Medzinárodná kybernetická kriminalita, riziko a preventívne opatrenia pre Európsku úniu

Autori:

Jana Müllerová[1] & Eleonóra Benčíková[2]

Abstrakt

Vedecká štúdia je súčasťou vedecko-výskumnej úlohy Grantovej agentúry Akadémie Aurea č. GA/14/20192 s názvom Analýza právnej úpravy v oblasti zaistenia vnútornej bezpečnosti a verejného poriadku v Českej republike a na Slovensku.

Štúdia sa zaoberá témou kybernetickej bezpečnosti a právnymi možnosťami jej zvýšenia. Štatistické ukazovatele zo štúdií uskutočnených v USA poukazujú na enormne rastúci trend a gigantické straty, vrátane dominantného zneužívania kryptomien na kriminálne aktivity. Autori rozoberajú systém právnych riešení boja proti počítačovej kriminalite vo Francúzsku, ako vedúcej krajine v implementácii opatrení na ochranu IT v rámci EÚ. Francúzsky systém je základným základom pre implementáciu celoeurópskych pravidiel boja proti kybernetickej bezpečnosti. Na bežných príkladoch sa diskutuje o otázkach individuálnej ochrany pred kybernetickými hrozbami, ako aj o podpore zo strany vládnych agentúr.

Keywords: *Kybernetická kriminalita, kybernetický priestor, prevencia rizík, globálna bezpečnosť, medzinárodné právo kybernetickej bezpečnosti*

Úvod

Existujú dva typy digitálnej kriminality: činy, pri ktorých je digitálna technológia prostriedkom, a tie, ktoré sú zamerané na bezpečnosť informačného systému. Najčastejšie kybernetické útoky majú rôzne podoby ako krádež identity či prezidentský podvod, phishing na odcudzenie súkromných údajov alebo ransomvér, ktorý blokuje prístup do informačného systému. Najprepracovanejšie útoky idú tak ďaleko, že zničia alebo znefunkčnia produkčný nástroj. Je

[1] prof. Ing. Jana Mullerova, PhD., Akadémia Policajného zboru v Bratislave, Sklabinská 1, 835 17 Bratislava, Slovenská republikaj ana.mullerova@akademiapz.sk
[2] Mgr. Ing. Eleonóra Benčíková, PhD., MPH, MHA, Univerzita Tomáš Bati ve Zlíně, Fakulta logistiky a krizového řízení, Studentské nám. 1532, 686 01 Uherské Hradiště, Česká republika bencikova@utb.cz

dôležité pochopiť, že počítačová kriminalita je čoraz viac dielom organizovaných a štruktúrovaných sietí na medzinárodnej úrovni.[3]

V USA, ktoré boli v roku 2021 základom pre mnohé z najškodlivejších a najrozsiahlejších kybernetických útokov, má takmer polovica opýtaných organizácií (47 %) zavedenú stratégiu kybernetickej odolnosti. Saudská Arábia, Nemecko a Dánsko nezaostávajú (44 %, 43 % a 42 %, Krajiny ako Švédsko a Holandsko nebezpečne zaostávajú, pričom len približne jedna zo štyroch spoločností (26 % a 21 %) spoločností už implementovala stratégiu kybernetickej odolnosti.[4]

1. Hrozby a trendy počítačovej kriminality v USA

Teroristické skupiny dokázali na boj využiť kyberpriestor. Považovali to za spôsob, ako vyvážiť pomer síl vo svoj prospech, keďže internet im umožňuje vykonávať rozsiahle ofenzívy s obmedzenými prostriedkami. Vďaka digitálnemu nástroju sa im teda podarilo získať finančné prostriedky, naverbovať bojovníkov alebo hacknúť webové stránky na propagandistické účely.

Úrady sa však teraz obávajú útokov väčšieho rozsahu, ako je prevzatie strategickej infraštruktúry. Vo februári 2017 Bezpečnostná rada Organizácie Spojených národov prijala rezolúciu, v ktorej vyzýva štáty, aby boli pripravené účinne reagovať na útoky na kritickú infraštruktúru..

Dôsledky kybernetického útoku

Môžu byť katastrofálne. Kybernetické útoky vedú najmä k finančným stratám, ale aj k stratám dát a v najvážnejších prípadoch až k paralýze spoločnosti. Nesmieme zanedbávať imidžové efekty a degradáciu dobrého mena značky. Jeden údaj vyjadruje závažnosť tohto javu: 80 % spoločností, ktoré sa stali obeťami ransomvéru, zaniká do 12 mesiacov.

Štúdia DataProt ponúka rozsiahlu štatistiku americkej počítačovej kriminality:[5]

• 6 biliónov USD – škody, ktoré počítačová kriminalita spôsobila v roku 2021.

• Prevažná väčšina (74 %) útokov sa zameriava na finančný sektor.

• V roku 2023 bude narušených 33 miliárd účtov.

---

[3] Müllerová, J. & Sisulak, S. Criminality software control tools of environmental crime. 2020
[4] Mimecast. Confronting the new wave of cyberattacks - The State of Email Security 2022. www.mimecast.com
[5] Vojinovic I., More Than 70 Cybercrime Statistics - A $6 Trillion Problem https://dataprot.net/statistics/cybercrime-statistics/

• Počet útokov ransomvéru sa v roku 2018 zvýšil o 350 %.

• 97,2 % malvéru, ktorý bol zablokovaný v roku 2018, bolo zameraných na počítače a notebooky so systémom Microsoft Windows.

• Vyhrážky sa stávajú častejšími v 68 % prípadov, keď obeť sexuálneho vydierania vyhovie požiadavkám.

• 59 % Američanov uvádza, že zažili počítačovú kriminalitu alebo sa nejakým spôsobom dostali do rúk počítačového hackera.

• 70 % malých podnikov je úplne nepripravených na kybernetický útok.

• 88 % profesionálnych hackerov dokáže infiltrovať vytipovanú organizáciu do 12 hodín.

Štatistiky tiež tvrdia, že do roku 2021 bolo 70 % transakcií s kryptomenami použitých na nelegálnu činnosť. Transakcie s kryptomenami sú anonymné, čo z nich robí dokonalý spôsob podpory trestnej činnosti. Podľa štúdie z roku 2018, ktorú zverejnila Univerzita v Sydney (Austrália), nezákonné bitcoinové transakcie sú na rovnakej úrovni ako americký a európsky trh s nelegálnymi drogami – 75 miliárd dolárov ročne. Crypto eliminuje papierové stopy špinavých peňazí. Niet divu, že je to hlavná mena požadovaná hackermi ransomvéru.

Je to enormné a neustále sa zvyšuje: každý rok v priemere o 22 %. Minulý rok bolo vo Francúzsku hlásených 100 000 trestných činov a prvé obdobie zadržiavania, minulú jar, poznačené zvýšeným využívaním digitálnych technológií, zaznamenalo päťnásobný nárast útokov. A opäť, toto je len špička ľadovca, keďže sa odhaduje, že na každý 1 nahlásený incident pripadá 267 spáchaných. Nie všetky spoločnosti deklarujú, že sú obeťami kybernetického útoku, a nie všetky si to uvedomujú: napríklad odhalenie narušenia automatizovaného spracovania údajov trvá v priemere 197 dní a náprava 69 dní. V roku 2021 sa prostredie kybernetických hrozieb v USA stalo zradnejším, nie menej. Vzhľadom na to, že počet verejne nahlásených únikov údajov prudko prekonal minuloročný celkový počet, rok 2021 sa zdá byť najhorším rokom v histórii kybernetickej bezpečnosti.

Najväčším vinníkom bol phishing, pričom 36 % porušení údajov bolo prinajmenšom čiastočne spôsobené ukradnutými povereniami zamestnancov prostredníctvom phishingového útoku2, z ktorých 96 % prebieha prostredníctvom e-mailu. Ransomvér je tiež šialený. Podľa posledných správ ohromujúcich 84 % U.S. organizácie za posledných 12 mesiacov nahlásili phishing alebo

ransomvérové útoky a priemerná platba za ransomvér sa počas prvého polroka 2021 vyšplhala na 570 000 USD, oproti 312 000 USD v roku 2020.[6]

Spoločnosti predstavujú 57 % z celkového počtu porušení a administratívy 7 %. Jednotlivci sú tiež hlavnými cieľmi a ako takí predstavujú pre spoločnosti miesto zraniteľnosti, najmä s rozvojom práce na diaľku a väčšou priepustnosťou profesionálnej a súkromnej sféry. Hlavnými sektormi sú najmä obrana, financie, energetika a zdravotníctvo.

2. Prevencia kybernetického ohrozenia a reakcia

Francúzska národná agentúra ANSSI [7] navrhuje prístup podľa typológie rizika s cieľom vždy čo najpresnejšie prispôsobiť svoju reakciu. Agentúra vyvinula digitálnu pyramídu riadenia rizík s 3 hlavnými kategóriami kybernetických útokov. Rozsiahle, necielené útoky, ktoré sa týkajú každého, si vyžadujú jednoduché reakcie, ktoré uplatňujú základné princípy bezpečnosti informačných systémov. Ransomvérové útoky, ktoré sú trochu prepracovanejšie, vyžadujú implementáciu skutočného obranného systému. Nakoniec, na samom vrchole pyramídy sú útoky na strategické ciele: v tomto prípade, keď sa incidentu nedá vyhnúť, musíte byť pripravení reagovať scenármi, ktoré obmedzia dopad a zabezpečia kontinuitu podnikania. Základom zostáva individuálna prevencia užívateľov.

ANSSI a CGPME[8] vydali praktickú príručku, v ktorej uvádzajú 12 základných pravidiel na zabezpečenie digitálneho zariadenia Ak neexistuje nulové riziko, ostražitosť v súvislosti s heslami a pravidelná aktualizácia informačného systému vám umožní vyhnúť sa 90 až 95 % nepríjemných prekvapení súvisiacich s prehliadaním internetu. Medzi základnými zásadami je aj mnoho zdravých pravidiel týkajúcich sa používania správ, online platieb alebo súkromného používania internetu a sociálnych sietí.

Implementácia účinného riadenia rizík

Malo by sa to uskutočniť tak, že sa predvídajú a poskytnú sa prostriedky na účinnú ochranu. Ide o technickú aj ľudskú záležitosť. ANSSI ponúka niekoľko kníh, ktoré majú spoločnostiam pomôcť zlepšiť riadenie rizík: príručku so 42 základnými hygienickými opatreniami na

---

[6] Mimecast. Confronting the new wave of cyberattacks - The State of Email Security 2022. www.mimecast.com

[7] Agence nationale de la sécurité des systèmes d'information - ANSSI - National Cybersecurity Agency of France

[8] Confédération générale des petites et moyennes entreprises

posilnenie bezpečnosti informačných systémov,[9] a komplexnejší dokument[10] na vytvorenie stratégie v štyroch krokoch:

1. Meranie digitálneho rizika;
2. Pochopenie digitálneho rizika a organizácia;
3. Budovanie bezpečnostných základov;
4. Riadenie digitálneho rizika a zvyšovanie kybernetickej bezpečnosti.

V prípade rozsiahleho útoku na informačný systém spoločnosti je pravdepodobnosť úniku osobných údajov pomerne vysoká. V rámci európskeho nariadenia RGPD je manažér právne zodpovedný za ochranu svojho informačného systému. Na túto tému existuje príručka CNIL so 17 opatreniami.

K dispozícii je taktiež poistné krytie, ktoré môže byť užitočné na riešenie krízy a obmedzenie jej škôd, alebo dokonca môže pomôcť spoločnosti získať zrelosť prostredníctvom minimálnych preventívnych opatrení. Skutočnosť, že sa človek poistí, ho však nezbavuje povinnosti zaviazať sa k skutočnému prístupu ku kybernetickej bezpečnosti.

V prípade kybernetického útoku ho najprv nahláste a podajte sťažnosť. Hovoríme o trestných činoch spáchaných organizáciami a práve súdne vyšetrovanie umožňuje ich zadržanie. Zlatým pravidlom je nikdy nehrať hru kyberzločinca. Napríklad v prípade ransomvéru by ste nikdy nemali platiť za obnovenie svojich údajov, čím riskujete podporu tohto javu.

Kybernetická bezpečnosť

Kybernetický priestor možno definovať ako globálne bojisko, kde komunikačný priestor otvorený prepojením všetkých počítačov prostredníctvom internetu. Zahŕňa verejný (blog) aj súkromný priestor (e-mail, firemný intranet, smart spotrebiče). Je to priestor, v ktorom sa uplatňujú kybernetické hrozby. Zvláštnosťou kybernetického priestoru je zrušenie vzdialeností a štátnych hraníc. Vzhľadom na svoju globálnu povahu kybernetická hrozba narúša tradičné kritériá bezpečnosti. Kybernetická bezpečnosť zabezpečuje, aby sa údaje spravovali v optimálnych a bezpečných podmienkach. Umožňuje ochranu informačných systémov a údajov v obehu pred tzv. kybernetickými zločincami. Počítačové zručnosti, ktoré získali zlomyseľné osoby, predstavujú riziko, ktoré by sa nemalo brať na ľahkú váhu. Bezpečnosť IT sa týka

[9] https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique
[10] https://www.ssi.gouv.fr/guide/maitrise-du-risque-numerique-latout-confiance/)

všetkých profesií, od inštalácie antivírusového softvéru až po konfiguráciu serverov a stráženie dátových centier a kancelárií.

Okrem kybernetických útokov umožňuje kybernetická bezpečnosť zaviesť medzi zamestnancami procesy na zavedenie správnych postupov. Ľudské chyby sú skutočným zdrojom úniku údajov. Zvyšovanie povedomia tímov o problematike phishingu alebo krádeže identity je dôležitou súčasťou politiky IT bezpečnosti.

Mechanizmy kybernetickej bezpečnosti zahŕňajú:

- identifikačné procesy

- šifrovanie údajov a spojení,

- procesy monitorovania a merania zavedených mechanizmov,

- neustála aktualizácia softvéru,

- zavedenie zariadení umožňujúcich rýchle obnovenie citlivých údajov v prípade technických problémov,

Kybernetická bezpečnosť zahŕňa všetky prostriedky na zabezpečenie ochrany a integrity citlivých alebo iných údajov v rámci digitálnej infraštruktúry. Je to špecializácia v rámci profesií informačných systémov. Pojem kybernetická bezpečnosť nadobúda čoraz väčší význam v dôsledku digitálnej transformácie spoločností, ktoré vo veľkej miere využívajú IT nástroje a komunikáciu prostredníctvom internetu. Na kybernetickej bezpečnosti sa podieľajú subjekty veľmi rôzneho postavenia a veľkosti. Sú tu krajiny, ich verejná správa vrátane krízového manažmentu a ich ozbrojené sily; hospodárske subjekty od malých a stredných podnikov až po nadnárodné spoločnosti.

Zvláštnosťou kybernetického priestoru je rozmazanie tradičných kritérií moci. Digitálni giganti tak majú často akčné kapacity porovnateľné s akčnými kapacitami štátov. Podobne aj izolovaný jednotlivec môže sám ohroziť počítačové systémy veľkej spoločnosti alebo štátu. Motivácia týchto kybernetických útokov je najmä ekonomická a politická.

Hospodárske a politické záujmy

Krádež peňazí od súkromnej osoby alebo spoločnosti (napríklad prostredníctvom falošných e-mailov, ktoré ich nabádajú, aby poskytli svoje bankové identifikačné údaje); kampaň na očiernenie spoločnosti s cieľom získať jej zákazníkov; priemyselná špionáž atď.

Medzi politické záujmy patrí:

- ovplyvňovať kampaň zameranú na orientáciu výsledku hlasovania;

- politická a vojenská špionáž;

- prevzatie kontroly nad nástrojmi diaľkovej komunikácie atď.

Monitorovanie internetu

S cieľom monitorovať kybernetickú komunikáciu a bojovať proti kybernetickej kriminalite zriadili štáty špecializované systémy internetového dohľadu. Existujú medzištátne dozorné orgány, ako napríklad sieť Echelon. Sieť Echelon, ktorú spoločne spravujú Spojené štáty, Kanada, Austrália, Spojené kráľovstvo a Nový Zéland, je najväčšou telekomunikačnou a kybernetickou monitorovacou sieťou na svete. Takéto nástroje sú však dvojsečné, pretože sa môžu používať na špionážne účely (hospodárske, vojenské) alebo na kontrolu obyvateľstva.

Spolupráca s internetovými gigantmi - zložitá medzinárodná reakcia

Aby mohli štáty vykonávať svoju moc nad kybernetickým priestorom, musia sa spoliehať na spoluprácu internetových gigantov. Okrem toho, že majú väčšie technické a finančné zdroje ako mnohé štáty, majú aj moc utajovať alebo naopak zverejňovať informácie, ktoré sa šíria prostredníctvom ich služieb.

Vzhľadom na medzinárodný charakter kybernetickej hrozby si štáty rýchlo uvedomili potrebu spoločnej medzinárodnej reakcie. Túto reakciu však brzdí pomalosť vnútroštátnych postupov spolupráce, ako aj neochota štátov deliť sa o určité informácie. Nedostatky medzinárodnej spolupráce v oblasti kybernetickej bezpečnosti sa prejavili pri teroristických útokoch, ktoré v posledných rokoch zasiahli Európu. V reakcii na tieto útoky sa rôzne vlády zaviazali k väčšej spolupráci.

Na ceste k medzinárodnému právu v oblasti kybernetickej bezpečnosti

Napriek opakovaným výzvam mnohých politických lídrov stále neexistuje záväzné medzinárodné právo v oblasti kybernetickej bezpečnosti. V prístupe štátov ku kybernetickej bezpečnosti totiž existujú zásadné rozdiely. Európska výnimka v roku 2001 Rada Európy vytvorila prvú medzinárodnú zmluvu o spolupráci v oblasti kybernetickej bezpečnosti. Túto zmluvu známu ako Budapeštiansky dohovor , podpísali členské štáty Rady Európy, hoci nie všetky ju následne ratifikovali.

V rámci Europolu Európska únia (EÚ) v roku 2013 otvorila Európske centrum pre boj proti počítačovej kriminalite, ktorého cieľom je uľahčiť spoluprácu medzi európskymi štátmi v boji proti počítačovej kriminalite.

V septembri 2017 Európska komisia navrhla "balík kybernetickej bezpečnosti", ktorý zahŕňa celý rad opatrení vrátane zavedenia celoeurópskej certifikácie kybernetickej bezpečnosti. V júni 2019 potom nadobudlo účinnosť nariadenie EÚ o kybernetickej bezpečnosti. Zaviedol sa ním celoeurópsky systém certifikácie a zároveň sa posilnil nový mandát Agentúry EÚ pre kybernetickú bezpečnosť. Okrem toho v decembri 2020 Európska komisia a Európska služba pre vonkajšiu činnosť predstavili novú stratégiu kybernetickej bezpečnosti EÚ s cieľom posilniť odolnosť Európy voči kybernetickým hrozbám. Rada po prijatí záverov tejto stratégie kybernetickej bezpečnosti v marci 2021 tiež pripomenula, že kybernetická bezpečnosť má naďalej zásadný význam pre budovanie digitálnej Európy. Aj preto EÚ stále skúma dva legislatívne návrhy týkajúce sa súčasných a budúcich rizík (online a offline) prostredníctvom smernice, ktorá má lepšie chrániť siete a informačné systémy.

ANSSI 26. a 27. januára 2022 spojila 27 členských štátov siete CyCLONe, agentúru ENISA a Európsku komisiu (GR CONNECT) v rámci sekvencie cvičení EU-CYCLES (EU Cyber Crisis Linking Exercise on Solidarity), ktoré sa uskutočnia v januári a februári 2022.[11]

Systém kybernetickej bezpečnosti Francúzska

Francúzsko ako vedúca krajina EÚ v oblasti IT bezpečnosti považuje kybernetickú bezpečnosť za svoju prioritu už od roku 2000. Návrat teroristickej hrozby v roku 2015 ho prinútil zintenzívniť svoje úsilie v tejto oblasti. Národná stratégia digitálnej bezpečnosti stanovila päť cieľov:

- zaručiť národnú suverenitu ;

- reagovať na činy kybernetickej kriminality

- informovať širokú verejnosť;

- urobiť z digitálnej bezpečnosti konkurenčnú výhodu pre podniky;

- posilniť postavenie Francúzska na medzinárodnej scéne.

Sledovanie internetu vo francúzskom právnom systéme

[11] https://www.ssi.gouv.fr/en/

Boj proti počítačovej kriminalite sa začína sledovaním internetu. Vyhláška 2015-125 umožňuje administratívne blokovanie stránok s detskou pornografiou a stránok propagujúcich terorizmus. V roku 2015 bol prijatý zákon o "spravodajských službách", ktorý posilňuje prostriedky pôsobenia spravodajských služieb v digitálnej sfére. Po parížskych útokoch v roku 2015 vláda spustila aj operáciu "Stop Djihadisme " na boj proti džihádistickým propagandistickým kampaniam na sociálnych sieťach.

Vo Francúzsku sa kybernetická kriminalita zohľadňuje v právnych predpisoch od roku 1978, keď bol prijatý zákon o ochrane údajov (loi informatique et libertés), ktorý upravuje slobodu archivovania ľudských údajov. V súčasnosti sa digitálne praktiky riadia právnym systémom, ktorý za počítačové útoky stanovuje tresty odňatia slobody až do výšky piatich rokov a pokutu 75 000 eur. Zákon tiež stanovuje zvýšené tresty v prípade kybernetických útokov zameraných priamo na štát.

Vypátranie kyberzločincov

Polícia a žandárstvo majú rôzne orgány zamerané na potláčanie počítačovej kriminality . Patria medzi ne:

- Ústredný úrad pre boj proti trestnej činnosti v oblasti informačných a komunikačných technológií v rámci justičnej polície;

- Centrum pre boj proti digitálnej kriminalite (C3N) v rámci Národného žandárstva;

- Brigáda pre vyšetrovanie podvodov v oblasti informačných technológií (BEFTI) v rámci parížskej policajnej prefektúry.

Francúzska národná agentúra pre bezpečnosť informačných systémov (ANSSI) bola vytvorená v roku 2009 s cieľom brániť a chrániť informačné systémy a digitálnych používateľov pred kybernetickými útokmi. Jej úlohy sú nasledovné:

- monitorovať siete s cieľom odhaliť útoky a čo najrýchlejšie reagovať;

- vyvíjať produkty a služby kybernetickej bezpečnosti pre používateľov;

- poskytovať odborné znalosti a pomoc vládnym agentúram a podnikom;

- zvyšovať povedomie verejnosti o kybernetických hrozbách.

V roku 2017 francúzska vláda spustila národný program na pomoc obetiam kybernetických škodlivých činov. Platforma cybermalveillance.gouv.fr, ktorú inkubovala spoločnosť Anssi a

na ktorej sa podieľalo ministerstvo vnútra, spája obete kybernetických útokov - jednotlivcov, spoločnosti alebo miestne orgány - s poskytovateľmi služieb, ktorí im môžu pomôcť s ich postupmi. Platforma, ktorá bola začiatkom roka 2020 prepracovaná, zaznamenala nárast návštevnosti o +155 %.

Webová stránka CNIL poskytuje používateľom nástroje a príručky na posilnenie ich kybernetickej bezpečnosti.[12]

Zákonom z 3. marca 2022 sa mení a dopĺňa spotrebiteľský kódex, aby sa hlavným digitálnym platformám uložili nové povinnosti v oblasti kybernetickej bezpečnosti. Títo prevádzkovatelia budú musieť informovať používateľov internetu prostredníctvom "kybernetického skóre" o bezpečnosti svojich stránok, ako aj o bezpečnosti a umiestnení údajov, ktoré sú na nich umiestnené.

Kybernetická obrana

V strategickom preskúmaní obrany a národnej bezpečnosti z roku 2017 sa uvádza posilnenie hrozieb v kybernetickom priestore, kde "niektoré útoky by vzhľadom na ich rozsah a závažnosť mohli spadať pod kvalifikáciu ozbrojenej agresie". V strategickej aktualizácii z roku 2021 sa dodáva, že "kybernetický a vesmírny priestor sa v súčasnosti považujú za oblasti trvalého strategického súperenia, dokonca konfliktu" a sú "novými oblasťami prejavu moci".

Veliteľstvo kybernetickej obrany (Comcyber), ktoré bolo vytvorené v roku 2017 a je závislé od ministerstva ozbrojených síl, je zodpovedné za vojenskú kybernetickú obranu, ktorá zahŕňa všetky obranné a útočné akcie vykonávané v kybernetickom priestore. Comcyber tvorí 3 400 kybernetických bojovníkov. V zákone o vojenskom programovaní na roky 2019 - 2025, v ktorom je na kybernetickú obranu vyčlenených 1,6 miliardy eur, sa počet týchto bojovníkov do roku 2025 zvýši na 4 000.

Minister ozbrojených síl 18. januára 2018 predstavil doktrínu ofenzívnej kybernetickej vojny, ktorá dopĺňa defenzívnu kybernetickú vojnu. Minister tak formalizoval ofenzívnu zložku francúzskej kybernetickej doktríny. Umožňuje trvalú ochranu všetkých vojenských sietí a schopnosť reagovať na akýkoľvek útok proti obranným záujmom Francúzska.

[12] Commission Nationale Informatique & Libertés, CNIL, Data Protection Authority for France. The authority is established in Paris and is in charge of enforcing GDPR for France, as well as the national law for data protection "Loi Informatique et Libertés".

Bielu knihu o kybernetickej obrane, strategický prehľad kybernetickej obrany, zverejnil vo februári 2018 Generálny sekretariát národnej obrany.

Novinkou je podľa slov ministra ozbrojených síl "považovať kybernetický priestor za samostatné bojisko, Uznať, že kybernetický priestor je zbraň s potenciálom, ktorý môže byť oveľa škodlivejší a nebezpečnejší ako rakety".[13]

3. Nástroje kybernetickej reakcie Európskej únie

Právnym základom nariadenia EÚ - ENISA je nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 (Akt o kybernetickej bezpečnosti) o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií, ktorým sa zrušuje nariadenie (EÚ) č. 526/2013. CSIRT[14] funguje ako rozšírenie procesu núdzového plánovania vzhľadom na jeho zameranie na pripravenosť reagovať na vzniknuté hrozby. CSIRT poskytuje prostriedky na hlásenie incidentov a na šírenie dôležitých informácií súvisiacich s incidentmi príslušným orgánom a zákazníkom CSIRT. Poslaním a účelom rámca sluţieb CSIRT je uľahčiť zriadenie a zlepšenie činnosti CSIRT, najmä pri podpore tímov, ktoré sú v procese výberu, rozširovania alebo zlepšovania svojho portfólia služieb.[15]

CSIRT sa zaväzuje pomáhať našim zákazníkom pri nahlasovaní a vyšetrovaní incidentov počítačovej bezpečnosti, poskytovať informácie o technických zdrojoch a rýchlo, presne a účinne šíriť informácie ostatným bezpečnostným tímom na celom svete.

Služby reakcie na incidenty 24/7

CSIRT poskytuje služby reakcie na incidenty v oblasti počítačovej bezpečnosti 24x7 všetkým používateľom, spoločnostiam, vládnym agentúram alebo organizáciám. CSIRT poskytuje spoľahlivé a dôveryhodné jednotné kontaktné miesto na nahlasovanie incidentov v oblasti počítačovej bezpečnosti na celom svete.

Všeobecné služby zahŕňajú nasledujúce:

---

[13] Minister of the Armed Forces, speech on cybersecurity and cyber defense, Lille, September 8, 2021.
[14] The Computer Security Incident Response Team (CSIRT)
[15] First CSIRT Services Framework
https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

- Kriminalita bielych golierov
- Obnova údajov
- Zneužitie internetu
- Krádež chránených informácií
- Zhromažďovanie dôkazov
- Odovzdávanie incidentov
- Počítačová kriminalistika
- Reakcia na incidenty 24x7
- Reakcia na vírusy
- Obnova po havárii
- Penetračné testovanie
- Riešenia systému detekcie narušenia (IDS)
- Vývoj politík

Postupná implementácia nástrojov CSIRT pod patronátom ENISA podporuje efektívnejší boj proti kybernetickej kriminalite v jednotlivých členských krajinách EÚ.

ZÁVER

Obrovské straty spôsobené počítačovou kriminalitou si vyžadujú zníženie počtu týchto trestných činov. Francúzsko bolo jednou z prvých krajín (po Slovensku), ktorá prijala národnú stratégiu boja proti počítačovej kriminalite. Vládne agentúry ANSSI a CNIL vytvárajú významnú podporu pre jednotlivcov, spoločnosti, štátne a neštátne organizácie prostredníctvom masívnych investícií do poradenstva a zabezpečenia systémov verejnej správy proti kybernetickým útokom. Podobné úrady zriadené vládou sa zriaďujú vo väčšine krajín EÚ s podobnými kompetenciami a stratégiami ako uvedené francúzske agentúry s podporou tímov ENISA pre riešenie počítačových bezpečnostných incidentov.

Cieľom štúdie je najmä poukázať na možnosti podpory zo strany verejných inštitúcií, ako aj na individuálnej úrovni v boji proti rýchlo rastúcej počítačovej kriminalite. Otázkou do budúcnosti je nájsť spôsoby merania účinnosti prijatých opatrení a investovaných prostriedkov. Táto otázka si zaslúži samostatné riešenie v rámci rozsiahlej vedeckej štúdie.

REFERENCES

Müllerová, J. & Sisulak, S. *Criminality software control tools of environmental crime.* 20th International Multidisciplinary Scientific GeoConference Proceedings SGEM 2020. STEF92 Sofia 2020

Mimecast. Confronting the new wave of cyberattacks - The State of Email Security 2022. www.mimecast.com

Vojinovic I., More Than 70 Cybercrime Statistics - A $6 Trillion Problem https://dataprot.net/statistics/cybercrime-statistics/

Vie Publique. Cybersécurité : quelles réponses face aux menaces nouvelles? 22-05-2022 https://www.vie-publique.fr/eclairage/18469-cybersecurite-quelles-reponses-face-aux-menaces-nouvelles

Cybersecurity, SAGE. https://www.sage.com/fr-fr/blog/glossaire/cybersecurite-definition-de-la-cybersecurite/

ENISA – European Union Agency for Internet Security. https://www.enisa.europa.eu/topics/csirt-cert-services

CSIRT Services https://www.csirt.org/services/index.html

First CSIRT Services Framework https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1