Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost
Mučednická 1125/31
616 00 Brno – Žabovřesky
IČ: 05800226
ID datové schránky: zzfnkp3

Spisová značka:
350-647/2025-E
Číslo jednací:
6159/2025-NÚKIB-E/350

Brno 3. září 2025

VAROVÁNÍ

Národní úřad pro kybernetickou a informační bezpečnost, se sídlem Mučednická 1125/31, 616 00 Brno (dále jen „Úřad“), podle § 12 odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „zákon o kybernetické bezpečnosti“) vydává toto

varování

před hrozbou v oblasti kybernetické bezpečnosti spočívající

1. v předávání systémových a uživatelských dat do Čínské lidové republiky, na území zvláštních administrativních oblastí či subjektům usídleným na území Čínské lidové republiky nebo zvláštních administrativních oblastí, a
2. ve vzdálené správě technických aktiv vykonávané z území Čínské lidové republiky, zvláštních administrativních oblastí či ze strany subjektů usídlených na území Čínské lidové republiky nebo zvláštních administrativních oblastí.

Úřad hrozbu hodnotí na úrovni **Vysoká – Hrozba je pravděpodobná až velmi pravděpodobná**.

Orgány a osoby, které jsou povinny zavést bezpečnostní opatření podle zákona o kybernetické bezpečnosti, jsou povinny tuto hrozbu v souvislosti s řízením rizik podle § 5 odst. 1 písm. d) vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „vyhláška o kybernetické bezpečnosti“), hodnotit na úrovni Vysoká – Hrozba je pravděpodobná až velmi pravděpodobná. V případě, že povinná osoba využívá v souladu s odst. 5 přílohy č. 2 vyhlášky o kybernetické bezpečnosti jinou metodu pro hodnocení rizik, je nutno tuto hrozbu hodnotit v rámci této metody na srovnatelné úrovni, jako by tomu bylo v případě postupu podle § 5 odst. 1 písm. d) vyhlášky o kybernetické bezpečnosti.

Mučednická 1125/31, 616 00 Brno
tel.: 541 110 777, e-mail: posta@nukib.gov.cz, datová schránka: zzfnkp3, nukib.gov.cz

ODŮVODNĚNÍ

1. Zákon o kybernetické bezpečnosti ve svém § 11 odst. 1 definuje opatření (úkony sloužící k ochraně před hrozbou nebo incidentem v oblasti kybernetické bezpečnosti nebo k jejich řešení), mezi něž podle § 11 odst. 2 písm. a) zákona o kybernetické bezpečnosti patří mimo jiné i varování. Podle § 12 odst. 1 zákona o kybernetické bezpečnosti Úřad vydá varování, dozví-li se o hrozbě v oblasti kybernetické bezpečnosti.

2. Na základě skutečností zjištěných při výkonu své působnosti, doplněných o neutajované i utajované informace získané od domácích i zahraničních partnerů, dospěl Úřad k tomu, že předávání systémových a uživatelských dat do Čínské lidové republiky (dále jen „ČLR“), na území zvláštních administrativních oblastí či subjektům usídleným na území ČLR nebo zvláštních administrativních oblastí, resp. umožnění výkonu vzdálené správy technických aktiv z území ČLR, zvláštních administrativních oblastí či ze strany subjektů usídlených na území ČLR nebo zvláštních administrativních oblastí, představuje hrozbu v oblasti kybernetické bezpečnosti, a proto podle § 12 odst. 1 zákona o kybernetické bezpečnosti vydává toto varování.

3. K vydání tohoto varování vedla kombinace následujících poznatků a zjištění.

4. Při posuzování, zda předávání systémových a uživatelských dat, resp. umožnění výkonu vzdálené správy technických aktiv tak, jak je popsáno ve výrokové části tohoto varování, představuje z pohledu kybernetické bezpečnosti pro Českou republiku hrozbu, je nutné analyzovat celou řadu aspektů. Mezi ně se řadí mimo jiné např. důvěryhodnost právního prostředí ČLR a zvláštních administrativních oblastí. Úroveň důvěryhodnosti právního prostředí totiž přímo ovlivňuje i důvěryhodnost společností či subjektů na daných územích usídlených, neboť tyto společnosti, resp. subjekty, danému právnímu prostředí plně podléhají, a musí se jím tudíž řídit. Právní prostředí ČLR je ze strany Úřadu dlouhodobě monitorováno a analyzováno, na základě čehož v tomto ohledu Úřad v současné době na území ČLR eviduje některé platné právní předpisy, které v kombinaci s dalšími (níže uvedenými) zjištěními představují pro bezpečnost České republiky hrozbu. Dotčené právní předpisy totiž mimo jiné např. umožňují významné zásahy vládních orgánů do fungování soukromých společností či dávají vládním orgánům ČLR nástroje pro vynucení spolupráce soukromých firem při špionážních aktivitách ČLR, na což ostatně ve své výroční zprávě za rok 2024 upozorňuje i Bezpečnostní informační služba.

5. Jedná se např. o zákon o státní bezpečnosti (国家安全法) z roku 2015, který všem čínským občanům a organizacím ukládá obecnou povinnost poskytnout pomoc státním orgánům v otázkách státní bezpečnosti. Současně pak zákon o státní zpravodajské činnosti (中华人民共和国国家情报法) z roku 2017 stanovuje ve svém čl. 7, že každý občan a organizace musí podpořit národní zpravodajskou činnost, poskytnout součinnost a spolupráci a zachovat mlčenlivost o utajovaných záležitostech, o kterých se v souvislosti s národní zpravodajskou činností dozví. Dále zákon o státní kontrašpionážní činnosti (中华人民共和国反间谍法) z roku 2014 ukládá povinnost poskytnout součinnost a informace o zahraničních klientech čínských společností v případě, že je budou státní orgány podezřívat ze špionážní činnosti, přičemž dle jeho čl. 6 je tento zákon aplikovatelný i vůči institucím, organizacím a jednotlivcům, kteří organizují nebo financují špionážní aktivitu proti ČLR mimo její teritorium, kdy za

Mučednická 1125/31, 616 00 Brno
tel.: 541 110 777, e-mail: posta@nukib.gov.cz, datová schránka: zzfnkp3, nukib.gov.cz

špionáž mohou čínské orgány označit široké množství aktivit, a to vše bez možnosti nezávislého soudního přezkumu. Státní orgány ČLR mohou díky širokým a neurčitým definicím obsaženým v tomto zákoně (např. definice národní bezpečnosti) požadovat po společnostech poskytnutí téměř jakékoli informace, přičemž dané společnosti nemají nad drženými informacemi de facto žádnou kontrolu. V roce 2023 vstoupila v platnost novela tohoto zákona, která rozšířila nejen definici špionáže, ale obecně i celkový rozsah věcné působnosti tohoto zákona, v důsledku čehož se daný zákon vztahuje na jakékoliv dokumenty, data či předměty, o kterých čínské orgány určí, že mají spojitost s národní bezpečností. Dalším z těchto problematických předpisů je zákon o obchodních společnostech (中华人民共和国公司法 2013修订) z roku 2013 umožňující Komunistické straně Číny (dále jen „KSČ“) účinně ovlivňovat chod soukromých společností. Podle čl. 19 zmíněného zákona musí být totiž ve společnosti ustanovena organizace KSČ za účelem výkonu aktivit KSČ ve shodě s jejími stanovami, přičemž daná společnost musí pro tyto aktivity poskytnout nezbytné podmínky. Problematickými jsou pak i pravidla pro nahlašování zranitelností v síťových zařízeních (公安部关于印发网络产品安全漏洞管理规定的通知) z roku 2021, podle nichž mají výrobci technologií povinnost nahlašovat bezpečnostní zranitelnosti čínskému Ministerstvu průmyslu a IT (dále jen „MPIT“), a to nejpozději do dvou dnů od jejich zjištění. MPIT následně nahlašuje takovýto nález Ministerstvu státní bezpečnosti ČLR a dalším relevantním institucím, přičemž je výrobcům technologií zakázáno zveřejňovat tyto zranitelnosti nebo je nahlašovat zahraničním organizacím a jednotlivcům.

6. Všechny tyto právní předpisy umožňují zvýšenou kontrolu vládních orgánů ČLR nad čínským internetovým prostředním a (mimo jiné i) technologickými společnostmi. KSČ přitom současně zasahuje do všech oblastí občanské společnosti (včetně nevládních organizací, státních podniků, soukromých společností a poboček zahraničních společností se sídlem v ČLR). Čínský stát navíc může do fungování a struktur mnoha formálně soukromých společností zasahovat i skrze vlastnické podíly (tzv. Golden Shares), přičemž státní dohled nad těmito společnostmi je ještě více prohlubován právě činností stranických buněk KSČ, které jsou v těchto společnostech na základě výše zmiňovaného zákona o obchodních společnostech (中华人民共和国公司法 2013修订) z roku 2013 povinně zřizovány. Poznatky partnerů Úřadu ostatně potvrzují, že KSČ ovlivňuje rozhodovací procesy např. při jmenování zaměstnanců jednotlivých společností. Současně také platí, že je vyvíjen silný tlak na to, aby právě členové KSČ obsazovali manažerské pozice v těchto společnostech.

7. Výše uvedené právní předpisy ČLR, které jsou z pohledu bezpečnosti České republiky hodnoceny jako problematické, jsou přitom reálně aplikovatelné též na území zvláštních administrativních oblastí, jimiž jsou ke dni vydání tohoto varování Hongkong a Macao. Jedná se o teritoria, která spadají pod suverenitu ČLR, ale netvoří část pevninské Číny. Tato teritoria si sice udržují své ekonomické systémy a vysokou míru autonomie, ovšem vláda pevninské Číny zůstává i nadále odpovědná za obrannou a zahraniční politiku těchto zvláštních administrativních oblastí. Dokladem úzkého propojení mezi ČLR a zvláštními administrativními oblastmi je např. způsob jmenování nejvyšších představitelů Hongkongu či Macaa, tedy předsedů Výkonné rady, kteří jsou sice voleni volebními komisemi uvedených zvláštních administrativních oblastí, avšak do jejich funkce je definitivně jmenuje až čínská ústřední vláda.

Mučednická 1125/31, 616 00 Brno
tel.: 541 110 777, e-mail: posta@nukib.gov.cz, datová schránka: zzfnkp3, nukib.gov.cz

8. Přímo na území Hongkongu jsou přitom platné některé další právní předpisy, které lze z pohledu bezpečnosti České republiky rovněž považovat za problematické. Jedná se např. o základní zákon z roku 1990 (香港基本法, Basic Law), jehož čl. 23 zmocňuje hongkongskou zákonodárnou moc k přijetí vlastních bezpečnostních zákonů, které by poskytovaly ochranu před různými protistátními činy (včetně vlastizrady či rozvracení státu), ovšem ne pouze ve vztahu k Hongkongu, nýbrž k celé ČLR, čímž mocenské a bezpečnostní zájmy ČLR vstupují přímo do ústavního zřízení Hongkongu. Dalším z těchto předpisů je pak nařízení o ochraně státní bezpečnosti z roku 2024 (護國家安全條例, Safeguarding National Security Ordinance), jehož prostřednictvím je v podstatě usilováno o integraci rámce státní bezpečnosti ČLR do legislativního rámce Hongkongu, v důsledku čehož v tomto právním předpisu obsažený pojem „státní tajemství“ může souviset de facto s jakýmkoli aktem ekonomického, společenského, technologického nebo vědeckého rázu, a to i v případě, že dané předtím jako státní tajemství označeno nebylo. Jedná se tedy o velice vágní a nejasný právní rámec.

9. Z pohledu bezpečnosti České republiky problematické právní předpisy lze identifikovat též na území Macaa. Jedná se např. o základní zákon z roku 1993 (中华人民共和国澳门特别行政区基本法, Basic Law), který (stejně jako v případě Hongkongu) zmocňuje zákonodárnou moc Macaa k přijetí vlastních bezpečnostních zákonů, které by poskytovaly ochranu před různými protistátními činy (a to včetně vlastizrady či rozvracení státu), ovšem ne pouze ve vztahu k Macau, nýbrž k celé ČLR, čímž mocenské a bezpečnostní zájmy ČLR vstupují přímo do ústavního zřízení Macaa. Dalším z těchto právních předpisů je zákon o kybernetické bezpečnosti z roku 2019 (網絡安全法, Cybersecurity Law), který se týká kritické infrastruktury a jenž dává orgánu Macaa zkráceně označovanému jako CARIC (Cybersecurity Incident Alert and Response Center) mandát provádět v reálném čase monitoring počítačových dat přenášených mezi provozovateli sítí kritické infrastruktury a internetem. Nad CARIC přitom neexistuje žádný dozorový mechanismus, čímž se otevírá značný prostor pro sledování ze strany orgánů Macaa.

10. Z výše provedené analýzy právního prostředí ČLR i zvláštních administrativních oblastí vyplývá, že na těchto územích platné právní předpisy umožňují vládním orgánům vyvíjet aktivní a efektivní nátlak na soukromé společnosti či subjekty, které mohou být tímto způsobem nuceny stavět zájmy ČLR či zvláštních administrativních oblastí nad zájmy subjektů, jejichž systémová a uživatelská data jsou na výše uvedená území předávána či jejichž technická aktiva jsou z těchto území vzdáleně spravována tak, jak je uvedeno ve výrokové části tohoto varování.

11. Rizikovost přenosu dat do ČLR, popř. na území zvláštních administrativních oblastí, dokládá dále též studie z roku 2021 nazvaná „Government access to data in third countries“, kterou pro Evropský sbor pro ochranu osobních údajů vypracovali výzkumníci z Centre for IT and IP Law z Katolické univerzity v Lovani. Tato studie uvádí, že zákony ČLR umožňují široký přístup státních orgánů ČLR k datům, a to bez dostatečné nezávislé kontroly. Dle Úřadu se však jedná o přístup, jenž je v příkrém rozporu s principy nařízení Evropského parlamentu a rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES, které vyžaduje naopak transparentnost, proporcionalitu a právní ochranu subjektů údajů.

Mučednická 1125/31, 616 00 Brno
tel.: 541 110 777, e-mail: posta@nukib.gov.cz, datová schránka: zzfnkp3, nukib.gov.cz

12. Metodický pokyn Evropského sboru pro ochranu osobních údajů nazvaný „Guidelines 02/2024 on Article 48 GDPR“ pak současně stanovuje, že většina přenosů dat do ČLR je riziková a právně neudržitelná bez dalších opatření. Rizikovost přenosu dat do ČLR je přitom umocněna i čínským zákonem o ochraně osobních údajů (中华人民共和国个人信息保护法, Personal Information Protection Law of the People's Republic of China) z roku 2021, který KSČ svěřuje rozsáhlé pravomoci v oblasti kontroly a vynucování poskytování informací z důvodu národní bezpečnosti, která je obdobně jako další pojmy v daném zákoně definována vágně a velmi široce.

13. Nejasný právní rámec, který vládním orgánům ČLR reálně umožňuje v zásadě neomezený přístup k veškerým datům, která jsou na území ČLR (a přeneseně též na území zvláštních administrativních oblastí) předávána, představuje z pohledu bezpečnosti České republiky značnou hrozbu. Tím spíše, pokud se předávaná (ať již systémová, či uživatelská) data týkají systémů, na něž dopadá regulace zákona o kybernetické bezpečnosti. Jedná se totiž o páteřní systémy zajišťující poskytování velmi důležitých služeb. Narušení dostupnosti, důvěrnosti či integrity těchto systémů, resp. dat v nich obsažených, by tudíž potenciálně mohlo mít významný dopad na značnou část osob nacházejících se na území České republiky. Z téhož důvodu je současně nutné proaktivně přistupovat také k hrozbě, která spočívá v umožnění vzdálené správy technických aktiv těchto systémů vykonávané tak, jak je popsáno ve výroku tohoto varování.

14. K vydání tohoto varování Úřad dospěl též s ohledem na objektivně neustále rostoucí vliv čínských státních nebo státem podporovaných společností v oblasti evropské kritické infrastruktury (např. energetika, 5G sítě či datové toky), na nějž ve svém usnesení ze dne 17. ledna 2024, o bezpečnostních a obranných důsledcích vlivu Číny na kritickou infrastrukturu v Evropské unii (2023/2072(INI)), upozorňuje i Evropský parlament. Zmíněné usnesení uvádí, že přenosy dat konkrétně do čínských cloudů či datacenter, podléhající (výše popsané, z pohledu bezpečnosti České republiky problematické) legislativě ČLR, jsou neslučitelné s evropskými principy ochrany soukromí a zajišťování bezpečnosti.

15. Čínské investice do české a evropské kritické infrastruktury, stejně jako čínská dominance ve strategických dodavatelských řetězcích, jsou přitom Bezpečnostní strategií České republiky z roku 2023 výslovně označeny za riziko. Z bližší analýzy významných čínských technologických společností vyplývá riziko zneužití uživatelských dat. Ta mohou být použita nejen pro komerční účely, ale s ohledem na legislativu ČLR i pro potřeby bezpečnostních složek a státu. Riziko zneužití těchto dat se zvyšuje s mírou propojení společnosti s ČLR.

16. Před nebezpečím spočívajícím v navyšování podílu čínských technologií zejména v prvcích kritické infrastruktury ve svých výročních zprávách opakovaně varuje i Bezpečnostní informační služba, která dlouhodobě zdůrazňuje, že mimo jiné technologická závislost České republiky na ČLR, jakožto autokratickém režimu majícím globální ambice vytvořit účinnou protiváhu zemím G7, představuje stav, na nějž je nutné aktivně reagovat. Ve své výroční zprávě za rok 2024 pak Bezpečnostní informační služba již přímo uvádí, že „čínská snaha o obchodní a technologickou dominanci představuje výzvu pro ochranu českých společností, jejich know-how a dodavatelských

Mučednická 1125/31, 616 00 Brno
tel.: 541 110 777, e-mail: posta@nukib.gov.cz, datová schránka: zzfnkp3, nukib.gov.cz

řetězců“. Stejně tak Bezpečnostní informační služba upozorňuje na narůstající snahy aktérů napojených na ČLR napadat významné státní instituce i testovat odolnost kritické infrastruktury, přičemž součástí sběru zájmových informací užitečných pro zpravodajské služby ČLR jsou i soukromé IT společnosti. Toto vyplývá i ze studie analyzující tisíce akademických publikací čínských výzkumníků, které se zabývají simulací útoků proti rozvodným sítím na území Evropy a Spojených států amerických. Je též známo, že ČLR již přes dvacet let zkoumá evropské sítě, a to s důrazem na jejich případnou zranitelnost vůči kybernetickým či fyzickým útokům.

17. Na základě vlastních zjištění a závěrů z nich učiněných Úřad opakovaně varuje, že většina států (včetně České republiky) nedisponuje dostatečnými kapacitami na to, aby dokázaly pravidelně a účinně prověřovat bezpečnost technologických produktů, obzvlášť v případech, kdy je výrobci umožněna jejich vzdálená správa např. z důvodu potřeby doručovat bezpečnostní aktualizace. Pouhá kontrola používaných zařízení je s ohledem na jejich komplexitu nedostatečná. Uživatelé proto musí brát v potaz i netechnické faktory výrobků, jako důvěru ve výrobce a právní nebo politické prostředí, ve kterém se výrobce pohybuje. Řada kyberbezpečnostních autorit v různých státech se shoduje, že výběr dodavatele nemůže být podmíněn pouze technickými aspekty. Klíčovým faktorem je proto důvěra v dodavatele, že nezneužije své unikátní postavení ve prospěch svůj nebo svého domovského státu či jiného aktéra. Ostatně i Bezpečnostní informační služba ve své výroční zprávě za rok 2023 uvádí, že v důsledku nedostatečných kapacit státy většinou nemají plnou kontrolu nad dodavatelským řetězcem, a musí proto spoléhat na důvěryhodnost výrobce. Právě v takových případech (a to zejména u prvků kritické infrastruktury) je pak zásadní obracet se jen na výrobce pocházející ze zemí se stejným nebo podobným politickým, právním či podnikatelským prostředím. Význam výše popsaného obezřetného počínání jednotlivých států je pak umocňován nejen celosvětovým trendem, jímž je přesun provozu softwarových produktů včetně jejich dat do cloudového prostředí, ale v neposlední řadě též neustále se zhoršující globální bezpečnostní situací, v níž snaha o zajištění kybernetické bezpečnosti nabývá výrazně na důležitosti.

18. Ve své výroční zprávě za rok 2023 Bezpečnostní informační služba také zdůrazňuje, že zvýšená pozornost by měla být věnována zejména vysoce komplexním osobním zařízením, jako jsou chytré telefony, hodinky, elektroautomobily, avšak stejně tak i cloudové služby. Riziko těchto zařízení, popř. služeb, totiž nespočívá pouze v možnosti instalace vysoce sofistikovaného špionážního softwaru, ale též ve shromažďování údajů o poloze, datové i hlasové komunikaci, nebo dokonce i pořizování audiovizuálních záznamů. Takto získaná data jsou uchovávána na serverech v ČLR, ke kterým má vláda ČLR dle čínských právních předpisů přístup. Z výše uvedených důvodů by se uživatelé těchto zařízení, popř. služeb, měli aktivně zajímat o to, zda daná zařízení či služby nepochází ze zemí, jejichž politický režim a legislativa zvyšují možnost zneužití dat státní mocí. Na základě analýzy provedené výše v tomto varování lze přitom dospět k jednoznačnému závěru, že právě ČLR a zvláštní administrativní oblasti se mezi takováto území řadí. S ohledem na závěry učiněné v rámci své vlastní činnosti pak Úřad dále dodává, že ve výše uvedeném kontextu jsou dalšími rizikovými výrobky např. střídače ve fotovoltaických elektrárnách, IP kamery, zdravotechnika či tzv. smartmetry.

Mučednická 1125/31, 616 00 Brno
tel.: 541 110 777, e-mail: posta@nukib.gov.cz, datová schránka: zzfnkp3, nukib.gov.cz

19. Vydání tohoto varování Úřad považuje za nezbytné i s ohledem na některé škodlivé aktivity, které ČLR vůči České republice přinejmenším již v minulosti prokazatelně vyvíjela, neboť tyto aktivity jsou v příkrém rozporu s bezpečnostními zájmy České republiky. Na tyto aktivity upozorňuje i Bezpečnostní informační služba, která ve své výroční zprávě za rok 2023 mimo jiné uvedla, že ve zmíněném roce se Česká republika stala cílem čínské kyberšpionáže usilující o extrakci strategických dat. V témže roce se Česká republika navíc stala také obětí čínských útoků zacílených na „postpandemické pokusy západního světa" o diverzifikaci dodavatelských řetězců, které mají přímý dopad i na českou ekonomiku. Realizaci těchto aktivit ze strany ČLR vůči České republice dokládá mimo jiné i škodlivá kybernetická kampaň, za jejíhož pachatele byla veřejnou atribucí vlády České republiky v roce 2025 označena skupina APT31, jež je spojována s čínskou zpravodajskou službou Ministerstva státní bezpečnosti. Tato skupina od roku 2022 útočila na jednu z neutajovaných sítí Ministerstva zahraničních věcí České republiky. Závěry analýzy provedené Úřadem, Vojenským zpravodajstvím, Úřadem pro zahraniční styky a informace a Bezpečnostní informační službou jednoznačně ukazují, že za touto dlouhodobou škodlivou kampaní stojí ČLR a přímo skupina APT31 (známá též pod jménem Zirconium nebo Judgment Panda), která je spojována s celou řadou útoků proti politickým a jiným cílům mimo jiné též na území dalších členských států Evropské unie či Severoatlantické aliance.

20. Česká republika tudíž není jediným státem, vůči němuž ČLR tyto škodlivé aktivity vyvíjí. Atribuci připisující odpovědnost za kybernetický útok na některou ze státních institucí aktéru napojenému na ČLR již v minulosti učinily i další členské státy Evropské unie. Mezi tyto státy patří např. Belgie, jejíž Ministerstvo zahraničních věcí v roce 2022 veřejně uvedlo, že za útokem na tamní Ministerstvo vnitra stojí skupiny APT27, APT30 a APT31, jež jsou navázané na vládu ČLR. Obdobně pak (tehdy již bývalý členský stát Evropské unie) Spojené království v roce 2024 veřejnou atribucí připsalo skupině APT31 odpovědnost za kybernetický útok, který v roce 2021 cílil na členy britského parlamentu.

21. Dle závěrů výroční zprávy Bezpečnostní informační služby za rok 2022 ruská invaze na Ukrajinu ostatně přiměla ČLR zvýšit její zájem o situaci v Evropě a zintenzivnit její kyberšpionážní aktivity v tomto regionu. V České republice se výše uvedené projevilo např. realizací spear-phishingových útoků, u nichž v několika případech došlo k zacílení i na české státní instituce. Postupně se začala projevovat vyšší sofistikovanost útoků, a to za současného snížení počtu cílů. V některých případech pak došlo k zacílení útoku dokonce přímo na konkrétního jednotlivce. Skutečnost, že bezpečnostní hrozbu, kterou ČLR pro Českou republiku v této souvislosti představuje, rozhodně nelze brát na lehkou váhu, dokládají i slova ministra zahraničních věcí ČLR, Wang Iho, který veřejně prohlásil, že ČLR si nepřeje prohru Ruska ve válce na Ukrajině.

22. Kybernetickým útokům aktérů napojených na ČLR však v minulosti čelily i státy mimo Evropskou unii. Zejména pak ze strany Spojených států amerických dochází v této souvislosti ke zveřejňování atribucí opakovaně, a to již od roku 2014.

23. Závažnost tohoto (výše popsaného) závadového počínání ze strany ČLR podtrhuje též aktivní snaha jednotlivých států čelit této hrozbě společně, ve vzájemné spolupráci. Dokladem této snahy je např. činnost aliance zpravodajský agentur a služeb známé jako

Mučednická 1125/31, 616 00 Brno
tel.: 541 110 777, e-mail: posta@nukib.gov.cz, datová schránka: zzfnkp3, nukib.gov.cz

FVEY („five eyes“), v níž jsou zastoupeny Spojené království, Spojené státy americké, Kanada, Nový Zéland a Austrálie. Tato aliance za současné podpory Německa, Jižní Koreje a Japonska vydala v roce 2024 tzv. advisory, popisující tradecraft aktéra (TTPs) označovaného jako APT40, který je napojen na vládu ČLR, a jehož aktivity měly negativní dopad především na území Austrálie. Výše uvedené jednoznačně dokládá, že škodlivé kyberšpionážní aktivity aktérů napojených na ČLR mají globální rozměr.

24. Je přitom zcela evidentní, že Česká republika není jediným státem, který v přenosu dat do ČLR (a popř. též do zvláštních administrativních oblastí) či ve výkonu vzdálené správy technických aktiv z výše uvedených území identifikuje hrozbu pro národní bezpečnost. Z důvodu neprůkazného nakládání s daty, která jsou do ČLR přenášena (přičemž v některých případech dokonce docházelo přímo k nezákonnému přenosu těchto dat do ČLR), či kvůli nedostatečné ochraně práv subjektů těchto údajů na území ČLR přistoupily k některým opatřením také země jako např. Itálie, Německo, Nizozemsko či Austrálie. Ačkoli se zmíněná opatření u výše uvedených zemí týkala výhradně některých produktů a služeb společnosti Hangzhou DeepSeek Artificial Intelligence Basic Technology Research Co., Ltd., hlavní důvody pro jejich přijetí se principiálně shodují s důvody, na jejichž základě Úřad vydává toto varování, jímž usiluje o minimalizaci hrozby, kterou představuje předávání dat do ČLR a zvláštních administrativních oblastí, resp. výkon vzdálené správy technických aktiv z těchto území.

25. Skutečnost, že předávání dat do ČLR či zvláštních administrativních oblastí, resp. umožnění výkonu vzdálené správy technických aktiv z těchto území, představuje pro Českou republiku bezpečnostní hrozbu, v neposlední řadě dokládá též rozhodnutí vlády České republiky, jímž bylo čínské společnosti Emposat Co., Ltd., zakázáno provozovat pozemní družicovou stanici ve Vlkoši na Hodonínsku, a to právě kvůli obavám, že by ČLR mohla tuto družicovou stanici zneužít pro špionážní účely. Jedná se o zcela objektivně zhodnocenou a reálnou hrozbu zdůrazňovanou i Bezpečnostní strategií České republiky z roku 2023, která uvádí, že ČLR provádí kyberšpionáž, stejně jako se snaží dosáhnout kontroly globálního datového provozu, pročež ze strany ČLR dochází mimo jiné i k využívání rozličných forem sociálně-ekonomického nátlaku a dalších nástrojů hybridního působení.

26. Úřad hodnotí úroveň hrozby jako vysokou, tedy v souladu se stupnicí pro hodnocení hrozeb obsaženou v příloze č. 2 k vyhlášce o kybernetické bezpečnosti jako pravděpodobnou až velmi pravděpodobnou. Úroveň hrozby je dána především kombinací nedůvěryhodného (a pro bezpečnost České republiky problematického) právního prostředí ČLR, které má zcela reálný potenciál být aplikováno též na území zvláštních administrativních oblastí, a prokázaného dlouhodobého škodlivého působení aktérů napojených na vládní orgány ČLR vůči České republice, jejichž aktivity jsou v příkrém rozporu s bezpečnostními zájmy České republiky. Nelze přitom opomenout ani globální mocenské ambice ČLR a její geopolitickou inklinaci, která se v mnoha ohledech s orientací České republiky zásadně rozchází. To ostatně potvrzuje i Bezpečnostní strategie České republiky z roku 2023, která ČLR označuje za zásadní systémovou výzvu v globální perspektivě i v jejím přímém působení vůči demokratickým zemím, a to právě včetně České republiky.

27. Všem fyzickým osobám, jejichž data by mohla být cílem aktivit zahraničních zpravodajských služeb (tzv. zájmové osoby, tedy osoby, které zastávají např. vysoké

Mučednická 1125/31, 616 00 Brno
tel.: 541 110 777, e-mail: posta@nukib.gov.cz, datová schránka: zzfnkp3, nukib.gov.cz

politické, veřejné či rozhodovací funkce), Úřad doporučuje, aby zvážily případné omezení či úplný zákaz využívání technologií či služeb, jejichž prostřednictvím by mohlo docházet k přenosu systémových a uživatelských dat do ČLR či zvláštních administrativních oblastí nebo jejichž technická aktiva by mohla být vzdáleně spravována z těchto území tak, jak je popsáno ve výroku tohoto varování.

28. Široké veřejnosti pak Úřad doporučuje věnovat zvýšenou pozornost tomu, jaké přístupy po nich požadují technologie či služby, jež využívají. Stejně tak by se široká veřejnost měla zajímat, jakým způsobem tyto technologie či služby nakládají s daty, která jim uživatelé poskytují (mimo jiné pak o to, zda, popř. kam, jsou tato data odesílána). Úřad obecně doporučuje instalovat a používat pouze takové technologie, kterým jejich uživatel důvěřuje.

29. Úřad přistoupil k vydání tohoto varování, jelikož jeho úkolem je dle § 22 písm. j) zákona o kybernetické bezpečnosti zajišťovat prevenci v oblasti kybernetické bezpečnosti, jejíž součástí je také poskytování informací zjištěných o hrozbách v oblasti kybernetické bezpečnosti. Veškeré výše uvedené informace dle Úřadu dokládají, že – ve výrokem tohoto varování stanoveném rozsahu – předávání systémových a uživatelských dat do ČLR či zvláštních administrativních oblastí nebo umožnění výkonu vzdálené správy technických aktiv z těchto území představuje pro Českou republiku bezpečnostní hrozbu, o níž nepostačuje veřejnost informovat běžnými způsoby preventivní činnosti Úřadu. Pravomoc Úřadu k vydání tohoto varování je dána ustanovením § 22 písm. b) zákona o kybernetické bezpečnosti.

30. Úřad na závěr upozorňuje, že v souladu s § 4 odst. 4 zákona o kybernetické bezpečnosti jsou orgány a osoby uvedené v § 3 písm. c) až f) zákona o kybernetické bezpečnosti povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační nebo komunikační systém a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou. Zohlednění požadavků vyplývajících z bezpečnostních opatření podle věty první v míře nezbytné pro splnění povinností podle zákona o kybernetické bezpečnosti nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.

Elektronický podpis: 3.9.2025
Certifikát autora podpisu:
Jméno: Ing. Lukáš Kintr
Vydal: I.CA EU Qualified CA2/RSA 06/2022
Platnost do: 4.2.2026 13:05 +01:00

Ing. Lukáš Kintr
ředitel
Národní úřad pro kybernetickou a informační bezpečnost

Mučednická 1125/31, 616 00 Brno
tel.: 541 110 777, e-mail: posta@nukib.gov.cz, datová schránka: zzfnkp3, nukib.gov.cz