



Červenec 2022

KYBERNETICKÁ BEZPEČNOST A KRIMINALITA V ČR

Roman Máca

Shrnutí

Kybernetická kriminalita vykazuje v posledních letech rostoucí trend. Do kyberprostoru se promítá i nynější napjatá mezinárodní situace. Vzhledem k vynalézavosti útočníků se neustále objevují nové hrozby. S postupující digitální transformací přichází i větší důraz na kybernetickou bezpečnost. Studie mapuje jednotlivé oblasti relevantní pro Českou republiku a rozebírá konkrétní příklady. Závěrem jsou uvedena doporučení vycházející z konzultací s experty.

Studie byla vytvořena za podpory
společnosti Microsoft.



Česká republika se stejně jako další země potýká s řadou problémů spojených s kybernetickou bezpečností. Běžná veřejnost, ale i firmy a instituce, se stávají cílem různých podvodů, phishingu, ransomware či DDoS útoků a rovněž útoků s cílem získat citlivé informace. Kybernetická kriminalita v ČR navíc v posledních letech, jak uvádí zpráva Národní centrály proti organizovanému zločinu, vykazuje rostoucí trend.¹

A jak si v oblasti kybernetické bezpečnosti jako česká společnost stojíme? „Nemyslím si, že je to až tak špatné nebo tragické, ale povědomí není dostatečné,“ zhodnotil situaci v květnu 2022 ředitel Národního úřadu pro kybernetickou a informační bezpečnost Karel Řehka.²

Kromě obvyklých zločineckých skupin či jednotlivců v kyberprostoru působí i státní aktéři reprezentovaní autoritářskými režimy s mocenskými ambicemi. Ty tento prostor využívají k prosazování svých cílů. V roce 2016 ministři obrany členských zemí Severoatlantické aliance uznali kyberprostor za bojovou oblast. „Dnes si lze jen těžko představit nějaký vojenský konflikt bez užití kyberprostoru,“ uvedl tehdy generální tajemník Aliance Jens Stoltenberg.³ Konflikty z reálného světa se zrcadlově přelévají do toho virtuálního a například Ruská federace kybernetické útoky běžně využívá proti svým oponentům jako nástroj odvety či pomsty.

V oblasti kybernetické bezpečnosti a obrany hraje stát zásadní roli. Jedná se ale o horizontální téma procházející všemi aspekty společnosti. Klíčem je zodpovědný přístup celé společnosti spočívající v posilování kolektivní odolnosti.

Vynalézavost podvodníků a sofistikovanější phishing

Internet je místem, kde se jeho uživatelé mohou setkat s širokým spektrem podvodníků. Vzhledem k určité naivitě a nedostatečné informovanosti řada lidí přichází o peníze, kdy neodolají na první pohled výhodné nabídce. Ta se ale později změní v noční můru.

Evergreenem jsou podvody na různých internetových tržištích, aukčních portálech, bazarech apod. Typickým schématem je, že zboží (např. auto za výhodnou cenu)⁴ se nachází v zahraničí. Zájemce následně dostává zprávu, že je potřeba poslat zálohu na přepravu do ČR, že auto uvázlo na hranicích a kupující má poslat peníze na celní poplatky apod. Využíváno je samozřejmě různých manipulativních a přesvědčovacích technik. Když podvodník od své oběti získá maximum peněz, veškerá komunikace jednoduše skončí.

Obvyklým jevem jsou i podvody označované v angličtině jako romance scams. Českou ženu např. kontaktuje údajný americký voják sloužící kdesi v zahraničí. Ten své oběti slíbí, že jí zašle balíček s cennostmi, že za ní následně přijede, vezmou se a budou žít spolu. Žena má samozřejmě za balíček

¹ Policie České republiky (28. června 2022). Výroční zpráva NCOZ 2021. <https://www.policie.cz/clanek/vyrocnizprava-ncoz-2021.aspx>.

² Institut pro politiku a společnost (13. května 2022). VII International Conference Digital Czech Republic 2022. <https://youtu.be/lqupxh9AjZ4>.

³ Natoaktual (15. června 2016). Alianční ministři obrany uznali kyberprostor za bojovou oblast. https://www.natoaktual.cz/v-mediich/aliancni-ministri-obrany-uznali-kyberprostor-za-bojovou-oblast.A160615_171942_na_media_m02.

⁴ iDNES.cz (10. června 2022). Nabízeli ojetá auta na internetu a podvedli skoro 200 lidí, zadržela je policie. https://www.idnes.cz/zpravy/cerna-kronika/policie-podvody-ojeta-auta-internet-rumunsko-cesko.A220610_150156_domaci_pukk.

uhradit poštovné, celní poplatky apod.⁵ Stejný modus operandi funguje z hlediska pohlaví i naopak. Amerického vojáka jen nahradí zpravidla „nevěsta“ ze zemí bývalého Sovětského svazu. Po navázání kontaktu a „zpracování“ oběti tak „nevěsta“ požaduje peníze na letenku do ČR, na víza, následně jí ale onemocní dcera, kdy současně nemá peníze na operaci, a další různé problémy, které má oběť prostřednictvím zaslaných peněz vyřešit. Využíváno je samozřejmě citového vydírání a dalších manipulativních technik.⁶

Dalšími častými praktikami jsou phishing (v ČR se také používá pojem rhybaření) či sofistikovanější spear phishing využívající metod sociálního inženýrství. Motivace bývá zpravidla finanční, kdy je cílem útočníka získat citlivých údajů, jako jsou hesla, údaje k platebním kartám apod. Ty následně využívá sám útočník nebo je přeprodává dále. Tzv. credentials⁷ se podle Microsoft Digital Defense Report prodávají za cenu od 1 do 50 USD.⁸ Phishingové útoky s cílem krádeže hesel a identit jsou podle zmiňované zprávy levné a v průběhu času vykazují rostoucí trend.

U phishingu, kdy je cílem získat od oběti přímo finanční prostředky, se útočníci logicky snaží vyvolat dojem, že jde o zprávu banky, finančního úřadu, pošty, ale i dalších organizací, se kterými veřejnost běžně provádí finanční transakce.

Níže je uvedený příklad podvodného e-mailu, který má oběť nalákat pod příslibem vyplacení finanční částky. Funguje to i naopak v podobě zprávy typu „máte nedoplatek na daních, pro vyřešení klikněte zde“. Při obdržení takového e-mailu se řada lidí onoho „nedoplatku“ vyděsí a s určitou naivitou klikne na odkaz či otevře přílohu. V těchto situacích je ale lepší zdrženlivost a zachovat chladnou hlavu. Ta nám může napovědět, že se jedná o podvod. V případě velmi sofistikovaných aktivit, které neobsahují jazykové chyby, využívají tzv. spoofing⁹, je na místě kontaktovat dotčenou instituci jinou cestou např. telefonicky či osobně a ověřit si, zda se jedná o autentickou zprávu nebo ne. Informování instituce navíc pomůže ochránit i další osoby, jelikož po zaznamenání takového incidentu obvykle dochází k varování klientů před podvodnými e-maily a dalšími riziky.

⁵ Policie České republiky – KŘP Královéhradeckého kraje (6. května 2022). *"Americký voják opět v akci"*. <https://www.policie.cz/clanek/americky-vojak-opet-v-akci-80760.aspx>.

⁶ Sobotková, M. (18. února 2021). *Ja tebja ljublju! Jak ruské krásy loví české ženichy a obírají je o peníze*. Seznam Zprávy. <https://www.seznamzpravy.cz/clanek/ja-tebja-ljublju-jak-ruske-krasky-lovi-ceske-zenichy-a-obiraji-je-o-penize-142435>.

⁷ Credentials jsou data požadovaná systémem pro ověření práva přístupu k informacím nebo prostředkům (k dokumentu, do počítače, sítě, aplikace atd.), tedy pro autentifikaci. Nejčastěji se jedná o heslo, kombinaci přihlašovacího jména a hesla apod.

⁸ Microsoft (říjen 2021). *Microsoft Digital Defense Report*. <https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report>.

⁹ Praktika, jejíž prostřednictvím se podvodníci maskují za pravé telefonní číslo, e-mail, IP adresu či věrohodně vypadající webovou stránku.

Obrázek 1: Ukázka podvodného e-mailu



Máte nárok na vrácení částky 136,99 EUR.
Zašlete prosím následující formulář, abychom ho mohli zpracovat
vrátit se co nejdříve.

[klikněte zde](#)

Po přijetí formuláře vám bude naúčtována refundace
ekvivalent našich služeb.
Odesílání nebo zaznamenávání neplatného souboru po určitém limitu může
oddálit vrácení platby
Brzy dostanete formulář na vrácení platby

Finanční ředitelství SR

[GFŘ](#)

[Novinky přes RSS](#)

[Prohlášení o přístupnosti](#)

[Novinky e-mailem](#)

[Kontakty](#)

Zdroj: Finanční správa, 2021.¹⁰

Obecným trendem je, že se stoupající osvětou v dané problematice se podvodníci adaptují a využívají sofistikovanějších metod v podobě spear phishingu a sociálního inženýrství. V takových případech útočník neoslovuje plošně bez většího rozmyšlení, ale svou oběť si důkladněji vybírá a zkoumá, aby u ní vzbudil zdání důvěryhodnosti a mohl se vydávat například za kolegu z práce. Motivace tak nemusí být pouze čistě finanční, ale cílem bývají i citlivé informace týkající se například duševního vlastnictví.

Poměrně novým fenoménem je tzv. vishing (voice phishing), kdy je oběť kontaktována nejdříve telefonicky s tím, že jí volá například údajný pracovník banky či policista, aby ji informoval o podezřelých transakcích na bankovním účtu. Cílem bývá získání údajů o platební kartě či vzdáleného přístupu k počítači oběti a z něj odeslání peněz na konto útočníka.¹¹

Schopnost rychlé adaptace podvodníků ukazuje i následující příklad. „Stávající mezinárodní geopolitické situace využívají ve velkém kybernetičtí podvodníci. Jejich cílem jsou klienti tuzemských bank, především pak rusky a ukrajinsky hovořící občané. Podvodníci těží z nepozornosti klientů a jejich

¹⁰ Finanční správa (22. března 2021). *Finanční správa varuje před podvodnými e-maily*. <https://www.financnisprava.cz/cs/financni-sprava/novinky/novinky-2021/financni-sprava-varuje-pred-podvodnymi-e-maily>.

¹¹ Adamcová, P. (14. června 2021). *Na vybílání účtu stačí jeden telefonát. Poslechněte si, jak útočník láká z oběti data*. Aktuálně.cz. <https://zpravy.aktualne.cz/finance/banky-vishing/r~ef8a7f48ca7911ebad06ac1f6b220ee8/>.

strachu o budoucnost a pod záminkou, že jsou jejich peníze v ohrožení, je donutí sdělit citlivé údaje. Ty následně zneužijí pro získání jejich úspor,” uvedla na začátku března Česká bankovní asociace.¹²

Vyděračský ransomware

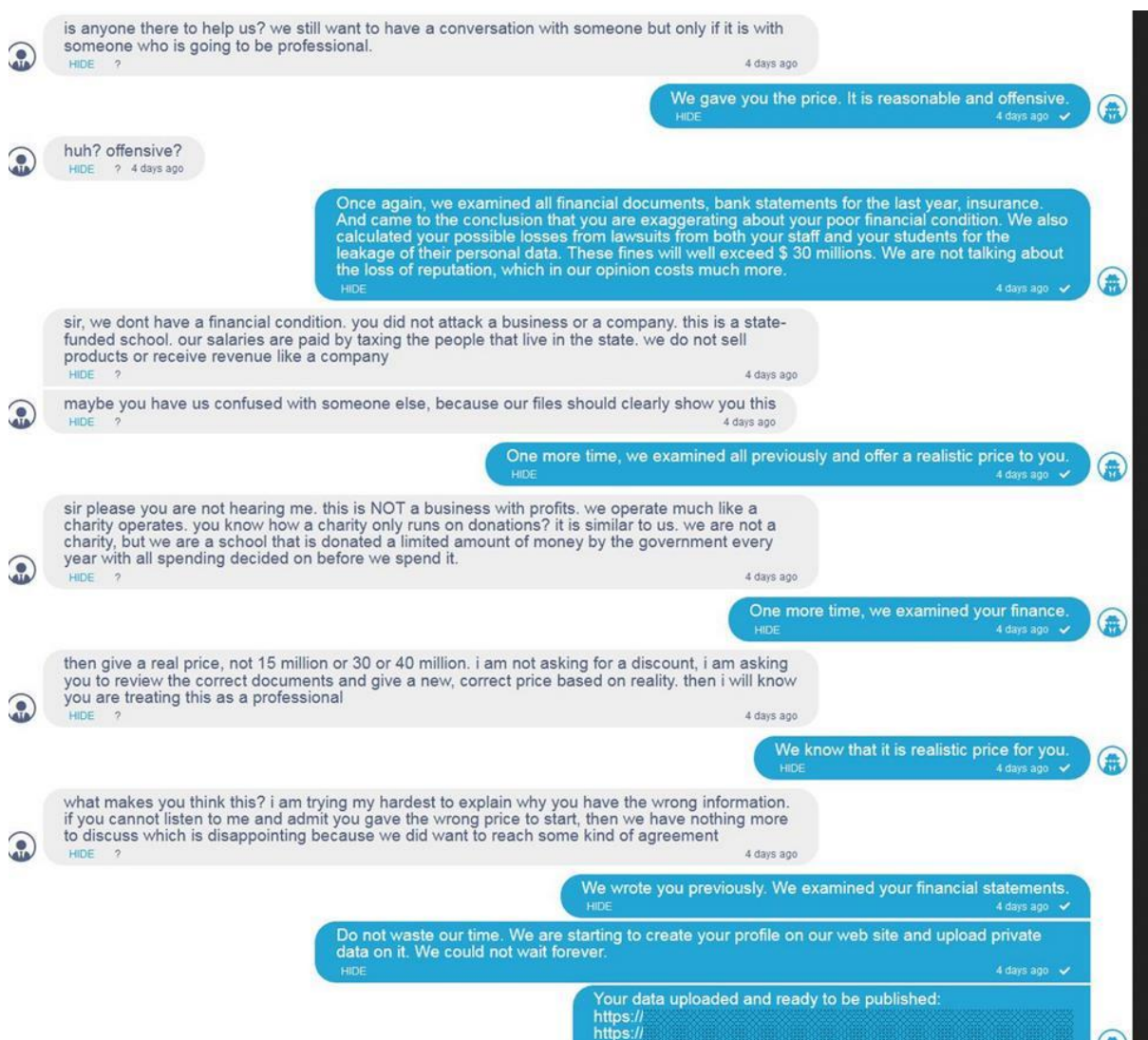
Kybernetická kriminalita je v drtivé většině případů motivována finančním zájmem. Tomu je ideálně přizpůsoben vyděračský škodlivý software označovaný jako ransomware. Ten se oběti nevědomky dostane do počítače, následně dochází k zašifrování dat a nakonec se objeví informace, že data jsou zašifrována a aby je dotyčná osoba získala zpět, musí zaplatit výkupné.

Trendem v této oblasti je, že zatímco dříve se útočníci plošně soustředili na běžné uživatele a požadovali výkupné v řádech okolo 100 eur, což je částka, kterou jsou lidé ochotni zaplatit za záchranu svých fotografií, běžných dokumentů apod., nyní se útočníci více soustředí na větší organizace. Dochází tak k sofistikovaným útokům, jejichž příprava nezahrnuje pouze nalézání jednotlivých zranitelností pro provedení útoku, ale rovněž pachatelé zkoumají finanční aspekty jako obrat, zisk, aktiva dané společnosti. Podle toho stanovují výši výkupného tak, aby byla co nejvyšší, ale útočník měl současně naději, že oběť může částku zaplatit.

Následující obrázek ukazuje komunikaci, kdy na jedné straně poškozený uvádí, že požadovaný obnos je nad jeho možnosti, zatímco útočník tvrdí, že prověřil finanční dokumentaci společnosti a částka je realistická.

¹² Česká bankovní asociace (6. března 2022). ČBA varuje před podvodnými útoky na klienty bank. <https://cbaonline.cz/tz-cba-varuje-pred-podvodnymi-utoky-na-klienty-bank-utocnici-ve-zvysene-mire-cili-na-rusky-a-ukrajinsky-hovori-ci-obcany->.

Obrázek 2: Komunikace o zaplacení výkupného



Zdroj: Microsoft, 2021.¹³

Pachatelé dokáží rovněž útoky cílit na aktuálně kritická místa. Například nemocnice, které jsou v době covidu pod značným tlakem a je tak větší šance, že oběť výkupné zaplatí, aby dokázaly, v tomto případě, poskytovat zdravotní péči. Jinou formou jak oběť přimět k platbě, je výhrůžka, že např. citlivé informace dané firmy budou přeprodány konkurenci.

Zřejmě nejznámějším ransomware útokem v České republice v poslední době byl útok na Ředitelství silnic a dálnic (ŘSD).¹⁴ Útok způsobil natolik rozsáhlé škody, že vedení ŘSD zvažovalo, zda není výhodnější zaplatit výkupné v řádech desítek milionů korun.¹⁵ Zde by ale vznikl značný problém, jelikož organizace hospodaří s veřejnými prostředky a v jejím rozpočtu se pochopitelně nenachází

¹³ Microsoft (říjen 2021). *Microsoft Digital Defense Report*. <https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report>.

¹⁴ České noviny (20. května 2022). *NÚKIB: Kyberútok na weby ŘSD byl profesionální, zašifroval data*. <https://www.ceskenoviny.cz/zpravy/nukib-kyberutok-na-weby-rsd-byl-profesionalni-zasifroval-data/2208924>.

¹⁵ Novinky.cz (9. června 2022). *Hackeri chtějí po ŘSD desítky milionů za odblokování přístupu k datům*. <https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/hackeri-chteji-po-rsd-desitky-milionu-za-odblokovani-pristupu-k-datum-40399634>.

kapitola na úhradu výkupného pro pachatele trestné činnosti, jinými slovy na financování trestné činnosti. Navíc, pokud by k uhrazení došlo, jednalo by se o stimul pro další útoky na české instituce s tím, že Češi jsou na útoky nepřipraveni a následně ochotně zaplatí. ŘSD se rozhodlo výkupné nezaplatit, i když se s důsledky útoku bude potýkat ještě dlouho a škody budou značné.

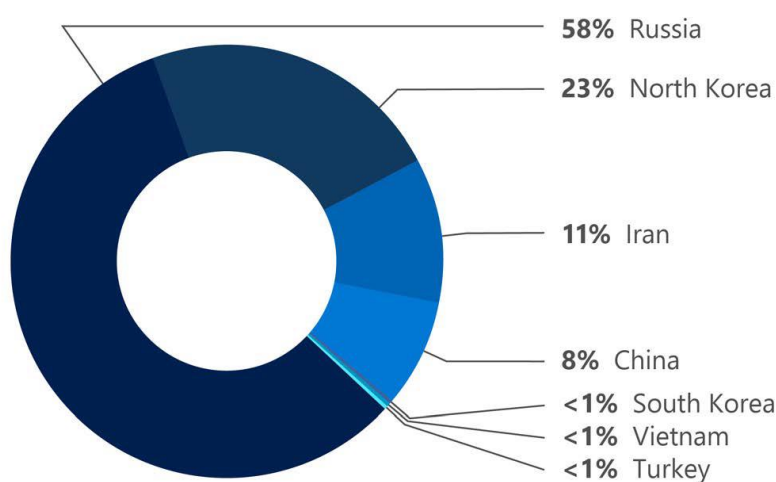
Tento a další případy ukazují, jak je důležité data správně zálohovat a rovněž proces zálohování testovat, zda je skutečně plně funkční. Nicméně ani zaplacení výkupného není zárukou, že se data dostanou zpět k jejich vlastníkovi. Jak uvádí zmiňovaná zpráva společnosti Microsoft, organizacím, které zaplatily výkupné, se v průměru dostalo 65 % jejich dat. Téměř ve třetině případů získaly zpět méně než polovinu dat.¹⁶

Státní aktéři

Kyberprostor je místem, kde se promítají i mocenské ambice jednotlivých států, resp. jejich vlád. Nedemokratické režimy v něm provádějí široké spektrum aktivit od kybernetických útoků, špionáže až po informační působení. Kyberprostor je do značné míry zrcadlem reálného světa. Jednotlivé konflikty se tak z hlediska geografické distribuce promítají i do něj.

Pokud se zaměříme na útoky dle země původu za období červen 2020 – červen 2021 podle Microsoft Digital Defense Report, dominantní roli sehraává Ruská federace (58 %) následovaná Severní Koreou (23 %), Íránem (11 %) a Čínou (8 %).

Graf 1: Útoky dle země původu



Zdroj: Microsoft, 2021.¹⁷

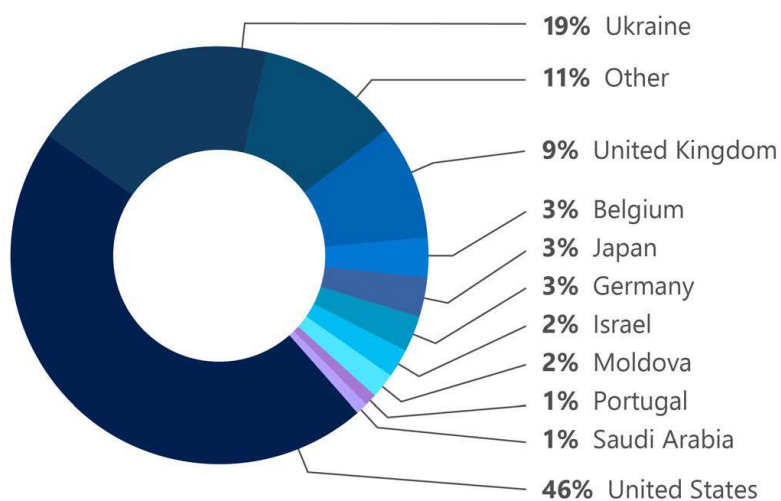
Cílem se naopak stávají země, které lze považovat za jejich politické oponenty. Prim tak hrají Spojené státy (46 %) následované Ukrajinou (19 %), Spojeným královstvím (9 %) a Belgií, Japonskem a Německem (3 %). Belgie, ačkoliv se jedná o poměrně malou zemi, je pro nepřátelské státní aktéry zajímavá vzhledem k umístění centrálních mezinárodních institucí EU a NATO. Útoky nebývají motivované

¹⁶ Microsoft (říjen 2021). *Microsoft Digital Defense Report*. <https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report>.

¹⁷ Microsoft (říjen 2021). *Microsoft Digital Defense Report*. <https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report>.

pouze politickým zájmem, ale mají za cíl pro autoritářské režimy, které se často nacházejí v izolaci a pod sankcemi, získávat finanční prostředky. To je typické pro Severní Koreu.¹⁸

Graf 2: Cílové země útoků



Zdroj: Microsoft, 2021.¹⁹

Zejména Ukrajina se od počátku agrese Ruské federace v roce 2014 potýká s řadou kybernetických útoků. Ty mají za cíl nejen získávat citlivé informace, ale rovněž útočit na infrastrukturu země (energetika, doprava, média, komunikace, banky atd.). Jejich motivací je jednoduše navozovat problémy a oslabovat důvěru ve vládu a obecně v instituce.

Těsně před vypuknutím únorové invaze byl na Ukrajinu veden útok malwarem nazvaným HermeticWiper, který způsobuje smazání dat včetně části systému. Ten napadl stovky zařízení ukrajinských společností a státních institucí. Podle dostupných informací wiper mířil na finanční instituce a vládní kontraktory.²⁰

DDoS útoky jako nástroj odplaty

Jedním z obvyklých typů útoků, které jsou poměrně jednoduché a levné (jejich cena se podle Microsoft Digital Defense Report pohybuje v řádech stovek USD), jsou DDoS (Distributed Denial of Service) útoky. Při nich je cílová služba zahlcena příliš mnoha připojeními a požadavky, což vede k jejímu výpadku.

Je v podstatě pravidlem, že když určitá suverénní země učiní rozhodnutí, které se nelíbí kremelskému režimu, jako odplata přijdou právě DDoS útoky na weby jejích ministerstev, služeb eGovernmentu, médií, bank, dopravců apod. U tohoto typu útoku se plně ukazuje zmiňované zrcadlení reálného světa do virtuálního.

¹⁸ BBC (14. ledna 2022). *North Korea hackers stole \$400m of cryptocurrency in 2021, report says.* <https://www.bbc.com/news/business-59990477>.

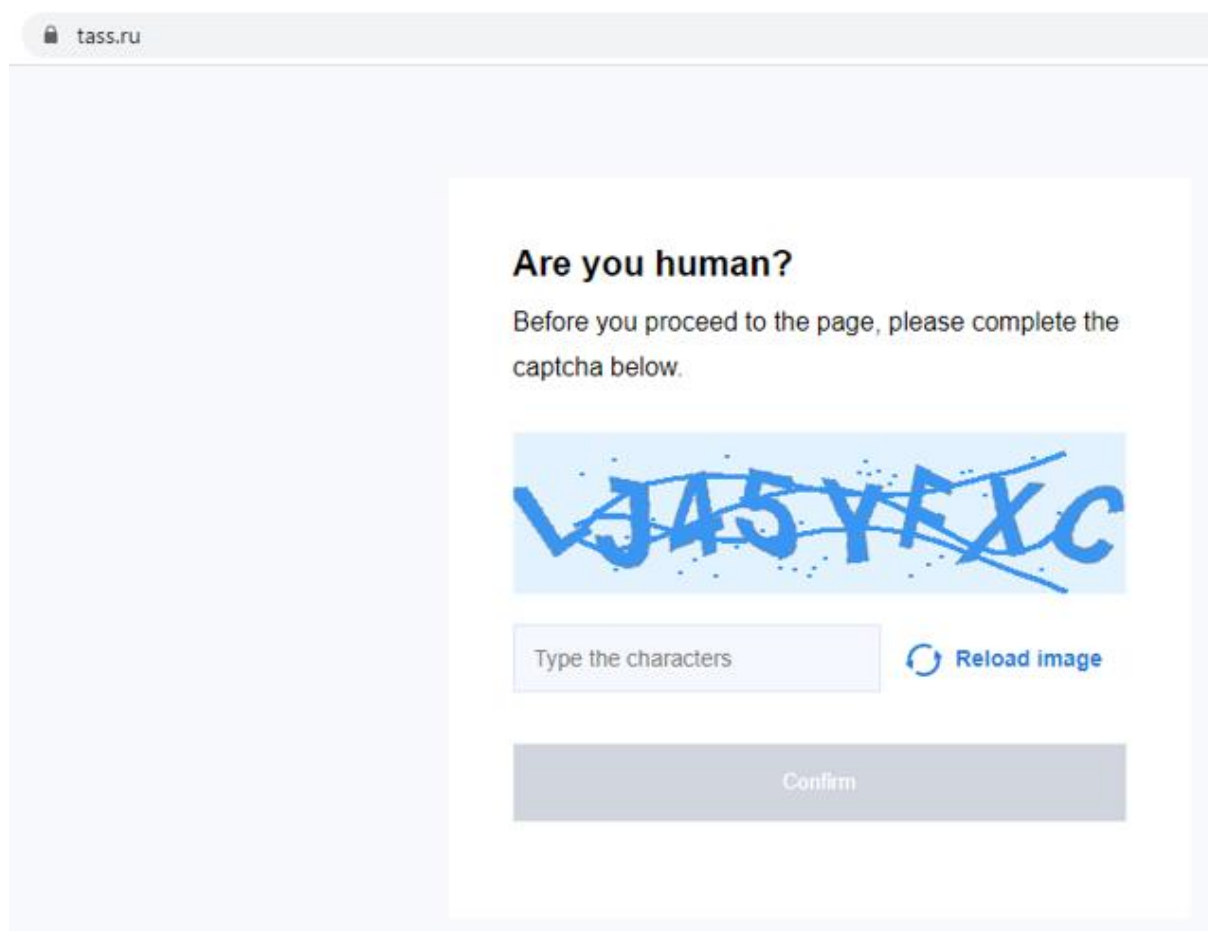
¹⁹ Microsoft (říjen 2021). *Microsoft Digital Defense Report.* <https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report>.

²⁰ NÚKIB (25. února 2022). *Upozornění na výskyt nového destruktivního malware typu wiper.* <https://www.nukib.cz/cs/infoservis/hrozby/1813-upozorneni-na-vyskyt-noveho-destruktivniho-malware-typu-wiper/>.

Poslední větší vlnu těchto útoků zažila Česká republika v dubnu tohoto roku. K útokům se přihlásila ruská skupina Killnet.²¹ Podobná situace nastala i v Litvě, když země přes své území omezila dopravu zboží z a do Kaliningradské oblasti Ruské federace.²² A stejně tak i v Norsku, když nastal obdobný logistický problém tentokrát na Špicberkách.²³

Po únorové invazi se cílem DDoS útoků stává i Ruská federace, její instituce a „médiá“. Za útoky stály různé hacktivistické skupiny jako například Anonymous. Cílem bylo způsobit Rusům problémy a omezit šíření válečné propagandy. Na situaci reagovaly i jednotlivé tamní portály, které aktivovaly ochranu před DDoS útoky. Ta spočívá v odfiltrování reálných uživatelů od botů dříve, než se k požadované službě připojí.

Obrázek 3: CAPTCHA při přístupu na web ruské státní agentury TASS



Zdroj: TASS, 2022.

²¹ iRozhlas.cz (27. dubna 2022). *Vnitro, hasiči i policie. Weby ministerstva čelily DDoS útoku, přihlásila se k nim ruská skupina.* https://www.irozhlas.cz/zpravy-domov/rusko-killnet-ddos-ministerstvo-vnitro_2204270856_pj.

²² iRozhlas.cz (27. června 2022). *Litevské weby pod kybernetickým útokem. Přihlásili se k němu proruští hackeři z Killnetu.* https://www.irozhlas.cz/zpravy-svet/litva-kyberutok-hacker-killnet-ddos-valka-na-ukrajine_2206271641_gut.

²³ Novinky.cz (29. června 2022). *Norsko se stalo terčem kybernetického útoku, podezírá proruskou skupinu.* <https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/norsko-se-stalo-tercem-kybernetickeho-utoku-podezira-proruskou-skupinu-40401639>.

Dezinformace v kyberprostoru

Kyberprostor lze rovněž považovat za informační prostor. Vzhledem k jeho univerzální přístupnosti a do značné míry absence regulace (není např. potřeba licence pro rozhlasové a televizní vysílání) je využíván i pro šíření dezinformací, a to ze strany státních aktérů s mocenskými ambicemi, jejich místních spojenců a rovněž osob, které šíří dezinformace za účelem výdělku.

V České republice se tzv. fake news šíří hlavně prostřednictvím dezinformačních webů vydávajících se za zpravodajské, na sociálních sítích a v řetězových e-mailech cílících především na seniory.

Zatímco weby ztrácejí na popularitě, k čemuž přispěla i jejich únorová blokáda, těžiště se stále více přesouvá do oblastí sociálních sítí, kde působí řada tzv. aktivistů, trollů a dalších uživatelů, kteří dezinformace vytvářejí, přejímají a dále šíří.

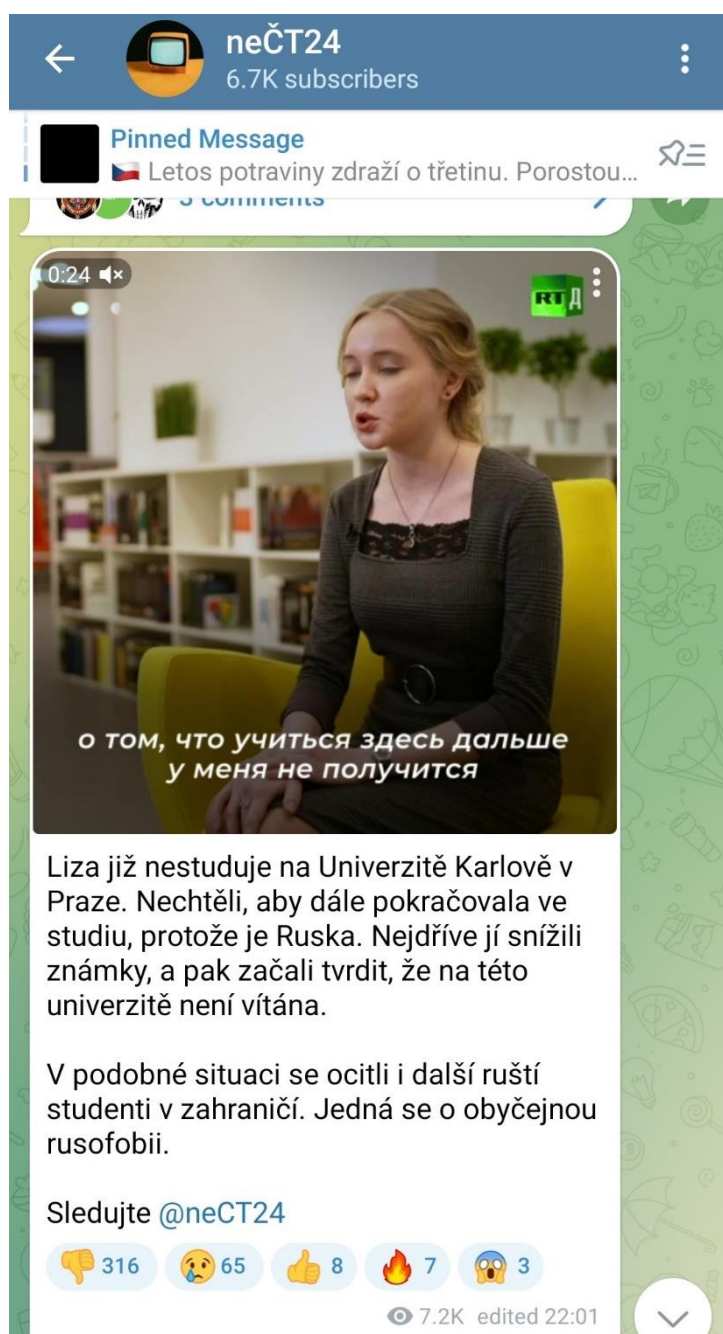
Pokles návštěvnosti dezinformačních webů je dlouhodobým trendem. Ty nicméně na blokaci reagovaly a jednoduše se přesunuly na novou doménu či zvolily jiný komunikační kanál. Příkladem je zablokovaný ruský státní propagandistický web Sputnik fungující v českém jazyce.

Po jeho zablokování vznikl na sociální síti Telegram kanál Sputniku s názvem „neČT24“, což má navozovat dojem, že se jedná o nějaký „nezávislý“ zdroj a nikoliv o ruskou státní agenturu podléhající Kremlu.

Na tomto kanálu se například objevila lživá reportáž od ruské státní televize RT (dříve Russia Today). V ní vystupuje údajná bývalá studentka Univerzity Karlovy, které mělo být studium ukončeno vzhledem k tomu, že pochází z Ruska. Problém je ale v tom, že daná studentka na Univerzitu Karlovu nikdy nenastoupila.²⁴

²⁴ Pika, T. (10. května 2022). *Případ ruské studentky Lizy z reportáže RT? Přihlásila se na jiný obor, na školu nikdy nenastoupila*. iRozhlas.cz. https://www.irozhlas.cz/zpravy-domov/praha-univerzita-karlova-liza-reportaz-russia-today_2205100500_pik.

Obrázek 4: Údajná oběť rusofobie



Zdroj: Telegram, neČT24, 2022.

Vzhledem k tomu, že v České republice síť Telegram není příliš populární, obsah kanálu „neČT24“ spamují napříč Facebookem falešné účty trollů, které ho vkládají do jednotlivých skupin či diskusí pod příspěvky a články zpravodajských webů. Ovládnutím diskusí se snaží podkopat důvěru v tradiční média nebo alespoň navodit dojem, že „všichni lžou“.

Obrázek 5: Šíření obsahu Sputniku anonymním trollem



Zdroj: Facebook, 2022.

Řetězové e-maily týkající se celospolečenských témat, jako jsou politická situace, migrace či válka, dostává 37 % Čechů. Část z nich, konkrétně pak 460 tisíc, je poté přeposílá dál.²⁵

Oblast dezinformací se logicky rovněž přizpůsobuje situaci v reálném světě. Zatímco tradiční proruští aktivisté si v předchozích dvou letech udělali odbočku ke covidu, rouškám a vakcínám, nyní se vrátili ke svému původnímu tématu. Současně se k nim přidala i tzv. anticovid scéna, která okamžitě přesedlala na (pro)ruské dezinformace, propagandu a obhajobu ruské invaze.

²⁵ CEDMO (11. července 2022). *Více než třetina Čechů dostává řetězové emaily, statisíce je přeposílají dál.* <https://cedmohub.eu/cs/vice-nez-tretina-cechu-dostava-retezove-emaily-statisice-je-preposilaji-dal/>.

Další politické aspekty

V oblasti kyberbezpečnosti dále vyvstávají otázky spojené zejména s dodavateli z nedemokratických zemí. Jedná se nejen o problematické dovozní závislosti, ale rovněž o nedůvěryhodnost takových dodavatelů, kteří jsou fakticky ovládáni tamním režimem. Tato rizika se ukázala při debatě o výstavbě 5G sítí. NÚKIB také varoval před používáním chytrých elektroměrů ze zemí s nedůvěryhodným právním prostředím.²⁶ Rizikem se tak stávají i prvky tzv. chytrých domácností a obecně internet věcí (internet of things).

Závěry a doporučení

Kyberbezpečnost je horizontálním tématem a vyžaduje zapojení všech částí společnosti. Zásadním principem je posilování odolnosti, kdy rozhodující roli hraje kontinuální vzdělávání a informovanost reagující na aktuální trendy. Neméně důležitá je tzv. kybernetická hygiena (používání antiviru, jasně stanovená uživatelská práva, multifaktorová autentizace, pravidelné aktualizace a ochrana dat), která podle společnosti Microsoft dokáže ochránit před 98 % útoků.²⁷

Důležitá je rovněž kvalitní a efektivní regulace, která by neměla bránit rozvoji, ale současně by měla zabránit negativním dopadům. Z hlediska problematických závislostí na technologiích z třetích potenciálně rizikových zemí je důležité zvažovat i politický aspekt (risk based regulation).

V globálním světě a ve světě internetu, který nezná hranice, je taktéž zásadní mezinárodní spolupráce zejména s hodnotově blízkými partnery. A stejně tak spolupráce veřejného a soukromého sektoru a dále institucí zajišťujících bezpečnost státu s vědeckovýzkumnými organizacemi (systémy včasné detekce, umělá inteligence apod.).

Kromě kritické a významné informační infrastruktury nelze zapomínat ani na další oblasti důležité pro chod státu (zásobování vodou a potravinami, doprava, zdravotnictví, průmysl 4.0 apod.). Jak již bylo zmíněno, útočníci se dokáží rychle adaptovat a útočit na místa aktuálně citlivá (nemocnice v době covidu).

Jelikož ochrana není nikdy 100%, důležitá je snaha o minimalizaci škod při útoku v budoucnu. Jinými slovy provádět zálohy a proces zálohování průběžně kontrolovat, což snižuje potenciál pro vydírání v případě ransomware útoků. Na místě je mít zpracované tzv. contingency plans stanovující postupy, jak v případě určitého incidentu jednat.

Dlouhodobým problémem je nedostatek odborníků na kyberbezpečnost. Státní organizace se také potýkají s problémem, že jen těžko mohou konkurovat soukromému sektoru v oblasti IT. Na místě je jednak otevírání nových studijních oborů zaměřených na kyberbezpečnost, ale současně učinit práci „pro stát“ atraktivnější. Jednotlivé instituce dále upozorňují na nedostatek nejen technických pracovníků, ale i manažerů a analytiků kybernetické bezpečnosti.

Mezi aktuální výzvy patří i kybernetické hrozby ve vztahu k proměně výkonu práce (home office) a stále se rozvíjející oblast internetu věcí (internet of things), které mohou přinášet nová rizika. Na vzestupu

²⁶ NÚKIB (30. května 2022). *NÚKIB vydal Varování před použitím chytrých elektroměrů ze zemí s nedůvěryhodným právním prostředím*. <https://nukib.cz/cs/infoservis/hrozby/1837-nukib-vydal-varovani-pred-pouzitim-chytrych-elektromeru-ze-zemi-s-neduvveryhodnym-pravnim-prostredim/>.

²⁷ Microsoft (říjen 2021). *Microsoft Digital Defense Report*. <https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report>.

jsou i tzv. supply chain attacks.²⁸ Obecným trendem také je, že se snižuje doba od objevení zranitelnosti k jejímu následnému zneužití. V budoucnu bude dozajista čím dál větší otázkou bezpečnost autonomních dopravních prostředků či inteligentních měst (smart cities).

Do oblasti kybernetické bezpečnosti se také stále více prolínají témata jako zahraniční politika, kybernetická diplomacie a digitální suverenita. Kyberbezpečnost tak nemá jen úroveň národní, ale také evropskou a globální, což bude vzhledem k současnému mezinárodnímu vývoji stále více akcentováno. Ostatně posílení evropských obranných kapacit a bezpečnost kybernetického prostoru je jednou z priorit českého předsednictví v Radě Evropské unie.²⁹

²⁸ Útoky na dodavatele softwarových řešení, kdy jsou jejich produkty napadeny, což představuje hrozbu pro koncového uživatele.

²⁹ České předsednictví v Radě Evropské unie (2022). *Priority*. <https://czech-presidency.consilium.europa.eu/cs/program/priority/>.

Zdroje

Adamcová, P. (14. června 2021). *Na vybilení účtu stačí jeden telefonát. Poslechněte si, jak útočník láká z oběti data.* Aktuálně.cz. <https://zpravy.aktualne.cz/finance/banky-vishing/r~ef8a7f48ca7911ebad06ac1f6b220ee8/>.

BBC (14. ledna 2022). *North Korea hackers stole \$400m of cryptocurrency in 2021, report says.* <https://www.bbc.com/news/business-59990477>.

CEDMO (11. července 2022). *Více než třetina Čechů dostává řetězové emaily, statisíce je přeposílají dál.* <https://cedmohub.eu/cs/vice-nez-tretina-cechu-dostava-retezove-emaily-statisice-je-preposilaji-dal/>.

Česká bankovní asociace (6. března 2022). *ČBA varuje před podvodnými útoky na klienty bank.* <https://cbaonline.cz/tz-cba-varuje-pred-podvodnymi-utoky-na-klienty-bank-utocnici-ve-zvysene-mire-cili-na-rusky-a-ukrajinsky-hovorici-obcany->.

České noviny (20. května 2022). *NÚKIB: Kyberútok na weby ŘSD byl profesionální, zašifroval data.* <https://www.ceskenoviny.cz/zpravy/nukib-kyberutok-na-weby-rsd-byl-profesionalni-zasifroval-data/2208924>.

České předsednictví v Radě Evropské unie (2022). *Priority.* <https://czech-presidency.consilium.europa.eu/cs/program/priority/>.

Finanční správa (22. března 2021). *Finanční správa varuje před podvodnými e-maily.* <https://www.financnisprava.cz/cs/financni-sprava/novinky/novinky-2021/financni-sprava-varuje-pred-podvodnymi-e-mailly>.

iDNES.cz (10. června 2022). *Nabízeli ojetá auta na internetu a podvedli skoro 200 lidí, zadržela je policie.* https://www.idnes.cz/zpravy/cerna-kronika/policie-podvody-ojeta-auta-internet-rumunsko-cesko.A220610_150156_domaci_pukk.

Institut pro politiku a společnost (13. května 2022). *VII International Conference Digital Czech Republic 2022.* <https://youtu.be/lqupxh9AjZ4>.

iRozhlas.cz (27. června 2022). *Litvské weby pod kybernetickým útokem. Přihlásili se k němu proruští hackeři z Killnetu.* https://www.irozhlas.cz/zpravy-svet/litva-kyberutok-hacker-killnet-ddos-valka-na-ukrajine_2206271641_gut.

iRozhlas.cz (27. dubna 2022). *Vnitro, hasiči i policie. Weby ministerstva čelily DDoS útoku, přihlásila se k nim ruská skupina.* https://www.irozhlas.cz/zpravy-domov/rusko-killnet-ddos-ministerstvo-vnitra_2204270856_pj.

Microsoft (říjen 2021). *Microsoft Digital Defense Report.* <https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report>.

Natoaktual (15. června 2016). *Alianční ministři obrany uznali kyberprostor za bojovou oblast.* https://www.natoaktual.cz/v-mediich/aliancni-ministri-obrany-uznali-kyberprostor-za-bojovou-oblast.A160615_171942_na_media_m02.

Novinky.cz (9. června 2022). *Hackeři chtějí po ŘSD desítky milionů za odblokování přístupu k datům.* <https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/hackeri-chteji-po-rsd-desitky-milionu-za-odblokovani-pristupu-k-datum-40399634>.

Novinky.cz (29. června 2022). *Norsko se stalo terčem kybernetického útoku, podezírá proruskou skupinu.* <https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/norsko-se-stalo-tercem-kybernetickeho-utoku-podezira-proruskou-skupinu-40401639>.

NÚKIB (30. května 2022). *NÚKIB vydal Varování před použitím chytrých elektroměrů ze zemí s nedůvěryhodným právním prostředím.* <https://nukib.cz/cs/infoservis/hrozby/1837-nukib-vydal-varovani-pred-pouzitim-chytrych-elektromeru-ze-zemi-s-neduveryhodnym-pravnim-prostredim/>.

NÚKIB (25. února 2022). *Upozornění na výskyt nového destruktivního malware typu wiper.* <https://www.nukib.cz/cs/infoservis/hrozby/1813-upozorneni-na-vyskyt-noveho-destruktivniho-malware-typu-wiper/>.

Pika, T. (10. května 2022). *Případ ruské studentky Lizy z reportáže RT? Přihlásila se na jiný obor, na školu nikdy nenastoupila.* iRozhlas.cz. https://www.irozhlas.cz/zpravy-domov/praha-univerzita-karlova-liza-reportaz-russia-today_2205100500_pik.

Policie České republiky (28. června 2022). *Výroční zpráva NCOZ 2021.* <https://www.policie.cz/clanek/vyrocní-zprava-ncoz-2021.aspx>.

Policie České republiky – KŘP Královéhradeckého kraje (6. května 2022). *"Americký voják opět v akci".* <https://www.policie.cz/clanek/americky-vojak-opet-v-akci-80760.aspx>.

Sobotková, M. (18. února 2021). *Ja tebja ljublju! Jak ruské krásy loví české ženichy a obírají je o peníze.* Seznam Zprávy. <https://www.seznamzpravy.cz/clanek/ja-tebja-ljublju-jak-ruske-krasky-lovi-ceske-zenichy-a-obiraji-je-o-penize-142435>.

Autor



ROMAN MÁCA

Analytik

Roman Máca vystudoval obor Mezinárodní rozvojová studia na Univerzitě Palackého v Olomouci. Dlouhodobě se věnuje zejména mezinárodním tématům s důrazem na oblast obrany a bezpečnosti, konkrétně se zaměřením na nové hrozby. Jako řešitel pracoval na regionálních, celostátních i mezinárodních projektech. Je autorem řady článků a příspěvků na konferencích. Častým cílem jeho cest je Ukrajina, kde se zapojuje do projektů podpory občanské společnosti.

Vydavatel



INSTITUT PRO POLITIKU A SPOLEČNOST

Posláním Institutu je zkvalitňování českého politického a veřejného prostředí prostřednictvím profesionální a otevřené diskuse a vytvoření živé platformy, která pojmenovává zásadní problémy, vypracovává jejich analýzy a nabízí recepty pro jejich řešení formou spolupráce expertů a politiků, mezinárodních konferencí, seminářů, veřejných diskuzí, politických a společenských analýz dostupných celé české společnosti. Jsme přesvědčeni, že otevřená odborná diskuse a poznání podstaty a příčin jednotlivých problémů jsou nutným předpokladem jakéhokoli úspěšného řešení problémů současné společnosti.



Martinská 2, 110 00 Praha 1



+420 602 502 674



www.politikaspolecnost.cz



office@politikaspolecnost.cz