESE; LAZER, op. cit., s. 694.

[79] Viz tamtéž, s. 711.

[80] Viz SMEDINGHOFF, op. cit., s. 61–62.

[81] Příkladem performativního pravidla v českém zákoně o kybernetické bezpečnosti je bezpečnostní opatření (§ 4 odst. 1 zákona č. 181/2014 Sb.)

3. CERTIFIKACE V SYSTÉMU KYBERNETICKÉ BEZPEČNOSTI

Na začátku této kapitoly stručně popíšu fungování zabezpečování v kybernetické bezpečnosti, aby bylo možné si představit konkrétní bezpečnostní opatření, která jsou v průběhu certifikačního procesu testována, a nezůstalo jen u prázdných pojmů. Cílem a posláním kybernetické bezpečnosti je zabezpečení a ochrana prostředí pro realizaci práv člověka (pro potřeby tohoto článku si vystačíme i s ochranou informací a informační infrastruktury před hrozbami). Zájem na tom, aby v rámci informačních systémů byla zachována důvěrnost, integrita a dostupnost dat (tzv. CIA triáda, vycházející z anglického Confidentiality, Integrity a Availability; tato triáda je pravidelně využívána k definování toho, jaké vlastnosti mají mít „*zabezpečené informace*“[82]) je hnán snahou zabezpečit zájmy jak soukromých, tak veřejnoprávních subjektů. Výsledkem tohoto zájmu je pak určité regulované chování v kyberprostoru. Jako regulátor může vystupovat jak stát (výsledkem je právní předpis), tak i sdružení soukromých subjektů. Ti se mohou dohodnout na sdílení a plošném užívání osvědčené praxe, které pak mohou vynucovat i proti menším nebo začínajícím subjektům na trhu (tato pravidla tak budou mít podobu soft law). De facto tak vznikne standardizované bezpečné chování, které může být následně trhem vyžadované.[83]

Hrozby ohrožující bezpečnost a integritu informací se obecně dělí do tří kategorií podle oblastí, z nichž pocházejí – fyzické, technické a lidské. Fyzické v sobě zahrnují incidenty, jako jsou krádež nebo povodně. Technické hrozby jsou takové, které se provádějí za pomocí škodlivého počítačového kódu nebo jiného zautomatizovaného systému. A lidskými hrozbami jsou myšlena rizika mající svůj původ v operačním personálu (typicky zaměstnanec s lístečkem přilepeným na monitoru, a na lístečku má napsané heslo) a ti, kteří se snaží informační systém či část infrastruktury

[82] Viz BASKERVILLE, Richard; STRAUB, Detmar W; GOODMAN, Seymour E. *Information Security* [online]. Armonk, NY, USA: Routledge, 2008, s. 57 [vid. 11. listopad 2018]. Advances in Management Information Systems.

[83] Viz SMEDINGHOFF, op. cit., s. 15–17 a 61-63.

napadnout, zničit nebo zneužít.[84] Kybernetická bezpečnost implementuje bezpečnostní řešení, která mají za cíl minimalizovat dosah jednotlivých hrozeb, a zároveň lidově řečeno „*zacpávat bezpečnostní díry*“. Tento systém by měl ideálně fungovat tak, že se útočníkovi nepovede využít dvakrát stejné zranitelnosti (bezpečnostní díry).

Bezpečnosti je v této oblasti dosahováno nejen za pomoci různých technických prvků v podobě hardwarových a softwarových řešení (např. firewall), ale stejně tak i za pomoci různých interních předpisů, organizačních struktur či bezpečnostních politik. Jedním z nejdůležitějších prvků kontrování hrozeb jsou analýzy a analytické dokumenty (např. analýza rizik), které slouží k odhalení slabin a incidentů. Proškolení vlastního personálu ohledně pravidel bezpečnosti a zmíněných bezpečnostních procedur (v případě, že jsou reálně a dobře nastaveny) může také značně přispět ke zvýšení bezpečnosti prostředí (v praxi jsou pokyny pro zaměstnance často vytvářeny jako pouhá formalita, takže jim nikdo ve výsledku nerozumí).[85]

Bezpečnostní řešení se dělí, kromě druhu kontrované hrozby, i z pohledu času, a to na preventivní a reaktivní. Preventivní mají hrozbám předcházet (působit ex ante na základě již vyřešeného kybernetického bezpečnostního incidentu; český zákon o kybernetické bezpečnosti s nimi počítá v případě ochranných opatření[86]) a reaktivní opatření (tak je zná i český zákon[87]) se aktivují až při probíhajícím incidentu, kdy jejich účelem je minimalizace škod a zastavení útoku/incidentu.[88] Příkladem preventivního opatření kontrujícího hrozbu fyzické povahy je zámek na vstupních dveřích. Preventivní ochranou před technologickou hrozbou můžou být firewall, hesla, PIN kódy nebo šifrování, a před lidskou hrozbou zase důkladné proškolení zaměstnanců o bezpečnosti a kyber-hygieně.[89]

---

[84] Viz SMEDINGHOFF, op. cit., s. 26–28.

[85] Viz POLČÁK; HARAŠTA; STUPKA, op. cit., s. 37; SMEDINGHOFF, op. cit., s. 29–30.

[86] Viz § 14 zákona o kybernetické bezpečnosti.

[87] Viz § 13 zákona o kybernetické bezpečnosti.

[88] Viz KYSELOVSKÁ, Tereza et al. *Cofola 2015: Sborník z konference* [online]. Edice Scientia. Brno: Masarykova univerzita, 2015, s. 20 [vid. 22. listopad 2018].

[89] Viz SMEDINGHOFF, op. cit., s. 30–34.

3.1 SPECIFIKA CERTIFIKACE V KYBERNETICKÉ BEZPEČNOSTI

Oblast kybernetické bezpečnosti a celkově IT prostředí se vyznačuje vysokou mírou inovativnosti a rychlostí technologického pokroku a nutí tak zabezpečovací opatření do převážně reaktivní polohy (výše zmíněné „*zacpávání děr*“). To je patrné zvlášť v momentě, kdy je v procesu certifikace testováno, jestli objekt neobsahuje známé zranitelnosti.

V oblasti kybernetické bezpečnosti je hned několik objektů, u kterých je možné certifikovat soulad – jedná se o technologie (produkty a služby), bezpečnostní procesy (např. systém řízení bezpečnosti informací), zabezpečení organizační struktury společností, případně i osoby ad. Pro účely tohoto článku je důležitá zejména certifikace technologií, ale nový Akt o kybernetické bezpečnosti, který bude rozebrán v dalších kapitolách, obsahuje i úpravu certifikace procesů, tudíž by mohl zasáhnout i do certifikace systémů řízení bezpečnosti informací (také jako „ISMS“), a tak je nutné zde vysvětlit i tento pojem.

Certifikace ISMS je primárně prováděna podle mezinárodního standardu ISO/IEC 27001:2013. Mezinárodní organizace pro standardizaci označuje ISMS za „*systematický přístup ke správě citlivých informací společnosti za účelem zachování bezpečnosti těchto informací. Tento přístup zahrnuje užití procesu zvládání rizik na personální složku, procesy i IT systémy společnosti*“.[90] ISMS zná i český zákon o kybernetické bezpečnosti včetně (nové) vyhlášky o kybernetické bezpečnosti. Ta ISMS definuje v § 2 písm. j) jako „*část systému řízení povinné osoby založená na přístupu k rizikům informačního a komunikačního systému, která stanoví způsob ustavení, zavádění, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací a dat*“.[91] Jedná se o komplexní řídící proces sloužící k zabezpečení informací, který je založen na hodnocení rizik hrozících subjektu, a tudíž je možné jeho „*přísnost*“ přizpůsobit prostředí společnosti. Vedení subjektu

[90] Autorův překlad z anglického originálu: „*systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.*“ Více viz ISO/IEC 27001 Information security management. *ISO* [online]. [vid. 25. prosinec 2018]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/home/standards/popular-standards/isoiec-27001-information-securit.html.

musí na základě zprávy o hodnocení rizik rozhodnout, která rizika jsou ještě tolerovatelná a která již nikoliv. Na základě tohoto rozhodnutí pak dochází k řízení rizik (tedy k odstranění či minimalizaci netolerovatelných hrozeb). Vzhledem k tomu, že ISMS je procesem, dochází k hodnocení rizik v pravidelných intervalech a nikoliv pouze jednou. Hodně zjednodušeně řečeno by se tedy dalo říci, že ISMS upravuje chování, organizační opatření a procesy probíhající ve společnosti. A pokud ISMS odpovídá bezpečnostním požadavkům nadefinovaným v určitém standardu, je možné, aby příslušná certifikační autorita takový soulad certifikovala, pokud takový postup standard umožňuje.[92]

Certifikace kyberbezpečnostních technologií je oproti tomu zaměřená na stavební prvky informačních systémů. Nejčastěji se těmito prvky myslí IT produkty (Common Criteria tímto myslí software, hardware i firmware). Méně často se mezi technologie řadí i služby. To je způsobené především tím, že Common Criteria, která jsou momentálně hlavním mezinárodním certifikačním rámcem pro ICT/kyberbezpečnostní produkty, nejsou vhodná ani žádaná k certifikaci služeb (ani procesů).[93] Když celou problematiku ještě více zjednoduším, certifikace kyberbezpečnostních technologií se bude týkat bezpečnosti věcí, jako je např. router, nebo služeb, jako je např. provoz autentizace klientů, ale nebude dopadat na úpravu vnitřních procesů povinného subjektu, nebude posuzovat, jak se subjekt, který tento

[91] Viz § 2 vyhlášky 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). In: *CODEXIS ACADEMIA* [právní informační systém]. ATLAS consulting [vid. 6. listopadu 2018]

[92] Viz BÂRSAN, Mihai. Aspects regarding the implementation of information security standards in organizations. *Revista Română de Biblioteconomie și Știința Informării = Romanian Journal of Library and Information Science* [online]. 2017, roč. 13, č. 1, s. 22–24 [vid. 29. říjen 2018].

[93] Certifikace je velice nákladný proces a zároveň i proces značně zdlouhavý, kdy jedno posouzení může zabrat až 12 měsíců. Zakonzervovat podobu poskytované služby na 12 měsíců je v prostředí, kde se služba musí neustále vyvíjet, aby zůstala schopná reagovat na nové trendy a hrozby, nemyslitelné. Takový styl certifikace by dokázal konstatovat pouze to, že před rokem byla tato služba bezpečná. Pro budoucí možnost certifikace služeb je příslibem nový model certifikace kyberbezpečnostních technologií v EU, ale o tom bude podrobněji pojednáno v dalších kapitolách. Dále viz KALUVURI; BEZZI; ROUDIER, op. cit., s. 1.

router vlastní, stará o bezpečnost informací obecně. To je doména certifikace ISMS. Je tak patrné, že oba zmíněné certifikační systémy nemají mnoho společného, přestože mohou dobře pracovat vedle sebe, a porovnávat je je účelné jenom kvůli Aktu.

Po provedeném srovnání se vrátím k obecnému pojednání, co vlastně certifikace kyberbezpečnostních technologií představuje. Technologie, o jejíž certifikaci výrobce usiluje, musí podstoupit sérii různě náročných testů, které prověří, jakým kyberbezpečnostním hrozbám je schopna tato technologie čelit.[94] To, jak náročné testy budou, závisí na tom, na jakou bezpečnostní úroveň chce investor technologii certifikovat. Pokud zůstane při testování i jen jediný bezpečnostní požadavek dané úrovně nenaplněn, technologie certifikát nezíská. Problematickým se může stát testovací prostředí. Není představitelné, že by bylo možné otestovat určitou technologii v nějakém *„univerzálním“* všeobjímajícím prostředí, které by obsahovalo všechny typy hrozeb. Proto si investor nebo v některých případech i spotřebitel musí/může nadefinovat, v jakém prostředí (jaký typ uživatelů bude technologii užívat, jaké fyzické podmínky budou v okolním světě, jaké hrozby jsou pro technologii relevantní, k čemu bude technologie využívána atd.) má být technologie testována. Pro takové prostředí pak bude vydán certifikát.

Pokud uživatel překročí poučení výrobce o specifickém prostředí užívání a užije technologii v rozporu s certifikátem, nedojde případnou škodou z bezpečnostní vady technologie k porušení certifikační záruky za bezpečný výkon technologie, neboť ta panuje toliko nad určitým prostředím. Zároveň nemusí dojít ani k uplatnění odpovědnosti výrobce. Investor totiž oficiálně proklamoval a informoval uživatele o určité úrovni zabezpečení, kterou uživatel navzdory tomu překročil a následek tak je zodpovědností uživatele.

[94] Některé hodnotící systémy (zvláště u testů na vyšší bezpečnostní úrovně) posuzují i výrobce/vývojáře – např. kde vyrábějí, zabezpečení výrobního procesu, ad.

3.2 AKTUÁLNÍ ÚPRAVA CERTIFIKACE V KYBERNETICKÉ BEZPEČNOSTI

3.2.1 STAV V ČESKÉ REPUBLICE

V České republice ke dni 12. 10. 2019 neexistuje žádná obecná vnitrostátní právní úprava certifikace kyberbezpečnostních technologií. Nezmiňuje se o ní ani zákon o kybernetické bezpečnosti, ani žádná z vyhlášek o kybernetické bezpečnosti. Tato absence oficiální compliance procedury způsobuje povinným subjektům značnou právní nejistotu ohledně zvoleného řešení, které požaduje český zákon o kybernetické bezpečnosti, a řadu dalších negativních důsledků, které byly již rozebrány v druhé kapitole.[95] Jedná se o příklad jednoho z největších problémů, se kterými se certifikace potýká – v mnoha odvětvích vůbec neexistuje. Přesto však na českém trhu existuje poptávka po certifikační proceduře, primárně mezi veřejnoprávními korporacemi a velkými soukromoprávními subjekty, které se dostanou pod dosah zákona o kybernetické bezpečnosti.

Polčák tento zarážející stav vysvětluje takto:

„Zavedení státní certifikace by vyžadovalo důkladnou přípravu institucionální a personální a je třeba v tomto směru konstatovat, že na našem pracovním trhu zdaleka není přebytek pracovní síly disponující dostatečnou mírou kvalifikace v oboru kybernetické bezpečnosti a k tomu náležitě motivované za aktuálních platových podmínek ke vstupu do služeb státu. Příprava adekvátní procedury by tedy z hlediska organizačního i personálního vyžadovala takovou časovou a finanční dotaci, kterou si vzhledem k vývoji bezpečnostní situace nemůže v současné době Česká republika dovolit (kromě toho je třeba po bohatých našich zkušenostech připomenout, že nemá smysl uvádět v účinnost právní úpravu, na jejíž implementaci není státní exekutiva náležitě připravena).“[96]

Čistá varianta státní certifikační procedury tak podle něj není v momentálním rozložení trhu reálná. Jedinou variantou přímého zapojení státního aparátu je pak možnost státní akreditace nezávislého subjektu

[95] Viz POLČÁK; HARAŠTA; STUPKA, op. cit., s. 76.

[96] Viz tamtéž, s. 79-80.

(v podobě profesního či oborového sdružení, komerčního subjektu nebo i akademické instituce, případně kombinace všeho). Ten by k tomu, aby mohl sloužit jako certifikační autorita, musel samozřejmě vládnout požadovanou personální i technologickou kapacitou. Vzájemná spolupráce zájmových sdružení, působících v oblasti kybernetické bezpečnosti, je v tomto ohledu pozitivní kombinací transparentnosti, profesní specializace a společných podnikatelských zájmů.[97]

Je sice pravdou, že situace na českém trhu momentálně není k zavedení možnosti státem uznávané certifikace nejpříznivější,[98] ale Česká republika má již zkušenost s procedurou, která je obecné certifikaci kyberbezpečnostních technologií velice podobná, a to v oboru ochrany utajovaných informací. Jak Polčák dále uvádí, ani v této oblasti se kapacity pro provoz takového systému původně nevyskytovaly, ale byly postupně vytvořeny. Překvapením byla i příznivá situace ohledně korupčních tlaků, které zde nezaznamenaly výraznější úspěch (a to i přesto, že vzhledem k povaze této agendy není možné dosáhnout tak vysoké míry transparentnosti, jak by tomu bylo v případě kyberbezpečnostních technologií).[99]

Certifikace ISMS se v českém právním prostředí nachází v daleko lepším postavení, neboť s ní v podobě komerční certifikace podle standardu ISO/IEC 27001 právo přímo počítá a je státem uznána. Stará vyhláška o kybernetické bezpečnosti ji v § 29 stanovila jako podmínku presumpce naplnění zákonných požadavků (viz níže). Nová vyhláška již celá vychází ze stejných principů a pravidel jako standardy z rodiny ISO 27K, a přestože výslovná úprava vztahu certifikátu a povinností podle vyhlášky z textu předpisu zmizela, v důvodové zprávě k vyhlášce se o tomto vztahu píše v části vztahující se k § 3 následující:

---

[97] Viz POLČÁK; HARAŠTA; STUPKA, op. cit., s. 79-80.

[98] Je ovšem nutné jedním dechem zdůraznit, že se situace od roku 2016 přece jenom zlepšila a dle konzultačního emailu s doc. JUDr. Radimem Polčákem, Ph.D. z října 2019 se nyní v České republice vyskytují kapacity, soustředěné zejména na univerzitách, které provádějí certifikaci pro zahraniční certifikační autority.

[99] Viz tamtéž.

„Zmíněná norma (ISO/IEC 27001 – pozn. autora) po jejích uživatelích vyžaduje mimo jiné respektování zákonných závazků, u zákonem regulovaných subjektů, tedy i povinností vyplývajících ze zákona o kybernetické bezpečnosti. Z toho důvodu není potřeba zvyšovat administrativní zátěž, kterou by především znamenalo dodržování jak požadavků normy, tak požadavků na bezpečnostní opatření, daných touto vyhláškou. Je tedy možné respektovat certifikaci ISMS dle ISO/IEC 27001 jako adekvátní k dodržování bezpečnostních opatření daných touto vyhláškou. Výkon kontroly v oblasti kybernetické bezpečnosti není tímto ustanovením nijak dotčen, přičemž kontrola bude provedena pouze v rozsahu informačního a komunikačního systému.“[100]

Zmíněný standard je produktem práce Mezinárodní společnosti pro standardizaci, které je Česká republika plnoprávným členem. Na poli této organizace je reprezentována Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví (detailní pojednání o členství v ISO a mezinárodní organizaci samotné je v páté kapitole).[101] Dále je pak Česká republika tzv. konzumujícím členem dohody CCRA (Common Criteria Recognition Arrangement – jedná se o dohodu o vzájemném uznávání certifikátů systému Common Criteria). To znamená, že není oprávněná vytvářet nová Common Criteria schémata, ani vydávat certifikáty (takovou pravomoc má toliko 17 států), ale certifikáty, které jsou autorizačními členy vydávány, uznává. Je tedy možné mluvit o určitém nepřímém dosahu certifikace kyberbezpečnostních technologií na území České republiky.[102]

---

[100] Viz Důvodová zpráva k vyhlášce č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.

[101] Viz Členství v mezinárodních organizacích. *ÚNMZ* [online]. [vid. 25. prosinec 2018]. Získáno z: http://www.unmz.cz/urad/clenstvi-v-mezinarodnich-organizacich ; UNMZ. *ISO* [online]. [vid. 25. prosinec 2018]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/member/00/21/2133.html.

[102] Viz Common Criteria. *New CC Portal* [online]. [vid. 12. říjen 2019]. Získáno z: https://www.commoncriteriaportal.org/ ; Members of the CCRA: *New CC Portal* [online]. [vid. 25. prosinec 2018]. Získáno z: https://www.commoncriteriaportal.org/ccra/members/

Důvodem k tomu, proč existuje tak málo autorizačních států, je vzájemná mezinárodně-bezpečnostní nedůvěra. Aby na poli kybernetické bezpečnosti vznikla spolupráce založená na vzájemném uznávání certifikátů, musí mezi těmito státy panovat skutečně vysoká míra důvěry ohledně svědomitosti, zodpovědnosti a dostatečné pokročilosti bezpečnostních testů a procedur prováděných dalšími členy. Česká republika, i kdyby měla politický potenciál na to, aby se stala autorizačním členem, nemá na tuto funkci zdaleka potřebné kapacity ani dostatečně vybavené laboratoře.

Česká republika není členem užší evropské spolupráce na poli Common Criteria, která je představována dohodou SOG-IS MRA (z angl. „Senior Officials Group Information Systems Security – Mutual Recognition Agreement“, o této dohodě viz níže).[103]

3.2.2 POTENCIÁLNÍ MÍSTO CERTIFIKACE KYBERBEZPEČNOSTNÍCH TECHNOLOGIÍ V ČESKÉM SYSTÉMU KYBERNETICKÉ BEZPEČNOSTI

Zákon o kybernetické bezpečnosti pracuje zejména s bezpečnostními opatřeními. Ta jsou definována jako „*souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru.*“[104] Takováto opatření musí povinné subjekty provádět v rozsahu, který je nezbytný pro zajištění bezpečnosti informačního systému kritické informační infrastruktury. Dále zákon pracuje s institutem opatření, která definuje jako „*úkony, jichž je třeba k ochraně informačních systémů nebo služeb a sítí elektronických komunikací před hrozbou v oblasti kybernetické bezpečnosti nebo před kybernetickým bezpečnostním incidentem anebo k řešení již nastalého kybernetického bezpečnostního incidentu*“.[105] Ta se dělí na varování, reaktivní opatření a ochranné opatření. Poslední zmíněná se vydávají ve formě

[103] Viz SOG-IS - Home. *SOG-IS* [online]. [vid. 12. říjen 2019]. Získáno z: http://sogis.org/index_en.html.

[104] Viz § 4 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *CODEXIS ACADEMIA* [právní informační systém]. ATLAS consulting [vid. 6. listopadu 2018].

[105] Viz § 11 zákona č. 181/2014 Sb.

opatření obecné povahy a jsou svojí povahou daleko blíže normálnímu správnímu rozhodování než reaktivní opatření, která jsou spíše faktickým zásahem.[106] Pokud by tedy, čistě teoreticky, došlo k zavedení oficiální certifikační procedury kyberbezpečnostních technologií, je pravděpodobné, že by se její pozice pohybovala buď v okruhu bezpečnostních, nebo ochranných opatření,[107] případně pak by mohla fungovat stejně, jako fungovala certifikace podle ISO/IEC 27001 podle staré vyhlášky o kybernetické bezpečnosti. Určujícím je, jestli by certifikace byla vedena jako povinná nebo dobrovolná, případně smíšená.

Certifikace by sama o sobě nemusela být povinná (např. pro výkon určité činnosti nebo provoz kritické informační infrastruktury). Mohla by být formulována jako součást podmínek kvalifikace zadávacího řízení veřejných zakázek, zejména pak těch, které se týkají kritické informační infrastruktury, případně i dalších, bude-li tento požadavek shledán opodstatněným a v souladu se zásadami veřejného investování. V rámci veřejných zakázek si lze držení certifikace (v některých případech) představit rovněž jakožto jedno z kritérií hodnocení. Subjekty k ní také mohou přistoupit např. z tržních důvodů, kdy jim daná certifikace může poskytnout výhodu (zejména z hlediska zvýšení důvěryhodnosti v daný produkt) oproti ostatním konkurentům. Certifikace navíc může být pozitivním znamením pro potenciální investory daného subjektu. Získání certifikace totiž nejen ukazuje splnění určitých kvalitativních požadavků, ale i motivaci (a dispozici s potřebnými prostředky) projít časově a finančně nezanedbatelným procesem.[108] Podmínku certifikace by pak mohlo být možné stanovit jen dodavatelům (a jejich subdodavatelům), kteří by se chtěli účastnit soutěže, aniž by povinnost certifikovat dopadla na ostatní. Pokud by certifikace byla povinná bez dalšího, byla by dle mého názoru jedním z bezpečnostních technických opatření. Takovou certifikaci

[106] Viz POLČÁK; HARAŠTA; STUPKA, op. cit., s. 34.

[107] Dá se usuzovat, že užití certifikovaných technologií by bylo možné opatřením v případě potřeby nařídit.

[108] Certifikace může být ve vztahu k veřejným zakázkám realizována i vícero způsoby – např. jako podmínka akceptace (výsledné řešení získá certifikát). Certifikáty mohou být zároveň součástí i souvisejících povinností, jako např. kodexů podle nařízení GDPR.

by musel mít každý povinný subjekt, jinak by nemohl regulovanou činnost provozovat.

V případě, který jsem nazval jako „*smíšená závaznost*“, jsem měl na mysli obecnou dobrovolnost certifikace, kdy jenom v určitých případech by regulátor (pravděpodobně NÚKIB, případně Komise) stanovil povinnost pro určité subjekty si certifikaci obstarat, případně ji vyžadovat po svých dodavatelích. Tak by byla certifikace svým způsobem ochranným opatřením.

Jako fakultativní může certifikace fungovat buď jako výše zmíněná tržní výhoda, informace pro investory nebo i jen jako informace pro spotřebitele a důkaz, že subjekt naplnil, co mu právo ukládalo, a dosáhl tak stavu compliance. Míra hodnověrnosti certifikátu závisí na povaze certifikačního tělesa, ale pokud budou tato tělesa akreditována státem, neměl by problém s důvěrou nastat. V případě, že by povinný subjekt držel určitý certifikát, vycházelo by se při státní kontrole pravděpodobně z vyvratitelné domněnky, že povinný subjekt je v souladu s právem (bylo by tedy zapotřebí najít důkaz, že není).[109] To je pro povinný subjekt o hodně příznivější situace. Pokud by tedy certifikace byla zavedena jako dobrovolná, jasnou analogií by bylo fungování certifikace dle ISO 27001 ve staré vyhlášce o kybernetické bezpečnosti. Podle ustanovení § 29 této vyhlášky bylo na subjekt, jehož bezpečnostní řešení bylo certifikováno akreditovaným certifikačním orgánem a který vedl v tomto paragrafu specifikovanou dokumentaci, nahlíženo jako na subjekt *„splňující požadavky na zavedení bezpečnostních opatření podle zákona a této vyhlášky*“.[110]

3.2.3 STAV V EVROPSKÉ UNII

V Evropské unii ke dni 12. 10. 2019 neexistuje žádná plně účinná právní úprava unifikující nebo alespoň harmonizující materii obecné certifikace v oblasti kybernetické bezpečnosti (jak bylo zmíněno, část Aktu

[109] Viz POLČÁK; HARAŠTA; STUPKA, op. cit., s. 80.

[110] Viz § 2 9 vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). In: *CODEXIS ACADEMIA* [právní informační systém]. ATLAS consulting [vid. 6. listopadu 2018].

o kybernetické bezpečnosti věnující se jednotnému certifikačnímu rámci je stále ještě z velké části neúčinná a běží implementační lhůta, která končí 27. června 2021). Vyskytují se sice úpravy certifikací pro účely nařízení eIDAS (což je svým uspořádáním velice podobný a již fungující systém), téměř nepoužívaná úprava certifikací pro účely nařízení GDPR, ale v oblasti kybernetické bezpečnosti se vyskytuje pouze směrnice NIS a ta certifikaci neupravuje. Přitom se stav kybernetické bezpečnosti v rámci EU zhoršuje.[111]

Celý stav je ještě umocněn skutečností, že vnitřní kyberbezpečnostní trh Unie byl v absenci jednotného certifikačního systému plně roztříštěn. Je rozpadlý na jednotlivá národní a sektorová řešení bez možnosti vzájemného uznávání certifikátů mezi členskými státy, různé interní standardy, a nejvíce připomíná jakousi širší spolupráci dohoda SOG-IS MRA. Počet různých druhů certifikátů pohybujících se na vnitřním trhu je tím pádem nesmírný.[112] Takováto roztříštěnost trhu způsobuje až absurdní situaci, kdy výrobce, který chce svůj produkt prodávat ve Francii, Německu a Nizozemí, musí tento svůj produkt nechat certifikovat podle „*Certification Cécuritaire de Premier Niveau*" ve Francii, „*Baseline Product Assessment*" v Nizozemí a podle speciálně upraveného modelu Common Criteria v Německu (tzv. „*Německý certifikát*"). Je tak nucen podstoupit tři zdlouhavé a nákladné procedury, což před mnoho podnikatelů staví překážku, kterou nejsou ochotni/schopni překonat.[113]

Panující stav je opakem myšlenky jednotného digitálního trhu, o který Evropská unie usiluje. Již dříve zmíněná směrnice NIS nebo nařízení eIDAS byly významné kroky, které Unii posunuly směrem k unifikaci digitálního

[111] Ekonomický dopad kyber-incidentů se v roce 2016 pohyboval celosvětově okolo jedné miliardy dolarů. Podle Evropské komise se v roce 2016 uskutečnilo více než 4 000 ransomware-útoků denně, což je nárůst o víc jak 300 % oproti roku 2015. Viz NEGREIRO ACHIAGA, Maria Del Mar. *EU Legislation in Progress - Briefing: ENISA and a new cybersecurity act (stav ke dni 16. 1. 2018)* [online]. B.m.: European Parliament Research Service. [vid. 11. říjen 2018].

[112] Viz DROGKARIS, op. cit. ; Pracovní dokument útvarů komise - Souhrn posouzení dopadů k návrhu aktu o kybernetické bezpečnosti [online]. B.m.: Evropská komise. 2017 [vid. 12. červenec 2018].

[113] Viz NEGREIRO ACHIAGA, op. cit.

trhu, ale jak je ze stávající situace patrné, bez sjednocení kyberbezpečnostní certifikace nebude pokrok možný.[114] Členské státy nejsou bez dalšího schopny nebo ochotny hlubší kooperace, která by vedla ke zlepšení kyberbezpečnostní situace v rámci EU, což způsobuje částečnou neúčinnost výhod vnitřního trhu.[115]

Spolupráce v Evropské unii na poli certifikace kyberbezpečnostních technologií je alespoň částečně upravena dohodou SOG-IS, kterou mezi sebou uzavřely některé členské státy.[116] Toto seskupení bylo vytvořeno na základě rozhodnutí Rady ze dne 31. 3. 1992 č. 92/242/EEC, o bezpečnosti informačních systémů, a doporučení Rady ze dne 7. 4. 1995 č. 1995/144/EC, o obecných kritériích pro posuzování bezpečnosti informačních systémů. Jedná se o sdružení 14 členských států (zejména pokročilé státy s vlastními testovacími laboratořemi) a Norska. Toto sdružení mezi sebou úzce spolupracuje na vytváření nových CC schémat, koordinuje své standardizační a certifikační aktivity a členové vzájemně uznávají CC certifikáty až do bezpečnostní úrovně EAL 4.[117] Česká republika není členem dohody SOG-IS a ani nemá zájem se do budoucna jejím členem stát.[118]

Popsaný stav dlouho beze změny přetrvával nejen v České republice, ale především v Unii navzdory tomu, že poptávka po certifikaci byla a je značná,[119] a to zejména ze strany povinných subjektů. Pro ty, na které dopadly compliance povinnosti vycházející z regulace kybernetické

[114] Srovnej s JEŽOVÁ, Daniela. EU Digital Single Market - Are we there yet? *Ad Alta: Journal of Interdisciplinary Research* [online]. 2017, roč. 7, č. 2, s. 1–3.

[115] Viz Pracovní dokument útvarů komise - Souhrn posouzení dopadů k návrhu aktu o kybernetické bezpečnosti [online]. B.m.: Evropská komise. 2017 [vid. 12. červenec 2018].

[116] Viz SOG-IS Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, verze 3.0 [online]. 2010 [vid. 27. říjen 2018].

[117] Viz MITRAKAS, Andreas. The emerging EU framework on cybersecurity certification. *Datenschutz und Datensicherheit* [online]. 2018, roč. 42, č. 7, s. 3–5 [vid. 11. září 2018].

[118] Získáno na základě konzultací s odborníky z NÚKIB. Dále viz SOG-IS - Home. *SOG-IS* [online]. [vid. 12. říjen 2019]. Získáno z: http://sogis.org/index_en.html.

[119] To je patrné hlavně u vyspělejších kyberbezpečnostních trhů s velkým počtem povinných subjektů. Velice žádaný je např. Německý certifikát, stejně tak i některá další národní schémata, případně pak i certifikace podle CC v režimu schémat vytvořených spoluprací SOG-IS. Pro podrobnější informace, viz kapitoly 5 a 6.

bezpečnosti,[120] totiž představuje certifikace jedinou možnost spolehlivého řešení compliance. Větší zájem panuje samozřejmě ve státech, kde je dodržení určité compliance povinnosti navázané na možnost podnikání v určité oblasti. Tak je tomu např. ve Francii, kde je naplnění daného bezpečnostního standardu nutným předpokladem k obchodování se státním sektorem (v oblasti zařízení připojitelných na internet).[121] Pro veřejnoprávní subjekty má certifikát význam i kvůli tomu, že bezpečnostní opatření financují z nejrůznějších projektů (dotací). Jakmile drží certifikát, mohou fungovat bez obavy z toho, že by se později zjistilo nedodržení standardu (který většinou funguje jako závazná podmínka pro udělení dotace), což by dále vedlo k povinnosti dotaci vrátit. Pro členy statutárních orgánů jak soukromoprávních, tak veřejnoprávních subjektů mají certifikáty ještě jeden velice lákavý účinek – mohou posloužit jako štít před osobní odpovědností těchto členů.[122]

4. PERSPEKTIVNÍ ÚPRAVA V EU

4.1 CESTA K NOVÉMU NAŘÍZENÍ

Problematický stav popsaný v závěru minulé kapitoly však nebyl Evropskou unií úplně ignorován. Už v roce 2014 se intenzivně pracovalo na tom, jak tuto situaci změnit. Dne 6. 10. 2014 zorganizovala ENISA (Agentura Evropské unie pro bezpečnosti sítí a informací) společně s Evropskou komisí workshop na téma ICT certifikace a budoucnosti SOG-IS. Tohoto workshopu se zúčastnilo přibližně 60 expertů z různých oblastí představujících různé zájmové skupiny (zúčastnili se reprezentanti veřejných i soukromých certifikačních a standardizačních orgánů, výrobců, spotřebitelů, průmyslových asociací, testovacích laboratoří atd.). Účelem

[120] Např. v Nizozemí musí být povinné subjekty v souladu se standardem definovaným v *„Baseline Informatiebeveiliging Rijksdienst“*.

[121] Viz CSPN: What U.S. companies need to know about the security certification process [online]. [vid. 25. prosinec 2018]. Získáno z: http://www.embedded-computing.com/embedded-computing-design/cspn-what-u-s-companies-need-to-know-about-the-security-certification-process.

[122] Tyto informace byly získány z konzultací a konzultačních emailů s doc. JUDr. Radimem Polčákem, Ph.D.

setkání bylo uvést zúčastněné strany do myšlenky společného certifikačního rámce pro celou Evropskou unii, zjistit jejich názory a probrat s odborníky z oblasti kybernetické bezpečnosti výzvy, kterým bude muset takový rámec čelit. Zpočátku se uvažovalo o rozšíření dosahu dohody SOG-IS na celou Unii, ale tento záměr si nakonec nezískal dostatečnou podporu, a to hlavně kvůli nedostatkům, kterými je systém Common Criteria postižen.[123,124]

Zúčastněné strany (český překlad pro „*Stakeholders*“) vyzdvihly na tomto setkání potřebu společného evropského postupu, potřebu vzájemného uznávání certifikátů a odstranění roztříštěnosti způsobené národními přístupy, která nesmyslně zvyšuje podnikatelské náklady a mnohé z malých a středních podniků úplně vyřazuje z možnosti nechat si svůj produkt certifikovat. Zároveň není takový postup ani moc výhodný pro velké podniky, což ve svém důsledku znamená, že evropský ICT a kyberbezpečnostní průmysl ztrácí (zejména) na USA. Vzhledem k tomu, že mnohé ze zúčastněných stran jsou mezinárodně působící korporace, bylo zdůrazňováno, že nová evropská certifikace by neměla jít proti uznávaným mezinárodním standardům třetích zemí jako např. ISO/IEC a Common Criteria. Řešil se i vztah mezi SOG-IS a touto novou úpravou. Byl vyzdvižen přínos skupiny SOG-IS a prosazována pozitiva adopce jeho standardů a profilů.[125] Kromě tohoto workshopu byly dále svolány i velké veřejné konzultace, a to na konci roku 2015 a začátku roku 2016. Na nich byly provedeny průzkumy mínění zainteresovaných subjektů. Z těchto výzkumů vyšlo najevo, že optimálním řešením by byla obecná a dobrovolná verze

[123] Bez debat se jedná o dominantní certifikační systém na poli kybernetické bezpečnosti ICT produktů, ale má i mezery, u kterých již není pravděpodobné, že by došlo k jejich odstranění. Zvláště byl vyzdvižen naprosto nedostatečně nastavený režim pro certifikaci velkých systémových řešení a služeb, kdy Common Criteria jednoduše neumožňují testovat službu jako kontinuální proces zasazený do určitého prostředí různě interagující se svým okolím. Místo toho se soustředí na certifikaci jednotlivých jeho částí a výsledné chování služby nikdo nekontroluje.

[124] Viz Joint EC/ENISA SOG-IS and ICT certification workshop – Minutes of the workshop [online]. 6. říjen 2014 [vid. 24. srpen 2018].

[125] Viz Joint EC/ENISA SOG-IS and ICT certification workshop – Minutes *of the workshop* [online]. 6. říjen 2014 [vid. 24. srpen 2018].

certifikace, spravovaná agenturou ENISA, jíž by byl stanoven permanentní mandát a rozšířeny pravomoci.[126]

Na základě těchto výstupů tedy Komise ve spolupráci s ENISA začala pracovat na posílení kybernetické bezpečnosti a odolnosti v Unii. Se zhoršující se kyberbezpečnostní situací stoupala i priorita vyřešení společného postupu v této otázce. To se odrazilo např. v rezoluci Evropského parlamentu ze dne 3. 10. 2017, ve které byly členské státy vyzvány k boji proti kyber-zločinu a k urychlení budování kyberbezpečnostní infrastruktury, nebo na společném sdělení Evropskému parlamentu a Radě – „*Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU*“, které předložila Vysoká představitelka Unie pro zahraniční věci a bezpečnostní politiku necelý měsíc předtím.[127]

Jednou z nejdůležitějších částí sdělení, které vydal téhož dne (13. 9. 2017) předseda Komise Jean-Claude Juncker ohledně zvyšování schopností Unie reagovat na kyber-útoky, bylo, že po zohlednění závěrů uvedených mimo jiné ve sdělení Komise o přezkumu naplňování strategie pro jednotný digitální trh,[128] byl Komisí toho samého dne předložen návrh nařízení na posílení mandátu a pravomocí agentury ENISA a o zavedení certifikace kybernetické bezpečnosti informačních a komunikačních technologií (anglicky „*The Cybersecurity Act*“) jako součást tzv.

[126] Viz NEGREIRO ACHIAGA, op. cit..

[127] Viz VYSOKÁ PŘEDSTAVITELKA UNIE PRO ZAHRANIČNÍ VĚCI A BEZPEČNOSTNÍ POLITIKU. *Společné sdělení Evropskému parlamentu a Radě ze dne 13. 9. 2017: Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU* [online]. 2017 [vid. 11. říjen 2018].

[128] Viz Sdělení Komise Evropskému parlamentu, Radě, EHS-výboru a výboru regionů ze dne 10. 5. 2017 o přezkumu v polovině období provádění strategie pro jednotný digitální trh [online]. B.m.: Evropská komise. 10. květen 2017 [vid. 11. říjen 2018] .

Kyberbalíčku[129] a stává se jednou z priorit k naplnění jednotného digitálního trhu.[130]

4.2 AKT O KYBERNETICKÉ BEZPEČNOSTI

Náročná legislativní pouť tohoto revolučního návrhu, která započala dne 13. 9. 2017, byla dokončena dne 17. dubna 2019, přičemž část úpravy certifikačního rámce se použije až od 28. června 2021. Výsledné podoby Aktu se de facto podařilo dosáhnout již 10. prosince 2018, kdy podle tiskové zprávy Evropské komise byla po dlouhých a náročných vyjednáváních ukončena fáze trialogu, kdy Evropský parlament, Rada a Evropská komise konečně nalezly kompromis ohledně podoby Aktu. Od té doby již došlo toliko k oficiálnímu překladu[131] a podoba Aktu se téměř nezměnila, což utlo naděje, že dojde k napravení některých vad Aktu, které jsou zmíněné níže.

Akt má dvě části – 1) rozšíření pravomocí a mandátu ENISA, přičemž tato část není předmětem tohoto článku, 2) zavedení jednotného evropského certifikačního systému. Je vhodné zdůraznit, že Akt samotný nezavádí jednotlivá certifikační schémata, to by bylo legislativně i pragmaticky neúnosné (představa, že by se kvůli každé změně certifikačního schématu muselo měnit nařízení samo, je absurdní). Místo

[129] Kyberbalíček je soubor opatření (zvlášť Junckerova komise byla těmito balíčky známá), které mají vést k posílení bezpečnosti v kyberprostoru. Mimo jiné obsahuje několik opatření ke zlepšení informovanosti o bezpečném chování na internetu či opatření ke zlepšení kyber-hygieny uživatelů. Ostatně i v Aktu o kybernetické bezpečnosti je několikrát zmíněna nově vzniklá povinnost Agentury ENISA k péči o kyber-hygienu a šíření informací o kybernetické bezpečnosti. De facto dostala ENISA za úkol naučit uživatele v Unii, jak se chovat na internetu bezpečněji.

[130] Viz State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks [online]. B.m.: European Comission – Press release. 19. září 2017 [vid. 11. říjen 2018].

[131] Oficiální překlad do českého jazyka s sebou přinesl několik poněkud nešťastných řešení této problematiky. Příkladem budiž překlad anglického „*certification scheme*" do českého „*certifikační systém*". Tato volba je dle mého názoru nejen zbytečná, ale zároveň i matoucí. Certifikační systém je totiž např. Common Criteria, kdežto schéma (jak by se anglické „scheme" dalo jednoduše přeložit) označuje dílčí set kritérií, podmínek a požadavků vztahujících se k danému produktu, službě nebo procesu. Tento článek primárně vychází z anglické varianty a kdykoliv, kdy budu pojednávat o schématu, v řeči české verze Aktu mluvím o certifikačním systému.

toho vytváří rámec pro přijímání evropských certifikačních schémat, a to nejen pro ICT produkty, ale zároveň i pro služby, čímž by měl předčít systém Common Criteria, a pro procesy, čímž se stává vskutku revolučním, neboť dosud žádný mezinárodně přijímaný certifikační rámec nebyl tak ambiciózní, aby integroval všechny tři aspekty dohromady.[132] Svou materií tak může částečně zasáhnout i do oblasti upravené standardy ISO/IEC 27001 ad. Výstupem certifikačních procesů prováděných dle schválených schémat budou v celé Unii univerzálně uznávané certifikáty.[133]

4.2.1 PRÁVNÍ ZÁKLAD NAŘÍZENÍ

Za právní základ Aktu byl zvolen čl. 114 Smlouvy o fungování Evropské unie (dále jen jako „SFEU"), tedy „*oprávnění Evropského parlamentu a Rady přijímat řádným legislativním postupem po konzultaci s Hospodářským a sociálním výborem opatření ke sbližování ustanovení právních a správních předpisů členských států, jejichž účelem je vytvoření a fungování vnitřního trhu a naplňování tak cílů uvedených v článku 26 (který sám stanovuje cíl vytvoření a zajištění fungování vnitřního trhu – poznámka autora)*". Zdůrazněno bylo právě zajištění fungování vnitřního trhu, což vzhledem k tomu, co jsem psal na konci minulé kapitoly, je pochopitelné. Mitrakas k tomuto bodu dodává, že vhodnost užití tohoto ustanovení SFEU byla již v minulosti potvrzena Soudním dvorem Evropské unie v případu C-216/04 (autor dotyčného článku zde pravděpodobně myslel rozhodnutí ve věci C-217/04 Spojené království proti Evropskému parlamentu a Radě) a v Nařízení Parlamentu a Rady č. 526/2013 ze dne 21. 5. 2013 (dosavadní nařízení regulující působení ENISA).[134] Uvádí dále, že „*potenciální fragmentace a omezení možnosti Evropské unie vytvořit vnitřní trh pro kyberbezpečnostní produkty*

[132] Zmíněné tři „*oblasti certifikace*" představují velice rozdílné certifikační systémy, podmiňující si užívání jiných metodik a certifikačních procesů. Zároveň jsou rozdílné i z pohledu vyžadovaných kapacit (technických i personálních) pro provádění certifikace. Jak již bylo zmíněno, certifikační systém Common Criteria, který představuje jeden z nejvíce využívaných certifikačních systémů pro oblast kyberbezpečnostních technologií, je postaven toliko na certifikaci produktů. Měl umožňovat též certifikaci služeb, ale tento cíl se až dosud nepodařilo naplnit.

[133] Viz odstavec 10 článku 56 Aktu o kybernetické bezpečnosti.

[134] Viz MITRAKAS, op. cit., s. 4.

a služby je dostatečným důvodem pro spuštění legislativního procesu v souladu se subsidiaritou.“[135] V odůvodnění první verze návrhu nařízení je toto ještě dále rozvíjeno navázáním na cíle stanovené směrnicí NIS (směrnice o bezpečnosti sítí a informací, jejímž právním základem je též článek 114 SFEU).[136] Vzhledem k tomu, že cílem Aktu je odstranit roztříštěnost evropského trhu a že individuální opatření členských států se neukazují pro posílení společné kybernetické odolnosti Unie jako dostatečná, souhlasím, že opatření ve formě nařízení je vhodné, pochopitelné a potřebné.

Ovšem samotná volba právního základu nařízení může být trochu sporná, což cítili i právníci z Council Legal Service.[137] Proti vystavění Aktu na základech článku 114 SFEU však po celou dobu nikdo ze zúčastněných stran ani států nepodal žádnou zásadní námitku. Nařízení je výsledkem spojení zájmů jednotného a konkurenceschopného trhu, který skutečně je plně v pravomoci Unie, s kybernetickou bezpečností a obecně bezpečnostní politikou, která je stále pod většinovou pravomocí členských států. Dle mého osobního názoru je přinejmenším sporné, jaký efekt je v Aktu důležitější a v praxi se silněji projeví, jestli unifikace roztříštěného trhu a zvýhodnění situace spotřebitelů, nebo posílení kybernetické bezpečnosti a odolnosti Unie. Zvláště když přihlédnu ke skutečnosti, že u systému Common Criteria byl dopad na obyčejné spotřebitele minimální a certifikátů bylo využíváno primárně při interakci se státním sektorem (dodavatelé zabezpečených systémů, provozovatelé kritické informační infrastruktury).[138] Na druhou stranu je nepopiratelným faktem, že nařízení nezasahuje do samotných pravomocí bezpečnostních složek. Je tak pochopitelné zaštítění článkem 114 SFEU. Jednotného certifikačního systému jednoduše bylo na území Unie potřeba a jiná řešení bezpečnosti Unie nebyla dostatečná. A vzhledem k absenci námitek, i přestože je zde pro ně místo, je patrné, že i členské státy si tuto potřebu fakticky

[135] Viz tamtéž.

[136] Toto se zachovalo až do výsledné verze návrhu, přestože vliv NIS na spuštění jednotného certifikačního rámce byl podstatně snížen.

[137] Council Legal Service je právně-poradenský orgán spadající pod Sekretariát Komise.

[138] Viz HEARN, J. Does the common criteria paradigm have a future? *IEEE Security & Privacy Magazine* [online]. 2004, roč. 2, č. 1, s. 1 [vid. 18. říjen 2018].

uvědomovaly. V tomto ohledu jednoduše převážily politické důvody nad čistě formalisticky – právními.

4.2.2 PŘEDSTAVENÍ CERTIFIKAČNÍHO RÁMCE

Vzhledem k tomu, že podrobný rozbor certifikační procedury podle Aktu bude předmětem sedmé kapitoly, zde bude nařízení představeno jako celek.

Akt vytváří páteřní úpravu pro tvorbu dílčích certifikačních schémat – modelových podmínek, podle nichž bude následně certifikovaný produkt (nebo služba či proces) testován. Jedná se o organizační, procesní, technologickou a právní úpravu celého certifikačního procesu. Smyslem nařízení je kromě zvýšení kybernetické bezpečnosti i povzbuzení evropského trhu s kyberbezpečnostními produkty, procesy a službami k vytvoření celosvětově konkurenceschopných subjektů. Akt je naprosto revoluční v unifikaci certifikace produktů, služeb a procesů pod jeden obecný rámec a v případě, že se tento systém osvědčí, mohl by být následně přejímán i státy mimo EU (dle mého názoru je velice pravděpodobné, že prvním nečlenským státem přistoupivším k Aktu bude Norsko, které se již nyní podílí na spolupráci SOG-IS a velice pravděpodobně s ním bude sjednána speciální smlouva o přístupu k certifikačnímu rámci brzo po vstoupení celého Aktu v účinnost).

Unie se přístupem ke kybernetické bezpečnosti liší od toho v USA, mimo jiné také proto, že Unie je v oblasti kybernetické bezpečnosti stále nováčkem. Rychle se rozvíjejícím, ale stále nováčkem (zvláště je to poznat na vyspělosti trhů). Spojené státy americké vyzkoušely několik různých přístupů k regulaci kybernetické bezpečnosti, ale nakonec se rozhodly do standardizační a certifikační regulace tolik nezasahovat (přestože v oblasti pravomocí zpravodajských služeb jsou zásahy stále vcelku citelné) a přenechat ji průmyslu, trhu a soukromým subjektům samotným. Prostředí Států je tak na jednu stranu daleko uvolněnější a prosycené lobbingem, ale na stranu druhou se velice těžko reguluje, když je zapotřebí bezpečnostních opatření. Unie se oproti tomu vydala cestou veřejnoprávní regulace (nařízení je první veřejnoprávní úpravou mezinárodně uznávané

kyberbezpečnostní certifikace) celé materie.[139] Dle mého názoru je prostředí v Unii mimo jiné i kvůli nedostatku zkušeností s certifikací vhodnější právě k rigorózní úpravě. Nedostatek zkušeností by podle mého názoru způsoboval v uvolněném prostředí chaos, nejistotu nebo přebírání nápadů, a tím pádem závislost na jiných, vyspělejších trzích.

Produkty, procesy a služby se podle Aktu budou testovat na naplnění bezpečnostních požadavků, které na ně ukládají jednotlivá certifikační schémata. Náročnost testování se odvíjí od požadované bezpečnostní úrovně produktu, kterou si vybírá investor (schéma samotné může uvést jednu až tři možné úrovně, podrobněji v sedmé kapitole). Akt respektuje a zdůrazňuje skutečnost, že certifikát sám o sobě nemůže garantovat absolutní bezpečnost testovaného produktu, pouze přísnost testů a relativní bezpečnostní úroveň záruky.[140]

Testování v rámci certifikace budou provádět testovací laboratoře. To je subjekt, který vládne dostatečnými kapacitami na to, aby mohl posoudit zabezpečení jednotlivých produktů. Testovací laboratoře mohou být buď samostatné a s certifikační autoritou (subjekt, který posuzuje shodu), pouze spolupracují na základě smlouvy, nebo mohou být přímo její součástí.[141] Vybudování takové testovací laboratoře je finančně nesmírně náročná záležitost. K tomu, aby byli investoři k takovému vytvoření přilákáni, musí trh nabízet dostatečnou možnost návratnosti investice. Certifikační proces totiž samozřejmě nebude zadarmo a testovacím laboratořím se bude za provedení testů platit. Investoři tedy musí očekávat, že zájem o certifikace bude dostatečně velký, aby se jim vybudování testovací laboratoře komerčně vyplatilo. Celé toto schéma však bylo v průběhu vyjednávání o Aktu ohroženo. A dle mého názoru, mohl mít dále popsaný pozměňovací návrh katastrofální následky pro celé uplatnění certifikace v praxi.

---

[139] Viz BELLANTUONO, Giuseppe. Comparing Smart Grid Policies in the USA and EU. *Law, Innovation and Technology* [online]. 2014, roč. 6, č. 2, s. 234–241 [vid. 22. červenec 2018]; KOVÁCS, László. Cyber Security Policy and Strategy in the European Union and NATO. *Revista Academiei Fortelor Terestre* [online]. 2018, roč. 23, č. 1, s. 10–13 [vid. 22. červenec 2018].

[140] Viz body 77–86 odůvodnění Aktu o kybernetické bezpečnosti.

[141] Viz článek 60 a příloha k Aktu o kybernetické bezpečnosti.

Pozměňovací návrh, jednoduše řečeno, navrhoval, aby skutečná certifikace, tedy certifikační proces v testovacích laboratořích pod taktovkou subjektu pro posuzování shody, probíhala jenom v případech, že by si výrobce nechával svůj produkt certifikovat na nejvyšší (a nejpřísnější) bezpečnostní úroveň. Ve střední a nízké úrovni by byla certifikace nahrazena postupem tzv. vlastního posouzení („*conformance self-assessment*"), kdy si podnikatel sám posoudí naplnění stavu compliance. V takovém případě by samozřejmě nikomu nic neplatil (kromě zvýšených nákladů na posouzení bezpečnostních kritérií, což je proti certifikaci stále podstatně nižší částka). Subjekty pro posuzování shody (také jako „CAB") a testovací laboratoře by tak přišly o všechny zájemce o bezpečnostní posouzení nižší a střední úrovně. Očekává se ovšem, že největší zájem bude právě o tyto dvě úrovně, a tak je v nich také ukryt největší komerční potenciál. CAB a testovací laboratoře by tak byly odkázány na komerční potenciál nejvyšší úrovně, který by je na menších a mladších trzích vůbec neuživil. Přijetí tohoto pozměňovacího návrhu by tak vedlo k faktickému zabránění vytvoření CAB a testovacích laboratoří v některých členských státech.

Ani otázka samotných certifikačních autorit nebyla bezproblémová. Zjednodušeně řečeno, certifikační autorita má být nezávislým subjektem, který byl akreditační autoritou akreditován k provádění certifikačních procesů po splnění podmínek, které jsou stanoveny v příloze k tomuto nařízení.[142] Panovala (a domnívám se, že vcelku oprávněná) obava, že státy nebudou dodržovat podmínky akreditace a na vnitřním trhu tak budou vznikat certifikační autority, které nebudou splňovat podmínky nařízení. Je pak představitelné, že by produkty certifikované těmito autoritami nemusely fakticky mít proklamovanou bezpečnostní úroveň. To by mohlo vést až k tomu, že certifikáty z některých států budou mít jinou reálnou hodnotu než ze států jiných, resp. by některé nemusely být fakticky vůbec akceptované (tržní subjekty by si jednoduše vybíraly certifikáty udělené spolehlivějšími autoritami), přestože by byly automaticky uznatelné podle práva. Aby se tento scénář nenaplnil, bylo do Aktu zařazeno několik

[142] Viz tamtéž.

kontrolních opatření. Kontrolu nad subjekty pro posuzování shody budou vykonávat jak národní autority pro certifikaci kybernetické bezpečnosti, tak i akreditační autority, které v případě nesplňování podmínek mohou akreditaci zase odebrat. Navíc certifikační subjekt by se nezodpovědným výkonem certifikačního testování vystavoval riziku, že v případě vzniku újmy kvůli chybě v produktu, procesu nebo službě mu vznikne odpovědnost za tuto škodu.

Komise zpočátku přenechává členským státům moc rozhodnout, jestli učinit certifikaci podle určitého schématu pro povinné subjekty na jejich území obligatorní. Do Aktu byl ovšem s tímto ústupkem prosazen i mechanismus, který dovoluje Komisi po určité časové prodlevě zvážit účinky certifikace na vnitřní trh a učinit certifikaci podle zvoleného schématu obligatorní.[143] Obecně dobrovolný princip byl pro Českou republiku jedním z nejdůležitějších bodů při vyjednávání,[144] a to z důvodu obav z přílišné moci Komise (která si faktickou moc diktovat certifikaci víceméně ponechala, jenom ji časově odsunula) a zároveň kvůli obavám, že se na českém trhu nevyskytuje dostatek kapacit pro institucionální a organizační zabezpečení obligatorní certifikace. V případě, že by byla prosazena plošná povinnost certifikovat produkty kybernetické bezpečnosti, jak navrhovalo např. Nizozemí s odvoláním na lepší implementaci produktů spadajících pod internet věcí, hrozilo by jednotnému trhu soutěžní ohnutí. Evropské certifikační velmoci – Francie, Německo, Nizozemí – by mohly využívat svých stávajících kapacit a nemusely by investovat do zřizování nových testovacích laboratoří žádné prostředky, případně jen velmi málo v porovnání s tím, jaké prostředky by musely vynaložit členské státy, které jsou „*certifikačními nováčky*“. Mezi ty se řadí i Česká republika. Čekala by je buď honba za subjektem či sdružením subjektů, jež by se vybudování CAB a testovacích laboratoří ujaly, nebo by menší státy musely vytvoření laboratoří zafinancovat samy. Na to ovšem většina z nich nemá dostatek volných prostředků, příp. politické vůle, takže není nepředstavitelné, že by

[143] K prvnímu takovému hodnocení dojde do 31. prosince 2023 (tedy po pouhých dvou rocích fungování certifikačního rámce) a dále alespoň každé dva roky.

[144] Ještě na začátku prosince 2018 byla tato otázka otevřena a probíhala bouřlivá jednání, kdy Česká republika stála téměř jako jediná za tímto principem bezpodmínečné dobrovolnosti.

existoval stát bez certifikační autority a laboratoře. To se může stát samozřejmě i při využití dobrovolného principu, ale při takovém rozvržení zůstane na členských státech, aby samy dobře zvážily následky takového kroku a povinné subjekty by tak nemusely zbytečně podstupovat certifikační proces v jiném státu (což opět představuje zvýšení nákladů a přenáší finanční prostředky subjektu do jiného členského státu). S ohledem na dlouho neupravenou implementační dobu nařízení (mohlo se stát, že by Akt vstoupil v účinnost příliš brzo pro certifikační nováčky a vytvoření CAB a laboratoří na mladších trzích by se pak nestihlo) hrozilo, že povinnost certifikace by vedla až k certifikačnímu „*monopolu*" laboratoří Francie, Německa a Nizozemí (pokud nedojde k Brexitu, pravděpodobně by do tohoto uskupení zapadla i Velká Británie), a to podobně, jak je tomu ve zbrojním průmyslu. Riziko monopolu bohužel zůstává, i kvůli nastavení požadavků na CAB, ale kvůli dobrovolnému principu certifikace je nižší a navíc se dá očekávat, že menší státy budou velice tvrdě bojovat proti tomu, aby si trh mezi sebou rozdělily německé a francouzské CAB. Česká republika má v úmyslu využít této šance, zhodnotit tento velký investiční potenciál (zvláště pokud dojde k rychlé implementaci a vytvoření relevantních kapacit) a stát se též jednou z certifikačních velmocí, přestože začíná na pozici relativního certifikačního nováčka.

4.2.3 HARMONIZAČNÍ PŘÍSTUP VS. PŘÍSTUP NA ZÁKLADĚ HODNOCENÍ RIZIK

Při vyjednávání finální podoby nařízení byla dlouho otevřená otázka „*obsahu*" certifikátu, tedy co by vlastně certifikát měl proklamovat a na jakém principu vystavět testování. Harmonizační přístup říká, že není možné za pomoci testování spolehlivě konstatovat, jestli je nějaký produkt bezpečný či nikoliv, a to převážně kvůli neustále se vyvíjejícímu prostředí kyberprostoru (vlastně jediné, co můžeme konstatovat s jistotou, je, že nic není úplně bezpečné). Zastánci tohoto názoru prosazovali zavedení jediné společné úrovně záruky bezpečnosti, která by de facto proklamovala, že produkt byl otestován určitou sérií testů, ve kterých obstál, a tak by se v něm neměly opakovat chyby, které byly v minulosti zneužity.

Princip hodnocení rizik (z angl. „*Risk-based approach*") je oproti tomu založen na kontinuálním procesu vyhodnocování rizik a jejich zvládání, řízení, kontrování nebo alespoň minimalizaci. Subjekt tedy nejdříve stanoví hranici, pod kterou je již riziko přijatelné (může jít buď o riziko sice závažné, ale je velice nepravděpodobné, že by riziková událost nastala, nebo může být riziková událost naopak velice pravděpodobná, ale závažnost následků je minimální) a může se tedy dočasně ignorovat a posléze začne vyhodnocovat jednotlivá rizika na základě předem stanovených kritérií (ta můžou být stanovena externě nebo interně). Zvládání rizik (z angl. risk-management) je pak proces, který snižuje rizika na úroveň přijatelnosti.[145,146] V případě aktu o kybernetické bezpečnosti šlo o stanovení tří rozdílných úrovní záruky, kdy u každé další úrovně je hranice přijatelnosti rizik vyšší a tím pádem je testování na danou úroveň přísnější a požadovaná bezpečnostní protiopatření komplexnější. Produkty se pak hodnotí ad hoc podle toho, jaká rizika jim mohou reálně hrozit v určitém prostředí a též podle toho, na jakou úroveň je daný produkt certifikován. Tento přístup byl podporován i ze strany různých zainteresovaných stran, např. Schneider Electric[147] nebo TÜV SÜD a TÜV NORD[148] (jedná se o jednu z největších německých elektrotechnických inspekčních a certifikačních asociací), takže není divu, že nakonec převážil. V Aktu je však patrný i určitý průnik harmonizačního přístupu, zvlášť ve formulaci bezpečnostních úrovní. Princip hodnocení rizik má totiž sám o sobě jednu velkou slabinu – může způsobit pocit falešného bezpečí, a to zvláště ve spotřebitelích. Akt o kybernetické bezpečnosti však zvládl tuto

[145] Viz KRISTENSEN, V.; AVEN, T.; FORD, D. A new perspective on Renn and Klinke's approach to risk evaluation and management. *Reliability Engineering & System Safety* [online]. 2006, roč. 91, č. 4, s. 1–3 [vid. 11. listopad 2018].

[146] Srov. s KLINKE, Andreas; RENN, Ortwin. A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies. *Risk Analysis* [online]. 2002, roč. 22, č. 6, s. 1–2 [vid. 11. listopad 2018].

[147] Viz STANTCHEV, Pentcho. Cybersecurity of Industrial Systems. In: *Effectively Implementing the EU Certification Framework: Market Perspectives* [online]. Brusel, Belgie. 2018 [vid. 25. září 2018].

[148] Viz PRILLER, Christian. Effectively Implementing the EU Certification Framework: Market Perspectives - TÜV-SÜD-AG. In: *Effectively Implementing the EU Certification Framework: Market Perspectives* [online]. Brusel, Belgie. 2018 [vid. 25. září 2018].

nevýhodu alespoň v teorii kontrovat povinností informovat o rozsahu bezpečnostních záruk. V praxi bude potřeba osvětové činnosti ENISA a ostatních k tomu, aby koncoví uživatelé a spotřebitelé tomuto negativnímu následku nepodléhali.

5. AKTUÁLNÍ CERTIFIKAČNÍ ŘEŠENÍ – MEZINÁRODNÍ INICIATIVY

V této kapitole přistoupím k prvnímu konkrétnímu pojednání o tom, jak fungují certifikační systémy v praxi. Představím Mezinárodní organizaci pro standardizaci (oficiálním českým překladem ISO je *„Mezinárodní organizace pro normalizaci*“, ale s ohledem na kulturně-historické důvody jsem toho názoru, že je tento způsob překladu poněkud nešťastný, a místo toho se tak přikláním k verzi „*Mezinárodní organizace pro standardizaci*“) jako největší a pravděpodobně nejvýznamnější mezinárodní organizaci působící v této oblasti a rodinu kyberbezpečnostních standardů ISO 27K, kterým dala vzniknout. Těmto standardům se budu věnovat kvůli výše zmíněnému rozsahu Aktu o kybernetické bezpečnosti. Hlavní pozornost této kapitoly bude však zaměřena na představení a detailní rozebrání certifikačního rámce Common Criteria.

5.1 ISO

5.1.1 HISTORIE

Mezinárodní organizace pro standardizaci vznikla v roce 1946. Stalo se tak na konferenci v Londýně spojením dvou jiných organizací – ISA (International Federation of the National Standardizing Associations, která byla založena v New Yorku v roce 1926 s ústředím ve Švýcarsku) a UNSCC (United Nations Standards Coordinating Committee, založená v roce 1944 s ústředím v Londýně). Na konferenci, která představovala začátek ISO, se sešlo 65 delegátů z celkem 25 zemí. Organizace oficiálně započala svoji činnost v roce 1947.[149]

[149] Viz INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; CENTRAL SECRETARIAT. *Friendship among equals: recollections from ISO's first fifty years.* [online]. Geneva: ISO Central Secretariat, 1997, s. 15–18 [vid. 25. prosinec 2018].

Svůj první standard (v té době označovaný jako doporučení) publikovalo ISO v roce 1951. Stal se prvním krokem směrem ke skutečně velkému úspěchu organizace – publikaci unifikovaného mezinárodního systému jednotek SI v roce 1960. V 60. letech minulého století zároveň vznikl nový typ členství v ISO (neboť organizace se začala rozrůstat o rozvojové země) – tzv. „*Correspondent membership*“. Rozvojové země si tak mohly udržet přehled o dění v této mezinárodní organizaci, aniž by musely platit plné členské poplatky. Velký rozmach a opravdovou internacionalizaci zažilo ISO v 80. letech a také později pod vedením Lawrence D. Eichera, po kterém je pojmenována cena za vynikající práci v oboru standardizace.[150]

5.1.2 ČLENSTVÍ

Členství v organizaci ISO získávají přímo standardizační orgány daných zemí (vždy ten nejvíce vlivný orgán, členství je omezeno na jeden orgán za stát), přičemž každý člen pak reprezentuje ISO ve své zemi. Členem se nemůže stát obchodní společnost ani fyzická osoba. Organizace se rozrostla až tak, že ke dni 12. 10. 2019 má celkem 164 členů. Členství se dělí na „*Full Member*“ s plnými členskými právy a možností vyjadřovat se k připravovaným standardům, „*Correspondent Member*“, který vývoj uvnitř ISO sice jenom sleduje a sám ovlivnit nemůže, ale připravené standardy může prodávat nebo sám adoptovat, a „*Subscriber Member*“, který je o dění v organizaci informován, ale nemůže se na ní nijak podílet (je jim znemožněno veškeré oficiální nakládání se standardy). Úrovni členství odpovídá výše členských příspěvků.[151]

Na přijímání standardů se kromě členů podílí více než 250 různých sektorových výborů. Členové ISO se mohou rozhodnout, jestli k určitému výboru vůbec přistoupí, a zároveň mohou nadefinovat míru své účasti – „*účastnící se*“ členové jsou nadáni hlasovacími právy, kdežto „*sledující*“ členové mohou zasahovat do dění pouze radami, kritikou nebo

[150] Viz The ISO Story. *ISO* [online]. [vid. 25. prosinec 2018]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/home/about-us/the-iso-story.html.

[151] Viz *Members ISO* [online]. [vid. 12. říjen 2019]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/home/about-us/members.html.

připomínkami. Při vývoji standardů je vývoj konzultován se zástupci rozvojových zemí, kteří jsou členy ISO, i se zástupci zúčastněných stran. Samotný proces přijímání je založen na konsensu.[152]

5.1.3 CERTIFIKACE

ISO samo o sobě certifikace svých standardů neprovádí a výslovně na to upozorňuje. Uživatel by tak měl zpozornět, pokud by mu podnikatel tvrdil, že produkt byl certifikován Mezinárodní organizací pro standardizaci. Je možné certifikovat soulad s některým ze standardů ISO (poté se tedy uvádí, že je např. ISMS certifikován podle ISO/IEC 27001:2013, přičemž první číslo značí řadu standardu a druhé rok revidované verze standardu), posouzení shody však musí provést některá z externích společností – certifikačních autorit, které jsou k tomu akreditovány akreditačním orgánem. Proces akreditace, zjednodušeně řečeno, představuje oficiální uznání, že určitý subjekt (certifikační autorita) je způsobilý provádět certifikační proces a že funguje v souladu s určitými standardy, které obsahují podmínky provozu takového tělesa. Tyto standardy vydává i Výbor pro posuzování shody („*Committee on Conformity Assessment*“ nebo ve zkratce CASCO), který patří pod ISO a který se otázkou posuzování shody zabývá.[153] Akreditační autoritou v České republice je z pohledu ISO Český institut pro akreditaci, o. p. s.[154]

Vzhledem k tomu, že proces certifikace se nachází mimo působení a zájem ISO, není explicitně řešena ani otázka vzájemného uznávání certifikátů napříč jednotlivými státy. Zůstává tak na členech, aby mezi sebou uzavřely dohody (anglicky označovaných jako „Mutual Recognition Agreements”, krátce MRA), které by zaručovaly vzájemné uznávání

[152] Viz Developing standards. *ISO* [online]. [vid. 25. prosinec 2018]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/home/developing-standards.html ; Who develops standards. *ISO* [online]. [vid. 25. prosinec 2018]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/home/developing-standards/who-develops-standards.html.

[153] Viz *Certification.ISO* [online]. [vid. 25. prosinec 2018]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/home/standards/certification--conformity/certification.html.

[154] Viz IAF MEMBERS: Czech Republic. *International Accreditation Forum* [online]. [vid. 25. prosinec 2018]. Získáno z: https://www.iaf.nu/articles/IAF_MEM_Czech_Republic/66.

vydávaných certifikátů. Ukázkou takovéto dohody je dohoda SOGIS-MRA, která zaručuje uznávání certifikátů Common Criteria mezi členy evropského sdružení SOGIS.[155]

5.1.4 IEC – MEZINÁRODNÍ ELEKTROTECHNICKÁ ORGANIZACE

Z pojmenování standardu ISO/IEC 27001:2013 je patrné, že ISO není jediná organizace, která se na tvorbě standardu podílela. IEC je zkratka z „*International Electrotechnical Commission*" – organizace založené v roce 1906. IEC je vedoucí světovou organizací pro standardizaci produktů v oboru elektrotechniky,[156] a není tak divu, že při přípravě standardů z oblasti IT a ICT spojily organizace ISO a IEC síly ve formě Společného Technického Výboru ISO/IEC JTC 1 (Joint Technical Committee ISO/IEC JTC 1). Jeho podvýbor pojmenovaný ISO/IEC JTC 1/SC 27, který funguje od roku 1989, se zabývá vytvářením standardů v oblasti informační bezpečnosti (ke dni 12. 10. 2019 byl přímo odpovědný za 187 funkčních a 74 připravovaných standardů, a to včetně rodiny ISO/IEC 27K). Česká republika (přesněji řečeno Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, dále jen jako „ÚNMZ") s tímto podvýborem aktivně spolupracuje na tvorbě standardů a je tak jedním z 49 členů ISO, kteří v tomto výboru působí.[157]

5.1.5 RODINA MEZINÁRODNÍCH STANDARDŮ O INFORMAČNÍ BEZPEČNOSTI ISO/IEC 27K

Nejznámějším členem této rodiny je již zmiňovaný standard ISO/IEC 27001:2013 (= jeho poslední revize pochází z roku 2013), který představuje poněkud rigidní úpravu vytvoření, zabezpečení a udržení funkčního ISMS. Jeho první verze vznikla v roce 2005 a byla založena na

[155] Viz HEAD, Katie Bird. ISO workshop on Mutual Recognition Agreements. *ISO* [online]. [vid. 25. prosinec 2018]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/contents/news/1998/04/Ref749.html.

[156] Viz IEC - About the IEC [online]. [vid. 25. prosinec 2018]. Získáno z: https://www.iec.ch/about/?ref=menu.

[157] Viz ISO/IEC JTC 1/SC 27 - IT Security techniques. *ISO* [online]. [vid. 12. říjen 2019]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/committee/04/53/45306.html.

bezpečnostním standardu z Velké Británie (BS 7799-2). Určený je primárně společnostem, které jakýmkoliv způsobem operují s informacemi, ale obecně řečeno není z možnosti implementace vyloučen žádný subjekt.[158] Ani tento standard nevládne sám o sobě žádnou právní závazností, ale i kvůli své kvalitě a širokému uznávání se v mnohých státech dočkal buď právního uznání (ČR), nebo je přímo právem vyžadován (Japonsko).[159]

Standard se skládá ze dvou částí – z obligatorních specifikací, podle kterých se hodnotí shoda v certifikačním procesu, a z „*Code of Practice*", což je návod, ve kterém je popsána osvědčená praxe („*Best Practice*"). Specifikem druhé části je používání slov jako „*should*" (oproti první části, která užívá „*shall*"), z čehož je patrný doporučující charakter druhé části. Shoda s ní není pro účely certifikace nutná. Společnosti tak mohou použít třeba jenom některé z praktik zde popsaných, případně vůbec žádné, aniž by to mělo jakýkoliv negativní dopad na shodu.[160]

ISO 27001 úzce souvisí s dalším standardem – ISO 27002:2013. Kde ISO 27001 popisuje nástroje (především tedy z přílohy A), ISO 27002 obsahuje návod, jak takové nástroje správně implementovat. Oba dva standardy pak pracují s charakteristikami, definicemi a názvoslovím, jež jsou zakotveny ve standardu ISO 27000. Posledně zmíněný standard snižuje riziko nedorozumění při komunikaci jak v rámci společnosti, tak i s certifikačním orgánem.[161]

Aby mohl proces implementace ve společnosti započít, je nutné si pořídit kopie zmíněných standardů, neboť ty (na rozdíl od dokumentace Common Criteria) nejsou zdarma přístupné. Aktuální text standardu ISO 27001:2013 je k dostání za 300-500,- Kč.[162] Ceny zbylých dvou standardů se pohybují v obdobné výši. Nejnáročnější část celého procesu (kromě samotného vytvoření ISMS) bude pro většinu společností komplexní posouzení a vyhodnocení rizik (jak interních, tak externích), které

[158] Viz BÂRSAN, op. cit., s. 21.

[159] Viz SMEDINGHOFF, op. cit., s. 44.

[160] Viz CALDER, Alan. *Nine steps to success an ISO27001:2013 implementation overview* [online]. Ely, Cambridgeshire, U.K.: IT Governance Pub., 2013, s. 9–17 [vid. 11. listopad 2018].

[161] Viz tamtéž.

[162] K dostání např. zde: https://shop.normy.biz/detail/95805.

provádějí v přípravné fázi samy. Identifikují tak relevantní hrozby i zranitelné oblasti. ISMS by mělo být uzpůsobeno právě tomuto hodnocení a schopno adekvátně reagovat. Mělo by být přizpůsobeno jednotlivým částem společnosti a jednotlivým typům osob, které s ním přijdou do styku (spotřebitelé i zaměstnanci). Zúžení záběru ISMS pouze na relevantní oblasti se však může ukázat jako nemožné, případně popírající smysl ISMS jako celku, a musí tak pokrýt celou aktivitu společnosti.[163]

Proces implementace pokračuje stanovením interní politiky společnosti integrující ISMS, pro jejíž obsah standard ISO 27001 stanovuje sérii minimálních požadavků. Mezi témata, která mohou být takto upravena, patří politika utajení informací, kontrola přístupu k informacím, politika hesel či politika využívání kryptografických nástrojů. Po stanovení politik a vyhodnocení rizik jsou na řadě opatření, která mají rizika vyhodnocená jako nepřijatelná kontrovat. Taková opatření mohou mít podobu „*krizových*" plánů a dalších prvků řízení (celkem jich standard uvádí 114 v příloze A). Nezávislá certifikační autorita poté kontroluje vymezení rozsahu ISMS, jeho interakce s prostředím a hodnotí efektivitu zavedených protiopatření. V případě, že subjekt splní minimální požadavky stanovené ve standardu (subjekt může implementovat i daleko přísnější opatření, případně inovativnější, které nemusí standard explicitně uvádět, a pak je čistě na certifikační autoritě, aby posoudila efektivitu takového opatření), udělí mu certifikační autorita certifikát.[164]

Rodina standardů ISO 27K momentálně obsahuje již víc než 30 standardů, které jsou zacíleny na informační bezpečnost (každý další standard se zabývá specifickou částí zabezpečení informací).[165] Např. ISO 27040 obsahuje doporučení pro bezpečné ukládání dat, ISO 27037 doporučení pro zjišťování, sběr, získávání a uchovávání digitálních důkazů, nebo standard ISO 27032, který obsahuje bezpečnostní doporučení týkající se kyberprostoru.[166]

[163] Viz BÂRSAN, op. cit., s. 21-22.

[164] Viz tamtéž, s. 22–26.

[165] Viz CALDER, op. cit., s. 9–17.

[166] Viz MEHAN, op. cit., s. 183–188.

5.2 COMMON CRITERIA

Common Criteria nejsou „*pouhým*“ certifikačním schématem jako je ISO/IEC 27001:2013. Jedná se o komplexní certifikační systém pro bezpečnost IT technologií, sestávající z mnoha dílčích certifikačních schémat pro jednotlivé produkty, které mají „*poskytovat záruky, že procesy specifikace, implementace a vyhodnocení prvku počítačové bezpečnosti bylo provedeno standardním rigorózním a opakovatelným postupem na úrovni odpovídající cílovému prostředí použití*“.[167] Common Criteria byla vytvořena k tomu, aby „*umožňovala srovnatelnost výsledků nezávislých bezpečnostních hodnocení (a odstraňovala vícekolejnost právních úprav certifikačních režimů – pozn. autora). Činí tak stanovením obecného souboru požadavků pro bezpečnostní funkčnost IT produktů a pro úrovně záruky za spolehlivost produktů, kdy tyto požadavky jsou pak v procesu hodnocení na produkt aplikovány. IT produkty zahrnují řešení hardwarová, softwarová i firmwarová. Hodnotící proces, splňující požadavky stanovené v CC, zajišťuje společnou úroveň důvěry ve funkčnost bezpečnostních řešení i záruky za jejich spolehlivost a výsledky takového procesu mohou pomoci spotřebitelům určit, zda IT produkty splňují jejich bezpečnostní požadavky.*“[168]

Jedná se tak o prostředek, který umožňuje mezinárodní spolupráci v oboru hodnocení bezpečnosti ICT produktů. Jeho cílem je zvyšovat bezpečnostní úroveň pomocí předvídání a ex ante kontrování rizik a zranitelností, stejně jako odstraňování známých zranitelností, tedy postup ex post. Nejedná se o rigidní řešení předepisující pevnou sadu minimálních požadavků na zabezpečení tak, jak to dělá ISO 27001, ale umožňuje i uživatelům, aby nadefinovali své vlastní požadavky na bezpečnost, funkčnost a spolehlivost produktů. Zároveň usnadňuje uživatelům orientaci v nabízených bezpečnostních řešeních a umožňuje porovnávat úrovně jejich faktické „*bezpečnosti*“. Common Criteria mohou využít i vývojáři ke

[167] Viz JIRÁSEK; NOVÁK; POŽÁR, op. cit., s. 35.

[168] Viz Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model [online]. Verze 3.1, páté vydání. B.m.: Common Criteria Management Committee, 2017, s. 11 [vid. 12. září 2018].

kvalitnější implementaci bezpečnostních řešení, která by zároveň vyhovovala přáním uživatelů, a to již v rámci vývoje produktu.[169]

5.2.1 HISTORIE

V roce 1993 započalo uskupení složené z reprezentantů společností operujících v oblasti IT bezpečnosti a standardizace z USA (založené na systému TCSEC), Kanady (CTCPEC) a Evropského společenství (ITSEC)[170] práci na vytvoření nového certifikačního rámce, který by kombinoval všechna tři zmíněná kritéria a odstranil tak roztříštěnost úprav. Na tento nově vzniklý rámec měla dohlížet Mezinárodní organizace pro standardizaci (ovšem naplnění tohoto cíle se v průběhu příprav kritérií trochu zkomplikovalo). Kritéria byla dokončena v roce 1996 (verze 1.0), ovšem oficiálně publikována byla až verze 2.0, která následovala v roce 1998 po rozsáhlých revizích. Systém „*Common Criteria for Information Technology Security Evaluation*" (jednoduše Common Criteria nebo též pod oficiální zkratkou CC) si získal od počátku neobvyklou oblibu. Po publikaci verze 2.0 společně uzavřely Kanada, Francie, Německo, Spojená království a USA dohodu o vzájemném uznávání certifikátů vzešlých ze systému CC (CCRA – CC Recognition Agreement), čímž byl projekt oficiálně spuštěn. Hned následujícího roku se k dohodě přidala Austrálie a Nový Zéland a další státy následovaly nedlouho poté. Ještě téhož roku (tj. 1999) byla vydána první úprava – verze 2.1, která byla po dohodě adoptována Mezinárodní organizací pro standardizaci a Common Criteria byla přejata do mezinárodního standardu ISO 15 408 (text CC je totožný se zněním standardu).[171]

---

[169] Srov. ISA, Mohd Anuar Mat et al. Finest authorizing member of common criteria certification. In: *2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)* [online]. Kuala Lumpur, Malaysia: IEEE, 2012, s. 156 [vid. 22. červenec 2018].

[170] TCSEC = Trusted Computer System Evaluation Criteria, CTCPEC = Canadian Trusted Computer Product Evaluation Criteria, ITSEC = Information Technology Security Evaluation Criteria.

[171] Viz TANTAWI, Randa. Common Criteria. *Salem Press Encyclopedia* [online]. 2013 [vid. 13. září 2018].

Common Criteria se dočkala napříč lety ještě několika přepracování a nejaktuálnější (vydaná v dubnu 2017) je verze 3.1, páté vydání.[172] Přepracovávání kritérií je v poslední době motivováno především snahou zjednodušit celý proces, dokumentaci, odstranit podvojnou úpravu z jednotlivých dokumentů a urychlit certifikační proces.

V roce 2003 došlo k pokusu ustanovit Common Criteria jako oficiální a povinný certifikační rámec pro organizaci NATO. Mezi členskými státy ovšem nebylo dosaženo shody, a tak byla vydána pouze směrnice NATO, podle které je certifikace podle CC sice doporučeným, ale nikoliv povinným bezpečnostním řešením. I přesto jsou schémata a certifikáty, které byly schváleny orgány členských států, uznávány v rámci celého NATO jako projev vzájemné důvěry.[173]

Ke dni 12. 10. 2019 bylo členem dohody CCRA 31 zemí světa. Největší událostí nedávné minulosti byla změna statusu Velké Británie, která odstoupila od statusu „*produkující certifikáty*" a stala se jen dalším z konzumentů (dle vyjádření pro nedostatečnou poptávku po certifikaci na území Velké Británie). Členství má dvě formy – 17 států má status „*produkují certifikáty*" (tj. ti, kteří mohou provádět certifikaci podle schémat CC) a 14 států „*uznávající certifikáty*".[174] Tzv. „*Consuming*" členové certifikáty vyprodukované první skupinou uznávají, ale jim samotným není umožněno certifikáty autorizovat. Tento typ členství vznikl po roce 2000, aby se mohly přidat k CCRA i státy, jejichž vnitrostátní kapacity neumožňují provádět certifikaci na požadované úrovni.[175] Česká republika je od roku 2004 jedním z těchto států a mezinárodní normě ISO/IEC 15408 byl udělen status české technické normy (tedy ČSN EN ISO/IEC 15408). Reprezentaci ČR v rámci CCRA zajišťuje podle oficiálních stránek CC

[172] Viz Common Criteria. *New CC Portal* [online]. [vid. 12. říjen 2019]. Získáno z: https://www.commoncriteriaportal.org/.

[173] Viz Informace o hodnocení bezpečnosti informačních technologií Common Criteria (CC) [online]. B.m.: Národní bezpečnostní úřad. 2005 [vid. 4. leden 2019].

[174] Viz Common Criteria. *New CC Portal* [online]. [vid. 12. říjen 2019]. Získáno z: https://www.commoncriteriaportal.org/.

[175] Viz TANTAWI, op. cit.

Národní bezpečnostní úřad,[176] ale jedná se dle mého názoru o zastaralou informaci, neboť působnost na poli kybernetické bezpečnosti měl převzít NÚKIB beze zbytku.

5.2.2 SYSTEMATIKA CC

Páteří celého systému Common Criteria je samotný dokument CC rozdělený do 3 částí – Úvod a obecný model, Požadavky na funkčnost zabezpečení (SFR) a Požadavky na spolehlivost (SAR). Tento ústřední dokument je pak v praxi doplněn řadou podpůrných či vysvětlujících dokumentů a zpráv, mezi kterými zastává výsostné postavení tzv. CEM – Common Evaluation Methodology. Jedná se o metodologii, která byla vyvinuta specificky pro provádění posuzování podle Common Criteria, aby bylo dosaženo maximálně jednotného postupu při provádění testů napříč různými státy.[177]

První část obsahuje zejména základní definice, principy a zásady hodnocení, a jak už název oddílu napovídá, je zde i představen naprosto nejzákladnější model hodnocení. Druhá část je de facto seznamem zabezpečovacích funkčních komponent, které jsou roztříděné do 11 tříd – např. třída využívání zdrojů, kryptografické podpory, správy bezpečnosti, komunikace či soukromí. Každá ze tříd se dále dělí na rodiny a ty dále na komponenty. Tyto komponenty jsou pak středobodem funkčního hodnocení produktů. Třetí část CC stanovuje soubor komponent pro formulaci a popis požadavků na záruku spolehlivosti, který je možné použít jako určitou formu základní šablony. Zároveň jsou zde stanoveny hodnotící kritéria pro profily ochrany a bezpečnostní cíle (vysvětleno níže). Jednotlivé komponenty jsou opět sdruženy do jednotlivých rodin a tříd podle obsahové sounáležitosti (např. třída zaměřující se na průvodní dokumentaci, vývoj, testování, správu konfigurace aj.). Oproti druhé části je řazení komponent v tomto oddíle přísně hierarchizováno s rostoucí

[176] Viz Members of the CCRA. *New CC Portal* [online]. [vid. 25. prosinec 2018]. Získáno z: https://www.commoncriteriaportal.org/ccra/members/#CZ.

[177] Viz *Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model* [online]. Verze 3.1, páté vydání. B.m.: Common Criteria Management Committee, 2017, s. 37 [vid. 12. září 2018]; Informace o hodnocení bezpečnosti informačních technologií Common Criteria (CC) [online]. B.m.: Národní bezpečnostní úřad. 2005 [vid. 4. leden 2019].

složitostí a úrovní formálnosti. Z tohoto uspořádání pak vychází 7 úrovní záruky spolehlivosti produktů (Evaluation Assurance Levels – EAL), což jsou již v samotných CC vytvořené balíčky komponent pro hodnocení záruky jednotlivých produktů. Pro složené produkty byla vytvořena obdoba EAL nazvaná „*Composed Assurance Packages*“ (nebo zkráceně jednoduše CAP).[178]

5.2.3 EALS

EAL 1-7 formulují různé úrovně záruky, že je produkt spolehlivý a bezpečný. Vyjadřují, jak přísným testováním produkt před udělením certifikátu prošel a jak vážným hrozbám by měl produkt odolat. Vývojář si sám vybírá, na jakou úroveň svůj výrobek nechá certifikovat (přitom obvykle vychází nejen z vlastního odhadu závažnosti hrozeb, ale i požadavků uživatelů a ostatních zúčastněných stran).

EAL 1 je nejnižší stupeň záruky, který je určen pro případy, kdy je potřeba určité minimální záruky za bezpečnost produktu, ovšem v prostředí, ve kterém je výskyt závažnějších hrozeb nepravděpodobný. Hodnocení probíhá neformálně a soustředí se primárně na dokumentaci. Není vyžadována zvláštní spolupráce vývojářů produktu a hodnocení probíhá bez funkčního testování produktu samotného. V případě EAL 2 vývojář již musí spolupracovat a dodat specifické informace o produktu a jeho bezpečnostních funkcích. Testování sice probíhá stále ještě primárně na základě dodané dokumentace, ale aspekty a zranitelnosti, které vyjdou najevo z prozkoumání dokumentace, se testují již přímo na produktu (analýza zřejmých zranitelností atp.). Příprava na testování na tento stupeň již vyžaduje speciální přípravu a vypracování bezpečnostních procedur, ale zásadně ještě nezvyšuje náklady, jako je tomu u dalších úrovní. EAL 3 již zahrnuje rozsáhlejší a podrobnější testování produktu, zároveň se v něm jako v prvním objevuje i kontrola vývojového prostředí. EAL 4 je poslední, kterého lze ze zásady dosáhnout bez speciálních znalostí a dovedností v oboru. Je zároveň poslední, kterého lze dosáhnout pro již existující

[178] Viz Informace o hodnocení bezpečnosti informačních technologií Common Criteria (CC) [online]. B.m.: Národní bezpečnostní úřad. 2005 [vid. 4. leden 2019].

produkt, vyšší úrovně již vyžadují promítnutí bezpečnostních opatření do celého životního cyklu produktu, tedy již od vývojového stádia („*Security by design*“). Pro standardní produkty již tato úroveň představuje střední až vysokou úroveň záruky bezpečnosti a pro vývojáře představuje vynaložení zvýšených nákladů na správu zabezpečení. Tato úroveň pracuje s detailní dokumentací doprovázející produkt (v některých případech se stále jedná o zkoumání neformální – např. u modelu bezpečnostní politiky). Zároveň často vyžaduje dodání alespoň části zdrojových kódů bezpečnostních opatření, což některým vývojářům nemusí být příjemné. Při hodnocení se testuje schopnost odolat útočníkům s nízkým útočným potenciálem (tzn., že takový útočník má značně omezené zdroje či vědomosti, příkladem může být útočník označovaný v hackerské komunitě jako „*Script kiddie*“ – využívající toliko hotových skriptů a aplikací, bez skutečné znalosti materie). Až do této úrovně včetně je metodika hodnocení upravena v CEM. U vyšších úrovní je testování již tak komplexní, že metodika pro tuto oblast zatím vyhotovena nebyla. Pro porovnání uvedu, jak vypadá nejvyšší úroveň EAL 7. Tato úroveň je určená pro extrémně rizikové prostředí nebo pro ochranu extrémně hodnotných aktiv. Zároveň není mnoho testovacích laboratoří, které by zvládly otestovat produkty na tuto úroveň. Vývojář již musí dodat plně formální dokumentaci v celé její šíři včetně modelů bezpečnostní politiky. Při testování produktu se využívá metody „*white-box*“ – testy jsou zaměřené na vnitřní strukturu produktu, na jeho kódování a design. V tomto typu testování je celý kód zpřístupněn testujícímu subjektu a jedná se tak o hloubkový test (oproti tomu stojí tzv. „*black-box*“ testování, kdy testovacímu subjektu kód zpřístupněn není, testování probíhá z pohledu konečných uživatelů a zaměřuje se na funkčnost produktu).[179]

5.2.4 ORGANIZAČNÍ STRUKTURA

Na fungování projektu Common Criteria dohlíží tzv. „*Common Criteria Management Committee*“ (dále také jako „CCMC“), výbor, který je složen ze

[179] Viz Informace o hodnocení bezpečnosti informačních technologií Common Criteria (CC) [online]. B.m.: Národní bezpečnostní úřad. 2005 [vid. 4. leden 2019]; ISA et al, op. cit., s. 156.

zástupců jednotlivých členských států. CCMC je nejvyšším orgánem, který řídí zejména politická rozhodnutí související se spoluprací na CC. Od roku 2000 navíc pravidelně pořádá Mezinárodní konference o Common Criteria (ICCC), které jsou pokaždé pořádány v jiném členském státě. Tyto konference slouží k šíření osvědčených praktik, představování nových výzev a technologií a zprostředkování dialogu mezi zúčastněnými stranami a organizačním aparátem Common Criteria. CCMC má dva pomocné orgány – CCDB („*Common Criteria Development Board*"), která se zabývá technickým vývojem kritérií a dohlíží na jejich správnou a zodpovědnou aplikaci v členských státech, a CCMB („*Common Criteria Maintenance Board*"), jejíž úkol spočívá v hodnocení návrhů na změnu kritérií a udržování dialogu s členskými státy a Mezinárodní organizací pro standardizaci.[180]

Kromě organizačního aparátu, dohlížejícího na stav kritérií samotných, spadají do organizační struktury i testovací laboratoře a certifikační autority, bez nichž by faktický provoz certifikace nebyl možný. Common Criteria, respektive CCRA specificky rozlišuje testovací laboratoře od certifikačních autorit a dává tak možnost komerčnímu vzniku testovacích laboratoří, které mohou sloužit pro vícero certifikačních autorit nebo naopak. Testovací laboratoře jsou vázané podmínkami provozu stanovenými v CCRA – tzn., že tyto podmínky čerpají svou závaznost z možnosti uznávání certifikátů. Bez naplnění těchto podmínek nebudou certifikáty uznány a subjekt dostane pouze hezký vnitrostátní certifikát s potenciálně špatnou reputací. Hlavní podmínkou je akreditace laboratoře v souladu se standardem ISO/IEC 17025 v aktuálním znění, případně jinou formu licencování laboratoře splňující požadavky uvedené v příloze B. Ta stanovuje v bodě B.3 podmínky pro licencování a akreditování laboratoře – primárně materiální podmínky ISO/IEC 17025, technickou vybavenost, nezávislost, nepodjatost a metodologickou a procesuální kompetentnost. Splnění těchto podmínek musí prokazovat hlavně certifikačnímu orgánu a k jeho spokojenosti. Podmínky pro výkon funkce samotné certifikační autority jsou uvedené v článku 5. Certifikační autorita musí být akreditována v souladu se standardem ISO/IEC 17065 v aktuálním znění,

[180] Viz TANTAWI, op. cit.

nebo obdobou splňující požadavky podle přílohy C. Zároveň k tomu, aby byly její certifikáty uznávány, musí vykonávat hodnocení nezávisle, přísně aplikovat CEM tam, kde to bude možné, a chránit utajované informace, které se při výkonu hodnocení dozvěděla. Příklady základních práv a povinností certifikačních orgánů jsou stanoveny v bodě B.2 přílohy – patří mezi ně možnost autorizovat účast testovací laboratoře na schématu (tedy že laboratoř může testovat produkty podle určitého schématu), dohled nad plněním podmínek pro výkon testování v laboratořích, vydávat podpůrné dokumenty k vydaným schématům, vydávat CC certifikáty nebo zprostředkovávat komunikaci mezi všemi zúčastněnými stranami.[181]

Celý organizační komplex je de facto doplněn i soukromými subjekty a spotřebiteli, neboť ti mohou definovat bezpečnostní požadavky na jednotlivé produkty (popsáno v dalším oddílu), proti kterým se pak produkty poměřují.

5.2.5 TOE, ST, PP A CERTIFIKAČNÍ SCHÉMA

Common Criteria operují ve své dokumentaci s mnoha pojmy, které je vhodné pro účely tohoto článku vysvětlit. Základním pojmem je TOE – „*Target of Evaluation*“, česky předmět posuzování. Může se jednat jak o softwarové, tak o hardwarové či firmwarové řešení. Na TOE jsou navázané pojmy PP a ST. PP je zkratkou pro „*Protection Profile*“ – profil ochrany, ST pro „*Security Target*“ – bezpečnostní cíl.[182]

Profily ochrany poskytují uživatelům možnost nadefinovat svá přání a požadavky na bezpečnost nevázaně na určitém produktu a jeho implementačním procesu (tedy se může jednat např. o bezpečnostní požadavky k blíže nespecifikovanému firewallu). Profil ochrany je tedy spíše šablonou pro skupinu produktů než konkrétním schématem, vyznačuje se obecností (tím se liší od ST) a může být použit opakovaně pro několik různých TOE. K tomu, aby mohl být PP používán jako základ pro

[181] Viz Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security [online]. 2. červenec 2014 [vid. 12. září 2018].

[182] Viz Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model [online]. Verze 3.1, páté vydání. B.m.: Common Criteria Management Committee, 2017 [vid. 12. září 2018].

ST, je nutné, aby sám prošel náležitým posouzením. Teprve PP, který je schválen, je zapsán do registru profilů ochrany a zveřejněn. Úplný profil ochrany může obsahovat následující kapitoly: úvod, popis TOE, definici bezpečnostního prostředí TOE (zasazení produktu do reálného světa a jaké relevantní hrozby mohou produktu hrozit), bezpečnostní cíle produktu a prostředí, bezpečnostní požadavky a zdůvodnění.[183]

Bezpečnostní cíle jsou oproti tomu definice, které vytvořili vývojáři, stanovující, jaké by měl mít produkt konkrétní bezpečnostní vlastnosti. Pravost těchto sdělení se pak bude při hodnocení testovat. Bezpečnostní cíle mohou být založené na jednom nebo i více profilech ochrany, aby vývojáři demonstrovali, že vyhověli přáním uživatelů. Jsou ovšem vázané na konkrétní produkt a implementaci bezpečnostních řešení. Pokud ST udá, že je založeno na více PP, musí dodržet požadavky všech těchto profilů. V rámci ST jsou definovány bezpečnostní rizika, problémy a zároveň i dílčí bezpečnostní cíle, kterých by měl hodnocený produkt dosáhnout. Oproti PP není v případě ST žádný registr, neboť se jedná o konkrétní, ve většině případů jednou použitelný set požadavků. I ST však musí projít posouzením a až prověřený může být použit k testování v samotném certifikačním procesu TOE.[184]

Posledním pojmem je hodnotící/certifikační schéma. Jedná se o regulatorní a administrativní rámec vytvořený na základě obecného modelu stanoveného v dokumentaci Common Criteria, podle kterého certifikační orgán hodnotí soulad s konkrétním druhem produktů. Může být výsledkem spojení uvedených PP a užívaných ST, zároveň se může jednat i o průmět určitých vnitrostátních regulatorních požadavků.[185]

Z výše uvedeného je patrné, že nová schémata mohou vzniknout v tomto systému na popud kohokoliv. Common Criteria se tak v teorii

[183] Viz tamtéž.

[184] Viz Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model [online]. Verze 3.1, páté vydání. B.m.: Common Criteria Management Committee, 2017 [vid. 12. září 2018].

[185] Viz Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model [online]. Verze 3.1, páté vydání. B.m.: Common Criteria Management Committee, 2017 [vid. 12. září 2018].

vyznačují neobyčejnou flexibilitou a otevřeností novým nápadům, technologiím a postupům.

5.2.6 PROCES CERTIFIKACE

Proces získání certifikátu Common Criteria zde bude popsán za pomoci dvou zdokumentovaných zkušeností s certifikačními procesy – v jednom případě certifikace chytré televize (LG SmartTV) na úroveň EAL 2,[186] v druhém případě certifikace distribuce operačního systému Linux.[187] Druhý případ ovšem zaznamenává zkušenosti ze získávání certifikátu ještě před velkou revizí dohody CCRA v roce 2015, která odklonila zaměření dohody od úrovní EAL a zároveň snížila obecně mezinárodně uznávaný stupeň záruky z EAL4 na EAL2, takže informací v této případové studii bylo využito jenom k doplnění informací z certifikačního procesu SmartTV. Překvapivé může být, že snížením vzájemného uznávání na úroveň EAL2 se zájem o certifikaci na vyšší úrovně snížil jen lehce,[188] a to přestože vyšší úrovně jsou nyní použitelné pouze pro vnitrostátní aplikaci.

Než celý proces započne, musí se vývojáři rozhodnout, na jakou úroveň je certifikace z hlediska potřebnosti a nákladovosti vhodná. Vývojáři LG SmartTV se rozhodli podstoupit proces certifikace na úroveň EAL 2. Prvním krokem je vypracování ST a dokumentace, která se na této úrovni neformálně posuzuje – manuál, design a popis TOE, zvláště pak jeho bezpečnostních funkcí. V případě chytré televize tedy byla popsána zejména architektura bezpečnostních řešení (např. instalace aplikací v režimu „*sand box*“) a dále rizika a jejich kontrování v celém procesu vývoje produktu. V případě bezpečnostní díry je nutné, aby došlo k odstranění vadné aplikace či kódu, a je třeba se ujistit, že zranitelnou oblast není možné obejít. Celý tento proces je vhodné zdokumentovat, aby

[186] Viz KANG, Sooyoung; KIM, Seungjoo. How to Obtain Common Criteria Certification of Smart TV for Home IoT Security and Reliability. *Symmetry* [online]. 2017, roč. 9, č. 10 [vid. 22. červenec 2018].

[187] Viz RECCHIA, Luca et al. Security Evaluation of a Linux System: Common Criteria EAL4 + Certification Experience. In: *2014 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)* [online]. Naples, Italy: IEEE, 2014 [vid. 22. červenec 2018].

[188] Viz https://www.commoncriteriaportal.org/products/stats/.

mohla být dostatečnost bezpečnostních protiopatření otestována i při certifikačním procesu.

V rámci ST je potřeba správně nadefinovat relevantní požadavky na funkčnost zabezpečení (SFR) z části druhé CC a popsat způsoby jejich naplnění a přijatá opatření (např. správa přístupu k informacím). To samé je nutné i u požadavků na spolehlivost (SAR) podle části třetí. Hotové ST tak obsahuje definici TOE pomocí SFR, SAR, bezpečnostních rizik a hrozeb, dílčích bezpečnostních úkolů, cílů a funkcí (obvykle ve formě nejrůznějších analýz mapujících chování produktu v rizikových situacích). Je důležité dbát o to, aby se TOE v průběhu vývoje od ST neodklonil, jinak je potřeba aktualizovat ST.

V případě, že existuje PP, je vhodné se alespoň pokusit ho zahrnout do bezpečnostního cíle. Pro chytrou televizi ovšem žádný zveřejněný oficiální PP neexistoval, tudíž ST byl v tomto případě vytvořen na základě analogických PP. Vývojáři při tvorbě ST zároveň připisují jednotlivým aktivům produktu různou důležitost a tím pádem i míru ochrany (k určení hodnoty aktiva slouží právě PP).

Jakmile je ST (i produkt samotný) hotový, přichází fáze testování. V případě nových technologií bývá problematické najít laboratoř schopnou testování[189], referenční materiály či testovací metody a nástroje. Ty musí vývojáři v takovém případě vyhledat a referenční materiály a testy případně sestavit. Pro zmíněnou chytrou televizi, protože na úroveň EAL2 musela projít i praktickým testováním, vytvořili vývojáři na základě žádosti certifikační autority 4 druhy testů: funkční testování (testuje, zda specifikované funkce pracují a pracují dobře a v souladu s bezpečnostními požadavky), testování zranitelností (testuje odolnost proti již známým hrozbám a slabinám), penetrační testování (testovací hackerské pokusy o převzetí vlády nad zařízením) a „*fuzz*“ testování (testující schopnost vypořádat se s chybovou hláškou na vstupu, čímž se testují zbylé zranitelnosti). Certifikační autorita si pak sama vybere, který typ testování bude proveden.

[189] Informace o licencovaných laboratořích je možné najít mimo jiné zde: https://www.commoncriteriaportal.org/labs/.

Pokud je certifikace produktu první svého druhu (tedy dosud nebylo testováno nic ani ze skupiny podobných produktů), musí certifikační orgán provést speciální verifikační proces ohledně schopnosti certifikovat. V jeho procesu si musí hodnotitel obstarat certifikát osvědčující, že je schopen certifikaci provést, a dále sehnat potřebné případové („*hacking*“)[190] studie, seznamy známých zranitelností, hodnotící metody atp. S mnohým mohou pomoci vývojáři samotní, proto se při nedostatku referenčních materiálů a postupů může stát, že hodnotitel požádá vývojáře produktu, aby takové materiály a testy vyvinul. Tento verifikační proces protáhl čekací dobu u certifikace chytré televize o 1,5 měsíce, tzn. 1,5 měsíce se čekalo, než se vůbec započne s testováním samotným. Pokud je produkt a ST komplexnějšího rázu, je pravděpodobné, že verifikační proces zabere ještě delší dobu.

Poté, co vývojáři naleznou a kontaktují testu-schopnou testovací laboratoř a odpovídající certifikační autoritu, případně skončí verifikační proces u certifikační autority, může započít testování samotné (v souladu s pravidly stanovenými v CEM). Testování je řízeno certifikační autoritou a prováděno testovací laboratoří. TOE se testuje podle specifik daných v ST a podpůrné dokumentaci (např. manuál) – nejdřív je prozkoumána dokumentace, design a funkce TOE a podle výsledků z tohoto průzkumu je následně předepsáno, jakým způsobem, co a v jakém prostředí bude testováno. Vývojáři v případu chytré televize podotýkali, že u společnosti, která poprvé absolvuje certifikační proces, je nepřítomnost bezpečnostního inženýra, který by dohlížel na rychlou implementaci bezpečnostních řešení, značně zdržující (navíc mnohé společnosti nemají dostatečné kapacity ani zdroje, aby jeho přítomnost materiálně nahradily). Tento problém se však projeví jen v případě, kdy není TOE nebo ST dostatečně důkladně a detailně připraveno a při certifikačním procesu se projeví neočekávaná situace nebo chyba, kterou je zapotřebí rychle odstranit.

[190] Tyty případové studie jsou často zdokumentovaným postupem penetračního testování, popisují tedy způsob provádění testu a to, jak využít známých zranitelností z podobných případů.

Jakmile je testování dokončeno, podá testovací laboratoř report certifikační autoritě, která na jeho základě (v případě, že je report pozitivní) vydá pro produkt certifikát, TOE zařadí do registru a certifikát zveřejní.[191]

5.2.7 MEZINÁRODNÍ UZNÁVÁNÍ CERTIFIKÁTŮ

Mezinárodní a vzájemné uznávání certifikátů je zaručeno primárně na základě dohody CCRA, která nyní zajišťuje automatické vzájemné uznávání jen do úrovně EAL2 (ve specifických případech do EAL4). Původně bylo zajištěno uznávání do úrovně EAL4 (a ve specifických oblastech až do úrovně EAL7). Omezení na úroveň 4 bylo způsobeno rozsahem CEM, který sahal právě jenom do čtvrté úrovně. Vyšší úrovně již neměly upravenou metodiku testování (kvůli komplexní povaze přísnějších testů bylo vytvoření takové úpravy přinejmenším velice nesnadné), a tím pádem neměly ostatní členské státy dohody CCRA záruku, že testování bude probíhat zodpovědně a podle jednotného klíče, který by mohl vytvářet důvěru ve výsledek. Přestože je nyní uznávání omezeno jenom do úrovně 2, jedná se o uznávání automatické a nositelé certifikátu tak nemusí podstupovat žádné další řízení o uznání.[192]

Dohoda SOG-IS MRA byla v tomto článku již představena. Zajišťuje uznávání certifikátů až do úrovně čtvrté, případně sedmé ve specifických technických oblastech.[193] Toto sdružení není sjednoceno jenom vzájemným uznáváním, ale úzce spolupracuje i na vytváření nových schémat a PP.[194] Stejně jako CCRA i SOG-IS MRA má dvě formy členství – země produkující certifikáty a země certifikáty akceptující. Pro připomenutí – ČR není

[191] Pro představu o počtech certifikovaných produktů viz https://www.commoncriteriaportal.org/products/stats/.

[192] Viz Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security - Ratifikováno 8. 9. 2014 [online]. 2014 [vid. 12. září 2018].

[193] To byl i jeden z důvodů, proč byl SOG-IS vytvořen – mělo dojít k limitaci vzájemného uznávání certifikátů na vyšších bezpečnostních úrovních na technické oblasti, kde je již nadefinována metodologie, požadavky na laboratoře a na testování samotné.

[194] Impulzem ke stvoření nového schématu je často moment, kdy Evropská komise vydá směrnici týkající se IT bezpečnosti, která by měla být vnitrostátně implementována určitým (nejlépe jednotným) způsobem.

členem této dohody a ani nemá na členství zájem. Slovensko oproti tomu je jedním ze států uznávajících certifikáty (a 17. září 2019 se stalo i konzumujícím členem dohody CCRA).[195]

5.2.8 SLABINY A NEVÝHODY SYSTÉMU COMMON CRITERIA

Jedna z největších slabin CC je závislost na mezistátní důvěře. Tato závislost bohužel není ze strany CC ani CCRA odstranitelná, je neochvějně spojená se spoluprací v oblasti bezpečnosti, neboť v takových chvílích sice samy sobě poskytují členské státy výhody a informace, ale zároveň poskytují informace o zabezpečení vlastní infrastruktury dalším státům. A to je potenciálně zneužitelné. V ideálním světě by důvěra samozřejmě mohla fungovat bez problémů i bez regionálních uskupení, jako je Evropská unie, ale realita je bohužel jiná a ani Unie není nedůvěry prosta. Princip fungování CC je založen na idealistické vizi, která rozevřela nůžky mezi právně-technickým vnímáním světa a jeho skutečným politickým fungováním. Vzájemné uznávání tak funguje bez problémů jen mezi spojenci, kdežto mezi potenciálními nepřáteli takové uznávání nikdy naplno fungovat nebude, resp. bude sloužit jako třecí plocha. Common Criteria vznikala v období po pádu SSSR, které se vyznačovalo umírněním celé mezinárodní situace a vzrůstající spoluprací mezi státy. To období však skončilo. Kvůli nedostatku vzájemné důvěry tak širší implementace systému Common Criteria patrně svědky nebudeme, přestože se stále ještě jedná o „*state of the art*“ světa certifikace kyberbezpečnostních technologií.[196]

Common Criteria se potýkají i s dalšími problémy, které jsou alespoň částečně mimo dosah samotných kritérií. Jedná se o hrubě neaktuální profily ochrany a další schémata, kdy některá PP, stále ještě v užívání, pocházejí z roku 1999. To způsobuje odtržení požadavků na bezpečnost od reálného světa a staví vývojáře do nelehkých pozic, ze kterých často uniknou rezignací na certifikaci. Zároveň se CC minula s plánovaným

[195] Viz SOG-IS - Home. *SOG-IS* [online]. [vid. 12. říjen 2019]. Získáno z: http://sogis.org/index_en.html; SOG-IS - Status of participants. *SOG-IS* [online]. [vid. 25. prosinec 2018]. Získáno z: http://sogis.org/uk/status_participant_en.html.

[196] Viz KALLBERG, Jan. The Common Criteria Meets Realpolitik: Trust, Alliances, and Potential Betrayal. *IEEE Security & Privacy Magazine* [online]. 2012, roč. 10, č. 4, s. 50–52 [vid. 22. říjen 2018].

účinkem na trh. Většina certifikátů je vystavována pro produkty ve vládním nebo vojenském sektoru, co se ovšem týká soukromého – zde je výskyt minimální. To snižuje zapojení subjektů průmyslových odvětví a soukromého výzkumu do inovací schémat pod CC, a tak snižují relevanci CC v čase. CC tak nedokáží reagovat na chyby, případně na zranitelnosti přicházejí moc pozdě. Efektivita certifikace tím značně trpí.[197]

Problémem, který byl již v tomto článku rozebrán a který vychází z kritérií samotných, je nevhodnost tohoto systému pro hodnocení TOE, jako jsou big data, cloudové služby a služby celkově, o čemž vypovídá i počet certifikovaných služeb (0, viz výše). Zároveň další velkou slabinou tohoto systému je délka a nákladnost certifikačního procesu. Zvláště při certifikaci nových produktů je tento proces dlouhý až 12 měsíců a značně nákladný, což je naprosto tristní, zvláště u nižších úrovní EAL, a k zajištění funkčnosti certifikovaných produktů hrubě nedostatečné. Common Criteria mají značný problém i s údržbou certifikátu (trvanlivost má 5 let, pak je nutné ho obnovit) a aktualizačním procesem certifikovaných produktů (certifikát se pojí jen k určité verzi produktu). To mimo jiné vedlo ze strany nespokojených členských států k zakládání vlastních certifikačních řešení soustředících se na limitaci času a zdrojů potřebných k provedení certifikace a zároveň na vyřešení slabiny certifikátů v evolučním cyklu produktů.[198,199]

Poslední velkou slabinou ukrytou přímo v dokumentech CC je vnitřní rozpornost. Metodologie si s touto vnitřní rozporností povětšinou neumí poradit a v mnohých případech ji neumí ani zjistit. Jedná se o skutečnost, že CC sice vývojářům produktu mnohdy stanoví při implementaci prvku A povinnost zavést i prvek B, ovšem v celém systému se neřeší, že při zavedení prvku X se již nesmí zavést prvek Y. Systém tak vůbec nemapuje vztahy, kdy se jednotlivé prvky mohou kontrovat až do absolutní neúčinnosti. Tento problém je zvlášť patrný, jakmile je potřeba zaručit jak anonymitu, tak přezkoumatelnost v rámci daného produktu (např. online

[197] Viz HEARN, op. cit., s. 64–65; ISA et al, op. cit.; KALLBERG, op. cit., s. 50-52.

[198] Viz KALLBERG, op. cit., s. 52.

[199] Srov. ISA et al, op. cit.

volby). Požadavek anonymity zabraňuje užití dostatečných nástrojů na zajištění přezkoumatelnosti a požadavek přezkoumatelnosti zároveň vylučuje možnost efektivního zaručení anonymity.[200]

6. AKTUÁLNÍ CERTIFIKAČNÍ ŘEŠENÍ – VYBRANÉ EVROPSKÉ STÁTY

V oboru certifikace kyberbezpečnostních technologií v Evropské unii vyčnívají nad ostatními čtyři státy, které za absence unifikovaného evropského řešení (a částečně i kvůli nespokojenosti se systémem Common Criteria) vytvořily vlastní úpravu, většinou pro nižší úrovně bezpečnostní záruky. Jsou jimi Velká Británie (až do Brexitu stále součástí EU), Francie, Německo a Nizozemí. V této kapitole budou stručně představeny jejich národní modely certifikace, které společně se systémem Common Criteria inspirovaly podobu nové jednotné evropské certifikace a které po jejím příchodu postupně zaniknou. Bude tak zodpovědností celého budoucího evropského certifikačního aparátu, aby nedošlo k zániku kvalitních a trhem žádaných certifikačních schémat. To by paradoxně vedlo ke stavu opačnému, než o jaký Akt o kybernetické bezpečnosti usiluje – ke snížení kybernetické bezpečnosti v některých státech. Kromě čtyř výše zmíněných států významně pracují na vlastní regulaci této materie i Itálie, Švédsko a Norsko (přestože není členem Evropské unie, je členem uskupení SOG-IS).

6.1 VELKÁ BRITÁNIE

Velká Británie spustila na začátku roku 2011 národní certifikační schéma pojmenované „*Commercial Product Assurance*“ (dále jen jako „CPA“) pro komerční kyberbezpečnostní produkty prodávané ve VB. Je určené pro produkty (nikoliv služby) pracující v méně rizikovém prostředí, které však musí vykonávat určitou zabezpečovací funkci (např. firewall nebo šifrování). Produkty jsou pak v tzv. „*CPA testovacích laboratořích*“ testovány proti požadavkům stanoveným v předem publikovaných bezpečnostních standardech (tzv. „*Security Characteristics*“, dále také jako „SC“), které

[200] Viz MERCURI, Rebecca. Uncommon criteria. *Communications of the ACM* [online]. 2002, roč. 45, č. 1, s. 172 [vid. 22. říjen 2018].

vydává Národní centrum kybernetické bezpečnosti („*National Cyber Security Centre*“).[201]

SC jsou dokumenty, které definují, jaké předpoklady musí produkt splňovat. Vzhledem k tomu, že není možné certifikovat produkt, pro který neexistuje SC, je patrné, že toto certifikační schéma je podstatně rigidnější než Common Criteria. Bezpečnostní standardy jsou rozděleny do 11 kategorií – vyskytuje se zde např. kategorie pro VPN, pro zabezpečení komunikace v reálném čase nebo pro firewall.[202]

V případě, že produkt v testech obstojí, je mu udělen certifikát „*Foundation Grade*“, který potvrzuje, že takto ohodnocený produkt je v souladu s dobrou obchodní bezpečnostní praxí. Spotřebitel je tak ujištěn, že produkt bude plnit to, co výrobce slíbil (v definovaném prostředí). Tento certifikát může být získán v určitých případech i pomocí certifikace v systému Common Criteria (pokud je produkt certifikován podle CC, může získat i „*Foundation Grade*“, systémy nejsou prostupné opačným směrem).[203] Certifikát ze schématu CPA drželo ke dni 12. 10. 2019 celkem 233 kyberbezpečnostních technologií a dalších 9 bylo posuzováno (oproti 25. 12. 2018, kdy bylo certifikováno toliko 35 kyberbezpečnostních produktů, přičemž dalších 8 bylo posuzováno).[204]

V případě, že si výrobce chce nechat svůj produkt certifikovat podle schématu CPA, musí se nejdříve ujistit, že jeho produkt je vůbec způsobilý k certifikaci (ICT produkt s aktivně zabezpečovací funkcí) a že je certifikace předpokládána, tedy, že existuje oficiální bezpečnostní standard, pod který je možné produkt podřadit. Tento standard si musí výrobce zvolit. Poté kontaktuje určitou testovací laboratoř a odešle jí specifika produktu, aby zjistil její faktické možnosti určitý výrobek otestovat. V případě, že

[201] Viz Commercial Product Assurance (CPA). *NCSC Site* [online]. [vid. 25. prosinec 2018]. Získáno z: https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa.

[202] Viz Security Characteristics collection. *NCSC Site* [online]. [vid. 28. prosinec 2018]. Získáno z: https://www.ncsc.gov.uk/document/security-characteristics-collection.

[203] Viz Commercial Product Assurance (CPA). *NCSC Site* [online]. [vid. 25. prosinec 2018]. Získáno z: https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa.

[204] Viz Certified Products. *NCSC Site* [online]. [vid. 12. říjen 2019]. Získáno z: https://www.ncsc.gov.uk/index/certified-product?f[0] = field_assurance_scheme %3A226&f[1] = field_assurance_status%3AAssured.

laboratoř shledá svoji vlastní schopnost otestování, pošle doporučující stanovisko k Národnímu centru kybernetické bezpečnosti, které následně vyhodnotí, jestli je produkt skutečně možné otestovat podle daného standardu SC. V případě kladného výsledku může pak testovací laboratoř produkt otestovat, z čehož vzejde zpráva o průběhu testu, která je opět poslána Národnímu centru kybernetické bezpečnosti. Pokud byl test úspěšný, Národní centrum kybernetické bezpečnosti udělí certifikát „*Foundation Grade*" a zpřístupní produkt veřejnosti na webových stránkách.[205] Kromě nákladů testovacích laboratoří, které musí výrobce pokrýt, si i Národní centrum kybernetické bezpečnosti účtuje 4 690 liber (certifikát podle CC je ohodnocen stejně).[206]

Oproti CC má toto certifikační schéma jednu velikou výhodu – umožňuje bezpečnostní evoluci produktu, takže se certifikát nevztahuje pouze k jedné verzi produktu, ale k celému životnímu procesu. To, že bezpečnostní aktualizace nesnižují celkovou úroveň zabezpečení produktu, hlídá Národní centrum kybernetické bezpečnosti. Certifikát CPA je platný pouze dva roky a poté je nutné ho obnovit.[207]

Nevýhodou oproti Common Criteria je již výše zmíněná rigidita a možnost použití ve většině případů pouze na území Velké Británie. Držitel certifikátu „*Foundation Grade*" však může požádat, aby jeho produkt byl zapsán do katalogů bezpečných produktů, které vede NATO i EU.[208] NATO plně respektuje záruku poskytnutou britským Národním centrem kybernetické bezpečnosti, Evropská unie však provádí sekundární posouzení jedním ze šesti (ve skutečnosti pěti, protože Velká Británie nemůže hodnotit svůj vlastní produkt) tzv. AQUA („*Appropriately Qualified*

[205] Viz Foundation Grade explained. *NCSC Site* [online]. [vid. 25. prosinec 2018]. Získáno z: https://www.ncsc.gov.uk/articles/foundation-grade-explained.

[206] Viz Products and Services Scheme fees. *NCSC Site* [online]. [vid. 25. prosinec 2018]. Získáno z: https://www.ncsc.gov.uk/articles/products-and-services-scheme-fees.

[207] Viz Foundation Grade explained. *NCSC Site* [online]. [vid. 25. prosinec 2018]. Získáno z: https://www.ncsc.gov.uk/articles/foundation-grade-explained.

[208] Viz Commercial Product Assurance (CPA). *NCSC Site* [online]. [vid. 25. prosinec 2018]. Získáno z: https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa.

Authorities“) – orgány situované ve Švédsku, Nizozemí, Itálii, Německu, Francii a Velké Británii.[209]

6.2 FRANCIE

Francie již po delší dobu není spokojená s kyberbezpečností certifikací prováděnou v režimu Common Criteria. Francouzi nejsou spokojeni s cenou ani s délkou testování, které jsou i u nejnižší bezpečnostní úrovně mnohdy mimo dosah malých a středních podniků (a stejně tak mimo zájem velkých).[210] Zároveň (alespoň podle neveřejných zdrojů) by se chtěli vyhnout tomu, aby museli data o svých kyberbezpečnostních produktech nadále zpřístupňovat Spojeným státům americkým, jak je tomu u systému Common Criteria. To je jedna z možných motivací, které směřovaly k vytvoření jednotného evropského certifikačního systému. Doba a cena CC certifikace pak byly motivací k vytvoření schématu „*Certification Sécuritaure de Premier Niveau*“ (dále jen jako „CSPN“), a to už v roce 2008. Tento systém je opět národním schématem a aplikuje se tak pouze na území Francie bez možnosti vzájemného uznávání. Pokud ovšem podnikatel (z jakékoliv země) chce dodávat francouzské vládě zařízení přístupná přes internet (např. webkamera), je tento certifikát stanoven jako minimální bezpečnostní požadavek.[211]

CSPN má obdobný záběr a rozsah jako Common Criteria a nabízí tak podobnou úroveň důvěryhodnosti certifikačního procesu, jenž je představován tradičním modelem (nezávislý subjekt – testovací laboratoř hodnotí, jestli produkt nebo systém splňuje bezpečnostní požadavky tak, jak je výrobce nadefinoval → obdoba Security Target u Common Criteria). CSPN se ovšem poučilo z chyb ostatních certifikačních modelů a nabízí tak značně urychlený proces testování ve lhůtě 8 týdnů. Tento systém se také

[209] Pro více informací viz https://www.ncsc.gov.uk/content/files/scheme_downloads/nato_eu_process_flow_chart.pdf.

[210] Viz Certification CSPN. *ANSSI* [online]. [vid. 25. prosinec 2018]. Získáno z: https://ssi.gouv.fr/administration/produits-certifies/cspn/.

[211] Viz CSPN: What U.S. companies need to know about the security certification process [online]. [vid. 25. prosinec 2018]. Získáno z: http://www.embedded-computing.com/embedded-computing-design/cspn-what-u-s-companies-need-to-know-about-the-security-certification-process.

vypořádal s bezpečnostní evolucí produktu (ovšem trochu robustnějším způsobem než ve Velké Británii). Na nové verze systému/produktu se certifikát sice vztahovat nutně nemusí, ale systém CSPN pak umožňuje dodatečné kontinuální certifikační procesy za sníženou cenu.[212]

CSPN je zaštítěn organizací „*Agence nationale de la sécurité des systémes d'information*" (dále jen jako „ANSSI"). Ta akredituje testovací laboratoře podle úrovně technického vybavení, tedy podle toho, co ještě mohou funkčně certifikovat, a určí jim rozsah produktů, které mohou platně certifikovat. ANSSI produkuje, stejně jako v britské verzi Národní centrum kybernetické bezpečnosti, bezpečnostní standardy a hodnotící kritéria, která opět tím pádem nemohou být tak jednoduše vytvářena, jak je tomu u Common Criterií. Proces certifikace je též totožný s britskou variantou, ovšem s tím rozdílem, že výrobce či obecně žadatel musí v dokumentaci (Security Target) k produktu nadefinovat též prostředí, ve kterém se bude produkt či systém používat.[213] V případě nejasností ohledně certifikovatelnosti produktu může žadatel kontaktovat ANSSI, které mu případně pomůže i s nalezením správné testovací laboratoře. Pokud bude překročena lhůta 8 týdnů k dokončení certifikace, může ANSSI certifikaci ukončit. Aby tomuto žadatel předešel, může navrhnout upravení časového plánu testovací laboratoři, aby bylo testování co možná nejefektivnější. Po skončení certifikačního procesu, v případě pozitivního výstupu, vyplní ANSSI certifikační zprávu, ve které ohodnotí, jak odolný je produkt vůči hrozbám. Tuto zprávu pak pošle žadateli a zveřejní ji na svých internetových stránkách, pokud k tomu žadatel dá souhlas.[214]

[212] Viz Certification CSPN. *ANSSI* [online]. [vid. 25. prosinec 2018]. Získáno z: https://ssi.gouv.fr/administration/produits-certifies/cspn/.

[213] Jedná se tak o konkrétnější záběr oproti britské variantě, která bez dalšího počítá s obecným, ale málo rizikovým prostředím. Tento model byl pravděpodobně zvolen kvůli časové limitaci francouzského testování a tedy snaze na limitaci rozsahu testování.

[214] Viz Certification CSPN. *ANSSI* [online]. [vid. 25. prosinec 2018]. Získáno z: https://ssi.gouv.fr/administration/produits-certifies/cspn/; CSPN: What U.S. companies need to know about the security certification process [online]. [vid. 25. prosinec 2018]. Získáno z: http://www.embedded-computing.com/embedded-computing-design/cspn-what-u-s-companies-need-to-know-about-the-security-certification-process

ANSSI na svých stránkách varuje spotřebitele, že udělený certifikát ještě neznamená, že produkt je nezranitelný (což osobně považuji za krok správným směrem). Zájem o tento typ certifikátu byl v roce 2019 přibližně srovnatelný s certifikačním systémem ve Velké Británii. Ke dni 1. června 2019 vstoupilo do hodnotícího procesu celkem 320 produktů, z nichž certifikát obdrželo 141.[215]

6.3 NIZOZEMÍ

Nizozemí se k národní regulaci kyberbezpečnostní certifikace přidalo oproti Francii a Velké Británii až relativně nedávno. Pilotní fáze projektu „*Baseline Security Product Assessment*" (dále jen jako „BSPA") byla spuštěna v roce 2015, přičemž plně funkční je až od roku 2017. Certifikační schéma BSPA je spravováno nizozemskou Národní agenturou pro bezpečnost komunikací („*Nationaal Bureau voor Verbindingsbeveiliging*", dále jen jako „NLCSA"), což je orgán kybernetické obrany spadající pod nizozemskou informační a bezpečnostní službu (obdoba naší BIS). Stejně jako francouzská úprava i BSPA nabízí možnost nezávislého posouzení souladu produktu s výrobcem proklamovanými bezpečnostními požadavky (Security Target) v omezeném čase a s omezenými náklady. Ve skutečnosti byl BSPA francouzskou úpravou notně inspirován. Poptávka po této certifikační službě rychle roste, a to zejména kvůli tomu, že společnosti podnikající v nizozemském vládním sektoru musí být v souladu se standardem definovaným v „*Baseline Informatiebeveiliging Rijksdienst*" (jednoduše BIR:2017). Certifikace podle BSPA jim tak podnikání ve vládním sektoru značně zjednodušuje, neboť byla stvořena mimo jiné pro soulad s BIR:2017.[216]

Stejně jako francouzské schéma se i BSPA soustředí na hardwarová i softwarová řešení, která mají ochránit citlivé (ale ne tajné) údaje. I zde je patrné, že se jedná o řešení nabízející nižší bezpečnostní úroveň těm, pro které jsou vyšší bezpečnostní kategorie podle CC zbytečné. Obdobně jako francouzská úprava i BSPA počítá s certifikačním procesem v maximální

[215] Viz Les produits CSPN. *ANSSI* [online]. [vid. 12. říjen 2019]. Získáno z: https://ssi.gouv.fr/administration/produits-certifies/cspn/produits-certifies-cspn/.

[216] Viz Baseline Security Product Assessment. *SECURA* [online]. [vid. 25. prosinec 2018]. Získáno z: https://www.secura.com/pathtoimg.php?id=1326&image=bspa.pdf.

délce 25 člověkodnů, v případě systému zahrnujícího kryptografické řešení maximálně 35 člověkodnů. K tomu, aby bylo tohoto cíle dosaženo, se pracuje toliko s nainstalovaným, pracujícím prototypem a úplnou dokumentací. Samotný certifikační proces je prováděn testovacími laboratořemi, nad kterými vykonává dohled NLCSA.[217]

Security Target, který je v tomto modelu označován jako „*Security Evaluation Target*" (dále jen SET), musí opět obsahovat nejen specifikaci produktu a jeho tvrzených bezpečnostních vlastností, ale zároveň i prostředí, ve kterém bude produkt používán a kým bude používán, stejně tak jako stanovení relevantních hrozeb a následných protiopatření, jejichž spolehlivost má být testována.[218] Testovací laboratoř se tak nesoustředí na situace, které pro produkt nejsou relevantní. Explicitně jsou otestovány právě ty, které nadefinuje samotný žadatel. BSPA obsahuje 8 kategorií kyberbezpečnostních produktů (např. řešení v kategorii bezpečnost sítí = VPN, v kategorii bezpečnost souborů = šifrování složek).[219]

Testovací laboratoře netestují pouze to, jestli produkt odpovídá vlastnostem nadefinovaným v SET, ale zároveň hodnotí i efektivitu použitých bezpečnostních řešení (jestli efektivně brání proti útočníkům s nízkým a středním útočným potenciálem) a nakonec i celkový účinek produktu na cílový systém (tedy jestli není firewall tak účinný, že znemožní jakékoliv připojení k internetu). Výstupem z certifikačního procesu je tzv. „*Evaluation Technical Report*" a dokument určený spotřebitelům a zákazníkům, ve kterém je po schválení výstupní dokumentace NLCSA obsaženo oficiální Prohlášení o shodě (Statement of Conformity). Toto Prohlášení informuje o souladu produktu s tvrzenými bezpečnostními vlastnostmi a požadavky a zároveň o souladu s BIR:2017.[220]

[217] Viz Baseline Security Product Assessment [online]. B.m.: SECURA. [vid. 25. prosinec 2018]

[218] Viz Baseline Security Product Assessment. In: *BlackHat Sessions* [online]. Nieuwegein, Nizozemí. 14. červen 2018 [vid. 25. prosinec 2018].

[219] Viz Baseline Security Product Assessment. *SECURA* [online]. [vid. 25. prosinec 2018]. Získáno z: https://www.secura.com/pathtoimg.php?id=1326&image=bspa.pdf.

[220] Viz tamtéž.

6.4 NĚMECKO

Poněkud zvláštní úpravu má v tomto ohledu Německo. Spolkový úřad pro informační bezpečnost (BSI) je podle zákona o BSI oprávněn provádět certifikaci kyberbezpečnostních technologií a vydávat tak tzv. Německý certifikát. Schémata se však řídí podmínkami, postupy a kritérii, která jsou zavedena v systému Common Criteria a která jsou nezbytná pro mezinárodní uznávání, ať už v režimu CCRA nebo SOGIS-MRA. BSI totiž tento systém oficiálně na Common Criteria založilo, jedná se toliko o jeho modifikovanou verzi, kdy jsou využívány např. i profily ochrany z původního systému CC. Oproti ostatním, výše zmíněným, řešením se tedy nejedná o čistě národní certifikační systém. Ohledně uznávání Německého certifikátu BSI podepsalo dohodu o uznávání certifikátů vydaných v rámci SOGIS-MRA a přistoupilo i na celosvětovou dohodu o uznávání certifikátů vydaných v rámci Common Criterií – CCRA.[221]

Německo si tak uchovalo větší dohled nad testovacími laboratořemi (v Německu je jich devět) a ve speciálních případech i produkty (může odmítnout certifikát udělit nebo uznat z důvodu veřejného zájmu). Německá vláda může vyvíjet speciální standardy a iniciativy jak na národní, tak i na evropské úrovni. Zachovala si tak několik výhod národního řešení, aniž by obětovala mezinárodní možnost uznávání certifikátů. O Německý certifikát je veliký zájem – udává se, že je uděleno více než 100 certifikátů ročně (přičemž okolo 75 % na vysokou úroveň bezpečnostní záruky).[222]

---

[221] Viz Technical information on the IT security certification of products, protection profiles and sites - BSI 7138 [online]. Bonn, Německo: Bundesamt für Sicherheit in der Informationstechnik, 2012 [vid. 12. říjen 2019].

[222] Viz BSI – Certification. *Bundesamt für Sicherheit in der Informationstechnik* [online] b.n. nedatováno [vid. 12. říjen 2019]. Získáno z: https://www.bsi.bund.de/EN/Topics/Certification/certification_node.html; *Technical information on the IT security certification of products, protection profiles and sites – BSI 7138* [online]. Bonn, Německo: Bundesamt für Sicherheit in der Informationstechnik, 2012 [vid. 12. říjen 2019]; WEBER, Joachim. *The German IT Security Certification Scheme* [online]. Bonn, Německo: Bundesamt für Sicherheit in der Informationstechnik, 2017 [vid. 28. prosinec 2018].

6.5 SPOLEČNÉ VYHODNOCENÍ NÁRODNÍCH SCHÉMAT

Právě popsaná schémata obsahují určité prvky, které mezi sebou sdílejí. Z těchto prvků je možné vyvodit, jaké aspekty státům nevyhovovaly na stávajícím systému Common Criteria až do té míry, že přistoupily k vytvoření vlastních certifikačních schémat.

V první řadě je to délka certifikačního procesu a výše nákladů. To je patrné z toho, že národní schémata obsahují limitaci obou těchto prvků. Důkladný a finančně náročný certifikační proces je jistě pochopitelný a omluvitelný v případě vysokých úrovní zabezpečení a rizikovosti prostředí, ale z úpravy schémat, které jsou naformulované zejména pro málo rizikové prostředí, vyplývá, že veliká poptávka je právě po nižších bezpečnostních úrovních, které jsou určené pro „*běžné*“ situace. A na těch je skutečně systém Common Criteria až zbytečně náročný.

Za druhé je to vnitrostátní dohled a moc nad certifikací. Tyto aspekty jsou patrné ve všech zmíněných schématech, přičemž nejvíce pravděpodobně v Německém certifikátu, který modifikoval systém CC mimo jiné právě tím, že do něj vložil možnost odmítnout certifikaci nebo certifikát pro rozpor s veřejným pořádkem nebo kvůli ohrožení bezpečnosti. K tomuto problému se přidává i politické napětí a vzájemná nedůvěra mezi členy CCRA, jak bylo napsáno v podkapitole věnující se francouzskému schématu. Státy se vcelku pochopitelně nechtějí vzdát moci nad svojí vlastní bezpečností a modifikovat chyby certifikačního systému pouze po dohodě s dalšími členy se ukázalo pro některé z nich jako příliš iritující.

Za třetí je to zvládání evoluce produktu nebo služby. Toto jsem zmiňoval i v podkapitole věnující se přímo slabinám systému CC. Většina těchto schémat přišla s vlastní variantou, jak tuto slabinu odstranit – jedná se tak o další ze silných příspěvků směrem ke konstrukci Aktu o kybernetické bezpečnosti.

Posledním přínosem, který je viditelný hlavně v případě nizozemského schématu, je hodnocení účinků bezpečnostního produktu v rámci informačního systému. I to totiž odpovídá na jednu ze slabin CC, neboť ty

jsou často zaměřené až přespříliš konkrétně a ignorují celistvý obraz bezpečnostní situace.

Na závěr si dovolím ještě podotknout jednu zajímavost, které jsem si všiml u všech schémat. Úloha akreditačního orgánu, který povoluje provoz laboratoří a CAB, je v těchto schématech přidělena vždy národní verzi úřadu pro kybernetickou bezpečnost, nikoliv národní akreditační autoritě, jako je tomu v případě Common Criterií. Tuto skutečnost si vysvětluji buď touhou států vyhnout se byrokratizaci procesu zavlečením dalšího orgánu, nebo touhou po vyšší odbornosti celého procesu. Úřad pro kybernetickou bezpečnost v postavení akreditačního orgánu je sám plně odborně způsobilý posoudit naplnění kritérií, a dokonce si troufám říct, že možná i více než akreditační orgán samostatný oddělený. To usuzuji zejména z hypotetického porovnání personálních kapacit orgánu, který se zabývá pouze kyberbezpečnostní tématikou, a orgánu, který se zabývá akreditací na daleko širším poli. Tím pádem bych se v případě druhého orgánu nedivil, kdyby bylo posuzování splněných podmínek bližší spíše formálnímu pohledu. Akt o kybernetické bezpečnosti se ovšem vydal jinou cestou, jak je popsáno v následující kapitole.

7. CERTIFIKACE PODLE AKTU O KYBERNETICKÉ BEZPEČNOSTI

V této kapitole bude kriticky rozebrána institucionální, organizační i procesní stránka certifikace podle Aktu o kybernetické bezpečnosti,[223] a kde to bude vhodné, bude provedeno i srovnání s nařízením eIDAS. Na konci kapitoly ještě stručně zrekapituluji pozitiva, která Akt do certifikace kyberbezpečnostních technologií přinese.

7.1 CÍLE CERTIFIKACE A BEZPEČNOSTNÍ CÍLE SCHÉMAT

Certifikace prováděná podle Aktu by měla směřovat ke zvýšení důvěry v kybernetickou bezpečnost ICT produktů, a to prostřednictvím osvědčení, že produkty byly důsledně prověřeny a splňují určité bezpečnostní

[223] Kdykoliv je v článku zmíněn „Akt“ bez dalšího, je tím myšlena finální verze Aktu o kybernetické bezpečnosti. Zároveň kdekoliv, kde v této kapitole budu pojednávat o produktech, jsou tím myšleny i služby a procesy, jejichž certifikaci Akt upravuje také.

požadavky. Ty jsou obsaženy v certifikačních schématech a směřují k ochraně důvěrnosti, dostupnosti, autenticity a integrity dat. Certifikace ovšem neznamená, že je otestovaný produkt naprosto bezpečný, a Akt na to sám upozorňuje v bodě 77 odůvodnění Aktu. Je pravděpodobné, že toto varování by se v budoucnu mohlo vyskytovat i v textech certifikátů samotných. V tomto bodě je zřejmý vliv francouzského národního schématu, které na nemožnost absolutní garance bezpečnosti upozorňuje (viz kapitola č. 6). Cílem celé certifikace je, aby výrobci a vývojáři pozvolna akceptovali standardy „*security by design*" (kdy se zabezpečení řeší v celém životním cyklu produktu už od projektové dokumentace) a „*security by default*" (produkty by v momentě, kdy je koncoví uživatelé převezmou, měly být již v nejbezpečnějším možném nastavení, a to bez vyžadování dalších úkonů ze strany uživatele) jako normální, běžné a přirozené.[224]

Základem důvěry v bezpečnost bude kvalitní schéma, které stanovuje dostatečné pojistky proti rizikům kyberprostoru. Akt samotný stanovuje zásady, konkrétní bezpečnostní cíle a obecný rámec pro tvorbu takových schémat, jak bylo ostatně již řečeno ve čtvrté kapitole. Konkrétní postupy certifikace by měly být stanoveny v jednotlivých schématech, aby bylo možné přizpůsobit se ad hoc potřebám produktů.[225]

Bezpečnostní cíle schémat jsou uvedeny v demonstrativním výčtu v článku 51 Aktu. Každé schéma by podle něj mělo směřovat zejména k ochraně dat před zničením, ztrátou, nedostupností, pozměněním a neautorizovaným přístupem, ukládáním nebo zpracováváním. Dále by měly obsahovat pojistky, že osoby i programy se mohou dostat jen k těm částem produktu, ke kterým mají mít přístup, a že o celkovém chování produktu jsou činěné záznamy (tzv. logy aktivit). Schémata by se zároveň měla zaměřovat na kontinuální vyhledávání a dokumentaci zranitelností a s ohledem na to také obsahovat opatření zajišťující, že produkt tyto známé zranitelnosti neobsahuje.

[224] Viz body 7 až 12 a 75 až 77 odůvodnění Aktu o kybernetické bezpečnosti.

[225] Viz bod 69 odůvodnění Aktu o kybernetické bezpečnosti.

Naplnění bezpečnostních cílů bude důležité zejména pro informovanější uživatele a profesionální odběratele produktů (příp. pro státní sektor), ale pro průměrného uživatele bude mít certifikace hodnotu spíše ve větší informovanosti o bezpečnosti produktů, jejich porovnatelnosti a možnosti učinit tak lepší volbu na trhu. Akt tak v bodě 93 odůvodnění stanovuje požadavek, aby certifikáty byly psány co možná nejvíce s ohledem na znalostní úroveň průměrných uživatelů a vystavovány online. K tomu, aby uživatelé mohli certifikáty snadno najít, dokonce Akt ukládá v článku 50 povinnost ENISA, aby za tímto účelem zřídila webovou stránku, na které budou všechny potřebné informace o certifikaci, certifikátech i platných a připravovaných schématech.

7.2 ÚROVNĚ ZÁRUKY CERTIFIKÁTŮ

Stejně jako systém Common Criteria poskytuje uživatelům možnost různé úrovně záruky za bezpečnost certifikovaného produktu (EAL), který vyjadřuje, jak náročnými testy produkt prošel a jakým hrozbám by měl být schopen čelit, zavádí úrovně záruky bezpečnosti i Akt. Oproti Common Criteria (celkem sedm) zavádí úrovně jenom tři, a to základní, významnou a vysokou.[226] V rámci každého schématu bude upraveno, na jakou úroveň záruky je umožněno produkty podle tohoto schématu certifikovat. Minimálně by tedy každé schéma mělo obsahovat jednu libovolnou úroveň, mohou však být obsaženy i všechny tři.[227] Při zahrnování úrovní do schématu by se mělo postupovat dle hodnocení rizik pro daný produkt. Stejně by mělo být postupováno i při samotném certifikování, vývojáři

[226] Takto byly úrovně přeloženy již v červencové (2018) verzi Aktu. Může se zdát trochu zbytečné, aby bezpečnostní úrovně záruk v nařízení eIDAS byly „nízká, značná a vysoká" a v Aktu „základní, významná a vysoká", když faktická bezpečnostní záruka je obdobná.

[227] V článku 54 anglické verze Aktu je formulován požadavek, aby schéma obsahovalo alespoň jednu bezpečnostní úroveň, (cituji) „*pokud je to možné*". V české verzi je tento požadavek stanoven takto: „ v *příslušných případech*". Toto považuji za velice nešťastně zvolenou formulaci, neboť v každém případě by ve schématu měla být uvedena alespoň jedna úroveň. Není znám případ, kdy by schéma nemělo obsahovat bezpečnostní úroveň, ani taková situace nedává smysl. Nad tímto se pozastavili i právní lingvisté v rámci překladu Aktu do dalších jazyků. Podle informací, které jsem měl tou dobou k dispozici po konzultacích s odborníky z prostředí Komise a Rady EU, mělo dojít k odstranění tohoto problému při překladu, leč „v příslušných případech" neshledávám jako vyřešení této nejasnosti.

a výrobci by tak před zahájením certifikačního procesu měli zhodnotit rizika, která mohou hrozit konkrétně jejich produktu, a podle výsledků se rozhodnout pro určitou úroveň záruky certifikátu. Jenom certifikát může být udělen na jakoukoliv úroveň záruky, vlastní posouzení je možné provést jen a pouze k základní úrovni záruky.[228]

Základní úroveň záruky jako taková proklamuje schopnost produktu odolat naprosto základním kybernetickým incidentům a útokům. Opatření, která takový produkt zavádí, by měla být snadno a dostatečně kontrolovatelná pouhou revizí technické dokumentace (případně obdobného testu, pokud ze své podstaty není revize dokumentace možná), tedy bez faktického testování produktu samotného. Tato úroveň je tedy určena do prostředí, kde se vyskytují buď jen základní rizika s minimálním dopadem, nebo je výskyt závažných rizik s nebezpečným dopadem vysoce nepravděpodobný. Významná úroveň záruky uživatele informuje o tom, že produkt neobsahuje známé zranitelnosti, riziko výskytu známého kybernetického incidentu je minimální a produkt je schopen odolat kybernetickým útokům ze strany aktérů s limitovanými zdroji anebo schopnostmi. Posuzování na tuto úroveň sestává z testů známých zranitelností (a zda jim produkt nepodlehne) a faktického testování dostatečné implementace nezbytných bezpečnostních opatření. Nejzajímavější v Aktu je úroveň vysoká. Ta osvědčuje, že produkt obsahuje dostatečná bezpečnostní řešení a prošel natolik důkladným testováním, že *„minimalizuje riziko výskytu kybernetických útoků využívajících nejmodernějších technologií („state-of-the-art cyber attacks“) provedených aktéry, kteří vládnou značnými zdroji a znalostmi.“*[229] Ve starší verzi návrhu byl v odůvodnění[230] uveden jako příklad takového útočníka financovaný multidisciplinární tým. Testování by mělo být prováděno alespoň formou penetračního testování a je nutné ověřit implementaci nejmodernějších

[228] Viz body 78 a 79 odůvodnění a článek 52 Aktu o kybernetické bezpečnosti.

[229] Viz článek 52 Aktu o kybernetické bezpečnosti.

[230] Viz bod 56b odůvodnění návrhu Aktu o kybernetické bezpečnosti, verze z července 2018.

bezpečnostních opatření, která mají proti takovým útokům produkt chránit.[231]

Jednotlivá schémata pak mohou nadefinovat několik různých úrovní testování produktů, která se budou lišit v přísnosti, důkladnosti a užité metodologii. Každá z testovacích úrovní by však měla odpovídat jedné z úrovní záruky. Schéma může zároveň ve speciálních případech specifikovat, že k vydání certifikátů je příslušná jenom národní autorita pro certifikaci kybernetické bezpečnosti nebo veřejnoprávní orgány akreditované na pozici subjektů posuzování shody (certifikačních těles).[232] V případě, kdy schéma vyžaduje certifikaci na vysoké úrovni záruky, je takový postup dokonce přikázaný a i zmíněné veřejnoprávní akreditované subjekty mohou certifikaci provést jen tehdy, pokud jim to povolí národní autorita pro certifikaci kybernetické bezpečnosti (případně takový orgán a priori deleguje svou pravomoc).[233]

7.3 ORGANIZAČNÍ STRUKTURA

Správa celého evropského certifikačního rámce byla primárně svěřena ENISA (dále také jako „Agentura“) ve spolupráci s Komisí. Akt je v tomto ohledu dle mého názoru trochu nerealistický, neboť faktický rozsah povinností, které uložil Agentuře, je nezměrný.

7.3.1 ENISA

Agentura je pověřená permanentním monitoringem kyberbezpečnostní situace v Evropě, stavu na trhu s kyberbezpečnostními technologiemi a vývoje v ohledu standardizace a dalších technických norem. Výstupy z tohoto monitoringu mají být zohledněny při tvorbě nových schémat, což je další velká povinnost, kterou Agentura obdržela. Na žádost (proces přípravy schémat bude rozebrán níže) musí totiž připravit návrh schématu, který je pak schválen Komisí. Dále musí Agentura vyhodnocovat fungování a účinky již schválených schémat, aby bylo v případě nutnosti možné

[231] Viz body 87 až 90 odůvodnění a článek 52 Aktu o kybernetické bezpečnosti.

[232] Viz články 52, 54 a 58 Aktu o kybernetické bezpečnosti.

[233] Viz bod 87 odůvodnění Aktu o kybernetické bezpečnosti.

nefunkční schémata upravit. Tyto revize je ENISA povinna u každého schématu udělat alespoň jednou za pět let. Rovněž je povinna zprovoznit a udržovat internetovou stránku věnovanou certifikaci, evropským certifikačním schématům platným, připravovaným, navrhnutým i zamítnutým, informacím o dotčených národních schématech i samotných certifikátech.[234]

K tomu, aby usnadnila provádění certifikací a přípravu vývojářů na ni, je povinna vytvářet a publikovat návody, výkladové materiály k bezpečnostním požadavkům a metodické manuály k zavedení osvědčené praxe ohledně certifikovaných skutečností. Agentura musí poskytovat i poradní a konzultační služby, primárně ostatním subjektům podílejícím se na vytváření schémat, ale zároveň i certifikačním tělesům, koncovým uživatelům či členským státům v ohledu certifikace.[235]

Akt sice obsahuje zvýšení ekonomických i personálních kapacit Agentury, ale dle mého názoru je zvýšení neproporcionální s množstvím povinností, které jí byly přiděleny.[236] Osobně bych očekával, že až bude certifikační rámec spuštěn, bude buď alespoň zpočátku docházet k velkým prostojům a dlouhým čekacím dobám, nebo bude většina práce „outsourcována" na ad hoc pracovní skupiny, případně bude docházet pouze k přejímání již hotové práce. Ale až praxe ukáže, jestli jsou tyto obavy oprávněné.

Minulé verze Aktu, včetně debat v rámci trialogu, obsahovaly možnost rozdělit povinnosti Agentury mezi další subjekty (např. nechat i Skupině zúčastněných stran pro certifikaci možnost připravovat návrhy schémat). V případě, že by vydání schématu stále předcházel víceúrovňový

[234] Viz články 7, 8, 39 a 48 až 50 Aktu o kybernetické bezpečnosti.

[235] Viz body 26 až 42 odůvodnění a články 48 až 50 Aktu o kybernetické bezpečnosti.

[236] Ke konci roku 2018 bylo v ENISA zaměstnáno 70 zaměstnanců (viz Annual Activity Report 2018 [online]. Řecko: European Union Agency for Cybersecurity, 2018, s. 57 [vid. 12. říjen 2019]). Do pěti let mají personální kapacity narůst o 50 % a finanční kapacity se zdvojnásobit (na 23 mil EUR, viz Questions and Answers - EU Cybersecurity. *European Commission* [online]. [vid. 12. říjen 2019]. Získáno z: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_19_3369). Toto navýšení Agentuře tedy jistě pomůže, ale jenom náročnost udržování a vytváření certifikačního rámce dle mého názoru dalece přesahuje toto navýšení.

konzultační proces, jak je nyní nastaveno, mohlo by se možná jednat o stejně bezpečné řešení, jenom efektivnější, ale byl zvolen princip ad hoc pracovních skupin.

7.3.2 EVROPSKÁ KOMISE

Komise je nejvyšším orgánem, který zaštiťuje celý certifikační aparát. Komisi vznikne v souvislosti se spuštěním certifikačního rámce povinnost zpracovat, přijmout a zveřejnit do 28. června 2020 Průběžný pracovní program Unie pro evropskou certifikaci kybernetické bezpečnosti (dále jen jako „Program"), ve kterém budou vymezeny strategie a cíle evropské kyberbezpečnostní certifikace. Primárně bude Program obsahovat seznam produktů, pro které je nutné/potřebné/vhodné vytvořit schéma. Na seznam se produkt může dostat z několika důvodů – existuje-li pro kategorii produktů národní schéma a hrozí kvůli tomu fragmentace trhu; pokud tak stanoví právní předpis Unie nebo je to z důvodu jejího směřování a politik vhodné; existuje po takovém schématu dostatečná poptávka na trhu; vyžaduje si to vývoj v oblasti kybernetické bezpečnosti, anebo pokud si přípravu schématu vyžádá Evropská skupina pro certifikaci kybernetické bezpečnosti (dále jen jako „Skupina").[237]

V souladu s Programem může Komise podávat žádosti Agentuře, aby připravila návrh schématu nebo provedla revizi již stávajícího. Ve výjimečných situacích může Komise (a v tomto případě i Skupina) požádat Agenturu, aby návrh připravila, dokonce i když takové schéma/postup není uveden v Programu, přičemž v takové situaci je pak nutné Program aktualizovat. Komise je nadána pravomocí přijímat schémata připravená Agenturou, a to ve formě implementačních aktů.[238]

Přestože je certifikace obecně dobrovolná a ponechána tedy v rozhodovací kompetenci členských států, jestli neučiní některé schéma obligatorním pro povinné subjekty, Komise je pověřena průběžným vyhodnocováním funkčnosti a užívání schémat, jejich celkového účinku na bezpečnost v Unii a zjištěním, zdali by neměla být určitá schémata přijata

[237] Viz článek 47 Aktu o kybernetické bezpečnosti.

[238] Viz článek 48 a 49 Aktu o kybernetické bezpečnosti.

jako povinná pro celou Unii. Při tomto hodnocení však musí dbát zejména na to, jaký by takový krok měl vliv na jednotný trh a dostupnost produktů.[239]

Evropská komise je zároveň, ve spolupráci s Agenturou a Skupinou, nadána pravomocí vstoupit do jednání s dalšími mezinárodními subjekty o uzavření dohod o vzájemném uznávání evropských certifikátů (MRA).[240]

7.3.3 PORADNÍ SKUPINA ENISA A SKUPINA ZÚČASTNĚNÝCH STRAN PRO CERTIFIKACI

Aby ENISA zůstala při svých aktivitách v kontaktu s okolním světem, vytvoří čl. 21 Aktu tzv. Poradní skupinu ENISA, která má být složena ze zástupců průmyslu (ICT odvětví), poskytovatelů služeb internetové společnosti, malých a středních podniků, správců informačních infrastruktur, spotřebitelů i akademické půdy. Součástí poradní skupiny by měly být i policejní složky a orgány dohledu nad ochranou osobních údajů. Poradní skupina radí a pomáhá tak Agentuře při naplňování jejích povinností v odborných otázkách. Její působnost se však nevztahuje na otázky ohledně certifikace. V této oblasti zastává poradní funkci Skupina zúčastněných stran pro certifikaci, která bude vytvořena podle čl. 22 Aktu. Jejími členy budou přední experti relevantních zúčastněných stran. Kromě poradní funkce ohledně certifikačního rámce má ještě za úkol na žádost poskytnout rady při formování nových schémat a standardizace, asistovat při tvorbě Programu (a zároveň má právo se k němu vyjádřit, přičemž názor této skupiny musí být vzat v potaz) a v naléhavých případech zpravit Komisi a Skupinu o potřebě vytvořit jiné schéma, než jaké je zahrnuté v Programu. Tento orgán má čistě poradní funkci, je nutné neplést ho se Skupinou (Evropská skupina pro certifikaci kybernetické bezpečnosti).[241]

V minulých verzích Aktu měly mít zúčastněné strany daleko vyšší pravomoci, ovšem v prvotním návrhu Komise se s nimi, kromě čistě

[239] Viz článek 56 Aktu o kybernetické bezpečnosti.

[240] Viz bod 105 odůvodnění Aktu o kybernetické bezpečnosti.

[241] Viz články 21 a 22 Aktu o kybernetické bezpečnosti.

konzultační role, vůbec nepočítalo. Je tak patrný vliv velice nesouhlasné reakce zúčastněných stran, která přišla po zveřejnění první verze Aktu.

7.3.4 EVROPSKÁ SKUPINA PRO CERTIFIKACI KYBERNETICKÉ BEZPEČNOSTI

Skupina je orgán ustavený v čl. 62 Aktu. Jeho název se v průběhu legislativního procesu vcelku dost měnil.[242] Jedná se o uskupení složené ze zástupců vnitrostátní orgány certifikace kybernetické bezpečnosti (dále jen jako „NCCA" z angl. „*National cybersecurity certification authorities*"), případně dalších relevantních vnitrostátních autorit. Jedná se o pomocný orgán, který má pomáhat Agentuře v naplňování a implementaci certifikačních aktivit po celé Unii, udržení konzistence implementace, koordinaci vnitrostátních politik a pomoc při přípravě schémat, přičemž Skupina je oprávněna přijmout názor k chystanému schématu, který sice není závazný, ale Agentura se s ním musí vypořádat. Skupina má právo ve zvláště odůvodněných případech požádat Agenturu o vytvoření schématu i mimo Program. Agentura je, oproti žádosti od Komise, které musí vyhovět, oprávněna tuto žádost zamítnout, ale musí takový svůj postup řádně odůvodnit.[243]

Skupina má dále usnadňovat kooperaci mezi jednotlivými NCCA, zajišťovat výměnu informací a osvědčených praktik, prozkoumávat vývoj, který se odehrává na poli kybernetické bezpečnosti a zajišťovat soulad mezi schématy a mezinárodními certifikáty. V případě úkolu posledně zmíněného je dokonce oprávněna navrhnout Agentuře zahájení jednání s příslušnou mezinárodní organizací o vyplnění úpravy a odstranění nedokonalostí. Skupina by též měla hrát významnou roli při sjednávání a zprostředkování vzájemného hodnocení, kterému budou podrobeny NCCA.[244]

Co se týká vzájemného hodnocení a křížového posuzování NCCA, jedná se o problematiku, která by mohla být Aktem upravena podstatně lépe.

[242] Např. ve verzi z července roku 2018 byla Skupina nazvána jako Skupina členských států pro certifikaci kybernetické bezpečnosti.

[243] Viz článek 48 a 62 Aktu o kybernetické bezpečnosti.

[244] Viz článek 59 a 62 Aktu o kybernetické bezpečnosti.

Obsahuje totiž několik mezer, které jsou vcelku zásadní. V rámci hodnotícího procesu např. není moc dobře upravena situace, kdy bude zjištěno, že certifikát byl vydán v rozporu s Aktem nebo schématem. Případně postup, který bude následovat poté, co se NCCA v rámci vzájemného hodnocení neshodnou. Tato část bohužel nebyla oproti prosincové finální verzi dotvořena.

7.3.5 VNITROSTÁTNÍ ORGÁNY CERTIFIKACE KYBERNETICKÉ BEZPEČNOSTI

NCCA je vnitrostátní orgán určený členským státem k výkonu dozorčí funkce nad dodržováním povinností plynoucích z tohoto nařízení pro subjekty na jeho území (subjekty posuzování shody i ostatní tržní subjekty). Členský stát může určit více než jeden NCCA nebo se domluvit s jiným členským státem na ustavení společného. Ať už členské státy rozhodnou jakkoliv, musí informovat Komisi o identitě tohoto orgánu a v případě, kdy je orgánů více, také o rozdělení jejich pravomocí. Je možné, aby byla tato role přisouzena i již existujícímu orgánu, což bude patrně situace ve většině členských států.[245]

Od NCCA je v některých případech vyžadováno též vydávání certifikátů a provádění hodnocení produktů, a proto by měly být vybavené dostatečnými kapacitami (nebo mít možnost přenést toto posuzování na veřejnoprávní CAB). Zároveň je však nutné poskytnout záruky, aby bylo posuzování produktů důsledně odděleno od výkonu dozorčí funkce. Vzhledem k tomu, že NCCA budou často orgánem členského státu, je nezbytné poskytnout záruky, aby byl nadán dostatečnou nezávislostí na ostatních složkách státní moci, jinak by dohled nad certifikací prováděnou směrem ke státnímu sektoru nebylo možné nezávisle vykonávat.[246]

Členské státy by měly zajistit, aby byly NCCA nadány dostatečnými pravomocemi a zdroji k efektivnímu a účinnému výkonu dozoru. Tento dozor se vztahuje na implementaci a vynucování případných budoucích povinných schémat; na subjekty posuzování shody (soukromoprávní

[245] Viz článek 58 Aktu o kybernetické bezpečnosti.

[246] Viz tamtéž.

i veřejnoprávní), kde NCCA aktivně spolupracují s akreditačními autoritami; a na výrobce a poskytovatele služeb, pokud provádějí vlastní posouzení shody. Mezi další úkoly patří mimo jiné i příjem a vyřizování stížností vzešlých buď z certifikačního procesu provedeného NCCA samotnou, nebo provedeného veřejnoprávním subjektem posuzování shody při certifikaci na vysokou úroveň záruky. V případě, že pokynů NCCA nebude v jakémkoliv ohledu uposlechnuto, měla by být nadána pravomocí ukládat pokuty, jejichž výši mají nadefinovat členské státy tak, aby byly přiměřené, ale účinné.[247] To by v praxi mohlo činit problémy s usazováním subjektů ve státech s nižšími pokutami, neboť pokud mají být pokuty přiměřené, tak by měly vycházet alespoň přibližně z parity kupní síly v daném státě. V tomto by mohly vzniknout rozdíly mezi státy východní Evropy a zbytkem Evropy. A pokud mají být pokuty účinné, tak se zase západ nemůže přizpůsobovat ekonomicky slabšímu východu. Ovšem záleží i na celkové výši pokut, jestli budou natolik citelné pro subjekty, že by kvůli tomu docházelo k většímu stěhování.

Všechny NCCA by měly úzce spolupracovat, koordinovat své postupy, metody a politiky a zároveň podléhat vzájemnému hodnocení („*peer review*“), aby bylo docíleno jednotného standardu při vydávání certifikátů a dohledu nad certifikačními aktivitami. Hodnocení bude probíhat na základě předem upravené a pravděpodobně jednotné metodiky[248] a bude se soustřeďovat na organizační, personální a procesuální řešení hodnotícího procesu, bezpečnostní řešení důvěrnosti informací a efektivitu vyřizování stížností. Zároveň se pak budou hodnotit i autorizované certifikáty, které by v případě nalezení neshod v certifikačním procesu mohly být staženy.[249] Otázkou zůstává, jak se bude postupovat v případě, že by se jednalo o certifikát autorizovaný spoluprací dvou a více certifikačních těles a chyba v procesu by byla nalezena pouze u jedné z nich. Já osobně zastávám názor, že by certifikát nadále zůstával potvrzením dané úrovně zabezpečení, protože by ho stále jedna z certifikačních autorit ověřila

[247] Viz článek 65 Aktu o kybernetické bezpečnosti.

[248] Jedná se o domněnku autora, Akt toto neupravuje.

[249] Viz článek 59 Aktu o kybernetické bezpečnosti. Připomínám ovšem, že tento proces není dostatečně upraven a představuje značnou slabinu Aktu.

platným způsobem. Tím pádem by nemuselo být potřeba jej z pragmatického hlediska rušit. Pádný argument ovšem nabízí i opačné řešení – porušení pravidel vydání certifikátu stanovených schématem samo o sobě vybízí ke stažení certifikátu a opačný postup posiluje možnost diskrece ohledně osudu certifikátů na velice nejistou úroveň.[250]

Provádět toto hodnocení budou alespoň dvě další NCCA z jiných členských států, přičemž každá NCCA musí být předmětem vzájemného hodnocení alespoň jednou za pět let.[251] To, jak se budou NCCA vybírat, příp. podle jakého klíče, není upravené. Dle mého názoru by mohla v tomto ohledu významně pomoci Skupina. K založení dalších pravomocí Skupiny by však bylo nutné zakomponovat takové pravomoci přímo do Aktu, což se nestalo.

Na rozdíl od CAB ovšem Akt neobsahuje konkrétnější podmínky k provozu NCCA. Původně měly být uvedeny v Příloze, ale odtud byly nakonec vyškrtnuty bez náhrady. To může představovat problém pro udržení jednotného standardu kvality mezi jednotlivými NCCA.

Zároveň je v Aktu uvedeno, že za jednání NCCA jsou odpovědné členské státy. To je sice vcelku pochopitelné, i nařízení eIDAS obsahuje podobnou úpravu, tato odpovědnost je ale v případě Aktu naformulována příliš obecně. Není patrné, jestli členské státy v případě vadného certifikátu odpovídají za skutečnou škodu, která vznikne na základě toho, že se produkt nechoval tak, jak podle certifikátu měl, nebo odpovídají i jen za pouhou skutečnost, že certifikát je vadný, aniž by vznikla reálná škoda.[252]

7.3.6 SUBJEKTY POSUZOVÁNÍ SHODY

Subjektem posuzování shody je myšlen „*subjekt, který vykonává činnosti prokazující, že byly splněny konkrétní požadavky týkající se výrobku, postupu,*

[250] Jak je vidět, bylo by třeba tuto mezeru napravit, protože obě možnosti přístupu jsou odůvodněné, jedna opírající se o formální stránku certifikátu, druhá o materiální.

[251] Co se týká procesu „*peer review*“, bylo by možné se inspirovat i v již fungujícím systému eIDAS, kde tento systém též funguje.

[252] Nařízení eIDAS obsahuje úpravu odpovědnosti za potenciální škodu, nutí tak členské státy k větší opatrnosti. Dle mého nepříliš vyhraněného názoru by však potenciální škoda např. u formálních vad certifikátů mohla být až příliš přísná a místo toho by stačila odpovědnost za skutečnou škodu.

služby, systému, osoby nebo subjektu (v případě Aktu je relevantní pouze výrobek, proces nebo služba), včetně kalibrace, zkoušení, certifikace a inspekce“.[253] K samotnému posuzování shody je nezbytná akreditace, která bude rozebrána níže. Jako subjekt posuzování shody může (a měl by) být akreditován i certifikační orgán, který je součástí NCCA, neboť je v některých případech vyžadováno, aby byla certifikace prováděna přímo NCCA. Pokud evropské certifikační schéma stanoví speciální požadavky na certifikační těleso, provádět certifikaci podle takového schématu může jen subjekt posuzování shody, který byl pro naplnění speciálních podmínek k takové certifikaci autorizován od NCCA. U každého takového schématu musí NCCA zpravit Komisi o všech autorizovaných subjektech posuzování shody.[254]

Akt se ve své úpravě soustředí na certifikační autority a odpovědnost za testovací laboratoře a úpravu vztahu mezi dvěma zmíněnými přenáší na certifikační těleso. To však stvořilo vcelku závažný problém – chybí institucionální požadavky na testovací laboratoře, včetně požadavku na umístění. Sídlo sice CAB musí mít v rámci Unie, ale o tom, kde jsou umístěné jeho laboratoře, Akt nepojednává. Je pochopitelné, že při testování produktů, které mají zabezpečovat kybernetickou bezpečnost ve členských státech, nebude žádoucí posílat tyto produkty na otestování např. do Číny nebo do Ruska. Akt ve své momentální podobě ovšem nenabízí mechanismus, jak tomuto předejít. Tato mezera nebyla vyřešena, je možné ji zhojit ještě nepřímo (např. v jednotlivých schématech).

Požadavky na provoz subjektu posuzování shody jsou upraveny v příloze k Aktu. Zprvu se musí jednat o subjekt mající právní subjektivitu a zřízený v souladu s vnitrostátním právem. Může se však jednat i o státní subjekty nebo korporace a profesní sdružení reprezentující výrobce a podnikatele v oblasti vývoje, výroby a dalšího nakládání s ICT produkty. Jediné, co musí být splněno v takových případech, je zaručení absolutní nezávislosti (a to i na úrovni vrcholného managementu), neboť subjekt

[253] Viz čl. 2 nařízení Evropského parlamentu a Rady (ES) č. 765/2008 ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93.

[254] Viz článek 60 a 61 Aktu o kybernetické bezpečnosti.

posuzování shody musí být vždy nezávislý na žadateli, jehož produkty posuzuje. Pokud by tedy takové těleso posuzovalo produkt, nesmí být v žádném ohledu spojeno s produktem – nesmí být ani dodavatelem, ani vlastníkem, ani investorem. Vždy musí být zaručena plná svoboda úsudku při posuzování produktu.

Celý model nezávislosti stojí dle mého názoru na bodu 8 přílohy k Aktu, který (mimo jiné) stanovuje, že jak subjekty posuzování shody, tak jejich personál by měly posuzování provádět prosty jakýchkoliv nátlaků a vlivů, včetně finanční závislosti, které by mohly ovlivnit výsledek posuzování. To je ustanovení, které považuji více za vroucí přání než skutečné pravidlo. Subjekty posuzování shody budou často komerčního charakteru a finance budou tedy získávat zejména z provádění certifikačních testů. Je tím pádem možné, že se CAB budou snažit provádět testování tak, aby nepřišly o zákazníky. Případně mohou žadatelé o certifikaci nechat CAB „*vyhladovět*" (buď za trest za neudělený certifikát, nebo jako motivaci pro budoucí udělení certifikátu). A možnost ekonomického „*hladovění*" certifikačních těles a jejich touhy nepřijít o zákazníky očekávám daleko silnější právě na menších trzích, které nebudou nabízet takovou soutěž mezi žadateli o certifikaci. To by pak vedlo k ohybání trhu, snížení důvěry v certifikáty a jiné nežádoucí efekty. Proto by tyto situace měly být kontrovány právě procedurami vzájemného hodnocení a revokacemi vadných certifikátů.

Co se týká úrovně technologického vybavení CAB, příloha formuluje požadavek, aby CAB byly schopné provést všechny certifikační úkony, které jim ukládá Akt. To je, dle mého názoru, další poněkud nešťastná formulace. Neznamená totiž, že všechny CAB mají vládnout kapacitami k provozování všech schémat, ale jen těch, které se samotné CAB rozhodne provozovat. Základní myšlenkou tohoto ustanovení bylo, že všechny CAB by z důvodu stejné základní bezpečnostní úrovně měly mít stejné základní vybavení, speciální požadavky by byly nadefinovány až v jednotlivých schématech. Je zde samozřejmě nebezpečí, že si trh skrz toto ustanovení rozdělí např. německé a francouzské CAB, které již potřebné vybavení mají, ale je opět otázkou budoucnosti, jestli bude tato obava naplněna. Mezi onu zmíněnou základní úroveň tedy patří nezbytný a dostatečně zkušený personál,

technologické vybavení, popisy všech hodnotících procedur (k zajištění transparentnosti), plány a politiky k přizpůsobení posuzovacího procesu velikosti žadatele (v případech právnických osob, nikoliv fyzických). Náročnost i jen základní úrovně těchto požadavků je tedy značná.

Příloha specifikuje i požadavky na personál subjektů posuzujících shodu – dostatečné odborné technické znalosti pokrývající celou materii posuzovacích aktivit, znalost bezpečnostních požadavků certifikačních schémat, přiměřenou znalost použitelných testovacích standardů a technických požadavků a schopnost odpovídajícího zaznamenávání celého certifikačního procesu, stejně tak jako schopnost vyhotovit certifikáty samotné. Jak je patrné z prvních dvou kapitol, český pracovní trh není pracovní silou, která by podobné kvalifikace splňovala, zrovna přeplněn, a tak se i tato část podmínek k vytvoření subjektu posuzování shody může ukázat pro český trh jako problematická.

Stejně jako v případě CC i Akt klade subjektům posuzování shody povinnost opatřit si certifikát podle příslušného standardu pro provoz certifikačních těles, tedy např. mezinárodní standard ISO/IEC 17065 v aktuálním znění, a zároveň jsou CAB povinny zajistit, aby odpovídající certifikát vlastnily i využívané testovací laboratoře – např. ISO/IEC 17025 v aktuálním znění. Je možné využít i jiný standard, který zajistí podobnou úroveň certifikace a testování.[255]

7.3.7 NÁRODNÍ AKREDITAČNÍ ORGÁN

Národní akreditační orgán je „*orgánem, který na základě státem delegované pravomoci v daném státě osvědčuje, že subjekt posuzování shody splňuje požadavky pro provádění konkrétních činností posuzování shody, které stanoví harmonizované normy (…).*“[256] V případě Aktu se jedná o požadavky, o kterých jsem pojednával v přechozí podkapitole. Akreditace by měla být udělována na maximální dobu 5 let a může být opakovaně udělena znovu. Akreditační orgány mohou udělenou akreditaci omezit, pozastavit její

[255] Viz body 19 a 20 Přílohy k Aktu o kybernetické bezpečnosti.

[256] Viz čl. 2 nařízení Evropského parlamentu a Rady (ES) č. 765/2008 ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93.

účinnost, nebo ji úplně odebrat, pokud subjekt posuzování shody přestane splňovat podmínky pro udělení akreditace a tento stav ani dodatečně nenapraví (případně hrubě porušuje povinnosti stanovené v Aktu). V českém prostředí je národním akreditačním orgánem Český institut pro akreditaci, o.p.s.[257]

7.3.8 KAPACITY PRO POSUZOVÁNÍ SHODY V ČR

V České republice sice s obecnou certifikací kyberbezpečnostních technologií zkušenosti zatím chybí, ovšem začaly přípravy struktur pro vytvoření vlastního CAB, k čemuž je možné využívat zkušeností z již existujících oblastí (mimo jiné eIDAS). Česká republika již také není prosta technických kapacit (soustředících se zejména na univerzitách), které jsou momentálně využívány k certifikacím pro zahraniční certifikační autority. Je proto možné, alespoň částečně, odhadnout, jak bude systém na území ČR vypadat. Podle zákona č. 90/2016 Sb., o posuzování shody stanovených výrobků při jejich dodávání na trh, by se NCCA dalo pravděpodobně přirovnat k úloze, kterou zastává Úřad pro technickou normalizaci, meteorologii a státní zkušebnictví (dále jen „Úřad“), přičemž všechny činnosti související s tvorbou, vydáváním a distribucí technických norem (mezi které patří i standard ČSN EN ISO/IEC 27001) přešly k 1. 1. 2018 na Českou agenturu pro standardizaci.[258] Subjekty pro posuzování shody v tomto modelu posuzují shodu výrobků s technickými normami, které vydává vláda, systém tudíž není natolik rozdílný od chystaného Rámce. Podobně jako NCCA i Úřad autorizuje subjekty pro posuzování shody u vybraných produktů, u kterých je zapotřebí naplnění dalších požadavků k posuzování. Mezi autorizované subjekty patří mimo jiné TÜV SÜD Czech s. r. o. (pobočka zmíněného německého elektrotechnického standardizačního gigantu), Strojírenský zkušební ústav, s. p., či Institut pro testování a certifikaci, a.s.[259] Celkem existuje na území ČR přibližně 1200 akreditovaných subjektů pro posuzování shody a přibližně 50

[257] Viz Český institut pro akreditaci, o.p.s. *ČIA - Národní akreditační orgán* [online]. [vid. 20. leden 2019]. Získáno z: http://www.cia.cz/.

[258] Viz O Úřadu - ÚNMZ [online]. [vid. 9. únor 2019]. Získáno z: http://www.unmz.cz/urad/o-uradu.

autorizovaných. Zákon o posuzování shody výrobků při jejich dodávání na trh uvádí ještě speciální kategorii subjektů, a to tzv. notifikované subjekty, které mají přesah do EU. Ty Úřad oznamuje Komisi a zavádí je do systému NANDO.[260]

Příkladem kvalitativně jiného subjektu pro posuzování shody je Elektrotechnický zkušební ústav, který byl prvním z momentálně tří CAB, které jsou akreditovány k provádění certifikace podle nařízení eIDAS. [261,262]

Pozici NCCA v ČR pravděpodobně zaujme Národní úřad pro kybernetickou a informační bezpečnost, akreditační orgán by se měnit neměl, neboť je jím i v případě nařízení eIDAS Český institut pro akreditaci, a v případě subjektů pro posuzování shody je možné, že vznikne sdružení ze stávajících certifikačních těles založený na bázi akademického spin-off, které dokáže vyhovět přísným požadavkům Aktu.

7.4 CERTIFIKAČNÍ PROCES

Celý certifikační proces je rozdělen na dvě fáze. První fází je tvoření certifikačních schémat, druhou certifikační proces samotný (případně provedený formou vlastního posouzení) a udělení certifikátu.

7.4.1 TVORBA SCHÉMAT

Tvoření schémat začíná na úrovni Komise, a to formulováním Programu.[263] Na vytváření programu má Komise úzce spolupracovat se Skupinou zúčastněných stran pro certifikaci a Skupinou. Program musí být průběžně aktualizován, nejdéle jednou za tři roky (zpočátku to ovšem bude pravděpodobně mnohem častěji, nebo bude docházet primárně

[259] Viz Vybrané výrobky - ÚNMZ [online]. [vid. 9. únor 2019]. Získáno z: http://www.unmz.cz/urad/vybrane-vyrobky.

[260] Viz GUEBEL, Martine. *NANDO Information System (Europa)* [online]. [vid. 5. únor 2019]

[261] Nařízení eIDAS ovšem neobsahuje jednotlivá konkrétní certifikační schémata, požadavky na akreditované kvalifikované poskytovatele služeb jsou formulovány obecně.

[262] Viz Seznam akreditovaných subjektů pro posuzování shody podle nařízení eIDAS platný ke dni 5. 2. 2019. *European Commission - Futurium: eIDAS Observatory* [online]. [vid. 28. únor 2019]. Získáno z: https://ec.europa.eu/futurium/en/system/files/ged/list_of_eidas_accredited_cabs-2019-02-05.pdf.

[263] Program nebude mít právně závaznou formu.

k mimořádným žádostem o tvorbu schémat). Hlavním smyslem Programu je stanovení strategických cílů Unie v oblasti certifikace transparentním a veřejným způsobem tak, aby se všechny zúčastněné strany mohly na nástup schémat připravit. Pro tento účel by měl být součástí Programu i časový plán/odhad předkládání žádostí o vytvoření schémat.[264]

Program je obecně potřeba k tomu, aby mohla Komise požádat Agenturu k vytvoření návrhu schématu, které je uvedené v Programu.[265] Ve speciálních a zvláště odůvodněných případech[266] však může Agenturu požádat Komise i Skupina k vytvoření návrhu schématu, které není upraveno v Programu.[267] Agentura může s odůvodněním odmítnout žádost o vytvoření schématu, kterou jí předloží Skupina, není však oprávněna odmítnout žádost Komise.[268]

Komise by měla před podáním žádosti dobře zvážit účinky schématu na trh, na inovační postup, na malé a střední podniky a na konečné uživatele. Jakmile Agentura obdrží žádost, začne s přípravou schématu. V procesu přípravy schémat podle Programu by měly proběhnout konzultace se všemi podstatnými zúčastněnými stranami. Dokonce chce Agentura (jedná se o její dobrovolný krok) do konzultačního procesu zavést i veřejné konzultace, které budou přístupné komukoliv (což považuji za velice nerozumné řešení, které bude mít za následek jenom další časové prodloužení procesu tvorby schémat). Z úpravy je patrné, že při „neprogramové“ přípravě schémat se počítá s potřebou urychleného přípravného procesu, neboť do něj nejsou konzultace se zúčastněnými stranami zapojené (zůstávají ovšem dobrovolné a Agentura se možná

[264] Viz článek 47 Aktu o kybernetické bezpečnosti.

[265] Ještě v červencové verzi Aktu byl přímo v článcích zahrnut požadavek na obsah žádosti – rozsah a předmět chystaného schématu, účel a mimo jiné i doba, do kdy má být schéma hotové – max. 6 měsíců. Tento požadavek se však do finální verze nedostal kvůli tomu, že se přesně neví, jak bude příprava schémat v praxi fungovat. Byla tak Agentuře dána větší volnost.

[266] Odůvodnění Aktu uvádí jako příklad tohoto speciálního případu rapidní vzestup nové technologie. Reálně se ovšem dá očekávat, že zpočátku Program nebude příliš zaplněn a tudíž bude frekventovanější spíše „*neprogramová*“ varianta žádosti.

[267] Program je pak nutné aktualizovat, aby byla stále zachována transparentnost.

[268] Viz článek 48 Aktu o kybernetické bezpečnosti.

i v tomto ohledu přikloní k preferenci transparentnosti). Pro přípravu každého schématu zřídí Agentura ad hoc pracovní skupinu, která bude pomocným a poradním expertním orgánem. Při celé přípravě by měla ENISA kooperovat se Skupinou, která jí bude při přípravě též pomáhat, zároveň je pak Skupina nadána možností vyslovit k připravovanému schématu názor. Tento názor sice není závazný, ale ENISA by ho měla vzít v potaz vzhledem k tomu, že je Skupina složena z jednotlivých NCCA. Agentura by své tvořící aktivity měla zároveň konzultovat s evropskými standardizačními organizacemi, aby bylo dosaženo optimálního harmonizovaného vývoje.[269] Je tedy patrné, že doba přípravy složitějších schémat bude trvat skutečně dlouho.

Akt v článku 54 upravuje minimální rozsah prvků, které by schéma mělo obsahovat.[270] Schéma by mělo umožňovat technologický vývoj a být tak dostatečně flexibilní, aby nebylo třeba jej často měnit jen kvůli přílišné navázanosti na určité technologie. Některá schémata mohou z důvodu svého významu obsahovat mechanismy ke křížovému certifikačnímu procesu mezi více certifikačními tělesy. Tím by měla být kontrolována úroveň služeb poskytovaných při certifikačních procesech u zvlášť důležitých produktů. Tento systém však není dodělaný a může způsobovat problémy, neboť neobsahuje systém pro řešení konfliktu mezi CAB, ani případné následky toho, co se stane, když jeden z CAB při posuzování pochybí a druhý nikoliv.

Při formulování obsahu a vlastností schémat došlo i k teoretickému odstranění jedné z největších slabin systému CC → schémata by měla

[269] Viz článek 49 Aktu o kybernetické bezpečnosti.

[270] Jsou jimi mimo jiné předmět a rozsah schématu, účel schématu, bezpečnostní požadavky, uvedení dotčených národních schémat a také to, podle jakých standardů se případně při posuzování postupuje, úroveň záruky bezpečnosti (jedna až tři uvedené), umožnění nebo zákaz vlastního posouzení, specifické požadavky na certifikační tělesa nebo posuzovací metody, pravidla pro dohled nad zachováním compliance (tedy, že podmínky pro udělení certifikátu jsou stále splněné), úprava následků non-compliance s požadavky schématu, dobu platnosti certifikátu (v červencové verzi Aktu byla maximální doba platnosti certifikátu stanovena pro všechny budoucí schémata fixně na 5 let, ani toto ustanovení se však do závěrečné podoby textu nedostalo), pravidla pro oznamování zranitelností produktů, podmínky pro vzájemné uznávání certifikátu s třetími zeměmi nebo i formát a podoba certifikátu samotného.

obsahovat specifickou úpravu, po jakém typu aktualizace produktu je potřeba znovu provést certifikaci. Byl tedy (teoreticky) vyřešen problém bezpečnostní evoluce produktu.[271]

Hotový návrh schématu předloží Agentura Komisi. Ta může (není povinna) schéma schválit a vydat ho ve formě implementačního aktu. Schéma je přímo použitelné, není tedy nutný žádný další krok k tomu, aby ho mohly začít využívat subjekty posuzování shody. Aktivní schéma bude pak uveřejněno na webových stránkách provozovaných Agenturou. Současně budou na těchto stránkách zveřejňovány informace výrobců a vývojářů o kybernetické bezpečnosti určené pro spotřebitele a koncové uživatele.[272]

Součástí schémat by mohly (nebo i měly) být i různé správní procesy, ke kterým může při aplikace schématu dojít. Jedním z takových procesů je i revokace certifikátu. To je problematika, které se Akt úplně vyhýbá a přesunuje její úpravu na jednotlivá schémata. Kromě jádra procesu by ovšem bylo potřeba upravit i revokační proces v případě, že se na vadu certifikátu přijde při vzájemném hodnocení NCCA, tedy když bude návrh na revokaci směřovat z jiného členského státu. Otázkou zůstává i to, kdo bude mít pravomoc certifikát stáhnout, a to nejen v této situaci, ale rovněž když bude certifikát produktem křížového posuzování.

Agentura musí alespoň jednou za pět let zhodnotit fungování schémat a zjistit si zpětnou vazbu ode všech zúčastněných stran. V případě nutnosti může být Agentura pověřena Komisí nebo Skupinou k revizi schématu, případně k vytvoření revidovaného schématu.[273]

7.4.2 CERTIFIKACE

Výrobce nebo vývojář produktu, na který je připraveno schéma, by se měl se schématem seznámit (informace o něm budou zveřejňovány na internetu) a zhodnotit rizika, která hrozí jeho produktu. Na základě tohoto vyhodnocení si pak vybere požadovanou úroveň záruky bezpečnosti (pokud

[271] Viz bod 96 odůvodnění Aktu o kybernetické bezpečnosti.

[272] Viz článek 49 a 50 Aktu o kybernetické bezpečnosti.

[273] Viz tamtéž.

to schéma umožňuje), na kterou nechá svůj produkt certifikovat, a kontaktuje příslušné CAB, které testování provede v testovací laboratoři. Žadatel o certifikát by měl s hodnotitelem spolupracovat a poskytnout mu veškerou potřebnou dokumentaci společně se všemi relevantními informacemi. V případě, že produkt v testech obstojí a splní bezpečnostní požadavky, které na něj klade schéma, udělí takovému produktu CAB certifikát. Udělení certifikátu bude zaznamenáno i na internetových stránkách k tomu určených. Držitel certifikátu by měl uživatele při koupi informovat o bezpečnostních požadavcích, rizicích, spolehlivosti certifikátu, určeném prostředí ad., a to buď prostřednictvím internetu, nebo fyzicky.[274]

U držitele certifikátu se presumuje, že je v souladu s bezpečnostními požadavky daného schématu. Členské státy mohou stanovit získání certifikátu podle určitého schématu jako podmínku presumpce naplnění souladu s vnitrostátním právem (tato možnost bude pravděpodobně vcelku hojně využívána, neboť se jedná o skvělý nástroj odstranění dvojí administrativní zátěže). V případě, že po udělení certifikátu zjistí výrobce či vývojář novou zranitelnost produktu, která by mohla mít negativní vliv na bezpečnostní záruku poskytovanou certifikátem, je povinen neprodleně informovat subjekt posuzování shody, který bude řídit další postup (v případě zásadní zranitelnosti může dojít až k recertifikaci).

Certifikace by měla být implementována jednotně ve všech členských státech, aby nedocházelo k tzv. „*certification shopping*“. To označuje využívání nejednotných podmínek pro získání certifikátů, kdy je pro investory výhodnější, levnější nebo jednodušší podstoupit certifikaci v určitém členském státě.[275]

V případě, že žadatel o certifikaci nesouhlasí se subjektem posuzování shody (nebo NCCA, pokud je v roli subjektu posuzování shody) ohledně vyřízení žádosti o udělení certifikátu, je oprávněn podat proti vyřízení stížnost. K vyřízení této stížnosti je příslušný orgán, který napadané rozhodnutí vydal. Ten je povinen stěžovatele informovat o průběhu řízení, jeho vyřízení a případně i o možnosti nápravy soudní cestou. Žadatelé jsou

[274] Viz článek 55 a 56 Aktu o kybernetické bezpečnosti.

[275] Viz bod 70 odůvodnění Aktu o kybernetické bezpečnosti.

totiž podle Aktu oprávněni k efektivnímu prostředku nápravy soudní cestou, a to proti rozhodnutí o vyřízení stížnosti (stejně jako v obecném správním řízení je tedy nutné vyčerpat všechny prostředky ochrany před využitím řízení před soudem) nebo proti nečinnosti certifikačního orgánu v řízení o stížnosti. Příslušné jsou soudy toho členského státu, kde sídlí daný certifikační orgán.[276]

7.4.3 VLASTNÍ POSOUZENÍ ANEB CONFORMITY SELF-ASSESSMENT

Evropské certifikační schéma může umožnit i zvláštní režim posuzování shody a tím je vlastní posouzení. Jedná se o posouzení shody samotným výrobcem či poskytovatelem na jeho vlastní odpovědnost. Musí provést všechny kontroly toho, že produkt je skutečně ve shodě s daným schématem, a tuto kontrolu zdokumentovat. Takové posouzení je vhodné jenom pro základní bezpečnostní úroveň.

Schéma může umožňovat cestu jak vlastního posouzení, tak certifikace, ovšem v takovém případě musí stanovit jasné způsoby, jak od sebe odlišit produkty certifikované a sebehodnocené. Vlastní ohodnocení se může jevit sice jednodušší a rychlejší než hodnotící proces provedený CAB, ale v případě certifikace zůstává faktem, že za určité chování produktu se zaručila třetí osoba nezávislá na výrobci. To samo o sobě povzbuzuje důvěru (např. spotřebitele) více než vlastní posouzení. Ovšem vzhledem k tomu, že se tato metoda bude pravděpodobně masově využívat, tržní dopad této skutečnosti bude zřejmě minimální. Odpovědnost za řádné provedení vlastního posouzení spočívá plně na výrobci, což vede ke snížení limitace odpovědnosti jako účinku certifikace.[277]

Výrobce, který provede vlastní posouzení produktu a vyhodnotí, že splňuje všechny příslušné bezpečnostní požadavky, může vydat tzv. EU prohlášení o shodě, ve kterém je uvedeno, že produkt prokázal splnění bezpečnostních požadavků schématu.[278] Vydání prohlášení je dobrovolné, pokud není uvedeno v právu Unie nebo členských států jinak,

[276] Viz článek 63 a 64 Aktu o kybernetické bezpečnosti.

[277] Viz článek 53 a bod 79 až 81 odůvodnění Aktu o kybernetické bezpečnosti.

[278] V případě vydání EU prohlášení o shodě je výrobce povinen zaslat kopie tohoto prohlášení příslušné NCCA a Agentuře.

což se může jevit jako poněkud překvapivé řešení vzhledem k tomu, že je to jediný prostředek, jak informovat uživatele o provedeném vlastním posouzení.[279] Jakmile takové prohlášení vydá, přejímá plnou odpovědnost za soulad produktu se schématem. Nebezpečnou pro prohlašujícího je tak situace, kdy by došlo k revokaci certifikátu ze strany NCCA a panovaly by pochybnosti o procesu posouzení shody. V takové chvíli může totiž příslušný prodejce/dodavatel přijít o shodu u všech svých produktů.[280]

Výrobce je povinen uchovávat k dispozici NCCA jak prohlášení, tak i dokumentaci zachycující všechny skutečnosti relevantní pro posouzení shody, neboť i samoposouzený produkt se může stát předmětem kontroly nebo kontrolního posouzení provedeného NCCA.[281]

7.5 VZTAH EVROPSKÉHO CERTIFIKAČNÍHO RÁMCE K DALŠÍM CERTIFIKAČNÍM SYSTÉMŮM

Evropský certifikační rámec (dále jen „Rámec“) má být vystavěn na základech již funkčních národních a mezinárodních schémat, především tedy schématech vzešlých ze spolupráce SOG-IS. Vhodná schémata by měla být absorbována (a upravena, aby vyhovovala novým potřebám) evropským systémem tak, aby přechod mezi jednotlivými systémy byl pro členské státy co nejhladší a aby nedošlo k výraznému poklesu bezpečnostní úrovně. Rámec se tedy nesnaží o novoty za každou cenu, spíše by měl převzít, co bude možné, a učit se z chyb svých předchůdců. Tato „*zásada kontinuality*“ je explicitně uvedena mimo jiné v bodě 71 odůvodnění Aktu.

Ve vztahu k národním schématům předpokládá Rámec ukončení účinnosti takových národních schémat, která budou nahrazena evropským schématem (tedy kdy obě schémata dopadají na stejnou materii), a to od momentu účinnosti implementačního aktu Komise. Certifikátům, které byly vydány podle těchto národních schémat, doběhne doba platnosti normálně, ovšem nové již nebude možné vydat. Akt zároveň klade členským státům

[279] Je možné, že toto řešení bylo zvoleno kvůli tomu, aby subjekty, které potřebují provést vlastní posouzení jenom pro naplnění určitých interních pokynů, nemusely o takovém postupu ještě vydávat Prohlášení.

[280] Viz tamtéž.

[281] Viz bod 81 až 82 odůvodnění Aktu o kybernetické bezpečnosti.

na srdce, aby byla zrušena neúčinná, přesto nadále platná národní schémata, aby tak bylo zamezeno nepřehlednostem pro koncové uživatele.[282] Členským státům se dále zakazuje vydávat národní schémata v oblastech, nad kterými již působí některé ze schémat Rámce.[283] Tento zákaz se ovšem nevztahuje na situace, kdy jde o zachování národní bezpečnosti. Zásadně je tedy možné vydat národní schéma z důvodu národní bezpečnosti, ale členský stát o tomto svém záměru musí dopředu informovat Komisi a Skupinu. Ty zváží, jestli význam takového schématu není natolik velký, že by bylo lepší jej přijmout jako schéma Rámce, a tedy pro dobro celé Unie. Značná část těchto požadavků je zmíněna toliko v odůvodnění (bod 94) a do článků Aktu (článek 57) se dostalo pouze vyhasnutí národních schémat.

U mezinárodních iniciativ, nad nimiž nemá Unie moc, není možné nařídit vyhasnutí, dojde tak pravděpodobně ke koexistenci více certifikačních systémů, jejichž vzájemný vztah bude muset být upraven. K vedení takových jednání byla udělena pravomoc Komisi (za asistence Agentury). Výsledná dohoda může mít podobu MRA. Otázkou, která není Aktem řešena, je další osud spolupráce SOG-IS. V praxi se očekává, že by evropský rámec mohl postupně SOG-IS nahradit. Dokud ale není upraven vztah CCRA a Rámce, není rozumné SOG-IS rušit, neboť zůstává branou k úpravě certifikace podle systému Common Criteria.[284]

7.6 VZTAH AKTU KE SMĚRNICI NIS A NAŘÍZENÍ GDPR

Akt se úzce vztahuje ke dvěma důležitým unijním předpisům – směrnici NIS a nařízení GDPR. Stručně shrnuto, Akt má pomoci s implementací NIS

[282] Tato část nařízení není upravena formou příkazu, ale doporučení (z textu Aktu to téměř působí jako prosba).

[283] Viz článek 57 Aktu o kybernetické bezpečnosti.

[284] Zajímavé bylo sledovat vývoj bodu 68 odůvodnění Aktu, který se věnuje spolupráci SOG-IS, napříč různými verzemi. V textu se vystřídal přístup, který aktivity SOG-IS vychvaloval a vyzdvihoval jeho zásluhy (jedny z prvních verzí návrhu nařízení), s přístupem, který jeho aktivity odsuzoval, vyzdvihoval nedostatečnost a důvody, proč je třeba ho nahradit (např. červencové pozměňovací návrhy). Nakonec se podoba ustálila na konstatování, že spolupráce SOG-IS došla v rámci spolupráce nad CC pravděpodobně nejdál, ovšem stále se nejedná o dostatečné řešení.

a sloužit jako cesta k zabezpečení systémů, které NIS označil za podstatné. NIS se v certifikačním procesu projeví také v momentě hodnocení schémat Komisí podle článku 56, tedy zda není třeba učinit certifikaci podle některého ze schémat obligatorní. Primárně se Komise musí zaměřit na sektory, které jsou vyjmenovány v příloze II směrnice NIS, přičemž toto posouzení musí být provedeno nejpozději do dvou let od vstupu Aktu v účinnost.

Akt je stvořen jako lex generalis unijní kyberbezpečnostní certifikace, neměl by se tudíž nikterak dotknout zvláštních pravidel o certifikaci produktů, např. právě těch, která upravuje nařízení o ochraně osobních údajů. Bod 74 odůvodnění Aktu konkretizuje certifikační aktivity zavedené GDPR, na které Akt nedopadne, takto: „*(…) mechanismy pro vydávání osvědčení a zavedení pečetí a známek dokládajících ochranu údajů pro účely prokázání souladu s tímto nařízením v případě operací zpracování prováděných správci a zpracovateli.*“

7.7 DALŠÍ POTENCIÁLNÍ SLABINY A NEVÝHODY AKTU

Dne 16. srpna 2017, tedy ještě před zveřejněním první verze návrhu Aktu, byl zaslán Komisi otevřený dopis[285] podepsaný představiteli několika předních svazů, uskupení a komor na poli transatlantického trhu s ICT produkty a službami.[286] V tomto dopise byla Komise vyzvána, aby při přijímání Aktu a „*honu za kyberbezpečností*“ nebyl ohrožen nástup IoT v Unii. Zainteresovaná uskupení se bála zejména spojeného efektu GDPR, NIS a Aktu mimo Unii, což zůstalo obavou oprávněnou. Přestože GDPR a Akt mají mezi sebou vztah upravený, kumulativní efekt těchto tří předpisů může být pro subjekty ze třetích zemí značný, zvláště v momentě, kdy bude některé ze schémat Rámce ustanoveno jako obligatorní. V dopise byla i další varování, např. „*moc bezpečí zpomalí inovace a pokrok*“, ale jsem toho názoru, že Akt na tato varování v průběhu své legislativní evoluce uspokojivě zareagoval (důležité bude zvládnout tyto výzvy v praxi).

[285] Viz IoT Cybersecurity Coalition Letter [online]. 16. srpen 2017.

[286] Signatářem byly mimo jiné United States Chamber of Commerce, American Chamber of Commerce to the European Union, Svaz průmyslu a dopravy ČR nebo Confederation of Danish Industry.

Otázkou, která nakonec nebyla Aktem vyřešena, je délka certifikačního procesu. Ta byla jednou z hlavních slabin systému CC a bylo by rozhodně vhodné ji alespoň nějakým způsobem regulovat. Limitace délky certifikačního procesu by nyní bylo nejvhodnější upravit v rámci jednotlivých certifikačních schémat, délka procesu by se tak mohla upravit ad hoc potřebám jednotlivých produktů.

Další zajímavou otázkou je odpovědnost. V případě, že certifikovaný produkt způsobí škodu a členský stát s držením certifikátu spojil účinek „*přijetí všech rozumných opatření k zamezení újmy*“, byla odpovědnost držitele certifikátu limitována. V případě, že všechny prvky certifikačního procesu budou splněny řádně, odpovědný by pravděpodobně nebyl nikdo. Pokud by koncový uživatel užil produkt v rozporu s poučením, odpovědnost by byla jeho. Pokud by certifikační autorita provedla testování nedostatečně, odpovědnost by připadla jí (nebo členskému státu, pokud odpovědnost převezme). Nedostatečná úprava odpovědnosti států zde již byla řešena. Ale otázkou je, zdali by bylo možné se dovolat odpovědnosti Unie, resp. Komise, která schémata vydává jako implementační akty, za nedokonale připravené schéma. Podle mého názoru by takový postup byl hypoteticky možný, a to v případě zjevné nesprávnosti nebo jiném projevu hrubé nedbalosti při přípravném procesu. To ale nejen že není příliš pravděpodobné vzhledem k víceúrovňovému konzultačnímu procesu, ale též by se případné pochybení velmi obtížně prokazovalo. Proto tato otázka pravděpodobně zůstane jenom hypotetickou.

7.8 POZITIVA, KTERÁ AKT PŘINÁŠÍ

Na konec této kapitoly bych ještě rád zrekapituloval přínosy Aktu. Přes všechna negativa se totiž stále jedná o naprosto revoluční legislativní krok, který přináší certifikaci kyberbezpečnostních produktů, služeb a procesů, kdy certifikáty budou automaticky a univerzálně akceptovány napříč celou Unií. Akt má potenciál zvýšit úroveň kybernetické bezpečnosti napříč celou Unií, sjednotit evropský kyberbezpečnostní trh a zlepšit konkurenceschopnost unijních výrobců. A navíc se teoreticky dokázal

vypořádat s některými vadami certifikačních systémů, které přišly před ním (např. bezpečnostní evoluce certifikovaného produktu).

8. ZÁVĚR

Ať už za účelem zvýšit bezpečnost v kyberprostoru nebo sjednotit unijní trh s kyberbezpečnostními produkty, je zřejmé, že ekonomický i bezpečnostní význam certifikace bude v Unii významně vzrůstat. Toto téma je ovšem v České republice takřka neznámé (až na pár autorů, kteří se touto problematikou zabývají), a proto cílem tohoto článku bylo zmapovat a představit čtenáři problematiku certifikace kyberbezpečnostních technologií.

K tomu, abych tento cíl naplnil, jsem si stanovil dvě výzkumné otázky. Uspokojivá odpověď na první otázku[287] si vyžádala vcelku široký teoretický rozbor pojmů shoda (compliance), certifikace a způsobů naformulování regulatorních požadavků, stejně jako můj pokus o rámcové zasazení certifikace do systému kybernetické bezpečnosti v ČR. Při analýze stávajícího stavu v ČR a Unii vyšlo najevo, že v České republice ani Unii po dlouhou dobu neexistovala[288] žádná účinná právní úprava certifikace kyberbezpečnostních technologií. To obzvlášť v Unii vytvořilo velice neuspokojivý stav naprosto roztříštěného trhu. Vyskytuje se zde sice spolupráce SOG-IS, ale ta jednotný trh není schopná spasit. Ve zvláštní části jsem pak přešel k analýze konkrétních stávajících certifikačních systémů, zejména systému Common Criteria, který je stále ještě nejvýznamnějším z mezinárodně uznávaných certifikačních iniciativ. Při rozboru tohoto systému jsem narazil na několik podstatných slabin, které se při absenci mezinárodní politické vůle již pravděpodobně nepodaří odstranit. Národních schémat jsem pak využil k analýze toho, jak by bylo možné některé ze slabin Common Criteria „*vyléčit*“. Tím jsem tedy zjistil a zmapoval, jak fungují nejvýznamnější stávající certifikační systémy. Rozbor standardů ISO 27K v páté kapitole byl proveden naopak za účelem

[287] „Jak fungují stávající certifikační systémy?“

[288] A vzhledem k tomu, že ke dni 12. 10. 2019 stále ještě běží implementační lhůta části ustanovení Aktu týkajících se certifikace, tak taková účinná úprava ještě stále není.

odpovědi na druhou otázku, přesněji řečeno pochopení dosahu a povahy části Aktu, která dopadá na certifikaci procesů.

Odpověď na druhou otázku[289] byla analyzována primárně ve čtvrté a sedmé kapitole. Zde jsem rozebral jak legislativní vývoj Aktu, tak i jeho strukturu, kterou jsem podrobil kritické analýze. Jak je v textu patrné, Akt obsahuje mnoho slabin a vad, ale přesto se jedná o naprosto revoluční tah, který zavede do všech členských států Unie certifikaci kyberbezpečnostních produktů, služeb a procesů. Funkci stávajících certifikačních systémů tak v některých členských státech pozvedne (minimálně o certifikaci služeb), v dalších, které se doposud certifikaci nevěnovaly, pomůže certifikaci vzít na vědomí. Reaguje přitom na nejrůznější vady stávajících certifikačních systémů, jako je nevyřešení bezpečnostní evoluce produktů, nemožnost certifikovat služby, neuznávání certifikátů napříč Unií.

Jednotný evropský certifikační rámec má dostatečně velký potenciál k tomu, aby pomohl Unii se stát vůdčí certifikační silou na světě. Institucionální zabezpečení a struktura však tomuto potenciálu dle mého názoru neodpovídá a představuje slabinu Aktu. Stejně tak obsahuje Akt mnoho odvážných, přínosných, ale často nedotažených myšlenek (např. problém revokace certifikátu po vzájemném hodnocení). V rámci těchto kapitol jsem se tak pokusil odhadnout, jaký dopad může Akt na stávající podobu certifikace mít, ale je samozřejmě nutné počítat s tím, že se jedná zatím jen o teoretické úvahy a praxe může odhalit úplně jiné problémy. Zároveň byl tak naplněn i dílčí cíl článku, neboť kritické analýze a vyhodnocení slabin byl podroben jak systém Common Criteria, tak i Akt samotný.

[289] „Jak tuto funkci zlepší evropský návrh Aktu o kybernetické bezpečnosti?“

9. POUŽITÉ ZDROJE

9.1 MONOGRAFIE

[1] BASKERVILLE, Richard; STRAUB, Detmar W; GOODMAN, Seymour E. Information Security [online]. Armonk, NY, USA: Routledge, 2008, 297 s. Advances in Management Information Systems [vid. 11. listopad 2018]. ISBN 978-0-7656-1718-7. Získáno z: https://eds.b.ebscohost.com/eds/ebookviewer/ebook/bmxlYmtfXzI3NTUxM19fQU41?sid=00dfa7ac-8a44-4ecf-adbf-3fe96185f3c3@pdc-v-sessmgr03&vid=9&format=EB&rid=1.

[2] CALDER, Alan. Nine steps to success an ISO27001:2013 implementation overview [online]. Ely, Cambridgeshire, U.K.: IT Governance Pub., 2013, 128 s. [vid. 11. listopad 2018]. Získáno z: https://eds.b.ebscohost.com/eds/ebookviewer/ebook/bmxlYmtfXzEyMzI1NDFfX0FO0?sid=00dfa7ac-8a44-4ecf-adbf-3fe96185f3c3@pdc-v-sessmgr03&vid=7&format=EB&rid=1.

[3] HURYCHOVÁ, Klára; SÝKORA, Michal. Compliance programy (nejen) v České republice. Praha, Česká republika: Wolters Kluwer, 2018, 287 s. ISBN 978-80-7552-667-0.

[4] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; CENTRAL SECRETARIAT. Friendship among equals: recollections from ISO's first fifty years. [online]. Geneva: ISO Central Secretariat, 1997, 87 s. [vid. 25. prosinec 2018]. ISBN 978-92-67-10260-3. Získáno z: https://www.iso.org/files/live/sites/isoorg/files/about%20ISO/docs/en/Friendship_among_equals.pdf.

[5] JIRÁSEK, Petr; NOVÁK, Luděk; POŽÁR, Josef. Výkladový slovník kybernetické bezpečnosti. 3., aktualiz. vyd. Praha, Česká republika: Policejní akademie ČR v Praze: Česká pobočka AFCEA, 2015.

[6] KYSELOVSKÁ, Tereza et al. Cofola 2015: Sborník z konference [online]. Edice Scientia. Brno: Masarykova univerzita, 2015, 1081 s. Acta Universitatis Brunensis Iuridica, 532 [vid. 22. listopad 2018]. ISBN 978-80-210-7976-2. Získáno z: https://www.law.muni.cz/sborniky/cofola2015/cofola2015.pdf.

[7] MEHAN, Julie E. CyberWar, CyberTerror, CyberCrime. [online]. 2nd ed. Ely, Cambridge, UK: IT Governance Publishing, 2014, 352 s. [vid. 19. srpen 2018]. ISBN 978-1-905356-48-5. Získáno z: https://eds.b.ebscohost.com/eds/ebookviewer/ebook/bmxlYmtfXzgzODczMF9fQU41?sid=c0a75452-4a36-406f-82ad-2eb06c7ca5c0@pdc-v-sessmgr06&vid=8&format=EB&rid=2.

[8] POLČÁK, Radim; HARAŠTA, Jakub; STUPKA, Václav. Právní problémy kybernetické bezpečnosti [online]. 1. vydání. Brno: Masarykova univerzita, 2016, 215 s. ISBN 978-80-210-8426-1. Získáno z: https://is.muni.cz/auth/repo/1375719/Polcak_kniha2.pdf?fakulta=1422;obdobi=7343;kod=MV735K;predmet=1120828.

[9] SMEDINGHOFF, Thomas J. Information Security Law [online]. Ely, Cambridge, UK: IT Governance Publishing, 2008, 182 s. [vid. 11. říjen 2018]. ISBN 978-1-905356-66-9. Získáno z: https://eds.b.ebscohost.com/eds/ebookviewer/ebook/bmxlYmtfXzM5MTA5NV9fQU41?sid=00dfa7ac-8a44-4ecf-adbf-3fe96185f3c3@pdc-v-sessmgr03&vid=3&format=EB&rid=2.

[10] Technical information on the IT security certification of products, protection profiles and sites [online]. Bonn, Německo: Bundesamt für Sicherheit in der Informationstechnik, 2012, 39 s. [vid. 12. říjen 2019]. Získáno z: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/7138_e_pdf.pdf;jsessionid=28944A61E3001F0324FDE8F91C9B173A.1_cid360?_blob=publicationFile&v=1.

9.2 ČLÁNKY Z ODBORNÝCH PUBLIKACÍ

[11] ALKALBANI, Ahmed et al. Information Security Compliance in Organizations: An Institutional Perspective. Data and Information Management [online]. 2017, roč. 1, č. 2, s. 104–114 [vid. 23. červenec 2018]. ISSN 2543-9251. Získáno z: https://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?vid=28&sid=13ed30fd-ac9c-4f33-80e5-02ccf3fc761e%40sessionmgr4007.

[12] AXELROD, C. Warren. The creation and certification of software cybersecurity standards. In: 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT) [online]. Farmingdale, NY, USA: IEEE, 2016, s. 1–6 [vid. 22. červenec 2018]. ISBN 978-1-4673-8490-2. Získáno z: https://ieeexplore.ieee.org/document/7494112.

[13] BÂRSAN, Mihai. Aspects regarding the implementation of information security standards in organizations. Revista Română de Biblioteconomie și Știința Informării = Romanian Journal of Library and Information Science [online]. 2017, roč. 13, č. 1, s. 21–26 [vid. 29. říjen 2018]. ISSN 18411940, 25595490. Získáno z: doi:10/gfgkt8.

[14] BELLANTUONO, Giuseppe. Comparing Smart Grid Policies in the USA and EU. Law, Innovation and Technology [online]. 2014, roč. 6, č. 2, s. 221–264 [vid. 22. červenec 2018]. ISSN 1757-9961, 1757-997X. Získáno z: https://www.tandfonline.com/doi/full/10.5235/17579961.6.2.221.

[15] COGLIANESE, Cary. The Limits of Performance-Based Regulation. University of Michigan Journal of Law Reform [online]. 2016, roč. 50, č. 3, s. 525–564 [vid. 12. září 2018]. ISSN 0363-602X. Získáno z: https://scholarship.law.upenn.edu/faculty_scholarship/1858/.

[16] COGLIANESE, Cary; LAZER, David. Management-Based Regulation: Prescribing Private Management to Achieve Public Goals. Law & Society Review [online]. 2003, roč. 37, č. 4, s. 691–730 [vid. 12. září 2018]. ISSN 0023-9216, 1540-5893. Získáno z: https://eds.b.ebscohost.com/eds/pdfviewer/pdfviewer?vid=2&sid=45e13b2c-08ac-42fd-94dd-ce0d386287f7 %40pdc-v-sessmgr02.

[17] COGLIANESE, Cary; NASH, Jennifer; OLMSTEAD, Todd. Performance-Based Regulation: Prospects and Limitations in Health, Safety and Environmental Protection. Administrative Law Review [online]. 2003, roč. 55, č. 4, s. 705–730 [vid. 20. září 2018]. ISSN 0001-8368. Získáno z: https://heinonline.org/HOL/Page?handle=hein.journals/admin55&div=29.

[18] D'AMATO, Anthony. Legal Uncertainty. California Law Review [online]. 1983, roč. 71, č. 1, s. 1 [vid. 25. únor 2019]. ISSN 00081221. Získáno z: doi:10/d48z36

[19] HEARN, J. Does the common criteria paradigm have a future? IEEE Security & Privacy Magazine [online]. 2004, roč. 2, č. 1, s. 64–65 [vid. 18. říjen 2018]. ISSN 1540-7993. Získáno z: http://ieeexplore.ieee.org/document/1264857/.

[20] ISA, Mohd Anuar Mat et al. Finest authorizing member of common criteria certification. In: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec) [online]. Kuala Lumpur, Malaysia: IEEE, 2012, s. 155–160 [vid. 22. červenec 2018]. ISBN 978-1-4673-1426-8. Získáno z: http://ieeexplore.ieee.org/document/6246109/.

[21] JEŽOVÁ, Daniela. EU Digital Single Market - Are we there yet? Ad Alta: Journal of Interdisciplinary Research [online]. 2017, roč. 7, č. 2, s. 99–102. ISSN 1804-7890. Získáno z: https://eds.b.ebscohost.com/eds/pdfviewer/pdfviewer?vid=12&sid=f9683978-876b-416a-a2d0-5fa83e889a40 %40sessionmgr120.

[22] KALLBERG, Jan. The Common Criteria Meets Realpolitik: Trust, Alliances, and Potential Betrayal. IEEE Security & Privacy Magazine [online]. 2012, roč. 10, č. 4, s. 50–53 [vid. 22. říjen 2018]. ISSN 1540-7993. Získáno z: http://ieeexplore.ieee.org/document/6148206/.

[23] KALUVURI, Samuel Paul; BEZZI, Michele; ROUDIER, Yves. Bringing Common Criteria Certification to Web Services. In: 2013 IEEE Ninth World Congress on Services (SERVICES) [online]. Santa Clara, CA, USA: IEEE, 2013, s. 98–102 [vid. 22. červenec 2018]. ISBN 978-0-7695-5024-4. Získáno z: http://ieeexplore.ieee.org/document/6655681/.

[24] KANG, Sooyoung; KIM, Seungjoo. How to Obtain Common Criteria Certification of Smart TV for Home IoT Security and Reliability. Symmetry [online]. 2017, roč. 9, č. 10, s. 12 [vid. 22. červenec 2018]. ISSN 2073-8994. Získáno z: https://www.mdpi.com/2073-8994/9/10/233/htm.

[25] KLINKE, Andreas; RENN, Ortwin. A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies. Risk Analysis [online]. 2002, roč. 22, č. 6, s. 1071–1094 [vid. 11. listopad 2018]. ISSN 02724332, 15396924. Získáno z: https://eds.b.ebscohost.com/eds/pdfviewer/pdfviewer?vid=16&sid=00dfa7ac-8a44-4ecf-adbf-3fe96185f3c3%40pdc-v-sessmgr03.

[26] KNEEPKENS, Jules. Performance Based Regulation. In: EASA Safety Conference [online]. B.m. 2012. [vid. 20. září 2018]. Získáno z: https://www.easa.europa.eu/conferences/pbo/doc/presentations/3%20-%20Kneepkens%20EU%20Performance%20Based%20Regulation.pdf.

[27] KOVÁCS, László. Cyber Security Policy and Strategy in the European Union and NATO. Revista Academiei Fortelor Terestre [online]. 2018, roč. 23, č. 1, s. 16–24 [vid. 22. červenec 2018]. ISSN 15826384. Získáno z: https://content.sciendo.com/view/journals/raft/23/1/article-p16.xml.

[28] KRISTENSEN, V.; AVEN, T.; FORD, D. A new perspective on Renn and Klinke's approach to risk evaluation and management. Reliability Engineering & System Safety [online]. 2006, roč. 91, č. 4, s. 421–432 [vid. 11. listopad 2018]. ISSN 09518320. Získáno z: doi:10/db47fv.

[29] MAY, Peter J. Performance-Based Regulation and Regulatory Regimes: The Saga of Leaky Buildings. Law & Policy [online]. 2003, roč. 25, č. 4, s. 381–401 [vid. 22. září 2018]. ISSN 0265-8240, 1467-9930. Získáno z: https://heinonline.org/HOL/Page?handle=hein.journals/lawpol25&div=28.

[30] MERCURI, Rebecca. Uncommon criteria. Communications of the ACM [online]. 2002, roč. 45, č. 1, s. 172–172 [vid. 22. říjen 2018]. ISSN 00010782. Získáno z: http://portal.acm.org/citation.cfm?doid=502269.502310.

[31] MITRAKAS, Andreas. The emerging EU framework on cybersecurity certification. Datenschutz und Datensicherheit [online]. 2018, roč. 42, č. 7, s. 411–414 [vid. 11. září 2018]. ISSN 16140702. Získáno z: https://link.springer.com/content/pdf/10.1007%2Fs11623-018-0969-2.pdf.

[32] RECCHIA, Luca et al. Security Evaluation of a Linux System: Common Criteria EAL4+ Certification Experience. In: 2014 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW) [online]. Naples, Italy: IEEE, 2014, s. 77–81 [vid. 22. červenec 2018]. ISBN 978-1-4799-7377-4. Získáno z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6983806.

[33] TANTAWI, Randa. Common Criteria. Salem Press Encyclopedia [online]. 2013 [vid. 13. září 2018]. Získáno z: https://eds.a.ebscohost.com/eds/detail/detail?vid=1&sid=65cb00d8-2765-434e-802f-29a488b6180b%40sdc-v-sessmgr04&bdata=JkF1dGhUeXBlPWlwLGNvb2tpZSx1aWQmbGFuZz1jcyZzaXRlPWVkcy1saXZlJnNjb3BlPXNpdGU%3d#db=ers&AN=90558266.

9.3 PREZENTACE Z ODBORNÝCH KONFERENCÍ

[34] PRILLER, Christian. Effectively Implementing the EU Certification Framework: Market Perspectives - TÜV-SÜD-AG. In: Effectively Implementing the EU Certification Framework: Market Perspectives [online]. Brusel, Belgie. 2018. [vid. 25. září 2018]. Získáno z: ftp://ftp.cencenelec.eu/EN/News/Events/2018/Cybersecurity_ENISA_CEN_CL_ETSI_Presentations/Christian-PRILLER_T%C3 %9CV-S%C3 %9CD-AG.pdf.

[35] STANTCHEV, Pentcho. Cybersecurity of Industrial Systems. In: Effectively Implementing the EU Certification Framework: Market Perspectives [online]. Brusel, Belgie. 2018. [vid. 25. září 2018]. Získáno z: ftp://ftp.cencenelec.eu/EN/News/Events/2018/Cybersecurity_ENISA_CEN_CL_ETSI_Presentations/Pentcho-STANTCHEV_ORGALIME.pdf.

[36] Baseline Security Product Assessment. In: BlackHat Sessions [online]. Nieuwegein, Nizozemí. 2018. [vid. 25. prosinec 2018]. Získáno z: https://www.blackhatsessions.com/presentaties/2018/BSPA%20-%20BlackHatSessions%2003_1.pdf.

9.4 INTERNETOVÉ STRÁNKY A ZDROJE

[37] ČERMÁK, Miroslav. Regulatorní požadavky představují jen další riziko, a tak je s nimi třeba i zacházet. CleverAndSmart [online]. 2018. [vid. 8. listopad 2018]. Získáno z: https://www.cleverandsmart.cz/regulatorni-pozadavky-predstavuji-jen-dalsi-riziko-a-tak-je-s-nimi-treba-i-zachazet/.

[38] WEBER, Joachim. The German IT Security Certification Scheme [online]. Bonn, Německo: Bundesamt für Sicherheit in der Informationstechnik, 2017, 25 s. [vid. 28. prosinec 2018]. Získáno z: http://www.isccc.gov.cn/zlzx/kyxx/images/2017/09/10/AF5C39A704EA2F5CE84A2D0419EA383C.pdf.

[39] Baseline Security Product Assessment. SECURA [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: https://www.secura.com/pathtoimg.php?id=1326&image=bspa.pdf.

[40] BSI – Certification. Bundesamt für Sicherheit in der Informationstechnik [online] b.n. nedatováno [vid. 12. říjen 2019]. Získáno z: https://www.bsi.bund.de/EN/Topics/Certification/certification_node.html.

[41] Certification CSPN. ANSSI [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: https://ssi.gouv.fr/administration/produits-certifies/cspn/.

[42] Certification. ISO [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/home/standards/certification--conformity/certification.html.

[43] Certified Products List - Statistics. New CC Portal [online] b.n. nedatováno [vid. 12. říjen 2019]. Získáno z: https://www.commoncriteriaportal.org/products/stats/.

[44] Certified Products. NCSC Site [online] b.n. nedatováno [vid. 12. říjen 2019]. Získáno z: https://www.ncsc.gov.uk/index/certified-product?f[0]=field_assurance_scheme%3A226&f[1]=field_assurance_status%3AAssured.

[45] Commercial Product Assurance (CPA). NCSC Site [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa.

[46] Common Criteria. New CC Portal [online] b.n. nedatováno [vid. 12. říjen 2019]. Získáno z: https://www.commoncriteriaportal.org/.

[47] CSPN: What U.S. companies need to know about the security certification process [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: http://www.embedded-computing.com/embedded-computing-design/cspn-what-u-s-companies-need-to-know-about-the-security-certification-process.

[48] Český institut pro akreditaci, o.p.s. ČIA - Národní akreditační orgán [online] b.n. nedatováno [vid. 20. leden 2019]. Získáno z: http://www.cia.cz/.

[49] Členství v mezinárodních organizacích. ÚNMZ [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: http://www.unmz.cz/urad/clenstvi-v-mezinarodnich-organizacich.

[50] Developing standards. ISO [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/home/developing-standards.html.

[51] Foundation Grade explained. NCSC Site [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: https://www.ncsc.gov.uk/articles/foundation-grade-explained.

[52] IAF MEMBERS: Czech Republic. International Accreditation Forum [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: https://www.iaf.nu/articles/IAF_MEM_Czech_Republic/66.

[53] IEC - About the IEC [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: https://www.iec.ch/about/?ref=menu.

[54] ISO/IEC 27001 Information security management. ISO [online] b.n. nedatováno [vid. 24. prosinec 2018]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/home/standards/popular-standards/isoiec-27001-information-securit.html.

[55] ISO/IEC JTC 1/SC 27 - IT Security techniques. ISO [online] b.n. nedatováno [vid. 12. říjen 2019]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/committee/04/53/45306.html.

[56] Les produits CSPN. ANSSI [online] b.n. nedatováno [vid. 12. říjen 2019]. Získáno z: https://ssi.gouv.fr/administration/produits-certifies/cspn/produits-certifies-cspn/.

[57] Members. ISO [online] b.n. nedatováno [vid. 12. říjen 2019]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/home/about-us/members.html.

[58] Members of the CCRA. New CC Portal [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: https://www.commoncriteriaportal.org/ccra/members/#CZ.

[59] O Úřadu - ÚNMZ [online] b.n. nedatováno [vid. 9. únor 2019]. Získáno z: http://www.unmz.cz/urad/o-uradu.

[60] Products and Services Scheme fees. NCSC Site [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: https://www.ncsc.gov.uk/articles/products-and-services-scheme-fees.

[61] Questions and Answers - EU Cybersecurity. European Commission [online] b.n. nedatováno [vid. 12. říjen 2019]. Získáno z: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_19_3369.

[62] SCORM Compliant, SCORM Conformant, SCORM Certified. SCORM.com [online] b.n. nedatováno [vid. 26. říjen 2018]. Získáno z: https://scorm.com/scorm-explained/scorm-resources/conformance-vs-compliance/.

[63] Security Characteristics collection. NCSC Site [online] b.n. nedatováno [vid. 28. prosinec 2018]. Získáno z: https://www.ncsc.gov.uk/document/security-characteristics-collection.

[64] Seznam akreditovaných subjektů pro posuzování shody podle nařízení eIDAS platný ke dni 5. 2. 2019. European Commission - Futurium: eIDAS Observatory [online] b.n. nedatováno [vid. 28. únor 2019]. Získáno z: https://ec.europa.eu/futurium/en/system/files/ged/list_of_eidas_accredited_cabs-2019-02-05.pdf.

[65] SOG-IS - Home. SOG-IS [online] b.n. nedatováno [vid. 12. říjen 2019]. Získáno z: http://sogis.org/index_en.html.

[66] SOG-IS - Status of participants. SOG-IS [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: http://sogis.org/uk/status_participant_en.html.

[67] The ISO Story. ISO [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/home/about-us/the-iso-story.html.

[68] UNMZ. ISO [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/member/00/21/2133.html.

[69] Vybrané výrobky - ÚNMZ [online] b.n. nedatováno [vid. 9. únor 2019]. Získáno z: http://www.unmz.cz/urad/vybrane-vyrobky.

[70] What's the Difference Series: Compliance vs. Certification. Mireaux Management Solutions [online]. 2013. [vid. 26. říjen 2018]. Získáno z: http://mireauxms.com/vanguard-blog/whats-the-difference-series-compliance-vs-certification.

[71] Who develops standards. ISO [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/home/developing-standards/who-develops-standards.html.

9.5 PRÁVNÍ PŘEDPISY

9.5.1 ZÁKONY A VYHLÁŠKY

[72] 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). In: CODEXIS ACADEMIA [právní informační systém]. ATLAS consulting [vid. 6. listopadu 2018].

[73] Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). In: CODEXIS ACADEMIA [právní informační systém]. ATLAS consulting [vid. 6. listopadu 2018].

[74] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: CODEXIS ACADEMIA [právní informační systém]. ATLAS consulting [vid. 6. listopadu 2018].

9.5.2 PRÁVNÍ PŘEDPISY EU

[75] Nařízení Evropského parlamentu a Rady (ES) č. 765/2008 ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93 [online]. Získáno z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32008R0765&from=EN.

[76] Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES [online]. Získáno z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex:32014R0910

[77] Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost"), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 [online]. Získáno z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri = CELEX:32019R0881&from = CS

[78] Návrh nařízení Evropského parlamentu a Rady o agentuře ENISA, Evropské agentuře pro kybernetickou bezpečnost, a zrušení nařízení (EU) č. 526/2013 a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií („akt o kybernetické bezpečnosti") ze dne 20. 12. 2018 [online]. Získáno z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?
uri = CONSIL:ST_15786_2018_INIT&from = EN.

9.5.3 MEZINÁRODNÍ SMLOUVY A SMLOUVY O MEZINÁRODNÍ SPOLUPRÁCI

[79] Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security [online]. 2. červenec 2014. [vid. 12. září 2018]. Získáno z: https://www.commoncriteriaportal.org/files/CCRA%20-%20July %202,%202014 %20-%20Ratified%20September%208 %202014.pdf.

[80] SOG-IS Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, verze 3.0 [online]. 2010. [vid. 27. říjen 2018]. Získáno z: https://www.sogis.eu/documents/mra/20100107-sogis-v3.pdf.

9.6 KVALIFIKAČNÍ PRÁCE

[81] HARAŠTA, Jakub. Princip technologické neutrality v kybernetické bezpečnosti [online]. Brno 2017 [vid. 26. únor 2019]. Disertační práce. Masarykova univerzita, Právnická fakulta. Získáno z: https://is.muni.cz/auth/th/agnuc/Princip_technologicke_neutrality_v_kyberneticke_bezpecnosti.pdf.

9.7 OSTATNÍ ZDROJE

[82] DROGKARIS, Prokopios. Considerations on ICT security certification in EU - Survey Report [online]. 2017. B.m.: European Union Agency for Network and Information Security. Získáno z: https://www.enisa.europa.eu/publications/certification_survey/at_download/fullReport.

[83] GUEBEL, Martine. NANDO Information System (Europa) [online]. [vid. 5. únor 2019]. Získáno z: http://ec.europa.eu/growth/tools-databases/nando/index.cfm?fuseaction = help.main.

[84] HEAD, Katie Bird. ISO workshop on Mutual Recognition Agreements. ISO [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: http://www.iso.org/cms/render/live/en/sites/isoorg/contents/news/1998/04/Ref749.html.

[85] NEGREIRO ACHIAGA, Maria Del Mar. EU Legislation in Progress - Briefing: ENISA and a new cybersecurity act (stav ke dni 16. 1. 2018) [online]. B.m.: European Parliament Research Service. [vid. 11. říjen 2018]. Získáno z: http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614643/EPRS_BRI(2017)614643_EN.pdf.

[86] VYSOKÁ PŘEDSTAVITELKA UNIE PRO ZAHRANIČNÍ VĚCI A BEZPEČNOSTNÍ POLITIKU. Společné sdělení Evropskému parlamentu a Radě ze dne 13. 9. 2017: Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU [online]. 2017. [vid. 11. říjen 2018]. Získáno z: https://publications.europa.eu/en/publication-detail/-/publication/794f8627-985b-11e7-b92d-01aa75ed71a1/language-cs.

[87] Annual Activity Report 2018 [online]. Řecko: European Union Agency for Cybersecurity, 2018, 72 s. [vid. 12. říjen 2019]. ISBN 978-92-9204-297-4. Získáno z: https://www.enisa.europa.eu/publications/corporate-documents/enisa-annual-activity-report-2018.

[88] Commission Staff Working Document: Advancing the Internet of Things in Europe [online]. 2016. B.m.: European Commission. [vid. 12. říjen 2019]. Získáno z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0110&from=EN.

[89] Důvodová zpráva k vyhlášce č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.

[90] Informace o hodnocení bezpečnosti informačních technologií Common Criteria (CC) [online]. 2005. B.m.: Národní bezpečnostní úřad. [vid. 4. leden 2019]. Získáno z: https://www.nbu.cz/download/bezpecnost-informacnich-systemu/container-nodeid-748/infoobit.pdf.

[91] IOCTA: Internet Organised Crime Threat Assessment 2019 [online]. 2019. B.m.: Europol – European Cybercrime Centre. [vid. 12. říjen 2019]. Získáno z: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019.

[92] Joint EC/ENISA SOG-IS and ICT certification workshop – Minutes of the workshop [online]. 6. říjen 2014. [vid. 24. srpen 2018]. Získáno z: https://www.enisa.europa.eu/events/sog-is/minutes/view.

[93] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model [online]. Verze 3.1, páté vydání. B.m.: Common Criteria Management Committee, 2017, 106 s. [vid. 12. září 2018]. Získáno z: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5_marked_changes.pdf.

[94] IoT Cybersecurity Coalition Letter [online]. 16. srpen 2017. Získáno z: https://www.uschamber.com/iot%26cybersecurity.

[95] Pracovní dokument útvarů komise - Souhrn posouzení dopadů k návrhu aktu o kybernetické bezpečnosti [online]. 2017. B.m.: Evropská komise. [vid. 12. červenec 2018]. Získáno z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52017SC0501&from=CS.

[96] Procedure File: 2017/0225(COD). Legislative Observatory | European Parliament [online] b.n. nedatováno [vid. 25. prosinec 2018]. Získáno z: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=&reference=2017/0225(COD)#tab-0.

[97] Report: EU coordinated risk assessment of the cybersecurity of 5G networks [online]. 2019. B.m.: NIS Cooperation Group. [vid. 12. říjen 2019]. Získáno z: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132.

[98] Sdělení Komise Evropskému parlamentu, Radě, EHS-výboru a výboru regionů ze dne 10. 5. 2017 o přezkumu v polovině období provádění strategie pro jednotný digitální trh [online]. 10. květen 2017. B.m.: Evropská komise. [vid. 11. říjen 2018]. Získáno z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52017DC0228&from=EN.

[99] State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks [online]. 19. září 2017. B.m.: European Comission - Press release. [vid. 11. říjen 2018]. Získáno z: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwiK-rnCys3gAhVtRhUIHUkMA5gQFjABegQICBAC&url=http%3A%2F%2Feuropa.eu%2Frapid%2Fpress-release_IP-17-3193_en.pdf&usg=AOvVaw261JlgSpwwQ0lkHOTKTV-A.

[100] Technical information on the IT security certification of products, protection profiles and sites [online]. 2012. B.m.: Bundesamt für Sicherheit in der Informationstechnik. [vid. 12. říjen 2019]. Získáno z: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Certification/7138_e_pdf.pdf?_blob=publicationFile&v=1.