

POHLED MLADÝCH ČECHŮ V EU

KYBERNETICKÉ HROZBY A BEZPEČNOST

Předmluva



Luděk Niedermayer
europoslanec



Pandemie COVID-19 znovu ukázala, že i přes všechny nedostatky je pro naši zemi zcela zásadní být součástí "společné Evropy", kterou dnes reprezentuje Evropská unie. Hrozby a problémy, kterým čelíme a čelit budeme, jsou stále častěji takové povahy, že ani velké a silné země jim nejsou schopny čelit samy. I proto je našim zájmem nejen udržovat "naši Unii" funkční a akceschopnou (což není vždy snadné), ale též ji rozvíjet a na základě zkušeností její nedostatky napravit.

Je důležité, abychom nebrali stávající přínosy České republiky jako něco samozřejmého a oprostili se od u nás tak častého předpokladu, že Unie je pro naši zemi tak trochu kasička na peníze. I to je důležité, stejně tak, jako u nás vyzdvihovaný přínos společného trhu. Ale význam Unie pro své členy, nás nevyjímaje, je mnohem širší. Jsem rád, že na textu TOP týmu z.s., který je výsledkem diskuse mladých pravicově, či středově smýšlejících lidí u příležitosti blížícího se českého předsednictví Rady EU, je vidět, že toto si uvědomuje i generace dnešních vysokoškoláků.

Jako europoslanec rád vidím, že se text snaží postihnout mnoho dimenzí dnešní evropské spolupráce. TOP tým navíc ukazuje, že umí jít do detailu při posuzování problémů a výzev a hledání nejlepších řešení. Dělá mi velkou radost, že se mladí lidé z TOP týmu ve svém volném čase detailně a kompetentně zabývají otázkami, které jsou pro Evropany důležité. A tam, kde to je relevantní, se snaží hledat přístup k jejich řešení, který vychází ze stavu a potřeb života v České republice.

Vůbec mě nepřekvapují často zaznívající kritické tóny. Mnoho z nich sám sdílím a velmi vítám konstruktivní přístupy k hledání řešení.

Hloubka zpracování i samotný výběr témat dokazují, že mladí lidé dění v Evropské unii sledují a umí se v něm velmi dobře orientovat. A to přesto, že jak pravidla fungování Unie, tak hlavně problémy, kterým čelíme, jsou velmi složité. Nyní je ten pravý čas na vznik takových textů. Neb v reakci na vývoj ve světě, (například stále probíhající tragickou pandemii), musíme spolu hledat cesty, jak udělat svět (nejen pro Evropany) bezpečnější, stabilnější a odolnější. I

proto je třeba, aby se Unie (i mnoho věcí ve fungování jednotlivých zemí) změnila a byla schopna to, co od ní očekávají občané, lépe plnit. Proto věřím, že výsledkem všech budoucích debat na toto téma, včetně "Konference o budoucnosti Evropy", bude shoda na změnách, která ovlivní k lepšímu životy nás všech na desetiletí.

Ale jako vždy bude záležet na každém z nás, neb změny nemusí být automaticky k lepšímu. Jen kompetentní diskuse při porozumění stavu věcí a pochopení světa, ve kterém žijeme, může přinést ona "dobrá rozhodnutí". A proto je tak cenné, že si lidé z TOP týmu dali práci nad diskusí nad těmito tématy, prokázali vysokou kompetenci a též potřebnou ochotu hledat dobré kompromisy a ukazují, že to jde. Právě takový přístup by měl být v rámci nadcházejících diskusí pravidlem.

Pokud Vás budoucnost EU zajímá, a chápete, že i na Vašich názorech závisí, zda spolu dosáhneme toho, aby byl svět, ve kterém žijeme alespoň o trochu lepší, věřím, že Vás tato publikace zaujme. Srdečně Vás zvu i k přečtení všech 8 dalších bílých knih. Věřím, že Vás nezklamou a čas strávený nad jejich čtením bude i pro Vás časem dobře využitým.



POHLED MLADÝCH ČECHŮ V EUKYBERNETICKÉ HROZBY A BEZPEČNOST**1. Popis aktuálního stavu**

Digitální transformace přináší nespočet příležitostí. Pojí se s ní i celá řada rizik a výzev. Kybernetické útoky a hrozby představují jednu z hrozeb. Jsou čím dál více sofistikované. Jak digitalizace postupuje a počet propojených zařízení neustále roste, bude se z kybernetických útoků stávat čím dál palčivější problém. Na podobná nebezpečí je nutné pružně reagovat. Činnosti, techniky a mechanismy, které vedou k ochraně počítačových sítí, informačních systémů a jejich uživatelů se souhrnně nazývají kybernetická bezpečnost (Cyber Security).

Obrázek č. 1 zobrazuje pět nejzávažnějších kybernetických hrozeb v letech 2019 až 2020. Ohroženy jsou všechny vrstvy informační společnosti. Běžní uživatelé informačních systémů a internetu bývají nejčastěji vystaveni útokům skrze webové stránky či malware, což vede ke krádežím dat nebo majetku. Firmy, státy a veřejné instituce čelí cíleným kybernetickým útokům, jejichž důsledkem může být únik citlivých dat, korupce a v nejhorších případech i ochromení celkového fungování. Ochrana klíčové infrastruktury je proto obzvláště důležitá.



Obr. č. 1 – pět nejzávažnějších kybernetických hrozeb v EU (10)

Otázka kybernetické bezpečnosti se ukázala být velkým tématem i během pandemie onemocnění covid-19. Lidé se přesunuli do virtuálního prostoru. S větší online aktivitou přichází i více hrozeb. Jak je vidět na obrázku č. 2, kybernetická kriminalita se nezmírnila, ba právě naopak. Cílem se staly zdravotnické organizace a testovací aplikace, děly se různé podvody se zdravotnickým materiálem. Pandemii ke svým cílům zneužila celá dezinformační scéna.



Obr. č. 2 – zneužití pandemie (10)

Česká republika si rizika kybernetických hrozeb uvědomuje. Reagovala na ně schválením zákona o kybernetické bezpečnosti již v roce 2014 (1). Následně vznikl Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) (2). Zabývá se veškerými aktivitami, které souvisejí s prevencí, hrozbami, výzkumem a mezinárodní spoluprací v oblasti kybernetické bezpečnosti. Podobným tématům se věnuje i Bezpečnostní informační služba (BIS). Šetří převážně kybernetické hrozby, jež mají dopad na chráněné zájmy České republiky. Zajímá se o ochranu kritické infrastruktury, nelegální obchod či terorismus. Kybernetická obrana je důležitým tématem i pro Armádu České republiky, v jejímž rámci působí tři instituce: Národní centrum kybernetických operací, které má v gesci Vojenské zpravodajství (3), Velitelství kybernetických sil a informačních operací a Agenturu komunikačních a informačních systémů.

Evropská unie stanovila následující cíle v rámci své agendy kybernetické bezpečnosti (viz obrázek č. 3):

- zlepšení kybernetické odolnosti – strategie a související opatření, která vedou k posílení odolnosti Evropy vůči kybernetickým hrozbám
- boj proti kybernetické kriminalitě – boj proti trestné činnosti páchané prostřednictvím počítačů v online světě
- podpora kybernetické diplomacie – snaha o mezinárodní spolupráci a dialog (v horším případě sankce), které by sloužily k prevenci kybernetických útoků
- posílení kybernetické obrany – kyberprostor je dnes nedílnou součástí vojenských operací
- podpora výzkumu a inovací
- ochrana kritické infrastruktury, např. zabezpečení 5Gsítí

Klíčový krok Evropské unie představuje Akt o kybernetické bezpečnosti. Dokument zavádí jednotný celounijní systém certifikace kybernetického zabezpečení – komplexního souboru pravidel, technických požadavků, norem a postupů (4). Jedná se o žádanou změnu a reakci na kauzy typu Huawei. Společnost Huawei čelí dlouhodobému podezření ze spolupráce s čínským komunistickým režimem a celou řadou informačních služeb a je pravidelně označována za firmu s významným bezpečnostním rizikem. Spojené státy v reakci na kauzu zakázaly použití amerických technologií v Huawei zařízeních. V evropském prostoru se firma Huawei zapojuje do tendrů stavby 5G sítí.

V dubnu 2021 se Evropská unie rozhodla zřídit centrum kompetencí pro kybernetickou bezpečnost. Má za cíl posílit bezpečnost internetu a ostatních kritických sítí a informačních systémů (5).





Obr. č. 3 – zajištění kybernetické bezpečnosti z pozice EU (10)

TOP 09 se kybernetické bezpečnosti věnuje na evropské úrovni. Luděk Niedermayer zasedá ve Výboru Evropského parlamentu pro průmysl, výzkum a energetiku (ITRE) a aktivně se podílí na legislativě, která s kybernetickou bezpečností aktivně pracuje. Jedním z problémů, které řeší, je nastavení standardů kybernetické bezpečnosti na úrovni EU (6). Kybernetická bezpečnost je důležitým tématem i pro YEPP, mládežnickou organizaci Evropské lidové strany. YEPP plánuje rezoluci, jež by volala po koordinovaném postupu ohledně kybernetické bezpečnosti při budování 5G sítí (zdroj zatím není veřejný).

Jedním z klíčových témat, která s kybernetickou bezpečností souvisejí, je šifrování. Jedná se o proces, který transformuje nezabezpečená elektronická data pomocí kryptografických algoritmů na data zašifrovaná, tedy běžným způsobem nečitelná. Šifrovat se dají soubory, emaily, disky, ale i různé typy komunikací. Na půdě Evropské unie se ohledně šifrování střetávají dva protichůdné názorové proudy. Jeden zdůrazňuje důležitost ochrany základních práv, digitální bezpečnost občanů, vlád a společností. Druhý naopak akcentuje závislost donucovacích a justičních orgánů na přístupu k elektronickým důkazům. Dobře šifrovaná data totiž často bez „zadních vrátek“ v šifrovacím algoritmu neumožní přístup ani justiční moci. Evropská unie vyvíjí aktivní snahy, aby našla rovnováhu mezi využíváním šifrovací technologie a zaručením pravomocí donucovacích orgánů a justice tak, aby svoji činnost mohly provádět za stejných podmínek jako v off-line světě. V prosinci 2020 přijala EU usnesení, že je nutné zajistit jak bezpečnost prostřednictvím šifrování, tak bezpečnost šifrování navzdory (5).

Velmi aktuálním a diskutovaným tématem je problematika masového biometrického sledování. V dnešní době jsou běžné chytré kamery obsluhovány algoritmy umělé inteligence. Dokážou identifikovat lidské tváře (facial recognition), stereotyp chůze i SPZ vozidla. Uloženým údajům, které jednoznačně identifikují lidský obličej nebo otisky prstů, se říká biometrické. Pokud se biometrická data lidské tváře budou nacházet v databázi propojené s kamerovým systémem, bude rozpoznání konkrétní osoby otázkou několika málo sekund. Pokud jsou záběry z chytrých kamer nedokonalé, poslouží pro lepší identifikaci konkrétní osoby doplňující informace jako styl chůze nebo SPZ auta. Vzhledem k faktu, že se kamerový systém využívá poměrně masivně, je relativně snadné zapojit konkrétní osobu do kontextu a vysledovat její pohyb v prostoru či interakci s ostatními lidmi pomocí lokalizačních dat. Lze tím předpovídat a odhadovat potenciálně škodlivé chování. Jedná se však o značné riziko, které technologický pokrok způsobuje. Dříve kamerové systémy nepracovaly v reálném čase a zaznamenávaly pouze obraz. Případná analýza natočeného záznamu vyžadovala náročnou následnou ruční práci.

2. Vymezení cílového stavu a zhodnocení rizik

1.1 Kybernetické hrozby vůči kritické infrastruktuře

Vznik celounijního systému certifikace kybernetické bezpečnosti je skvělým krokem, který velmi kvítujeme. Problémem však je, že celá řada zařízení infrastruktury různých států běží na hardwaru, u kterého není jisté, co se „uvnitř“ něj děje. Informace o zneužívání telekomunikačních technologií či o průmyslové špionáži se objevují pravidelně.

Velká Británie, Francie nebo Švédsko jsou země, které bychom v jejich přístupu mohli následovat. Vyřazují z budování 5G sítí nedůvěryhodné dodavatele, jakým je kupříkladu Huawei. Nicméně potenciálně rizikový je ve své podstatě každý dodavatel tzv. „uzavřených“ produktů. Certifikace technologií by se neměla nikdy dostat do stavu, ve kterém se hodnotí vstupy a výstupy nějakého uzavřeného zařízení. Vždy by měla existovat možnost nahlédnout dovnitř. To bude vyžadovat otevřenou specifikaci hardwaru minimálně pro potřeby EU.

1.2 Šifrování

Možné prolomení šifrování by se mohlo stát extrémně nebezpečným precedents. Základní důvěra v informační systémy spočívá v praktické neprolomitelnosti šifer, pokud jsou splněny konkrétní předpoklady. Hypoteticky vzniklá povinná zadní vrátka však s sebou přinášejí velké

riziko zneužití, úniku dat a podobných hrozeb. Nelze předpokládat, že jakýkoli strůjce nelegálních aktivit bude používat systémy s prolomitelnými šiframi, ať už vědomě či nevědomě. Pokud někdo páchá trestnou činnost (nejen) v kyberprostoru, nebýt odhalen je jedním z jeho primárních zájmů. Prolomitelné šifrování může být likvidační pro firemní prostředí. Firmy, které jsou donucené používat šifry s tzv. „backdoorem“, riskují u svých klientů okamžitou ztrátu důvěryhodnosti.

1.3 Masové biometrické sledování

Centralizované ukládání biometrických dat považujeme za příliš velký a problematický zásah do základních lidských práv. Jedná se o jednoznačnou lidskou identifikaci, osobní údaj. Rozpoznat nás může kdokoli, kdo má k databázi s biometrickými údaji přístup. Neméně závažným problémem je nespolehlivost systémů a modelů umělé inteligence. Biometrická identifikace je sice relativně spolehlivá, ale veškerý navázaný software se může v některých specifických situacích zásadně mýlit. To by mohlo vést k celé řadě lidských tragédií. Masové zapojení podobných technologií zavání „Velkým bratrem“, tedy podléhání neustálému dohledu. V zásadě ani neexistuje jistota, že uložená data nebudou dále nevyžádaným způsobem zpracována.

Zdviženým prstem pro všechny je kreditový systém v Číně, který může na první pohled vypadat až dystopicky. Systém vám přiřadí sociální skóre podle toho, jak moc spořádaným občanem jste v očích komunistické strany. Při nízkém skóre můžete mít například zakázáno vycestovat. To vše umožňuje masivní sledovací systém. Kamery běžně občany identifikují, čímž odhalí, že provádí nekalou „protistátní“ činnost. Na základě prohrěšku systém sníží sociální kredit daného jedince. S nízkým kreditem je snadné člověka kamerovým systémem odhalit třeba při vstupu na letiště.

Evropská komise přišla 21. dubna s návrhem umělou inteligenci regulovat. V dokumentu přiznává rizika masového biometrického sledování a navrhuje zakázat některé z praktik všem unijním donucovacím orgánům. Je to dozajista dobrý první krok. Obáváme se však, že je nedostatečný a regulace nepokrývá všechna výše zmíněná rizika. Kromě toho vytváří i problémy zcela nové. Ty se však netýkají kybernetické bezpečnosti, tudíž je v tomto textu nebudeme detailněji probírat ([7](#)). Z obav vůči masivnímu biometrickému sledování vznikla iniciativa Reclaim your face. Klade si za cíl dosáhnout dialogu s Evropskou komisí pomocí nástroje ECI (Evropská občanská iniciativa), k čemuž potřebuje sesbírat pod petici alespoň milion podpisů občanů EU ([9](#)).

Nutnost mít nějaké kamerové systémy na důležitých místech veřejného prostoru si uvědomujeme. Jejich nezbytnost je logická u veřejných institucí, kritické infrastruktury, na letištích a podobně. Využití kamer na důležitých místech kvůli bezpečnosti nelze směřovat s problémem masového sledování občanů.

1.4 Dezinformace využívající nové technologie

Některá témata nelze zařadit striktně do oblasti kybernetické bezpečnosti. Deepfake videa k takovým tématům patří – pohybují se na pomezí kybernetiky a oblasti dezinformací. V dnešní době lze relativně snadno pomocí umělé inteligence vytvořit video s veřejnou osobou či politikem, které je na první i druhý pohled k nerozeznání od videí autentických. Sofistikované systémy, které deepfake videa dokážou rozpoznat, již vnikají. Běžný konzument ovšem nebude s největší pravděpodobností nikdy pravost videa do takové hloubky zkoumat. Typickým účelem dezinformací je, aby se „stokrát opakovaná lež stala pravdou“. Hromadný a vytrvalý útok pomocí deepfake videí má hrozivý potenciál uštědřit nenapravitelné škody naší společnosti. Některé veřejné platformy proto začaly podobný obsah blokovat (8).



3. Navrhovaná opatření

- TOP tým prosazuje, aby jednotná certifikace kybernetické bezpečnosti EU vyžadovala otevřenou specifikaci hardwaru. Jedině zařízení, která jsou auditovatelná v plném rozsahu, jsou důvěryhodná.
- TOP tým podporuje nadnárodní spolupráci při výběrových řízeních dodavatelů kritické infrastruktury.
- TOP tým souhlasí s plánovanou rezolucí YEPP, která bude volat po koordinovaném postupu v oblasti kybernetické bezpečnosti při budování 5G sítí.
- TOP tým nepodporuje zavedení povinnosti používat šifrovací algoritmy s možným backdoorem.
- TOP tým navrhuje zákaz masového sledování pomocí kamerových systémů, které využívají jakoukoli formu biometrické identifikace, a to nejen v reálném čase, ale i v pozdějším zpracování.
- TOP tým podporuje zákaz ukládání biometrických údajů občanů v centrálních databázích. Výjimkou jsou databáze hledaných osob (například Interpolu).
- TOP tým se hlásí k iniciativě Reclaim your face a z ní vyplývající petici, jež vyzývá Evropskou komisi k dialogu o podobě budoucí legislativy ([9](#)).
- TOP tým se domnívá, že případná regulace deepfake videí a dezinformací vytvářených pomocí nových technologií nikdy nedosáhne zamýšleného cíle. TOP tým je přesvědčen, že je potřeba se zaměřit především na osvětu, vzdělání a kvalitní práci s informacemi.
- TOP tým podporuje, aby se orgány kybernetické bezpečnosti zapojily do odhalování deepfake videí a dalších druhů dezinformací vytvářených pomocí moderních technologií. Podporujeme, aby veřejné platformy označovaly (nikoli blokovaly) potenciálně nebezpečný obsah.



4. Bibliografie a další zdroje

- (1) <https://www.psp.cz/sqw/sbirka.sqw?cz=181&r=2014>
- (2) <https://www.nukib.cz/cs/kyberneticka-bezpecnost/>
- (3) <https://www.mocr.army.cz/informacni-servis/zpravodajstvi/narodni-centrum-kybernetickych-operaci-vypracovalo-strategii-kyberneticke-obrany-cr-201906/>
- (4) <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act>
- (5) <https://www.consilium.europa.eu/cs/policies/cybersecurity/>
- (6) <https://www.top09.cz/co-delame/tiskove-zpravy/kybernetickou-bezpecnosti-a-kauzou-huawei-se-bude-zabyvat-evropsky-parlament-25463.html>
- (7) <https://reclaimyourface.eu/european-commission-proposal-new-ai-regulation-fighting-ban-biometric-mass-surveillance/>
- (8) <https://democracy-reporting.org/wp-content/uploads/2020/08/2020-09-01-DRI-deepfake-publication-no-1.pdf>
- (9) <https://reclaimyourface.eu/cs/>
- (10) <https://www.consilium.europa.eu/cs/infographics/cybersecurity-in-the-eu/>