Auditní kompendium

Kybernetická bezpečnost v EU a jejích členských státech: audit odolnosti kritických informačních systémů a digitálních infrastruktur vůči kybernetickým útokům

Auditní zprávy
zveřejněné mezi lety 2014 a 2020

prosinec 2020

Kontaktní výbor vedoucích představitelů nejvyšších kontrolních institucí Evropské unie (EU) nabízí fórum pro diskutování a řešení otázek týkajících se veřejného auditu v EU. Posilováním dialogu a spolupráce mezi svými členy pomáhá výbor účinnějšímu provádění opatření a programů EU v oblasti vnějšího auditu. Pomáhá rovněž zvyšovat odpovědnost, zlepšovat finanční řízení EU a konsolidovat řádnou správu věcí veřejných ve prospěch všech občanů EU.

Kontakt: www.contactcommittee.eu

Obsah

Úvodní slovo 6

Shrnutí 8

ČÁST I – Kybernetická bezpečnost v evropském kontextu 9

Co je to kybernetická bezpečnost? 10

Kybernetická bezpečnost ovlivňuje každodenní život všech občanů EU 10

Existuje celá řada různých typů hrozeb v oblasti kybernetické bezpečnosti 11

Hospodářský dopad kybernetických útoků je značný. 14

S častějšími útoky se zvyšuje i povědomí o kybernetických bezpečnostních hrozbách 18

Kybernetická bezpečnost je důležitá pro sociální soudržnost a politickou stabilitu 19

Kybernetická bezpečnost v EU: pravomoci, aktéři, strategie a právní předpisy 27

Výdaje spojené s kybernetickou bezpečností v EU jsou rozptýlené a pokulhávající 34

Část II – Přehled práce nejvyšších kontrolních institucí 38

Úvod 39

Metodika a témata auditu 39

Auditované období 41

Cíle auditu 41

Hlavní auditní připomínky 45

Část III – Shrnutí zpráv nejvyšších kontrolních institucí 51

Dánsko – *Rigsrevisionen* 52

Ochrana před ransomwarovými útoky 52

Obsah

Estonsko – *Riigikontroll* 56

Zajištění bezpečnosti a ochrana kritických státních databází v Estonsku 56

Irsko – Office of the Comptroller and Auditor General 60

Opatření týkající se národní kybernetické bezpečnosti 60

Francie – *Cour des comptes* 63

Přístup k vysokoškolskému vzdělávání: počáteční posouzení zákona o studijním poradenství a úspěšnosti studia 63

Lotyšsko – *Valsts Kontrole* 69

Využila veřejná správa všech příležitostí k účinnému řízení infrastruktury IKT? 69

Litva – *Valstybės Kontrolė* 72

Řízení kritických státních informačních zdrojů 72

Maďarsko – *Národní kontrolní úřad* 76

Audit ochrany údajů – Audit vnitrostátního rámce na ochranu údajů a některých záznamů prioritních údajů v rámci mezinárodní spolupráce 76

Nizozemsko – *Účetní dvůr* 79

Kybernetická bezpečnost kritických vodních staveb a hraničních kontrol v Nizozemsku 79

Polsko – *Najwyższa Izba Kontroli (NIK)* 84

Zajištění bezpečnosti provozu informačních systémů používaných k plnění veřejných úkolů 84

Portugalsko – *Tribunal de Contas* 89

Audit portugalského elektronického pasu 89

Finsko – *Valtiontalouden tarkastusvirasto* 95

Zajištění kybernetické ochrany 95

Švédsko – *Riksrevisionen* 100

Zastaralé systémy IT – překážka účinné digitalizace 100

Obsah

Evropská – unie *Evropský účetní dvůr* 104

Informační dokument: Výzvy pro účinnou politiku kybernetické bezpečnosti 104

Zkratková slova a zkratky 107

Glosář 109

Úvodní slovo

Vážený čtenáři,

digitalizace a stále rozsáhlejší využívání informačních technologií ve všech oblastech našeho každodenního života otevírají nepřeberné množství nových příležitostí. Spolu s tím se však zároveň zvýšilo riziko, že se jednotlivci, podniky a veřejné orgány stanou obětí kybernetické kriminality nebo kybernetického útoku, jejichž společenské a hospodářské dopady jsou stále citelnější.

V EU je kybernetická bezpečnost výsadou členských států. EU musí hrát roli při vytváření společného regulačního rámce v rámci jednotného trhu EU a při vytváření podmínek pro spolupráci členských států v rámci vzájemné důvěry.

Kybernetická bezpečnost a naše digitální autonomie se staly věcí strategického významu pro EU a její členské státy. V oblasti správy kybernetické bezpečnosti přetrvávají ve veřejném i soukromém sektoru všech členských států nedostatky, i když na různé úrovni. Naše schopnost zamezovat kybernetickým útokům a v případě potřeby na ně reagovat je v důsledku toho narušená. Dezinformace, často organizované ze zemí mimo EU, jsou na vzestupu, jak se opět ukázalo během letošní pandemie onemocnění COVID-19. Dezinformace jsou hrozbou pro sociální soudržnost našich společností a pro důvěru občanů v naše demokratické systémy, hrozbou, kterou nemůžeme ignorovat.

Z průzkumu provedeného v roce 2018 mezi nejvyššími kontrolními institucemi v EU vyšlo najevo, že přibližně polovina z nich se ve svých auditech otázkou kybernetické bezpečnosti dosud nezabývala. Od té doby se však situace změnila a naše nejvyšší kontrolní instituce se na tuto otázku ve své auditní činnosti začaly zaměřovat, přičemž se soustředily především na ochranu údajů, připravenost systému proti kybernetickým útokům a ochranu systémů základních veřejně prospěšných služeb. Je pochopitelné, že výsledky některých těchto auditů nemohou být zveřejněny, protože se mohou týkat (z hlediska národní bezpečnosti) citlivých informací.

Letošní koronavirová krize je zatěžkávací zkouškou hospodářského a sociálního systému našich společností. „Kybernetická krize“ by se vzhledem k naší závislosti na informačních technologiích mohla stát další pandemií. Musíme být připraveni a posílit odolnost kritických informačních systémů a digitálních infrastruktur vůči kybernetickým útokům.

Věříme, že přehled, který nabízí toto kompendium, vyvolá na straně veřejných auditorů v celé Unii ještě větší zájem o tuto zásadně důležitou oblast.

Klaus-Heiner Lehne

předseda Evropského účetního dvora
předseda Kontaktního výboru
a vedoucí projektu

Shrnutí

I Kybernetická bezpečnost a digitální autonomie se staly **věcí strategického významu pro EU a její členské státy** a s rostoucí mírou ohrožení musíme zvýšit úsilí o ochranu našich kritických informačních systémů a digitálních infrastruktur před kybernetickými útoky. Kybernetická bezpečnost se netýká pouze našich veřejných služeb, obrany či systémů zdravotní péče, ale také ochrany našich osobních údajů, obchodních modelů a duševního vlastnictví. Vlastním smyslem kybernetické bezpečnosti je pak ochrana našich demokratických společností, nezávislosti nás jako Evropanů a způsobu našeho společného života.

II V první části tohoto třetího kompendia Kontaktního výboru je vysvětleno, **co všechno s sebou kybernetická bezpečnost nese**. Je v ní popsáno, proč je kybernetická bezpečnost výzvou pro veřejné orgány, podniky i jednotlivce, a upozorňuje také na nový fenomén dezinformací, který představuje stále větší hrozbu pro sociální soudržnost našich společností a demokratických systémů. Objasňuje rovněž pravomoci a aktéry EU v oblasti kybernetické bezpečnosti, její strategii a právní předpisy, jakož i finanční prostředky EU, které jsou v této oblasti k dispozici.

III Ve druhé části kompendia jsou shrnuty **výsledky vybraných auditů provedených dvanácti nejvyššími kontrolními institucemi přispívajících členských států a Evropským účetním dvorem**, které byly zveřejněny v letech 2014 až 2020. Tyto audity se zabývaly důležitými stránkami kybernetické bezpečnosti, jako je ochrana soukromých údajů, integrita vnitrostátních datových center, zabezpečení zařízení veřejně prospěšných služeb a provádění vnitrostátních strategií kybernetické bezpečnosti v širším smyslu.

IV Třetí část kompendia obsahuje **podrobné informativní přehledy o vybraných auditech** spolu se shrnutím dalších auditů týkajících se tématu kybernetické bezpečnosti, které zveřejnily nejvyšší kontrolní instituce.

ČÁST I – Kybernetická bezpečnost v evropském kontextu

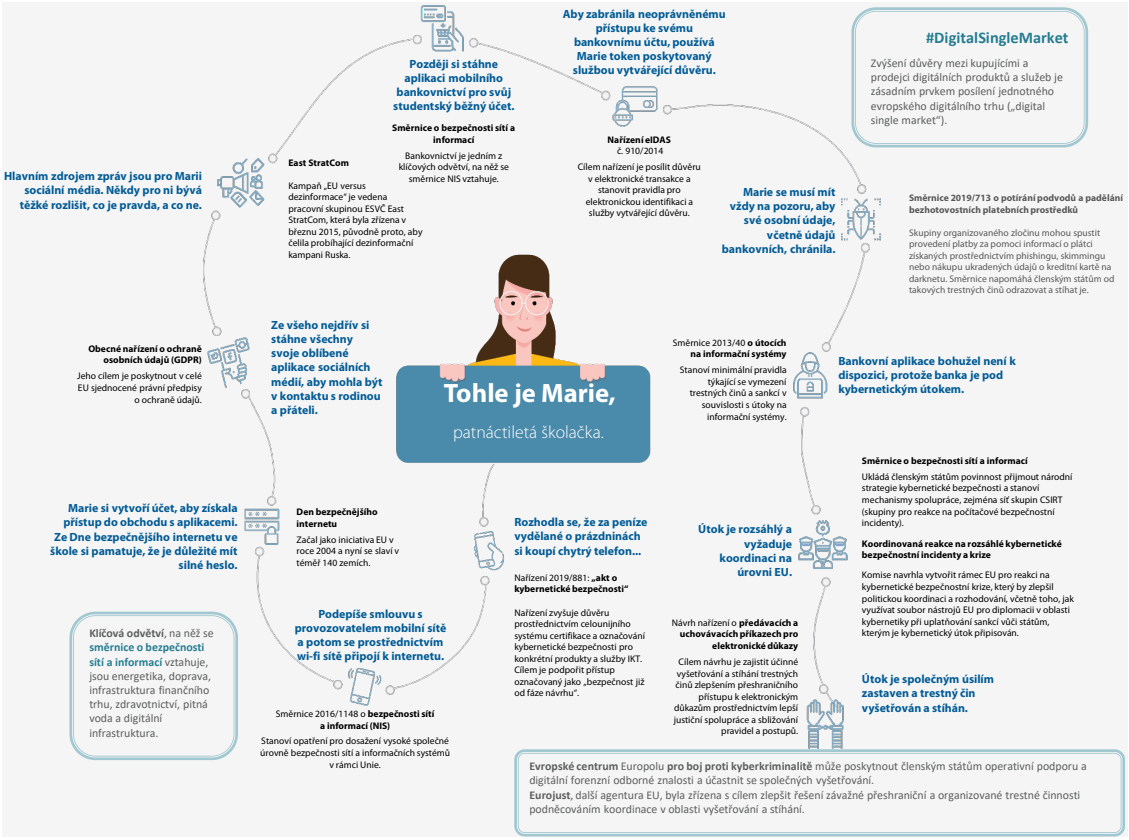
Co je to kybernetická bezpečnost?

01 Neexistuje žádná standardní, obecně platná **definice kybernetické bezpečnosti**. V tomto dokumentu se kybernetickou bezpečností míní vyvíjení **činností nezbytných k ochraně sítí a informačních systémů, jejich uživatelů a dalších osob dotčených kybernetickými hrozbami**. Zahrnuje předcházení kybernetickým incidentům, jejich odhalování, reakci na tyto incidenty a napravování jejich důsledků. Tyto incidenty mohou být úmyslné nebo neúmyslné, od náhodného zveřejnění informací až po útoky na podniky a kritickou infrastrukturu, odcizení osobních údajů, nebo dokonce zasahování do demokratických procesů či zasahování do průběhu voleb nebo obecné dezinformační kampaně, jejichž cílem je ovlivnit veřejnou diskusi.

Kybernetická bezpečnost ovlivňuje každodenní život všech občanů EU

02 Kybernetická bezpečnost ovlivňuje každodenní život všech občanů EU, kdykoli používáme osobní IT zařízení, jako jsou chytré telefony, bezdrátové sítě, sociální média nebo elektronické bankovnictví. V roce 2020 platí víc než kdykoli předtím, že otázka nezní, zda k počítačovým útokům dojde, ale jak a kdy k nim dojde. To se týká nás všech: **jednotlivců, podniků i veřejných orgánů**. *Obrázek 1* znázorňuje způsob, jakým EU podporuje kybernetickou bezpečnost, a rámec vytvořený na ochranu každodenní elektronické činnosti občanů před kybernetickými útoky. Ochrana kritických informačních systémů a digitálních infrastruktur před kybernetickými útoky se stala strategickou výzvou.

Obrázek 1 – EU podporuje kybernetickou bezpečnost v každodenním životě občanů EU

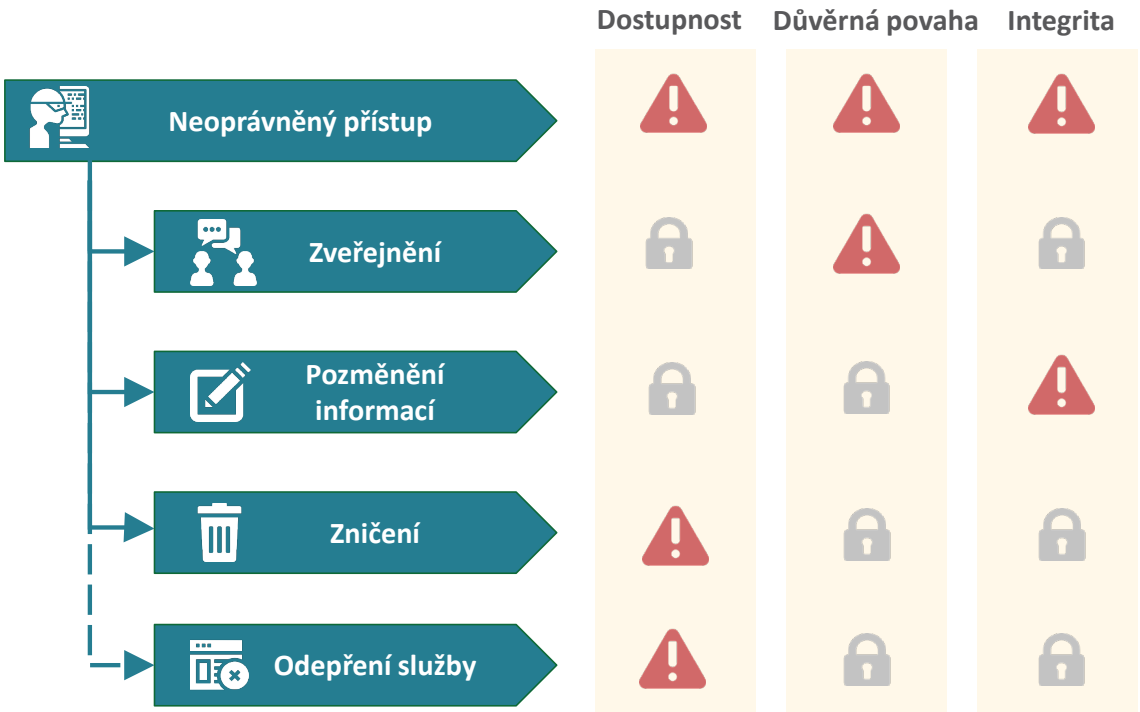


Zdroj: ikony vytvořené Pixel perfect z www.flaticon.com.

Existuje celá řada různých typů hrozeb v oblasti kybernetické bezpečnosti

03 Velké množství různých typů kybernetických bezpečnostních hrozeb, kterým naše společnosti čelí, je možné klasifikovat podle toho jejich **důsledků pro data** – **zveřejnění, změna, zničení nebo odepření přístupu** – nebo podle základních zásad zabezpečení informací, které porušují (viz ***obrázek 1***).

Obrázek 1 – Typy hrozeb a zásady zabezpečení informací, které ohrožují



Zámek = bezpečnost zajištěna; vykřičník = bezpečnost ohrožena

Zdroj: EÚD na základě studie Evropského parlamentu[1].

04 Kdykoli se nějaké zařízení připojí k internetu nebo se spojí s jinými zařízeními, zvětšuje se tzv. prostor ke kybernetickému útoku. Exponenciální růst internetu věcí, cloudů, dat velkého objemu a digitalizace průmyslu jsou doprovázeny nárůstem expozice zranitelných míst, což útočníkům umožňuje zaměřovat se na stále více obětí. V důsledku rozmanitosti typů útoků a jejich rostoucí sofistikovanosti je obtížné udržet krok[2]. V ***rámečku 1*** jsou popsány příklady **možných kybernetických útoků**.

[1] Evropský parlament, *Kybernetická bezpečnost v Evropské unii a ve světě: zkoumání hrozeb a jejich řešení*, Studie pro výbor LIBE, září 2015.

[2] ENISA, *ENISA Threat Landscape Report 2017* (ENISA, Situační zpráva o hrozbách), 18. ledna 2018.

Rámeček 1

Druhy kybernetických útoků

Malware (škodlivý software) je navržen tak, aby poškozoval zařízení nebo sítě. Může jít o viry, trojské koně, ransomware, červy, adware a spyware (např. NotPetya).

Ransomware šifruje údaje, brání uživatelům v přístupu k vlastním souborům, dokud není zaplaceno výkupné, zpravidla v kryptoměně, nebo proveden určitý krok. Podle Europolu jsou útoky ransomware převládajícím typem útoku a v posledních několika letech došlo doslova k explozi počtu druhů ransomware (např. Wannacry[3]).

Dochází také k nárůstu útoků **distribuovaného odepření služby** (DDoS), které znepřístupňuje služby nebo zdroje tím, že je zaplaví větším množstvím požadavků, než jsou schopny zvládnout. K tomuto typu útoku došlo v roce 2017 u jedné třetiny organizací[4].

Útoky vedené z webových stránek jsou oblíbenou metodou jejich pachatelů, kteří mohou tímto způsobem zneužívat uživatele těchto webových systémů a služeb bez jejich vědomí jako vektory útoků. Prostor pro takové útoky je rozsáhlý. Snadno může například docházet k tomu, že škodlivé adresy URL nebo skripty nasměrují uživatele nebo oběť na kýženou internetovou stránku, nebo ke stažení škodlivého obsahu (útoky typu watering hole či drive-by) či k **vložení** škodlivého kódu do legitimních, avšak málo chráněných internetových stránek, který umožní neoprávněně získávat informace (tzv. formjacking) za účelem finančního zisku nebo za účelem krádeže informací[5].

Uživatelé mohou být vmanipulováni do nechtěného provedení určité akce nebo do zveřejnění důvěrných informací. Tento trik může být použit pro krádež údajů nebo kybernetickou špionáž a je známý jako **sociální inženýrství**. Existují různé způsoby, jak toho dosáhnout, ale běžnou metodou je phishing, kdy e-maily, které vypadají, jako by pocházely z důvěryhodných zdrojů, vybízejí uživatele k odhalení informací nebo kliknutí na odkazy, které pak infikují zařízení staženým malwarem. Více než polovina členských států informovala o vyšetřování těchto síťových útoků[6].

Snad nejnekalejším typem hrozeb jsou **pokročilé trvalé hrozby** (APT). Jejich původci jsou sofistikovaní útočníci zabývající se dlouhodobým sledováním a krádežemi údajů, kteří někdy mají destruktivní záměry. Jejich cílem je zůstat co nejdéle v utajení. Pokročilé trvalé hrozby mají často vazby na stát a zaměřují se na obzvláště citlivá odvětví, jako jsou technologie, obrana a kritická infrastruktura. Tento typ **kybernetické špionáže** údajně představuje nejméně jednu čtvrtinu všech kybernetických bezpečnostních incidentů[7].

Hospodářský dopad kybernetických útoků je značný.

05 Hrozba **kybernetických útoků a kybernetické kriminality** se v posledních letech stala vážným problémem. Již v roce 2016 mělo 80 % podniků v EU zkušenost nejméně s jedním kybernetickým bezpečnostním incidentem[8]. V roce 2018 uvedlo 40 % respondentů z organizací využívajících robotiku nebo automatizaci, že nejkritičtějším důsledkem kybernetického útoku na jejich systémy by bylo přerušení provozu. Navzdory povědomí o zásadních kybernetických rizicích však společnosti často nemají žádný systém, který by je před těmito riziky chránil[9].

06 Počet kybernetických útoků, jejich závažnost i finanční náklady s nimi spojené se od té doby zvyšují. Lze odhadovat, že **finanční dopady** kybernetické kriminality pro světovou ekonomiku budou **do roku 2021 dosahovat 6 bilionů USD** ročně ve srovnání s odhadovanými náklady ve výši 3 bilionů USD v roce 2015[10], přičemž odhadovaný celosvětový HDP dosahoval v roce 2020 výše 138 bilionů USD. Náklady na

---

[3] Ransomware *Wannacry* využíval zranitelná místa v protokolu Microsoft Windows umožňující vzdálené převzetí jakéhokoli počítače. Poté, co společnost Microsoft tato slabá místa objevila, vydala opravné řešení. Stovky tisíc počítačů však nebyly aktualizovány a mnoho z nich bylo následně infikováno. *Zdroj:* A. Greenberg, *Hold North Korea Accountable For Wannacry—and the NSA, too*, WIRED, 19. prosince 2017.

[4] Europol, *Internet Organised Crime Threat Assessment 2018* (Posouzení hrozeb organizované trestné činnosti na internetu za rok 2018).

[5] ENISA, *ENISA Threat Landscape 2020 – Web-based attacks* (Situační zpráva o hrozbách z roku 2020 – internetové útoky), 20. října 2020.

[6] Europol, viz výše, 2018.

[7] Evropské středisko pro politickou ekonomii, *Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?* (O krok napřed: dovolíme kybernetické špionáži zbrzdit Evropu v globálním soupeření o průmyslovou konkurenceschopnost?), příležitostný dokument č. 2/18, únor 2018.

[8] Europol, *Internet Organised Crime Threat Assessment 2017* (Posouzení hrozeb organizované trestné činnosti na internetu za rok 2017).

[9] PWC, Global State of Information Security (GSISS), *Survey – Strengthening digital society against cyber shocks* (Průzkum – zvyšování odolnosti digitální společnosti proti kybernetickým otřesům), 2017.

[10] Cybersecurity Ventures, *2019 Official Annual Cybercrime Report* (oficiální výroční zpráva o kybernetické kriminalitě za rok 2019) sponzorovaná skupinou Herjavec, 2019.

kybernetickou kriminalitu zahrnují poškození a zničení údajů, odcizení peněz, ztrátu produktivity, krádeže duševního vlastnictví, krádeže osobních a finančních údajů, následné narušení běžného obchodního styku, poškození dobrého jména. Evropská rada pro systémová rizika (ESRB) odhaduje, že průměrné náklady na kybernetické incidenty se mezi lety 2015 a 2020 zvýšily o 72 %[11].

07 Nedávná studie z roku 2020[12] ukazuje, že **kybernetická kriminalita má na různá hospodářská odvětví různé dopady**: ve vládě a veřejné správě, v odvětví technologií, sdělovacích prostředků a telekomunikací a ve zdravotnictví představovala nejrušivější podvodný fenomén (viz ***rámeček 2***); byla také druhým nejrušivějším podvodným fenoménem ve finančním sektoru a v průmyslovém a výrobním sektoru.

Rámeček 2

Finští psychoterapeutičtí pacienti vydíraní na základě osobních zdravotních údajů odcizených v letech 2018 a 2019

Pacienti jedné velké finské psychoterapeutické kliniky s pobočkami v celé zemi byli v roce 2020 jednotlivě kontaktováni a vydíráni na základě jejich osobních údajů, které byly v listopadu 2018 odcizeny, přičemž k dalšímu možnému narušení ochrany došlo v březnu 2019. Zdá se, že tyto údaje zahrnovaly osobní záznamy a poznámky o rozhovorech probíhajících v rámci léčby.

Klinika i pacienti byli vyzváni, aby výkupné za nezveřejnění údajů zaplatili vyděračovi měnou bitcoin. Tato událost vedla finskou vládu k uspořádání mimořádného zasedání[13].

---

[11] ESRB, European Systematic Risk Board, *Systemic cyber risk* (Systémová kybernetická rizika), únor 2020.

[12] PWC, *Fighting fraud: A never-ending battle PwC's Global Economic Crime and Fraud Survey* (Boj proti podvodům: nekonečný boj), průzkum PWC zaměřený na celosvětovou hospodářskou kriminalitu a podvody) 2020.

[13] BBC News, *Therapy patients blackmailed for cash after clinic data breach* (Pacienti vydíráni na základě odcizených údajů o jejich psychoterapii), 26. října 2020.

08 V roce 2019 EUROPOL[14] opětovně zdůraznil, že **řada zásadních hrozeb v oblasti kybernetické kriminality stále trvá a nijak neslábne:**

- hlavní hrozbou jsou stále útoky s použitím softwaru požadujícího výkupné (tzv. ransomware); útoky bývají přesněji zacílené, výnosnější a způsobují větší hospodářské škody. Dokud bude ransomware poskytovat pachatelům kybernetické trestné činnosti relativně snadný příjem a způsobovat tak jako doposud významné škody a finanční ztráty, je pravděpodobné, že zůstane největší hrozbou v oblasti kybernetické kriminality;
- nejdůležitějšími primárními cestami pronikání malwaru jsou phishing a zranitelné protokoly ovládání vzdálené plochy (RDP);
- klíčovým cílem, komoditou a faktorem umožňujícím kybernetickou kriminalitu jsou údaje.

09 Podobně Agentura Evropské unie pro kybernetickou bezpečnost (ENISA) ve své **zprávě z roku 2020 nazvané „Nejvýznamnější incidenty v EU a ve světě“**[15] uvádí řadu příkladů kybernetických bezpečnostních incidentů (viz ***rámeček 3***).

[14] EUROPOL, *INTERNET organised crime threat assessment (IOCTA)* (Posouzení hrozeb organizované trestné činnosti (IOCTA) na internetu), 2019.

[15] ENISA, *Main incidents in the EU and worldwide – January 2019 to April 2020* (Nejvýznamnější incidenty v EU a ve světě) – leden 2019 až duben 2020, říjen 2020.

Rámeček 3

Agentura Evropské unie pro kybernetickou bezpečnost (ENISA): kybernetické bezpečnostní incidenty v období 2019–2020

K závažnému narušení ochrany údajů v důsledku používání nechráněné databáze MongoDB došlo na platformě pro elektronickou poštu verification.io. Útočník tak získal přístup k údajům z více než 800 milionů e-mailů, které obsahovaly citlivé informace, jejichž součástí byly i informace, které bylo možno ztotožnit (PII).

Na oblíbeném hackingovém fóru, které hostí cloudová služba MEGA1, získal útočník přístup k více než 770 milionům e-mailových adres a 21 milionu jedinečných hesel. Stal se v historii vůbec nejvýznamnějším souborem osobních údajů získaných na základě narušení jejich ochrany, který byl nazván „Soubor #1“.

Obětí cíleného kybernetického útoku se stal i poskytovatel cloudových a virtualizačních služeb Citrix. Přístup k systémům společnosti Citrix získali útočníci tím, že využili několika kritických slabin softwaru, jako je CVE-2019–19781, a použili techniku mnohočetné aplikace častých hesel, zvanou password spraying.

Poskytovatel cloudových služeb iNSYNQ19 se stal předmětem útoku za použití ransomware, který jeho zákazníkům znemožnil přístup k jejich údajům na více než týden, takže museli využívat své lokální zálohy.

10 Podle Europolu se kybernetické útoky, jejichž účelem je způsobit **trvalé škody**, během prvních šesti měsíců roku 2019 zdvojnásobily, a to zejména ve výrobním odvětví. Na rozdíl od konvenčních útoků za pomoci ransomware se jedná o sabotáž, která trvale vymazává nebo jinak nevratně poškozuje údaje společnosti (viz ***rámeček 4***).

Rámeček 4

Destruktivní ransomware – útoky typu „Germanwiper“ uskutečněné v roce 2019

V roce 2019 byla zjištěna řada útoků za pomoci ransomware, které cílily na společnosti působící v Německu. Ransomware, označovaný jako *Germanwiper*, dokáže nahradit infikované soubory nulami a jedničkami a znemožnit tak jejich obnovení. Ransomware se šíří prostřednictvím e-mailových phishingových kampaní a zejména pak cíleným kontaktováním zaměstnanců působících v oddělení lidských zdrojů v předních společnostech, neboť byl začleněn do falešných žádostí o zaměstnání[16].

S častějšími útoky se zvyšuje i povědomí o kybernetických bezpečnostních hrozbách

11 Až donedávna bylo ovšem povědomí o těchto rizicích a pochopení jejich závažnosti poměrně nízké. V roce 2017 nemělo 69 % společností v EU žádnou nebo pouze základní představu o tom, do jaké míry **jsou vystaveny kybernetickým hrozbám**[17], a 60 % z nich nikdy neprovedlo odhad **potenciálních finančních ztrát**[18]**.** Navíc podle globálního průzkumu z roku 2018 by jedna třetina organizací raději zaplatila hackerovi výkupné, než aby investovala do informační bezpečnosti[19].

[16] Cybersecurity Insiders, *GermanWiper Ransomware attack warning for Germany* (Útoky prostřednictvím ransomware GermanWiper – varování pro Německo), nedatováno.

[17] Evropská komise, *Informativní přehled o kybernetické bezpečnosti*, září 2017.

[18] Tyto náklady mohou zahrnovat: ztrátu příjmů, náklady na opravu poškozených systémů, případné závazky spojené s krádeží aktiv nebo informací, pobídky k udržení zákazníků, vyšší pojistné, zvýšené náklady na ochranu (nové systémy, zaměstnanci, odborná příprava), případné vypořádání nákladů na soulad nebo soudní spory.

[19] NTT Security, *Risk: Value 2018 Report* (Riziko: hodnotová zpráva za rok 2018).

12 **Průzkum Eurobarometr provedený v roce 2020** a nazvaný **„Postoj Evropanů ke kybernetické bezpečnosti“**[20] poukazuje na rostoucí povědomí a obavy občanů EU:

- respondenti využívající internet se nejčastěji obávají zneužití svých osobních údajů (46 %), bezpečnosti svých plateb on-line (41 %), dále toho, že nemohou ověřit stav zboží nebo požádat o radu skutečnou osobu, nebo uvádějí, že se obávají nedoručení zboží či neposkytnutí služby, které nakupují on-line (v obou případech 22 %);
- více než tři čtvrtiny (76 %) respondentů se domnívají, že riziko, že se stanou obětí kybernetické kriminality, vzrůstá. Mnohem méně z nich (52 %) si však myslí, že se proti němu mohou dostatečně chránit – což ve srovnání s rokem 2018 představuje pokles o devět procentních bodů.
- o něco více než polovina respondentů (52 %) se však domnívá, že jsou o kyberkriminalitě dobře informováni, ale pouze 11 % uvádí, že se cítí být velmi dobře informováni.

Kybernetická bezpečnost je důležitá pro sociální soudržnost a politickou stabilitu

Nová hrozba: kybernetická bezpečnost a dezinformace

13 Šíření velkého množství záměrných a systematických **dezinformací je pro naše demokracie naléhavou strategickou výzvou**[21]. Dezinformace a falešné zprávy („fake news“) mohou rozdělovat společnosti, zasévat nedůvěru, ale i podrývat sociální soudržnost a důvěru v demokratické procesy (viz ***rámeček 5***).

[20] Evropská komise, *Special Eurobarometer 499 – Europeans' attitudes towards cyber security*, leden 2020.

[21] Podle studie *The Global Disinformation Order*, kterou vypracovala Univerzita v Oxfordu (září 2019), se počet zemí s politickými dezinformačními kampaněmi v posledních dvou letech více než zdvojnásobil na 70.

Rámeček 5

Dezinformace

Evropská komise definuje dezinformace jako vytváření, prezentaci a šíření prokazatelně falešných nebo zavádějících informací za účelem ekonomického prospěchu nebo úmyslného klamání veřejnosti, pokud může přivodit veřejnou újmu[22]. Veřejná újma může zahrnovat narušení demokratických procesů nebo veřejných statků, jako např. zdraví, životního prostředí nebo bezpečnosti.

Na rozdíl od nezákonného obsahu (který zahrnuje nenávistné projevy, teroristický obsah nebo materiál zobrazující pohlavní zneužívání dětí) je obsah, který přinášejí dezinformace, legální. Dezinformace se proto protínají se základními hodnotami EU, jimiž jsou svoboda projevu a svoboda sdělovacích prostředků. Podle definice Komise mezi dezinformace nepatří klamavá reklama, chyby ve zpravodajství, satira a parodie ani předpojaté zprávy a komentáře, které se jako vyhraněné jasně identifikují.

14 Nové technologie a software umožňují snadno a relativně levně šířit dezinformace prostřednictvím **sociálních a jiných médií provozovaných online**. Dezinformace se obvykle soustřeďují na citlivá témata, která mohou polarizovat veřejné mínění a vyvolávat emoce, a proto budou s větší mírou pravděpodobnosti sdílena. Mezi tato témata patří otázky zdraví (např. kampaně proti očkování), migrace, změna klimatu nebo otázky sociální spravedlnosti.

Dezinformační kampaně třetích zemí vedené snahou ovlivnit demokratické procesy

15 Cílem dezinformací je polarizovat demokratickou diskusi, vytvářet nebo zintenzivňovat napětí ve společnosti a narušovat volební systémy a získávat širší dopad na evropské společnosti a na evropskou bezpečnost. Ve svém důsledku narušují svobodu přesvědčení a projevu. Dezinformace jsou často **sponzorovány aktéry ze třetích zemí**, jejichž cílem je destabilizovat naše společnosti a demokratické systémy. V této souvislosti může být součástí rozsáhlých dezinformačních kampaní také internetové hackerství. Příkladem je kampaň prosazující ruský vliv na referendum Spojeného království o vystoupení z Evropské unie (viz *rámeček 6*).

[22] Evropská komise, *Sdělení o boji proti dezinformacím na internetu*, COM(2018) 236.

Rámeček 6

Ruské dezinformační kampaně zaměřené na demokratické rozhodovací procesy[23]

V polovině roku 2016 zahájili ruští aktéři kampaň, jejímž cílem bylo ovlivnit referendum ve Spojeném království o vystoupení z EU, které se konalo v červnu 2016. Z jedné analýzy tweetů vyplynulo, že během 48 hodin před hlasováním více než 150 000 ruských účtů tweetovalo na téma *#Brexit* a zveřejnilo více než 45 000 zpráv o hlasování. V den referenda ruské účty tweetovaly 1 102 krát s hashtagem *#ReasonsToLeaveEU*.

16 Boj proti dezinformacím představuje velkou výzvu, protože vyžaduje nalezení správné rovnováhy mezi bezpečností a našimi základními právy a svobodami, podporou inovací a otevřeným trhem. EU přijala řadu opatření, která mají **problém dezinformací řešit**.

- V roce 2015 byla vytvořena **pracovní skupina East StratCom** se základnou v ESVČ, která vyzývá k boji proti ruským dezinformačním kampaním[24]. Odborníci ocenili její práci při prosazování politik EU, podpoře nezávislých sdělovacích prostředků v zemích evropského sousedství a předvídání, sledování a potírání dezinformací[25].

[23] Park advisors, *Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age* (Zbraně hromadného matení: dezinformace sponzorované cizími státy v digitálním věku), Christina Nemr a William Gangware, 2019.

[24] Závěry Evropské rady, EUCO 11/15, 20. března 2015. Od té doby přibyly dvě další pracovní skupiny: pro západní Balkán a pro jižní sousedství.

[25] Zpráva Atlantické rady vyzvala EU, aby požadovala od všech členských států, aby do pracovní skupiny vyslaly své vlastní odborníky. Viz: D. Fried a A. Polyakova, *Democratic Offense Against Disinformation* (Demokratická obrana proti dezinformacím), 5. března 2018.

- V roce 2018 vydala ENISA **sdělení o boji proti dezinformacím na internetu**[26]**.** Opatření zahrnují pomoc při zvyšování důvěryhodnosti obsahu a podporu úsilí o zvyšování mediální a zpravodajské gramotnosti.

- Společné výzkumné středisko Komise vypracovalo dobrovolný, **seberegulační kodex chování** založený na stávajících politických nástrojích, který byl přijat online platformami a reklamním průmyslem[27].

- Byla vytvořena nezávislá evropská **síť ověřovatelů faktů**.

Dezinformace v dobách pandemie COVID-19 a odezvy EU na ně

17 Dezinformace jsou rovněž problémem v souvislosti se zdravotní **krizí způsobenou onemocněním COVID-19**[28] (viz ***rámeček 7***, kde jsou uvedeny příklady takových dezinformací).

[26] ENISA, *Strengthening Network & Information Security & Protecting Against Online Disinformation („Fake News")* (Posílení síťové a informační bezpečnosti a ochrana proti dezinformacím šířeným po internetu), duben 2018.

[27] Společné výzkumné středisko, *The digital transformation of news media and the rise of disinformation and fake news* (Digitální transformace zpravodajských médií a nárůst dezinformací a falešných zpráv), Technické zprávy SVS, pracovní dokument SVS k digitální ekonomice 2018-02, duben 2018.

[28] Reuters Institute and University of Oxford, *Types, Sources, and Claims of Covid-19 Misinformation* (Typy, zdroje a obsah klamných informací o onemocnění COVID-19), duben 2020.

Rámeček 7

Příklady dezinformací týkajících se onemocnění COVID-19 uvedené ve zprávě Komise[29]

Nepravdivá tvrzení, např. že „lze onemocnění způsobené koronavirem léčit pitím bělicích prostředků nebo čistého alkoholu“: naopak, pitím bělidla nebo čistého alkoholu si lze způsobit závažnou újmu na zdraví. **Belgické toxikologické informační středisko zaznamenalo 15% zvýšení počtu případů souvisejících s konzumací bělicích látek.**

Konspirační teorie, jako je tvrzení, že koronavirus je „infekce vytvořená světovými elitami v zájmu snížení růstu populace“. Vědecké důkazy jsou jasné: jedná se o virus z čeledi virů pocházejících ze zvířat, do níž patří i další viry, jako je SARS či MERS.

Nevědecká tvrzení, že „stanice 5G by mohly být využívány k šíření viru“. Tyto teorie však nebyly podloženy žádnými konkrétními důkazy a vedly k útokům na vysílače.

18 V březnu 2020 vydaly Komise, agentura ENISA, skupina CERT-EU a EUROPOL **společné prohlášení o hrozbách souvisejících s onemocněním COVID-19**[30], v němž se uvádí, že nepřátelští aktéři aktivně využívají náročné podmínky, které jsou spojeny s krizí v oblasti veřejného zdraví, a zaměřili se na pracovníky pracující na dálku, podniky i jednotlivce. Agentura ENISA navíc připravila cílené informační kampaně pro odvětví zasažená dezinformacemi během pandemie COVID-19[31].

---

[29] Evropská komise, *Tackling coronavirus disinformation* (Boj proti dezinformacím o koronaviru), nedatováno.

[30] Společné prohlášení Evropské komise, agentury ENISA, skupiny CERT-EU a Europolu, *Coronavirus outbreak* (Šíření koronaviru), 20. března 2020.

[31] ENISA, *Informační listy týkající se onemocnění COVID-19*, 2020.

Zásadní význam pro boj proti dezinformacím má ověřování faktů

19 EU rovněž zintenzivnila své úsilí v oblasti podpory evropských ověřovatelů faktů a výzkumných pracovníků zabývajících se problematikou dezinformací. Zřídila především **Evropské středisko pro sledování digitálních médií**, které má zkoumat jednotlivé fenomény týkající se dezinformací a lépe jim porozumět, jako jsou jejich aktéři, nosiče, nástroje, metody, dynamika jejich šíření, přednostní cíle a dopady na společnost. Dalšími příklady projektů financovaných z prostředků EU a zaměřených na boj proti dezinformacím jsou projekty PROVENANCE, SocialTruth, EUNOMIA a WeVerify.

20 V roce 2018 navrhla EU v rámci svého **kodexu zásad boje proti dezinformacím**[32] první celosvětový seberegulační soubor norem pro boj proti dezinformacím. V říjnu 2018 podepsaly tento dobrovolný kodex platformy, přední sociální sítě, zadavatelé reklamy a reklamní průmysl. Jeho signatáři jsou Facebook, Twitter, Mozilla, Google a sdružení a členové reklamního průmyslu. Společnost Microsoft se ke kodexu připojila v květnu 2019. Síť TikTok se k tomuto kodexu připojila v červnu 2020.

Zabezpečení voleb do Evropského parlamentu v roce 2019

21 Legitimita našich evropských demokratických systémů je založena na informovaných voličích, kteří vyjadřují svou demokratickou vůli prostřednictvím **svobodných a spravedlivých voleb**. Jakýkoli pokus zlovolně a úmyslně podrývat základy veřejného mínění proto představuje vážnou hrozbu pro naši společnost. Zasahování do voleb a volební infrastruktury může mít za cíl ovlivnit preference voličů, volební účast nebo samotný volební proces, včetně skutečného hlasování, sčítání hlasů a komunikace. Po referendu ve Spojeném království byla v souvislosti s konáním voleb do Evropského parlamentu v roce 2019 přijata první koordinovaná opatření mezi členskými státy na **ochranu integrity demokratických voleb**: voleb do Evropského parlamentu, ale i voleb do vnitrostátních parlamentů.

22 Jak již bylo uvedeno výše, v dubnu 2018 vydala Komise **sdělení o boji proti dezinformacím na internetu: evropský přístup**[33]. Po něm v září 2018 následoval

[32] *Evropský kodex zásad boje proti dezinformacím*, září 2018.

[33] Evropská komise, *Boj proti dezinformacím na internetu: evropský přístup*, COM(2018) 236 final.

„volební balíček“[34], jehož účelem bylo zajistit ochranu voleb do EU a volby v členských státech před dezinformacemi a kybernetickými útoky. Balíček se zaměřil na ochranu údajů, transparentnost politické reklamy a financování, kybernetickou bezpečnost a volby, ale i na sankce za porušování pravidel pro ochranu údajů politickými stranami. Kromě toho proběhlo **společné cvičení**, jehož cílem bylo vyzkoušet účinnost reakce členských států a EU a jejich krizových plánů EU z hlediska zajištění ochrany voleb do Evropského parlamentu (viz ***rámeček 8***).

[34] European Commission, *Projev o stavu Unie v roce 2018*, září 2018.

Rámeček 8

ELEx19 – ochrana voleb do Evropského parlamentu v roce 2019[35]

Cílem průzkumu ELex19 zaměřeného na odolnost nadcházejících voleb do Evropského parlamentu bylo určit způsoby prevence, odhalování a zmírňování kybernetických bezpečnostních incidentů, které mohly mít dopad na volby v roce 2019.

Na základě různých scénářů kybernetických hrozeb a incidentů měli účastníci tohoto cvičení možnost:

— získat přehled o míře odolnosti (na základě přijatých politik, dostupných schopností a dovedností) volebních systémů v celé EU;

— posílit spolupráci mezi příslušnými orgány na vnitrostátní úrovni (včetně volebních orgánů a dalších příslušných subjektů a agentur);

— prověřit stávající plány krizového řízení, jakož i příslušné postupy pro prevenci, odhalování a zvládání kybernetických bezpečnostních útoků a hybridních hrozeb, včetně dezinformačních kampaní, a odezvy na ně;

— zlepšit přeshraniční spolupráci a posílit propojení s příslušnými skupinami pro spolupráci na úrovni EU (např. sítí pro volební spolupráci, skupinou pro spolupráci v oblasti bezpečnosti sítí a informací (NIS), skupinami pro reakce na počítačové bezpečnostní incidenty (CSIRT));

— určit všechny případné další nedostatky, jakož i vhodná opatření ke zmírnění rizik, která by měla být před volbami do Evropského parlamentu provedena.

Tohoto cvičení se zúčastnilo více než 80 zástupců členských států EU spolu s pozorovateli z Evropského parlamentu, Komise a Agentury EU pro kybernetickou bezpečnost.

[35] ENISA, *EU Member States test their cybersecurity preparedness for fair and free 2019 EU elections* (Členské státy EU prověřují svou připravenost v oblasti kybernetické bezpečnosti na spravedlivé a svobodné volby do Evropského parlamentu v roce 2019), 5. dubna 2019.

23 V prosinci 2018 přijala Evropská rada **akční plán proti dezinformacím**[36], který měl zajistit koordinovanou odezvu a doplnit úsilí členských států. Tento plán zahrnoval konkrétní opatření spočívající na čtyřech pilířích: zlepšení schopností orgánů EU odhalovat, analyzovat a zveřejňovat dezinformace; posílení koordinovaných a společných reakcí na dezinformace; mobilizace soukromého sektoru k boji proti dezinformacím; zvyšování povědomí a odolnosti společnosti.

Kybernetická bezpečnost v EU: pravomoci, aktéři, strategie a právní předpisy

Kybernetická bezpečnost je primárně odpovědností členských států

24 Kybernetická bezpečnost je v EU v prvé řadě **odpovědností členských států**. Platí to zejména pro ochranu citlivých informací týkajících se národní bezpečnosti. Všechny členské státy mají **národní strategii kybernetické bezpečnosti**, s jejíž pomocí řeší rizika, která by mohla ohrozit využívání hospodářských a sociálních přínosů kybernetického prostoru. Mezi členskými státy však stále existují rozdíly, pokud jde o jejich kapacitu a závazky v oblasti kybernetické bezpečnosti.

25 EU se musí podílet na budování **společného regulačního rámce** v rámci jednotného trhu EU a na vytváření podmínek pro účinnou spolupráci členských států v různých oblastech politiky, které jsou významné z hlediska kybernetické bezpečnosti, jako je oblast spravedlnosti, vnitra, jednotného trhu, dopravy, veřejného zdraví, spotřebitelské politiky a výzkumu. V zahraniční politice je kybernetická bezpečnost jedním z témat diplomacie a ve stále větší míře je také součástí vznikající obranné a bezpečnostní politiky EU.

26 Hlavní **aktéři** v oblasti kybernetické bezpečnosti **na úrovni EU** jsou popsáni níže v ***rámečku 9***.

---

[36] Evropská komise, vysoká představitelka Unie pro zahraniční věci a bezpečnostní politiku, *Akční plán proti dezinformacím*, JOIN(2018) 36 final. Plán se zaměřuje na zlepšení schopností orgánů EU odhalovat, analyzovat a zveřejňovat dezinformace, na posílení koordinovaných a společných reakcí, na mobilizaci soukromého sektoru, na zvyšování povědomí a zlepšení odolnosti společnosti.

Rámeček 9

Hlavní aktéři v oblasti kybernetické bezpečnosti na úrovni EU

Cílem **Evropské komise** je rozšířit schopnosti a spolupráci v oblasti kybernetické bezpečnosti, posílit EU jako aktéra v oblasti kybernetické bezpečnosti a začlenit kybernetickou bezpečnost do dalších politik EU.

Komisi v tomto ohledu podporuje řada agentur EU, zejména **ENISA**, **EC3** a **CERT-EU**. **Agentura Evropské unie pro kybernetickou bezpečnost** (známá pod zkratkou ENISA podle svého původního názvu Evropská agentura pro bezpečnost sítí a informací) je především poradním orgánem, který podporuje rozvoj politik, budování kapacit a osvětu. Za účelem posílení odezvy EU na kyberkriminalitu v oblasti vymáhání práva bylo zřízeno **Evropské centrum Europolu pro boj proti kyberkriminalitě (EC3)**. **Skupina pro reakci na počítačové hrozby (CERT-EU)**, která podporuje všechny orgány, instituce a agentury Unie, je pod záštitou Komise.

Vedoucí úlohu v oblasti kybernetické obrany, kybernetické diplomacie a strategické komunikace zastává **Evropská služba pro vnější činnost (ESVČ)**, jejíž součástí je i zpravodajské a analytické středisko. **Evropská obranná agentura (EDA)** se zaměřuje na rozvoj schopností kybernetické obrany.

Na úrovni EU jednají členské státy prostřednictvím **Rady**, která má řadu orgánů pro koordinaci a sdílení informací (mezi nimi Horizontální pracovní skupinu pro otázky kybernetiky). **Evropský parlament** jedná jako spolunormotvůrce.

Organizace soukromého sektoru, včetně průmyslu, orgánů pro správu internetu a akademické obce, přispívají jako partneři k vytváření a provádění politik, například v rámci smluvního partnerství veřejného a soukromého sektoru (**cPPP**).

Kybernetická strategie EU: kybernetická bezpečnost je od roku 2013 jedním z hlavních problémů

27 Kybernetická bezpečnost je jedním z hlavních politických problémů přinejmenším od roku 2013, kdy Komise přijala svou **strategii kybernetické bezpečnosti**[37]**.** Tato strategie má pět hlavních cílů:

- zvýšení kybernetické odolnosti;

[37] Evropská komise, *Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor*, JOIN (2013) 1 final, 7. února 2013.

- omezení kyberkriminality;
- rozvoj politiky a kapacit kybernetické obrany;
- rozvoj průmyslových a technologických zdrojů pro kybernetickou bezpečnost;
- zavedení mezinárodní politiky týkající se kyberprostoru, která bude v souladu se základními hodnotami EU.

V následujících letech se otázkou kybernetické bezpečnosti zabývaly i jiné strategie EU (viz ***rámeček 10***).

Rámeček 10

Další strategie EU zabývající se otázkou kybernetické bezpečnosti

- **Evropský program pro bezpečnost** (2015)[38], jehož cílem bylo zlepšit vymáhání práva a reakci justice na kyberkriminalitu, zejména obnovením aktualizace stávajících politik a právních předpisů.
- **Strategie pro jednotný digitální trh** (2015)[39], jejímž cílem bylo zajistit lepší přístup k digitálnímu zboží a digitálním službám, pro které má posílení bezpečnosti internetu, důvěry a začleňování zásadní význam
- **Globální strategie EU** (2016)[40], která stanoví řadu iniciativ zaměřených na posílení úlohy EU ve světě. Základním pilířem této politiky byla kybernetická bezpečnost a vyvracení dezinformací prostřednictvím strategické komunikace.

28 Kromě toho v roce 2017 vydaly Evropský parlament a Rada **společné sdělení o kybernetické bezpečnosti pro EU**[41], v němž vyzvaly k vytvoření robustnějších a účinnějších struktur, které podpoří kybernetickou bezpečnost a umožní reagovat na

[38] Evropská komise, *Evropský program pro bezpečnost*, COM(2015) 185 final, 28. dubna 2015.

[39] Evropská komise, *Strategie pro jednotný digitální trh v Evropě*, COM(2015) 192 final, 6. května 2015.

[40] EEAS, *Sdílená vize, společný postup: silnější Evropa. Globální strategie zahraniční a bezpečnostní politiky EU*, červen 2016.

[41] Evropská komise a vysoká představitelka Unie pro zahraniční věci a bezpečnostní politiku, *Společné sdělení – Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU*, JOIN(2017) 450, 13. září 2017.

kybernetické útoky v členských státech, ale také v orgánech, agenturách a institucích EU.

29 V červenci 2020 Evropská komise aktualizovala svůj program na rok 2015 a přijala **strategii bezpečnostní unie EU**[42] na období 2020–2025, v níž označila kybernetickou bezpečnost za otázku strategického významu. V této strategii Komise zejména zdůrazňuje tzv. hybridní hrozby zahrnující kybernetické útoky a dezinformační kampaně, kdy státní a nestátní subjekty ze třetích zemí jednají ve vzájemné shodě s úmyslem manipulovat s informačním prostředím a napadat základní infrastruktury.

Právní předpisy EU týkající se kybernetické bezpečnosti: směrnice o bezpečnosti sítí a informací, obecné nařízení o ochraně osobních údajů, akt o kybernetické bezpečnosti a nový mechanismus sankcí

30 Hlavním pilířem strategie kybernetické bezpečnosti z roku 2013 je ústřední právní předpis, jímž je **směrnice o bezpečnosti sítí a informací**[43] z roku 2016, která je prvním právním předpisem o kybernetické bezpečnosti platným v celé EU. Tato směrnice má za cíl dosáhnout minimální úrovně harmonizovaných kapacit tím, že zaváže členské státy k přijetí národních strategií bezpečnosti sítí a informací a k vytvoření jednotných kontaktních míst a skupin pro reakce na počítačové bezpečnostní incidenty (týmy CSIRT)[44]. Stanoví rovněž bezpečnostní požadavky a požadavky na hlášení incidentů pro poskytovatele základních služeb v kritických odvětvích a pro poskytovatele digitálních služeb.

31 Členské státy měly **směrnici o bezpečnosti sítí a informací** provést **ve svých vnitrostátních právních předpisech** do května 2018. Do listopadu 2018 měly rovněž určit tzv. „provozovatele základních služeb“. Evropská komise je povinna pravidelně

---

[42] Evropská komise, *Sdělení o strategii bezpečnostní unie EU*, COM (2020)605 final, 24. července 2020.

[43] 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.

[44] Jsou integrovány do kooperačních struktur stanovených směrnicí, do sítě CSIRTS (síť složená z CSIRT stanovených členskými státy EU a CERT-EU, ENISA je hostitelem sekretariátu) a skupiny pro spolupráci (podporuje a usnadňuje strategickou spolupráci a výměnu informací mezi členskými státy, sekretariát hostí Komise).

přezkoumávat fungování této směrnice. V období od července do října 2020 vedla Komise s ohledem na jeden ze svých klíčových politických cílů, jímž je to, aby byla „Evropa připravená na digitální věk“, a v souladu s cíli bezpečnostní unie konzultace, jejichž výsledky měly posloužit při prvním hodnocení a následném posouzení dopadů směrnice o bezpečnosti sítí a informací.

32 Současně s tím vstoupilo v roce 2016 v platnost **obecné nařízení o ochraně osobních údajů**[45](GDPR), které platí od května 2018. Jeho cílem je chránit osobní údaje evropských občanů stanovením pravidel pro jejich zpracování a šíření. Zaručuje subjektům údajů určitá práva a ukládá povinnosti správcům údajů (poskytovatelům digitálních služeb), pokud jde o používání a přenos informací.

33 **Akt EU o kybernetické bezpečnosti**[46] kromě toho poprvé zavádí celounijní rámec certifikace kybernetické bezpečnosti produktů, služeb a procesů IKT. Společnosti, které v EU podnikají, budou mít díky tomuto rámci prospěch z toho, že své produkty, procesy a služby IKT budou muset certifikovat pouze jednou a jejich certifikáty budou platit v celé EU. Aktem EU o kybernetické bezpečnosti byla rovněž zřízena **Agentura Evropské unie pro kybernetickou bezpečnost** (označovaná ENISA, což bylo převzato od bývalé Evropské agentury pro bezpečnost sítí a informací). Agentura je tímto aktem pověřena úkolem posilovat operativní spolupráci na úrovni EU a pomáhat za tímto účelem členským státům EU, které o to požádají, při řešení kybernetických bezpečnostních incidentů a podporovat koordinaci EU v případě rozsáhlých přeshraničních kybernetických útoků a krizí.

34 V květnu 2019 Rada rovněž vytvořila právní nástroj, který EU umožňuje ukládat cílená omezující **opatření s cílem odrazovat od kybernetických útoků**, které

[45] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

[46] Nařízení Evropského parlamentu a Rady (EU) 2019/881 o agentuře ENISA (Agentura Evropské unie pro kybernetickou bezpečnost) a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií, 17. dubna 2019.

představují vnější hrozbu pro EU nebo její členské státy, a reagovat na ně[47]. V důsledku toho má EU právní pravomoc postihovat osoby nebo subjekty, které:

- jsou odpovědné za kybernetické útoky nebo za pokusy o ně; nebo
- poskytují finanční, technickou či materiální podporu na kybernetické útoky; nebo jsou do nich jiným způsobem zapojeny.

V červenci 2020 Rada poprvé využila těchto nových pravomocí (viz ***rámeček 11***).

Rámeček 11

Posílení obrany – EU ukládá vůbec první sankce proti kybernetickým útokům[48]

V červenci 2020 Rada uložila sankce šesti osobám a třem subjektům, které jsou odpovědné za různé kybernetické útoky nebo jsou do nich zapojeny. Patří mezi ně pokus o kybernetický útok na Organizaci pro zákaz chemických zbraní a útoky veřejné známé pod označením „WannaCry“, „NotPetya“ a „Operation Cloud Hopper“.

Uložené sankce zahrnují zákaz cestování a zmrazení majetku. Osoby a subjekty z EU kromě toho nesmějí osobám a subjektům zařazeným na seznam zpřístupňovat finanční prostředky.

[47] Rozhodnutí Rady (SZBP) 2019/797 o omezujících opatřeních proti kybernetickým útokům ohrožujícím Unii nebo její členské státy, 17. května 2019.

[48] Rozhodnutí Rady (SZBP) 2020/1127 ze dne 30. července 2020, kterým se mění výše uvedené rozhodnutí (SZBP) 2019/797 o omezujících opatřeních proti kybernetickým útokům ohrožujícím Unii nebo její členské státy.

Kybernetická bezpečnost a kybernetická obrana

35 V posledních letech se kyberprostor stále více militarizuje[49] a vyzbrojuje[50]. Je nyní považován za pátou oblast vojenské činnosti vedle oblasti pozemní, námořní, vzdušné a kosmické. **Politický rámec EU pro kybernetickou obranu** byl přijat v roce 2014 a aktualizován v roce 2018[51]. Toto aktualizované znění z roku 2018 stanoví priority, včetně rozvoje schopností kybernetické obrany a ochrany komunikačních a informačních sítí společné bezpečnostní a obranné politiky EU (SBOP). Kybernetická obrana je také součástí rámce stálé strukturované spolupráce (PESCO) a spolupráce mezi EU a NATO.

36 Běžně se objevují případy využívání kyberprostoru pro politické prostředky a agresivní testování kybernetické bezpečnosti EU a členských států a její narušování se stalo běžným jevem. Tyto činnosti v oblasti kybernetické špionáže a hackerství – jejichž terčem jsou vlády členských států, politické subjekty a orgány EU a jejichž účelem je získávat a shromažďovat utajované informace – svědčí o tom, že proti EU a jejím členským státům jsou prováděny sofistikované kybernetické špionáže a manipulace s údaji. **Společný rámec EU pro boj proti hybridním hrozbám** (2016) se zabývá kybernetickými hrozbami pro kritickou infrastrukturu i soukromé uživatele a klade důraz na skutečnost, že kybernetické útoky lze provádět také prostřednictvím dezinformačních kampaní na sociálních sítích[52]. Zaznamenává také potřebu zlepšit

---

[49] Centrum pro evropská politická studia, *Strengthening the EU's Cyber Defence Capabilities – Report of a CEPS Task Force* (Posílení kybernetické obrany EU – zpráva pracovní skupiny CEPS), listopad 2018.

[50] Malware za útokem ransomware Wannacry, který byl Spojenými státy, Spojeným královstvím a Austrálií připisován Severní Koreji, byl původně vyvinut a držen Agenturou pro národní bezpečnost USA za účelem využití zranitelných míst ve Windows.
Zdroj: A. Greenberg, WIRED, 19. prosince 2017. Ihned po útocích společnost Microsoft odsoudila skutečnost, že státy shromažďují slabá místa softwaru, a opětovně vyzvala, aby byla uzavřena ženevská úmluva o používání digitálních technologií.

[51] *Politický rámec EU pro kybernetickou obranu (aktualizace z roku 2018)*, 14413/18, 19. listopadu 2018.

[52] Evropská komise/Evropská služba pro vnější činnost, *Společný rámec pro boj proti hybridním hrozbám: reakce Evropské unie*, JOIN(2016) 18 final, 6. dubna 2016.

informovanost a posílit spolupráci mezi EU a NATO, jejíž základ byl dán ve společných prohlášeních EU-NATO z roku 2016 a 2018[53].

Výdaje spojené s kybernetickou bezpečností v EU jsou rozptýlené a pokulhávající

Výdaje na kybernetickou bezpečnost v EU-27 jsou ve srovnání s USA nižší

37 Odhadnout veřejné výdaje na kybernetickou bezpečnost je obtížné, a to z důvodu jejich průřezové povahy a proto, že výdaje na kybernetickou bezpečnost a všeobecné výdaje na IT jsou často nerozlišitelné[54]. I při zohlednění této skutečnosti lze na základě dostupných údajů nicméně říci, že **veřejné výdaje na kybernetickou bezpečnost** v EU jsou poměrně nízké:

- Jen v roce 2020 činil rozpočet federální vlády USA na kybernetickou bezpečnost přibližně **17,4 miliardy USD**[55]**.**
- Pro srovnání: Komise odhaduje, že veřejné výdaje na kybernetickou bezpečnost všech členských států EU (které dohromady mají téměř stejný HDP jako USA) se pohybují v rozmezí **od jedné do dvou miliard EUR** ročně[56].
- U mnoha členských států se veřejné výdaje na kybernetickou bezpečnost vyjádřené jako procento HDP odhadují na **jednu desetinu úrovně USA**, anebo ještě menší zlomek[57].

---

[53] Společné prohlášení předsedy Evropské rady, předsedy Evropské komise a generálního tajemníka Severoatlantické aliance, 8. července 2016 a 10. července 2018.

[54] Evropská komise, COM(2018) 630 final, 12. září 2018.

[55] Bílý dům, *Cybersecurity budget fiscal year 2020* (Rozpočet na kybernetickou bezpečnost na fiskální rok 2020).

[56] Evropská komise, pracovní dokument útvarů Komise: Hodnocení dopadu jako doložka k dokumentu „Návrh nařízení Evropského parlamentu a Rady, kterým se zavádí program Digitální Evropa na období 2021–2027“, SWD(2018) 305 final, 6. června 2018.

[57] Haagské středisko pro strategické studie, *Dutch investments in ICT and cybersecurity: putting it in perspective* (Nizozemské investice do IKT a kybernetické bezpečnosti: souvislosti), prosinec 2016.

2014–2020: Finanční prostředky EU na kybernetickou bezpečnost jsou rozptýlené do několika různých nástrojů

38 Podle Komise[58] existuje v rámci souhrnného rozpočtu EU nejméně **deset různých nástrojů**, jejichž prostřednictvím lze financovat záležitosti související s kybernetickou bezpečností (viz ***rámeček 12***, kde jsou uvedeny rozpočty hlavních programů). Úhrnné finanční prostředky EU určené na nevojenskou kybernetickou bezpečnost činily v letech 2014–2020 **méně než 200 milionů EUR ročně**. Neexistuje ani žádný celounijní nástroj financování, který by podporoval členské státy v koordinaci jejich činností v oblasti kybernetické bezpečnosti.

[58] Evropská komise, *Impact assessment accompanying the proposal for a Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres* (Posouzení dopadů připojené jako průvodní dokument k návrhu nařízení, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center), SWD(2018) 403 final, 12. září 2018.

Rámeček 12

Programy EU na podporu projektů v oblasti kybernetické bezpečnosti (2014–2020)

- V rámci **výzkumných programů EU Horizont 2020** bylo na projekty v oblasti kybernetické bezpečnosti a kyberkriminality na období 2014–2020 vyčleněno přibližně 600 milionů EUR. Součástí těchto prostředků je i 450 milionů EUR na tzv. smluvní partnerství veřejného a soukromého sektoru (cPPP) v oblasti kybernetické bezpečnosti na období 2017–2020, jež má umožnit získání další 1,8 miliardy EUR ze soukromého sektoru;

- **Evropské strukturální a investiční fondy (ESI fondy)** poskytují do konce roku 2020 příspěvek ve výši až 400 milionů EUR na investice členských států do kybernetické bezpečnosti;

- v rámci **Nástroje pro propojení Evropy (CEF)** byly financovány investice ve výši přibližně 30 milionů EUR ročně. Z těchto prostředků byly spolufinancovány vnitrostátní skupiny pro reakci na počítačové hrozby (CERT), které jsou členské státy podle směrnice o bezpečnosti sítí a informací povinny zřídit, a to ve výši přibližně 13 milionů EUR ročně od roku 2016 do roku 2018[59];

- **Fond pro vnitřní bezpečnost – policie (ISF-P)** podporuje studie, setkání odborníků a komunikační aktivity; v období od roku 2014 do roku 2017 bylo na tyto účely vynaloženo 62 milionů EUR. Členské státy mohou rovněž získávat granty na vybavení, odbornou přípravu, výzkum a sběr údajů v rámci sdíleného řízení. Těchto grantů využilo 19 členských států a jejich celkové výše dosáhla 42 milionů EUR;

- z prostředků **programu Spravedlnost** bylo poskytnuto 9 milionů EUR na podporu dohod o soudní spolupráci a vzájemné právní pomoci se zvláštním zaměřením na výměnu elektronických údajů a finančních informací.

[59] Čl. 9 odst. 2 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 („směrnice o bezpečnosti sítí a informací“, směrnice NIS).

39 Kromě toho bylo z rozpočtu EU vyčleněno 500 milionů EUR na **Evropský program rozvoje obranného průmyslu** na období 2019–2020[60]. Program se zaměřuje na zlepšování koordinace a účinnosti výdajů členských států na obranu prostřednictvím pobídek pro společný rozvoj. Jeho cílem je vytvořit v rámci Evropského obranného fondu celkem 13 miliard EUR, které budou určeny na investice do obranných schopností po roce 2020, z nichž některé se budou týkat kybernetické obrany.
V neposlední řadě poskytne Evropská investiční banka v letech 2018 až 2020 v rámci **Evropské bezpečnostní iniciativy** 6 miliard EUR na financování dvojího užití (výzkum a vývoj/kybernetická bezpečnost a civilní bezpečnost)[61].

2021–2027: nový program Digitální Evropa

40 Ve svých závěrech z července 2020 o novém víceletém finančním rámci (VFR) na období 2021–2027 Rada rozhodla, že v rámci **programu Digitální Evropa (DEP)**[62] se bude investovat do klíčových strategických digitálních kapacit, jako je vysoce výkonná výpočetní technika EU, umělá inteligence a kybernetická bezpečnost. Program bude doplňovat další nástroje podporující digitální transformaci Evropy, zejména program Horizont Evropa a Nástroj pro propojení Evropy.

41 Rada se rovněž rozhodla přidělit na program Digitální Evropa 6,8 miliardy EUR na období 2021–2027, tj. přibližně **970 milionů EUR ročně**. Ve srovnání s obdobím 2014–2020 se jedná o značné navýšení, které je však stále menší, než jaké původně navrhovala Komise (8,2 miliardy EUR na stejné období, přičemž 2 miliardy EUR by byly vyčleněny na posílení odvětví kybernetické bezpečnosti EU a celkové ochrany společnosti, například v podobě podpory provádění směrnice o bezpečnosti sítí a informací).

---

[60] Evropská komise, nařízení Evropského parlamentu a Rady (EU) 2018/1092 ze dne 18. července 2018, kterým se zřizuje Evropský program rozvoje obranného průmyslu s cílem podpořit konkurenceschopnost a inovační kapacitu obranného průmyslu Unie (Úř. věst. L 200, 7.8.2018, s. 30)

[61] Evropská investiční banka, *The EIB Group Operating Framework and Operational Plan 2018* (Operační rámec a operační plán skupiny EIB v roce 2018), 12.12.2017.

[62] Evropská komise, *Europe investing in digital: the Digital Europe Programme* (Evropské investice v oblasti digitalizace: program Digitální Evropa), září 2020.

Část II – Přehled práce nejvyšších kontrolních institucí

Úvod

42 Kybernetická bezpečnost a naše digitální autonomie se staly věcí strategického významu pro EU a její členské státy. V oblasti správy kybernetické bezpečnosti přetrvávají ve veřejném i soukromém sektoru všech členských států nedostatky, i když na různé úrovni. Naše schopnost zamezovat kybernetickým útokům a v případě potřeby na ně reagovat je v důsledku toho narušená.

43 Z průzkumu provedeného v roce 2018 mezi nejvyššími kontrolními institucemi v EU vyšlo nicméně najevo, že přibližně polovina z nich se ve svých auditech otázkou kybernetické bezpečnosti dosud nezabývala. Od té doby se však situace změnila a nejvyšší kontrolní instituce se na tuto otázku ve své auditní činnosti začaly zaměřovat, přičemž se soustředily především na ochranu údajů, připravenost systému proti kybernetickým útokům a ochranu systémů základních veřejných služeb. Zabývaly se také dalšími velmi důležitými tématy. Je pochopitelné, že výsledky některých těchto auditů nemohou být zveřejněny, protože se mohou týkat (z hlediska národní bezpečnosti) citlivých informací.

44 Vzhledem k významu kybernetické bezpečnosti pro fungování našich společností a politických institucí se kontaktní výbor rozhodl věnovat tomuto tématu letošní auditní kompendium. V této jeho druhé části jsou shrnuty výsledky vybraných auditů provedených v oblasti kybernetické bezpečnosti dvanácti nejvyššími kontrolními institucemi přispívajících členských států a Evropským účetním dvorem. Každá zúčastněná nejvyšší kontrolní instituce přispěla jednou vybranou zprávou o auditu, která je dále shrnuta v části III. Na toto téma bylo provedeno mnoho dalších auditů, jak ukazují další zprávy uvedené zúčastněnými nejvyššími kontrolními institucemi.

Metodika a témata auditu

45 Pokud jde o druh auditu prováděného pro účely auditních zpráv shrnutých v tomto kompendiu, většina zúčastněných nejvyšších kontrolních institucí provedla audity výkonnosti v oblastech souvisejících s kybernetickou bezpečností, zatímco dvě (NKI Polska a Maďarska) provedly audity souladu s předpisy a jeden subjekt (EÚD) provedl přezkum politiky.

46 Při vymezování svého kontrolního přístupu koncipovala většina nejvyšších kontrolních institucí své audity tak, aby zahrnovaly alespoň dva způsoby posouzení

předmětu auditu. Tento přístup mohl spočívat v přezkumu strategických dokumentů na vysoké úrovni (např. celostátní) nebo vymezených politik nebo v přezkumu postupů za účelem posouzení jejich souladu se zavedenou metodikou COBIT (viz ***rámeček 13***) nebo v přezkumu účinnosti zavedených systémů řízení IT. Jedna nejvyšší kontrolní instituce (Nizozemský účetní dvůr) dokonce použil etické hackery, aby prověřili účinnosti systémů kybernetické bezpečnosti při ochraně hranic a u kritických vodních staveb. V ***rámečku 14*** shrnujeme metody a technické postupy, které jednotlivé nejvyšší kontrolní instituce použily k provádění své auditní činnosti.

Rámeček 13

Co je COBIT?

Kontrolní cíle pro oblast informační a související technologie (COBIT – *Control Objectives for Information and Related Technology*) představují rámec uznávaných osvědčených postupů a postupů pro řízení IT a správu IT, který vymezila ISACA (Asociace auditu a kontroly informačních systémů). Organizace mohou s jeho pomocí dosahovat strategických cílů účinným využíváním dostupných zdrojů a minimalizací rizik v oblasti informačních technologií. COBIT propojuje řízení podniků a správu IT. Vytváří vazby mezi obchodními záměry a cíli v oblasti IT, definuje metriky a modely vyspělosti, které umožňují měřit dosahování cílů, a vymezuje odpovědnost vlastníků obchodních a IT procesů.

47 Témata, která byla předmětem auditů kybernetické bezpečnosti, se značně lišila. Některé nejvyšší kontrolní instituce se ve svých auditech zabývaly velmi specifickými oblastmi veřejného zájmu: například nizozemský nejvyšší kontrolní orgán provedl audit kybernetické bezpečnosti, který se zaměřil na životně důležité ochranné mořské hráze a vodohospodářské systémy. Jiné nejvyšší kontrolní instituce, jako například irská a maďarská, se zabývaly průřezovějšími otázkami, jako je provádění národní strategie kybernetické bezpečnosti a ochrana osobních údajů a vnitrostátních datových souborů. Všechny nejvyšší kontrolní instituce se nicméně zabývaly záležitostmi, které by mohly mít negativní dopad na veřejné služby nebo infrastrukturu.

48 Estonský a litevský nejvyšší kontrolní orgán si uvědomují strategický význam vnitrostátních datových souborů, které jsou zásadně důležité z hlediska národní bezpečnosti a ochrany jejich integrity před vnějšími kybernetickými útoky. Dánský nejvyšší kontrolní orgán se ve svém auditu zabýval konkrétně posouzením bezpečnosti čtyř veřejných subjektů s ohledem na možnost ransomwarových útoků. Nejvyšší kontrolní orgány Nizozemska, Polska a Portugalska provedly audit účinnosti různých IT

systémů používaných pro účely hraničních kontrol (na letišti Schiphol, hlavní velení pohraniční stráže a ministerstva vnitra a správy v Polsku a na portugalských hranicích), zabývaly se proto i otázkou bezpečnosti v rámci EU.

Auditované období

49 Vybrané zprávy o auditu obsažené v tomto kompendiu byly zveřejněny v letech 2014 až 2020. U většiny z nich trvalo auditované období dva roky nebo více let, ačkoli v případě čtyř zpráv (Dánsko, Estonsko, Francie a Portugalsko) šlo o jednoleté auditované období.

Cíle auditu

50 Jednotlivé nejvyšší kontrolní instituce, které do tohoto kompendia přispěly, se v rámci své auditní práce zabývaly celou řadou rizik. Patří mezi ně ohrožení práv jednotlivých občanů EU v důsledku nepatřičného zacházení s osobními údaji, riziko, že instituce nebudou schopny poskytovat důležitou veřejnou službu nebo budou mít omezenou výkonnost, vážné důsledky pro veřejnou bezpečnost, blahobyt a hospodářství členského státu, jakož i pro kybernetickou bezpečnost v EU. Nejméně čtyři nejvyšší kontrolní instituce (Estonsko, Maďarsko, Nizozemsko a Portugalsko) se zabývaly třemi nebo více tématy uvedenými v jejich zprávách o auditu, které jsou součástí tohoto kompendia.

51 Kybernetická bezpečnost zůstává v pravomoci členských států. Nicméně vzhledem k tomu, že právní předpisy EU se postupem času rozšířily a konkretizovaly, většina orgánů a institucí, u nichž nejvyšší kontrolní instituce provedly audit, již přispívá k dosažení strategických cílů EU v oblasti kybernetické bezpečnosti, i když v různé míře. Například irský Nejvyšší kontrolní a auditní úřad (*Office of the Comptroller and Auditor General*) se ve svém auditu zabýval prováděním směrnice EU o sítích a informačních systémech, jejímž cílem je zvýšit odolnost klíčových sítí a informačních systémů, a vydal doporučení, jak její provádění zlepšit. Podobně se audit maďarského nejvyššího kontrolního orgánu zabýval otázkou souladu s platnými směrnicemi EU.

52 V ***rámečku 14*** je znázorněno, kdy výsledek auditu buď přispěl ke zvýšení kybernetické odolnosti prověřovaných subjektů, k omezení kybernetické kriminality, nebo kdy by napomohl vypracování politiky kybernetické obrany a posílení pravomocí, lepšímu rozvoji technologií a dosažení pokroku v oblasti mezinárodní spolupráce, což

jsou hlavní cíle strategie kybernetické bezpečnosti Evropské unie. Doporučení nejvyšších kontrolních institucí se ve většině případů týkala více než dvou strategických cílů, kterých chce EU dosáhnout.

53 Díky práci nejvyšších kontrolních institucí byly rovněž zjištěny nedostatky v oblasti bezpečnosti nebo provádění, které byly pro kontrolované orgány podnětem k vyvinutí dalšího úsilí. Například čtyři orgány, které byly prověřovány v Dánsku, začaly již v průběhu auditu provádět několik bezpečnostních kontrol zaměřených na předcházení budoucím rizikům, aby si zajistily podstatně vyšší úroveň ochrany před ransomwarovými útoky a aby posílily své obranné schopnosti a zvýšily kybernetickou odolnost, což je do budoucna více ochrání před kybernetickou kriminalitou.

54 Viděli jsme také, že doporučení vydaná na základě auditu byla předložena na různých úrovních řízení a odpovědnosti, takže některá byla určena ústřední vládě, jiná byla předložena na operační úrovni ministerstev a agentur, jiná vlastníkům systémů IT.

Rámeček 14

Přehled auditní činnosti nejvyšších kontrolních institucí vztahující se k příspěvkům zahrnutým v kompendiu (část 1)

Hlavní oblast zájmu		Dánsko	Estonsko	Irsko	Francie	Lotyšsko	Litva	Maďarsko	Nizozemsko	Polsko	Portugalsko	Finsko	Švédsko	EU (EÚD)
Typ auditu	Výkonnost	✓	✓	✓	✓	✓	✓		✓		✓	✓	✓	
	Soulad s předpisy							✓		✓				
	Přezkum													✓
Koncepce auditu	Přezkum politik	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓
	Přezkum postupů	✓	✓		✓		✓	✓		✓	✓	✓		
	Přezkum systémů	✓			✓	✓	✓	✓	✓	✓	✓		✓	
	Posouzení robustnosti přímým testováním								✓		✓			
Prověřované hrozby	Dopad na práva jednotlivců		✓		✓			✓			✓			✓
	Dopad na veřejnou infrastrukturu nebo služby	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Dopad na národní bezpečnost		✓	✓		✓	✓	✓	✓		✓			
	Dopad na bezpečnost v EU	✓							✓		✓			✓

Přehled auditní činnosti nejvyšších kontrolních institucí vztahující se k příspěvkům zahrnutým v kompendiu (část 2)

Hlavní oblast zájmu		Dánsko	Estonsko	Irsko	Francie	Lotyšsko	Litva	Maďarsko	Nizozemsko	Polsko	Portugalsko	Finsko	Švédsko	EU (EÚD)
Tematizované strategické cíle EU v oblasti kybernetické bezpečnosti	Zvýšení kybernetické odolnosti	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
	Omezení kyberkriminality	✓					✓							✓
	Rozvoj politiky a kapacit kybernetické obrany	✓	✓	✓		✓	✓	✓	✓	✓				✓
	Rozvoj technologických zdrojů				✓	✓			✓				✓	
	Zlepšení mezinárodní spolupráce (politik)			✓				✓						✓
Úroveň adresáta doporučení	Ústřední vláda	✓	✓				✓					✓	✓	✓
	Operační (ministerstva a agentury)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Vlastníci IT systémů	✓			✓			✓	✓	✓				

Hlavní auditní připomínky

55 Hlavní připomínky nejvyšších kontrolních institucí k auditu jsou shrnuty v následujících oddílech.

Audity výkonnosti

56 **Dánský *Rigsrevisionen*** posuzoval, zda vybrané základní vládní instituce mají uspokojivou ochranu před ransomwarem. Vládní instituce bývají častým terčem kybernetických útoků a ransomware je v současnosti jednou z největších hrozeb pro kybernetickou bezpečnost. Audit se týkal dánského Úřadu pro zdravotní evidenci, Ministerstva zahraničních věcí, společnosti Banedanmark (dánské železniční sítě) a dánské Agentury pro řízení mimořádných situací. Tyto čtyři instituce byly vybrány proto, že jsou odpovědné za poskytování základních služeb v oblasti zdraví, zahraničních věcí, dopravy a připravenosti na mimořádné události, kde může mít zajištění přístupu k údajům zásadní význam. Při auditu bylo zjištěno, že tyto čtyři instituce neměly uspokojivou ochranu před ransomwarem. Z auditu vyplynulo, že nezavedly několik společných bezpečnostních kontrolních opatření pro zmírnění rizika takových útoků. Audit vedl k závěru, že je důležité, aby orgány zvážily zavedení bezpečnostních kontrol předjímajících budoucí rizika, které zvýší jejich odolnost vůči ransomwarových útokům.

57 **Estonský *Riigikontroll*** si uvědomuje, že zachování estonské nezávislosti vyžaduje nejen fyzickou ochranu území, ale také ochranu digitálních statků, které mají pro stát prvořadý význam. Digitální statky, které potřebují nejvíce chránit, jsou údaje týkající se občanů, území a právních předpisů. Rovněž je třeba zabezpečit údaje týkající se majetku, nemovitostí a práv osob s trvalým pobytem v Estonsku. Estonský kontrolní úřad vyhodnotil možnosti kybernetických hrozeb v případě eskalace bezpečnostních problémů. Takové rizikové scénáře a nárůst počtu incidentů v oblasti zabezpečení informací, jako jsou kybernetické útoky a úniky údajů, mohou být nebezpečné pro ochranu údajů a databází, které mají pro stát největší význam. Audit se proto zaměřil na to, jakým způsobem stát určil, které údaje a databáze mají zásadní význam pro zaručení národní bezpečnosti. Audit vedl k závěru, že navzdory zavedení třístupňového základního bezpečnostního systému ISKE[63], které je pro státní agentury povinné,

[63] Systém ISKE je norma pro bezpečnost informací, která byla vytvořena pro estonský veřejný sektor; je povinná pro organizace státní správy i místní samosprávy, které mají přístup do databází / rejstříků.

vykazovalo několik kritických databází z hlediska zajištění bezpečnosti informací významné nedostatky.

58 **Irský Nejvyšší kontrolní a auditní úřad** (*Office of the Comptroller and Auditor General*) prověřoval, jakého pokroku bylo dosaženo, pokud jde o opatření v oblasti kybernetické bezpečnosti, od zřízení irského Národního střediska pro kybernetickou bezpečnost. Toto středisko, které podléhá Ministerstvu pro komunikace, klimatická opatření a životní prostředí, bylo zřízeno v roce 2011. Zaměřuje se především na zabezpečení vládních sítí, na pomoc průmyslu a jednotlivcům při zajišťování ochrany jejich vlastních systémů a na zabezpečení kritické vnitrostátní infrastruktury. Audit vedl k závěru, že ačkoli Národní středisko pro kybernetickou bezpečnost plní zásadní funkci, v prvních čtyřech letech svého provozu mělo oproti původním představám výrazně nižší objem prostředků a jeho celkové strategické směřování postrádalo plán. Nebyly také dostatečně jasně vymezeny příslušné úlohy orgánů zapojených do vyšetřování kybernetické kriminality a vnitrostátních bezpečnostních incidentů. Kromě toho ještě nebyly provedeny požadavky týkající se vypracování vnitrostátní strategie, které stanoví směrnice EU o informačních a komunikačních systémech.

59 **Francouzský *Cour des comptes*** zkoumal „*Parcoursup*“, novou digitální platformu, která funguje jako zdroj informací o dostupných vysokoškolských kursech a požadavcích na přijetí uchazečů ke studiu a která si klade za cíl dosažení většího souladu mezi schopnostmi a akademickými výsledky středoškolských studentů a obsahem kursů terciárního vzdělávání. Na základě auditu bylo zjištěno, že vláda prostřednictvím digitální platformy úspěšně centralizovala přístup ke všem druhům postsekundárního studia, což ji umožnilo řešit otázku rozšiřování vysokoškolského vzdělávání. Nový „*Parcoursup“* byl však vytvořen z předchozího systému příliš rychle, a na provedení podstatných strukturálních změn už nezbyl čas. Slabá místa informačního systému z hlediska bezpečnosti, výkonnosti a robustnosti proto nebyla odstraněna. Platforma je stále zatížena významnými riziky, pokud jde o kvalitu a kontinuitu veřejné služby a bezpečnost osobních údajů.

60 **Lotyšský *Valsts Kontrole*** dokončil audit výkonnosti týkající se účinnosti veřejné infrastruktury informačních a komunikačních technologií (IKT). Účelem auditu bylo ověřit, zda veřejná správa měla jednotný přístup k účinnému řízení infrastruktury IKT a zda příslušné instituce provedly posouzení přínosů centralizace. Na základě auditu bylo zjištěno, že zdráhavý postoj orgánů k centrálnímu řízení infrastruktury IKT vedl k tomu, že vznikl větší počet serverových místností, což výrazně zvýšilo náklady na údržbu. Ve většině serverových místností se objevily bezpečnostní hrozby a datová centra nebyla

dostatečně chráněna před vstupem nepovolaných osob a před riziky pro životní prostředí. Dotčené instituce navíc neměly zaveden žádný postup pro pravidelné posuzování otázky, zda by bylo levnější udržovat infrastrukturu IKT interně, spolupracovat s jinou institucí nebo údržbu IKT svěřit externímu poskytovateli. Audit doporučil zavést systém pravidelného monitorování, který by umožnil hodnotit celou veřejnou správu jako jediný systém.

61 **Litevský *Valstybės kontrolė*** si uvědomuje význam kritických elektronických státních informačních zdrojů, jako je správa veřejných financí, daňová správa a zdravotní péče. Ztráta kritických informací a nedostupnost odpovídajících informačních systémů by mohly mít závažné důsledky pro veřejnou bezpečnost, blahobyt i hospodářství. Cílem auditu bylo zhodnotit řízení (obecnou kontrolu) a vyspělost kritických státních informačních zdrojů. Na jeho základě byly odhaleny systémové problémy jak při vytváření a provádění politiky státních informačních zdrojů, tak v jejich mechanismu řízení. Audit vedl k závěru, že nízká úroveň vyspělosti kritických státních informačních zdrojů svědčí o nedostatcích ve vytváření a provádění politiky státních informačních zdrojů, které jsou v důsledku toho zranitelnější. Pokud se má bezpečnost státních informačních zdrojů zvýšit, je třeba zlepšit mechanismus řízení.

62 V roce 2018 **nizozemský *Účetní dvůr*** rozhodl, že provede audity kybernetické bezpečnosti v odvětvích, která mají pro společnost kritický význam. První dvě auditovaná odvětví se týkala řízení vodních zdrojů a automatizovaných hraničních kontrol, přičemž první z nich je důležité kvůli tomu, že velká část území se nachází pod úrovní mořské hladiny, druhé kvůli úloze amsterdamského letiště Schiphol jako mezinárodního uzlu a vstupní brány do země. Ministr infrastruktury a řízení vodních zdrojů určil jako „kritické části“ vodohospodářského odvětví řadu vodních staveb spravovaných Generálním ředitelstvím pro veřejné práce a řízení vodních zdrojů (dále jen „auditovaný subjekt“). Mnoho počítačových systémů používaných k řízení provozu kritických vodních staveb pochází z 80. a 90. let 20. století, kdy se na kybernetickou bezpečnost obvykle nebral zřetel. Ministr obrany a ministr spravedlnosti a bezpečnosti jsou společně odpovědní za hraniční kontroly prováděné nizozemskou pohraniční stráží na letišti Schiphol. Obě ministerstva vlastní IT systémy, na které se příslušníci pohraniční stráže spoléhají. Systémy mají zásadní význam pro provoz letiště a používají se ke zpracování vysoce citlivých údajů. Jsou tak zajímavým terčem kybernetických útoků zaměřených na sabotáž, špionáž nebo manipulaci s hraničními kontrolami. Při auditu se prověřovalo, zda byly auditované subjekty připraveny řešit kybernetické hrozby a zda je řešily účinným způsobem. V případě vodních staveb bylo nezbytné, aby auditovaný subjekt přijal některá další opatření pro odhalování hrozeb a reakci na ně,

aby splnil své vlastní cíle, které si v oblasti kybernetické bezpečnosti stanovil. Pokud jde o hraniční kontroly, bylo zjištěno, že opatření pro zajištění kybernetické bezpečnosti jsou nepřiměřená nebo nevyhovující s ohledem na budoucí rizika.

63 **Portugalský *Tribunal de Contas*** provedl audit informačních systémů, které slouží pro účely udělování, vydávání a používání portugalského elektronického pasu (PEP), zejména v rámci automatizovaného prověřování cestujících na portugalských hranicích za pomoci biometrických údajů. Audit ověřoval soulad s právními předpisy EU a vnitrostátními právními předpisy, mezinárodními normami a pokyny pro udělování, vydávání a používání PEP, včetně přiměřenosti vnitrostátního právního rámce. Prověřil účinnost klíčových procesů souvisejících s životním cyklem PEP, zejména pak procesů, které souvisejí s jeho udělováním, vydáváním a používáním. Audit rovněž přezkoumal kritické aspekty výkonnosti informačních systémů, zejména splnění bezpečnostních požadavků týkajících se informačních systémů PEP (SIPEP).

64 **Finská *Valtiontalouden tarkastusvirasto*** se zabývala otázkou, zda je kybernetická ochrana v ústřední vládě co nejúčinnější a nákladově nejefektivnější. Audit se zaměřil na způsob řízení kybernetické bezpečnosti ústředních vládních institucí. Předmětem auditu byly orgány odpovědné za kybernetickou ochranu v ústřední vládě (Úřad předsedy vlády, Ministerstvo financí a Ministerstvo dopravy a spojů) a orgány pověřené centralizovanými úkoly v oblasti kybernetické ochrany a centralizované služby IT v ústřední vládě. Ve finské vládě je odpovědnost za kybernetickou ochranu decentralizována, přičemž každá právnická osoba je odpovědná za svou vlastní kybernetickou bezpečnost. Audit doporučil, aby Ministerstvo financí definovalo a zavedlo obecný model provozního řízení pro případy kybernetických bezpečnostních incidentů, k nimž dojde ve službách IKT ústředních vládních institucí. Ministerstvo financí by mělo rovněž zjistit, jak se má řešit otázka kybernetické bezpečnosti služeb v rámci financování služeb po celou dobu jejich životního cyklu, a mělo by zlepšit operativní znalosti o situaci tím, že orgánům vydá pokyn, aby případy kybernetických útoků hlásily Středisku pro kybernetickou bezpečnost.

65 **Švédský *Riksrevisionen*** se zabýval výskytem zastaralých systémů IT v rámci ústřední státní správy, přičemž jeho cílem bylo posoudit, zda vláda a orgány přijaly vhodná opatření, která vyloučí, aby se systémy IT staly překážkou účinné digitalizace. Na základě auditu bylo zjištěno, že zastaralé informační systémy se používají v celé řadě vládních agentur. V mnoha auditovaných agenturách byl zastaralý jeden nebo více informačních systémů kriticky důležitých pro jejich činnost a velká část prověřovaných agentur neměla k vývoji a správě IT vybavení správný přístup. Značná část agentur

neměla celkový popis propojení strategií, operačních procesů a systémů. Z auditu celkově vyplynulo, že většině agentur se dosud nepodařilo účinný způsobem řešit problémy spojené se zastaráváním informačních systémů. Švédský kontrolní úřad se domnívá, že problém je tak závažný a rozšířený, že představuje překážku pro další účinnou digitalizaci státní správy.

Audity souladu s právními předpisy v oblasti kybernetické bezpečnosti

66 **Maďarský Nejvyšší kontrolní úřad** si uvědomuje, že zabezpečení národních datových souborů je jedním z hlavních zájmů společnosti usilující o zachování a ochranu národních hodnot. Zajištění větší bezpečnosti osobních i veřejných údajů, které jsou součástí národních datových souborů Maďarska, má zásadní význam pro posílení důvěry občanů ve stát a pro zajištění nepřetržitého a bezproblémového fungování veřejné správy. Účelem auditu souladu s právními předpisy v oblasti ochrany údajů bylo posoudit, zda je v Maďarsku zaveden regulační a operační rámec pro ochranu údajů a zda nejvýznamnější organizace zajišťující správu údajů splňují požadavky na bezpečnou správu údajů a externí zpracovávání údajů. Audit dospěl k závěru, že vnitřní předpisy organizací spravujících údaje vztahující se na činnosti v oblasti správy údajů zajišťovaly ochranu národních datových souborů jako součásti národního majetku v souladu s právními předpisy platnými v letech 2011 až 2015. Správci údajů řádně uplatňovali požadavky a předávání údajů třetím stranám probíhalo řádným způsobem.

67 **Polská *Najwyższa Izba Kontroli*** posuzovala, zda jsou údaje shromažďované v systémech, které mají sloužit k plnění důležitých veřejných úkolů, bezpečné. Audit se týkal šesti vybraných institucí, které plní významné veřejné úkoly. Míra připravenosti a zavedenosti systému zabezpečení informací nezajišťovala přijatelnou úroveň bezpečnosti údajů shromažďovaných v informačních systémech, které slouží k plnění důležitých veřejných úkolů. Procesy, které mají zajišťovat bezpečnost informací, byly uplatňovány chaoticky a intuitivně, protože nebyly stanoveny příslušné postupy. Z šesti kontrolovaných oddělení mělo pouze jedno zavedený systém zabezpečení informací, ale je třeba poznamenat, že i jeho provoz se vyznačoval závažnými nedostatky. Audit vedl k závěru, že je třeba vypracovat obecná doporučení a požadavky týkající se bezpečnosti IT a že tato doporučení je třeba provést na centrální úrovni s platností pro všechny veřejné subjekty.

Přezkumy kybernetické bezpečnosti

68 ***Evropský účetní dvůr*** se v rámci svého přezkumu zaměřil na situaci politiky EU v oblasti kybernetické bezpečnosti a určil hlavní výzvy pro účinné provádění politik. Zabýval se bezpečností sítí a informací, kyberkriminalitou, kybernetickou obranou a dezinformacemi. Přezkum odhalil řadu nedostatků v právních předpisech EU týkajících se kybernetické bezpečnosti a konstatoval, že stávající právní předpisy nebyly členskými státy důsledně provedeny. Upozornil rovněž na skutečnost, že na úrovni EU chybějí spolehlivé údaje o kybernetických incidentech a neexistuje komplexní přehled o výdajích EU a jejích členských států na kybernetickou bezpečnost. Přezkum také poukázal na omezení týkající se zdrojů, která mají dopad na agentury EU, jejichž činnost souvisí s kybernetickou oblastí, včetně obtíží se získáváním a udržením talentů. Další výzva se týkala nesouladu financování kybernetické bezpečnosti se strategickými cíli EU.

Část III – Shrnutí zpráv nejvyšších kontrolních institucí

Dánsko
Rigsrevisionen

Ochrana před ransomwarovými útoky

Datum zveřejnění: 2017

Odkaz na zprávu: Shrnutí zprávy (anglické znění)

Druh auditu a auditované období

Druh auditu: Audit výkonnosti

Auditované období: duben – září 2017

Shrnutí zprávy

Téma auditu

Tato zpráva se zabývala otázkou, zda vybrané základní vládní instituce mají uspokojivou ochranu před ransomwarem.

Vládní instituce bývají častým terčem kybernetických útoků a ransomware je v současnosti jednou z největších hrozeb pro kybernetickou bezpečnost. Ransomware je škodlivý software, který blokuje přístup k datům. Obecně lze říci, že ransomware zašifruje data a napadeným institucím brání v jejich používání. Hackeři požadují výkupné s tím, že teprve po jeho zaplacení údaje dešifrují a umožní orgánům znovu získat přístup k údajům. Z toho vyplývá, že ransomware ohrožuje především přístupnost údajů.

Pro instituce může být v takové nečekané situaci, kdy ztratí přístup k údajům, obtížné, nebo dokonce zcela nemožné zajistit poskytování důležitých služeb. Instituce zasažené ransomwarovým útokem jsou obvykle nuceny zčásti nebo úplně zavřít své informační sítě, aby zjistily rozsah útoku. Ransomwarové útoky mohou mít významný hospodářský dopad, protože pro instituce představují riziko ztráty produkce, například když je jim zabráněno v přístupu na jejich IT síť nebo když ztratí údaje nashromážděné a zpracovávané během delšího časového úseku. V roce 2017 vedl ransomwarový útok na

britskou národní zdravotní službu ke zrušení 19 000 operací a návštěv u lékaře. Vedení institucí by proto mělo riziku ransomwarových útoků věnovat pozornost a provádět nezbytné bezpečnostní kontroly, které zajistí ochranu před ransomwarem a sníží dopady možného útoku.

Předmětem studie byl dánský Úřad pro zdravotní evidenci, Ministerstvo zahraničních věcí, společnost Banedanmark (dánská železniční síť) a dánská Agentura pro řízení mimořádných situací. Tyto čtyři instituce byly vybrány proto, že jsou odpovědné za poskytování základních služeb v oblasti zdraví, zahraničních věcí, dopravy a připravenosti na mimořádné události, kde může mít přístup k údajům zásadní význam. Úřad pro zdravotní evidenci rovněž poskytuje centralizované služby v oblasti IT většině vládních orgánů spadajících pod Ministerstvo zdravotnictví.

Účelem studie bylo posoudit, zda uvedené čtyři orgány mají uspokojivou ochranu před ransomwarovými útoky vedenými prostřednictvím e-mailů. *Rigsrevisionen* proto přezkoumal 20 společných bezpečnostních kontrol, které poskytují základní ochranu proti ransomware. Kromě toho tento nejvyšší kontrolní orgán přezkoumal pět bezpečnostních kontrol, které by orgány měly zvážit v souvislosti s budoucím posuzováním rizik. Příkladem kontrol předjímajících budoucí rizika je nová technologie, která může omezit počet falešných e-mailů, které přicházejí do instituce, nebo odhalit neobvyklou činnost na počítačích a odesílat upozornění. Studie, k jejímuž vypracování dal podnět *Rigsrevisionen*, vycházela ze zjištění čtyř auditů IT provedených od dubna do září 2017. Nabízí momentální přehled o tom, jak důkladně jsou instituce chráněny před ransomwarem. Instituce měly možnost provést po dokončení auditů IT 20 společných bezpečnostních kontrol. Výsledky studie se proto týkají pouze ochrany těchto institucí před ransomwarem v době, kdy byly tyto čtyři audity IT prováděny. Studie ukazuje výkonnost těchto čtyř institucí, ale neobsahuje srovnávací analýzu a hodnocení jejich výkonnosti.

Zjištění a závěry

Rigsrevisionen ve svém posouzení uvedl, že tyto čtyři instituce nemají uspokojivou ochranu před ransomwarem. Ze studie vyplývá, že neprovedly některé společné bezpečnostní kontroly pro zmírnění rizika útoků. Zejména Úřad pro zdravotní evidenci a společnost Banedanmark měly značné nedostatky v oblasti bezpečnosti. Následkem tohoto byly všechny čtyři instituce vystaveny zvýšenému riziku ransomwarových útoků vedených prostřednictvím e-mailu, které by jim znemožnily poskytovat své služby po různě dlouhou dobu. Všechny čtyři instituce informovaly *Rigsrevisionen*, že od té doby,

co byla studie dokončena, se zasadily o zavedení několika bezpečnostních kontrol, jejichž účelem je zvýšit úroveň ochrany před ransomwarem.

Jejich prevence ransomwarových útoků, včetně vnitřních i vnějších hrozeb, byla nedostatečná. Obzvláště znepokojivá je skutečnost, že žádná z těchto institucí se nestarala o to, aby měla nainstalované nejnovější bezpečnostní opravy a že tři instituce nepoužívaly seznam povoleného softwaru, který by vyloučil spuštění škodlivého softwaru ze strany zaměstnanců. Riziko, že ransomware napadne celou IT síť a nebo její část a začne se šířit, je pak větší.

V případě třech těchto orgánů vedení nevěnovalo dostatečnou pozornost hrozbě ransomwarového útoku a posouzení rizik provedená vedením Úřadu pro zdravotní evidenci a společnosti Banedanmark nezahrnovala všechny relevantní aspekty. Instituce tak neměly k dispozici aktuální posouzení hrozby ransomwarového útoku, a pokud jde o předcházení novým útokům a omezení dopadu budoucích útoků, jejich postavení bylo slabé. Vedení Úřadu pro zdravotní evidenci a společnost Banedanmark nevěnovalo dostatečnou pozornost posouzení rizik, a zabezpečení IT v těchto dvou institucích proto nevycházela z priorit, které stanovilo jejich vedení.

Ve třech institucích nebyly zavedeny odpovídající plány odezvy na incidenty, které by jim po ransomwarovém útoku pomohly obnovit činnost. Obzvláště významná je skutečnost, že tři instituce pravidelně neověřovaly, zda budou schopny své údaje a systémy zasažené ransomwarovým útokem obnovit. Zvyšuje se tak riziko, že údaje nacházející se v držení těchto institucí budou v souvislosti s ransomwarovým útokem ztraceny a že instituce nebudou schopny poskytovat své služby po delší dobu.

Vzhledem k tomu, že tyto rizikové scénáře se neustále mění, je důležité, aby orgány zvážily zavedení bezpečnostních kontrol předjímajících budoucí rizika a mohly tak zvýšit odolnost vůči ransomwarovým útokům, tj. kontrol, které usnadní ověřování totožnosti odesílatelů e-mailů a které umožní odhalovat a filtrovat potenciálně škodlivé e-maily. Všechny čtyři orgány v současné době pracují na některých bezpečnostních kontrolách předjímajících budoucí rizika, které mohou napomoci posílení jejich ochrany před ransomwarovými útoky.

Další zprávy v této oblasti

Název zprávy:	Zpráva o ochraně údajů z výzkumu na dánských univerzitách
Odkaz na zprávu:	Shrnutí zprávy (anglické znění)
Datum zveřejnění:	2019
Název zprávy:	Zpráva o ochraně informačních systémů a údajů o zdravotním stavu ve třech dánských regionech
Odkaz na zprávu:	Shrnutí zprávy (anglické znění)
Datum zveřejnění:	2017
Název zprávy:	Zpráva o řízení bezpečnosti IT v systémech zajišťovaných externími dodavateli
Odkaz na zprávu:	Shrnutí zprávy (anglické znění)
Datum zveřejnění:	2016
Název zprávy:	Zpráva o přístupu k informačním systémům, které podporují poskytování základních služeb dánské společnosti
Odkaz na zprávu:	Shrnutí zprávy (anglické znění)
Datum zveřejnění:	2015

Estonsko
Riigikontroll

Zajištění bezpečnosti a ochrana kritických státních databází v Estonsku

Datum zveřejnění: květen 2018

Odkaz na zprávu: Shrnutí zprávy (anglické znění)
Zpráva (estonské znění)

Druh auditu a auditované období

Druh auditu: Audit výkonnosti

Auditované období: 2017

Shrnutí zprávy

Téma auditu

Zachování estonské nezávislosti vyžaduje nejen fyzickou ochranu území, ale také ochranu digitálních statků, které s ohledem na incidenty představující největší hrozbu mají pro stát prvořadý význam. Digitální statky, které potřebují nejvíce chránit, jsou údaje týkající se občanů, území a právních předpisů. Zabezpečeny musí být rovněž údaje týkající se majetku, nemovitostí a práv osob s trvalým pobytem v Estonsku.

Národní kontrolní úřad prověřoval, jakým způsobem stát určil, které údaje a databáze mají zásadní význam pro zaručení národní bezpečnosti. Byla prověřována ochrana zabezpečení a kontinuity těchto údajů a databází, včetně přehledu nástrojů používaných k jejich ochraně.

Vzhledem k tomu, že Estonsko je nyní členem NATO a Evropské unie, je jeho fyzická bezpečnost zajištěna lépe než v době, kdy ještě nebylo součástí těchto sítí. Estonsko nicméně musí uvažovat o možnosti kybernetických hrozeb v případě eskalace bezpečnostních problémů. Takové rizikové scénáře a nárůst počtu incidentů v oblasti zabezpečení informací, jako jsou kybernetické útoky a úniky údajů, mohou být také nebezpečné pro ochranu údajů a databází, které jsou pro stát nejdůležitější. Pokud by

došlo k tomu, že údaje prvořadého významu pro stát byly neoprávněně změněny, nebo pokud by došlo k jejich úniku či ztrátě, stát by již nebyl schopen plnit nezbytné funkce, včetně zaručování bezpečnosti obyvatelstva, zajišťování nezbytných služeb, vytváření prostředí potřebného pro podnikání atd. Estonsko pro začátek plánuje vynaložit přibližně jeden milion EUR na uchovávání kritických údajů v zahraničí.

Auditní otázky

- Určila ministerstva všechny kritické databáze a požadavky na manipulaci s nimi?
- Jsou kritické databáze a rejstříky zabezpečeny?
- Je zaručena dlouhodobá kontinuita kriticky významných údajů a databází?

Zjištění

Pokud jde o kritické databáze, které byly předmětem auditu, vyslovil Národní kontrolní úřad následující připomínky:

- Pro účely provádění koncepce kritických databází nebyl stanoven žádný akční plán ani požadavky. Nebyly stanoveny podmínky pro výběr kritických databází a nebylo jisté, zda do tohoto procesu byly zahrnuty všechny potřebné databáze. Dodatečná ochrana databází byla organizována neformálně a nebyla povinná pro vlastníky databází. Údaje uložené v pěti kritických databázích nebyly proto zálohovány v zahraničí.
- V kritických databázích nebyla stanovena žádná další pravidla zajištění bezpečnosti informací. Ani bezpečnostní systém ISKE (norma pro bezpečnost informací, která byla vytvořena pro estonský veřejný sektor a která je povinná pro organizace státní správy i místní samosprávy mající přístup do databází / rejstříků), ani žádný právní akt či norma neobsahovaly dodatečné požadavky na kritické databáze, jako je zálohování údajů mimo Estonsko. Záložní kopie kontrolovaných databází byly odeslány do zahraničí, ale nebylo vyzkoušeno fungování informačních systémů po obnovení údajů z těchto záloh.
- Zavádění systému ISKE a provádění souvisejících auditů bylo v případě kritických databází problematické. V době konání auditu nebyl u dvou z deseti databází proveden jediný audit systému ISKE a audity byly zorganizovány teprve v závěru tohoto auditu (30. listopadu 2017). Pouze u dvou kritických databází byly prováděny audity tak často, jak to vyžaduje zákon. Vyskytly se také případy, kdy

auditor upozornil na problémy, ale tyto problémy nebyly v mezidobí mezi audity systému ISKE (tj. během dvou až tří let) vyřešeny.

- V průběhu auditu Národní kontrolní úřad zjistil, že v některých kritických databázích nebyla provedena některá důležitá opatření pro zajištění bezpečnosti informací. Například v pokynech pro bezpečnost informací nebyly stanoveny požadavky na pravidelné posuzování slabých míst informačních systémů, nebyly provedeny pravidelné kontroly nebo analýzy záznamů událostí, neexistovaly žádné plány odborné přípravy v oblasti bezpečnosti informací ani analýzy informovanosti o problematice bezpečnosti informací v oblasti veřejné správy, která má být základem těchto plánů odborné přípravy, v některých případech nebyla zkontrolována neporušenost souborů a nebyly provedeny žádné externí penetrační testy.

Závěry a doporučení

Na základě auditu se ukázalo, že navzdory zavedení třístupňového základního bezpečnostního systému ISKE, jehož používání je pro státní agentury a jejich audity povinné, vykazovalo několik kritických databází významné nedostatky z hlediska zajištění bezpečnosti informací, které se týkaly mj. analýzy protokolů, penetračního testování a ochrany mobilních zařízení. Zvláštní požadavky na ochranu kritických údajů nebyly dosud stanoveny.

Ministerstvo hospodářství a spojů začalo podnikat první kroky nezbytné k zajištění ochrany kritických údajů, projekt kritických databází byl nicméně ve fázi, kdy vyžadoval právně závazný soubor pravidel. Neexistovala ani podrobná analýza rizik, ani akční plán s výhledem do budoucna.

Záložní kopie pěti kritických databází byly uchovávány na velvyslanectvích v zahraničí, ale v případě fyzického zničení datových center nacházejících se v Estonsku by uchování kritických údajů ve zbývajících pěti databázích nebylo zaručeno.

Byla předložena dvě obecná doporučení:

- Stanovit pravidla pro dodatečnou ochranu kritických databází, včetně pravidel pro výběr kritických databází, zpracovávání údajů v těchto databázích a zálohování údajů, které jsou pro stát kriticky důležité, a posoudit, jak zajistit dodatečné financování těchto činností.

- Provést analýzu jednotlivých fází vytváření databází, a to jak z hlediska finančního plánování, tak z hlediska bezpečnosti informací, a při realizaci těchto fází uplatňovat osvědčené postupy projektového řízení.

Irsko
Office of the Comptroller and Auditor General

Opatření týkající se národní kybernetické bezpečnosti

Datum zveřejnění: září 2018

Odkaz na zprávu: Shrnutí zprávy (anglické znění)

Druh auditu a auditované období

Druh auditu: Audit výkonnosti

Auditované období: 2011–2018

Shrnutí zprávy

Téma auditu

Za politiku kybernetické bezpečnosti v Irsku odpovídá Ministerstvo pro komunikace, klimatická opatření a životní prostředí. Ministerstvo je rovněž jako zastřešující organizace Národního střediska pro kybernetickou bezpečnost odpovědné za koordinaci postupu vlády v mimořádných situacích způsobených bezpečnostními incidenty na celostátní úrovni.

Národní středisko pro kybernetickou bezpečnost bylo zřízeno v roce 2011. Zaměřuje se především na zabezpečení vládních sítí, na pomoc průmyslu a jednotlivcům při zajišťování ochrany jejich vlastních systémů a na zabezpečení kritické vnitrostátní infrastruktury.

Auditní otázky

V rámci tohoto šetření se prověřovalo, jakého pokroku bylo dosaženo, pokud jde o opatření v oblasti kybernetické bezpečnosti, od zřízení irského Národního střediska pro kybernetickou bezpečnost. Šetření se zabývá zejména otázkami, které se týkají:

- mandátu a zdrojů financování střediska;

- národní strategie kybernetické bezpečnosti (2015–2017);
- provádění směrnice EU o sítích a informačních systémech;
- mechanismů řízení a dohledu.

Zjištění a závěry

Vláda svým rozhodnutím o zřízení Národního střediska pro kybernetickou bezpečnost schválila roční rozpočet ve výši 800 000 EUR, skutečný roční rozpočet na kybernetickou bezpečnost v letech 2012 až 2015 však nedosahoval ani třetiny této částky. V roce 2017 se objem přidělených prostředků zvýšil na 1,95 milionu EUR. Počet zaměstnanců střediska se v roce 2017 téměř zdvojnásobil na 14,5 plného pracovního úvazku. V roce 2018 bylo schváleno jmenování dalších 16 zaměstnanců.

Národní strategie kybernetické bezpečnosti (2015–2017) stanovila 12 opatření, jichž má být v průběhu trvání této strategie dosaženo. Ke květnu 2018 byla dokončena čtyři opatření, čtyři byla provedena částečně a čtyři provedena nebyla.

Cílem směrnice EU o sítích a informačních systémech je zvýšit odolnost klíčových sítí a informačních systémů. Posouzení pokroku, jehož bylo v Irsku dosaženo ve vztahu ke všem třem pilířům, které tato směrnice stanoví, vedlo k těmto závěrům:

- *Pilíř 1 – Zlepšení schopností členských států EU v oblasti kybernetické bezpečnosti.* Částečně provedeno – pracuje se na plnění strukturální požadavků, ale ve strategickém plánování jsou stále mezery.
- Pilíř 2 – Usnadnění spolupráce v oblasti kybernetické bezpečnosti mezi členskými státy EU. Provedeno.
- *Pilíř 3 – Zavedení bezpečnostních opatření a povinností týkajících se hlášení incidentů pro klíčová odvětví.* Částečně provedeno – je třeba ještě dokončit práci spojenou s identifikací kritických sítí a informačních systémů formálním určením subjektů jako provozovatelů základních služeb (OES) a řízením poskytovatelů digitálních služeb.

Rozhodnutím vlády (červenec 2011), kterým se schvaluje zřízení Národního střediska pro kybernetickou bezpečnost, bylo schváleno rovněž zřízení meziresortního výboru pro stanovení a provádění politiky pro řešení problémů v oblasti kybernetické bezpečnosti v Irsku. V letech 2013 až 2015 se tato skupina sešla sice pětkrát, během

přezkumu byl však k dispozici zápis jen z jedné schůze. Od roku 2015 se už výbor nesešel.

Prováděcí plán národní strategie kybernetické bezpečnosti obsahuje závazek, že na konci roku 2017 bude zveřejněna výroční zpráva a provedeno formální posouzení dopadů činnosti střediska. To nebylo splněno, ačkoli práce střediska je popsána ve výroční zprávě ministerstva.

Ministerstvo formálně požádalo o posouzení výkonnosti střediska. O provedení tohoto posouzení nebyly předloženy žádné doklady. Ministerstvo uvedlo, že posouzení výkonnosti práce Národního střediska pro kybernetickou bezpečnost je součástí běžného řízení výkonnosti a správy a řízení ministerstva.

Audit vedl k závěru, že:

- ačkoli Národní středisko pro kybernetickou bezpečnost plní zásadní funkci, v prvních čtyřech letech svého provozu mělo oproti původním představám výrazně nižší objem prostředků.
- celkové strategické směřování střediska je nejasné a v současnosti mu chybí jakýkoli strategický plán.
- musí být také jasněji vymezeny příslušné úlohy orgánů zapojených do vyšetřování kybernetické kriminality a vnitrostátních bezpečnostních incidentů.
- provedeny musí být ještě požadavky týkající se vypracování vnitrostátní strategie, které stanoví směrnice EU o informačních a komunikačních systémech.
- struktury správy byly sice stanoveny, ale není jasné, jak tyto správní mechanismy fungují v praxi.

Chybí transparentní informace o dostupnosti a objemu prostředků vyhrazených na kybernetickou bezpečnost.

Francie
Cour des comptes

Přístup k vysokoškolskému vzdělávání: počáteční posouzení zákona o studijním poradenství a úspěšnosti studia

Datum zveřejnění: únor 2020

Odkaz na zprávu: Zpráva (francouzské znění)

Druh auditu a auditované období

Druh auditu: Audit výkonnosti

Auditované období: 2019–2020

Shrnutí zprávy

Téma auditu

Cílem zákona o volbě studijního zaměření a zvýšení úspěšnosti studentů z roku 2018 (*loi relative à l'orientation et à la réussite des étudiants*, zkr. ORE) bylo zlepšit tři hlavní etapy na cestě mladých lidí, kteří se hlásí ke studiu na vysoké škole: pomoc při volbě studijního zaměření a podpora pro studenty vyšších ročníků středních škol, výběr kursů a úspěšný průběh prvních let studia. Na základě tohoto zákona vznikl „*Parcoursup*“, nová digitální platforma, která slouží jako zdroj informací o nabízených kursech a požadavcích na přijetí ke studiu a která má za cíl posilovat soulad mezi schopnostmi a výsledky středoškolských studentů a obsahem kursů terciárního vzdělávání.

Během prvních dvou let platnosti zákona ORE byl učiněn první krok ke změně v přístupu k vysokoškolskému vzdělávání. Platformu „*Parcoursup*“ se navzdory četným omezením podařilo zprovoznit velmi hladce, třebaže stále postrádala záruky bezpečnosti a udržitelnosti a údaje bylo možné vzhledem k jejich důležitosti využívat lépe.

Zákon ORE byl přijat s tím, že má vyřešit dva hlavní problémy školské politiky. Prvním z nich byla vysoká míra předčasného ukončování školní docházky mezi vysokoškolskými

studenty. Druhým problémem bylo to, že stará digitální platforma vedla k hluboké nespokojenosti, protože v poslední fázi používala náhodný výběr.

Na reformu, kterou přinesl zákon ORE, byly během pěti let poskytnuty finanční prostředky ve výši 867 milionů EUR. Základem této reformy byla myšlenka kontinuální škály „-3/+3“ a jejím východiskem byla zásada, že čím více toho studenti vyšších ročníků středních škol vědí o obsahu kursů terciárního vzdělávání, tím lepší jsou jejich vyhlídky na úspěšné složení zkoušek, protože si budou vybírat kursy, které nejlépe odpovídají jejich způsobilosti a jejich ambicím. Zákon ORE byl veden snahou překonat situaci, kdy studenti vyšších ročníků středních škol nenacházejí dostatečnou pomoc při volbě studijního zaměření, a omezit tak přecházení na jiné studijní kursy, které s sebou podle odhadů *Cour de comptes* nese jen prvním roce vysokoškolského studia téměř 550 milionů EUR nákladů ročně.

Auditoři provedli úvodní posouzení dostupnosti vysokoškolského vzdělávání v rámci zákona ORE, přičemž se zaměřili na otázky bezpečnosti IT, které tato platforma otevřela.

Informační systém se vyznačoval stále větší přetížeností (v roce 2020 obsahoval všechny vysokoškolské kursy a v průběhu několika málo let se prudce zvýšil počet jeho uživatelů). Tento stav byl důsledkem příliš rychlého přechodu z předchozí platformy na platformu „*Parcoursup*“, k němuž došlo bez toho, aby se změnila její architektura, a s tím pak byla spojena značná rizika, pokud jde o kvalitu, kontinuitu, přizpůsobitelnost a další rozvoj této služby. Slabá místa systému v oblasti bezpečnosti, výkonnosti a robustnosti nebyla opravena. Rychlé vytvoření platformy „*Parcoursup*“ bylo možné díky tomu, že v beta režimu ji spravovala omezená skupina vysoce kvalifikovaných a motivovaných lidí, ale tento přístup s sebou nesl to, že opatření postrádala strategické směřování a uspokojivou správu.

Auditoři posuzovali kvalitu informačního systému a výkonnost nové platformy „*Parcoursup*“. Platforma „*Parcoursup*“ byla vytvořena na základě zákona ORE s cílem zlepšit kvalitu výběru vysokoškolských kursů a výrazně tak zvýšit podíl absolventů vysokých škol.

Zjištění

I když platforma „*Parcoursup*“ fungovala uspokojivě, byla zatížena riziky IT, která bylo třeba omezit. Nenabízela dostatečné záruky bezpečnosti a udržitelnosti a její údaje mohly být využívány lepším způsobem.

Zastaralost informačního systému

Platforma „Parcoursup“ obsahovala jen málo nových prvků a zdědila od předchozí platformy „Admission Post-Bac“ (APB) její těžkopádnost a nestabilitu a spolu s tím i řadu nevyřešených rizik. Informační systém tvořící strukturální základ platformy „*Parcoursup*“ byl převzat přímo z předchozí platformy. Přestože platforma „*Parcoursup*“ byla inzerována jako nástroj pro výběr vysokoškolských kursů, jádro jejího informačního systému se od platformy APB lišilo jen málo. Ve skutečnosti zůstalo více než 72 % informační infrastruktury beze změny a přepsáno bylo jen necelých 30 % kódu platformy APB.

Základní informační systém platformy byl navržen krátce po roce 2000, přičemž se vycházelo z představy, že platforma bude zpracovávat přibližně jeden milion žádostí na přibližně 100 000 míst ročně. Předpokládané zatížení nového informačního systému však bylo mnohem větší, protože měl každoročně zvládnout příliv přibližně 10 milionů žádostí na přibližně jeden milion míst. Platforma „*Parcoursup*“ vznikla renovací starého nástroje. Větší zatížení vyvolalo pochybnosti o tom, zda je platforma schopna plnit svůj zamýšlený účel.

Špatná dokumentace informačního systému

Navzdory úsilí ministerstva o transparentnost byl zdrojový kód platformy „*Parcoursup*“ z 99 % stále nepřístupný. To, co bylo zveřejněno, bylo příliš málo na to, aby na základě toho bylo možné pochopit, posoudit a zhodnotit proces přiřazování uchazečů k jednotlivým kursům.

Stejně jako její předchůdkyně měla i platforma „*Parcoursup*“ špatnou dokumentaci svého operačního informačního systému. Na základě výsledků auditu programového kódu bylo možné soudit, že aplikace je nekvalitní a vysoce riziková, a audit odhalil řadu kritických chyb. Systém byl méně kvalitní než jiný podobně starý software a riziko jeho selhání bylo vysoké.

Platforma „*Parcoursup*“ používala veřejný i nepřístupný zdrojový kód. Otevřený kód vykazoval mnohem vyšší míru kritických chyb než uzavřený kód, což s sebou neslo riziko narušení služby. Platforma nebyla ani chráněna před hackerskými útoky (bezpečnostní audit zdrojového kódu z července 2018). Na konci roku 2019 nicméně ministerstvo oznámilo, že zahájilo certifikační řízení pro kód „*Parcoursup*“.

Dokumentace zdrojového kódu, která existovala, nebyla ani ucelená, ani úplná. Kód aplikace „*Parcoursup*“ byl neobvykle složitý. Auditoři byli toho názoru, že zdrojový kód by měl být restrukturalizován, aby se počet jeho příliš složitých úseků snížil.

Architektura informačního systému „Parcoursup“ byla vysoce riziková; databáze byla spravována ručně, což je v dnešní době zcela nevídané. Nestabilita systému spočívala v tom, že systém předpokládal přítomnost a bdělost provozovatelů. Ministerstvo uznalo, že s architekturou platformy „*Parcoursup*“ jsou spojena vysoká rizika a že bez dalšího vývoje aplikace jsou tato rizika nenapravitelná.

Informační systém platformy „*Parcoursup*“ měl nedostatečnou dokumentaci a v podstatě bylo nutné spoléhat na znalosti zaměstnanců národní vládní agentury (Service à Compétence Nationale – SCN). V rámci dokumentace byly vkládány poznámky přímo do databáze, která tvoří jádro systému, což ztěžuje údržbu a vývoj informačního systému a využívání údajů. Informace o uživatelích uchovávané v rámci platformy nebylo možné snadno získat a vyhodnotit je bez hloubkového zkoumání. Vzhledem k nedostatku strukturované technické dokumentace je schopnost SCN plnit své strategické úkoly zcela závislá na vedoucím střediska informačních technologií.

Bezpečnostní strategie – potřebná zlepšení

Vzhledem k citlivosti osobních údajů obsažených v systému představuje aplikace „*Parcoursup*“ opravdovou bezpečnostní výzvu. Všechny organizace spravující nějaký informační systém by v zásadě měly mít formální písemně stanovená pravidla bezpečnosti informačních systémů (ISSP). Přestože aplikace „*Parcoursup*“ byla předsedou vlády schválena jako klíčový poskytovatel služeb, žádná pravidla bezpečnosti informačních systémů (ISSP) neměla. K zavedení těchto pravidel bylo zapotřebí okamžitého opatření.

Každý tým pro správu aplikace „*Parcoursup*“ měl svého referenta pro bezpečnost informačních systémů (ISSO) podléhajícího středisku IT. V souladu s osvědčeným postupem by bylo to, aby tito referenti podléhali přímo řediteli SCN, čímž by byla zaručena jejich nezávislosti.

Ještě v polovině roku 2019 se pracovalo na tom, aby platforma „*Parcoursup*“ byla v souladu s obecným nařízením o ochraně osobních údajů. Některá opatření nebyla stále ještě uskutečněna. Především bylo třeba formálně stanovit různé postupy používané pro zpracovávání údajů. Stále nebyla dostatečným způsobem zajištěna bezpečnost osobních údajů a stále se ukládalo zbytečně velké množství individuální údajů.

Oddělení pro platformu „*Parcoursup*“ se zodpovídalo jednak projektovému vedoucímu platformy, kterého jmenovalo ministerstvo, jednak odboru pro strategii odborné přípravy a studentské záležitosti Generálního ředitelství pro vysokoškolské vzdělávání a

profesní integraci, a bylo tudíž loajálním dvěma různým nadřízeným subjektům. Praktické otázky týkající se informačního systému „*Parcoursup*“ byly projednávány na schůzích, které se konaly jednou týdně. Tato forma organizace práce byla sice výhodná v tom, že umožňovala rychle reagovat, ale pokud jde o každodenní řízení studentských toků, byla platforma „Parcoursup“ bez jakéhokoli strategického řízení.

V neposlední řadě je třeba říci, že systém nebyl dostatečně transparentní. Navzdory obrovskému potenciálu neumožňoval optimální využívání údajů, které platforma uchovávala. Mobilizace tohoto potenciálu by téměř jistě přinesla výsledky v oblasti výkonnosti.

Závěry a doporučení

Vláda prostřednictvím digitální platformy zahrnující všechny vzdělávací programy úspěšně centralizovala přístup ke všem druhům postsekundárního studia, což ji umožnilo řešit otázku generalizace vysokoškolského vzdělávání. Předchozí systém, na jehož základě vznikla platforma „*Parcoursup*“, byl však přepracován příliš rychle, a na provedení podstatných strukturálních změn už nezbyl čas. Slabá místa informačního systému z hlediska bezpečnosti, výkonnosti a robustnosti proto nebyla odstraněna, ačkoli vzhledem k záměru obsáhnout všechny pregraduální kursy bylo nevyhnutelné, že zatížení aplikace se bude zvyšovat. Systém měl také špatnou dokumentaci, jeho vývoj svědčil o poněkud neprofesionálním přístupu a jeho neobvyklá složitost zvyšovala riziko chyb v případě jakýchkoli provozních změn. Platforma tak byla zatížena významnými riziky, pokud jde o kvalitu a kontinuitu veřejné služby a bezpečnost osobních údajů.

Cour des comptes vydal následující doporučení:

- IT tým SCN by měl mít lepší personální obsazení a finanční prostředky na provádění zákona ORE by měly být přerozděleny tak, aby byly posíleny lidské a finanční zdroje odboru pro informační systémy a statistický výzkum;
- informační systém by měl být vytvořen tak, aby mohl dlouhodobě fungovat, a za tímto účelem by měly být odstraněny jeho nejnaléhavější nedostatky, jeho architektura by měla být modernizována nebo nově vyvinuta a primární databáze starého systému i aplikace „*Parcoursup*“ by měly být systematickým a strukturovaným způsobem zdokumentovány;
- pro informační systém aplikace „*Parcoursup*“ by měla být stanovena bezpečnostní pravidla;

- měl by vzniknout společný řídící orgán Ministerstva školství a mládeže a Ministerstva pro vysokoškolské vzdělávání, výzkum a inovace, který by na platformu „*Parcoursup*“ dohlížel, přičemž jeho financování by mělo být zajištěno přerozdělením prostředků vyhrazených v rámci provádění zákona ORE na činnosti v oblasti „poradenství“.

Lotyšsko
Valsts Kontrole

Využila veřejná správa všech příležitostí k účinnému řízení infrastruktury IKT?

Datum zveřejnění: červen 2019

Odkaz na zprávu: Shrnutí zprávy (anglické znění)

Druh auditu a auditované období

Druh auditu: Audit výkonnosti

Auditované období: 2017–2019

Shrnutí zprávy:

Téma auditu

Lotyšský Státní kontrolní úřad dokončil audit výkonnosti, který se zaměřil na účinnost veřejné infrastruktury IKT. Účelem auditu bylo ověřit, zda je v oblasti veřejné správy uplatňován jednotný přístup k účinnému řízení infrastruktury IKT a zda dotčené instituce provedly posouzení přínosů centralizace. Pro hodnocení možností další optimalizace plánování byla za důležitou otázku považována také bezpečnost datových center.

Zdráhavý postoj orgánů k centrálnímu řízení infrastruktury IKT, projevující se přinejmenším na úrovni jednoho ministerstva, vedl k tomu, že vznikl větší počet serverových místností, což výrazně zvýšilo náklady na údržbu. Na čtyřech ministerstvech, kde byl proveden audit, bylo zjištěno, že jejich 22 dílčích útvarů využívá 38 datových center. V průběhu auditu národní kontrolní úřad zaznamenal situace, kdy informační systémy značného, dokonce celostátního významu byly umístěny v prostorách bez dostatečného zabezpečení. Optimalizace počtu serverových místností by umožnila nejen snížit náklady na IKT, ale zajistit i dostatečnou úroveň bezpečnosti, a to při nižších nákladech. V prověřovaných institucích byly tehdy již k dispozici důkladně zabezpečené serverové místnosti, které však nebyly plně využívány.

Hlavní předmět auditu

Cílem auditu bylo ověřit, zda byly vytvořeny a splněny všechny nezbytné podmínky jednotného řízení infrastruktury IKT, které by napomohlo účinnějšímu a bezpečnějšímu využívání zdrojů IKT.

Zjištění a závěry

Správa a optimalizace IKT

- Neexistovala dlouhodobá vize rozvoje a optimalizace IKT, a to ani na celostátní úrovni, ani na jednotlivých ministerstvech. Ministerstva a jejich útvary optimalizovaly infrastrukturu IKT v souladu podle vlastních představ a kapacit.

V letech 2011 až 2017 vzrostly institucím, u nichž byl prováděn audit, celkové náklady na údržbu IKT ze 17 na 20 milionů EUR ročně. Dotčené instituce neměly zaveden žádný postup pro pravidelné posuzování otázky, zda by pro ně bylo levnější, kdyby si svou infrastrukturu IKT udržovaly samy, nebo kdyby spolupracovaly s jinou institucí nebo kdyby údržbu IKT svěřily externímu poskytovateli. Centralizace ani decentralizace IKT není cílem sama o sobě, nýbrž je zapotřebí provést analýzu konkrétní situace a alternativních možností, aby se jasně ukázalo, jaké jsou stávající náklady a jaké jsou možné alternativy.

Bezpečnost informačních a komunikačních technologií

- Právní rámec nevymezil jasné bezpečnostní požadavky na infrastrukturu IKT, které by tvořily logický systém zohledňující význam zpracovávaných informací. Nebyly stanoveny žádné podrobné technické požadavky na ochranu datových center IKT.

- Důsledkem nedostatečně vymezených bezpečnostních požadavků byly zbytečně vysoké náklady na ochranu, nebo naopak to, že ochrana informací celostátního významu nebyla zajištěna. Důležité informační systémy byly dokonce umístěny v datových centrech s nedostatečným zabezpečením.

- Ve většině serverových místností byly nějaké bezpečnostní hrozby a datová centra nebyla dostatečně chráněna před vstupem nepovolaných osob a před riziky pro životní prostředí. Prevence bezpečnostních hrozeb by si v závislosti na zvoleném přístupu vyžádala nejméně 247 000 EUR – 765 000 EUR. Spočívala by: 1) v modernizaci serverových místností, ve kterých se nacházejí důležitější informační systémy a zajištění uchovávání významných zdrojů IKT v lépe zabezpečených datových centrech; nebo 2) v modernizaci všech stávajících

serverových místností. V takovém případě by si však vyžádala investice, které by podle auditorů byly ospravedlnitelné pouze za předpokladu minimalizace počtu datových center.

Právní rámec byl neúplný, protože pro infrastrukturu IKT nebyly stanoveny žádné podrobné bezpečnostní požadavky. Byly například stanoveny požadavky na různá kritéria týkající se logické bezpečnosti, ale nebyla však stanovena žádná kritéria pro fyzickou a environmentální bezpečnost infrastruktury, což má rovněž vliv na dostupnost systémů a ochranu údajů. V dokumentech, které se týkají plánování veřejné politiky, se sice zdůrazňoval význam bezpečnosti infrastruktury IKT a potřeba jejího posílení, ale nikdo v této oblasti neplánoval konkrétní činnosti. Skutečnost, že neexistovalo jasné, srozumitelné a logické rozlišení bezpečnostních požadavků, s sebou nesla riziko, že v rámci jedné a téže země budou platit různé bezpečnostní požadavky vztahující se na zpracovávání informací stejné důležitosti a stejného významu.

Sledování bezpečnosti v digitálním prostoru prováděl stát centrálně a stát také reagoval na incidenty, k nimž v tomto prostoru docházelo, ale odpovědnost za zajišťování bezpečnosti infrastruktury IT byla ponechána na každém vedoucímu jednotlivých institucí. V tom, jak vnímaly problematiku bezpečnosti IKT, jak hodnotily význam zpracovávaných informací a jaké zdroje měly pro řešení problémů v oblasti bezpečnosti IKT k dispozici, se tak mezi sebou tyto instituce značně lišily.

Bylo třeba stanovit systém pravidelného sledování těchto procesů, aby bylo možné nezávisle a za použití standardních kritérií hodnotit celou veřejnou správu jako jediný systém, identifikovat různé přístupy a předcházet jim zjišťováním společných rizik a plánovat preventivní opatření k jejich zmírnění.

Litva
Valstybės Kontrolė

Řízení kritických státních informačních zdrojů

Datum zveřejnění: červen 2018

Odkaz na zprávu: Shrnutí zprávy (anglické znění)
Zpráva (litevské znění)

Druh auditu a auditované období

Druh auditu: Audit výkonnosti

Auditované období: 2014–2017

Shrnutí zprávy

Téma auditu

Při využívání kritických státních informačních zdrojů – kriticky významných elektronických informací – vykonává vláda důležité správní funkce, jako je správa veřejných financí, daňová správa a řízení zdravotnictví. Jakákoli ztráta kritických informací nebo nedostupnost odpovídajících informačních systémů by mohla mít závažné důsledky pro veřejnou bezpečnost, blahobyt i hospodářství. Posuzování obecné kontroly IT, které prováděl litevský národní kontrolní úřad (NAOL) v letech 2006 až 2016, odhalilo opakující se problémy v oblasti řízení IT (plánování, definice informační architektury, organizační struktura, změny, zajištění kontinuity provozu, zabezpečení údajů, monitorování a hodnocení řízení IT). NAOL provedl audit kritických státních informačních zdrojů s cílem posoudit řízení a bezpečnost těchto zdrojů a stanovit opatření ke zlepšení.

Cílem auditu bylo zhodnotit řízení (obecnou kontrolu) a vyspělost kritických státních informačních zdrojů a určit systémové problémy.

NAOL posoudil vyspělost řízení IT ve 12 organizacích veřejného sektoru[64], které spravují 44 státních informačních systémů prvořadého významu. Audit byl proveden v souladu s požadavky na audit veřejných orgánů a mezinárodními normami nejvyšších kontrolních institucí. Posouzení bylo provedeno v souladu s metodikou COBIT[65] v níže uvedených nejrizikovějších oblastech: strategické plánování IT; určení informační architektury; řízení rizik IT; řízení změn; zajištění nepřerušeného poskytování služeb; zabezpečení systému; správa údajů; monitorování a hodnocení činností IT; zajištění řízení IT. Hodnocení procesu zahrnovalo jak organizační, tak vnitrostátní řízení IT a interakci těchto úrovní řízení.

Auditní zjištění

Změny v úrovni vyspělosti, pokud jde o řízení kritických státních informačních zdrojů, se vyvíjely pozitivně. Vzhledem k rostoucí míře kybernetických hrozeb byl však pozorovaný pokrok příliš pomalý a zabezpečení těchto zdrojů bylo nutné zlepšit. Důvodem byly níže uvedené nedostatky.

- Systém identifikace kritických státních informačních zdrojů nebyl dostatečně účinný, aby umožnil zavádět bezpečnostní řešení, která odpovídají skutečným potřebám:
  - hodnocení, která měla prokázat kritický význam státních informačních zdrojů, nebyla objektivní, při opětovném posuzování nebyly někdy vyhodnocovány změny, celý tento proces nebyl monitorován na celostátní úrovni a pokyny pro stanovení kritického významu informací nezajišťovaly účinné provádění.
  - systém pro určování kritických státních informačních zdrojů a kritické informační infrastruktury nebyl normalizován; zdroje a infrastruktura byly

[64] Státní daňová inspekce, Státní ústřední podnikatelský rejstřík, odbor informačních technologií a komunikací, Rada Státního fondu sociálního zabezpečení, Státní středisko pro zemědělské informace a podnikání na venkově, Středisko celního informačního systému, Státní potravinářská a veterinární služba, Úřad parlamentu Litevské republiky, Ministerstvo financí, Výbor pro rozvoj informační společnosti, Státní fond pacientů, Státní lesnická správa.

[65] COBIT (*Control Objectives for Information and Related Technologies*) je normou mezinárodní organizace ISACA, která stanoví osvědčené postupy pro řízení IT.

určovány na základě významu informací a služeb různým způsobem, což proces určování těchto zdrojů komplikovalo.

— nebyla vytvořena žádná celostátní informační architektura, která by představovala státní informační systémy a jejich vzájemné vztahy, znázorňovala rozsah kritických státních informačních zdrojů a umožňovala přijímat informovaná rozhodnutí o důležitosti těchto zdrojů.

o Řízení státních informačních zdrojů musí být více v souladu s osvědčenými postupy a normami řízení IT, aby bylo možné docílit v oblasti informačních technologií integrovaného zlepšení, které přispěje k většímu pokroku v řízení kritických státních informačních zdrojů:

— plánování IT nebylo udržitelné: plánované nástroje IT byly prezentovány v různých dokumentech, nadměrný počet strategických dokumentů znemožňoval jakýkoli systematický přístup, takže bylo obtížnější určit klíčové priority a prostředky nasměrovat na zajištění ochrany proti největším hrozbám.

— V rámci monitorování IT nebylo zajištěno, aby organizace měřily efektivnost IT operací a aby audity prováděné pracovníky odpovědnými za řízení kritických státních informačních zdrojů dosvědčovaly skutečnou vyspělost řízení IT. Státní řízení IT nebylo na celostátní úrovni předmětem kontroly a otázky řízení IT nebyly systematicky analyzovány. Byl vytvořen systém pro kontrolu souladu státních informačních zdrojů s požadavky na bezpečnost elektronických informací, jehož účelem je pouze usnadnit kontrolu dodržování bezpečnostních požadavků, avšak jeho funkce nebyly v dostatečné míře využívány.

o Opatření k zajištění odolnosti kritických informačních zdrojů na úrovni kybernetických hrozeb nebyla dostatečně účinná; riziko narušitelnosti těchto zdrojů proto stále trvá:

— účinnost posuzování rizik v oblasti bezpečnosti IT by se měla zvýšit, protože nebyla zjištěna všechna významná rizika a metodika jejich posuzování nebyla v souladu s nejnovějšími postupy řízení IT; nebylo zajištěno včasné řízení nepřijatelných rizik.

— nebyla systematicky využívána organizační bezpečnostní opatření, která by mohla rizika kybernetické hrozby omezit. Nedostatečné testování bezpečnosti, nedůsledné proškolování pracovníků v průběhu vývoje

informačních systémů, jejich modernizace a úprav; nevyhovující řízení kontinuity činnosti IT a vytváření záložních souborů ohrožovala obnovení funkčního celku; měření bezpečnostní výkonnosti bylo nedostatečné a nepřispívalo ke zvyšování bezpečnosti.

Závěry

Řízení IT u subjektů veřejného sektoru, které byly předmětem auditu, dosáhlo za posledních deset let v průměru první úrovně vyspělosti z celkových pěti[66] a v době sestavování této zprávy dosahovalo stupně 1,7. Tato nízká úroveň vyspělosti kritických státních informačních zdrojů svědčí o nedostatcích ve vytváření koncepce politiky státních informačních zdrojů a v jejím provádění, což zvýšilo zranitelnost těchto zdrojů. Pokud se má bezpečnost těchto zdrojů zvýšit, je třeba zlepšit mechanismus řízení státních informačních zdrojů, aby pokud možno co nejlépe odpovídala osvědčeným postupům. Auditoři rovněž konstatovali, že opatření, která mají zaručit odolnost kritických informačních zdrojů vůči kybernetickým hrozbám, nejsou dostatečně účinná. Posuzování rizik v oblasti bezpečnosti IT je proto třeba zefektivnit, a to tak, že při vytváření a modernizaci informačních systémů a v rámci vzdělávání zaměstnanců bude kladen větší důraz na testování bezpečnosti.

Další zprávy v této oblasti

Název zprávy:	Je boj proti kybernetické kriminalitě účinný?
Odkaz na zprávu:	Shrnutí zprávy (anglické znění) Zpráva (litevské znění)
Datum zveřejnění:	2020

Název zprávy:	Prostředí kybernetické bezpečnosti v Litvě
Odkaz na zprávu:	Shrnutí zprávy (anglické znění) Zpráva (litevské znění)
Datum zveřejnění:	2015

[66] Podle metodiky COBIT.

Maďarsko
Národní kontrolní úřad

Audit ochrany údajů – Audit vnitrostátního rámce na ochranu údajů a některých záznamů prioritních údajů v rámci mezinárodní spolupráce

Datum zveřejnění: březen 2017

Odkaz na zprávu: Zpráva (maďarské znění)

Druh auditu a auditované období

Druh auditu: Soulad s předpisy

Auditované období: 2011–2015

Shrnutí zprávy

Téma auditu

Zabezpečení národních datových souborů je jedním z hlavních zájmů společnosti usilující o zachování a ochranu národních hodnot. Zajištění větší bezpečnosti osobních i veřejných údajů, které jsou součástí národních datových souborů Maďarska, má proto zásadní význam pro posílení důvěry občanů ve stát a pro zajištění nepřetržitého a bezproblémového fungování veřejné správy. Proto má ochrana údajů a bezpečnostní síť, které zajišťuje právní rámec pro její prosazování, klíčový význam pro společnost.

Co se týče oblasti ochrany údajů, klíčovou úlohu při správě největších a nejcitlivějších rejstříků údajů, které patří k vnitrostátním datovým souborům, hraje veřejná správa. Správci údajů pro rejstříky spolu při plnění svých úkolů úzce spolupracují. Pravidelně převádějí rejstříky obsahující velké množství údajů a musejí se přitom řídit zákonnými požadavky na ochranu údajů. Používání elektronických informačních systémů pro správu a zpracování údajů má v současné době zásadní význam, takže řádné a spolehlivé fungování těchto systémů musí být zaručeno řádně navrženými a provozovanými kontrolami.

Maďarský Státní kontrolní úřad klade ve svých auditech velký důraz na ochranu údajů. V letech 2011 až 2015 provedl komplexní audity ochrany údajů, o nichž vydal v prvním čtvrtletí roku 2017 svou zprávu. Audit se rovněž zabýval otázkami paralelně probíhajících mezinárodních auditů, které byly prováděny ve spolupráci s pracovní skupinou EUROSAI IT a které se týkaly především souladu se stávajícími směrnicemi Evropské unie.

Účelem auditu souladu s právními předpisy v oblasti ochrany údajů v Maďarsku bylo posoudit, zda je v Maďarsku zaveden regulační a operační rámec pro ochranu údajů a zda nejvýznamnější organizace zajišťující správu údajů splňují požadavky na bezpečnou správu údajů a externí zpracovávání údajů. Audit se zaměřil zejména na ochranu osobních údajů a vnitrostátních datových souborů.

V rámci tohoto auditu Státní kontrolní úřad hodnotil správu dat v šesti organizacích pro správu údajů (například: finanční úřad, státní pokladna, zdravotní pojištění, vyplácení penzí, školský úřad, osobní údaje a adresy, evidence vozidel a cestovních dokladů a správní orgány pro správu údajů o trestné činnosti), jakož i činnosti úřadu pro ochranu údajů a orgánu pro bezpečnost informací.

Audit kladl zvláštní důraz na mandát organizací pro správu údajů, zejména pokud jde o předávání údajů třetím stranám. Během auditu vnitřních kontrol správy a zpracování údajů bylo hodnoceno, zda existují aktuální předpisy upravující povinnosti, odpovědnost a pravomoci, jakož i řízení lidských zdrojů a procesů.

Pokud jde o elektronické systémy používané pro účely správy údajů, Státní kontrolní úřad posuzoval související bezpečnostní opatření, a to i v oblasti fyzické ochrany, přístupových práv, protokolování, postupů pro posuzování bezpečnosti, bezpečnosti systémů a komunikací a souladu bezpečnostní klasifikace organizace jako celku.

Externí zajišťování zpracování údajů bylo kontrolováno na základě uzavřených smluv, přičemž se zjišťovalo, zda organizace spravující údaje zavazovaly organizace zpracovávající údaje k plnění požadavků týkajících se činností zpracování údajů v souladu s legislativními nařízeními.

Zjištění a závěry

Na základě tohoto auditu Státní kontrolní úřad v Maďarsku shledal, že vnitřní předpisy organizací spravujících údaje vztahující se na činnosti v oblasti správy údajů zajišťovaly ochranu národních datových souborů jako součásti národního majetku v souladu s právními předpisy platnými v letech 2011 až 2015. V praxi správci údajů řádně

uplatňovali požadavky na bezpečnou správu údajů a externí zajišťování zpracování údajů. Předávání údajů třetím stranám bylo prováděno na základě náležitého mandátu a s jasným vymezením odpovědností a pravomocí.

U některých správců údajů bylo zjištěno, že bezpečnostní klasifikace elektronických systémů a organizace jako celku nebyla vždy v souladu s právními požadavky, ale rozsah nedostatků podstatně neovlivnil bezpečnost zpracovávaných údajů. Na základě doporučení obsažených ve zprávě o auditu odstranily organizace pro správu údajů nedostatky v rámci akčních plánů schválených nejvyšším kontrolním orgánem.

V souvislosti s paralelně probíhajícím mezinárodním auditem realizovaným ve spolupráci s pracovní skupinou EUROSAI IT státní kontrolní úřad zjistil, že maďarské právní předpisy v oblasti ochrany údajů jsou v souladu se stávající směrnicí EU.

Závěrem lze říci, že auditem ochrany údajů přispěl maďarský Státní kontrolní úřad k řádné správě věcí veřejných a k ochraně vnitrostátních datových souborů.

Další zprávy v této oblasti

Název zprávy:	Zpráva – Následné audity – Audit ochrany údajů – Audit vnitrostátního rámce pro ochranu údajů a některých záznamů klíčových údajů v rámci mezinárodní spolupráce
Odkaz na zprávu:	Zpráva (maďarské znění)
Datum zveřejnění:	2020

Nizozemsko
Účetní dvůr

Kybernetická bezpečnost kritických vodních staveb a hraničních kontrol v Nizozemsku

Data zveřejnění: březen 2019 a duben 2020

Odkaz na zprávy: Shrnutí zprávy o kybernetické bezpečnosti a kritických vodních stavbách (anglické znění)

Shrnutí zprávy o kybernetické bezpečnosti a o automatizované hraniční kontrole (anglické znění)

Druh auditu a auditované období

Druh auditu: Audit výkonnosti

Auditované období: 2018–2020

Shrnutí zprávy

Téma auditu

V roce 2018 nizozemský Účetní dvůr rozhodl, že provede audity kybernetické bezpečnosti v odvětvích, která mají pro společnost kritický význam. Na základě dlouholetých zkušeností s auditem dodržování právních předpisů v oblasti bezpečnosti informací na úrovni ústřední vlády spatřoval Účetní dvůr přidanou hodnotu v tom, že provede audit *výkonnosti* politik a opatření v praxi. První dvě auditovaná odvětví se týkala řízení vodních zdrojů a automatizovaných hraničních kontrol, přičemž první z nich je důležité kvůli tomu, že velká část území se nachází pod úrovní mořské hladiny, a druhé kvůli úloze amsterdamského letiště Schiphol jako mezinárodního uzlu a vstupní brány do země.

Ministr infrastruktury a řízení vodních zdrojů určil jako „kritické části“ vodohospodářského odvětví řadu vodních staveb spravovaných Generálním ředitelstvím pro veřejné práce a řízení vodních zdrojů (dále jen „auditovaný subjekt“). Mnoho počítačových systémů používaných k řízení provozu kritických vodních staveb

pochází z 80. a 90. let 20. století, kdy se na „kybernetickou bezpečnost“ obvykle nebral zřetel. Tyto systémy byly původně navrženy pro samostatný provoz, postupně však byly propojeny s rozsáhlejšími počítačovými sítěmi, což mělo například usnadňovat jejich dálkové řízení. V důsledku tohoto vývoje jsou tyto systémy zranitelnější vůči kybernetickým hrozbám.

Ministr obrany a ministr spravedlnosti a bezpečnosti jsou společně odpovědní za hraniční kontroly prováděné nizozemskou pohraniční stráží na letišti Schiphol. Obě ministerstva (auditované subjekty) vlastní IT systémy, na které se příslušníci pohraniční stráže spoléhají. Systémy mají zásadní význam pro provoz letiště a používají se ke zpracování vysoce citlivých údajů. Jsou tak zajímavým terčem kybernetických útoků zaměřených na sabotáž, špionáž nebo manipulaci s hraničními kontrolami.

Při auditech se prověřovalo, jak byly auditované subjekty připraveny řešit kybernetické hrozby a zda je řešily účinným způsobem.

- Cílem auditu bylo získat odpovědi na tyto auditní otázky: Jak auditované subjekty *chrání* systémy před kybernetickými hrozbami a jak *předcházejí* kybernetickým útokům?
- Jakým způsobem auditované subjekty kybernetické hrozby a útoky *odhalují*?
- Jak auditované subjekty *reagují* v situaci, kdy ke kybernetickému útoku dojde?

Samostatným tématem obou auditů byla otázka účinnosti. V úzké spolupráci s auditovanými subjekty pracovali etičtí hackeři na testování kritických vodních staveb a na jednom ze systémů hraniční kontroly. Není třeba říkat, že pozitivní výsledky těchto testů vedly k přijetí opatření ještě před zveřejněním zpráv a že nebyly zveřejněny žádné technické podrobnosti.

Hlavní rozdíl mezi oběma audity spočíval v tom, že audit vodních staveb se zaměřil na plnění cílů auditovaného subjektu, zatímco audit ochrany hranic vycházel z rámce Národního ústavu pro normalizaci a technologie (NIST) pro kybernetickou bezpečnost.

Zjištění

Oba audity předně zjistily, že auditované subjekty byly obeznámeny s kybernetickými hrozbami a že v současné době pracují na zavedení profesionálního přístupu k této věci.

V případě vodních staveb bylo nicméně nezbytné, aby auditovaný subjekt přijal některá další opatření pro odhalování hrozeb a reakci na ně, aby splnil své vlastní cíle, které si v oblasti kybernetické bezpečnosti stanovil. Auditovaný subjekt zřídil Středisko pro bezpečnostní operace (SOC), které má odhalovat kybernetické útoky a reagovat na ně. Cíl, který měl být splněn do konce roku 2017 a který spočíval v tom, že má být zajištěno okamžité odhalení kybernetických útoků namířených proti kritickým vodním stavbám, však nebyl splněn ještě na podzim roku 2018. To znamená, že existuje riziko, že kybernetický útok zacílený na kritickou vodní stavbu nebude odhalen nebo bude odhalen pozdě. Zkouška provedená na jedné z kritických vodních staveb navíc ukázala, že k ní bylo možné získat fyzický přístup. Hackerům se podařilo získat přístup do řídicí místnosti a byli v ní sami s nezabezpečenými pracovními stanicemi. Auditovaný subjekt neměl také připravený žádný krizový scénář pro případ kybernetického útoku a informace týkající se reakce buď nebyly k dispozici, nebo nebyly aktualizovány. Dostupnost aktuálních informací by mohla být pro rychlou a účinnou reakci na krizovou situaci rozhodující.

Pokud jde o hraniční kontroly, opatření pro zajištění kybernetické bezpečnosti byla buď nepřiměřená, nebo nevyhovující s ohledem na budoucí rizika. Předně bylo nutné, aby před zahájením provozu byly důležité systémy hraniční kontroly formálně schváleny a byla tak zajištěna realizace všech opatření v oblasti kybernetické bezpečnosti. Zjistili jsme, že dva ze tří systémů byly v provozu bez předchozího schválení, tzn. že zavedení nezbytných bezpečnostních opatření nebylo zaručeno. Zadruhé jedno středisko pro bezpečnostní operace (SOC) sice fungovalo, ale nemělo přímé spojení s žádným z těchto systémů. Mělo sice spojení s obecnou infrastrukturou, ale riziko, že kybernetické útoky nebudou odhaleny nebo budou odhaleny pozdě, stále existuje. Zatřetí nebyly pravidelně prováděny bezpečnostní testy. V minulosti byl ve skutečnosti testován pouze jeden ze tří systémů, a to pouze v omezené míře. A konečně, stejně jako tomu bylo při prvním auditu, nebyl připraven žádný konkrétní krizový scénář pro případ kybernetického útoku.

Na základě bezpečnostního testu jednoho ze systémů, které nikdy předtím nebyly testovány, zjistili etičtí hackeři řadu slabých míst. Při součinnosti obeznámeného, ale neoprávněného zaměstnance, který by měl zlý úmysl, by tato slabá místa mohla být využita k zahájení kybernetického útoku s cílem získat přístup k informacím uloženým v systému, zkopírovat tyto informace, nebo s nimi dokonce manipulovat. Tyto výsledky ukazují význam pravidelného testování bezpečnosti.

Vzhledem k probíhající automatizaci hraničních procesů jsou uvedená zjištění znepokojivá. V blízké budoucnosti bude stále větší počet systémů hraniční kontroly

zpracovávat stále větší množství údajů a bude využívat stále větší počet propojení. Riziko kybernetických útoků se tím zvyšuje; uplatňovaný přístup byl proto s ohledem na budoucí rizika nevyhovující.

Závěry

V případě vodních staveb neumožnily některé klíčové prvky auditovanému subjektu přijmout konečná opatření v oblasti kybernetické bezpečnosti. Nebylo například jasné, jaká je míra ohrožení, takže bylo obtížné posoudit, zda přijatá opatření a přidělené rozpočtové prostředky jsou nebo nejsou dostatečné. Ústřední útvar odpovědný za kybernetickou bezpečnost navíc neměl mandát k provádění nezbytných opatření v oblasti kybernetické bezpečnosti v decentralizovaných vodních stavbách. Doporučení auditu byla v tomto ohledu dodržena a pomohla organizaci v dalším postupu.

Pokud jde o hraniční kontroly, neexistoval žádný jasný důvod, který by opodstatňoval nedostatečnou úroveň kybernetické bezpečnosti. Auditní šetření vedlo k závěru, že postupy a pravidla v oblasti kybernetické bezpečnosti jsou úplná a podrobná a že odborné znalosti a kvalifikace zaměstnanců jsou dostatečné. Doporučení auditu spočívalo proto především v tom, že je třeba zajistit faktické uskutečnění všech těchto možností.

Oba audity vzbudily velkou pozornost parlamentu a sdělovacích prostředků. Zvýšily povědomí o kybernetické bezpečnosti životně důležité infrastruktury a poskytly auditovaným subjektům informace o tom, jak svou kybernetickou bezpečnost mohou posílit. Úzká spolupráce s auditovaným subjektem měla pro úplné pochopení jeho situace a řešení rizik spojených s prověřováním a testováním kybernetické bezpečnosti zásadní význam.

V rámci této série auditů je rovněž naplánován třetí audit. Úroveň zabezpečení informací nizozemské národní vlády je navíc klíčovou součástí ročního cyklu auditu souladu s právními předpisy. V průběhu let nizozemský nejvyšší kontrolní orgán zjistil, že úroveň opatření v oblasti informační bezpečnosti je na mnoha ministerstvech nevyhovující. Účetní dvůr se v současné době snaží využít zkušeností, které na základě svých auditů kybernetické bezpečnosti získal, k rozšíření vlastního pohledu na prověřování zabezpečení informací a kromě dokumentů a politik testuje také skutečnou účinnost opatření.

Další zprávy v této oblasti

Název zprávy: Kapitola 3 dokumentu „Staat van de rijksverantwoording 2019“
Odkaz na zprávu: Zpráva (nizozemské znění)
Datum zveřejnění: 2020

Název zprávy: Zaměření na digitální práci z domova
Odkaz na zprávu: Zpráva (nizozemské znění)
Datum zveřejnění: 2020

Polsko
Najwyższa Izba Kontroli (NIK)

Zajištění bezpečnosti provozu informačních systémů používaných k plnění veřejných úkolů

Datum zveřejnění: 2016

Odkaz na zprávu: Zpráva (polské znění)

Druh auditu a auditované období

Druh auditu: Soulad s předpisy

Auditované období: 2014–2015

Shrnutí zprávy

Téma auditu

Účelem auditu bylo posoudit, zda byly údaje shromážděné v systémech určených k plnění důležitých veřejných úkolů v auditovaných útvarech zabezpečené. Audit se týkal šesti vybraných institucí, které plní významné veřejné úkoly. Na základě analýzy byl v každé z institucí vybrán jeden základní informační systém, který byl poté podrobně prověřen. Při auditu byla použita verze 4.1 metody COBIT (*Control Objectives for Information and related Technology*).

Tento audit byl proveden v návaznosti na audit plnění úkolů v oblasti kybernetické bezpečnosti polskými veřejnými subjekty[67], který proběhl v roce 2015 a který ve svých zjištěních poukázal na systémové problémy. Audit z roku 2016 mimo jiné prokázal, že státní správa doposud nepřijala opatření k zajištění bezpečnosti IT na celostátní úrovni. Vedl k závěru, že činnosti veřejných subjektů související s ochranou kybernetického prostoru byly prováděny namátkově a bez systematického přístupu. Vzhledem k tomu, že nebyla stanovena žádná ústřední opatření k zajištění konkrétních bezpečnostních podmínek pro konkrétní systémy IT, které jsou nezbytné pro fungování státu, se audit

[67] https://www.nik.gov.pl/kontrole/P/14/043/

zaměřil na ověření toho, zda orgány spravující informační systémy používané k plnění důležitých veřejných úkolů zajistily, aby tyto úkoly byly prováděny bezpečně.

V roce 2019 byl schválen další systémový audit týkající se kybernetické bezpečnosti nazvaný „Kybernetická bezpečnost v Polsku“. Zjištění tohoto auditu jsou však důvěrná.

Auditní otázky

Jednotlivé dílčí cíle spadaly do dvou oblastí hodnocení, přičemž šlo o nalezení odpovědí na konkrétní otázky.

V oblasti podpory bezpečnosti IT prošetřoval audit prováděný na úrovni celé organizace mimo jiné tyto otázky:

- zda je prováděno řízení bezpečnosti IT;
- zda jsou prováděny plány na zajištění bezpečnosti IT;
- zda je zabezpečení IT testováno, dozorováno a sledováno;
- zda jsou definovány bezpečnostní incidenty v oblasti IT;
- zda jsou při správě IT používány kryptografické klíče;
- zda je zaveden postupy na ochranu před škodlivým softwarem a postupy pro jeho odhalování a zda jsou aplikovány opravy;
- zda je zajištěna bezpečnost sítí.

V oblasti podpory bezpečnosti audit prošetřoval na úrovni vybraných systémů mimo jiné tyto otázky:

- zda jsou spravovány uživatelské identity a účty;
- zda jsou chráněny bezpečnostní technologie a citlivé údaje.

Zjištění a závěry

Míra připravenosti a zavedenosti systému zabezpečení informací nezajišťovala přijatelnou úroveň bezpečnosti údajů shromažďovaných v informačních systémech, které mají plnit důležité veřejné úkoly. Procesy, které mají zajišťovat bezpečnost informací, byly uplatňovány chaoticky a intuitivně, protože nebyly stanoveny příslušné postupy. Z šesti kontrolovaných oddělení mělo pouze jedno zavedený systém

zabezpečení informací a je třeba poznamenat, že i jeho provoz se vyznačoval závažnými nedostatky. V žádném z auditovaných útvarů kromě jednoho nebyla práce na zajištění vhodných podmínek zabezpečení informací zpracovávaných v informačních systémech na odpovídající úrovni, neboť se vzhledem k tomu, že byla zahájena teprve nedávno, nacházela ve své přípravné fázi, jejíž součástí bylo rovněž vytvoření nezbytných formálních základů. Práce probíhala na základě zjednodušených nebo neformálních ujednání, která vycházela z osvědčených postupů nebo z dosavadních zkušeností pracovníků IT.

V souladu s metodikou COBIT 4.1 se vyspělost procesu řízení bezpečnosti informací v různých auditovaných útvarech pohybovala na stupnici od nuly do pětky, která představuje maximum, v rozmezí od 1) počáteční/*ad hoc* do 3) definované.

Odpovědnost za zajištění bezpečnosti IT v auditovaných útvarech měl bezpečnostní koordinátor, který však v praxi neměl pravomoc řídit celý proces. Úkoly, které byly s tímto procesem spojeny, také často vykonávala pouze jedna osoba. I když byly jmenovány specializované týmy nebo byly uzavřeny dohody s externími dodavateli, nezbytná analýza, na jejímž základě by bylo možné zjistit, zda poskytované služby odpovídají bezpečnostním potřebám útvaru, nebyla provedena. Auditované útvary chápaly potřebu zajistit bezpečnost IT porůznu a v omezené míře. Zabezpečení údajů bylo považováno především za odpovědnost a oblast působnosti oddělení IT, a nikoli všech organizačních útvarů se statutárními úkoly, což značně bránilo vývoji soudržných systémů řízení bezpečnosti IT pro celou instituci.

Při srovnávání kvality způsobu plnění povinností týkajících se zajištění bezpečnosti informací na úrovni celé organizace i vybraných systémů se ukázalo, že ve druhém případě byla kvalita provádění vyšší. Důvodem mohou být dopady praktických znalostí a zapojení technických pracovníků střední úrovně do zajištění bezpečnosti, větší míra využívání komerčních informačních systémů založených na tržních normách ve veřejné správě a pokročilá bezpečnostní řešení. Díky uplatňování takových řešení, dříve získaných zkušeností a osvědčených postupů bylo možné zachovat určitou úroveň bezpečnosti provozu různých systémů i při omezených zdrojích, organizačních nedostatcích nebo nefunkčních předpisech. Takový stav ovšem nemůže být cílovým řešením, neboť v době dynamicky narůstajícího ohrožení nemůže být bezpečnost informačních systémů založena na opatřeních řízených chaotickým způsobem, která mají pouze překonávat bezprostřední potíže.

Závěry auditu

Pokud jde o zabezpečení IT, je třeba na ústřední úrovni vypracovat a provádět obecná doporučení a požadavky, které budou platit pro všechny veřejné subjekty. Je třeba najít systémové řešení, které umožní, aby výsledky auditů bezpečnosti IT byly zveřejňovány způsobem, který občanům umožní přístup k informacím o činnosti veřejných subjektů, ale aby přístup k informacím o opatřeních a metodách používaných k zajištění bezpečnosti zpracovávaných údajů byl omezen.

Další zprávy v této oblasti

Název zprávy:	Řízení zabezpečení informací na úrovni regionálních orgánů
Odkaz na zprávu:	Zpráva (polské znění)
Datum zveřejnění:	2019

Název zprávy:	Kybernetická bezpečnost v Polsku (utajované informace)
Odkaz na zprávu:	*Není veřejně dostupné.*
Datum schválení:	2019

Název zprávy:	Zajištění bezpečnosti informačních systémů na úrovni regionálních orgánů v Podleském vojvodství
Odkaz na zprávu:	Zpráva (polské znění)
Datum zveřejnění:	2018

Název zprávy:	Prevence kyberšikany a boj proti ní mezi dětmi a mládeží
Odkaz na zprávu:	Zpráva (polské znění)
Datum zveřejnění:	2017

Název zprávy:	Provádění úkolů v oblasti kybernetické bezpečnosti Polské republiky ze strany veřejných subjektů
Odkaz na zprávu:	Zpráva (polské znění)
Datum zveřejnění:	2015

Název zprávy:	Plnění vybraných požadavků vztahujících se na informační systémy, elektronickou výměnu informací a celostátní rámec pro interoperability na příkladech některých městských zastupitelstev a měst s postavením okresu.
Odkaz na zprávu:	Zpráva (polské znění)
Datum zveřejnění:	2015

Portugalsko
Tribunal de Contas

Audit portugalského elektronického pasu

Datum zveřejnění: 2014

Odkaz na zprávu: Zpráva (portugalské znění)

Druh auditu a auditované období

Druh auditu: Audit výkonnosti

Auditované období: 2013

Shrnutí zprávy

Téma auditu

Provozní audit portugalského elektronického pasu (PEP) se zaměřil na účinnost informačních systémů, které slouží pro účely jeho udělování, vydávání a používání, zejména v rámci automatizovaného prověřování cestujících na portugalských hranicích za pomoci biometrických údajů[68].

- Hlavní auditní cíle byly: ověřit soulad s právními předpisy EU a vnitrostátními právními předpisy, mezinárodními normami a pokyny pro udělování, vydávání a používání PEP, včetně přiměřenosti vnitrostátního právního rámce;
- prověřit účinnost klíčových procesů souvisejících s životním cyklem PEP, zejména pak procesů, které souvisejí s jeho udělováním, vydáváním a používáním;
- prověřit kritické aspekty výkonnosti informačních systémů, zejména splnění bezpečnostních požadavků týkajících se informačních systémů PEP (SIPEP).

[68] Odkazujeme na systémy automatizované hraniční kontroly (ABC) používané agenturou Frontex (Evropská agentura pro pohraniční a pobřežní stráž).

Mezi klíčové rizikové oblasti patřila:

- ztráta/odcizení hmotného majetku a/nebo elektronických informací;
- zneužití důvěrných informací;
- riziko neplnění předpisů (nedodržování právních a správních požadavků).

Auditované období: 1. leden 2013 – 31. prosinec 2013 (v některých případech i v předcházejících a následujících letech).

Zjištění a závěry

Portugalský elektronický pas (PEP) má tři kategorie: základní[69], diplomatický nebo speciální. Existuje rovněž pas pro cizí státní příslušníky, který poskytuje menší výsady.

Koncesní systém zahrnuje několik žádostí a několik subjektů pro shromažďování údajů a udělujících orgánů, ale pouze jeden vydávající orgán (který pas vystavuje, personalizuje a doručuje dotčené osobě).

Tohoto procesu se účastní několik subjektů (subjekty PEP). Níže uvedené subjekty shromažďují údaje a udělují pasy:

- Pevninské Portugalsko: Serviço de Estrangeiros e Fronteiras (SEF)[70] a rejstříkové služby Instituto dos Registos e do Notariado (IRN)[71];
- Autonomní oblasti Azory[72] a Madeira: služby poskytuje příslušné Vice-Presidência do Governo Regional[73]; v zahraničí: portugalské konzuláty;
- The Imprensa Nacional – Casa da Moeda, S.A. (INCM)[74] vystavuje a doručuje pasy.

---

[69] Přibližně 99 % z celkového počtu.

[70] Oddělení pro přistěhovalectví a hranice.

[71] Registrační úřad a notářství (pouze pro příjem).

[72] A kontaktní místa Agência para a Modernização e Qualidade do Serviço ao Cidadão, I. P. (RIAC) – Agentura pro modernizaci a kvalitu služeb pro občany, veřejný institut (pouze pro příjem).

[73] Úřad místopředsedy regionální vlády.

[74] Úřední tiskárna a mincovna, veřejná společnost.

Hlavní procesy zajišťuje většinou SIPEP (centrální systém pro vyřizování žádostí o vydání portugalských pasů). SIPEP umožňuje zaznamenávat, uchovávat, zpracovávat, ověřovat a poskytovat požadované informace související s udělením PEP, spouští proces personalizace, který provádí INCM, zajišťuje propojení s jinými systémovými aplikacemi a koordinuje všechny subjekty PEP zapojené do fyzické a logistické registrace shromažďovaných údajů.

Subjekty PEP mají organizační strukturu, která jim umožňuje plnit zákonné účely, které jsou s PEP spojeny. Pokud jde o žádosti a shromažďování údajů, je systém do značné míry stále závislý na lidských zdrojích. SIPEP však zahrnuje několik automatických zpracovatelských funkcí a ověřovacích kontrol.

Vzhledem k tomu, že postupy zajišťují kontrolní funkce a manipulaci s údaji, z nichž některé mohou být prováděny nezávisle bez lidského zásahu, má program SIPEP významný dopad z hlediska organizace a informačního systému, zejména pokud jde o: i) chápání a vymezení norem, procesů a požadovaných údajů; a ii) vymezování vlastních požadavků informačního systému.

Efektivnost a účinnost procesu shromažďování údajů zajišťuje interakce systému SIPEP s jinými informačními systémy[75] v souladu s právními předpisy.

Byl zaveden rámec pro celkovou kontrolu činností v oblasti informačních technologií (správa, vývoj a akvizice, operace IT, kontinuita činnosti a obnova po havárii, zabezpečení informací), který zajišťuje vývoj, provoz, řízení a údržbu systému SIPEP (není ovšem dostatečně podrobně zdokumentován).

Ukazatele činnosti (2013):

- Bylo uděleno přibližně 500 000 pasů PEP, z toho přibližně 63 % jich bylo uděleno prostřednictví systému SEF, 33 % z nich vydaly portugalské konzuláty a 4 % regionální vlády;
- Příjmy dosažené vydáváním PEP činily celkem 37 milionů EUR, přičemž jejich větší část připadá na INCM (43 %), SEF (32 %) a Ministério dos Negócios Estrangeiros (MNE)[76] (17 %).

[75] Jmenovitě: Integrovaný informační systém SEF (SIISEF; vnitrostátní součást schengenského informačního systému (NSIS)); databáze údajů o totožnosti občanů, trestní rejstřík.

[76] Ministerstvo zahraničních věcí.

Testy provedené v roce 2013 v rámci programu SIPEP nepotvrdily dodržování zákonem stanovené maximální dodací lhůty (od data podání žádosti do okamžiku, kdy je PEP připraven k vyzvednutí na výdejním místě), protože skutečné datum dodání na výdejní místo nebylo vždy včas evidováno.

Investice související s pořízením zařízení pro sběr biometrických údajů a podpisů (kiosky), vybavením pro systémy automatizované hraniční kontroly (ABC) a s nákupem a údržbou systémů IT a souvisejících služeb a technické pomoci, které realizovaly SEF, MNE, RIAC a INCM, činily 11 milionů EUR, přičemž nejvyšší částku vynaložil SEF.

Před zavedením PEP byla cena (nebiometrického) pasu Portugalské republiky 22,44 EUR; v roce 2006 byla cena běžného (biometrického) PEP stanovena na 60 EUR a v roce 2011 vzrostla na 65 EUR.

Žádosti o PEP

Žádosti o vydání PEP jsou zpracovávány osobně příslušnými útvary, které přijímají dokumenty tvořící součást žádosti, shromažďují biografické a biometrické údaje žadatelů, vybírají poplatky a následně doručují vystavený PEP.

Základní systém (SIPEP) slouží k ověřování správnosti a kvality údajů prostřednictvím virtuálních kontrol a křížových odkazů s jinými informačními systémy, konkrétně s databází údajů o totožnosti občanů, aby bylo zajištěno, že žádost je v souladu se stanovenými požadavky a splňuje podmínky pro udělení a vystavení PEP.

Související změny stavu se zaznamenávají v protokolových souborech, čímž je zajištěna kontrolovatelnost, integrita a nespornost transakcí.

Předávání údajů mezi subjekty pro shromažďování údajů (v Portugalsku a v zahraničí) a SEF probíhá prostřednictvím VPN (Virtual Private Network) na základě správy přístupu v souladu s pověřovacími údaji, které má pod kontrolou SEF[77].

Žádost o základní PEP se zpracovává odlišně, pokud ji předloží občané, kteří mají méně práv nebo jim jejich práva byla omezena. Patří mezi ně: i) osoby, které nemohou vykonávat svá práva (osoby nezletilé, nesvéprávné nebo podléhající zákazu); ii) osoby označené soudem nebo policií (trestní rejstřík, probíhající soudní řízení nebo zabavení

[77] Systém SIPEP je (prostřednictvím internetu) na vnitrostátní/regionální i mezinárodní úrovni přístupný útvarům, které sídlí na pevnině, v autonomních oblastech Azory a Madeira a v zahraničí (portugalské konzuláty).

dokumentů); a iii) pokud se žadatel o druhý PEP odvolává na státní nebo oprávněný zájem.

Udělení PEP

Rozhodnutí o udělení základního PEP může být:

- Automatické – automatické schválení prostřednictvím systému SIPEP pro vyřizování žádostí poté, co je potvrzena totožnost žadatele a skutečnost, že nemá záznam v trestním rejstříku (křížová kontrola v databázích IRN, tj. v databázi údajů o totožnosti občanů a v rejstříku trestů) a že s ním není vedeno soudní řízení. Automaticky lze schvalovat pouze žádosti o vydání PEP, které byly podány na pevnině prostřednictvím systému SEF[78].
- Kromě případů, kdy byly individuálně přijaty / schváleny jinými subjekty (regionální vlády a konzulární úřady) nebo v případě žádostí podaných prostřednictvím systému SEF, které obsahují požadavky, které automatické udělení pasu neumožňují[79].

Vystavení PEP

Vystavení PEP, které zahrnuje vytvoření, personalizaci a doručení pasu, spadá do pravomoci INCM. Poté, co je v systému SIPEP proveden záznam o doručení PEP, změní se stav pasu na „platný“.

Sazby za vydání PEP se liší v závislosti na úrovni požadované služby. Úroveň služeb lze měřit poté, co systém SIPEP zohlední skutečné datum dodání PEP.

Doručení PEP zajišťuje smluvní doručovatelská služba.

---

[78] Jedná se o automatizovanou funkci systému SIPEP, která umožňuje udělit pas (interně označováno jako „povolení žádosti“) zletilému občanovi s platným občanským průkazem, se kterým není vedeno soudní řízení a kterému není držení pasu zakázáno nebo k jeho držení není nezpůsobilý (a nežádá o vydání druhého PEP). Postupy automatického potvrzování a automatické rozhodování o udělení se uplatnily přibližně u 60 % základních pasů PEP, o něž bylo požádáno prostřednictvím systému SEF; zbytek přezkoumával a schvaloval *Direção Central de Imigração e Documentação (DCID)*.

[79] Zejména v případech, kdy žadatelé nemohou vykonávat svá práva (osoby nezletilé, nesvéprávné nebo podléhající zákazu), osoby označené soudem nebo policií nebo v případě žádosti o druhý PEP osoby, jejichž žádost posuzuje DCID individuálně.

Ukončení platnosti PEP

Pokud žadatel přinese dříve vydaný, ale stále platný pas PEP, měl by být tento pas zneplatněn, aby se zamezilo jeho dalšímu používání, tzn. že v systému SIPEP by se měl stav uvedený u příslušného pasového záznamu změnit na „neplatný“.

Finsko
Valtiontalouden tarkastusvirasto

Zajištění kybernetické ochrany

Datum zveřejnění: 2017

Odkaz na zprávu: Zpráva (finské znění)

Druh auditu a auditované období

Druh auditu: Audit výkonnosti

Auditované období: 2016–2017

Shrnutí zprávy

Téma auditu

Účelem auditu bylo zjistit, zda je kybernetická ochrana na úrovni ústřední vlády organizována co nejúčinnějším a nákladově nejefektivnějším způsobem. Audit se zaměřil na způsob organizace a řízení kybernetické bezpečnosti ústředních vládních institucí. Výsledky auditu mohly být využity ke zvýšení účinnosti a efektivnosti kybernetické bezpečnosti na úrovni ústřední vlády. Audit probíhal od 22. září 2016 do 4. září 2017. Následná kontrola byla provedena na podzim 2019. V rámci této následné kontroly národní kontrolní úřad prověřoval opatření přijatá na základě zjištění a doporučení auditu.

Předmětem auditu byly orgány pověřené zajišťováním kybernetické ochrany v ústředních vládních institucích (Úřad předsedy vlády, Ministerstvo financí a Ministerstvo dopravy a spojů) a orgány odpovědné za centralizované úkoly v oblasti kybernetické ochrany a centralizované služby IT na úrovni ústřední vlády (Národní středisko pro kybernetickou bezpečnost finské Agentury pro dopravu a komunikace, vládní středisko IKT Valtori, Agentura pro digitální a populační datové služby). Posuzována byla rovněž účinnost pokynů, a to na základě prověřování útvarů ústřední vlády, které zajišťují elektronické služby (Agentura digitálních a populačních datových služeb, finská Agentura pro dopravu a komunikace Traficom, Národní správní úřad pro

vymáhání práva a Ministerstvo spravedlnosti, které nad ním vykonává dohled, a Středisko služeb IKT při Ministerstvu spravedlnosti).

Auditní otázky

Audit organizace kybernetické bezpečnosti sledoval tyto auditní otázky:

- Měl auditovaný subjekt při zajišťování organizace kybernetické bezpečnosti na zřeteli v dostatečné míře ekonomické hledisko?
- Napomáhají znalosti auditovaného subjektu o situaci v oblasti kybernetické bezpečnosti zajišťování kybernetické bezpečnosti systémů?
- Má auditovaný subjekt dostatečnou schopnost reagovat na kybernetické útoky?

Téma auditu, tj. zajištění kybernetické ochrany, bylo součástí auditního tématu „Zajištění provozní spolehlivosti informační společnosti“ v rámci auditního plánu finského Národního kontrolního úřadu na období 2016–2020. Z hlediska toho, jak významné je toto téma auditu pro finance ústřední vlády, může být odůvodněno s poukazem na nevýhody spojené s výpadky služeb a narušením ochrany údajů, ale i s poukazem na negativní dopady nedostatečné kybernetické bezpečnosti na podnikatelskou činnost. Audit byl prováděn souběžně s auditem „Řízení provozní spolehlivosti elektronických služeb“, které patří do stejného tematického okruhu. Hlavní auditní materiál sestával z dokumentů a rozhovorů s orgány odpovědnými za danou činnost.

Zjištění a závěry

Finská strategie kybernetické bezpečnosti definuje klíčové cíle a politiky pro řešení problémů kybernetického prostředí a pro zajištění jeho fungování. V rámci prováděcího programu, jehož pokrok je každoročně vyhodnocován, je vyvíjeno úsilí o provádění strategie kybernetické bezpečnosti. Provádění strategie kybernetické bezpečnosti sleduje a koordinuje Bezpečnostní výbor, který je orgánem pro spolupráci v rámci Ministerstva obrany.

Účinná organizace kybernetické bezpečnosti spočívá v řízení rizik, které k tomu, aby bylo úspěšné, vyžaduje účinné řídicí struktury a mechanismy umožňující začlenit řízení rizik do činností na všech úrovních organizace. Stejně jako mnoho dalších zemí není ani Finsko a jeho ústřední vláda soběstačné, pokud jde o zdroje kybernetické ochrany. Právní předpisy Evropské unie se postupem času rozrostly a jsou závaznější. Ve finské

vládě je odpovědnost za kybernetickou ochranu decentralizována, přičemž každá právnická osoba je odpovědná za svou vlastní kybernetickou bezpečnost. Na úrovni ústřední vlády je rozdělení povinností, pokud jde o povahu, rozsah a provádění případných kybernetických útoků, složité.

V důsledku této složitosti může být reakce na mimořádné situace příliš pomalá a omezené je kvůli nedostatečnému financování také provádění finské strategie kybernetické bezpečnosti. Na základě auditních zjištění dospěl národní kontrolní úřad k níže uvedeným závěrům a vydal následující doporučení týkající se organizace kybernetické bezpečnosti na úrovni ústřední vlády:

Nebyl vymezen způsob provozního řízení v případě rozsáhlého narušení kybernetické bezpečnosti

Plánování provozního řízení v případě rozsáhlého narušení kybernetické bezpečnosti a rozdělení souvisejících povinností by mohlo umožnit rychlejší reakci a náležitou koordinaci a přidělování prostředků na protiopatření. V současném provozním modelu je každá agentura odpovědná za vlastní kybernetickou ochranu. V oblasti kybernetické ochrany však není k dispozici dostatek odborných znalostí, což brání vybudování kybernetické ochrany ať už interně, nebo s pomocí externích poskytovatelů.

Některých cílů strategie kybernetické bezpečnosti nebylo dosaženo

Prováděcí program finské strategie kybernetické bezpečnosti kybernetickou ochranu zlepšil. Některých cílů prvního prováděcího programu nebylo dosaženo, protože míra závaznosti jednotlivých opatření byla různá a dosáhnout zlepšení centralizovaným způsobem nebylo možné. Nový prováděcí program zahrnoval pouze opatření, k jejichž realizaci se příslušné orgány a další subjekty výslovně zavázaly. Mezi závazky a dostupnými zdroji existovala vzájemná závislost.

Vhodnost zvolených řešení financování kybernetické ochrany byla nejasná

Rozdíly ve vývoji kybernetické ochrany byly částečně způsobeny rozdíly v objemu prostředků určených na vývoj, které měly organizace k dispozici. V nařízeních týkajících se přípravy státního rozpočtu nebo přípravného procesu nebyly stanoveny žádné postupy, které by zajistily, aby finanční prostředky byly přiděleny na nejdůležitější cíle kybernetické ochrany. Agentury a orgány vyčlenily prostředky na kybernetickou bezpečnost v rozpočtu jako nespecifikovanou součást provozních výdajů agentury nebo orgánu. Opatření popsaná ve finské strategii kybernetické bezpečnosti byla provedena pouze v rozsahu, který dovolovalo množství prostředků.

Změny v organizaci IKT by měly rovněž zohledňovat potřebu zajištění kybernetické ochrany

Změny v organizaci IKT ústřední vlády měly vliv na opatření v oblasti kybernetické ochrany. Ukázalo se, že další rozvoj kybernetické bezpečnosti na centralizované úrovni Valtori je obtížný. Objevily se nedostatky při posuzování přiměřenosti praktických postupů kybernetické ochrany i při provádění nových opatření.

Je třeba zlepšit situační povědomí o operacích v oblasti kybernetické bezpečnosti

Středisko pro kybernetickou bezpečnost dbalo o celostátní situační povědomí o kybernetické bezpečnosti. V době auditu neexistovala povinnost hlásit případy narušení kybernetické bezpečnosti Středisku pro kybernetickou bezpečnost. Stanovení požadavku, aby vládní organizace hlásily případy narušení kybernetické bezpečnosti, by situaci zlepšilo, stejně jako rozšíření působnosti centralizovaných postupů pro odhalování takových případů.

Na základě výše uvedených důvodů národní kontrolní úřad doporučuje, aby Ministerstvo financí definovalo a zavedlo obecný model provozního řízení pro případy kybernetických bezpečnostních incidentů, k nimž dojde ve službách IKT ústředních vládních institucí. Ministerstvo financí by mělo rovněž zjistit, jak má být otázka kybernetické bezpečnosti služeb zohledněna v rámci financování služeb po celou dobu jejich životního cyklu, a mělo by zlepšit operativní znalosti o situaci tím, že orgánům vydá pokyn, aby případy kybernetických útoků hlásily Středisku pro kybernetickou bezpečnost. Bylo doporučeno, aby Valtori zlepšila provádění, hodnocení a vývoj postupů v oblasti kybernetické bezpečnosti a odhalování případů jejího narušení.

Následný audit prověřoval, jak byla doporučení vydaná během auditu realizována. Kontrolní úřad měl za to, že Ministerstvo financí jako orgán odpovědný za realizaci těchto doporučení nepřijalo v návaznosti na vydaná doporučení dostatečná opatření. Kybernetická bezpečnost byla nicméně ve Finsku zároveň posílena díky opatřením, která přijaly jiné orgány než Ministerstvo financí. Probíhá změna strategického řízení kybernetické bezpečnosti, které přechází na model počítající s funkcí ředitele pro kybernetickou bezpečnost. V návrhu rozpočtu na rok 2020 vláda navýšila prostředky pro ústřední orgány státní správy, které v rámci posilování kybernetické bezpečnosti hrají klíčovou úlohu. Valtori navíc přijímala opatření v souladu s doporučením národního kontrolního úřadu. Závěrem národní kontrolní úřad uvedl, že kvůli nerealizovaným doporučením je nutno provést následný audit a že vzhledem k probíhajícím změnám v opatřeních v oblasti kybernetické bezpečnosti a digitálním provozním prostředí a vzhledem k rizikům, která s tím souvisejí, ale i vzhledem

k významu kybernetické bezpečnosti pro finance ústředních vládních institucí a pro společnost je odůvodněné provést v této oblasti zcela nový audit.

Švédsko
Riksrevisionen

Zastaralé systémy IT – překážka účinné digitalizace

Datum zveřejnění: 2019

Odkaz na zprávu: Shrnutí zprávy (anglické znění)
Zpráva (švédské znění)

Druh auditu a auditované období

Druh auditu: Audit výkonnosti

Auditované období: 2018–2019

Shrnutí zprávy

Téma auditu

Zastaralost informačních systémů, které jsou kriticky důležité pro činnost organizací, s sebou nese značné riziko neefektivnosti, protože organizace jsou úměrně tomu nuceny vynakládat více prostředků na pouhé udržování systému. Lze se proto důvodně domnívat, že se zastaralými systémy IT je spojeno vysoké riziko nesprávného hospodaření s veřejnými prostředky. Důsledkem je rovněž nevyužívání inovačních kapacit agentury na vývoj nových informačních systémů. Avšak kromě toho, že zastarávající systémy IT vytvářejí rizika pro jednotlivé agentury, mohou mít problémy v jedné agentuře závažné důsledky pro její schopnost koordinovat operace s jinou agenturou nebo se zúčastněnými soukromými subjekty. Zastarávající informační systémy jsou rizikové také z hlediska bezpečnosti informací.

Definice hlavního předmětu auditu / Auditní otázky / Souvislosti

Účelem auditu bylo prozkoumat, zda se v ústřední státní správě vyskytují zastaralé systémy IT, a zjistit, zda orgány a vláda přijaly vhodná opatření, která vyloučí, aby se systémy IT staly překážkou účinné digitalizace. Auditní otázky byly následující:

- Přijaly orgány vhodná opatření k řešení problémů spojených se zastaralými systémy IT?
- Přijala vláda vhodná opatření k řešení problémů spojených se zastaralými systémy IT?

Zjištění a závěry

- Na základě auditu se ukázalo, že zastaralé informační systémy se používají v celé řadě vládních agentur. V mnoha agenturách byl navíc zastaralý jeden nebo více informačních systémů, které jsou pro jejich činnost kritické. Pokud je švédskému národnímu kontrolnímu úřadu známo, jedná se o nové informace a nikdo předtím si nebyl vědom rozsahu tohoto problému v ústřední státní správě. Přibližně 80 % agentur uvedlo, že zachovat příslušnou úroveň bezpečnosti informací v jednom nebo více svých kritických systémech je pro ně obtížné. Více než jeden z deseti orgánů odpověděl, že tato obtíž se týká všech systémů nebo jejich většiny.
- Velká část prověřovaných agentur neměla k vývoji a správě podpory IT správný přístup. Nevyužívaly existující nástroje pro operační rozvoj, aby s jejich pomocí určily, jak by podpora IT mohla nejlépe přispět k dosažení cílů hlavních operací. Značná část agentur, které byly předmětem auditu, neměla tudíž celkový popis propojení strategií, operačních procesů a systémů. To ve svém důsledku znamenalo, že měly potíže s analýzou a pochopením toho, jaký vliv mají změny na cíle organizace, a bylo proto obtížnější definovat, jaká situace je do budoucna žádoucí.
- Více než polovina orgánů uvedla, že nemá žádný schválený model pro zacházení se svými informačními systémy a rozhodování o nich od fáze vývoje systému až po postupné ukončení jejich provozu, obvykle nazývaný řízení životního cyklu. Podle švédského národního kontrolního úřadu to svědčí o tom, že řízení životního cyklu nebylo prováděno strukturovaným a metodickým způsobem. Objevily se rovněž nedostatky v analýzách rizik a ve schopnosti rozložit náklady na IT v takové míře podrobnosti, která je nezbytná pro řádné rozhodování.

- Téměř 60 % orgánů postrádalo plány životního cyklu systému pro všechny ostatní systémy kromě jednoho nebo několik málo dalších, které byly kriticky důležité pro jejich činnost. Skutečnost, že mnohé agentury neměly plány životního cyklu a další plánovací dokumentace, a nedostatky ve skutečném řízení životního cyklu svědčí obecně o tom, že si ke svým informačním systémům nevytvořily uvědomělý a vyjádřený postoj.
- Švédský národní kontrolní úřad dospěl k závěru, že ministerstva, která byla předmětem auditu, a tedy i vláda, postrádala povědomí o výskytu zastaralých informačních systémů a jeho důsledcích.

Z auditu celkově vyplynulo, že v době jeho konání se většině agentur ještě reálně nepodařilo účinný způsobem řešit problémy spojené se zastaráváním informačních systémů. Švédský národní kontrolní úřad byl toho názoru, že problém je tak závažný a tak široce rozšířený, že představuje překážku pro další efektivní digitalizaci státní správy. Audit rovněž ukázal, že vláda neměla dostatečné povědomí o existenci a důsledcích problémů spojených se zastaralými informačními systémy. Vláda navíc nepřijala žádná opatření, která by problém zastaralých informačních systémů řešila přímějším způsobem. Švédský národní kontrolní úřad proto dospěl k závěru, že nelze mít za to, že vláda přijala dostatečná opatření k zajištění toho, aby byly problémy omezeny nebo odstraněny.

Další zprávy v této oblasti

Název zprávy: Usnadnění zakládání podniků – vládní úsilí o podporu digitálního procesu (RiR 2019:14)

Odkaz na zprávu: Shrnutí zprávy (anglické znění)
Zpráva (švédské znění)

Datum zveřejnění: 2019

Název zprávy: Digitalizace veřejné správy – Jednodušší, transparentnější a účinnější správa (RiR 2016:14)

Odkaz na zprávu: Shrnutí zprávy (anglické znění)
Zpráva (švédské znění)

Datum zveřejnění: 2016

Název zprávy: Činnost v oblasti bezpečnosti informací v devíti agenturách (RiR 2016:8)

Odkaz na zprávu: Shrnutí zprávy (anglické znění)
Zpráva (švédské znění)

Datum zveřejnění: 2016

Název zprávy: Kyberkriminalita – postup policie a státních zástupců může být účinnější (RiR 2015:21)

Odkaz na zprávu: Shrnutí zprávy (anglické znění)
Zpráva (švédské znění)

Datum zveřejnění: 2015

Evropská unie
Evropský účetní dvůr

Informační dokument: Výzvy pro účinnou politiku kybernetické bezpečnosti

Datum zveřejnění: 2018

Odkaz na zprávu: Zpráva (23 jazykových znění)

Druh auditu a auditované období

Druh auditu: Přezkum politiky

Auditované období: duben – září 2018

Shrnutí zprávy

Téma přezkumu

Cílem tohoto informačního dokumentu, který není zprávou z auditu, bylo poskytnout přehled o komplexní politice EU v oblasti kybernetické bezpečnosti a identifikovat hlavní problémy při jejím účinném provádění. Zabývá se bezpečností sítí a informací, kyberkriminalitou, kybernetickou obranou a dezinformacemi.

Analýza EÚD vycházela z dokumentárního přezkumu informací, které jsou veřejně dostupné v oficiálních dokumentech, písemných stanoviscích a studiích třetích stran. Práce přímo na místě probíhala od dubna do září 2018 a zohledněn byl vývoj do prosince 2018. EÚD v rámci své práce provedl také průzkum mezi národními kontrolními úřady členských států a pohovory s hlavními zainteresovanými stranami z orgánů EU a zástupci soukromého sektoru.

Neexistuje žádná standardní definice kybernetické bezpečnosti. Obecně řečeno to jsou veškeré pojistky a opatření přijatá na ochranu informačních systémů a jejich uživatelů před nepovoleným přístupem, útokem a poškozením s cílem zajistit zachování důvěrnosti, integrity a dostupnosti údajů. Kybernetická bezpečnost zahrnuje předcházení kybernetickým bezpečnostním incidentům, jejich odhalování, reakci na ně a zotavení. Incidenty mohou či nemusí být záměrné a mohou se například týkat

náhodného zveřejnění informací, ale i útoků na podniky a kritickou infrastrukturu, krádeže osobních údajů a dokonce i zasahování do demokratických procesů.

Základním kamenem politiky EU je Strategie kybernetické bezpečnosti z roku 2013. Tato strategie usiluje o to, aby se digitální prostředí EU stalo nejbezpečnějším na světě a aby současně bránilo základní hodnoty a svobody. Má pět základních cílů: zvýšení kybernetické odolnosti, ii) snížení kyberkriminality, iii) rozvoj politik a schopností kybernetické obrany, iv) rozvoj průmyslových a technologických zdrojů kybernetické bezpečnosti a v) vytvoření mezinárodní kyberprostorové politiky sladěné se základními hodnotami EU.

Zjištění

Vzhledem k nedostatku spolehlivých údajů bylo obtížné přesně popsat dopad špatné připravenosti na kybernetický útok. Hospodářský dopad kyberkriminality se v letech 2013 až 2017 zvýšil pětinásobně, zasáhl státy a společnosti, a to jak velké, tak malé. Tento trend odráží předpokládaný nárůst pojistného v oblasti kybernetiky ze 3 miliard EUR v roce 2018 na 8,9 miliardy EUR v roce 2020. Přestože 80 % podniků z EU zaznamenalo v roce 2016 alespoň jeden incident v oblasti kybernetické bezpečnosti, je uznání vážnosti těchto rizik stále znepokojivě nízké. Pokud jde o společnosti v EU, 69 % z nich nemá žádné nebo jen základní znalosti o tom, jak jsou vystaveny kybernetickým hrozbám, a 60 % nikdy neprovedlo odhad případných finančních ztrát. Podle globálního průzkumu by jedna třetina organizací raději zaplatila hackerovi výkupné, než aby investovala do informační bezpečnosti.

Zjištění EÚD byla následující:

- Kybernetický ekosystém EU je složitý a mnohovrstevný a zahrnuje velké množství zúčastněných stran. Spojení všech jeho nesourodých částí je velkou výzvou.
- Záměrem EU je stát se nejbezpečnějším online prostředím na světě. Dosažení těchto cílů vyžaduje značné úsilí všech zúčastněných stran, včetně řádné a dobře řízené finanční základny. Údaje není snadné získat, ale odhaduje se, že veřejné výdaje EU na kybernetickou bezpečnost se pohybují mezi jednou a dvěma miliardami eur ročně. Ve srovnání s tím se v rozpočtu na rok 2019 počítá s tím, že výdaje federální vlády USA budou činit přibližně 21 miliard USD.
- Řízení informační bezpečnosti znamená zavedení struktur a politik, které zajistí důvěrnost, integritu a dostupnost údajů. Více než jen technické řešení vyžaduje efektivní vedení, spolehlivé procesy a strategie sladěné s organizačními cíli.

- Modely řízení kybernetické bezpečnosti se v jednotlivých členských státech liší a v rámci nich je odpovědnost za kybernetickou bezpečnost často rozdělena mezi mnoho subjektů. Tyto rozdíly by mohly bránit spolupráci potřebné k reakci na rozsáhlé, přeshraniční incidenty a k výměně zpravodajských informací o hrozbách na vnitrostátní úrovni, a tím spíše i na úrovni EU.

- Vytvoření účinné reakce na kybernetické útoky je zásadní pro jejich co nejrychlejší zastavení. Zvláště důležité je to, aby kritická odvětví, členské státy a orgány EU byly schopny rychle a koordinovaně reagovat. Nezbytným předpokladem toho je včasné odhalení těchto útoků.

Doporučení

Z přehledu EÚD vyplývá, že pro zajištění odpovědnosti a hodnocení je nutný posun směrem ke kultuře založené na výkonnosti se zabudovanými hodnotícími mechanismy. Některé mezery v právních předpisech nadále přetrvávají a stávající právní předpisy nejsou členskými státy důsledně prováděny do vnitrostátních právních řádů. To může ztížit dosažení plného potenciálu právních předpisů.

Další zjištěná výzva se týká sladění objemu investic se strategickými cíli, což vyžaduje zvýšení úrovně investic a dopadu. Zvládnout tuto výzvu bude obtížnější, pokud EU a její členské státy nebudou mít jasný přehled o výdajích EU v oblasti kybernetické bezpečnosti. Byla rovněž zaznamenána omezení, pokud jde o přiměřené financování agentur EU v oblasti kybernetiky, včetně obtížného získávání a udržení talentovaných odborníků.

Zkratková slova a zkratky

APT: pokročilá trvalá hrozba (*Advanced Persistent Threat*)

CEF: Nástroj pro propojení Evropy

CERT-EU: skupina pro reakci na počítačové hrozby

COBIT: kontrolní cíle pro oblast informační a související technologie (*Control Objectives for Information and Related Technology*)

COVID-19: koronavirové onemocnění COVID 2019

cPPP: smluvní partnerství veřejného a soukromého sektoru

CSIRT: skupina pro reakce na počítačové bezpečnostní incidenty (*Computer Security Incident Response Team*)

DDoS: distribuované odepření služby (*Distributed Denial of Service*)

DEP: program Digitální Evropa

EC3: Evropské centrum Europolu pro boj proti kyberkriminalitě

EDA: Evropská obranná agentura

ENISA: Agentura Evropské unie pro kybernetickou bezpečnost

ESI fondy: evropské strukturální a investiční fondy

ESRB: Evropská rada pro systémová rizika

ESVČ: Evropská služba pro vnější činnost

EU: Evropská unie

EÚD: Evropský účetní dvůr

EUROPOL: Agentura Evropské unie pro spolupráci v oblasti prosazování práva

GDPR: obecné nařízení o ochraně údajů

HDP: hrubý domácí produkt

HR: lidské zdroje

IKT: informační a komunikační technologie

IoT: internet věcí

ISACA: Asociace pro audit a kontrolu informačních systémů

ISF-P: Fond pro vnitřní bezpečnost – policie

IT: informační technologie

MERS: koronavirus z Blízkého východu způsobující respirační syndrom

NAO: národní kontrolní úřad

NATO: Organizace Severoatlantické smlouvy

NCSS: Národní strategie kybernetické bezpečnosti

PESCO rámec stálé strukturované spolupráce

RDP: protokol ovládání vzdálené plochy

SAI: nejvyšší kontrolní instituce

SARS: těžký akutní respirační syndrom

SBOP: společná bezpečnostní a obranná politika

Směrnice NIS: směrnice o bezpečnosti sítí a informací

UK: Spojené království

URL: jednotný lokátor zdroje

USA: Spojené státy americké

VFR: víceletý finanční rámec

Glosář

5G: jedná se o technickou normu páté generace širokopásmových mobilních sítí, kterou výrobci mobilních telefonů začali zavádět po celém světě v roce 2019 a která se má stát nástupcem sítí 4G, jež zajišťují připojení u většiny současných mobilních telefonů. Zvýšení rychlosti je dosaženo zčásti tím, že na rozdíl od předchozích mobilních sítí jsou využívány vysokofrekvenční rádiové vlny.

Adware: škodlivý software zobrazující reklamní bannery nebo vyskakovací okna, které obsahují kód pro sledování chování obětí on-line.

Bezpečnost sítě: podskupina kybernetické bezpečnosti chránící údaje předávané prostřednictvím zařízení ve stejné síti s cílem zajistit, že informace nebudou zachyceny ani změněny.

Biometrické údaje (biometrie): fyzikální (např. otisky prstů a oči) nebo behaviorální propočty na základě lidských rysů. Autentizace se v počítačové vědě používá jako forma ověření totožnosti a kontroly přístupu.

Bitcoin: digitální nebo virtuální měna vytvořená v roce 2009, která využívá technologie P2P k usnadnění okamžitých plateb.

Cloud computing: poskytování IT zdrojů a zdrojů na vyžádání – např. ukládání, výpočetní výkon nebo kapacita sdílení údajů – přes internet prostřednictvím hostingu na vzdálených serverech.

Červi: počítačový červ je samostatný malwarový počítačový program, který se replikuje a šíří do dalších počítačů. Ke svému šíření často využívá počítačové sítě, do níž získává přístup díky předpokládaným chybám v zabezpečení cílového počítače.

Dezinformace: prokazatelně falešná nebo zavádějící informace, která vzniká, prezentuje se a šíří se za účelem ekonomického prospěchu nebo úmyslného klamání veřejnosti a může přivodit veřejnou újmu.

Digitalizace: proces převádění informací do digitálního formátu, v němž jsou informace uspořádány do bitů. Výsledkem je reprezentace objektu, obrazu, zvuku, dokumentu nebo signálu generováním řady čísel, která popisují diskrétní soubor bodů nebo vzorků.

Digitální obsah: veškeré údaje – například text, zvuk, obrázky nebo video – uložené v digitálním formátu.

Digitální platforma: prostředí umožňující interakci alespoň mezi dvěma různými skupinami, z nichž jedna je obvykle dodavatelem a druhá spotřebitelem/uživatelem.

Může se jednat o hardware nebo operační systém, nebo i internetový prohlížeč a související aplikační rozhraní, nebo jiný podkladový software, pokud je jeho prostřednictvím spouštěn programový kód.

Digitální statek: Cokoli v digitálním formátu, co je ve vlastnictví jednotlivce nebo společnosti a je spojeno s užívacím právem (např. obrázky, fotografie, videa, soubory obsahující text atd.).

Distribuované odepření služby (DDoS, *Distributed Denial of Service*): kybernetický útok zabraňující oprávněným uživatelům v přístupu k on-line službě nebo zdroji tím, že je zahlcuje větším množstvím požadavků, než mohou zvládnout.

Dostupnost: zajištění včasného a spolehlivého přístupu k informacím a jejich využívání.

Etický hacker: osoba (odborník v oboru počítačové bezpečnosti), která proniká do počítačové sítě za účelem testování nebo hodnocení její bezpečnosti, nikoli se zlovolným nebo zločinným úmyslem.

Hacker: jednotlivec, který využívá počítačových, síťových nebo jiných dovedností k získání neoprávněného přístupu k údajům, počítačovému systému nebo síti.

Hybridní hrozba: uskutečňování nepřátelského záměru prováděného protivníky v intenzivní snaze o dosažení cílů za smíšeného použití konvenčních i nekonvenčních technik vedení války (tj. vojenských, politických, ekonomických a technologických metod).

Integrita: ochrana proti nekalému pozměnění nebo zničení informací a zaručení jejich autenticity.

Internet věcí (IoT): síť každodenních předmětů vybavených elektronikou, softwarem a senzory, aby mohly komunikovat a provádět výměnu údajů přes internet.

Kritická infrastruktura: fyzické zdroje, služby a zařízení, jejichž nefunkčnost nebo zničení by mělo vážný dopad na fungování hospodářství a společnosti.

Kritický informační systém: jakýkoli existující nebo plánovaný informační systém, který je považován za nezbytný pro efektivní a účinné fungování dané organizace.

Kryptoměna: digitální aktivum, které je emitováno a vyměňováno za použití šifrovacích technik, nezávisle na centrální bance. Mezi členy virtuální komunity je přijímáno jako platební prostředek.

Kyberkriminalita: různé trestné činnosti zahrnující počítače a informační systémy jako primární nástroj nebo primární cíl. Mezi tyto činnosti patří: tradiční trestné činy (např. podvody, padělání a krádež totožnosti), trestné činy související s obsahem (např. distribuce dětské pornografie on-line nebo podněcování k rasové nenávisti) a trestné činy specifické pro počítače a informační systémy (např. útoky na informační systémy, útoky vedoucí k odepření služby, malware nebo ransomware).

Kybernetická bezpečnost (kybernetická ochrana): veškerá ochranná a bezpečnostní opatření přijatá na obranu informačních systémů a jejich údajů před neoprávněným přístupem, útokem a poškozením za účelem zajištění jejich dostupnosti, důvěrné povahy a integrity.

Kybernetická diplomacie: využívání diplomatických zdrojů a vykonávání diplomatických funkcí za účelem zajištění národních zájmů ohledně kyberprostoru. Provádějí ji zcela nebo zčásti diplomaté, kteří spolu jednají na dvoustranných setkáních (např. dialog mezi USA a Čínou) nebo na mnohostranných fórech (např. na půdě OSN). Mimo sféru tradiční diplomacie jednají diplomaté i s různými nestátními subjekty, jako jsou vedoucí pracovníci internetových společností (např. Facebook nebo Google), podnikatelé v oblasti technologií nebo organizace občanské společnosti. Součástí diplomatické práce může být rovněž posilování postavení potlačovaných obyvatel v jiných zemích prostřednictvím technologií.

Kybernetická hrozba: zlovolné jednání, jehož cílem je poškodit nebo odcizit údaje nebo obecně narušit digitální život.

Kybernetická obrana: podskupina kybernetické bezpečnosti, jejímž cílem je obrana kyberprostoru pomocí vojenských a jiných vhodných prostředků za účelem dosažení vojensko-strategických cílů.

Kybernetická odolnost: schopnost zabránit kybernetickým útokům a bezpečnostním incidentům, připravit se na ně, odolat jim a zotavit se z nich.

Kybernetická špionáž: kybernetická špionáž je jednorázové nebo opakované jednání spočívající v získávání tajemství a informací bez svolení nebo vědomí držitele informací od jednotlivců, konkurentů, soupeřů, skupin, vlád a nepřátel za účelem dosažení osobních, hospodářských, politických nebo vojenských výhod prostřednictvím internetu, sítí nebo jednotlivých počítačů.

Kybernetický bezpečnostní incident: událost, která přímo nebo nepřímo poškozuje nebo ohrožuje odolnost a bezpečnost informačního systému a údajů, které zpracovává, uchovává nebo přenáší.

Kybernetický ekosystém: komplexní soubor zařízení, údajů, sítí, osob, procesů a organizací v interakci a prostředí procesů a technologií, které tuto interakci ovlivňují a podporují.

Kybernetický útok: pokus narušit nebo zničit důvěrnou povahu, integritu a dostupnost údajů nebo počítačový systém prostřednictvím kyberprostoru.

Kyberprostor: nehmotné globální prostředí, v němž dochází k on-line komunikaci mezi lidmi, softwarem a službami prostřednictvím počítačových sítí a technologických zařízení.

Malware: škodlivý software. Počítačový program určený k poškození počítače, serveru nebo sítě.

Ochrana důvěrných informací: ochrana informací, údajů nebo majetku před neoprávněným přístupem nebo zveřejněním.

Opravná řešení: zavádění změn v softwaru za účelem jeho aktualizace, opravy nebo vylepšení, včetně řešení nedostatků v jeho bezpečnosti.

Osobní údaje: informace týkající se identifikovatelné osoby.

Phishing: zasílání e-mailů navozujících zdání důvěryhodného původu s cílem přimět příjemce, aby na základě klamného dojmu klikli na škodlivé odkazy nebo sdíleli osobní údaje.

Pokročilé přetrvávající hrozby: útok, při němž neoprávněný uživatel získá přístup do systému nebo do sítě a setrvá tam po delší dobu, aniž by byl odhalen. Obzvláště nebezpečné pro podniky, neboť hackeři tímto způsobem získají trvalý přístup k citlivým údajům společnosti, zpravidla však nepoškozují podnikové sítě nebo místní počítače. Cíl – krádež údajů.

Porušení zabezpečení údajů: úmyslné nebo neúmyslné zpřístupnění zabezpečených nebo soukromých/důvěrných informací v nedůvěryhodném prostředí.

Poskytovatel digitálních služeb: kdokoli, kdo poskytuje jeden nebo více z těchto tří druhů digitálních služeb: on-line tržiště, internetové vyhledávače, služby cloud computingu.

Protokol ovládání vzdálené plochy (RDP): technická norma (vydaná společností Microsoft) pro používání stolního počítače na dálku. Uživatelé vzdálených stolních počítačů mají přístup na svou plochu, mohou otevírat a upravovat soubory a používat aplikace, jako kdyby seděli u svého stolního počítače.

Provozovatel základních služeb: veřejný nebo soukromý subjekt poskytující službu, která je základní z hlediska zachování kritických společenských a ekonomických činností.

Ransomware: škodlivý software, který oběti odpírá přístup k počítačovému systému nebo činí soubory nečitelné, obvykle prostřednictvím šifrování. Útočník potom obvykle vydírá oběť tím, že odmítne přístup obnovit, dokud nebude vyplaceno výkupné.

Sabotáž: jednání, jehož cílem je záměrně zničit nebo poškodit cílový předmět nebo zamezit jeho fungování, zejména za účelem získání politických nebo vojenských výhod.

Sociální inženýrství: v oblasti bezpečnosti informací psychologická manipulace usilující přimět člověka, aby na základě klamného dojmu provedl určitý úkon nebo prozradil důvěrnou informaci.

Spyware: software se škodlivými účinky, jehož účelem je shromažďovat informace o určité osobě nebo organizaci a zasílat tyto informace jinému subjektu způsobem, který uživatele poškozuje; například tím, že narušuje jejich soukromí nebo ohrožuje zabezpečení jejich zařízení.

Šifrování: přeměna čitelných informací na nečitelný kód za účelem jejich ochrany. Aby uživatel mohl informace přečíst, musí mít přístup k tajnému klíči nebo heslu.

Trojský kůň: typ škodlivého kódu nebo softwaru, který vzbuzuje dojem legitimity, ale může nad cizím počítačem převzít kontrolu. Trojský kůň je navržen tak, aby poškozoval, narušoval, odcizoval nebo obecně nějakým jiným způsobem napadal cizí údaje nebo sítě.

Údaje o přístupu: informace o přihlašování uživatele pro přístup ke službě a o jeho odhlašování, např. čas, datum a IP adresa.

Umělá inteligence: simulace lidské inteligence na strojích, které jsou naprogramovány tak, aby myslely jako lidé a napodobovaly jejich jednání; každý stroj, který vykazuje vlastnosti spojené s lidskou myslí, jako je učení a řešení problémů.

Útoky z webových stránek: uživatelé mají důvěru, že citlivé osobní informace, které uvádějí na určité internetové stránce, zůstanou soukromé a bezpečné. Vniknutím (útokem) se může rozumět zveřejnění informací o jejich kreditní kartě, sociálním zabezpečení nebo zdravotním stavu, což může mít závažné důsledky.

Vektorizace textu: proces konverze slov, vět nebo celých dokumentů do numerických vektorů, aby je mohly používat algoritmy pro strojové učení.

Volební infrastruktura: zahrnuje informační systémy a databáze kampaní, citlivé informace o kandidátech, systémy registrace voličů a řízení.

Vysoce výkonná výpočetní technika: schopnost zpracovávat data a provádět složité výpočty při vysokých rychlostech.

Zabezpečení informací: soubor postupů a nástrojů chránících fyzické a digitální údaje před neoprávněným přístupem, použitím, zveřejněním, narušením, pozměněním, zaznamenáním nebo zničením.

Zařízení veřejně prospěšných služeb: jakýkoli stožár, věž, jakékoli nadzemní nebo podzemní vedení, jakákoli nosná nebo opěrná konstrukce a jakýkoli výkop, jakož i příslušenství, které lze použít pro dodávku nebo distribuci elektrických, telefonních, telegrafních, kabelových nebo signalizačních služeb nebo jiných podobných služeb.

Zpracování údajů: provádění zejména počítačových operací s údaji za účelem získávání, transformace nebo utajení informací.