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

**Spisová značka:**
350 - 747/2022
**Číslo jednací:**
6548/2022-NÚKIB-E/350

Brno, 30. května 2022

# 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 v použití technických nebo programových prostředků, které nepochází ze států Evropské unie, Evropského hospodářského prostoru, Organizace pro hospodářskou spolupráci a rozvoj či Severoatlantické aliance, pro implementaci technologií umožňujících požadovanou úroveň přímého měření typu B, C1, C2 nebo C3 dle vyhlášky č. 359/2020 Sb., o měření elektřiny.

Národní úřad pro kybernetickou a informační bezpečnost tuto hrozbu hodnotí na úrovni Vysoká – Hrozba je pravděpodobná až velmi pravděpodobná.

## ODŮVODNĚNÍ

1. Na základě skutečností zjištěných při výkonu své působnosti, stejně tak jako na základě skutečností, které se Úřad dozvěděl od tuzemských partnerů, dospěl Úřad k zjištění hrozby v oblasti kybernetické bezpečnosti, spojené s použitím technických nebo programových prostředků, které nepochází ze zemí Evropské unie, Evropského hospodářského prostoru, Organizace pro hospodářskou spolupráci a rozvoj či Severoatlantické aliance, pro implementaci technologií umožňujících požadovanou úroveň přímého měření typu B, C1, C2 nebo C3 dle vyhlášky č. 359/2020 Sb., o měření elektřiny, proti této hrozbě tak vydává podle § 12 odst. 1 zákona o kybernetické bezpečnosti toto varování.

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

**Časové zasazení a povaha dané situace**

3. Některé osoby povinné dle zákona o kybernetické bezpečnosti, konkrétně pak provozovatelé distribuční soustavy elektřiny, musí bezodkladně započít přípravné práce pro nasazení technologie umožňující požadovanou úroveň přímého měření typu B, C1, C2 a C3 dle vyhlášky č. 359/2020 Sb., o měření elektřiny (dále jen „vyhláška o měření elektřiny“), která je předpisem provádějícím zákon č. 458/2000 Sb., o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů (energetický zákon), resp. směrnici Evropského parlamentu a Rady (EU) 2019/944 ze dne 5. června 2019 o společných pravidlech pro vnitřní trh s elektřinou a o změně směrnice 2012/27/EU (dále jen „směrnice o vnitřním trhu s elektřinou“). Nasazení těchto technologií tak není jen důsledkem technologického vývoje a zavádění inovací, ale jde o plnění povinnosti dané legislativou Evropské unie.

4. Skutečnost, že toto varování upozorňuje na existenci hrozby v oblasti kybernetické bezpečnosti pro konkrétní sektor, neznamená, že hrozba použití technologie pocházející ze států mimo okruh jmenovaných není relevantní i pro jiná odvětví. Úřad však na základě všech shromážděných informací ve vztahu k sektoru energetiky shledal, že tato hrozba se jeví jako pravděpodobná až velmi pravděpodobná.

5. Vzhledem k tomu, že vyhláška o měření elektřiny stanoví, že implementace technologií umožňujících požadovanou úroveň přímého měření typu B, C1, C2 a C3 dle vyhlášky o měření elektřiny musí být zahájena 1. července 2024 a všechna vyhláškou definovaná odběrná místa musí mít tuto technologii implementovánu do 1. července 2027, je ze strany provozovatelů distribuční soustavy nutné zahájit výběrová řízení, resp. zadávací řízení podle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, bezodkladně. Z informací poskytnutých provozovateli distribučních soustav vyplývá, že počítají s minimální dobou trvání zadávacího řízení 18 měsíců od spuštění zadávacího řízení do uskutečnění první dodávky a dále se zkušebním provozem na menším rozsahu zařízení. Vzhledem k rozsahu zakázek (danému celkovým počtem odběrných míst, která je potřeba novými zařízeními osadit) a ke lhůtám spjatým se zadávacími řízeními, stejně jako vzhledem k náročnosti celého procesu implementace nové technologie je tak potřeba zahájit výběrová řízení co nejdříve, aby k implementaci technologie mohlo dojít v termínu stanoveném legislativou.

6. Skutečnosti uvedené v bodech 3, 4 a 5 tohoto varování tak přispívají k vyšší míře aktuálnosti hrozby, na kterou varování reaguje.

**Význam a míra možného dopadu realizace hrozby**

7. Dopady narušení bezpečnosti informací systémů s technologií umožňující požadovanou úroveň přímého měření typu B, C1, C2 a C3 na zajišťování dodávek elektrické energie v České republice jsou v porovnání se v současnosti nasazenou technologií měření elektrické energie neporovnatelně vyšší. Rovněž zapříčinit takový dopad ze strany dodavatele technických a programových prostředků podporujících funkčnost této technologie je významně snadnější než u současných technologií.

8. Mezi možné dopady narušení bezpečnosti technologií umožňujících požadovanou úroveň přímého měření typu B, C1, C2 nebo C3 na zajišťování dodávek elektrické energie patří následující:

    a. Ovlivnění měření a odeslání chybných dat do centrály.

    b. Odpojení odběrného místa (například i hromadným příkazem z centrály). V případě některých řešení je pro opětovné zapojení nutná fyzická přítomnost na odběrném místě, tedy obnovení připojení odběrného místa nebude okamžité. V případě jiných řešení je možné opětovné zapojení odběrného místa z centrály, což může ovšem při opakovaných odpojeních a připojeních vést k destabilizaci přenosové soustavy.

    c. Při hromadném odpojení tisíců odběrných míst může dojít k narušení stability přenosové soustavy, které může vést až k blackoutu, a to nejen na úrovni odběrných míst, ale i přenosové soustavy jako celku.

9. Výše uvedené dopady jsou významné svým potenciálním možným rozsahem (jedná se až o cca 5,5 milionů elektroměrů, potažmo odběrných míst) a řadí se mezi jedny z největších a nejvíce ovlivňujících možné standardní fungování České republiky a její energetickou bezpečnost. Z tohoto důvodu je nutné zvažovat možné hrozby s nejvyšší možnou mírou detailu, k čemuž má za cíl přispět i toto varování.

10. Energetika jako odvětví, zejména pak její pododvětví elektřiny, zajišťuje jednu z vitálních funkcí státu. Dopad realizace uvedené hrozby se neprojeví izolovaně pouze v daném pododvětví, ale spustí dominový efekt, který v důsledku zasáhne veškerá další odvětví ekonomiky stejně jako každého jednotlivého občana této země. Negativní ovlivnění technologií zajišťujících řádné fungování elektroenergetické soustavy v České republice by tak mohla způsobit dopady rovnající se kompletní paralýze české ekonomiky i běžného života.

11. Zajištění energetické bezpečnosti zároveň patří mezi strategické cíle České republiky, jak vyplývá i z bezpečnostní strategie České republiky.[1] Vzhledem k současné situaci na poli energetiky, kde se setkávají faktory jako snaha o ekologičtější nakládání s přírodními zdroji či energetické dopady války na Ukrajině, je zajištění bezpečného fungování přenosu a distribuce elektrické energie ještě významnější.

12. S nasazením uvedené technologie budou spojeny významné finanční a kapacitní náklady. Mitigace rizika spojeného s realizací této hrozby až v budoucnu by znamenala vynaložit tyto náklady opětovně, a to mimo období, pro které byly tyto výdaje naplánovány, což by se mohlo odrazit v cenách energií koncových spotřebitelů. Nadto by nasazení rizikové technologie do provozu a řešení jejího nahrazení až zpětně mohlo významným způsobem ohrozit řádné poskytování přenosu, distribuce a dodávek elektrické energie konečným spotřebitelům, stejně jako energetickou bezpečnost České republiky. Z toho důvodu je nezbytné upozornit na existenci hrozby již nyní, před vlastním nákupem technických a programových prostředků, které představují hrozbu v oblasti kybernetické bezpečnosti, aby bylo energetickým

[1] Vláda ČR; Bezpečnostní strategie České republiky 2015, s. 7, dostupné zde: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf

společnostem, na které povinnost zavedení nové technologie dopadá, umožněno s identifikovanou hrozbou dále pracovat a zohlednit ji v procesu řízení rizik.

**Netechnické aspekty kybernetické bezpečnosti**

13. Kybernetická bezpečnost nespočívá pouze na posuzování technických aspektů používaných technologií, ale například při výběru dodavatelů je nutné zvážit i netechnické aspekty bezpečnosti daných technologií, tedy posoudit důvěryhodnost dodavatelů a poddodavatelů (výrobců) dané technologie. Důvěryhodnost dodavatele se pak přímo promítá do důvěryhodnosti dodané technologie a určuje úroveň rizika, které je s použitím takové technologie spojeno. Důvěra v dodavatele musí být přítomna jak na úrovni konečné podoby dodávaného řešení (kvality), tak na strategické – netechnické úrovni, a spočívá i v důvěře v podnikatelské, právní a politické prostředí, ve kterém se dodavatel pohybuje. Na tuto v praxi často opomíjenou skutečnost Úřad dlouhodobě poukazuje, přičemž nejaktuálněji tuto skutečnost zdůrazňuje společně s Ministerstvem průmyslu a obchodu, Ministerstvem zahraničních věcí, Bezpečnostní informační službou, Úřadem pro zahraniční styky a informace a Vojenským zpravodajstvím, jakožto veřejnoprávními zástupci bezpečnostní komunity České republiky v rámci veřejně vydaného Doporučení pro hodnocení důvěryhodnosti dodavatelů technologií do 5G sítí v České republice.[2]

14. Za státy s důvěryhodným právním prostředím lze považovat státy:

    a. které mají demokraticky volenou vládu, což mj. zahrnuje existenci nezávislé opozice, svobodných voleb, na základě jejichž výsledku může být stávající vláda vyměněna, a fungující princip tzv. brzd a protivah,

    b. které mají nezávislý soudní systém, jenž nepodléhá přímým politickým zásahům, jsou v něm dodržována závazná pravidla, zvyklosti a zásady právního státu, jako je právo na spravedlivý proces vč. ctění presumpce neviny, práva na veřejné projednání věci a práva být souzen bez zbytečného odkladu,

    c. jejichž právní předpisy a veřejné politiky se řídí zásadami právního státu a jsou vydávány s ohledem na ně,

    d. které dbají na ochranu duševního vlastnictví,

    e. které dlouhodobě či systematicky neporušují mezinárodní právo a vůči nimž nebo vůči jejichž aktivitám se oficiálně nevymezují mezinárodní a nadnárodní organizace či aliance, kterých je Česká republika členem, a to např. v podobě rezoluce Rady bezpečnosti Organizace spojených národů či omezujícího opatření společné zahraniční a bezpečnostní politiky Evropské unie,

    f. které udržují s Českou republikou partnerské vztahy a neprovádí činnosti, které jdou proti základním zájmům České republiky nebo jejích spojeneckých států,

[2] Dostupné zde: https://www.nukib.cz/cs/infoservis/doporuceni/1801-doporuceni-pro-hodnoceni-duveryhodnosti-dodavatelu-technologii-do-5g-siti-v-ceske-republice/

g. které nepovažují Českou republiku za nepřátelský stát.

15. Právní prostředí státu popsaného v přechozím bodě odůvodnění tohoto varování lze označit za obecně důvěryhodné. Státy Evropské unie, Evropského hospodářského prostoru, Organizace pro hospodářskou spolupráci a rozvoj či Severoatlantické aliance jsou skupinou států, které disponují důvěryhodným právním prostředím, a hrozba upřednostnění zájmů státu před zájmy zákazníka v těchto státech je tak výrazně méně pravděpodobná. Česká republika je zároveň členem všech těchto uskupení a jedná se tak o její spojenecké státy v různých oblastech od ekonomické a hospodářské spolupráce až po spolupráci vojenskou. U dodávky pocházející z těchto států je tak pravděpodobnost, že dojde k realizaci dopadů popsaných v bodě 8 odůvodnění tohoto varování, významně nižší.

16. Nedůvěryhodné právní prostředí některých států má přímý dopad na důvěryhodnost společností, které jsou v nich usídleny a jsou takovým právním prostředím podřízeny. Vzhledem k nedůvěryhodnosti právního prostředí pak nelze vyloučit, že dané společnosti budou ze strany státu nuceny upřednostnit zájmy svého státu před zájmy svých zákazníků.

**Posouzení dané hrozby**

17. Skutečnosti uvedené ve výše uvedených bodech tohoto varování přispívají k vyšší míře závažnosti hrozby, na kterou varování reaguje. Vzhledem k tomu, jak významný je dopad narušení bezpečnosti informací u těchto technologií a jakými možnostmi budou disponovat právě dodavatelé těchto technologií, je nezbytné, aby byla ve varování popisovaná hrozba ze strany povinných osob náležitě posouzena a aby byla přijata odpovídající bezpečnostní opatření.

18. Pro účely tohoto varování se pojmem technologie umožňující požadovanou úroveň přímého měření typu B, C1, C2 nebo C3 dle vyhlášky o měření elektřiny míní celý řetězec měření, přenosu a zpracování dat, a to včetně komunikačních prostředků, které jsou v tomto řetězci zahrnuty.

19. Ve vztahu k technologiím umožňujícím požadovanou úroveň přímého měření typu B, C1, C2 nebo C3 dle vyhlášky o měření elektřiny je, jak je uvedeno ve výroku tohoto varování, nutné zvážit, odkud daná technologie pochází. Původ technologie je pak nutné zohlednit ve vztahu k jejímu vývoji, výrobě, sestavení či servisu, tam, kde je tato technologie významná z hlediska zajištění bezpečnosti informací a zajištění ovládání a funkčnosti dané technologie.

20. Pravomoc Úřadu je pro vydání tohoto varování dána ustanovením § 22 písm. b) zákona o kybernetické bezpečnosti, které jej zmocňuje k vydávání opatření. Podle § 11 odst. 2 zákona o kybernetické bezpečnosti patří mezi tato opatření i varování podle § 12 zákona o kybernetické bezpečnosti. Varování vydá Úřad podle § 12 odst. 1 zákona o kybernetické bezpečnosti, dozví-li se zejména z vlastní činnosti nebo z podnětu provozovatele národního CERT anebo od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí, o hrozbě v oblasti kybernetické bezpečnosti. V souladu s § 12 odst. 2 zákona o kybernetické bezpečnosti Úřad zveřejní varování na svých internetových stránkách a oznámí je orgánům a osobám uvedeným v § 3 zákona o kybernetické bezpečnosti.

21. Úkolem Úřadu je podle § 22 písm. j) zákona o kybernetické bezpečnosti zajišťovat prevenci v oblasti kybernetické bezpečnosti. Součástí této preventivní činnosti je také poskytování informací o zjištěných hrozbách v oblasti kybernetické bezpečnosti. Pokud však hrozba dosahuje takové intenzity, že informování o ní nelze pokrýt běžnými způsoby preventivní činnosti Úřadu, je v souladu s výše uvedeným Úřad nucen přistoupit k vydání varování podle § 12 zákona o kybernetické bezpečnosti.

22. Úřad upozorňuje, že orgány nebo osoby, které jsou povinny zavést bezpečnostní opatření podle zákona o kybernetické bezpečnosti, v souvislosti s řízením rizik podle § 5 odst. 1 písm. h) bod 3 vyhlášky o kybernetické bezpečnosti při hodnocení rizik a v plánu zvládání rizik zohlední opatření podle § 11 zákona o kybernetické bezpečnosti. Jedním z těchto opatření je i varování podle § 12 zákona o kybernetické bezpečnosti. Na základě výše uvedeného Úřad považuje hrozbu ve výroku tohoto varování za pravděpodobnou až velmi pravděpodobnou. Orgány a osoby, které jsou povinny zavést bezpečnostní opatření podle zákona o kybernetické bezpečnosti a kterých se zároveň toto varování týká (tedy provozovatelé distribuční soustavy elektřiny), jsou proto povinny tuto hrozbu hodnotit na odpovídající úrovni, tedy na úrovni Vysoká. 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.

23. Úřad dále 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.

Digitálně podepsal:
Ing. Karel Řehka
Národní úřad pro kybernetickou a informační bezpečnost
Dne: 30.05.2022 11:03

NÚKIB

Ing. Karel Řehka
ředitel
Národní úřad pro kybernetickou a informační bezpečnost