Contact Committee

Kontaktný výbor
najvyšších kontrolných inštitúcií Európskej únie

Zhrnutie auditov

Kybernetická bezpečnosť v EÚ a jej členských štátoch

Vykonávanie auditov odolnosti kritických informačných systémov a digitálnych infraštruktúr voči kybernetickým útokom

Audítorské správy
uverejnené v rokoch 2014 až 2020

SK

December 2020

Kontaktný výbor najvyšších kontrolných inštitúcií Európskej únie (EÚ) predstavuje fórum na diskusiu o otázkach verejného auditu v EÚ a na ich riešenie. Zintenzívňovaním dialógu a spolupráce medzi svojimi členmi výbor pomáha zvyšovať účinnosť externého auditu politík a programov EÚ. Zároveň pomáha posilňovať zodpovednosť, zlepšovať finančné riadenie EÚ a konsolidovať dobrú správu vecí verejných v prospech všetkých občanov EÚ.

Kontakt: www.contactcommittee.eu

Obsah

Obsah

Obsah

Predslov

Vážení čitatelia,

digitalizácia a čoraz väčšie využívanie informačných technológií vo všetkých aspektoch nášho každodenného života otvárajú nový svet príležitostí. Zároveň sa zvýšilo riziko, že jednotlivci, podniky a subjekty verejného sektora sa stanú obeťou počítačovej kriminality alebo kybernetického útoku, a rovnako sa zvýšil spoločenský a hospodársky vplyv tohto rizika.

V EÚ patrí kybernetická bezpečnosť do právomoci členských štátov. Úlohou EÚ je vytvárať spoločný regulačný rámec na jednotnom trhu EÚ a vytvárať podmienky na to, aby členské štáty spolupracovali vo vzájomnej dôvere.

Kybernetická bezpečnosť a naša digitálna autonómia sa stali pre EÚ a jej členské štáty témou strategického významu. Nedostatky v riadení kybernetickej bezpečnosti vo verejnom a súkromnom sektore pretrvávajú vo všetkých členských štátoch, aj keď na rôznej úrovni. Znižuje sa tým naša schopnosť obmedziť kybernetické útoky a v prípade potreby na ne reagovať. Na vzostupe sú dezinformácie, často riadené spoza hraníc EÚ, čo sa opäť raz ukázalo počas tohtoročnej pandémie ochorenia COVID-19. Táto skutočnosť predstavuje ohrozenie sociálnej súdržnosti v našich spoločnostiach a dôvery občanov v naše demokratické systémy, ktoré nemôžeme ignorovať.

Z prieskumu medzi najvyššími kontrolnými inštitúciami v EÚ, ktorý sa uskutočnil v roku 2018, vyplynulo, že doposiaľ približne polovica z nich nevykonávala audit kybernetickej bezpečnosti. Naše najvyššie kontrolné inštitúcie odvtedy zintenzívnili činnosti auditu v oblasti kybernetickej bezpečnosti, s osobitným dôrazom na ochranu údajov, pripravenosť systému na kybernetické útoky a ochranu systémov základných verejných služieb. Z pochopiteľných dôvodov nemožno zverejniť všetky tieto audity, keďže niektoré sa môžu týkať citlivých informácií (národnej bezpečnosti).

V tomto roku je hospodárske a sociálne tkanivo našich spoločností vystavené skúške krízou spôsobenou pandémiou COVID-19. Vzhľadom na našu závislosť od informačných technológií by sa ďalšou pandémiou pokojne mohla stať „kybernetická kríza“. Musíme byť pripravení a musíme zvýšiť odolnosť kritických informačných systémov a digitálnych infraštruktúr voči kybernetickým útokom.

Dúfame, že prehľad uvedený v tomto zhrnutí bude ďalším podnetom na zvýšenie záujmu orgánov verejného auditu v celej Únii o túto kritickú oblasť.

Klaus-Heiner Lehne

predseda Európskeho dvora audítorov
predseda kontaktného výboru
a vedúci projektu

Zhrnutie

I Kybernetická bezpečnosť a naša digitálna autonómia sa stali **pre EÚ a jej členské štáty témou strategického významu**, a keďže úroveň ohrozenia sa zvyšuje, musíme zvýšiť naše úsilie na ochranu našich kritických informačných systémov a digitálnych infraštruktúr pred kybernetickými útokmi. Kybernetická bezpečnosť sa netýka len našich služieb, obrany či systémov zdravotnej starostlivosti, ale aj ochrany našich osobných údajov, obchodných modelov a duševného vlastníctva. Kybernetická bezpečnosť v konečnom dôsledku znamená ochranu našich demokratických spoločností, našej nezávislosti ako Európanov a spôsobu nášho spolunažívania.

II V prvom oddiele tohto tretieho zhrnutia, ktoré predkladá kontaktný výbor, uvádzame, **čo znamená kybernetická bezpečnosť**. Opisujeme, prečo kybernetická bezpečnosť predstavuje výzvu pre subjekty verejného sektora, podniky a jednotlivcov, a zdôrazňujeme nový fenomén dezinformácií, ktorý je rastúcou hrozbou pre sociálnu súdržnosť v našich spoločnostiach a demokratických systémoch. Zároveň vysvetľujeme kompetencie a aktérov, stratégiu a právne predpisy EÚ v oblasti kybernetickej bezpečnosti, ako aj finančné prostriedky EÚ dostupné v tejto oblasti.

III V druhej časti zhrnutia sumarizujeme **výsledky vybraných auditov, ktoré uskutočnilo dvanásť prispievajúcich najvyšších kontrolných inštitúcií členských štátov a Európsky dvor audítorov** a ktoré boli uverejnené v rokoch 2014 – 2020. V týchto auditoch sa riešili dôležité aspekty kybernetickej bezpečnosti, akými sú ochrana súkromných údajov, integrita národných stredísk pre údaje, bezpečnosť zariadení verejných služieb a vykonávanie národných stratégií kybernetickej bezpečnosti v širšom zmysle.

IV Tretia časť zhrnutia obsahuje **podrobné prehľady vybraných auditov** spolu so zhrnutím iných auditov týkajúcich sa témy kybernetickej bezpečnosti, ktoré uverejnili najvyššie kontrolné inštitúcie.

ČASŤ I – Kybernetická bezpečnosť v európskom kontexte

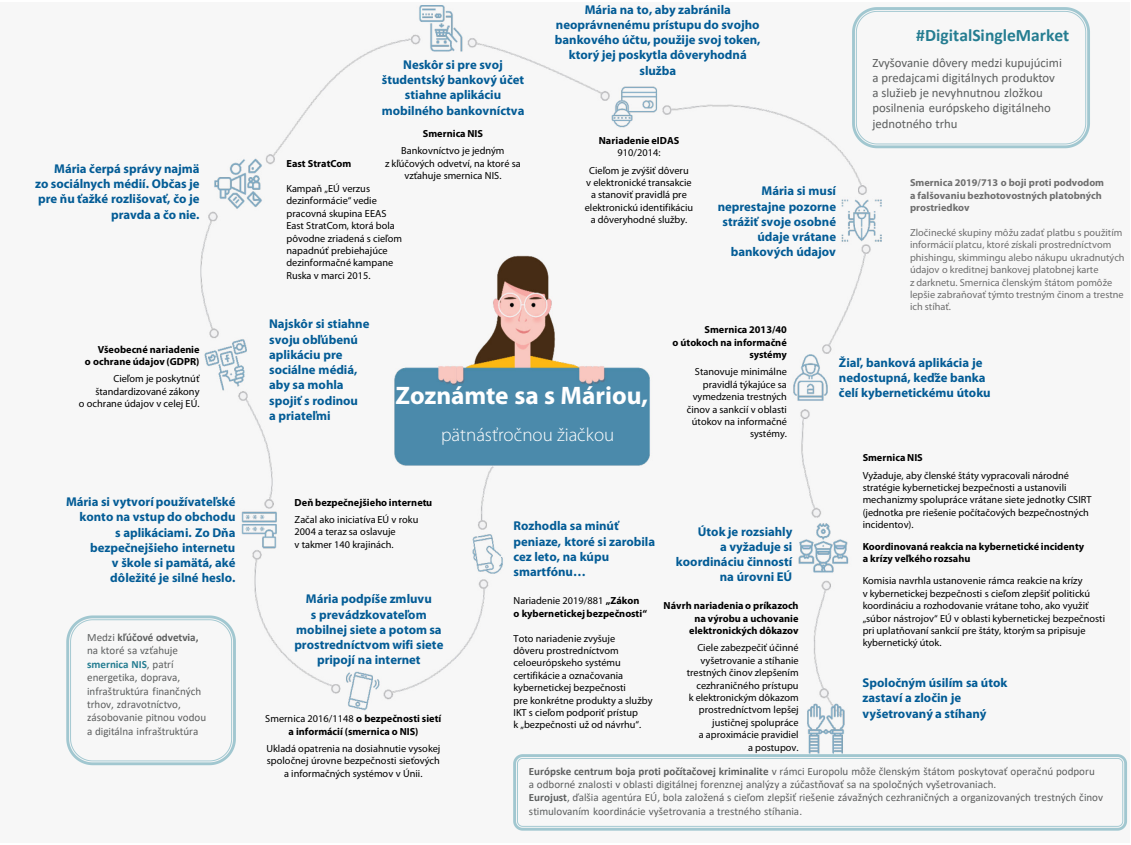
Čo je kybernetická bezpečnosť?

1 Všeobecné štandardné **vymedzenie pojmu kybernetická bezpečnosť** neexistuje. V tomto dokumente kybernetická bezpečnosť znamená **činnosti potrebné na ochranu sietí a informačných systémov, ich používateľov a iných osôb dotknutých kybernetickými hrozbami**. Kybernetická bezpečnosť zahŕňa prevenciu a odhaľovanie kybernetických útokov, reakciu na ne a obnovu po nich. Tieto incidenty môžu byť úmyselné alebo neúmyselné a môžu siahať od náhodného zverejnenia informácií po útoky na podniky a kritickú infraštruktúru, krádež osobných údajov, či dokonca až po zasahovanie do demokratických procesov vrátane zasahovania do volieb či všeobecné dezinformačné kampane na ovplyvnenie verejnej diskusie.

Kybernetická bezpečnosť ovplyvňuje každodenný život všetkých občanov EÚ

2 Kybernetická bezpečnosť má vplyv na každodenný život všetkých občanov EÚ vždy, keď používame osobné zariadenia informačných technológií, akými sú smartfóny, bezdrôtové miestne počítačové siete (Wi-Fi), sociálne médiá či elektronické bankovníctvo. V roku 2020 viac než kedykoľvek predtým už otázkou nie je, či ku kybernetickým útokom dôjde, ale ako a kedy k nim dôjde. Týka sa to nás všetkých: **jednotlivcov, podnikov a subjektov verejného sektora**. Na *obrázku 1* sa uvádza, ako EÚ potvrdzuje kybernetickú bezpečnosť a vytvorila rámec na ochranu každodenných elektronických činností občanov pred kybernetickými útokmi. Ochrana kritických informačných systémov a digitálnej infraštruktúry pred kybernetickými útokmi sa stala strategickou výzvou.

Obrázok 1 – EÚ potvrdzuje kybernetickú bezpečnosť v každodennom živote občanov EÚ

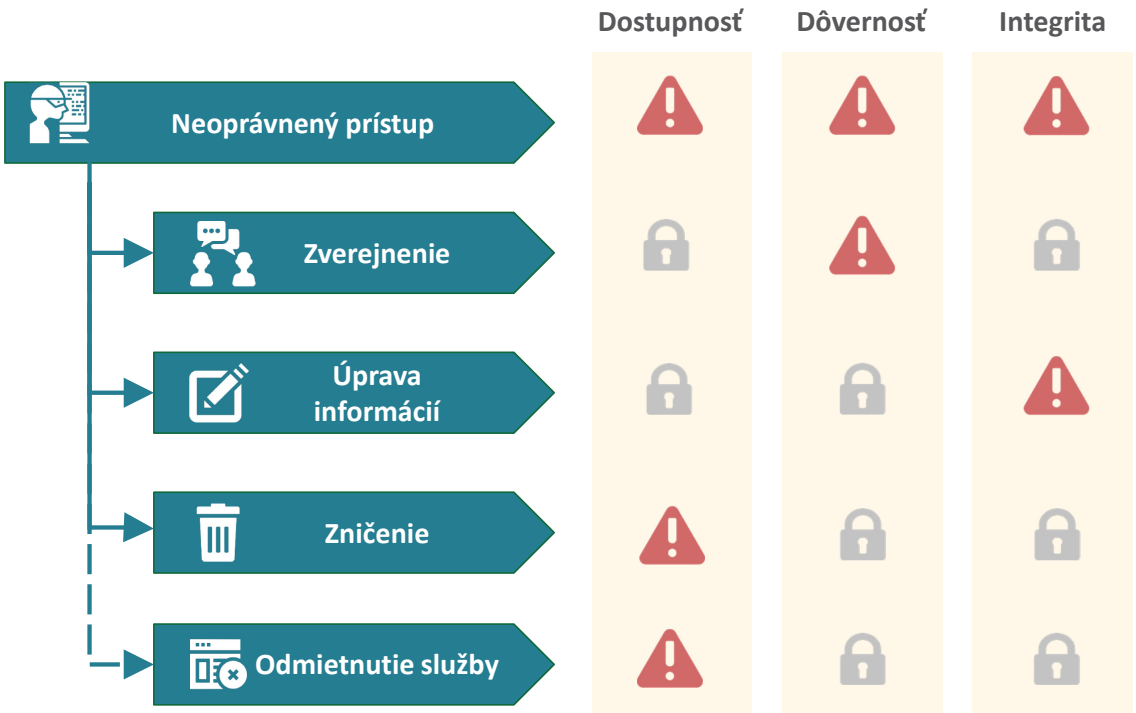


Zdroj: EDA, Ikony vytvorené Pixel perfect z https://flaticon.com.

Existuje mnoho druhov kybernetických hrozieb

3 Mnohé druhy kybernetických hrozieb, ktorým naše spoločnosti čelia, možno rozdeliť podľa toho, **čo sa pri nich deje s údajmi (zverejnenie, úprava, zničenie alebo zamietnutie prístupu)**, alebo podľa toho, ktoré základné zásady informačnej bezpečnosti porušujú (pozri ***ilustráciu 1***).

Ilustrácia 1 – Druhy hrozieb a zásady informačnej bezpečnosti, ktoré sú nimi ohrozené



Zámka = bezpečnosť nedotknutá, výkričník = bezpečnosť ohrozená.

Zdroj: EDA na základe štúdie Európskeho parlamentu[1].

4 Zakaždým, keď sa zariadenie pripojí na internet alebo sa prepojí s inými zariadeniami, zvyšuje sa možnosť útokov proti kybernetickej bezpečnosti. Exponenciálny rast internetu vecí, cloudu, veľkých dát (big data) a digitalizácie priemyslu sprevádza zvyšovanie expozície voči slabým miestam systému, ktoré útočníkom umožňujú cieliť na čoraz viac obetí. Rozmanitosť druhov útokov a ich čoraz väčšia dômyselnosť znemožňujú držať krok s ich vývojom[2]. V ***rámčeku 1*** sú opísané príklady **možných kybernetických útokov**.

[1] Európsky parlament, *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses*, štúdia pre Výbor pre občianske slobody, spravodlivosť a vnútorné veci (LIBE), september 2015.

[2] ENISA, *ENISA Threat Landscape Report 2017*, 18. januára 2018.

Rámček 1

Druhy kybernetických útokov

Malvér (škodlivý softvér) je navrhnutý tak, aby poškodzoval zariadenia alebo siete. Táto kategória zahŕňa vírusy, trójske kone, ransomvér, počítačové červy, advér a spyvér (napr. NotPetya).

Ransomvér je softvér, ktorý šifruje údaje, čím bráni používateľom v prístupe k ich súborom, kým nezaplatia výkupné, zvyčajne v kryptomene, alebo kým nevykonajú istú činnosť. Podľa Europolu prevládajú útoky typu ransomvéru a v niekoľkých posledných rokoch došlo k prudkému nárastu počtu druhov ransomvéru (napr. Wannacry[3]).

Pribúdajú útoky **distribuovaného odmietnutia služby** (ďalej len „útoky DDoS“), pri ktorých sa znemožní prístup k službám alebo zdrojom prostredníctvom zaplavenia týchto služieb alebo zdrojov vyšším počtom požiadaviek, než sú schopné zvládnuť, pričom v roku 2017 tento druh útokov postihol jednu tretinu organizácií[4].

Atraktívnou metódou sú **útoky prostredníctvom webu**, pomocou ktorých dokážu aktéri hrozby podviesť obete tak, že ako vektor hrozby použijú webové systémy alebo služby. Zahŕňa možnosť rozsiahlych útokov, napríklad uľahčenie škodlivých URL alebo škodlivých skriptov s cieľom nasmerovať používateľa alebo obeť na požadovanú webovú stránku alebo sťahovanie škodlivého (útoky typu *watering hole*, útoky typu *drive-by*), a **vloženie** škodlivého kódu do legitímneho, ale ohrozeného webového sídla na krádež informácií (t. j. *formjacking*) na účely finančného zisku alebo krádeže informácií[5].

Používateľov je možné zmanipulovať tak, aby nevedomky vykonali istú akciu alebo zverejnili dôverné informácie. Tento úskok sa môže použiť pri krádeži údajov alebo kybernetickej špionáži a je známy ako **sociálne inžinierstvo**. Existujú rozličné spôsoby, ako to dosiahnuť, bežnou metódou je však tzv. **phishing**, pri ktorom sa prostredníctvom e-mailových správ, ktoré vyzerajú, akoby pochádzali z dôveryhodných zdrojov, oklamú používatelia, aby prezradili informácie alebo klikli na odkazy, ktoré nakazia ich zariadenie stiahnutým malvérom. Vyše polovice členských štátov nahlásilo vyšetrovania týkajúce sa takýchto útokov na siete[6].

Asi najpohodlnejším druhom hrozieb sú **pokročilé pretrvávajúce hrozby**. Tieto hrozby sú dielom rafinovaných útočníkov, ktorí dlhodobo sledujú a kradnú údaje, niekedy s deštruktívnymi cieľmi. Ich cieľom je zostať čo najdlhšie neodhalení. Pokročilé pretrvávajúce hrozby sa často týkajú štátov a bývajú zamerané najmä na citlivé sektory, akými sú technológie, obrana a kritická infraštruktúra. Tento typ

kybernetickej špionáže údajne predstavuje najmenej jednu štvrtinu všetkých kybernetických incidentov[7].

Kybernetické útoky majú značný hospodársky dosah

5 Hrozba **kybernetických útokov a počítačovej kriminality** sa v posledných rokoch stala jednou z hlavných otázok. Už v roku 2016 80 % podnikov EÚ zažilo aspoň jeden kybernetický incident[8]. V roku 2018 40 % respondentov prieskumu z organizácií, ktoré využívajú robotiku alebo automatizáciu, uviedlo, že najkritickejším dôsledkom kybernetického útoku na ich systémy by bolo prerušenie prevádzky. Napriek informovanosti o rušivých kybernetických rizikách však spoločnosti často nemajú zavedený systém na ich riešenie[9].

6 Odvtedy sa počet kybernetických útokov, ich závažnosť a finančné náklady ďalej zvyšovali. Pokiaľ možno odhadnúť jej **finančný vplyv**, počítačová kriminalita bude do roku **2021** stáť svetové hospodárstvo **6 biliónov USD ročne**, čo je nárast z odhadovaných 3 biliónov USD v roku 2015[10], v porovnaní s odhadovaným celosvetovým HDP vo výške 138 biliónov USD v roku 2020. Náklady počítačovej

---

[3] Ransomvér *WannaCry* využíval chyby v protokole operačného systému Microsoft Windows, ktoré umožňovali prevziať na diaľku kontrolu nad akýmkoľvek počítačom. Spoločnosť Microsoft po odhalení chyby vydala opravu. Státisíce počítačov však neboli aktualizované a mnoho z nich bolo neskôr infikovaných. *Zdroj:* A. Greenberg, *Hold North Korea Accountable For Wannacry – and the NSA, too* WIRED, 19. decembra 2017.

[4] Europol, *Internet Organised Crime Threat Assessment 2018*.

[5] ENISA, *ENISA Threat Landscape 2020 – Web-based attacks*, 20. októbra 2020.

[6] Europol, pozri vyššie, 2018.

[7] European Centre for Political Economy, *Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?*, občasník č. 2/18, február 2018.

[8] Europol, *Internet Organised Crime Threat Assessment 2017*.

[9] *PWC, Global State of Information Security (GSISS) Survey – Strengthening digital society against cyber shocks*, 2017.

[10] Cybersecurity Ventures, *2019 Official Annual Cybercrime Report*, sponzorovaná spoločnosťou Herjavec Group, 2019.

kriminality zahŕňajú poškodenie a zničenie údajov, ukradnuté peniaze, stratu produktivity, krádež duševného vlastníctva, krádež osobných a finančných údajov, narušenie riadneho priebehu podnikania po útoku či poškodenie dobrej povesti. Európsky výbor pre systémové riziká (ESRB) odhaduje, že priemerné náklady na kybernetické incidenty sa v rokoch 2015 až 2020 zvýšili o 72 %[11].

7 Z nedávnej štúdie z roku 2020[12] vyplýva, že počítačová kriminalita **ovplyvňuje rôzne hospodárske odvetvia rôznym spôsobom**: bola najrušivejším podvodným javom vo vládnej sfére a verejnej správe, v sektoroch technológií, médií a telekomunikácií a v odvetví zdravotníctva (pozri ***rámček 2***) a zároveň bola druhým najrušivejším podvodným javom vo finančnom sektore a v sektore priemyslu a výroby.

Rámček 2

Fínski pacienti psychoterapie boli vydieraní pomocou osobných lekárskych údajov, ktoré boli ukradnuté v rokoch 2018 – 2019

Jednotlivých pacientov veľkej fínskej psychoterapeutickej kliniky s pobočkami po celej krajine, ktorých osobné údaje boli ukradnuté v novembri 2018, s ďalším možným narušením v marci 2019, oslovil v roku 2020 vydierač. Údaje zrejme obsahovali osobné identifikačné záznamy a poznámky o tom, čo sa hovorilo na terapeutických sedeniach.

Klinika aj pacienti mali vydieračovi zaplatiť výkupné v bitcoinoch, aby údaje neboli zverejnené. Incident viedol fínsku vládu k zorganizovaniu mimoriadneho stretnutia[13].

8 V roku 2019 EUROPOL[14] opäť zdôraznil **pretrvávanie a pevnosť viacerých kľúčových hrozieb v oblasti počítačovej kriminality:**

- najvyššou hrozbou zostávajú útoky ransomvérom, sú čoraz presnejšie zacielené, ziskovejšie a spôsobujú väčšie hospodárske škody. Pokiaľ bude ransomvér

[11] ESRB, Európsky výbor pre systémové riziká, *Systemic cyber risk*, February 2020.

[12] PWC, *Fighting fraud: A never-ending battle PwC's Global Economic Crime and Fraud Survey*, 2020.

[13] BBC News, *Therapy patients blackmailed for cash after clinic data breach*, 26. októbra 2020.

[14] EUROPOL, *INTERNET organised crime threat assessment (IOCTA)*, 2019.

zabezpečovať páchateľom počítačovej trestnej činnosti pomerne jednoduchý príjem, zrejme zostane najvyššou hrozbou počítačovej kriminality,

- kľúčovými hlavnými vektormi infekcie malvérom sú phishing a zraniteľné protokoly vzdialeného počítača (RDP) a
- hlavným cieľom, komoditou a umožňujúcim faktorom počítačovej kriminality zostávajú údaje.

9 Podobne Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA) vo svojej **správe z roku 2020 s názvom *Main incidents in the EU and worldwide***[15] uvádza niekoľko príkladov kybernetických incidentov (pozri ***rámček 3***).

Rámček 3

Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA): kybernetické bezpečnostné incidenty v rokoch 2019 – 2020

E-mailovú platformu verifications.io postihlo veľké porušenie ochrany údajov, ktorého príčinou bola nechránená databáza MongoDB. Zverejnené boli údaje z viac ako 800 miliónov e-mailov, ktoré obsahovali citlivé informácie vrátane informácií o totožnosti.

Na obľúbenom hackerskom fóre, ktorého hostiteľom je cloudová služba MEGA1, bolo zverejnených viac ako 770 miliónov e-mailových adries a 21 miliónov jedinečných hesiel. Stali sa najvýznamnejším súborom narušených osobných prvkov v histórii, ktorý dostal pomenovanie *Collection #1* (Zbierka č. 1).

Obeťou cieleného kybernetického útoku sa stala spoločnosť Citrix, ktorá je poskytovateľom cloudu a virtualizácie. Na získanie prístupu do systémov spoločnosti Citrix útočníci využili viacero kritických zraniteľných miest softvéru, napríklad CVE-2019 – 19781, a použili techniku tzv. *password spraying*.

Poskytovateľ hostiteľských služieb pre cloud iNSYNQ19 sa stal obeťou útoku ransomvérom, po ktorom zákazníci viac ako týždeň nemali prístup k svojim údajom a boli nútení využívať miestne zálohy.

10 Podľa Europolu sa počas prvých šiestich mesiacov roku 2019 zdvojnásobili kybernetické útoky, ktorých cieľom bolo spôsobenie **trvalej škody**, a to najmä

[15] ENISA, *Main incidents in the EU and worldwide – January 2019 to April 2020*, október 2020.

v sektore výroby. Na rozdiel od konvenčných útokov ransomvérom ide o akty sabotáže, ktorých cieľom je trvalé vymazanie alebo iné nezvratné poškodenie údajov podniku (pozri ***rámček 4***).

Rámček 4

Deštruktívny ransomvér – útoky Germanwiper v roku 2019

V roku 2019 bola odhalená séria útokov ransomvérom, ktoré boli zacielené na podniky pôsobiace v Nemecku. Ransomvér, ktorý dostal názov *Germanwiper*, dokáže nahradiť infikované súbory nulami a jednotkami, obnovenie súborov preto nie je možné. Ransomvér sa šíri prostredníctvom e-mailových phishingových kampaní a najmä cielených ľudských pracovníkov popredných spoločností, keďže bol začlenený do falošných žiadostí o zamestnanie[16].

Informovanosť o kybernetických bezpečnostných hrozbách sa zvyšuje zároveň s ich rastúcou frekvenciou

11 Až donedávna však informovanosť o týchto rizikách a ich uznávanie boli stále pomerne nízke. V roku 2017 69 % spoločností v EÚ nemalo znalosti o svojom **vystavení kybernetickým hrozbám**[17], alebo o ňom malo iba základné znalosti, a 60 % nikdy neuskutočnilo odhad **možných finančných strát**[18]. Navyše podľa globálneho prieskumu v roku 2018 by každá tretia organizácia radšej hackerom vyplatila výkupné, než by investovala do informačnej bezpečnosti[19].

[16] Cybersecurity Insiders, *GermanWiper Ransomware attack warning for Germany*, nedatované.

[17] Európska komisia, *Prehľad o kybernetickej bezpečnosti*, september 2017.

[18] Medzi tieto straty môžu patriť: strata príjmu, náklady na opravu poškodených systémov, možné dlhy vyplývajúce z ukradnutého majetku alebo informácií, stimuly na udržanie zákazníkov, vyššie poistné, vyššie náklady na ochranu (nové systémy, zamestnanci, odborná príprava), možné vyrovnanie nákladov na dodržiavanie predpisov alebo súdny spor.

[19] NTT Security, *Risk: Value 2018 Report*.

12 V prieskume **Eurobarometra z roku 2020 s názvom *Europeans' attitudes towards cyber security***[20] sa identifikuje rastúce povedomie a obavy občanov EÚ:

- respondenti, ktorí využívajú internet, sa najviac obávajú, že niekto zneužije ich osobné údaje (46 %), obávajú sa o bezpečnosť svojich online platieb (41 %) a o to, že nebudú môcť skontrolovať tovar alebo požiadať o radu skutočnú osobu alebo že nebudú môcť povedať, že sa obávajú, že im nemusia byť doručené tovary alebo služby, ktoré kúpia online (obe 22 %),
- viac ako tri štvrtiny (76 %) respondentov sú presvedčené, že sa zvyšuje riziko, že sa stanú obeťou počítačovej kriminality. Omnoho menej (52 %) sa však domnieva, že sa proti nej môžu dostatočne chrániť sami – čo predstavuje pokles o deväť percentuálnych bodov od roku 2018,
- o niečo viac ako polovica respondentov (52 %) sa napriek tomu domnieva, že sú o počítačovej kriminalite dobre informovaní, ale len 11 % uvádza, že sú veľmi dobre informovaní.

Kybernetická bezpečnosť je dôležitá pre sociálnu súdržnosť a politickú stabilitu

Nová hrozba: kybernetická bezpečnosť a dezinformácie

13 Šírenie úmyselných a systematických rozsiahlych **dezinformácií je pre naše demokracie akútnou strategickou výzvou**[21]. Dezinformácie a falošné správy (tzv. *fake news*) majú potenciál rozdeľovať spoločnosti, zasievať nedôveru a dokonca ohroziť sociálnu súdržnosť a dôveru v demokratické procesy (pozri ***rámček 5***).

[20] Európska komisia, *Special Eurobarometer 499 – Europeans' attitudes towards cyber security*, január 2020.

[21] Podľa štúdie *The Global Disinformation Order*, ktorú vypracovala Oxfordská univerzita (september 2019), sa počet krajín s politickými dezinformačnými kampaňami za posledné roky viac ako zdvojnásobil na 70.

Rámček 5

Dezinformácie

Európska komisia vymedzuje dezinformácie ako vytváranie, prezentácia a šírenie overiteľne nepravdivých alebo zavádzajúcich informácií na účely hospodárskeho zisku alebo úmyselného zavádzania verejnosti, čo by mohlo spôsobiť poškodenie verejnosti[22]. Poškodenie verejného záujmu môže zahŕňať ohrozenie demokratických procesov alebo verejných statkov, akými sú zdravie, životné prostredie a bezpečnosť.

Na rozdiel od nelegálneho obsahu (ktorý zahŕňa nenávistný prejav, teroristický obsah či materiál so sexuálnym zneužívaním detí) dezinformácie zahŕňajú obsah, ktorý je legálny. Preto sa nachádzajú na priesečníku s ústrednými hodnotami EÚ týkajúcimi sa slobody prejavu a slobody médií. Podľa vymedzenia Komisie medzi dezinformácie nepatrí klamlivá reklama, chyby v spravodajstve, satira a paródie, ani správy a komentáre naklonené jednej strane, ktoré sú takto zreteľne označené.

14 Nové technológie a softvér umožňujú jednoduché a pomerne lacné šírenie dezinformácií prostredníctvom **sociálnych a iných internetových médií**. Dezinformácie sa typicky sústreďujú na citlivé témy, ktoré môžu polarizovať názory a vzbudzovať emócie, a preto je pravdepodobnejšie, že sa budú zdieľať. K takýmto témam patria otázky zdravia (napr. kampane proti očkovaniu), migrácia, zmena klímy či otázky sociálnej spravodlivosti.

Dezinformačné kampane tretích krajín na ovplyvnenie demokratických procesov

15 Cieľom dezinformácií je polarizovať demokratickú diskusiu, vytvoriť alebo zintenzívniť napätie v spoločnosti a ohroziť volebné systémy, pričom majú širší vplyv na európske spoločnosti a bezpečnosť. V konečnom dôsledku oslabujú slobodu presvedčenia a prejavu. Dezinformácie často **podporujú aktéri v tretích krajinách** s cieľom destabilizovať naše spoločnosti a demokratické systémy. V tejto súvislosti môže byť súčasťou rozsiahlych dezinformačných kampaní aj hackovanie sietí. Príkladom je ruská kampaň na ovplyvnenie referenda o odchode z Európskej únie v Spojenom kráľovstve (pozri ***rámček 6***).

[22] Európska komisia, *Oznámenie Boj proti dezinformáciám na internete*, COM(2018) 236.

Rámček 6

Ruské dezinformačné kampane zamerané na demokratické rozhodovacie procesy[23]

V polovici roka 2016 aktéri z Ruska spustili kampaň na ovplyvnenie referenda, ktoré sa malo v Spojenom kráľovstve uskutočniť v júni 2016, tak, aby sa hlasovalo za odchod z EÚ. V jednej analýze tweetov sa zistilo, že počas 48 hodín pred hlasovaním sa tweetovalo s odkazom na *#Brexit* z viac ako 150 000 ruských účtov a uverejnilo sa viac než 45 000 správ o hlasovaní. V deň referenda sa z ruských účtov tweetovalo 1 102-krát s hashtagom *#ReasonsToLeaveEU*.

16 Boj proti dezinformáciám predstavuje veľkú výzvu vzhľadom na potrebu zachovania rovnováhy medzi bezpečnosťou a našimi základnými právami a slobodami na podporu inovácií a otvoreného trhu. EÚ prijala viacero opatrení na **boj proti dezinformáciám**.

- V roku 2015 bola v rámci ESVČ vytvorená **pracovná skupina East StratCom**, ktorej cieľom je napádať ruské dezinformačné kampane[24]. Odborníci chvália úsilie skupiny pri presadzovaní politík EÚ, podpore nezávislých médií v krajinách európskeho susedstva a predvídaní dezinformácií, ich sledovaní a boji proti nim[25].

[23] Park advisors, *Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age*, Christina Nemr a William Gangware, 2019.

[24] Závery Európskej rady, EUCO 11/15, 20. marca 2015. Odvtedy pribudli dve ďalšie pracovné skupiny, jedna pre krajiny západného Balkánu a jedna pre krajiny južného susedstva.

[25] V správe skupiny Atlantic Council sa EÚ vyzvala, aby od všetkých členských štátov vyžadovala, aby vyslali národných odborníkov do pracovnej skupiny. Pozri: D. Fried a A. Polyakova, *Democratic Offense Against Disinformation*, 5. marca 2018.

- V roku 2018 agentúra ENISA vydala **oznámenie o boji proti dezinformáciám na internete**[26]. Súčasťou opatrení je pomoc pri zvyšovaní dôveryhodnosti obsahu a podpora úsilia o zvýšenie mediálnej a spravodajskej gramotnosti.
- Spoločné výskumné centrum Komisie vypracovalo dobrovoľný **samoregulačný kód*ex post*upov** založený na existujúcich politických nástrojoch, ktorý prijali online platformy a reklamný priemysel[27].
- Pôsobiť začala nezávislá európska **sieť overovateľov faktov**.

Dezinformácie v čase ochorenia COVID-19 a reakcia EÚ na ne

17 Dezinformácie boli problémom aj v súvislosti so **zdravotnou krízou spôsobenou ochorením COVID-19**[28] (pozri ***rámček 7*** s príkladmi takýchto dezinformáciami).

[26] ENISA, *Strengthening Network & Information Security & Protecting Against Online Disinformation („Fake News")*, apríl 2018.

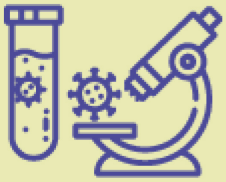
[27] Spoločné výskumné centrum, *The digital transformation of news media and the rise of disinformation and fake news*, Technické správy Spoločného výskumného centra, Pracovný dokument Spoločného výskumného centra o digitálnom hospodárstve 2018-02, apríl 2018.

[28] Reuters Institute a University of Oxford, *Types, Sources, and Claims of Covid-19 Misinformation*, apríl 2020.

Rámček 7

Príklady dezinformácií súvisiace s ochorením COVID-19 vykázané Komisiou[29]

Nepravdivé tvrdenia ako napríklad, že „požitie bielidla alebo čistého alkoholu môže vyliečiť infekciu spôsobenú koronavírusom“: naopak, požitie bielidla alebo čistého alkoholu môže byť veľmi škodlivé. **Belgické toxikologické centrum zaznamenalo nárast počtu incidentov súvisiacich s požitím bielidla o 15 %.**



Konšpiračné teórie, napríklad tvrdenie, že koronavírus je „infekcia spôsobená svetovými elitami s cieľom obmedziť rast obyvateľstva“. Vedecké dôkazy sú jasné: ide o vírus zo skupiny vírusov pochádzajúcich zo zvierat, do ktorej patria ďalšie vírusy, akými sú SARS a MERS.

Nevedecké tvrdenia, že „zariadenia siete 5G spôsobujú šírenie vírusu“. Tieto teórie nemali nijaké konkrétne opodstatnenie a viedli k útokom na telekomunikačné veže.

18 Komisia, ENISA, CERT-EU a EUROPOL vydali v marci 2020 **spoločné vyhlásenie o hrozbách súvisiacich s ochorením COVID-19**[30], v ktorom sa uvádza, že škodlivé subjekty aktívne zneužívajú náročné okolnosti počas krízy v oblasti verejného zdravia s cieľom zamerať sa na pracovníkov na diaľku, podniky aj jednotlivcov. Agentúra ENISA okrem toho vypracovala špecializované informačné kampane pre odvetvia postihnuté dezinformáciami počas pandémie COVID-19[31].

---

[29] Európska komisia, *Boj proti dezinformáciám týkajúcim sa koronavíru*, nedatované.

[30] Joint Statement European Commission, ENISA, CERT-EU and Europol, *Coronavirus outbreak*, 20. marca 2020.

[31] ENISA, *Information sheets relating to Covid 19*, 2020.

Overovanie faktov pomáha v boji proti dezinformáciám

19 EÚ zároveň zvýšila svoje úsilie na podporu európskych overovateľov faktov a výskumníkov dezinformácií. Zriadila najmä **Európske stredisko pre monitorovanie digitálnych médií** na skúmanie a lepšie pochopenie fenoménu dezinformácií: relevantných aktérov, vektorov, nástrojov, metód, dynamiky šírenia, prioritných cieľov a vplyvu na spoločnosť. Ďalšími príkladmi projektov na boj proti dezinformáciám financovaných z prostriedkov EÚ sú PROVENANCE, SocialTruth, EUNOMIA a WeVerify.

20 V roku 2018 EÚ vo svojom **Kódexe postupov proti šíreniu dezinformácií**[32] navrhla prvý celosvetový samoregulačný súbor noriem na boj proti dezinformáciám. Platformy, hlavné sociálne siete, inzerenti a reklamný priemysel podpísali tento dobrovoľný kódex v októbri 2018. Signatármi sú Facebook, Twitter, Mozilla, Google a združenia a členovia reklamného priemyslu. V máji 2019 pristúpila ku kódexu postupov spoločnosť Microsoft. Platforma TikTok pristúpila ku kódexu v júni 2020.

Zaistenie volieb do Európskeho parlamentu v roku 2019

21 Legitimita našich európskych demokratických systémov sa zakladá na informovaných voličoch, ktorí svoju demokratickú vôľu vyjadrujú prostredníctvom **slobodných a spravodlivých volieb**. Každý pokus zlomyseľne a úmyselne ohroziť a zmanipulovať verejnú mienku preto predstavuje závažné ohrozenie našich spoločností. Zasahovanie do volieb a volebnej infraštruktúry môže mať za cieľ ovplyvnenie preferencií voličov, ich účasti na voľbách alebo volebného procesu vrátane samotného hlasovania, ako aj sčítavania hlasov a oznámenia výsledkov. V európskych voľbách v roku 2019, ktoré sa uskutočnili bezprostredne po referende v Spojenom kráľovstve, sa po prvýkrát uskutočnili koordinované opatrenia členských štátov na **ochranu integrity demokratických volieb**, a to volieb do Európskeho parlamentu, ale aj volieb do národných parlamentov.

22 Ako už bolo uvedené, Komisia vydala **oznámenie Boj proti dezinformáciám na internete: európsky prístup**[33] v apríli 2018. Po ňom nasledoval v septembri 2018[34]

---

[32] *EU Code of Practice on Disinformation*, september 2018.

[33] Európska komisia, *Boj proti dezinformáciám na internete: európsky prístup*, COM(2018) 236 final.

[34] Európska komisia, *Správa predsedu Komisie o stave Únie za rok 2018*.

volebný balík zameraný na ochranu volieb v EÚ a členských štátoch pred dezinformáciami a kybernetickými útokmi. Tento balík bol zameraný na ochranu údajov, transparentnosť politickej reklamy a financovania politických strán, kybernetickú bezpečnosť a voľby, ako aj na sankcie za zneužívanie pravidiel na ochranu údajov politickými stranami. Okrem toho sa uskutočnilo **spoločné cvičenie** s cieľom overiť, aké účinné sú reakčné postupy a krízové plány členských štátov a EÚ pri ochrane volieb do Európskeho parlamentu (pozri *rámček 8*).

Rámček 8

ELEx19 – ochrana volieb do Európskeho parlamentu v roku 2019[35]

Cvičenie ELex19 týkajúce sa odolnosti nadchádzajúcich volieb do Európskeho parlamentu bolo zamerané na zistenie spôsobov prevencie, odhaľovania a zmierňovania kybernetických bezpečnostných incidentov, ktoré mohli mať vplyv na voľby v roku 2019.

Cvičenie založené na rôznych scenároch s prvkami kybernetických hrozieb a incidentov účastníkom umožnilo:

— získať prehľad o miere odolnosti (z hľadiska prijatých politík, dostupných spôsobilostí a zručností) volebných systémov v rámci EÚ,

— posilniť spoluprácu príslušných orgánov na vnútroštátnej úrovni (vrátane volebných orgánov a iných príslušných orgánov a agentúr),

— overiť existujúce plány krízového riadenia, ako aj príslušné postupy prevencie, odhaľovania a riadenia kybernetických bezpečnostných útokov a hybridných hrozieb vrátane dezinformačných kampaní a postupy reakcie na ne,

— zlepšiť cezhraničnú spoluprácu a posilniť prepojenie s príslušnými skupinami pre spoluprácu na úrovni EÚ (napr. sieť pre spoluprácu pri voľbách, skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti, sieť jednotiek pre riešenie počítačových bezpečnostných incidentov), a

— identifikovať všetky ďalšie potenciálne nedostatky, ako aj primerané opatrenia na zmiernenie rizík, ktoré by sa mali vykonať pred voľbami do Európskeho parlamentu.

Na tomto cvičení sa zúčastnilo viac ako 80 zástupcov z členských štátov EÚ spolu s pozorovateľmi z Európskeho parlamentu, Komisie a Agentúry EÚ pre kybernetickú bezpečnosť.

23 Európska rada napokon v decembri 2018 prijala **akčný plán proti dezinformáciám**[36] s cieľom poskytnúť koordinovanú reakciu a doplniť vnútroštátne

[35] ENISA, *EU Member States test their cybersecurity preparedness for fair and free 2019 EU elections*, 5. apríla 2019.

[36] Európska komisia, vysoká predstaviteľka Únie pre zahraničné veci a bezpečnostnú politiku, *Akčný plán proti dezinformáciám*, JOIN(2018) 36 final. Plán sa zameriava: na zlepšenie

úsilie. Tento akčný plán zahŕňal konkrétne opatrenia založené na štyroch pilieroch: zlepšenie spôsobilostí inštitúcií Únie zisťovať, analyzovať a odhaľovať dezinformácie; posilnenie koordinovaných, spoločných reakcií na dezinformácie; aktivizácia súkromného sektora pri boji proti dezinformáciám a zvyšovanie informovanosti a zvýšenie odolnosti spoločnosti.

Kybernetická bezpečnosť v EÚ: právomoci, aktéri, stratégie a právne predpisy

Kybernetická bezpečnosť je primárne zodpovednosťou členských štátov

24 V EÚ za kybernetickú bezpečnosť primárne **zodpovedajú členské štáty**. Osobitne to platí v prípade ochrany citlivých informácií týkajúcich sa národnej bezpečnosti. Všetky členské štáty majú **národnú stratégiu kybernetickej bezpečnosti**, ktorá im pomáha riešiť riziká, ktoré by potenciálne mohli oslabiť dosahovanie ekonomických a sociálnych prínosov kybernetického priestoru. Medzi členskými štátmi však stále existujú rozdiely, pokiaľ ide o ich kapacitu a odhodlanie v oblasti kybernetickej bezpečnosti.

25 EÚ zohráva úlohu pri vytváraní **spoločného regulačného rámca** na jednotnom trhu EÚ a vytváraní podmienok pre účinnú spoluprácu členských štátov v rôznych politických oblastiach relevantných pre kybernetickú bezpečnosť, ako sú spravodlivosť a vnútorné veci, jednotný trh, doprava, verejné zdravie, spotrebiteľská politika a výskum. V prípade vonkajšej politiky zohráva kybernetická bezpečnosť úlohu v diplomacii a čoraz viac sa stáva súčasťou vznikajúcej obrannej a bezpečnostnej politiky EÚ.

26 Hlavní **aktéri** v oblasti kybernetickej bezpečnosti **na úrovni EÚ** sa uvádzajú v *rámčeku 9* nižšie.

spôsobilostí inštitúcií EÚ zisťovať, analyzovať a odhaľovať dezinformácie; na posilnenie koordinovaných, spoločných reakcií; na aktivizáciu súkromného sektora a na zvyšovanie informovanosti a zvýšenie odolnosti spoločnosti.

Rámček 9

Hlavní aktéri v oblasti kybernetickej bezpečnosti na úrovni EÚ

Cieľom **Európskej komisie** je zvýšiť spôsobilosti a spoluprácu v oblasti kybernetickej bezpečnosti, posilniť EÚ v úlohe aktéra v tejto oblasti a začleniť kybernetickú bezpečnosť do ostatných politík EÚ.

Komisiu podporujú viaceré agentúry EÚ, najmä **ENISA**, **EC3** a **CERT-EU**. **Agentúra Európskej únie pre kybernetickú bezpečnosť** (známa ako **ENISA** podľa jej pôvodného názvu – Agentúra Európskej únie pre sieťovú a informačnú bezpečnosť) je predovšetkým poradným orgánom a podporuje rozvoj politiky, budovanie kapacít a zvyšovanie informovanosti. **Európske centrum boja proti počítačovej kriminalite (EC3)** pri Europole bolo zriadené s cieľom posilniť reakciu orgánov presadzovania práva EÚ na počítačovú kriminalitu. **Tím reakcie na núdzové počítačové situácie (CERT-EU)** podporujúci všetky inštitúcie, orgány a agentúry Únie zabezpečuje Komisia.

Európska služba pre vonkajšiu činnosť (ESVČ) má vedúcu úlohu v oblasti kybernetickej obrany, kybernetickej diplomacie a strategickej komunikácie a zabezpečuje spravodajské a analytické centrá. Cieľom **Európskej obrannej agentúry (EDA)** je rozvoj spôsobilostí v oblasti kybernetickej obrany.

Na úrovni EÚ konajú členské štáty prostredníctvom **Rady**, ktorá má množstvo orgánov na koordináciu a výmenu informácií (patrí medzi ne horizontálna pracovná skupina pre kybernetické otázky). **Európsky parlament** pôsobí ako spoluzákonodarca.

Organizácie súkromného sektora vrátane odvetvia, orgánov na správu internetu a akademickej obce sú partnermi prispievajúcimi k rozvoju a vykonávaniu politiky, a to napríklad aj prostredníctvom zmluvných verejno-súkromných partnerstiev (**cPPP**).

Kybernetická stratégia EÚ: kybernetická bezpečnosť je zdrojom veľkých obáv od roku 2013

27 Kybernetická bezpečnosť je hlavným politickým problémom aspoň od roku 2013, keď Komisia prijala svoju **stratégiu kybernetickej bezpečnosti**[37]. Táto stratégia má päť hlavných cieľov:

- zvyšovanie kybernetickej odolnosti,
- zníženie počítačovej kriminality,
- rozvoj politiky a spôsobilostí kybernetickej obrany,
- rozvoj priemyselných a technologických zdrojov pre kybernetickú bezpečnosť,
- vytvorenie medzinárodnej politiky kybernetického priestoru v súlade s kľúčovými hodnotami EÚ.

V nasledujúcich rokoch sa otázka kybernetickej bezpečnosti takisto riešila v ďalších stratégiách EÚ (pozri ***rámček 10***).

[37] Európska komisia, *Stratégia kybernetickej bezpečnosti Európskej únie:Otvorený, bezpečný a chránený kybernetický priestor*, JOIN(2013) 1 final, 7. februára 2013.

Rámček 10

Ďalšie stratégie EÚ riešiace otázku kybernetickej bezpečnosti

- **Európsky program v oblasti bezpečnosti** (2015)[38], ktorého cieľom bolo zlepšiť presadzovanie práva a reakciu justičného systému na počítačovú kriminalitu, a to najmä prostredníctvom obnovenia aktualizácií existujúcich politík a právnych predpisov.
- Digitálny jednotný trh (2015)[39], ktorého cieľom bolo poskytnúť lepší prístup k digitálnemu tovaru a službám: na tento účel je nevyhnutné posilniť online bezpečnosť, dôveru a inklúziu.
- **Globálna stratégia EÚ** (2016)[40], v ktorej sú stanovené viaceré iniciatívy na posilnenie úlohy EÚ vo svete. Kľúčový pilier pritom tvorili kybernetická bezpečnosť a vyvracanie dezinformácií prostredníctvom strategickej komunikácie.

28 Okrem toho Európska komisia a vysoká predstaviteľka Únie pre zahraničné veci a bezpečnostnú politiku vydali v roku 2017 **spoločné oznámenie o kybernetickej bezpečnosti pre EÚ**[41] určené Európskemu parlamentu a Rade, v ktorom vyzvali na silnejšie a účinnejšie štruktúry na podporu kybernetickej bezpečnosti a reakciu na kybernetické útoky v členských štátoch, ale aj v inštitúciách, agentúrach a orgánoch EÚ.

---

[38] Európska komisia, *Európsky program v oblasti bezpečnosti*, COM(2015) 185 final, 28. apríla 2015.

[39] Európska komisia, *Stratégia pre jednotný digitálny trh v Európe*, COM(2015) 192 final, 6. mája 2015.

[40] ESVČ, *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*, jún 2016.

[41] Európska komisia a vysoká predstaviteľka Únie pre zahraničné veci a bezpečnostnú politiku, *Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ*, JOIN(2017) 450, 13. septembra 2017.

29 V júli 2020 Európska komisia aktualizovala svoj program na rok 2015 a prijala **stratégiu EÚ pre bezpečnostnú úniu**[42] na roky 2020 – 2025, v ktorej označila kybernetickú bezpečnosť za strategicky dôležitú otázku. V tejto stratégii Komisia osobitne zdôrazňuje to, čo poznáme ako hybridné hrozby zahŕňajúce kybernetické útoky aj dezinformačné kampane, pri ktorých štátne a neštátne subjekty z tretích krajín konajú zosúladene so zámerom manipulovať informačné prostredie a útočiť na hlavné infraštruktúry.

Právne predpisy EÚ v oblasti kybernetickej bezpečnosti: smernica o sieťovej a informačnej bezpečnosti, nariadenie o ochrane osobných údajov, akt o kybernetickej bezpečnosti a nový systém sankcií

30 Hlavným pilierom stratégie kybernetickej bezpečnosti z roku 2013 a ústredným právnym predpisom je **smernica o kybernetickej bezpečnosti (smernica NIS)**[43] z roku 2016, ktorá je prvým celoeurópskym právnym predpisom o kybernetickej bezpečnosti. Cieľom smernice je dosiahnutie minimálnej úrovne harmonizovaných kapacít tým, že členským štátom ukladá povinnosť prijať národné stratégie pre sieťovú a informačnú bezpečnosť a zriadiť jednotné kontaktné miesta a jednotky pre riešenie počítačových bezpečnostných incidentov (jednotky CSIRT)[44]. Stanovujú sa v nej aj bezpečnostné a oznamovacie požiadavky pre prevádzkovateľov základných služieb v kľúčových odvetviach a pre poskytovateľov digitálnych služieb.

31 Členské štáty museli **transponovať smernicu NIS do svojho vnútroštátneho práva** do mája 2018. Takisto museli do novembra 2018 určiť takzvaných prevádzkovateľov základných služieb. Európska komisia je povinná pravidelne preskúmať fungovanie tejto smernice. Od júla do októbra 2020 v rámci svojho

---

[42] Európska komisia, *Oznámenie o stratégii EÚ pre bezpečnostnú úniu*, COM (2020)605 final, 24. júla 2020.

[43] Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii.

[44] Tieto tímy sú začlenené do štruktúr spolupráce zriadených na základe smernice, do siete jednotiek CSIRT (sieť tvorená určenými jednotkami CSIRT členských štátov EÚ a tímom CERT-EU; sekretariát zabezpečuje agentúra ENISA) a do skupiny pre spoluprácu (ktorá podporuje a uľahčuje strategickú spoluprácu a výmenu informácií medzi členskými štátmi a ktorej sekretariát zabezpečuje Komisia).

kľúčového politického cieľa „Európa pripravená na digitálny vek“, ako aj v súlade s cieľmi bezpečnostnej únie Komisia uskutočnila konzultáciu, ktorej výsledky sa použijú na prvé hodnotenie a *ex post* posúdenie vplyvu smernice NIS.

32 Súbežne s touto smernicou v roku 2016 nadobudlo účinnosť **všeobecné nariadenie o ochrane údajov**[45] (GDPR), ktoré sa uplatňuje od mája 2018. Jeho cieľom je ochrana osobných údajov občanov Európskej únie tým, že stanovuje pravidlá týkajúce sa ich spracovania a šírenia. Nariadenie dotknutým osobám priznáva isté práva a ukladá povinnosti prevádzkovateľom údajov (poskytovateľom digitálnych služieb), pokiaľ ide o používanie a prenos informácií.

33 Okrem toho sa v **akte EÚ o kybernetickej bezpečnosti**[46] po prvýkrát zavádza celoeurópsky rámec certifikácie kybernetickej bezpečnosti produktov, služieb a procesov IKT. Znamená to, že spoločnosti podnikajúce v EÚ získajú výhody plynúce z toho, že svoje produkty, služby a procesy IKT budú musieť certifikovať len raz a ich certifikáty budú uznávané v celej EÚ. Aktom o kybernetickej bezpečnosti sa takisto zriadila **Agentúra Európskej únie pre kybernetickú bezpečnosť** (ENISA, nahrádzajúca bývalú Európsku agentúru pre bezpečnosť sietí a informácií). Agentúra sa v ňom poveruje, aby posilnila operačnú spoluprácu na úrovni EÚ tým, že členským štátom EÚ, ktoré o to požiadajú, pomôže riešiť kybernetickobezpečnostné incidenty, a podporí koordináciu EÚ v prípade rozsiahlych cezhraničných kybernetických útokov a kríz.

34 Napokon v máji 2019 Rada vytvorila právny nástroj, ktorý EÚ umožňuje ukladať cielené reštriktívne **opatrenia na odrádzanie od kybernetických útokov**, ktoré predstavujú vonkajšiu hrozbu pre EÚ alebo jej členské štáty, a reakciu na ne[47]. Vďaka nemu má EÚ právomoc ukladať sankcie osobám alebo subjektom, ktoré:

- sú zodpovedné za kybernetické útoky alebo pokusy o ne alebo

[45] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

[46] Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií, 17. apríla 2019.

[47] Rozhodnutie Rady (CFSP) 2019/797 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty, 17. mája 2019.

- podporujú takéto útoky finančne, technicky či materiálne alebo sa na nich inak zúčastňujú.

V júli 2020 Rada prvýkrát využila tieto nové výsady (pozri ***rámček 11***).

Rámček 11

Zvyšovanie spoľahlivosti – EÚ uložila vôbec prvé sankcie za kybernetické útoky[48]

V júli 2020 Rada uložila reštriktívne opatrenia voči šiestim osobám a trom subjektom, ktoré sú zodpovedné za rôzne kybernetické útoky alebo sa na nich zúčastnili. Medzi príklady takéhoto správania patrí pokus o kybernetický útok na Organizáciu pre zákaz chemických zbraní a útoky známe pod názvami WannaCry, NotPetya a Operation Cloud Hopper.

Prijaté sankcie zahŕňajú zákaz cestovania a zmrazenie aktív. Okrem toho sa osobám a subjektom z EÚ zakazuje poskytovať finančné prostriedky osobám a subjektom zaradeným na zoznam.

Kybernetická bezpečnosť a kybernetická obrana

35 V posledných rokoch sa kybernetický priestor postupne militarizuje[49] a prispôsobuje na použitie vo vojne[50]. Popri zemi, mori, vzduchu a vesmíre sa považuje za piatu oblasť vedenia vojny. **Politický rámec EÚ pre kybernetickú obranu** bol prijatý

[48] Rozhodnutie Rady (CFSP) 2020/1127 z 30. júla 2020, ktorým sa mení rozhodnutie (SZBP) 2019/797 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty.

[49] Centrum pre európske politické štúdie, *Strengthening the EU's Cyber Defence Capabilities – Report of a CEPS Task Force*, november 2018.

[50] Malvér, ktorý bol zdrojom útokov prostredníctvom ransomvéru WannaCry, za ktorých pôvodcu Spojené štáty, Spojené kráľovstvo a Austrália označili Severnú Kóreu, pôvodne vyvinula americká Národná bezpečnostná agentúra, ktorá zhromažďovala údaje o chybách v operačnom systéme Windows s cieľom využiť tieto nedostatky.
Zdroj: A. Greenberg, WIRED, 19. decembra 2017. Hneď po útokoch Microsoft odsúdil zhromažďovanie chýb v softvéri zo strany vlád a zopakoval svoju výzvu na prijatie digitálneho ženevského dohovoru.

v roku 2014 a v roku 2018 bol aktualizovaný[51]. V rámci aktualizácie z roku 2018 sa určili priority vrátane budovania spôsobilostí v oblasti kybernetickej obrany, ako aj ochrany komunikačných a informačných sietí spoločnej bezpečnostnej a obrannej politiky EÚ (SBOP). Kybernetická obrana je takisto súčasťou rámca stálej štruktúrovanej spolupráce (PESCO) a spolupráce medzi EÚ a NATO.

36 Prípady využívania kybernetického priestoru na politické účely a agresívne skúšanie a prienik do kybernetickej bezpečnosti EÚ a členských štátov sa stali bežnými. Z týchto činov kybernetickej špionáže a hackingových činov, ktoré sa zameriavajú na národné vlády, politické subjekty a inštitúcie EÚ s cieľom získavať a zbierať utajované skutočnosti, vyplýva, že prebiehajú dômyselné operácie kybernetickej špionáže a manipulácie údajov namierené proti EÚ a jej členským štátom. **Spoločný rámec EÚ pre boj proti hybridným hrozbám** (2016) sa zaoberá riešením kybernetických hrozieb pre kritickú infraštruktúru aj pre súkromných používateľov, pričom sa v ňom zdôrazňuje skutočnosť, že kybernetické útoky sa môžu uskutočniť aj prostredníctvom dezinformačných kampaní v sociálnych médiách[52]. Takisto sa v ňom poukazuje na to, že treba zvýšiť informovanosť a posilniť spoluprácu medzi EÚ a NATO, čo sa potvrdilo v spoločných vyhláseniach EÚ – NATO z rokov 2016 a 2018[53].

Výdavky súvisiace s kybernetickou bezpečnosťou: rozptýlené a zaostávajúce

Menej výdavkov vynaložených na kybernetickú bezpečnosť v EÚ27 ako v USA

37 Je ťažké odhadnúť verejné výdavky na kybernetickú bezpečnosť z dôvodu ich prierezovej povahy a z toho dôvodu, že kybernetická bezpečnosť a všeobecné výdavky na informačné technológie sú často nerozoznateľné[54]. Napriek tomu by z dostupných

---

[51] *Politický rámec EÚ pre kybernetickú obranu (aktualizácia za rok 2018)*, 14413/18, 19. novembra 2018.

[52] Európska komisia/Európska služba pre vonkajšiu činnosť, *Spoločný rámec pre boj proti hybridným hrozbám: reakcia Európskej únie*, JOIN(2016) 18 final, 6. apríla 2016.

[53] Spoločné vyhlásenie predsedu Európskej rady, predsedu Európskej komisie a generálneho tajomníka Organizácie Severoatlantickej zmluvy, 8. júla 2016 a 10. júla 2018.

[54] Európska komisia, tamže, COM(2018) 630 final, 12. septembra 2018.

údajov vyplývalo, že **verejné výdavky na kybernetickú bezpečnosť** v EÚ sú relatívne nízke:

- v roku 2020 dosahoval rozpočet federálnej vlády USA určený výlučne na kybernetickú bezpečnosť výšku **17,4 mld. USD**[55],
- na porovnanie, Komisia odhaduje, že verejné výdavky na kybernetickú bezpečnosť sa pohybujú v rozmedzí od **jednej do dvoch miliárd EUR** ročne pre všetky členské štáty EÚ (ktoré majú spolu takmer rovnaký HDP ako USA)[56],
- v mnohých členských štátoch sa verejné výdavky na kybernetickú bezpečnosť odhadujú ako percentuálny podiel HDP na jednu desatinu úrovne v USA alebo sú ešte nižšie[57].

2014 – 2020: Financovanie kybernetickej bezpečnosti z prostriedkov EÚ je rozptýlené naprieč niekoľkými rôznymi nástrojmi

38 Podľa Komisie[58] existuje v rámci všeobecného rozpočtu EÚ najmenej **desať rôznych nástrojov**, prostredníctvom ktorých možno financovať záležitosti súvisiace s kybernetickou bezpečnosťou (pozri ***rámček 12*** pre hlavné programy z finančného hľadiska). V období 2014 – 2020 predstavovali finančné prostriedky EÚ na nevojenskú kybernetickú bezpečnosť menej ako **200 mil. EUR ročne**. Takisto neexistuje žiadny celoeurópsky nástroj financovania, ktorý by podporil členské štáty pri koordinácii ich činností v oblasti kybernetickej bezpečnosti.

---

[55] Biely dom, *Cybersecurity spending fiscal year 2020*.

[56] Európska komisia, Pracovný dokument útvarov Komisie: Posúdenie vplyvu, sprievodný dokument k návrhu nariadenia Európskeho parlamentu a Rady, ktorým sa stanovuje program Digitálna Európa na obdobie 2021 – 2027, SWD(2018) 305 final, 6. júna 2018.

[57] The Hague Centre for Strategic Studies, *Dutch investments in ICT and cybersecurity: putting it in perspective*, december 2016.

[58] Európska komisia, *Posúdenie vplyvu sprevádzajúce návrh nariadenia, ktorým sa zriaďuje Európske centrum odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier,* SWD(2018) 403 final, 12. septembra 2018.

Rámček 12

Programy EÚ podporujúce projekty v oblasti kybernetickej bezpečnosti (2014 – 2020)

- V rámci **výskumných programov EÚ Horizont 2020** sa na projekty v oblasti kybernetickej bezpečnosti a počítačovej kriminality v období 2014 – 2020 vyčlenilo približne 600 mil. EUR. Zahŕňa to 450 mil. EUR na cPPP („zmluvné verejno-súkromné partnerstvá“) v oblasti kybernetickej bezpečnosti v období 2017 – 2020 s cieľom prilákať ďalších 1,8 mld. EUR zo súkromného sektora.
- Z **európskych štrukturálnych a investičných fondov (EŠIF)** sa poskytol príspevok až do výšky 400 mil. EUR na investície členských štátov v oblasti kybernetickej bezpečnosti do konca roka 2020.
- Z **Nástroja na prepájanie Európy (NPE)** sa financovali investície vo výške približne 30 mil. EUR ročne. Zahŕňa to spolufinancovanie národných tímov reakcie na núdzové počítačové situácie (CERT), ktoré sú členské štáty povinné zriadiť podľa smernice NIS, vo výške približne 13 mil. EUR ročne v rokoch 2016 až 2018[59].
- **Časť Fondu pre vnútornú bezpečnosť týkajúca sa polície (ISF-P)** podporuje štúdie, stretnutia expertov a komunikačné aktivity a táto podpora v rokoch 2014 – 2017 dosiahla takmer 62 mil. EUR. Členské štáty takisto môžu prijímať granty na vybavenie, odbornú prípravu, výskum a zber údajov v rámci zdieľaného riadenia. Granty v hodnote 42 mil. EUR prijalo deväťnásť členských štátov.
- Z **programu Spravodlivosť** sa poskytla podpora vo výške 9 mil. EUR na podporu súdnej spolupráce a zmlúv vzájomnej právnej pomoci s osobitným zameraním na výmenu elektronických údajov a finančných informácií.

39 Okrem toho bolo v rokoch 2019 a 2020 z rozpočtu EÚ vyčlenených 500 miliónov na **Program rozvoja európskeho obranného priemyslu**[60]. Program sa zameriava

[59] Článok 9 ods. 2 smernice Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (smernica NIS).

[60] Európska komisia, Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1092 z 18. júla 2018, ktorým sa zriaďuje Program rozvoja európskeho obranného priemyslu zameraný

na zlepšenie koordinácie a efektívnosti výdavkov členských štátov na obranu prostredníctvom stimulov na spoločný vývoj. Jeho cieľom je vytvorenie investícií do obrannej spôsobilosti po roku 2020 vo výške 13 mld. EUR, a to prostredníctvom Európskeho obranného fondu, ktorých časť sa bude týkať kybernetickej obrany. Napokon poskytne v rokoch 2018 až 2020 **Európska investičná banka** v rámci európskej bezpečnostnej iniciatívy finančné prostriedky s dvojakým využitím vo výške 6 mld. EUR (výskum a vývoj/kybernetická bezpečnosť a civilná bezpečnosť)[61].

2021 – 2027: Nový program Digitálna Európa

40 Rada vo svojich záveroch z júla 2020 o novom viacročnom finančnom rámci (VFR) na roky 2021 – 2027 rozhodla, že z **programu Digitálna Európa (DEP)**[62] budú poskytované investície do kľúčových strategických digitálnych kapacít, ako sú vysokovýkonná výpočtová technika, umelá inteligencia a kybernetická bezpečnosť EÚ. V rámci podpory digitálnej transformácie Európy bude dopĺňať iné nástroje, najmä program Horizont Európa a Nástroj na prepájanie Európy.

41 Rada sa takisto rozhodla na program Digitálna Európa vyčleniť 6,8 mld. EUR na obdobie 2021 – 2027 alebo približne **970 mil. EUR ročne**. Ide o značný nárast v porovnaní s obdobím 2014 – 2020, ale stále je to menej, ako pôvodne navrhovala Komisia (8,2 mld. EUR za rovnaké obdobie, pričom 2 mld. EUR sú určené na posilnenie odvetvia kybernetickej bezpečnosti EÚ a celkovú spoločenskú ochranu, napríklad podporou vykonávania smernice NIS).

na podporu konkurencieschopnosti a inovačnej kapacity obranného priemyslu Únie (Ú. v. EÚ L 200, 7.8.2018, s. 30).

[61] Európska investičná banka, *The EIB Group Operating Framework and Operational Plan 2018*, 12. decembra 2017.

[62] Európska komisia, *Europe investing in digital: the Digital Europe Programme*, september 2020.

ČASŤ II – Prehľad činnosti najvyšších kontrolných inštitúcií

Úvod

42 Kybernetická bezpečnosť a naša digitálna autonómnosť sa pre EÚ a jej členské štáty stali strategicky dôležitými témami. Nedostatky v riadení kybernetickej bezpečnosti vo verejnom a súkromnom sektore pretrvávajú vo všetkých členských štátoch, hoci na rôznej úrovni. Znižuje sa tým naša schopnosť obmedziť kybernetické útoky a v prípade potreby na ne reagovať.

43 Napriek tomu z prieskumu najvyšších kontrolných inštitúcií (NKI) v EÚ z roku 2018 vyplynulo, že približne polovica nikdy nevykonávala audit kybernetickej bezpečnosti. Odvtedy NKI prispôsobili svoju audítorskú činnosť kybernetickej bezpečnosti, kladúc osobitný dôraz na ochranu osobných údajov, pripravenosť systémov na kybernetické útoky a ochranu systémov kľúčových verejných služieb. Takisto sa venovali ďalším vysoko relevantným témam. Z pochopiteľných dôvodov nemožno zverejniť všetky tieto audity, keďže niektoré sa môžu týkať citlivých informácií (národnej bezpečnosti).

44 Z dôvodu významu kybernetickej bezpečnosti pre fungovanie našej spoločnosti a našich politických inštitúcií sa Kontaktný výbor rozhodol venovať tohtoročné zhrnutie auditov tejto téme. Druhá časť obsahuje prehľad výsledkov vybraných auditov, ktoré vykonali NKI dvanástich prispievajúcich členských štátov a Európsky dvor audítorov, ktoré sa týkajú kybernetickej bezpečnosti. Každá zúčastnená NKI prispela jednou vybranou audítorskou správou, ktorá je podrobnejšie zhrnutá v tretej časti. K tejto téme sa vykonalo mnoho ďalších auditov, ako vyplýva z ďalších správ uvádzaných zúčastnenými NKI.

Audítorská metodika a zahrnuté témy

45 Pokiaľ ide o druh auditu vykonaného v súvislosti s audítorskými správami zhrnutými v tomto zhrnutí, väčšina najvyšších kontrolných inštitúcií, ktoré prispeli, vykonala audity výkonnosti v oblastiach kybernetickej bezpečnosti, zatiaľ čo dve (poľské a maďarské najvyššie kontrolné inštitúcie) vykonali audity zhody a jeden (EDA) vykonal preskúmanie politiky.

46 Pri stanovovaní svojho audítorského prístupu väčšina NKI naplánovala svoje audity tak, aby zahŕňali aspoň dva spôsoby posúdenia témy auditu. To by mohlo spočívať v preskúmaní strategických dokumentov alebo stanovených politík na vysokej (napr. na vnútroštátnej) úrovni, preskúmaní postupov na posúdenie ich súladu so stanovenou metodikou COBIT (pozri ***rámček 13***) alebo preskúmaní účinnosti zavedených riadiacich systémov IT. Jedna NKI (Holandský dvor audítorov) dokonca využila etických hackerov na testovanie účinnosti kybernetickobezpečnostných systémov na kontrolu hraníc a kritických vodných diel. V ***rámčeku 14*** uvádzame schematický prehľad metód a techník, ktoré použili rôzne NKI na výkon svojej audítorskej činnosti.

Rámček 13

Čo je to COBIT?

Kontrolné ciele pre informačné a príbuzné technológie (COBIT) predstavujú rámec uznávaných najlepších postupov a procesov v oblasti riadenia IT a správy IT, ktorý stanovila Asociácia auditu a kontroly informačných systémov (ISACA). Pomáha organizáciám dosahovať strategické ciele pomocou účinného využívania dostupných zdrojov a minimalizáciu rizík IT. COBIT prepája podnikovú správu a správu IT. Toto prepojenie sa dosahuje prepájaním podnikových cieľov a cieľov IT, vymedzovaním metrických a vývojových modelov na meranie dosahovania cieľov a vymedzovaním povinností vlastníkov podnikových procesov a procesov IT.

47 Témy riešené počas vykonávania auditu kybernetickej bezpečnosti sa značne líšili. Niektoré NKI vykonávali audit veľmi špecifických oblastí verejného záujmu, napríklad holandská NKI vykonala audit kybernetickej bezpečnosti kľúčových systémov holandskej morskej obrany a vodného hospodárstva. Ďalšie, ako napríklad írska a maďarská NKI, sa venovali horizontálnejším otázkam, ako je napríklad vykonávanie národnej stratégie kybernetickej bezpečnosti a ochrana osobných údajov a národných súborov údajov. Napriek tomu sa všetky NKI zaoberali otázkami, ktoré môžu mať negatívny vplyv na verejné služby alebo infraštruktúru.

48 Estónska a litovská NKI uznali strategický význam národných súborov údajov, ktoré majú kritický význam v rámci národnej bezpečnosti, a ochrany ich integrity pred kybernetickými útokmi zvonka. Dánska NKI venovala audit osobitne posúdeniu bezpečnosti štyroch orgánov, pokiaľ ide o útoky ransomvéru. Holandská, poľská

a portugalská NKI vykonali audity účinnosti rôznych systémov IT podporujúcich kontroly na hraniciach (na letisku Schiphol, na Hlavnom veliteľstve pohraničnej stráže a na Ministerstve vnútra a správy v Poľsku a na portugalských hraniciach v uvedenom poradí), ktoré sa preto takisto venovali bezpečnosti v rámci EÚ.

Obdobie auditu

49 Vybrané audítorské správy v tomto zhrnutí boli uverejnené v rokoch 2014 až 2020. Pri väčšine z nich trvalo obdobie auditu dva roky alebo viac rokov, hoci pri štyroch (Dánsko, Estónsko, Francúzsko a Portugalsko) trvalo kontrolované obdobie jeden rok.

Ciele auditu

50 Jednotlivé NKI prispievajúce do tohto zhrnutia sa pri vykonávaní auditu zaoberali širokou škálou rizík. Rizikami riešenými v ich príspevkoch boli: ohrozenie individuálnych práv občanov EÚ zneužitím osobných údajov, riziká hroziace inštitúciám, že nebudú schopné poskytovať dôležitú verejnú službu alebo budú fungovať obmedzene, vážne dôsledky pre verejnú bezpečnosť, kvalitu života a hospodárstvo členských štátov, ako aj kybernetickú bezpečnosť v rámci EÚ. Najmenej štyri NKI (estónska, maďarská, holandská a portugalská) sa zaoberali tromi alebo viacerými témami uvedenými v ich audítorských správach, ktoré sú zahrnuté v tomto zhrnutí.

51 Kybernetická bezpečnosť zostáva v právomoci členských štátov. Napriek tomu, keďže právne predpisy EÚ sa časom rozšírili a stali konkrétnejšími, väčšina inštitúcií a orgánov, ktorých audit NKI vykonali, už prispieva k dosahovaniu strategických cieľov EÚ v oblasti kybernetickej bezpečnosti, hoci v rôznom rozsahu. Napríklad írsky Úrad kontrolóra a generálneho audítora (*Office of the Comptroller and Auditor General*) vykonal audit vykonávania smernice EÚ o sieťovej a informačnej bezpečnosti, ktorej cieľom je zlepšiť odolnosť kľúčových sieťových a informačných systémov, a poradil, ako ho zlepšiť. Podobne aj Štátny kontrolný úrad Maďarska sa vo svojom audite venoval aspektu súladu s existujúcimi smernicami EÚ.

52 Z ***rámčeka 14*** takisto vyplýva, kedy výsledky auditu buď prispeli k zvýšeniu kybernetickej odolnosti kontrolovanej inštitúcie, k zníženiu počítačovej kriminality, alebo by pomohli rozvíjať politiku kybernetickej obrany a posilniť kompetencie, zlepšiť

vývoj technológii a dosiahnuť pokrok v spolupráci na medzinárodnej úrovni, čo predstavuje hlavné ciele stratégie kybernetickej bezpečnosti EÚ. Odporúčania vydané NKI sa vo väčšine prípadov týkali viac ako dvoch strategických cieľov, ktoré sa EÚ snaží dosiahnuť.

53 Okrem toho sa v rámci audítorskej činnosti vykonanej NKI odhalili bezpečnostné a implementačné medzery, ktoré podnietili kontrolované inštitúcie k ďalším snahám. Počas audítorskej činnosti napríklad štyri kontrolované inštitúcie v Dánsku už začali zavádzať viaceré výhľadové bezpečnostné kontroly s cieľom značne zvýšiť úroveň ochrany pred útokmi ransomvéru, rozvíjať obranné spôsobilosti a zvyšovať kybernetickú odolnosť, čím znížia svoje vystavenie počítačovej kriminalite v budúcnosti.

54 Takisto vidíme, že audítorské odporúčania boli vydané na rôznych úrovniach riadenia a zodpovednosti, pričom sa týkali ústrednej štátnej správy, ministerstiev a agentúr na operačnej úrovni alebo vlastníkov systémov IT.

Rámček 14

Prehľad audítorskej činnosti NKI v rámci príspevkov obsiahnutých v zhrnutí (časť 1)

Hlavná oblasť zamerania		Dánsko	Estónsko	Írsko	Francúzsko	Lotyšsko	Litva	Maďarsko	Holandsko	Poľsko	Portugalsko	Fínsko	Švédsko	EÚ (Európsky dvor audítorov)
Typ auditu	Výkonnosť	✓	✓	✓	✓	✓	✓		✓		✓	✓	✓	
	Súlad s pravidlami							✓		✓				
	Preskúmanie													✓
Audítorský prístup	Preskúmanie politík	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓
	Preskúmanie postupov	✓	✓		✓		✓	✓		✓	✓	✓		
	Preskúmanie systémov	✓			✓	✓	✓	✓	✓	✓	✓		✓	
	Posúdenie spoľahlivosti priamym testovaním								✓		✓			
Riešené hrozby	Vplyv na individuálne práva		✓		✓			✓			✓			✓
	Vplyv na verejnú infraštruktúru alebo služby	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Vplyv na národnú bezpečnosť		✓	✓		✓	✓	✓	✓		✓			
	Vplyv na bezpečnosť v rámci EÚ	✓							✓		✓			✓

Prehľad audítorskej činnosti NKI v rámci príspevkov obsiahnutých v zhrnutí (časť 2)

Hlavná oblasť zamerania		Dánsko	Estónsko	Írsko	Francúzsko	Lotyšsko	Litva	Maďarsko	Holandsko	Poľsko	Portugalsko	Fínsko	Švédsko	EÚ (Európsky dvor audítorov)
Pokryté strategické ciele EÚ v oblasti kybernetickej bezpečnosti	Zvyšovanie kybernetickej odolnosti	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
	Zníženie počítačovej kriminality	✓					✓							✓
	Rozvoj obrannej politiky a spôsobilostí	✓	✓	✓		✓	✓	✓	✓	✓				✓
	Rozvoj technologických zdrojov				✓	✓			✓				✓	
	Zlepšenie medzinárodnej spolupráce (politiky)			✓				✓						✓
Úroveň adresáta odporúčaní	Ústredná štátna správa	✓	✓				✓					✓	✓	✓
	Operačná (ministerstvá a agentúry)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Vlastníci systémov IT	✓			✓			✓	✓	✓				

Hlavné audítorské pripomienky

55 V nasledujúcich častiach sú zhrnuté hlavné audítorské pripomienky NKI.

Audity výkonnosti

56 **Dánsky** vnútroštátny kontrolný úrad ***Rigsrevisionen*** posudzoval, či vybrané kľúčové vládne inštitúcie majú dostatočnú ochranu pred ransomvérom. Vládne inštitúcie sú častými terčmi kybernetických útokov, pričom ransomvér je v súčasnosti jednou z najväčších hrozieb pre kybernetickú bezpečnosť. Audit sa týkal dánskeho Úradu pre zdravotné údaje, Ministerstva zahraničných vecí, spoločnosti Banedanmark (dánska železničná sieť) a dánskej Agentúry pre riadenie núdzových situácií. Tieto štyri inštitúcie boli vybrané preto, lebo zodpovedajú za poskytovanie základných služieb v oblasti zdravia, zahraničných vecí, dopravy a pripravenosti na núdzové situácie, v ktorých môže mať zabezpečenie prístupu k údajom kľúčový význam. Pri audite sa zistilo, že tieto štyri inštitúcie nemali dostatočnú ochranu pred ransomvérom. Z audítorskej činnosti vyplynulo, že inštitúcie nemali zavedené viaceré bežné bezpečnostné kontroly na zmiernenie následkov útokov. Záverom auditu bolo, že je dôležité, aby inštitúcie zvážili zavedenie výhľadových bezpečnostných kontrol, aby zvýšili svoju odolnosť voči útokom ransomvéru.

57 **Estónsky** vnútroštátny kontrolný úrad ***Riigikontroll*** uznal, že zachovanie estónskej nezávislosti si vyžaduje nielen fyzickú obranu územia, ale takisto ochranu digitálnych aktív, ktoré majú najvyšší štátny význam. Digitálne aktíva, ktoré si vyžadujú najväčšiu ochranu, sú údaje týkajúce sa občanov, územia a právnych predpisov. Takisto je potrebné zabezpečiť údaje týkajúce sa majetku, nehnuteľností a práv osôb s pobytom v Estónsku. Estónsky kontrolný úrad skúmal možnosť kybernetických hrozieb v prípade eskalácie bezpečnostných problémov. Takéto rizikové scenáre a nárast počtu incidentov v oblasti bezpečnosti informácií, ako napríklad kybernetické útoky alebo úniky údajov, by mohli ohroziť údaje a databázy najvyššieho štátneho významu. V rámci auditu sa preto skúmalo, ako štát určuje, ktoré údaje a databázy sú kľúčové na zaistenie národnej bezpečnosti. Pri audite sa dospelo k záveru, že napriek vykonávaniu trojúrovňového základného bezpečnostného systému ISKE[63], ktorý je

[63] ISKE je norma informačnej bezpečnosti, ktorá je vypracovaná pre estónsky verejný sektor; je povinná pre štátne a miestne vládne organizácie, ktoré spracúvajú databázy/registre.

povinný pre štátne agentúry, existujú výrazné nedostatky v zaisťovaní bezpečnosti informácií vo viacerých kritických databázach.

58 **Írsky Úrad kontrolóra a generálneho audítora** (***Office of the Comptroller and Auditor General)*** skúmal pokrok dosiahnutý v súvislosti s kybernetickobezpečnostnými opatreniami od zriadenia Írskeho národného centra pre kybernetickú bezpečnosť. Centrum, ktoré prevádzkuje Ministerstvo komunikácií, opatrení v oblasti klímy a životného prostredia, bolo zriadené v roku 2011. Jeho primárnym zameraním je zabezpečenie sietí verejnej správy, pomoc priemyslu a súkromným osobám pri ochrane ich vlastných systémov a zabezpečovanie kritickej vnútroštátnej infraštruktúry. Záverom auditu bolo, že hoci Národné centrum pre kybernetickú bezpečnosť vykonáva kľúčovú úlohu, úroveň zabezpečovania zdrojov za prvé štyri roky jeho fungovania bola výrazne nižšia, ako sa pôvodne plánovalo, a celkovému strategickému riadeniu centra chýba strategický plán. Ďalej sú potrebné jasnejšie informácie v súvislosti s príslušnými úlohami orgánov zapojených do vyšetrovania počítačovej kriminality a incidentov v oblasti národnej bezpečnosti. Okrem toho sa požiadavky smernice EÚ o sieťovej a informačnej bezpečnosti týkajúce sa vypracovania národnej stratégie ešte len majú vykonať.

59 **Francúzsky** účtovný **dvor** ***(Cour des comptes)*** skúmal novú digitálnu platformu s názvom *Parcoursup* fungujúcu ako zdroj informácií o dostupných univerzitných študijných programoch a podmienkach prijatia, ktorej cieľom je posilniť prepájanie schopností a akademických výsledkov stredoškolských žiakov a obsah kurzov terciárneho vzdelávania. Z auditu vyplynulo, že vláda úspešne centralizovala prístup k celému postsekundárnemu vzdelávaniu prostredníctvom digitálnej platformy s cieľom zvládnuť rozšírenie vysokoškolského vzdelávania. Nová platforma *Parcoursup* však vznikla rýchlym prepracovaním predchádzajúceho systému bez podstatných štrukturálnych zmien. Nenapravili sa tak nedostatky informačného systému, pokiaľ ide o bezpečnosť, výkonnosť a spoľahlivosť. Platforme stále hrozia závažné riziká v súvislosti s kvalitou a kontinuitou poskytovania verejnej služby a bezpečnosťou osobných údajov.

60 **Lotyšský vnútroštátny kontrolný úrad** ***(Valsts Kontrole***) vykonal audit výkonnosti zameraný na efektívnosť verejnej infraštruktúry informačných a komunikačných technológií (IKT). Cieľom auditu bolo overiť, či verejná správa jednotne pristupuje k efektívnemu riadeniu infraštruktúry IKT a či inštitúcie posúdili prínosy centralizácie. Z auditu vyplynulo, že neochota orgánov riadiť infraštruktúru IKT centrálne viedla

k tomu, že vzniklo viacero serverovní, čím sa značne zvýšili náklady na údržbu. Vo väčšine serverovní boli prítomné bezpečnostné hrozby, pričom dátové centrá neboli dostatočne chránené pred fyzickým prístupom a environmentálnymi rizikami. Okrem toho nemali inštitúcie zavedený žiadny postup na vykonávanie pravidelných hodnotení toho, či by nebolo lacnejšie spravovať infraštruktúru IKT interne, spolupracovať s inou inštitúciou alebo zabezpečovať údržbu IKT externe. V rámci auditu sa odporučil pravidelný monitorovací systém, ktorý by umožnil hodnotiť celú verejnú správu ako jeden systém.

61 **Litovský vnútroštátny kontrolný úrad** (***Valstybės kontrolė)*** uznal dôležitosť vykonávania kritických elektronických štátnych informačných zdrojov, ako je riadenie verejných financií, daňová správa a zdravotná starostlivosť. Strata kritických informácií a nedostupnosť príslušných informačných systémov by mohli mať vážne dôsledky pre verejnú bezpečnosť, kvalitu života a hospodárstvo. Cieľom auditu bolo zhodnotiť riadenie (všeobecnú kontrolu) a vyspelosť kritických štátnych informačných zdrojov. Odhalil systémové problémy v tvorbe a vo vykonávaní politiky v oblasti štátnych informačných zdrojov a v systémoch ich riadenia. Záverom auditu bolo, že nízka úroveň vyspelosti kritických štátnych informačných zdrojov poukazuje na slabé miesta v tvorbe a vo vykonávaní politiky v oblasti štátnych informačných zdrojov, v dôsledku čoho sú tieto zdroje zraniteľnejšie. Systémy riadenia sa musia zlepšiť, aby sa zvýšila bezpečnosť štátnych informačných zdrojov.

62 **Holandský *Dvor audítorov*** sa v roku 2018 rozhodol vykonať audity kybernetickej bezpečnosti v sektoroch, ktoré sú pre spoločnosť kľúčové. Prvými dvomi kontrolovanými sektormi boli vodné hospodárstvo, ktoré je kľúčové pre krajinu vo veľkej miere pod hladinou mora, a automatizovaný systém hraničnej kontroly, ktorý je pre ňu kľúčový vzhľadom na polohu letiska Amsterdam Schiphol ako medzinárodného centra a brány do krajiny. Ministerstvo infraštruktúry a vodného hospodárstva označilo niekoľko vodných diel spravovaných Generálnym riaditeľstvom pre verejné práce a vodné hospodárstvo (auditovaný subjekt) ako „kritické súčasti“ sektora vodného hospodárstva. Mnohé počítačové systémy používané na prevádzku kritických vodných diel pochádzajú z 80. a 90. rokov 20. storočia – z čias, keď sa kybernetická bezpečnosť bežne nezohľadňovala. Minister obrany a minister spravodlivosti a bezpečnosti spoločne zodpovedajú za hraničné kontroly, ktoré vykonáva holandská pohraničná stráž na letisku Schiphol. Obe ministerstvá vlastnia systémy IT, o ktoré sa opiera hraničná stráž. Systémy sú kritické pre letiskové operácie a používajú sa na spracovanie vysoko citlivých údajov. V dôsledku toho sú zaujímavým

terčom kybernetických útokov, ktorých cieľom je sabotáž, špionáž alebo manipulácia hraničných kontrol. V rámci auditu sa skúmalo, či sú kontrolované orgány pripravené na riešenie kybernetických hrozieb a či ich riešia účinne. V prípade vodných diel musel kontrolovaný subjekt vyvinúť ďalšie snahy, pokiaľ ide o odhaľovanie a reakciu, aby splnil svoje vlastné kybernetickobezpečnostné ciele. Pokiaľ ide o kontroly hraníc, zistilo sa, že opatrenia v oblasti kybernetickej bezpečnosti nie sú ani dostatočné, ani nadčasové.

63 **Portugalský dvor audítorov *Tribunal de Contas*** vykonal audit informačných systémov, ktoré podporujú udeľovanie, vydávanie a používanie portugalského elektronického pasu (PEP), a to najmä pri automatizovanom preverovaní pasažierov načítaním biometrických údajov na portugalských hraniciach. Pri audite sa preveril súlad s právom EÚ a vnútroštátnym právom, medzinárodnými normami a usmerneniami pre udeľovanie, vydávanie a používanie PEP vrátane primeranosti vnútroštátneho právneho rámca. Skúmal účinnosť kľúčových procesov súvisiacich so životným cyklom PEP, najmä procesov spojených s udeľovaním, vydávaním a používaním PEP. Počas auditu sa takisto skúmali kritické stránky výkonnosti informačných systémov, a to najmä spĺňanie bezpečnostných požiadaviek týkajúcich sa informačných systémov PEP (SIPEP).

64 **Fínsky vnútroštátny kontrolný úrad (*Valtiontalouden tarkastusvirasto)*** skúmal, či je kybernetická ochrana v ústrednej štátnej správe účinná a nákladovo efektívna v čo najväčšej miere. Audit bol zameraný na to, akým spôsobom sa riadi kybernetická bezpečnosť v ústrednej štátnej správe. Kontrolované subjekty zahŕňali orgány riadiace kybernetickú ochranu v ústrednej štátnej správe (kancelária premiéra, ministerstvo financií a ministerstvo dopravy a komunikácií) a orgány zodpovedné za centralizované úlohy v oblasti kybernetickej ochrany a centralizované IT služby v ústrednej štátnej správe. Vo fínskej štátnej správe je zodpovednosť za kybernetickú ochranu decentralizovaná, pričom každý orgán inštitúcie zodpovedá za svoju vlastnú kybernetickú bezpečnosť. V rámci auditu sa odporučilo, aby ministerstvo financií stanovilo a vykonávalo rozsiahly model operačného riadenia v prípade kybernetickobezpečnostných incidentov v rámci služieb IKT ústrednej štátnej správy. Ministerstvo financií by takisto malo zistiť, ako riešiť kybernetickú bezpečnosť služieb, pokiaľ ide o financovanie služieb počas ich celého životného cyklu, a zlepšiť operatívnu situačnú informovanosť tým, že orgánom nariadi, aby porušenia kybernetických zásad nahlasovali Centru pre kybernetickú bezpečnosť.

65 **Švédsky** vnútroštátny kontrolný úrad ***Riksrevisionen*** sa zaoberal výskytom zastaralých systémov IT v ústrednej štátnej správe s cieľom posúdiť, či štátna správa a orgány prijali vhodné opatrenia, aby zabránili tomu, že systémy IT budú prekážkou účinnej digitalizácie. Audit odhalil zastaralé systémy IT vo veľkom počte vládnych agentúr. V mnohých kontrolovaných agentúrach bol jeden alebo viac systémov IT kritických pre fungovanie zastaralý a veľká časť kontrolovaných agentúr nepristupovala správnym spôsobom k vývoju a správe podpory IT. Veľkej časti agentúr chýbal celkový opis toho, ako sú stratégie, operačné procesy a systémy prepojené. Celkovým záverom bolo, že väčšine agentúr sa zatiaľ nepodarilo účinne zvládať problémy spojené so zastaralými systémami IT. Podľa švédskeho kontrolného úradu je tento problém natoľko vážny a rozšírený, že predstavuje prekážku pre pokračujúcu efektívnu digitalizáciu štátnej správy.

Audity zhody vykonané v oblasti kybernetickej bezpečnosti

66 ***Štátny kontrolný úrad*** **Maďarska** uznal, že bezpečnosť národných dátových aktív je základným záujmom spoločnosti na zachovanie a ochranu národných hodnôt. Zabezpečenie zvýšenej bezpečnosti osobných a verejných údajov v rámci národných súborov údajov Maďarska je kľúčové pre posilnenie dôvery občanov v štát a zabezpečenie nepretržitého a bezproblémového fungovania verejnej správy. Účelom auditu zhody o ochrane údajov bolo posúdiť, či je v Maďarsku zavedený regulačný a operačný rámec pre ochranu údajov a či hlavné organizácie na správu údajov spĺňajú požiadavky bezpečnej správy údajov a externého zabezpečovania spracovania údajov. Záverom auditu bolo, že interné nariadenia organizácií pre správu údajov týkajúce sa činností v oblasti správy údajov zabezpečujú ochranu národných súborov údajov, ktoré sú súčasťou národných aktív, v súlade s právnymi ustanoveniami platnými v rokoch 2011 až 2015. Prevádzkovatelia riadne spĺňali požiadavky a prenos údajov tretím osobám sa vykonával náležitým spôsobom.

67 **Poľský** najvyšší kontrolný úrad ***Najwyższa Izba Kontroli*** posudzoval, či sú údaje zbierané v systémoch určených na vykonávanie dôležitých verejných úloh zabezpečené. Audit sa zaoberal šiestimi vybranými inštitúciami, ktoré plnia významné verejné úlohy. Stupeň prípravy vykonávania informačného bezpečnostného systému nezaisťoval prijateľnú úroveň bezpečnosti údajov zbieraných v systémoch IT používaných na vykonávanie dôležitých verejných úloh. Informačno-bezpečnostné procesy sa vykonávali neriadene a v dôsledku chýbajúcich postupov intuitívne. Zo

šiestich kontrolovaných útvarov mal len jeden zavedený informačný bezpečnostný systém. Je však potrebné poznamenať, že v tejto operácii sa takisto vyskytli závažné chyby. Záverom auditu bolo, že je potrebné vypracovať všeobecné odporúčania a požiadavky týkajúce sa bezpečnosti IT, ktoré budú uplatniteľné pre všetky verejné orgány, a vykonávať ich na ústrednej úrovni.

Preskúmania kybernetickej bezpečnosti

68 ***Európsky dvor audítorov*** preskúmal situáciu v oblasti politiky kybernetickej bezpečnosti EÚ a vymedzil hlavné prekážky pre jej účinnú realizáciu. Venoval sa sieťovej a informačnej bezpečnosti, počítačovej kriminalite, kybernetickej obrane a dezinformáciám. Preskúmanie odhalilo viaceré medzery v práve EÚ v oblasti kybernetickej bezpečnosti a poukázalo sa v ňom na to, že členské štáty netransponovali existujúce právne predpisy dôsledne. V preskúmaní sa napokon upozornilo na skutočnosť, že spoľahlivých údajov o kybernetických incidentoch na úrovni EÚ je nedostatok a chýba komplexný prehľad výdavkov EÚ a jej členských štátov na kybernetickú bezpečnosť. V preskúmaní sa takisto poukázalo na obmedzenia týkajúce sa zdrojov pre agentúry EÚ zaoberajúce sa oblasťou kybernetiky, ako aj ťažkosti pri lákaní talentov a ich udržaní. Druhá výzva súvisela s nesúladom financovania kybernetickej bezpečnosti a strategických cieľov EÚ.

ČASŤ III – Zhrnutie správ najvyšších kontrolných inštitúcií

Dánsko
Rigsrevisionen

Ochrana proti útokom ransomvéru

Dátum uverejnenia: 2017

Hypertextový odkaz na správu: Zhrnutie správy (anglická verzia)

Typ a obdobie auditu

Typ auditu: Audit výkonnosti

Kontrolované obdobie: apríl – september 2017

Zhrnutie správy

Téma auditu

V tejto správe sa skúmalo, či vybrané kľúčové správne inštitúcie majú dostatočnú ochranu pred ransomvérom.

Správne inštitúcie sú častými terčmi kybernetických útokov, pričom ransomvér je v súčasnosti jednou z najväčších hrozieb pre kybernetickú bezpečnosť. Ransomvér je škodlivý softvér, ktorý blokuje prístup k údajom. Vo všeobecnosti ransomvér šifruje údaje a bráni zasiahnutým inštitúciám v ich používaní. Hackeri žiadajú výkupné za odšifrovanie údajov a umožnenie inštitúciám znova získať prístup. Ransomvér tak predstavuje mimoriadnu hrozbu pre prístupnosť údajov.

Náhla neschopnosť dostať sa k údajom môže inštitúciám sťažiť poskytovanie dôležitých služieb alebo im brániť v ich poskytovaní v plnom rozsahu. Inštitúcie zasiahnuté útokom ransomvéru sú spravidla nútené odstaviť celú svoju sieť IT alebo jej časti, aby vyšetrili rozsah útoku. Útoky ransomvéru môžu mať vážne ekonomické dôsledky, keďže inštitúciám hrozí výpadok výroby, napríklad vtedy, ak im bránia v prístupe k ich sieti IT alebo ak dôjde k strate dlhodobo zbieraných a spracúvaných údajov. Útok ransomvéru na britský národný zdravotný systém v roku 2017 spôsobil zrušenie 19 000 operácií a vyšetrení. Vedenie inštitúcií by sa preto malo zamerať na riziko útokov

ransomvéru a zaviesť potrebné bezpečnostné kontroly na ochranu pred ransomvérom a zmiernenie dôsledkov potenciálneho útoku.

Štúdia zahŕňala dánsky Úrad pre zdravotné údaje, ministerstvo zahraničných vecí, spoločnosť Banedanmark (dánska železničná sieť) a dánsku Agentúru pre riadenie núdzových situácií. Tieto štyri inštitúcie boli vybrané preto, lebo zodpovedajú za poskytovanie základných služieb v oblasti zdravia, zahraničných vecí, dopravy a pripravenosti na núdzové situácie, v ktorých môže mať prístup k údajom kľúčový význam. Úrad pre zdravotné údaje takisto poskytuje centralizované služby IT väčšine orgánov verejnej správy patriacich pod ministerstvo zdravotníctva.

Cieľom štúdie bolo posúdiť, či majú tieto štyri inštitúcie dostatočnú ochranu pred útokmi ransomvéru prostredníctvom elektronickej pošty. Kontrolný úrad *Rigsrevisionen* preto skúmal 20 bežných bezpečnostných kontrol, ktoré poskytujú základnú ochranu pred ransomvérom. Okrem toho NKI preskúmala päť bezpečnostných kontrol, ktoré by mali inštitúcie zvážiť v súvislosti s budúcimi hodnoteniami rizika. Výhľadové kontroly zahŕňajú napríklad novú technológiu, ktorá môže znížiť počet falošných e-mailov doručených do inštitúcie alebo odhaľovať a zasielať upozornenia týkajúce sa nezvyčajnej aktivity na počítačoch. Štúdiu inicioval kontrolný úrad *Rigsrevisionen*, pričom vychádzala zo zistení štyroch auditov vykonaných od apríla do septembra 2017. Štúdia podáva obraz o tom, ako dobre boli inštitúcie chránené pred ransomvérom. Po ukončení auditov IT mali inštitúcie možnosť zaviesť 20 bežných bezpečnostných kontrol. Výsledky štúdie sa preto týkajú ochrany inštitúcií pred ransomvérom len v čase výkonu týchto štyroch auditov. Štúdia poskytuje pohľad na výkonnosť štyroch inštitúcií, ale nezahŕňa komparatívnu analýzu ani poradie ich výkonnosti.

Zistenia a závery

Podľa posudku kontrolného úradu *Rigsrevisionen* tieto štyri inštitúcie nemali dostatočnú ochranu pred ransomvérom. Zo štúdie vyplýva, že štyri inštitúcie nemali zavedené viaceré bežné bezpečnostné kontroly na zmiernenie následkov útokov. Značné nedostatky v bezpečnosti sa zistili najmä v prípade Úradu pre zdravotné údaje a spoločnosti Banedanmark. Znamená to, že všetky štyri inštitúcie boli vystavené zvýšenému riziku útokov ransomvéru prostredníctvom elektronickej pošty, v dôsledku ktorých by rôznu dobu neboli schopné poskytovať svoje služby. Od dokončenia štúdie všetky štyri inštitúcie informovali kontrolný úrad *Rigsrevisionen*, že pracujú na zavádzaní viacerých bezpečnostných kontrol, aby zvýšili úroveň ochrany pred ransomvérom.

Ochrana inštitúcií pred útokmi ransomvéru, pokiaľ ide o vnútorné aj vonkajšie hrozby, nebola primeraná. Mimoriadne znepokojujúca je skutočnosť, že žiadna z inštitúcií nezabezpečila, aby boli bezpečnostné softvérové záplaty aktuálne, a že tri z nich nemali zavedený whitelisting, aby zabránili zamestnancom spúšťať škodlivý softvér. Tým sa zvyšuje riziko, že ransomvér nakazí celú sieť IT alebo jej časť a bude sa šíriť.

V troch inštitúciách sa vedenie nezameriavalo na ohrozenie ransomvérom dostatočne a posúdenia rizika vykonané Úradom pre zdravotné údaje a spoločnosťou Banedanmark sa nevenovali všetkým relevantným aspektom. Znamená to, že inštitúcie nemali aktuálne hodnotenie ohrozenia ransomvérom, a preto boli v slabej pozícii na to, aby zabránili novým útokom a zmiernili dôsledky budúcich útokov. Vedenie Úradu pre zdravotné údaje a spoločnosť Banedanmark sa nezameriavali na posúdenie rizika dostatočne, a preto bezpečnosť IT v týchto dvoch inštitúciách nevychádzala z priorít stanovených vedením.

Tri z inštitúcií nemali zavedené primerané plány reakcie na incidenty, ktoré by im pomohli obnoviť svoju činnosť po útoku ransomvérom. Mimoriadne závažné je to, že tri z inštitúcií pravidelne netestovali, či by boli schopné obnoviť údaje a systémy zasiahnuté útokom ransomvéru. Tým sa zvyšuje riziko, že údaje, ktorými disponujú tieto inštitúcie, sa v dôsledku útoku ransomvéru stratia, a že inštitúcie nebudú dlhodobo schopné poskytovať svoje služby.

Keďže rizikové scenáre sa neustále menia, je dôležité, aby inštitúcie zvážili zavedenie výhľadových bezpečnostných kontrol, aby zvýšili svoju odolnosť voči útokom ransomvéru, napr. kontrol, ktoré umožňujú overenie totožnosti odosielateľov e-mailov a dokážu odhaľovať a vyfiltrovať potenciálne škodlivé e-maily. Všetky štyri inštitúcie v súčasnosti pracujú na viacerých výhľadových bezpečnostných kontrolách, ktoré môžu pomôcť zvýšiť ich ochranu pred útokmi ransomvéru.

Ďalšie správy v tejto oblasti

Názov správy:	Správa o ochrane výskumných údajov na dánskych univerzitách
Hypertextový odkaz na správu:	Zhrnutie správy (anglická verzia)
Dátum uverejnenia:	2019

Názov správy:	Správa o ochrane systémov IT a zdravotných údajov v troch dánskych regiónoch
Hypertextový odkaz na správu:	Zhrnutie správy (anglická verzia)
Dátum uverejnenia:	2017

Názov správy:	Správa o riadení bezpečnosti IT v systémoch zverených externým dodávateľom
Hypertextový odkaz na správu:	Zhrnutie správy (anglická verzia)
Dátum uverejnenia:	2016

Názov správy:	Správa o prístupe do systémov IT, ktoré podporujú poskytovanie základných služieb dánskej spoločnosti
Hypertextový odkaz na správu:	Zhrnutie správy (anglická verzia)
Dátum uverejnenia:	2015

Estónsko
Riigikontroll

Zaistenie bezpečnosti a ochrany kritických štátnych databáz v Estónsku

Dátum uverejnenia: máj 2018

Hypertextový odkaz na správu: Zhrnutie správy (anglická verzia)
Správa (estónska verzia)

Typ a obdobie auditu

Typ auditu: Audit výkonnosti

Kontrolované obdobie: 2017

Zhrnutie správy

Téma auditu

Zachovanie estónskej nezávislosti si vyžaduje nielen fyzickú obranu územia, ale aj ochranu digitálnych aktív najvyššieho štátneho významu, pokiaľ ide o udalosti predstavujúce najväčšiu hrozbu. Digitálne aktíva, ktoré si vyžadujú najväčšiu ochranu, sú údaje týkajúce sa občanov, územia a právnych predpisov. Takisto je potrebné zabezpečiť údaje týkajúce sa majetku, nehnuteľností a práv osôb s pobytom v Estónsku.

Národný kontrolný úrad skúmal to, akým spôsobom štát určoval, ktoré údaje a databázy sú kľúčové na zaistenie národnej bezpečnosti. Kontrolovala sa ochrana bezpečnosti a kontinuity týchto údajov a databáz vrátane prehľadu nástrojov používaných na ochranu.

Keďže Estónsko je už členom NATO a Európskej únie, jeho fyzická bezpečnosť je zaručená lepšie než pred pristúpením do týchto sietí. Estónsko však musí preskúmať možnosť kybernetických hrozieb v prípade eskalácie bezpečnostných problémov. Takéto rizikové scenáre a nárast počtu incidentov v oblasti bezpečnosti informácií, ako napríklad kybernetické útoky alebo úniky údajov, by takisto mohli ohroziť údaje

a databázy, ktoré sú pre štát najdôležitejšie. Ak by sa údaje najvyššieho štátneho významu zmenili bez oprávnenia, unikli by alebo stratili sa, štát by už nebol schopný vykonávať potrebné funkcie vrátane zaistenia bezpečnosti občanov, zabezpečovania základných potrieb, vytvárania vhodných podmienok na podnikanie a mnohých ďalších. Estónsko pôvodne plánuje vynaložiť na ukladanie kritických dát v zahraničí približne jeden milión EUR.

Audítorské otázky

- Identifikovali ministerstvá všetky kritické databázy a požiadavky na manipuláciu?
- Sú kritické databázy a registre zabezpečené?
- Je zaistená dlhodobá kontinuita kritických údajov a databáz?

Zistenia

Národný kontrolný úrad vydal tieto pripomienky týkajúce sa kontrolovaných kritických databáz:

- Nebol vypracovaný žiadny akčný plán ani požiadavky na vykonávanie koncepcie kritických databáz. Neboli stanovené podmienky výberu kritických databáz a nebolo isté, že v procese sú zahrnuté všetky potrebné databázy. Dodatočná ochrana databáz bola riadená neformálne a pre vlastníkov databáz nebola povinná, v dôsledku čoho neboli údaje piatich kritických databáz zálohované v zahraničí.
- Neboli zavedené žiadne dodatočné pravidlá informačnej bezpečnosti pre kritické databázy. Systém informačnej bezpečnosti ISKE (norma informačnej bezpečnosti vyvinutá pre estónsky verejný sektor povinná pre štátne a miestne organizácie verejnej správy, ktoré pracujú s databázami/registrami) ani žiadny právny akt alebo norma nezahŕňali dodatočné požiadavky na kritické databázy, ako napríklad zálohovanie údajov mimo Estónska. Zálohové kópie kontrolovaných databáz sa presunuli do zahraničia, ale obnova fungovania informačných systémov pomocou nich sa neodskúšala.
- Vykonávanie ISKE a vykonávanie súvisiacich auditov predstavovalo v súvislosti s kritickými databázami problém. V čase auditu neboli vykonané žiadne audity ISKE v prípade dvoch z desiatich databáz, pričom audity sa uskutočnili až pred ukončením tohto auditu (30. novembra 2017). Len v prípade dvoch kritických

databáz sa audit vykonával tak často, ako vyžaduje zákon. Takisto sa vyskytli prípady, kedy sa problémy, na ktoré upozornil audítor, počas obdobia medzi dvomi auditmi ISKE (dva až tri roky) nevyriešili.

- Počas auditu národný kontrolný úrad zistil, že v prípade niekoľkých kritických databáz neboli zavedené viaceré dôležité informačno-bezpečnostné opatrenia. Napríklad v usmerneniach pre informačnú bezpečnosť neboli stanovené požiadavky pravidelného posudzovania nedostatkov informačných systémov, nevykonávali sa pravidelné kontroly ani analýzy protokolov udalostí, neexistovali plány školení v oblasti informačnej bezpečnosti alebo analýza informovanosti o informačnej bezpečnosti v oblasti verejnej správy, ktorá je základom takýchto plánov školení, integrita súborov sa v niektorých prípadoch nekontrovala a nevykonali sa žiadne skúšky prieniku.

Závery a odporúčania

Z auditu vyplynulo, že napriek vykonávaniu trojúrovňového základného bezpečnostného systému ISKE, ktorého používanie je pre štátne agentúry a ich audity povinné, existujú výrazné nedostatky v zaisťovaní bezpečnosti informácií vo viacerých kritických databázach, ako je analýza protokolov, skúšanie prieniku a ochrana mobilných zariadení. Zatiaľ neboli stanovené osobitné požiadavky na ochranu kritických údajov.

Ministerstvo hospodárstva a komunikácie už začalo prvé činnosti potrebné na ochranu kritických údajov, ale projekt kritických databáz bol v štádiu, v ktorom by si vyžadoval právne záväzný súbor pravidiel. Neexistovala ani podrobná analýza rizík ani akčný plán do budúcnosti.

Zálohové kópie piatich kritických databáz boli uložené na veľvyslanectvách v iných krajinách, ale v prípade fyzického zničenia dátových centier nachádzajúcich sa v Estónsku by nebola zaistená ochrana kritických údajov zo zvyšných piatich databáz.

Vydali sa dve všeobecné odporúčania:

- stanoviť pravidlá pre dodatočnú ochranu kritických databáz vrátane výberu kritických databáz, spracúvania údajov v týchto databázach a zálohovania údajov, ktoré sú pre štát kritické, a posúdiť, ako zabezpečiť dodatočné financovanie týchto činností,

- vykonať analýzu rôznych štádií zriaďovania databáz, pokiaľ ide o finančné plánovanie aj informačnú bezpečnosť, a využívať pri implementácii týchto štádií najlepšie postupy z oblasti projektového riadenia.

Írsko
Office of the Comptroller and Auditor General

Opatrenia súvisiace s národnou kybernetickou bezpečnosťou

Dátum uverejnenia: september 2018

Hypertextový odkaz na správu: Zhrnutie správy (anglická verzia)

Typ a obdobie auditu

Typ auditu: Audit výkonnosti

Kontrolované obdobie: 2011 – 2018

Zhrnutie správy

Téma auditu

Za politiku kybernetickej bezpečnosti v Írsku zodpovedá Ministerstvo komunikácii, opatrení v oblasti klímy a životného prostredia. Prostredníctvom Národného centra pre kybernetickú bezpečnosť ministerstvo takisto zodpovedá za koordináciu reakcie verejnej správy na akékoľvek kybernetickobezpečnostné incidenty.

Národné centrum pre kybernetickú bezpečnosť bolo zriadené v roku 2011. Jeho primárnym zameraním je zabezpečenie sietí verejnej správy, pomoc priemyslu a súkromným osobám pri ochrane ich vlastných systémov a zabezpečovanie kritickej vnútroštátnej infraštruktúry.

Audítorské otázky

Toto preskúmanie je zamerané na pokrok dosiahnutý v súvislosti s kybernetickobezpečnostnými opatreniami od zriadenia Národného centra pre kybernetickú bezpečnosť. Skúma najmä otázky týkajúce sa:

- mandátu a zabezpečovania zdrojov pre centrum,

- národnej stratégie kybernetickej bezpečnosti (2015 – 2017),
- vykonávania smernice EÚ o sieťovej a informačnej bezpečnosti,
- mechanizmov správy a riadenia a dohľadu.

Zistenia a závery

Hoci sa v rozhodnutí vlády o zriadení Národného centra pre kybernetickú bezpečnosť schválilo financovanie vo výške 800 000 EUR ročne, skutočné ročné financovanie kybernetickej bezpečnosti predstavovalo v rokoch 2012 až 2015 menej ako tretinu tejto sumy. V roku 2017 sa zvýšili pridelené prostriedky na 1,95 mil. EUR. V tomto roku sa počet zamestnancov centra takmer zdvojnásobil na 14,5 ekvivalentu plného pracovného času. V roku 2018 sa schválilo prijatie ďalších 16 zamestnancov.

Národná stratégia kybernetickej bezpečnosti (2015 – 2017) obsahovala 12 opatrení, ktoré sa mali dosiahnuť počas jej trvania. K máju 2018 boli štyri opatrenia ukončené, štyri boli čiastočne vykonané a štyri neboli vykonané.

Cieľom smernice EÚ o sieťovej a informačnej bezpečnosti je zlepšiť odolnosť kľúčových sieťových a informačných systémov. Z posúdenia postupu v Írsku v súvislosti s tromi piliermi smernice vyplynulo, že:

- *Pilier 1 – zlepšenie spôsobilostí členských štátov EÚ v oblasti kybernetickej bezpečnosti.* Čiastočne vykonané – riešili sa štruktúrne požiadavky, ale pretrvávajú medzery v strategickom plánovaní.
- *Pilier 2 – uľahčenie spolupráce členských štátov EÚ v oblasti kybernetickej bezpečnosti.* Vykonané.
- *Pilier 3 – zavedenie bezpečnostných opatrení a povinnosti oznamovania incidentov pre kľúčové sektory.* Čiastočne vykonané – vyžaduje sa ďalšia práca v súvislosti s identifikáciou kritických sieťových a informačných systémov, formálnym označením subjektov ako prevádzkovateľov základných služieb a riadením poskytovateľov digitálnych služieb.

V rozhodnutí vlády (z júla 2011), ktorým sa schválilo zriadenie Národného centra pre kybernetickú bezpečnosť, sa takisto schválilo zriadenie medzirezortného výboru, ktorý bude stanovovať a vykonávať politiku na riešenie výziev v oblasti kybernetickej bezpečnosti v Írsku. Hoci v rokoch 2013 až 2015 skupina zasadala päťkrát,

na preskúmanie bola k dispozícii zápisnica len z jedného zasadnutia. Výbor nezasadal od roku 2015.

Plán vykonávania národnej stratégie kybernetickej bezpečnosti obsahuje záväzok uverejniť výročnú správu a vykonať formálne posúdenie vplyvu činnosti výboru koncom roka 2017. Výročná správa ani posúdenie vplyvu nie sú vypracované, hoci je činnosť centra načrtnutá vo výročnej správe ministerstva.

Ministerstvo formálne požiadalo o posúdenie výkonnosti centra. Neboli predložené žiadne dôkazy o tom, že sa posúdenie vykonalo. Ministerstvo sa vyjadrilo, že posúdenie výkonnosti práce Národného centra pre kybernetickú bezpečnosť tvorí súčasť bežného riadenia výkonnosti a podnikovej správy ministerstva.

Záverom auditu bolo, že:

- hoci Národné centrum pre kybernetickú bezpečnosť vykonáva kľúčovú úlohu, úroveň zabezpečovania zdrojov za prvé štyri roky jeho fungovania bola výrazne nižšia, ako sa pôvodne plánovalo,
- celkové strategické riadenie centra nie je prehľadné a v súčasnosti nie je zavedený žiadny strategický plán,
- sú potrebné jasnejšie informácie v súvislosti s príslušnými úlohami orgánov zapojených do vyšetrovania počítačovej kriminality a incidentov v oblasti národnej bezpečnosti,
- požiadavky smernice EÚ o sieťovej a informačnej bezpečnosti týkajúce sa vypracovania národnej stratégie sa ešte len majú vykonať,
- hoci boli stanovené správne štruktúry, nie je jasné, ako mechanizmy správy a riadenia fungujú v praxi.

Chýba transparentnosť, pokiaľ ide o dostupnosť a výšku zdrojov určených na kybernetickú bezpečnosť.

Francúzsko
Cour des comptes

Prístup k vysokoškolskému vzdelávaniu: prvotný posudok zákona o študijnom poradenstve a úspechu študentov

Dátum uverejnenia: február 2020

Hypertextový odkaz na správu: Správa (francúzska verzia)

Typ a obdobie auditu

Typ auditu: Audit výkonnosti

Kontrolované obdobie: 2019 – 2020

Zhrnutie správy

Téma auditu

Cieľom zákona o študijnom poradenstve a úspechu študentov (*loi relative à l'orientation et à la réussite des étudiants*, ORE) z roku 2018 bolo zlepšiť tri hlavné štádiá na ceste mladých ľudí za vysokoškolským vzdelaním: poradenstvo a podporu študentov vo vyššom sekundárnom vzdelávaní, výber študijného programu a úspech v prvých rokoch štúdia. Zákonom sa zaviedla nová digitálna platforma s názvom *Parcoursup* fungujúca ako zdroj informácií o dostupných študijných programoch a podmienkach prijatia, ktorej cieľom bolo posilniť prepájanie schopností a výsledkov stredoškolských žiakov a obsah programov terciárneho vzdelávania.

Počas prvých dvoch rokov od prijatia zákona ORE bol podniknutý prvý krok k transformácii prístupu k vysokoškolskému vzdelávaniu. Napriek početným obmedzeniam prebehlo spustenie platformy *Parcoursup* veľmi hladko, hoci jej stále chýbali zábezpeky bezpečnosti a udržateľnosti a údaje sa mohli vzhľadom na ich dôležitosť využívať lepšie.

Zákon ORE bol prijatý s cieľom vyriešiť dva hlavné problémy vo vzdelávacej politike. Prvým bola vysoká miera predčasného ukončenia štúdia u vysokoškolských študentov.

Druhým bolo, že stará digitálna platforma vyvolávala hlboko zakorenenú nespokojnosť, pretože vo svojom záverečnom štádiu využívala náhodný výber.

Na reformu ORE boli pridelené finančné prostriedky vo výške 867 mil. EUR na obdobie piatich rokov. Zakladala sa na myšlienke kontinua „-3/+3“, pričom základným princípom bolo, že čím viac stredoškolskí žiaci vedia o obsahu študijných programov terciárneho vzdelávania, tým väčšiu šancu na úspech na skúškach budú mať, keďže si vyberú študijné programy, ktoré najlepšie zodpovedajú ich schopnostiam a ambíciám. Cieľom ORE bolo prekonať nedostatok poradenstva dostupného pre stredoškolských žiakov, a tak obmedziť prechádzanie na iné študijné programy, ktoré podľa odhadov dvora len za prvý rok vysokoškolského vzdelávania stojí takmer 550 mil. EUR ročne.

Audítori vykonali prvotný posudok prístupu k vysokoškolskému vzdelávaniu v kontexte ORE, pričom skúmali otázky bezpečnosti IT vyplývajúce z platformy.

Informačný systém charakterizovalo rozšírenie koeficientov zaťaženia (zahrnutie všetkých vysokoškolských študijných programov v roku 2020 a prudký nárast počtu používateľov v priebehu len niekoľkých rokov). To sa odrazilo na náhlom prechode z predchádzajúcej platformy na platformu *Parcoursup* bez toho, aby sa zmenila architektúra, čím vzniklo závažné riziko v súvislosti s kvalitou, kontinuitou, prispôsobiteľnosťou a ďalším vývojom služby. Neopravili sa nedostatky systému, pokiaľ ide o bezpečnosť, výkonnosť a spoľahlivosť. Platformu *Parcoursup* bolo možné vytvoriť rýchlo, pretože ju v režime beta spravovala malá skupina vysoko kvalifikovaných a motivovaných osôb, ale tento prístup znamenal, že postupu chýbalo strategické riadenie a dostatočná správa.

Audítori posudzovali kvalitu informačného systému a výkonnosť novej platformy *Parcoursup*. Platforma *Parcoursup* bola zriadená zákonom ORE s cieľom zlepšiť kvalitu priraďovania k vysokoškolským študijným programom, a tým zvýšiť mieru osôb s absolvovaným vzdelaním.

Zistenia

Hoci platforma *Parcoursup* fungovala uspokojivo, bola vystavená rizikám IT, ktoré bolo potrebné znížiť. Boli potrebné zábezpeky bezpečnosti a udržateľnosti platformy a údaje sa mohli lepšie využívať.

Starý informačný systém

Platforma *Parcoursup* obsahovala len málo noviniek, pričom od predchádzajúcej platformy s názvom *Admission Post-Bac* (APB) zdedila nepraktickosť a labilnosť spolu s mnohými nevyriešenými rizikami. Informačný systém, ktorý tvoril štrukturálny základ platformy *Parcoursup*, bol prevzatý priamo z predchádzajúcej platformy. Napriek tomu, že informačný systém bol vnucovaný ako nový nástroj na priraďovanie, jadro informačného systému sa od APB zmenilo len nepatrne. V skutočnosti bolo viac ako 72 % informačnej infraštruktúry nezmenených, pričom sa prepísalo o niečo menej ako 30 % kódu APB.

Základy IT platformy boli začiatkom 21. tisícročia navrhnuté tak, aby každoročne zvládali približne jeden milión žiadostí z približne 100 000 miest, ale rozsah informačného systému sa rozšíril, aby zvládal ročný prílev približne 10 miliónov žiadostí z približne jedného milióna miest. Platforma *Parcoursup* pôsobila ako starý nástroj s novým názvom. Zvýšenie záťaže vyvolalo otázky súvisiace s kapacitou platformy plniť svoj zamýšľaný účel.

Slabo zdokumentovaný informačný systém

Napriek snahám ministerstva o transparentnosť bol zdrojový kód platformy *Parcoursup* z 99 % stále uzavretý. To málo, čo sa zverejnilo, malo len malý význam pre pochopenie, posudzovanie a hodnotenie procesu priraďovania žiadateľov k študijným programom.

Podobne ako jeho predchodca bol aj *Parcoursup* slabo zdokumentovaným operačným informačným systémom. Výsledky auditu kódu naznačovali, že aplikácia mala nízku kvalitu a sprevádzalo ju vysoké riziko, pričom audit odhalil početné kritické porušenia. Systém mal nižšiu kvalitu než iný softvér podobného veku a hrozilo vysoké riziko zrútenia.

Platforma *Parcoursup* používala verejný aj uzavretý kód. V prípade otvoreného kódu bola miera kritických porušení oveľa vyššia ako v prípade uzavretého kódu, čo znamená, že hrozilo prerušenie služby. Platforma takisto nebola zabezpečená proti hackerom (bezpečnostný audit zdrojového kódu z júla 2018). Koncom roka 2019 však ministerstvo oznámilo, že sa začal proces certifikácie kódu platformy *Parcoursup*.

Existujúca dokumentácia zdrojového kódu nebola ani súvislá, ani úplná. Kód platformy *Parcoursup* bol abnormálne zložitý. Audítori vyjadrili názor, že zdrojový kód by sa mal reštrukturalizovať, aby sa znížil počet zložitých komponentov.

Architektúra informačného systému *Parcoursup* bola vysoko riziková; databáza sa spravovala zastaralým spôsobom – manuálne. Labilnosť systému spočívala v jeho veľkej závislosti od dostupnosti a ostražitosti prevádzkovateľa. Ministerstvo uznalo, že s architektúrou platformy *Parcoursup* sú spojené veľké riziká a že bez ďalšieho vývoja aplikácie ich nemožno opraviť.

Informačný systém *Parcoursup* bol slabo zdokumentovaný a v podstate závisel od odbornosti zamestnancov národnej vládnej agentúry (*Service à Compétence Nationale,* SCN). Pokiaľ ide o dokumentáciu, poznámky boli zapísané do databázy v jadre systému, v dôsledku čoho bolo ťažké udržiavať a vyvíjať informačný systém a využívať údaje. Bez hĺbkového preskúmania nebolo možné jednoducho získať a vyhodnotiť používateľské informácie uložené na platforme. Vzhľadom na nedostatok štruktúrovanej technickej dokumentácie závisela schopnosť SCN vykonávať svoje strategické úlohy výlučne na riaditeľovi centra IT.

Bezpečnostná stratégia – potrebné zlepšenia

Vzhľadom na citlivosť osobných údajov obsiahnutých v systéme predstavuje platforma *Parcoursup* skutočnú bezpečnostnú výzvu. Všetky organizácie spravujúce informačný systém musia mať spravidla formálnu písomnú politiku v oblasti bezpečnosti informačných systémov (ISSP). Napriek tomu, že predseda vlády označil platformu *Parcoursup* za kľúčového poskytovateľa služieb, nemala žiadnu ISSP. Vyžadovali sa okamžité kroky na jej zavedenie.

Každý tím platformy *Parcoursup* mal jedného pracovníka pre bezpečnosť informačných systémov (ISSO) priradeného k centru IT. Osvedčeným postupom by bolo priradiť pracovníkov ISSO priamo k riaditeľovi SCN, aby sa zaručila ich nezávislosť.

V polovici roka 2019 sa stále pracovalo na dosiahnutí súladu platformy *Parcoursup* so smernicou GDPR. Niektoré opatrenia ešte neboli prijaté, a to najmä potreba formálne ustanoviť rôzne procesy používané na spracovanie. Bezpečnosť osobných údajov bola naďalej nedostatočná a stále sa ukladalo priveľa podrobných individuálnych údajov.

Útvar platformy *Parcoursup* podával správy projektovému manažérovi platformy *Parcoursup* pridelenému z kancelárie ministra, ako aj oddeleniu pre stratégiu odbornej prípravy a študentské záležitosti Generálneho riaditeľstva pre vysokoškolské vzdelávanie a odbornú integráciu, čo viedlo k rozdeleniu lojality. Praktické záležitosti súvisiace s informačným systémom *Parcoursup* sa riešili na týždenných schôdzach. Hoci výhodou tejto formy organizácie bol krátky reakčný čas, pokiaľ ide o každodennú

správu toku študentov, viedla k tomu, že platforme *Parcoursup* chýbalo strategické vedenie.

Napokon systém nebol dostatočne transparentný. Napriek obrovskému potenciálu neumožňoval čo najlepšie využívať údaje uložené na platforme. Využitie tohto potenciálu by takmer určite viedlo k zvýšeniu výkonnosti.

Závery a odporúčania

Vláda úspešne centralizovala prístup k postsekundárnemu vzdelávaniu prostredníctvom digitálnej platformy, ktorá spája všetky vzdelávacie programy, s cieľom zvládnuť zovšeobecnenie vysokoškolského vzdelávania. Platforma *Parcoursup* však vznikla rýchlym prepracovaním pôvodného systému bez zásadných štrukturálnych zmien. Nenapravili sa tak nedostatky informačného systému, pokiaľ ide o bezpečnosť, výkonnosť a spoľahlivosť, hoci zvýšenie záťaže isto muselo pokračovať vzhľadom na hlavný cieľ zahrnúť všetky vysokoškolské študijné programy. Systém bol takisto slabo zdokumentovaný a k vývoju IT sa pristupovalo do istej miery jednoducho, pričom jeho nezvyčajná zložitosť zvyšovala riziko chyby v prípade akýchkoľvek operačných zmien. Platforme preto stále hrozili závažné riziká v súvislosti s kvalitou a kontinuitou poskytovania verejnej služby a bezpečnosťou osobných údajov.

Účtovný dvor *Cour des comptes* preto vydal tieto odporúčania:

- Tím IT agentúry SCN by mal byť lepšie personálne vybavený a finančné prostriedky by sa mali presunúť tak, aby sa posilnili ľudské a finančné zdroje Riaditeľstva pre informačné systémy a štatistický výskum.
- Informačný systém by sa mal prispôsobiť dlhodobému horizontu opravou jeho najnaliehavejších chýb, modernizáciu alebo opätovným vývojom jeho architektúry a zdokumentovaním primárnych databáz starého systému aj platformy *Parcoursup* systematickým a štruktúrovaným spôsobom.
- K informačnému systému *Parcoursup* by sa mala vytvoriť bezpečnostná politika.
- Na Ministerstve školstva a mládeže a Ministerstve vysokoškolského vzdelávania, výskumu a inovácie by sa mal zriadiť spoločný riadiaci orgán pre dohľad nad platformou *Parcoursup*, pričom by sa zdroje presunuli z finančných prostriedkov zákona ORE na „poradenskú“ činnosť.

Lotyšsko
Valsts Kontrole

Využíva verejná správa všetky možnosti efektívneho riadenia infraštruktúry IKT?

Dátum uverejnenia: jún 2019

Hypertextový odkaz na správu: Zhrnutie správy (anglická verzia)

Typ a obdobie auditu

Typ auditu: Audit výkonnosti

Kontrolované obdobie: 2017 – 2019

Zhrnutie správy

Téma auditu

Lotyšský vnútroštátny kontrolný úrad vykonal audit výkonnosti zameraný na efektívnosť verejnej infraštruktúry IKT. Cieľom auditu bolo overiť, či verejná správa jednotne pristupuje k efektívnemu riadeniu infraštruktúry IKT a či inštitúcie posúdili prínosy centralizácie. Bezpečnosť dátových centier sa ďalej určila ako dôležitá otázka v rámci hodnotení možností ďalšieho plánovania optimalizácie.

Neochota orgánov riadiť infraštruktúru IKT centrálne, najmenej na úrovni jedného ministerstva, viedla k tomu, že vzniklo viacero serverovní, čím sa značne zvýšili náklady na údržbu. Zistilo sa, že v štyroch kontrolovaných ministerstvách používalo 22 podriadených útvarov 38 dátových centier. Počas auditu bol národný kontrolný úrad svedkom situácií, v ktorých sa informačné systémy veľkého, dokonca aj celoštátneho významu, nachádzali v priestoroch s nedostatočnou úrovňou zabezpečenia. Nielenže by optimalizácia počtu serverovní umožnila znížiť náklady na IKT, ale takisto by sa následne mohla zaistiť dostatočná úroveň zabezpečenia za nižšiu cenu. V čase auditu už boli v inštitúciách k dispozícii serverovne s vysokou úrovňou zabezpečenia, ale nevyužívala sa ich plná kapacita.

Hlavná téma auditu

Cieľom auditu bolo preveriť, že sú vytvorené a vykonávajú sa všetky predpoklady na jednotné riadenie infraštruktúry IKT s cieľom podporovať efektívnejšie a bezpečnostné používanie zdrojov IKT.

Zistenia a závery

Správa a optimalizácia IKT

- Na vnútroštátnej úrovni ani na úrovni ministerstiev neexistovala dlhodobá vízia vývoja a optimalizácie IKT. Ministerstvá a ich útvary optimalizovali infraštruktúru IKT v súlade so svojimi znalosťami a kapacitou.

V rokoch 2011 až 2017 stúpli celkové náklady na údržbu IKT kontrolovaných inštitúcií zo 17 na 20 mil. EUR ročne. Inštitúcie nemali zavedený žiadny postup na vykonávanie pravidelných hodnotení toho, či by nebolo lacnejšie spravovať infraštruktúru IKT interne, spolupracovať s inou inštitúciou alebo zabezpečovať údržbu IKT externe. Samotným cieľom nie je centralizácia ani decentralizácia IKT. Je však potrebná analýza konkrétnej situácie a alternatív, ktorá poskytne jasné informácie o existujúcich nákladoch a možných alternatívach.

Bezpečnosť IKT

- V právnom rámci nie sú jasne vymedzené bezpečnostné požiadavky na infraštruktúru IKT v logickom systéme v závislosti od relevantnosti informácií, ktoré sa majú spracúvať. Neexistovali podrobné technické požiadavky na ochranu dátových centier IKT.

- Nedostatky v bezpečnostných požiadavkách viedli k nákladnej ochrane alebo naopak, nebola zaistená ochrana informácií celoštátneho významu. Na dôležité informačné systémy sa dokonca využívali hostingové služby dátových centier s nízkym zabezpečením.

- Vo väčšine serverovní boli prítomné bezpečnostné hrozby, pričom dátové centrá neboli dostatočne chránené pred fyzickým prístupom a environmentálnymi rizikami. Ochrana pred bezpečnostnými hrozbami si vyžadovala najmenej 247 000 – 765 000 EUR v závislosti od zvoleného prístupu. Príklady: 1. zlepšenie serverovní obsahujúcich dôležitejšie informačné systémy a zabezpečenie uchovávania dôležitých zdrojov IKT v dátových centrách s vyšším zabezpečením alebo 2. zlepšenie všetkých existujúcich serverovní. To by si však vyžadovalo

investície, ktoré by audítori mohli odôvodniť len v prípade, že by sa minimalizoval počet dátových centier.

Právny rámec bol neúplný a neobsahoval žiadne podrobné bezpečnostné požiadavky na infraštruktúru IKT. Napríklad existovali požiadavky na rôzne kritériá súvisiace s logickou bezpečnosťou, ale neexistovali žiadne kritériá pre fyzickú a environmentálnu bezpečnosť infraštruktúry, čo takisto ovplyvňuje dostupnosť systémov a ochranu údajov. Hoci v dokumentoch o plánovaní verejnej politiky sa zdôrazňoval význam bezpečnosti infraštruktúry IKT a potreba ju posilniť, nikto nenaplánoval konkrétne činnosti v tejto oblasti. Chýbajúca jasná, sledovateľná a logická diferenciácia bezpečnostných požiadaviek predstavovala riziko, že bezpečnostné požiadavky na spracúvanie informácií rovnakej dôležitosti a významu sa bude naprieč krajinou líšiť.

Bezpečnosť v digitálnom priestore štát monitoroval centrálne a reagoval na incidenty, ktoré sa v ňom odohrávajú, ale zodpovednosť za vykonávanie bezpečnosti infraštruktúry IT spočívala na riaditeľovi každej inštitúcie. Znalosti inštitúcií o otázkach bezpečnosti IKT, posudzovaní dôležitosti spracúvaných informácií a zdrojoch na riešenie otázok bezpečnosti IKT dostupných pre inštitúcie sa tak značne líšili.

Vyžadoval sa systém pravidelného monitorovania týchto procesov, pomocou ktorého by sa celá verejná správa hodnotila nezávisle ako jeden systém a na základe štandardných kritérií, s cieľom identifikovať rôzne typy útokov a zabrániť im tým, že sa identifikujú spoločné riziká, a naplánovať preventívne opatrenia na ich zmiernenie.

Litva
Valstybės Kontrolė

Riadenie kritických štátnych informačných zdrojov

Dátum uverejnenia: jún 2018

Hypertextový odkaz na správu: Zhrnutie správy (anglická verzia)
Správa (litovská verzia)

Typ a obdobie auditu

Typ auditu: Audit výkonnosti

Kontrolované obdobie: 2014 – 2017

Zhrnutie správy

Téma auditu

Používaním kritických štátnych informačných zdrojov – kritických elektronických informácií – sa vykonávajú dôležité funkcie verejnej správy, ako napríklad riadenie verejných financií, daňová správa a zdravotná starostlivosť. Akákoľvek strata kritických informácií alebo nedostupnosť príslušných informačných systémov by mohli mať vážne dôsledky pre verejnú bezpečnosť, kvalitu života a hospodárstvo. Posudky všeobecnej kontroly IT, ktoré vykonal litovský Národný kontrolný úrad (NAOL) v rokoch 2006 až 2016, odhalili opakujúce sa problémy v riadení IT (plánovanie, definícia informačnej architektúry, organizačná štruktúra, zmeny, zabezpečenie kontinuity činností, bezpečnosť údajov, monitorovanie a hodnotenie riadenia IT). NAOL vykonal audit kritických štátnych informačných zdrojov s cieľom posúdiť riadenie a zabezpečenie týchto zdrojov a stanoviť opatrenia na zlepšenie.

Cieľom auditu bolo zhodnotiť riadenie (všeobecnú kontrolu) a vyspelosť kritických štátnych informačných zdrojov a odhaliť systémové problémy.

NAOL posúdil vyspelosť riadenia IT v 12 organizáciách verejného sektora[64], ktoré spravujú 44 štátnych informačných systémov triedy jedna. Audit sa vykonal podľa požiadaviek na výkon verejného auditu a medzinárodných noriem najvyšších kontrolných inštitúcií. Posúdenie sa vykonalo v súlade s metodikou COBIT[65] v týchto najrizikovejších oblastiach: strategické plánovanie IT, stanovenie informačnej architektúry, riadenie rizika v oblasti IT, riadenie zmien, zabezpečenie neprerušovaného poskytovania služieb, bezpečnosť systémov, správa údajov, monitorovanie a hodnotenie činností IT, stupeň spoľahlivosti riadenia IT. Procesné hodnotenie zahŕňalo organizačné aj vnútroštátne riadenie IT a interakciu týchto úrovní riadenia.

Kontrolné zistenia

Vývoj zmien úrovne vyspelosti riadenia kritických štátnych informačných zdrojov bol pozitívny. Vzhľadom na zvyšujúcu sa úroveň kybernetických hrozieb bol však zaznamenaný pokrok príliš pomalý a bolo potrebné zvýšiť zabezpečenie týchto zdrojov. Vyplývalo to z nasledujúcich nedostatkov. Systém na identifikáciu kľúčových štátnych informačných zdrojov nebol dostatočne účinný na to, aby umožnil zavádzanie bezpečnostných riešení, ktoré by uspokojovali skutočné potreby:

- V posudkoch určených na dokázanie kritickosti štátnych informačných zdrojov chýbala objektivita, v prehodnoteniach sa nie vždy hodnotili zmeny, tento proces sa nemonitoroval na vnútroštátnej úrovni a usmernenia k určovaniu kritickosti nezaručovali účinné vykonávanie.

  - Systém na identifikáciu kľúčových štátnych informačných zdrojov a kritická informačná infraštruktúra neboli štandardizované; zdroje a infraštruktúra boli identifikované rôznym spôsobom na základe dôležitosti informácií a služieb, čo komplikovalo proces identifikácie týchto zdrojov.

[64] Štátny daňový inšpektorát, Štátne podnikové stredisko registrov, Oddelenie pre informačné technológie a komunikáciu, Štátna rada fondu sociálneho poistenia, Štátne podnikové poľnohospodárske informačné a vidiecke podnikateľské centrum, Centrum pre colné informačné systémy, Štátna potravinová a veterinárna správa, Kancelária Parlamentu Litovskej republiky, Ministerstvo financií, Výbor pre rozvoj informačnej spoločnosti, Štátny nemocenský fond, Štátna lesná správa.

[65] COBIT (Ciele kontroly v oblasti informačných a súvisiacich technológií) je normou medzinárodnej organizácie ISACA, ktorá stanovuje najlepšie postupy riadenia IT.

— Nebola vyvinutá žiadna vnútroštátna informačná architektúra, ktorá by opisovala štátne informačné systémy a ich previazanosť, vyjadrovala rozsah kritických štátnych informačných zdrojov a umožňovala prijímanie informovaných rozhodnutí v súvislosti s dôležitosťou týchto zdrojov.

- Riadenie štátnych informačných zdrojov bolo potrebné lepšie zosúladiť s najlepšími postupmi a normami v oblasti IT, aby sa dosiahlo integrované zlepšenie oblasti IT, ktoré by prispelo k väčšiemu pokroku v riadení kritických štátnych informačných zdrojov:

  — Plánovanie IT nebolo udržateľné: plánované nástroje IT boli predstavené v rôznych dokumentoch, pre nadmerné množstvo strategických dokumentov chýbal akýkoľvek systematický prístup, v dôsledku čoho bolo ťažké určiť kľúčové priority a nasmerovať zdroje na zvládanie najväčších hrozieb.

  — Monitorovanie IT nezabezpečovalo, aby organizácie merali efektívnosť operácií IT a aby z auditov vykonávaných riadiacimi pracovníkmi kritických štátnych informačných zdrojov vyplývala skutočná vyspelosť riadenia IT. Štátne riadenie IT nebolo preskúmané na vnútroštátnej úrovni a otázky riadenia IT sa neanalyzovali systematicky. Vytvoril sa systém na monitorovanie súladu štátnych informačných zdrojov s požiadavkami na bezpečnosť elektronických informácií, ktorý bol určený len na uľahčenie monitorovania dodržiavania bezpečnosti, ale jeho funkcia sa nevyužívala dostatočne.

- Opatrenia na zaistenie odolnosti kritických informačných zdrojov voči úrovni kybernetických hrozieb neboli dostatočne účinné, preto týmto zdrojom stále hrozila zraniteľnosť:

  — Bolo potrebné zvýšiť účinnosť posudzovania bezpečnostných rizík IT, keďže sa neidentifikovali všetky relevantné riziká a metodika ich posudzovania nebola v súlade s najnovšími postupmi v oblasti riadenia IT; nebolo zabezpečené včasné riadenie neprijateľných rizík.

  — Organizačné bezpečnostné opatrenia, ktoré by dokázali znížiť počet kybernetických hrozieb, sa nevyužívali systematicky. Nedostatočné testovanie bezpečnosti, neúplné zaškolenie zamestnancov počas vývoja, aktualizácie a modifikácie informačného systému, neriadené bezpečné konfigurácie a aktualizácie softvéru, nevhodné riadenie kontinuity činností IT a zálohových súborov ohrozovali obnovu subjektov s predpokladom

nepretržitého pokračovania v činnosti, bezpečnostné výkonnostné merania boli nedostatočné a neprispievali k posilneniu bezpečnosti.

Závery

Riadenie IT subjektov verejného sektora, v ktorých sa uskutočnil audit v posledných desiatich rokoch uskutočnil audit, dosiahlo v priemere prvú úroveň vyspelosti z 5[66] a v čase písania správy bolo na úrovni 1,7. Táto nízka úroveň vyspelosti kritických štátnych informačných zdrojov poukazovala na slabé miesta vo formulácii a vo vykonávaní politiky v oblasti štátnych informačných zdrojov, v dôsledku čoho boli tieto zdroje zraniteľnejšie. Ak sa má zvýšiť bezpečnosť týchto zdrojov, systémy riadenia štátnych informačných zdrojov sa musia zlepšiť tak, aby boli v čo najväčšom súlade s najlepšími postupmi. Audítori takisto poukázali na to, že opatrenia na zaistenie odolnosti kritických informačných zdrojov voči kybernetickým hrozbám neboli dostatočne účinné. Preto je potrebné zefektívniť posudzovanie bezpečnostných rizík IT tým, že sa bude klásť väčší dôraz na testovanie bezpečnosti a vzdelávanie zamestnancov pri tvorbe a modernizácii informačných systémov.

Ďalšie správy v tejto oblasti

Názov správy:	Je boj proti počítačovej kriminalite účinný?
Hypertextový odkaz na správu:	Zhrnutie správy (anglická verzia) Správa (litovská verzia)
Dátum uverejnenia:	2020

Názov správy:	Kybernetickobezpečnostné prostredie v Litve
Hypertextový odkaz na správu:	Zhrnutie správy (anglická verzia) Správa (litovská verzia)
Dátum uverejnenia:	2015

[66] Podľa metodiky COBIT.

Maďarsko
Štátny kontrolný úrad

Audit ochrany údajov – Audit vnútroštátneho rámca na ochranu údajov a určitých prioritných dátových záznamov v rámci medzinárodnej spolupráce

Dátum uverejnenia: marec 2017

Hypertextový odkaz na správu: Správa (maďarská verzia)

Typ a obdobie auditu

Typ auditu: Súlad s pravidlami

Kontrolované obdobie: 2011 – 2015

Zhrnutie správy

Téma auditu

Bezpečnosť národných súborov údajov má základný význam pre spoločnosť každej krajiny, pokiaľ ide o zachovanie a ochranu národných hodnôt. Zabezpečenie zvýšenej bezpečnosti osobných a verejných údajov v rámci národných súborov údajov Maďarska je preto kľúčové pre posilnenie dôvery občanov v štát a zabezpečenie nepretržitého a bezproblémového fungovania verejnej správy. Ochrana údajov a bezpečnostná sieť na jej presadzovanie zaistená právnym rámcom majú tak pre spoločnosť kľúčový význam.

Pokiaľ ide o oblasť ochrany údajov, verejná správa zohráva kľúčovú úlohu v riadení najväčších a najcitlivejších registrov údajov, ktoré patria k národným súborom údajov. Prevádzkovatelia registrov pri vykonávaní svojich úloh úzko spolupracujú. Pravidelne prevádzajú registre obsahujúce veľké množstvá údajov a musia dodržiavať zákonné požiadavky na ochranu údajov. Používanie elektronických informačných systémov na riadenie a spracúvanie údajov je v súčasnosti kľúčové, a preto sa musí zaistiť náležité a spoľahlivé fungovanie systémov pomocou náležite navrhnutých a prevádzkovaných kontrol.

Počas svojich auditov kladie Maďarský štátny kontrolný úrad veľký dôraz na ochranu údajov. V rokoch 2011 až 2015 vykonal ŠKÚ komplexné audity ochrany údajov, pričom svoju správu vydal v prvom štvrťroku 2017. Audit takisto skúmal aspekty paralelných medzinárodných auditov vykonaných v spolupráci s pracovnou skupinou skupiny EUROSAI pre oblasť IT, ktoré sa týkali predovšetkým súladu s existujúcimi smernicami Európskej únie.

Účelom auditu zhody o ochrane údajov v Maďarsku bolo posúdiť, či je v Maďarsku zavedený regulačný a operačný rámec pre ochranu údajov a či hlavné organizácie na správu údajov spĺňajú požiadavky bezpečnej správy údajov a externého zabezpečovania spracovania údajov. Audit sa zameriaval najmä na ochranu osobných údajov a národných súborov údajov.

V kontexte auditu ŠKÚ hodnotil správu údajov šiestich organizácií na správu údajov (napríklad daňový orgán, štátnu pokladnicu, zdravotné poistenie, vyplácanie dôchodkov, úrad pre vzdelávanie, osobné údaje a záznamy o adresách, vozidlách a cestovaní a správne agentúry pre správu údajov o trestných činoch) a takisto činnosti orgánu pre ochranu osobných údajov a orgánu pre informačnú bezpečnosť.

Audit sa osobitne zameriaval na mandát organizácií na správu údajov, najmä v prípade prenosu údajov tretím stranám. Počas auditu vnútorných kontrol v oblasti správy údajov a spracovania údajov sa hodnotila existencia aktuálnych predpisov o povinnostiach, úlohách a kompetenciách, riadenie ľudských zdrojov a procesy.

Pokiaľ ide o elektronické systémy používané pri správe údajov, ŠKÚ posudzoval súvisiace bezpečnostné opatrenia, a to aj v oblastiach fyzickej ochrany, prístupových práv, protokolovania, postupov na hodnotenie bezpečnosti, zabezpečenie systému a komunikácie a súlad s bezpečnostnou klasifikáciou organizácie ako celku.

Audit externého zabezpečovania spracúvania údajov sa vykonával na základe uzavretých zmlúv, pričom sa skúmalo, či organizácie na správu údajov ukladali organizáciám na spracúvanie údajov povinnosť spĺňať požiadavky súvisiace s činnosťami v oblasti spracúvania údajov v súlade s legislatívnymi nariadeniami.

Zistenia a závery

Na základe auditu Maďarský štátny kontrolný úrad zistil, že interné nariadenia organizácií pre správu údajov týkajúce sa činností v oblasti správy údajov zaisťovali ochranu národných súborov údajov, ktoré sú súčasťou národných aktív, v súlade s právnymi ustanoveniami platnými v rokoch 2011 až 2015. Prevádzkovatelia v praxi

náležite spĺňali požiadavky bezpečnej správy údajov a externého zabezpečovania spracovania údajov. Prevod údajov tretím stranám sa vykonával na základe príslušného mandátu a jasného vymedzenia povinností a právomocí.

U niekoľkých prevádzkovateľov sa zistilo, že bezpečnostná klasifikácia elektronických systémov a organizácia ako celok neboli vždy v súlade so zákonnými požiadavkami, ale rozsah nedostatkov nemal podstatný vplyv na bezpečnosť spracúvaných údajov. Na základe odporúčaní zahrnutých v audítorskej správe organizácie na správu údajov napravili tieto nedostatky v rámci akčných plánov, ktoré schválil ŠKÚ.

V súvislosti s paralelným medzinárodným auditom vykonaným v spolupráci s pracovnou skupinou skupiny EUROSAI pre oblasť IT ŠKÚ zistil, že maďarské právne predpisy na ochranu osobných údajov sú v súlade s existujúcou smernicou EÚ.

Záverom sa uvádza, že vykonaním auditu ochrany údajov Maďarský štátny kontrolný úrad prispel k dobrej správe a ochrane národných súborov údajov.

Ďalšie správy v tejto oblasti

Názov správy:	Správa – Následné audity – Audit ochrany údajov – Audit vnútroštátneho rámca na ochranu údajov a určitých prioritných dátových záznamov v rámci medzinárodnej spolupráce
Hypertextový odkaz na správu:	Správa (maďarská verzia)
Dátum uverejnenia:	2020

Holandsko
Dvor audítorov

Kybernetická bezpečnosť kritických vodných diel a hraničných kontrol v Holandsku

Dátumy uverejnenia: marec 2019 a apríl 2020

Hypertextový odkaz na správy: Zhrnutie správy o kybernetickej bezpečnosti kritických vodných diel (anglická verzia)

Zhrnutie správy o kybernetickej bezpečnosti a automatizovanom systéme hraničnej kontroly (anglická verzia)

Typ a obdobie auditu

Typ auditu: Audit výkonnosti

Kontrolované obdobie: 2018 – 2020

Zhrnutie správy

Téma auditu

Holandský dvor audítorov sa v roku 2018 rozhodol vykonať audity kybernetickej bezpečnosti v sektoroch, ktoré sú pre spoločnosť kritické. Na základe dlhoročných skúseností s vykonávaním auditov zhody v oblasti informačnej bezpečnosti v ústrednej štátnej správe si Dvor audítorov uvedomuje pridanú hodnotu auditov *výkonnosti* politík a opatrení v praxi. Prvými dvomi kontrolovanými sektormi boli vodné hospodárstvo, ktoré je kľúčové pre krajinu prevažne pod hladinou mora, a automatizovaný systém hraničnej kontroly, ktorý je pre ňu kľúčový vzhľadom na polohu letiska Amsterdam Schiphol ako medzinárodného centra a brány do krajiny.

Ministerstvo infraštruktúry a vodného hospodárstva označilo niekoľko vodných diel spravovaných Generálnym riaditeľstvom pre verejné práce a vodné hospodárstvo (kontrolovaný subjekt) ako „kritické súčasti“ sektora vodného hospodárstva. Mnohé počítačové systémy používané pri prevádzke kritických vodných diel pochádzajú

z 80. a 90. rokov 20. storočia – z čias, keď sa „kybernetická bezpečnosť“ bežne nezohľadňovala. Tieto systémy boli pôvodne určené na samostatnú prevádzku, ale postupne sa prepájali s väčšími počítačovými sieťami, napríklad na to, aby sa uľahčila prevádzka na diaľku. V dôsledku tohto vývoja sa systémy stali zraniteľnejšími voči kybernetickým hrozbám.

Minister obrany a minister spravodlivosti a bezpečnosti spoločne zodpovedajú za hraničné kontroly, ktoré vykonáva holandská pohraničná stráž na letisku Schiphol. Obe ministerstvá (kontrolované subjekty) vlastnia systémy IT, o ktoré sa opiera hraničná stráž. Systémy sú kritické pre letiskové operácie a používajú sa na spracovanie vysoko citlivých údajov. V dôsledku toho sú zaujímavým terčom kybernetických útokov, ktorých cieľom je sabotáž, špionáž alebo manipulácia hraničných kontrol.

V rámci auditov sa skúmalo, ako sú kontrolované subjekty pripravené na riešenie kybernetických hrozieb a či ich riešia účinne.

- Audit sa zameriaval na zodpovedanie týchto otázok: Ako kontrolované subjekty *chránia* systémy pred kybernetickými hrozbami a *zabraňujú* kybernetickým útokom?
- Ako kontrolované subjekty *odhaľujú* kybernetické hrozby a útoky?
- Ako kontrolované subjekty *reagujú* v situácii, keď dôjde ku kybernetickému útoku?

Oba audity sa osobitne zameriavali na účinnosť. Etickí hackeri úzko spolupracovali s kontrolovanými subjektmi na vodných dielach a jednom systéme hraničnej kontroly. Nie je potrebné zdôrazňovať, že všetky zistenia testu sa vyriešili pred tým, než sa uverejnili správy, a nezverejnili sa žiadne technické podrobnosti.

Hlavným rozdielom medzi týmito dvomi auditmi bolo, že audit vodných diel bol zameraný na dosahovanie cieľov kontrolovaného subjektu, zatiaľ čo audit kontroly hraníc bol založený na rámci pre kybernetickú bezpečnosť NIST.

Zistenia

Po prvé, z oboch auditov vyplynulo, že kontrolované subjekty si uvedomujú kybernetické hrozby a už začali so zavádzaním profesionálneho prístupu k tejto záležitosti.

V prípade vodných diel však musel kontrolovaný subjekt vyvinúť ďalšie snahy, pokiaľ ide o odhaľovanie a reakciu, aby splnil svoje vlastné kybernetickobezpečnostné ciele. Kontrolovaný subjekt mal zriadené bezpečnostné operačné centrum (BOC) na odhaľovanie kybernetických útokov a reakciu na ne. Cieľ odhaliť akékoľvek kybernetické útoky namierené proti kritickým vodným dielam stanovený na rok 2017 však nebol do jesene roku 2018 splnený. Znamenalo to, že existuje riziko, že kybernetický útok namierený proti kritickej vodnej štruktúre sa neodhalí alebo sa odhalí príliš neskoro. Z testu vykonaného na jednom z kritických vodných diel ďalej vyplynulo, že je možné k nemu získať fyzický prístup. Hackeri dokázali vstúpiť do riadiacej miestnosti a zistili pri nezabezpečených pracovných staniciach sa ocitli sami. Napokon kontrolovaný subjekt nevypracoval žiadny scenár pre prípad krízy spôsobenej kybernetickým útokom a informácie týkajúce sa reakcie chýbali alebo neboli aktuálne. Prítomnosť aktuálnych informácií by sa mohla ukázať ako kritická pre rýchlu a účinnú reakciu na krízovú situáciu.

Čo sa týka kontroly hraníc, opatrenia v oblasti kybernetickej bezpečnosti neboli ani dostatočné, ani nadčasové. Po prvé, dôležité systémy na kontrolu hraníc sa museli formálne schváliť pred tým, ako mohli začať prevádzku, aby sa zabezpečilo, že sú zavedené všetky kybernetickobezpečnostné opatrenia. Zistili sme, že dva z troch systémov sa prevádzkovali bez schválenia, čo znamená, že nebolo zaručené, že sú zavedené potrebné bezpečnostné opatrenia. Po druhé, jedno BOC bolo funkčné, ale žiadny zo systémov nebol naň priamo napojený. Hoci bola generická infraštruktúra napojená na SOC, stále to predstavovalo riziko, že kybernetické útoky zostanú neodhalené alebo sa odhalia príliš neskoro. Po tretie, bezpečnostné testy sa nevykonávali pravidelne. V skutočnosti sa v minulosti testoval len jeden z troch systémov, a aj to len v obmedzenej miere. Napokon, podobne ako pri prvom audite, nebol vypracovaný žiadny konkrétny scenár pre prípad krízy spôsobenej kybernetickým útokom.

Počas testovania bezpečnosti jedného zo systémov, ktorý sa dovtedy nikdy netestoval, našli etickí hackeri viaceré slabé miesta. Kombináciu týchto slabých miest by mohla neoprávnená osoba zvnútra konajúca so zlým úmyslom využiť na spustenie kybernetického útoku s cieľom získať prístup k informáciám v systéme, kopírovať ich alebo dokonca ich zmanipulovať. Výsledky dokazujú dôležitosť pravidelného testovania bezpečnosti.

Zistenia sú znepokojivé z dôvodu prebiehajúcej automatizácie procesov na hraniciach. V blízkej budúcnosti bude čoraz väčší počet systémov hraničnej kontroly spracúvať

čoraz viac údajov pomocou rastúceho počtu prepojení. Tým sa zvyšuje riziko kybernetických útokov, a preto nebol používaný prístup nadčasový.

Závery

V prípade vodných diel bránili kontrolovanému subjektu podniknúť konečné kroky v oblasti kybernetickej bezpečnosti viaceré kľúčové prvky. Napríklad nebolo jasné, aká je úroveň ohrozenia, v dôsledku čoho bolo ťažké posúdiť, či sú prijaté opatrenia a pridelené rozpočtové prostriedky dostatočné. Ústredné oddelenie zodpovedné za kybernetickú bezpečnosť ďalej nemalo mandát na vykonávanie potrebných kybernetickobezpečnostných opatrení v oblasti v decentralizovaných vodných dielach. V tomto zmysle sa nadviazalo na audítorské odporúčania, čo pomohlo organizácii v ďalšom postupe.

V prípade hraničných kontrol neexistoval jasný dôvod nedostatočnej úrovne kybernetickej bezpečnosti. Z prieskumu počas auditu sa zistilo, že existujú úplné a podrobné postupy a politiky v oblasti kybernetickej bezpečnosti, ako aj dostatočná odborná úroveň a kvalifikovaní pracovníci. Audítorské odporúčania boli preto zamerané najmä na zabezpečenie toho, aby sa každý krok reálne uskutočnil.

Oba audity pritiahli veľkú pozornosť parlamentu a médií. Auditom sa zvýšila informovanosť o kybernetickej bezpečnosti v súvislosti s kľúčovou infraštruktúrou, pričom kontrolovaným subjektom poskytol informácie o tom, ako majú zlepšiť svoju kybernetickú bezpečnosť. Úzka spolupráca s kontrolovaným subjektom bola kľúčová na to, aby plne porozumel svojej situácii a riešil riziká spojené so skúmaním a testovaním kybernetickej bezpečnosti.

Takisto sa plánuje tretí audit z tohto radu. Okrem toho je úroveň informačnej bezpečnosti holandskej vnútroštátnej verejnej správy kľúčovým prvkom ročného cyklu auditov zhody. V minulých rokoch bola holandská NKI svedkom toho, že úroveň opatrení mnohých ministerstiev v oblasti informačnej bezpečnosti nedosahovala potrebnú úroveň. Dvor audítorov v súčasnosti využíva skúsenosti získané zo svojich auditov kybernetickej bezpečnosti na rozšírenie svojho pohľadu na vykonávanie auditu informačnej bezpečnosti, pričom sa zameriava na viac než len dokumenty a politiky a testuje skutočnú účinnosť opatrení.

Ďalšie správy v tejto oblasti

Názov správy: Kapitola 3 „Staat van de rijksverantwoording 2019“
Hypertextový odkaz na správu: Správa (holandská verzia)
Dátum uverejnenia: 2020

Názov správy: Digitálna práca z domu pod lupou
Hypertextový odkaz na správu: Správa (holandská verzia)
Dátum uverejnenia: 2020

Poľsko
Najwyższa Izba Kontroli

Zaistenie bezpečnosti prevádzky systémov IT používaných na výkon verejných úloh

Dátum uverejnenia: 2016

Hypertextový odkaz na správu: Správa (poľská verzia)

Typ a obdobie auditu

Typ auditu: Súlad s pravidlami

Kontrolované obdobie: 2014 – 2015

Zhrnutie správy

Téma auditu

Cieľom auditu bolo posúdiť, či sú údaje zbierané v systémoch určených na vykonávanie dôležitých verejných úloh v kontrolovaných útvaroch zabezpečené. Audit sa zaoberal šiestimi vybranými inštitúciami, ktoré plnia významné verejné úlohy. Po analýze bol v každej z inštitúcií vybraný jeden systém IT, ktorý sa následne podrobne preskúmal. Pri audite sa uplatňovala verzia 4.1 metódy COBIT (Kontrolné ciele pre informačné a súvisiace technológie).

Tento audit sa vykonal po audite „verejných orgánov“, ktorý sa týkal plnenia úloh v oblasti kybernetickej bezpečnosti v Poľsku[67] v roku 2015, ktorého zistenia poukázali na systémové problémy. Audit v roku 2016 názorne ukázal okrem iného to, že štátna správa k tomuto dňu nepodnikla kroky na zabezpečenie bezpečnosti IT na vnútroštátnej úrovni. Dospelo sa k záveru, že činnosti verejných subjektov súvisiace s ochranou kybernetického priestoru sa vykonávali neucelene a chýbal im systematický prístup. Keďže chýbali centrálne mechanizmy na zabezpečenie konkrétnych bezpečnostných podmienok pre špecifické systémy IT kľúčové pre fungovanie štátu,

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

cieľom auditu bolo preskúmať, či inštitúcie prevádzkujúce systémy IT používané na plnenie dôležitých verejných úloh zaisťovali, aby sa tieto úlohy mohli plniť bezpečne.

V roku 2019 bol schválený ďalší systémový audit kybernetickej bezpečnosti s názvom Kybernetická bezpečnosť v Poľsku, zistenia sú však dôverné.

Audítorské otázky

Čiastkové ciele boli rozdelené do dvoch oblastí hodnotenia, pričom sa zisťovali odpovede na konkrétne otázky.

V oblasti podpory bezpečnosti IT audit skúmal na úrovni celej organizácie okrem iného to, či:

- sa vykonávalo riadenie bezpečnosti IT,
- sa vykonávali plány na zaistenie bezpečnosti IT,
- sa bezpečnosť IT testovala, či sa nad ňou vykonával dozor a či sa monitorovala,
- boli vymedzené bezpečnostné incidenty IT,
- sa IT riadili pomocou šifrovacích kľúčov,
- sa vykonávala ochrana proti škodlivému softvéru a jeho odhaľovanie a opravy,
- bola zaistená sieťová bezpečnosť.

V oblasti podpory bezpečnosti audit skúmal na úrovni vybraných systémov okrem iného to, či:

- boli spravované používateľské identity a účty,
- boli bezpečnostné technológie a citlivé údaje chránené.

Zistenia a závery

Stupeň prípravy a vykonávania informačného bezpečnostného systému nezaisťoval prijateľnú úroveň bezpečnosti údajov zbieraných v systémoch IT určených na vykonávanie dôležitých verejných úloh. Informačno-bezpečnostné procesy sa vykonávali neriadene a v dôsledku chýbajúcich postupov intuitívne. Zo šiestich kontrolovaných útvarov mal len jeden zavedený informačný bezpečnostný systém,

pričom je potrebné poznamenať, že v tejto operácii sa takisto vyskytli závažné chyby. Vo všetkých kontrolovaných útvaroch s výnimkou jedného práca na zaisťovaní vhodných podmienok pre bezpečnosť informácií spracúvaných v systémoch IT nedosahovala náležitú úroveň, pretože začala len nedávno a bola v prípravnom štádiu, ktoré takisto zahŕňalo vytváranie potrebných formálnych základov. Vychádzala zo zjednodušených alebo neformálnych mechanizmov založených na osvedčených postupoch alebo predošlých skúseností zamestnancov IT.

V súlade s metodikou COBIT 4.1 sa vyspelosť procesov riadenia informačnej bezpečnosti v jednotlivých útvaroch na stupnici od nula do päť pohybovala od 1 – počiatočné/*ad hoc* do 3 – stanovené, pričom päť je maximum.

Zodpovednosť za zaistenie bezpečnosti IT v kontrolovaných útvaroch spočívala na bezpečnostnom koordinátorovi, ktorý však v praxi nebol spôsobilý riadiť celý proces. Súvisiace úlohy takisto často vykonávala len jedna osoba. Hoci boli vymenované tímy odborníkov alebo uzavreté zmluvy s externými dodávateľmi, nevykonala sa analýza potrebná na stanovenie toho, či poskytované služby spĺňajú bezpečnostné potreby útvaru. Znalosti kontrolovaných útvarov o potrebe zaistiť bezpečnosť informačných technológií boli neucelené a obmedzené. Bezpečnosť údajov sa vnímala predovšetkým ako zodpovednosť a pole pôsobnosti oddelenia IT, a nie všetkých organizačných útvarov so štatutárnymi úlohami, čo vo veľkej miere bránilo vývoju zosúladených systémov riadenia bezpečnosti IT pre celú inštitúciu.

Z porovnania kvality spôsobu, akým sa plnili povinnosti súvisiace so zabezpečením informačnej bezpečnosti, pokiaľ ide o celé organizácie aj o vybrané systémy, jasne vyplynulo, že kvalita vykonávania bola vyššia v druhom prípade. Dôvodom môže byť vplyv, ktorý mali na zaistenie bezpečnosti praktické znalosti a zapájanie technického personálu strednej úrovne, častejšie používanie komerčných systémov IT vychádzajúcich z trhových štandardov vo verejnej správe a pokročilé riešenia na zaistenie bezpečnosti. Uplatňovanie týchto riešení, predošlých skúseností a osvedčených postupov umožnilo udržiavať určitú úroveň bezpečnosti prevádzky rôznych systémov v podmienkach s obmedzenými zdrojmi, organizačnými nedostatkami alebo „nefunkčnou“ reguláciou. Nemôže to však byť cieľovým riešením, pretože v časoch dynamického rastu úrovne ohrozenia sa bezpečnosť systémov IT nemôže zakladať na opatreniach riadených chaotickým spôsobom a prispôsobených výlučne na prekonávanie bezprostredných ťažkostí.

Zistenia auditu

Na centrálnej úrovni je potrebné vypracovať a vykonávať všeobecné odporúčania a požiadavky na bezpečnosť IT uplatniteľné pre všetky verejné orgány. Vyžaduje sa systémové riešenie, v rámci ktorého sa výsledky auditov bezpečnosti IT uverejňujú spôsobom, ktorý umožňuje občanom prístup k informáciám o činnostiach verejných orgánov a zároveň obmedzuje prístup k informáciám o opatreniach a metódach používaných na zaistenie bezpečnosti spracúvaných informácií.

Ďalšie správy v tejto oblasti

Názov správy:	Riadenie informačnej bezpečnosti regionálnymi orgánmi
Hypertextový odkaz na správu:	Správa (poľská verzia)
Dátum uverejnenia:	2019

Názov správy:	Kybernetická bezpečnosť v Poľsku (utajované skutočnosti)
Hypertextový odkaz na správu:	*Verejne nedostupné*
Dátum schválenia:	2019

Názov správy:	Zaistenie bezpečnosti systémov IT regionálnymi úradmi v Podleskom vojvodstve
Hypertextový odkaz na správu:	Správa (poľská verzia)
Dátum uverejnenia:	2018

Názov správy:	Predchádzanie kybernetickému šikanovaniu medzi deťmi a mladými ľuďmi a boj proti nemu
Hypertextový odkaz na správu:	Správa (poľská verzia)
Dátum uverejnenia:	2017

Názov správy:	Plnenie úloh v oblasti kybernetickej bezpečnosti verejnými subjektmi v Poľsku
Hypertextový odkaz na správu:	Správa (poľská verzia)
Dátum uverejnenia:	2015

Názov správy:	Vykonávanie vybraných požiadaviek na informačné systémy, výmenu elektronických informácií a národný rámec pre interoperabilitu na príklade obecných rád a miest s okresnými právami.
Hypertextový odkaz na správu:	Správa (poľská verzia)
Dátum uverejnenia:	2015

Portugalsko
Tribunal de Contas

Audit portugalských elektronických pasov

Dátum uverejnenia: 2014

Hypertextový odkaz na správu: Správa (portugalská verzia)

Typ a obdobie auditu

Typ auditu: Audit výkonnosti

Kontrolované obdobie: 2013

Zhrnutie správy

Téma auditu

Operatívny audit portugalského elektronického pasu (PEP) bol zameraný na účinnosť informačných systémov, ktoré podporujú jeho udeľovanie, vydávanie a používanie, najmä pri automatizovanej kontrole cestujúcich čítaním biometrických údajov na portugalských hraniciach[68].

Hlavnými cieľmi auditu bolo:

- preveriť súlad s právom EÚ a vnútroštátnym právom, medzinárodnými normami a usmerneniami pre udeľovanie, vydávanie a používanie PEP vrátane primeranosti vnútroštátneho právneho rámca,
- preskúmať účinnosť kľúčových procesov spojených so životným cyklom PEP, najmä tých, ktoré sú spojené s udeľovaním, vydávaním a používaním pasu,

[68] Odvolávame sa na automatizované systémy hraničnej kontroly (ABC) v rámci agentúry Frontex (Európskej agentúry pre pohraničnú a pobrežnú stráž).

- preskúmať kritické stránky výkonnosti informačných systémov, a to najmä spĺňanie bezpečnostných požiadaviek týkajúcich sa informačných systémov PEP (SIPEP).

Medzi kľúčové rizikové oblasti patrili:

- strata/krádež hmotného majetku a/alebo elektronických informácií,
- zneužívanie dôverných informácií,
- riziko nedodržania súladu s predpismi (neplnenie zákonných a regulatórnych požiadaviek).

Obdobie auditu: 1. január 2013 – 31. december 2013 (v prípade potreby sa predĺži na skorší a neskorší rok)

Zistenia a závery

Portugalský elektronický pas (PEP) zahŕňa tri kategórie: spoločné[69], diplomatické alebo špeciálne. Takisto existuje pas pre cudzincov, ktorým sa udeľujú obmedzené výsady.

Systém schvaľovania zahŕňa niekoľko subjektov na zber žiadostí niekoľko subjektov na zber údajov a schvaľujúcich orgánov, ale len jedného vydavateľa (ktorý zodpovedá za výrobu, prispôsobenie a doručenie).

Na procese sa zúčastňuje niekoľko subjektov (subjekty PEP). Tieto subjekty zbierajú údaje a udeľujú pasy:

- Kontinentálne Portugalsko: Serviço de Estrangeiros e Fronteiras (SEF)[70] a registračné služby Instituto dos Registos e do Notariado (IRN)[71];

[69] Približne 99 % z celku.

[70] Portugalská služba pre prisťahovalectvo a ochranu hraníc/cudzinecká a pohraničná služba.

[71] Registračný úrad a notár (len príjem).

- Autonómne oblasti Azory[72] a Madeira: služby v rámci príslušného regiónu *Vice-Presidência do Governo Regional*[73]; v zahraničí: portugalské konzuláty;

- Imprensa Nacional – Casa da Moeda, S.A. (INCM)[74] vydáva pasy.

Hlavné procesy podporuje najmä SIPEP (centrálny riadiaci systém na podávanie žiadostí o vydanie portugalských pasov). SIPEP umožňuje zaznamenávanie, ukladanie, spracúvanie, validáciu a poskytovanie potrebných informácií súvisiacich s udeľovaním PEP, spúšťa proces prispôsobenia vykonávaný INCM a zaisťuje prepojenie s ďalšími systémovými aplikáciami, pričom koordinuje všetky subjekty PEP zapojené do fyzickej a logistickej registrácie zbieraných údajov.

Subjekty PEP majú organizačnú štruktúru, ktorá im umožňuje plniť zákonné ciele súvisiace s PEP. Systém sa vo veľkej miere stále opiera o ľudské zdroje na úrovni žiadostí a zberu. SIPEP však zahŕňa niekoľko funkcií automatizovaného spracúvania a validačných kontrol.

Keďže postupy zabezpečujú kontrolné funkcie a narábanie s údajmi, z ktorých sa niektoré môžu vykonávať nezávisle bez ľudského zásahu, SIPEP má významný vplyv v súvislosti s organizáciou a informačným systémom, najmä pokiaľ ide o: i) porozumenie štandardom, procesom a potrebným údajom a ich vymedzenie a ii) vymedzenie vlastných požiadaviek informačného systému.

Efektívnosť a účinnosť procesu zberu údajov sa zabezpečuje interakciou SIPEP s inými informačnými systémami[75] v súlade s právnymi predpismi.

Bol zriadený rámec celkovej kontroly činností IT (správa, vývoj a nákup, operácie IT, kontinuita činností a obnova po haváriách, informačná bezpečnosť), ktorý zabezpečuje

---

[72] A služobné miesta *Agência para a Modernização e Qualidade do Serviço ao Cidadão, I. P. (RIAC)* – Agentúry pre modernizáciu a kvalitu služieb pre občanov, verejný inštitút (len príjem).

[73] Podpredsedníctvo regionálnej vlády.

[74] Oficiálna tlačiareň a mincovňa, verejná spoločnosť.

[75] Konkrétne: Integrovaný informačný systém SEF (SIISEF); Národná časť Schengenského informačného systému (NSIS); Občianska identifikačná databáza, databáza registrov trestov.

vývoj, prevádzku, správu a údržbu systému SIPEP, hoci nie je rozsiahle zdokumentovaný.

Ukazovatele aktivity (2013):

- Udelilo sa približne 500 000 PEP, z ktorých približne 63 % udelil SEF, 33 % portugalské konzulárne úrady a 4 % regionálne vlády.
- Príjmy z emisie PEP predstavovali približne 37 mil. EUR, prevažne z INCM (43 %), SEF (32 %) a *Ministério dos Negócios Estrangeiros (MNE)*[76] (17 %).

Testy vykonané v systéme SIPEP v roku 2013 nepotvrdili dodržiavanie zákonne stanovenej maximálnej lehoty na doručenie (od dátumu žiadosti do pripravenosti PEP na vyzdvihnutie na mieste vydania), pretože skutočný čas doručenia na mieste vydania sa nezaznamenával vždy načas.

Subjekty SEF, MNE, RIAC a INCM uskutočnili investície vo výške 11 miliónov EUR súvisiace s nákupom zariadení na zber biometrických údajov a podpisov (kiosky), zariadení na automatizovaný systém hraničnej kontroly a s nákupom a údržbou systémov, služieb a technickej pomoci IT, pričom najvyššiu sumu vynaložil SEF.

Pred PEP bola cena (nebiometrického) pasu Portugalskej republiky 22,44 EUR; v roku 2006 stál štandardný (biometrický) PEP 60 EUR, pričom v roku 2011 sa jeho cena zvýšila na 65 EUR.

Žiadosti o vydanie PEP

Žiadosti o vydanie PEP spracúvajú pracovníci príslušných útvarov, ktorí prijímajú dokumenty súvisiace so žiadosťou, zbierajú biografické a biometrické údaje žiadateľov, vyberajú poplatky a neskôr doručujú vydané PEP.

Základný systém (SIPEP) validuje správnosť a kvalitu údajov pomocou virtuálnych kontrol a krížových odkazov na iné informačné systémy, konkrétne na občiansku identifikačnú databázu, aby sa zabezpečilo, že žiadosť je v súlade s pravidlami a môže sa na základe nej udeliť a vydať PEP.

V protokolových súboroch sa zaznamenávajú súvisiace zmeny stavu, čím sa zaisťuje overiteľnosť, integrita a nespornosť úkonov.

[76] Ministerstvo zahraničných vecí.

Prenos údajov medzi orgánmi zodpovednými za zber údajov (v Portugalsku a v zahraničí) a SEF sa uskutočňuje prostredníctvom VPN (*Virtual Private Network*), ktorý sa vykonáva na základe riadenia prístupu v súlade s prihlasovacími údajmi kontrolovanými SEF[77].

Žiadosť o štandardný PEP sa spracúva inak, ak ju predkladajú občania s obmedzenými právami, vrátane: i) osôb, ktoré nemôžu uplatňovať svoje práva (maloleté osoby, právne nespôsobilé osoby alebo zakázané osoby), ii) osôb vylúčených na základe súdneho alebo policajného rozhodnutia (záznam v registri trestov, prebiehajúce konanie alebo zadržanie dokladov) a iii) v prípade, že žiadateľ o druhý PEP sa odvoláva na celoštátny alebo oprávnený záujem.

Udeľovanie PEP

Rozhodnutie udeliť štandardný PEP môže byť:

- Automatické – automatické schválenie systémom SIPEP na podávanie žiadostí po validácii totožnosti žiadateľa, ak neexistuje záznam v registri trestov (krížovým odkazom na občiansku identifikačnú databázu a databázu registra trestov IRN) a ak voči žiadateľovi neprebieha žiadne konanie. Vyskytuje sa len v SEF pre žiadosti o vydanie PEP na pevnine[78].
- Podlieha individuálnemu prijatiu/schváleniu inými subjektmi (regionálne vlády a konzulárne úrady) alebo v prípade SEF požiadavkám, na ktoré sa nevzťahuje automatické udeľovanie[79].

[77] SIPEP je prístupný (prostredníctvom internetu) na vnútroštátnej/regionálnej a medzinárodnej úrovni pre služby nachádzajúce sa na pevnine, v autonómnych regiónoch Azory a Madeira a v zahraničí (portugalské konzuláty).

[78] Ide o automatickú funkciu systému SIPEP na udelenie (vnútorne označovanej ako „povolenie“) žiadosti (okrem druhého PEP) občanovi v zákonnom veku s platným občianskym preukazom, bez prebiehajúceho súdneho konania a ktorý nie je zakázaný ani vylúčený. Štandardné PEP udelené SEF, ktoré predstavujú približne 60 %, sa udelili na základe postupov automatickej validácie a rozhodovania o udelení, pričom zvyšné skúmal a schvaľoval subjekt *Direção Central de Imigração e Documentação* (DCID).

[79] Najmä v prípadoch, keď žiadatelia nemôžu uplatňovať svoje práva (maloletí, nespôsobilé osoby alebo osoby, ktoré majú zákaz), vylúčení súdnou cestou alebo políciou alebo v prípade druhého PEP, ktorých žiadosť posudzuje DCID v každom jednotlivom prípade.

Vydanie PEP

Vydanie PEP, ktoré zahŕňa výrobu, prispôsobenie a doručenie, patrí do právomoci INCM. Keď sa doručenie PEP zaznamená do systému SIPEP, stav pasu sa zmení na „platný“.

Ceny PEP sa líšia v závislosti od úrovne požadovanej služby. Pri meraní úrovne služby musí SIPEP zohľadniť skutočný dátum doručenia PEP.

PEP doručuje zmluvná prepravná služba.

Ukončenie platnosti PEP

Zakaždým, keď žiadateľ predloží predchádzajúci, stále platný PEP, mal by sa zablokovať, aby sa zabránilo jeho opakovanému použitiu, čo zodpovedá stavu „nepoužiteľný“ v zázname o pase v systéme na podávanie žiadostí SIPEP.

Fínsko
Valtiontalouden tarkastusvirasto

Mechanizmy kybernetickej ochrany

Dátum uverejnenia: 2017

Hypertextový odkaz na správu: Správa (fínska verzia)

Typ a obdobie auditu

Typ auditu: Audit výkonnosti

Kontrolované obdobie: 2016 – 2017

Zhrnutie správy

Téma auditu

Cieľom auditu bolo preskúmať, či je kybernetická ochrana v ústrednej štátnej správe účinná a nákladovo efektívna v čo najväčšej miere. Audit bol zameraný na to, akým spôsobom sa organizuje a riadi kybernetická bezpečnosť v ústrednej štátnej správe. Výsledky auditu by sa mohli použiť na rozvoj účinnosti a efektívnosti kybernetickej bezpečnosti v ústrednej štátnej správe. Audit prebiehal od 22. septembra 2016 do 4. septembra 2017. Následný audit sa uskutočnil na jeseň 2019. Počas následného auditu Národný kontrolný úrad skúmal opatrenia prijaté v nadväznosti na zistenia auditu a audítorské odporúčania.

Kontrolované subjekty zahŕňali orgány zodpovedné za kybernetickú ochranu v ústrednej štátnej správe (Kancelária premiéra, Ministerstvo financií, Ministerstvo dopravy a komunikácií) a orgány zodpovedné za centralizované úlohy v oblasti kybernetickej ochrany a centralizované IT služby v ústrednej štátnej správe (Národné centrum pre kybernetickú bezpečnosť Fínskej agentúry pre dopravu a komunikáciu, Centrum IKT verejnej správy Valtori, Agentúra pre služby v oblasti digitálnych údajov a údajov o obyvateľstve). Účinnosť usmernení sa takisto posudzovala preskúmaním útvarov ústrednej štátnej správy, ktoré poskytujú elektronické služby (Agentúra pre služby v oblasti digitálnych údajov a údajov o obyvateľstve, Fínska agentúra

pre dopravu a komunikáciu Traficom, Národný správny exekučný úrad a jeho dozorný orgán Ministerstvo spravodlivosti a Centrum pre služby IKT Ministerstva spravodlivosti).

Audítorské otázky

Na audit organizácie kybernetickej bezpečnosti sa použili tieto audítorské otázky:

- Zvážil kontrolovaný subjekt pri organizácii kybernetickej bezpečnosti dostatočne ekonomickú stránku?
- Podporuje situačná informovanosť auditovaného subjektu v oblasti kybernetickej bezpečnosti kybernetickú bezpečnosť systémov?
- Je schopnosť kontrolovaného subjektu reagovať na porušenia kybernetických zásad dostatočná?

Téma auditu mechanizmy kybernetickej ochrany bola súčasťou predmetu auditu „Zaistenie operačnej spoľahlivosti informačnej spoločnosti“ v pláne auditov Fínskeho národného kontrolného úradu na roky 2016 – 2020. Z hľadiska dôležitosti financií verejnej správy možno odôvodniť tému auditu nevýhodami súvisiacimi s prerušením poskytovania služieb a porušením ochrany údajov, ako aj negatívnymi dôsledkami slabej kybernetickej bezpečnosti pre obchodné činnosti. Audit sa vykonával paralelne s auditom s názvom „Usmerňovanie operačnej spoľahlivosti elektronických služieb“, ktorý patrí k tomu istému predmetu. Kľúčový audítorský materiál sa skladal z dokumentov a rozhovorov s orgánmi zodpovednými za danú činnosť.

Zistenia a závery

Vo fínskej stratégii kybernetickej bezpečnosti sa vymedzujú kľúčové ciele a politiky zamerané na riešenie výziev, ktorým čelí kybernetické prostredie, a zaistenie jeho fungovania. Vyvíjajú sa snahy o vykonávanie stratégie kybernetickej bezpečnosti pomocou programu vykonávania, ktorého postup sa každoročne hodnotí. Bezpečnostný výbor je orgán pre spoluprácu v rámci Ministerstva obrany, ktorý monitoruje a koordinuje vykonávanie stratégie kybernetickej bezpečnosti.

Účinnou organizáciou kybernetickej bezpečnosti je riadenie rizika, ktoré na to, aby bolo úspešné, vyžaduje účinné riadiace štruktúry a mechanizmy, ktoré začleňujú riadenie rizika do operácií na všetkých úrovniach organizácie. Podobne ako v mnohých iných krajinách ani Fínsko a jeho ústredná štátna správa nie sú sebestačné, pokiaľ ide

o zdroje kybernetickej ochrany. Počet právnych predpisov Európskej únie sa časom zvýšil a stali sa záväznejšími. Vo fínskej štátnej správe je zodpovednosť za kybernetickú ochranu decentralizovaná, pričom každý podnikový orgán zodpovedá za svoju vlastnú kybernetickú bezpečnosť. Prideľovanie úloh v súvislosti s povahou, rozsahom a vykonávaním možných porušení kybernetických zásad je v ústrednej štátnej správe zložité.

V dôsledku tejto zložitosti môže byť reakcia na anomáliu príliš pomalá, pričom nedostatočné financovanie obmedzuje vykonávanie fínskej stratégie kybernetickej bezpečnosti. Na základe kontrolných zistení dospel Národný kontrolný úrad k týmto záverom a vydal tieto odporúčania týkajúce sa organizácie kybernetickej bezpečnosti v ústrednej štátnej správe:

Operatívne riadenie rozsiahlych porušení kybernetickej bezpečnosti nebolo vymedzené

Plánovanie operatívneho riadenia rozsiahlych porušení kybernetickej bezpečnosti a rozdelenie súvisiacich úloh by mohlo umožniť rýchlejšie reakcie a vhodnú koordináciu a prideľovanie zdrojov na protiopatrenia. V rámci súčasného operačného modelu každá agentúra zodpovedá za svoju vlastnú kybernetickú ochranu. Nie sú však k dispozícii dostatočné odborné znalosti o kybernetickej ochrane, čo bráni vytvoreniu kybernetickej ochrany buď interne, alebo externým zabezpečením činností.

Niektoré ciele stratégie kybernetickej bezpečnosti neboli dosiahnuté

Program vykonávania fínskej stratégie kybernetickej bezpečnosti zlepšil kybernetickú ochranu. Niektoré ciele z prvého programu vykonávania sa nedosiahli, pretože úroveň snáh vo vzťahu k opatreniam sa líšila a nemohla sa zlepšiť centralizovaným spôsobom. Nový program vykonávania zahŕňal len opatrenia, v súvislosti s ktorými príslušné orgány a iní aktéri vyjadrili svoj záväzok. Záväzky a dostupné zdroje sú od seba navzájom závislé.

Primeranosť riešení financovania kybernetickej bezpečnosti nebola jasná

Rozdiely vo vývoji kybernetickej ochrany pramenili čiastočne z rozdielov vo výške zdrojov na vývoj, ktoré mali organizácie k dispozícii. V prepisoch o príprave štátneho rozpočtu ani v prípravnom procese sa nestanovili žiadne postupy, ktoré by zabezpečili, aby sa finančné prostriedky pridelili na najdôležitejšie ciele v rámci kybernetickej ochrany. Agentúry a inštitúcie zahŕňali rozpočtové prostriedky na kybernetickú bezpečnosť do rozpočtu ako bližšie neurčenú časť administratívnych výdavkov danej agentúry alebo inštitúcie. Opatrenia uvedené vo fínskej stratégii kybernetickej

bezpečnosti sa vykonávali len v takom rozsahu, v akom to umožňovali pridelené rozpočtové prostriedky.

Kybernetická ochrana by sa takisto mala zohľadňovať v rámci zmien organizácie IKT

Zmeny organizácie IKT ústrednej štátnej správy ovplyvňovali mechanizmy kybernetickej ochrany. Ukázalo sa, že vývoj kybernetickej bezpečnosti centrálne riadený centrom IKT Valtori je náročný. Existovali nedostatky v posudzovaní primeranosti praktických kybernetickobezpečnostných postupov a v zavádzaní nových mechanizmov.

Situačná informovanosť o kybernetickobezpečnostných operáciách by sa mala zlepšiť

Centrum pre kybernetickú bezpečnosť udržiavalo celoštátnu situačnú informovanosť o kybernetickej bezpečnosti. V čase auditu neexistovala povinnosť ohlasovať porušenia kybernetickej bezpečnosti Centru pre kybernetickú bezpečnosť. Situáciu by zlepšilo uloženie povinnosti organizáciám verejnej správy ohlasovať porušenia, ako aj zvýšenie rozsahu centralizovaných postupov na odhaľovanie porušení kybernetických zásad.

Na základe týchto vyjadrení Národný kontrolný úrad odporúča, aby Ministerstvo financií stanovilo a vykonávalo rozsiahly model operačného riadenia v prípade kybernetickobezpečnostných incidentov v rámci služieb IKT ústrednej štátnej správy. Ministerstvo financií by takisto malo zistiť, ako by sa mala zohľadňovať kybernetická bezpečnosť služieb, pokiaľ ide o financovanie služieb počas ich celého životného cyklu, a zlepšiť operatívnu situačnú informovanosť tým, že orgánom nariadi, aby porušenia kybernetických zásad nahlasovali Centru pre kybernetickú bezpečnosť. Odporučilo sa, aby centrum Valtori zlepšilo vykonávanie, hodnotenie a vývoj kybernetickobezpečnostných postupov a odhaľovanie porušení kybernetických zásad.

Následný audit skúmal to, ako sa vykonali odporúčania vydané počas auditu. Kontrolný úrad bol názoru, že Ministerstvo financií ako príslušný orgán pre vykonávanie odporúčaní neprijalo dostatočné opatrenia v reakcii na vydané odporúčania. Kybernetická bezpečnosť sa však vo Fínsku posilnila pomocou opatrení, ktoré prijali orgány iné ako Ministerstvo financií. Prebiehala zmena strategického riadenia kybernetickej bezpečnosti na riadiaci kybernetickobezpečnostný model. V návrhu rozpočtu na rok 2020 vláda navýšila rozpočtové prostriedky pre orgány ústrednej štátnej správy, ktoré zohrávajú kľúčovú úlohu v posilňovaní kybernetickej bezpečnosti. Okrem toho centrum Valtori prijímalo opatrenia v súlade s odporúčaniami Národného kontrolného úradu. Záverom Národný kontrolný úrad uviedol, že následný audit bol potrebný z dôvodu nevykonaných odporúčaní a že prebiehajúce zmeny mechanizmov kybernetickej bezpečnosti a digitálneho operačného prostredia a súvisiace riziká, ako

aj dôležitosť kybernetickej bezpečnosti pre financie ústrednej verejnej správy a spoločnosť odôvodňujú vykonanie úplne nového auditu v tejto oblasti.

Švédsko
Riksrevisionen

Zastaralé systémy IT – prekážka účinnej digitalizácie

Dátum uverejnenia: 2019

Hypertextový odkaz na správu: Zhrnutie správy (anglická verzia)
Správa (švédska verzia)

Typ a obdobie auditu

Typ auditu: Audit výkonnosti

Kontrolované obdobie: 2018 – 2019

Zhrnutie správy

Téma auditu

Zastaralé systémy IT kritické pre fungovanie predstavujú závažné riziko problémov s efektívnosťou, pretože nútia organizácie vynakladať úmerne viac zdrojov len na údržbu systému. Preto sa možno domnievať, že zastaralé systémy IT prinášajú so sebou vysoké riziko zlej správy verejných financií. Takisto so sebou prinášajú rozptýlenie inovatívnej kapacity agentúry, pokiaľ ide o vývoj nových systémov IT. Zo zastaralých systémov IT však nielenže vyplývajú riziká pre jednotlivé agentúry, ale problémy v jednej agentúre môžu mať vážne následky na jej schopnosť koordinovať operácie s inou agentúrou alebo so súkromnou zainteresovanou stranou. Zastaralé systémy IT sa takisto spájajú s rizikami z hľadiska informačnej bezpečnosti.

Vymedzenie hlavnej témy a auditu/audítorské otázky/kontext

Cieľom auditu bolo preskúmať výskyt zastaralých systémov IT v ústrednej štátnej správe a zistiť, či orgány a štátna správa prijali vhodné opatrenia, aby zabránili tomu, že tieto systémy IT budú prekážkou účinnej digitalizácie. Riešili sa tieto audítorské otázky:

- Prijali orgány vhodné opatrenia na riešenie problémov súvisiacich so zastaralými systémami IT?
- Prijala vláda vhodné opatrenia na riešenie problémov súvisiacich so zastaralými systémami IT?

Zistenia a závery

- Z auditu vyplynulo, že zastaralé systémy IT sa nachádzajú vo veľkom počte vládnych agentúr. Ďalej bol v mnohých agentúrach jeden alebo viac systémov IT kritických pre fungovanie zastaralý. Pokiaľ je švédskemu VKÚ známe, ide o novú informáciu a dovtedy si nikto neuvedomoval rozsah tohto problému v ústrednej štátnej správe. Približne 80 % agentúr uviedlo, že majú ťažkosti s udržiavaním úrovne informačnej bezpečnosti v jednom alebo vo viacerých svojich systémoch kritických pre fungovanie. Viac ako jeden z desiatich orgánov uviedol, že sa to vzťahuje na všetky systémy alebo na väčšinu z nich.
- Veľká časť kontrolovaných agentúr nepristupovala správnym spôsobom k vývoju a správe podpory IT. Nepoužívali existujúce nástroje na operačný vývoj, aby určili, ako môže podpora IT čo najlepšie prispievať k dosahovaniu cieľov kľúčových operácií. Veľkej časti kontrolovaných agentúr preto chýbal celkový opis toho, ako sú stratégie, operačné procesy a systémy prepojené. To zasa znamenalo, že mali problém analyzovať a porozumieť tomu, ako zmeny ovplyvňujú ciele organizácie, a preto bolo ťažšie stanoviť želanú situáciu v budúcnosti.
- Viac ako polovica orgánov uviedla, že neexistuje schválený model riešenia a prijímania rozhodnutí o ich systémoch IT od štádia vývoja systému až po postupné vyradenie, ktorý sa zvyčajne označuje ako riadenie životného cyklu. Podľa švédskeho VKÚ z toho vyplývalo, že riadenie životného cyklu sa nevykonáva štruktúrovaným a metodickým spôsobom. Takisto existovali nedostatky v činnosti v oblasti analýzy rizika a v schopnosti analyzovať náklady na IT na podrobnej úrovni potrebnej na prijímanie správnych rozhodnutí.

- Takmer v 60 % orgánov chýbali plány vývoja životného cyklu systému v prípade všetkých systémov s výnimkou jedného alebo niekoľkých systémov kritických pre fungovanie. Nedostatok plánov životného cyklu a inej plánovacej dokumentácie v mnohých agentúrach v kombinácii s nedostatkami v reálne vykonávanom riadení životného cyklu znamenal, že vo všeobecnosti nemožno povedať, že agentúry vedome a jasne pristupovali ku svojim systémom IT.
- Švédsky VKÚ zhodnotil, že zainteresovaným ministerstvám, a tým aj štátnej správe chýbali dostatočné vedomosti o výskyte, ako aj o následkoch zastaralých systémov IT.

Celkovým záverom bolo, že v čase auditu sa väčšine agentúr nepodarilo účinne zvládať problémy spojené so zastaralými systémami IT. Podľa švédskeho VKÚ bol tento problém natoľko vážny a rozšírený, že predstavoval prekážku pre pokračujúcu efektívnu digitalizáciu štátnej správy. Z auditu takisto vyplynulo, že štátnej správe chýbali znalosti o existencii a následkoch problémov zastaralých systémov IT. Štátna správa ďalej neprijala žiadne opatrenia na cielenejšie riešenie problému zastaralých systémov IT. Švédsky VKÚ preto zhodnotil, že nemožno usúdiť, že štátna správa prijala dostatočné opatrenia na zaistenie obmedzenia alebo odstránenia problémov.

Ďalšie správy v tejto oblasti

Názov správy: Uľahčenie začiatku podnikania – snahy verejnej správy o podporu digitálneho procesu (RiR 2019:14)

Hypertextový odkaz na správu: Zhrnutie správy (anglická verzia)
Správa (švédska verzia)

Dátum uverejnenia: 2019

Názov správy: Digitalizácia verejnej správy – jednoduchšia, transparentnejšia a účinná správa (RiR 2016:14)

Hypertextový odkaz na správu: Zhrnutie správy (anglická verzia)
Správa (švédska verzia)

Dátum uverejnenia: 2016

Názov správy: Činnosti v oblasti informačnej bezpečnosti v deviatich agentúrach (RiR 2016:8)

Hypertextový odkaz na správu: Zhrnutie správy (anglická verzia)
Správa (švédska verzia)

Dátum uverejnenia: 2016

Názov správy: Počítačová kriminalita – polícia a prokuratúry by mohli byť efektívnejšie (RiR 2015:21)

Hypertextový odkaz na správu: Zhrnutie správy (anglická verzia)
Správa (švédska verzia)

Dátum uverejnenia: 2015

Európska únia
Európsky dvor audítorov

Informačný dokument: Prekážky účinnej politiky v oblasti kybernetickej bezpečnosti

Dátum uverejnenia: 2018

Hypertextový odkaz na správu: Správa (23 jazykových verzií)

Typ a obdobie auditu

Typ auditu: Preskúmanie politiky

Kontrolované obdobie: apríl – september 2018

Zhrnutie správy

Téma preskúmania

Cieľom tohto informačného dokumentu, ktorý nie je audítorskou správou, bolo poskytnúť prehľad zložitej situácie EÚ v oblasti politiky kybernetickej bezpečnosti a určiť hlavné prekážky pre jej účinnú realizáciu. Informačný dokument sa venuje sieťovej a informačnej bezpečnosti, počítačovej kriminalite, kybernetickej obrane a dezinformáciám.

Analýza EDA sa zakladala na preskúmaní písomných, verejne dostupných úradných dokladov, pozičných dokumentoch a štúdiách tretích strán. Práca v teréne prebiehala od apríla do septembra 2018 a zohľadnil sa aj vývoj do decembra 2018. EDA svoju prácu doplnil prieskumom vo vnútroštátnych kontrolných úradoch členských štátov a rozhovormi s hlavnými zainteresovanými stranami spomedzi inštitúcií EÚ a zástupcov súkromného sektora.

Neexistuje nijaké štandardné vymedzenie pojmu „kybernetická bezpečnosť“. Vovšeobecnosti ide o všetky bezpečnostné záruky a opatrenia prijaté na ochranu informačných systémov a ich používateľov proti neoprávnenému prístupu, útoku a poškodeniu, ktorých cieľom je zabezpečenie dôvernosti, integrity a prístupnosti údajov. Kybernetická bezpečnosť zahŕňa kybernetickú prevenciu, odhaľovanie kybernetických útokov, reagovanie na ne a zaistenie nápravy. Incidenty môžu byť

úmyselné alebo neúmyselné a ich rozsah je napríklad od náhodného zverejnenia informácií po útoky na podniky a kritickú infraštruktúru, po krádež osobných údajov, či dokonca po zasahovanie do demokratických procesov.

Základným kameňom politiky EÚ je stratégia kybernetickej bezpečnosti z roku 2013, ktorej cieľom je dosiahnuť, aby digitálne prostredie EÚ bolo najbezpečnejším prostredím na svete, a zároveň ochraňovať základné hodnoty a slobody. Stratégia má päť hlavných cieľov: i) zvýšenie kybernetickej odolnosti; ii) zníženie počítačovej kriminality; iii) rozvoj politiky a spôsobilostí kybernetickej obrany; iv) rozvoj priemyselných a technologických zdrojov pre kybernetickú bezpečnosť a v) vytvorenie medzinárodnej politiky kybernetického priestoru v súlade s kľúčovými hodnotami EÚ.

Zistenia

Z dôvodu nedostatku spoľahlivých údajov bolo ťažké opísať účinky slabej prípravy na kybernetický útok. Hospodársky vplyv počítačovej kriminality sa medzi rokmi 2013 až 2017 päťnásobne zvýšil, pričom táto kriminalita postihla vlády a veľké aj malé spoločnosti. Tento trend sa odzrkadľuje v odhadovanom raste poistného pre prípad kybernetických útokov z 3 mld. EUR v roku 2018 na 8,9 mld. EUR v roku 2020. Hoci 80 % podnikov v EÚ v roku 2016 zaznamenalo aspoň jeden kybernetický bezpečnostný incident, miera uznania rizík je stále znepokojivo nízka. Znalosti o svojom vystavení kybernetickým hrozbám nemá 69 % spoločností v EÚ, alebo má o ňom iba základné znalosti, a 60 % nikdy neuskutočnilo odhad možných finančných strát. Podľa globálneho prieskumu by každá tretia organizácia radšej hackerom vyplatila výkupné, než by investovala do informačnej bezpečnosti.

EDA zaznamenal tieto zistenia:

- Ekosystém kybernetickej bezpečnosti v EÚ je komplexný a mnohovrstevný a týka sa veľkého množstva zainteresovaných strán. Spojiť všetky jeho nesúrodé časti je značne náročné.

- Európska únia sa plánuje stať najbezpečnejším online prostredím na svete. Dosiahnutie tejto ambície si vyžaduje značné úsilie všetkých zainteresovaných strán vrátane zdravého a dobre riadeného finančného základu. Číselné údaje sa ťažko získavajú, ale verejné výdavky EÚ na kybernetickú bezpečnosť sa odhadom pohybujú v rozpätí od jednej do dvoch miliárd EUR ročne. V porovnaní s tým výdavky federálnej vlády USA vyčlenené v rozpočte na rok 2019 predstavovali 21 mld. USD.

- V správe informačnej bezpečnosti ide o zavádzanie štruktúr a politík v záujme zabezpečenia dôverného charakteru údajov, ich integrity a dostupnosti. Nejde len o technický problém, správa si vyžaduje efektívne vedenie, spoľahlivé procesy a stratégie v súlade s organizačnými cieľmi.

- Členské štáty majú rôzne modely kybernetickej bezpečnosti a zodpovednosť za kybernetickú bezpečnosť v nich často býva rozdelená medzi množstvo subjektov. Tieto rozdiely by mohli prekážať spolupráci potrebnej na reakciu na rozsiahle, cezhraničné incidenty a na výmenu spravodajských informácií o hrozbách na vnútroštátnej úrovni a ešte viac na úrovni EÚ.

- Navrhnutie účinnej reakcie na kybernetické útoky je zásadné na ich zastavenie v čo najskoršej fáze. Obzvlášť je dôležité, aby kľúčové odvetvia, členské štáty a inštitúcie EÚ boli schopné pohotovo reagovať koordinovaným spôsobom. Na to je dôležité včasné odhalenie.

Odporúčania

Z prehľadu EDA vyplýva, že na zabezpečenie primeranej zodpovednosti a hodnotenia je potrebný prechod na kultúru výkonnosti, ktorej súčasťou sú hodnotiace postupy. Pretrvávajú isté medzery v práve a členské štáty netransponovali existujúce právne predpisy dôsledne. Táto skutočnosť môže sťažiť to, aby právne predpisy dosiahli svoj plný potenciál.

Ďalší zistený problém sa týka zosúladenia úrovne investícií so strategickými cieľmi, čo si vyžaduje zvýšiť úrovne investícií a ich vplyv. To je náročnejšie v prípade, keď EÚ a jej členské štáty nemajú jasný prehľad o výdavkoch EÚ na kybernetickú bezpečnosť. Nahlásené boli aj obmedzenia týkajúce sa primeraného zabezpečovania zdrojov pre agentúry EÚ zaoberajúce sa oblasťou kybernetiky, ako aj ťažkosti pri lákaní talentov a ich udržaní.

Akronymy a skratky

CERT-EU: tím reakcie na núdzové počítačové situácie

COBIT: kontrolné ciele pre informačné a súvisiace technológie

COVID-19: ochorenie spôsobené koronavírusom, ktorý sa objavil v roku 2019

cPPP: zmluvné verejno-súkromné partnerstvo

CSIRT: jednotka pre riešenie počítačových bezpečnostných incidentov

DDoS: distribuované odmietnutie služieb

EC3: Európske centrum boja proti počítačovej kriminalite pri Europole

EDA: Európsky dvor audítorov

ENISA: Agentúra Európskej únie pre kybernetickú bezpečnosť

EOA: Európska obranná agentúra

ESRB: Európsky výbor pre systémové riziká

ESVČ: Európska služba pre vonkajšiu činnosť

EŠIF: Európske štrukturálne a investičné fondy

EÚ: Európska únia

EUROPOL: Agentúra Európskej únie pre spoluprácu v oblasti presadzovania práva

GDPR: všeobecné nariadenie o ochrane údajov

HDP: hrubý domáci produkt

HR: ľudské zdroje

IKT: informačné a komunikačné technológie

IoT: internet vecí

ISACA: Asociácia auditu a kontroly informačných systémov

ISF-P: Fond pre vnútornú bezpečnosť – polícia

IT: informačné technológie

MERS: blízkovýchodný respiračný syndróm

NATO: Organizácia Severoatlantickej zmluvy

NKI: najvyššie kontrolné inštitúcie

NPE: Nástroj na prepájanie Európy

NSKB: národná stratégia kybernetickej bezpečnosti

PDE: program Digitálna Európa

PESCO: rámec stálej štruktúrovanej spolupráce

RDP: protokol RDP

SARS: ťažký akútny respiračný syndróm

SBOP: spoločná bezpečnostná a obranná politika

smernica NIS: smernica o kybernetickej bezpečnosti

UK: Spojené kráľovstvo

URL: jednotná adresa zdroja

USA: Spojené štáty americké

VFR: viacročný finančný rámec

VKÚ: vnútroštátny kontrolný úrad

Slovník

5G: je technická norma piatej generácie pre širokopásmové siete buniek, ktorú začali spúšťať mobilní operátori na celom svete v roku 2019. Je plánovaným nástupcom sietí 4G, ktoré zabezpečujú pripojiteľnosť väčšiny súčasných mobilných telefónov. Vyššia rýchlosť sa dosahuje čiastočne použitím rádiových vĺn s vyššou frekvenciou než v predchádzajúcich mobilných sieťach.

Advér: škodlivý softvér, ktorý zobrazuje reklamné nápisy alebo automaticky otvárané okná, ktorý obsahuje kód na sledovanie správania obetí na internete.

Bezpečnosť siete: podmnožina údajov na ochranu kybernetickej bezpečnosti odoslaných zo zariadení na tej istej sieti, ktorých cieľom je zabezpečiť, že nedôjde k zachyteniu alebo zmene informácií.

Biometrické údaje (biometria): fyzické (ako napríklad odtlačky prstov alebo oči) alebo behaviorálne výpočty súvisiace s ľudskými črtami. Overovanie sa v počítačovej vede používa ako forma identifikácie a kontroly vstupu.

Bitcoin: digitálna alebo virtuálna mena vytvorená v roku 2009, ktorá využíva partnerskú technológiu na uskutočňovanie okamžitých platieb.

Cloud computing: poskytovanie zdrojov na požiadanie a zdrojov výpočtovej techniky, ako sú napríklad úložiská, výpočtové kapacity alebo kapacity na výmenu údajov, cez internet prostredníctvom poskytovania hostiteľských služieb na vzdialených serveroch.

Červy: počítačový červ je samostatný škodlivý počítačový program, ktorý sa sám reprodukuje, aby sa rozšíril na ďalšie počítače. Na svoje šírenie často používa počítačovú sieť, pričom sa opiera o chyby v zabezpečení cieľového počítača, aby k nemu získal prístup.

Dezinformácia: overiteľne nepravdivá alebo zavádzajúca informácia, ktorá je vytvorená, prezentovaná a šírená na účely hospodárskeho zisku alebo zámerného zavádzania verejnosti a ktorá môže poškodiť verejný záujem.

Digitalizácia: Proces premeny informácií na digitálny formát, v ktorom je informácia usporiadaná v bitoch. Výsledkom je zachytenie objektu, obrázku, zvuku, dokumentu alebo signálu generovaním radu čísiel, ktoré opisujú samostatný súbor bodov alebo vzoriek.

Digitálna platforma: prostredie na interakciu najmenej dvoch rôznych skupín, pričom jednou sú zvyčajne dodávatelia a druhou spotrebitelia/používatelia. Môže ním byť hardvér alebo operačný systém, dokonca aj internetový prehliadač a súvisiace

aplikačné programovacie rozhrania alebo základný softvér, pokiaľ sa ním vykonáva programový kód.

Digitálne aktívum: všetko, čo existuje v digitálnom formáte, vo vlastníctve súkromnej osoby alebo spoločnosti, na čo sa vzťahuje právo na používanie (napr. obrázky, fotografie, videá, súbory obsahujúce text atď.).

Digitálny obsah: všetky údaje – ako je text, zvuk, obrázky alebo video – uložené v digitálnom formáte.

Distribuované odmietnutie služieb (útok DDoS): kybernetický útok, ktorý bráni oprávneným používateľom v prístupe k službe alebo zdrojom online tým, že túto službu či zdroj zaplaví takým množstvom požiadaviek, ktoré prevyšuje jej kapacity.

Dôvernosť: ochrana informácií, údajov alebo aktív pred neoprávneným prístupom alebo zverejnením.

Ekosystém kybernetickej bezpečnosti: komplexná komunita navzájom prepojených a komunikujúcich zariadení, údajov, sietí, osôb, procesov a organizácií a prostredie procesov a technológií, ktoré ovplyvňujú a podporujú túto vzájomnú prepojenosť a komunikáciu.

Etický hacker: osoba (odborník na počítačovú bezpečnosť), ktorá prenikne do počítačovej siete s cieľom otestovať alebo zhodnotiť jej bezpečnosť, a nie so zlým úmyslom alebo s úmyslom spáchať trestný čin.

Hacker: Osoba, ktorá používa počítač, vytváranie sietí alebo iné zručnosti na získanie neoprávneného prístupu k údajom, počítačovým systémom alebo sieťam.

Hybridná hrozba: prejav nepriateľského zámeru uskutočňovaný nepriateľmi s použitím kombinácie konvenčných a nekonvenčných metód boja (t. j. vojenských, politických, hospodárskych a technologických metód) v mocnom úsilí o dosiahnutie svojich cieľov.

Informačná bezpečnosť: skupina procesov a nástrojov, ktoré chránia fyzické a digitálne údaje pred neoprávneným prístupom, použitím, zverejnením, narušením, úpravou, zaznamenaním alebo zničením.

Integrita: ochrana proti nezákonnej úprave alebo zničeniu informácií a zaručenie ich pravosti.

Internet vecí: sieť každodenných predmetov vybavených elektronikou, softvérom a snímačmi, prostredníctvom ktorých môžu komunikovať a uskutočňovať výmenu údajov cez internet.

Kritická infraštruktúra: fyzické zdroje, služby a zariadenia, ktorých narušenie alebo zničenie budú mať závažný vplyv na fungovanie hospodárstva a spoločnosti.

Kritický informačný systém: akýkoľvek informačný systém, existujúci alebo plánovaný, ktorý sa považuje za kritický pre efektívne a účinné fungovanie organizácie.

Kryptomena: digitálny prostriedok, ktorý sa vydáva a vymieňa s použitím šifrovacích techník a nezávisle od centrálnej banky. Členovia virtuálneho spoločenstva ho prijímajú ako platobný prostriedok.

Kybernetická bezpečnosť (kybernetická ochrana): všetky bezpečnostné záruky a opatrenia prijaté na ochranu systémov IT a ich údajov proti neoprávnenému prístupu, útoku a poškodeniu, ktorých cieľom je zabezpečenie prístupnosti, dôvernosti a integrity údajov.

Kybernetická diplomacia: Využívanie diplomatických zdrojov a výkon diplomatických funkcií na zabezpečenie národných záujmov v oblasti kybernetického priestoru. V plnej alebo v čiastočnej miere ju vedú diplomati, ktorí sa stretávajú v bilaterálnych formátoch (ako napríklad dialóg USA – Čína) alebo v multilaterálnych fórach (ako napríklad OSN). Okrem tradičnej diplomatickej činnosti diplomati takisto spolupracujú s rôznymi neštátnymi subjektmi, ako sú riaditelia internetových spoločností (ako napríklad Facebook alebo Google), podnikatelia v oblasti technológií alebo organizácie občianskej spoločnosti. Diplomacia môže takisto zahŕňať posilňovanie postavenia potláčaných hlasov v iných krajinách prostredníctvom technológie.

Kybernetická hrozba: Úmyselný čin, ktorého cieľom je poškodiť údaje, ukradnúť údaje alebo vo všeobecnosti narušiť digitálny život.

Kybernetická obrana: podmnožina kybernetickej bezpečnosti zameraná na obranu kybernetického priestoru vojenskými a inými primeranými prostriedkami s cieľom dosiahnuť vojensko-strategické ciele.

Kybernetická odolnosť: schopnosť zabrániť kybernetickým útokom a incidentom, pripraviť sa na ne, odolať im a zotaviť sa po nich.

Kybernetická špionáž: kybernetická špionáž je činnosť alebo postup zameraný na získavanie tajomstiev a informácií bez povolenia alebo vedomia držiteľa informácií

od súkromných osôb, konkurentov, súperov, skupín, vlád a nepriateľov s cieľom získať osobnú, ekonomickú, politickú alebo vojenskú výhodu pomocou internetu, sietí alebo jednotlivých počítačov.

Kybernetický incident: udalosť, ktorá priamo alebo nepriamo poškodzuje alebo ohrozuje odolnosť a bezpečnosť systému IT a údajov, ktoré sa v tomto systéme spracúvajú, ukladajú alebo prenášajú.

Kybernetický priestor: nehmotné globálne prostredie, v ktorom dochádza k online komunikácii medzi ľuďmi, softvérom a službami prostredníctvom počítačových sietí a technologických zariadení.

Kybernetický útok: pokus o oslabenie alebo zničenie dôvernosti, integrity a prístupnosti údajov alebo počítačového systému prostredníctvom kybernetického priestoru.

Malvér: škodlivý softvér. Počítačový program navrhnutý tak, aby poškodzoval počítače, servery alebo siete.

Opravy: poskytnutie súboru zmien v softvéri na jeho aktualizáciu, opravu alebo zlepšenie vrátane odstránenia bezpečnostných chýb.

Osobné údaje: informácie týkajúce sa identifikovateľnej osoby.

Phishing: metóda posielania elektronickej pošty, ktorá vyvoláva zdanie, že pochádza z dôveryhodného zdroja, s cieľom podvodom prinútiť prijímateľov k tomu, aby klikli na škodlivý hypertextový odkaz alebo poskytli svoje osobné údaje.

Počítačová kriminalita: rôzne trestné činnosti, pri ktorých sa počítače a systémy informačných technológií buď používajú ako primárne nástroje, alebo slúžia ako primárne ciele. Medzi tieto činnosti patria: tradičné trestné činy (napr. podvod, falšovanie a krádež totožnosti), trestné činy súvisiace s obsahom (napr. online distribúcia detskej pornografie alebo podnecovanie k rasovej nenávisti) a trestné činy špecifické pre počítače a informačné systémy (napr. útok na informačné systémy, odmietnutie služby, škodlivý softvér alebo ransomvér).

Porušenie ochrany údajov: úmyselné alebo neúmyselné zverejnenie zabezpečených alebo súkromných/dôverných informácií v nedôveryhodnom prostredí.

Poskytovateľ digitálnych služieb: každý, kto poskytuje jednu alebo viaceré z týchto troch druhov digitálnych služieb – online trh, internetové vyhľadávače, služby cloud computing.

Prevádzkovateľ základných služieb: verejný alebo súkromný subjekt, ktorý poskytuje službu, ktorá má zásadný význam z hľadiska zachovania kľúčových spoločenských a hospodárskych činností.

Prístupnosť: zabezpečenie včasného a spoľahlivého prístupu k informáciám a ich používania.

Protokol RDP: technická norma (vydaná spoločnosťou Microsoft) na vzdialené používanie stolového počítača. Používatelia stolového počítača na diaľku môžu získať prístup k svojej pracovnej ploche, otvárať a upravovať súbory a používať aplikácie, ako keby sedeli za svojím stolovým počítačom.

Ransomvér: škodlivý softvér, ktorý obetiam bráni v prístupe do počítačového systému alebo znemožňuje čitateľnosť súborov, obvykle prostredníctvom šifrovania. Útočník následne zvyčajne obeť vydiera tým, že jej odmietne obnoviť prístup do chvíle, kým obeť nezaplatí výkupné.

Sabotáž: činnosť zameraná na úmyselné zničenie, poškodenie alebo blokovanie, najmä s cieľom získať politickú alebo vojenskú výhodu.

Sociálne inžinierstvo: v oblasti informačnej bezpečnosti ide o spôsob psychologickej manipulácie, ktorej cieľom je podvodom prinútiť ľudí k tomu, aby vykonali požadovanú akciu alebo prezradili informácie dôvernej povahy.

Spracovanie údajov: vykonávanie operácií s údajmi, najmä cez počítač, s cieľom získať, zmeniť alebo klasifikovať informácie.

Spyvér: softvér so škodlivým správaním, ktorého cieľom je získať informácie o osobe alebo organizácii a odoslať tieto informácie inému subjektu spôsobom, ktorý spôsobuje používateľovi škodu, napríklad tým, že porušuje ochranu jeho súkromia alebo ohrozuje bezpečnosť jeho zariadenia.

Šifrovanie: prevedenie čitateľných informácií na nečitateľný kód v záujme ochrany šifrovaných informácií. Na prečítanie informácií musí mať používateľ prístup k súkromnému kľúču alebo heslu.

Trójsky kôň: typ škodlivého kódu alebo softvéru, ktorý vyzerá legitímne, ale môže získať kontrolu nad vaším počítačom. Cieľom trójskeho koňa je poškodiť, narušiť, ukradnúť údaje alebo vo všeobecnosti spôsobiť škodu na vašich údajoch alebo sieti.

Údaje o prístupe: informácie o prihlásení sa používateľa do služby a odhlásení sa z nej, ako je čas, dátum a IP adresa.

Umelá inteligencia: simulácia ľudskej inteligencie v strojoch, ktoré sú naprogramované tak, aby mysleli ako ľudia a napodobovali ich činnosť; akýkoľvek stroj, ktorý má črty spojené s ľudskou mysľou, ako napríklad schopnosť učiť sa alebo riešiť problémy.

Útoky typu Advanced Persistent Threat: útok, pri ktorom neoprávnený používateľ získa prístup do systému alebo siete a zostane tam dlhší čas bez toho, aby bol odhalený. Osobitne nebezpečné pre podniky, keďže hackeri majú nepretržitý prístup k citlivým podnikovým údajom, vo všeobecnosti však nespôsobujú poškodenie sietí spoločnosti ani miestnych zariadení. Cieľ – krádež údajov.

Vektorizácia textu: proces premeny slov, viet alebo celých dokumentov na číselné vektory tak, aby ich mohli využiť algoritmy strojového učenia.

Volebná infraštruktúra: patria sem informačné systémy a databázy kampaní, citlivé informácie o kandidátoch, systémy na registráciu voličov a systémy riadenia.

Vysokovýkonná výpočtová technika: Schopnosť spracúvať údaje a vykonávať zložité výpočty veľkou rýchlosťou.

Webové útoky: definovaní používatelia veria, že citlivé osobné údaje, ktoré odhaľujú na webovej stránke, zostanú súkromné a zabezpečené. Neoprávnené vniknutie (útok) môže znamenať, že môže dôjsť k zverejneniu informácií o ich kreditnej karte, sociálnom zabezpečení alebo zdravotných údajov, čo môže mať závažné následky.

Zariadenia verejných služieb: všetky stĺpy, veže, vzdušné alebo podzemné privádzače, všetky ostatné podporné alebo oporné štruktúry a všetky výkopy spolu s príslušenstvom umožňujúce dodávku alebo distribúciu elektriny, telefonického, telegrafného a káblového prenosu alebo signálovej služby alebo všetkých podobných služieb.

Obráťte sa na EÚ

Osobne
V rámci celej EÚ existujú stovky informačných centier Europe Direct. Adresu centra najbližšieho k vám nájdete na tejto webovej stránke: https://europa.eu/european-union/contact_sk.

Telefonicky alebo e-mailom
Europe Direct je služba, ktorá odpovedá na vaše otázky o Európskej únii. Túto službu môžete kontaktovať:
— prostredníctvom bezplatného telefónneho čísla: 00 800 6 7 8 9 10 11 (niektorí operátori môžu tieto hovory spoplatňovať),
— prostredníctvom štandardného telefónneho čísla: +32 22999696, alebo
— e-mailom na tejto webovej stránke: https://europa.eu/european-union/contact_sk.

Vyhľadávanie informácií o EÚ

Online
Informácie o Európskej únii sú dostupné vo všetkých úradných jazykoch Európskej únie na webovej stránke Europa: https://europa.eu/european-union/index_sk.

Publikácie EÚ
Publikácie EÚ, bezplatné alebo platené, si môžete stiahnuť alebo objednať z kníhkupectva na webovej stránke https://publications.europa.eu/sk/publications. Ak chcete získať viac než jeden výtlačok bezplatných publikácií, obráťte sa na službu Europe Direct alebo vaše miestne informačné centrum (pozri https://europa.eu/european-union/contact_sk).

Právo EÚ a súvisiace dokumenty
Prístup k právnym informáciám EÚ vrátane všetkých právnych predpisov EÚ od roku 1952 vo všetkých úradných jazykoch nájdete na webovej stránke EUR-Lex: https://eur-lex.europa.eu.

Otvorený prístup k údajom z EÚ
Portál otvorených dát EÚ (http://data.europa.eu/euodp/sk) poskytuje prístup k súborom dát z EÚ. Dáta možno stiahnuť a opätovne použiť bezplatne na komerčné aj nekomerčné účely.

Contact Committee

Kontaktný výbor

najvyšších kontrolných inštitúcií Európskej únie