frank bold

Kyberbezpečnost OZE a veřejné zakázky

Jak mohou obce soutěžit bezpečné obnovitelné zdroje

Proč je kyberbezpečnost OZE tak zásadní?

Zabezpečení obnovitelných zdrojů energie (OZE) před hackery se v době masivního budování nových elektráren stává zásadním tématem **i pro veřejné zadavatele**. Fotovoltaika sice nabízí udržitelnou a levnou výrobu elektřiny, představuje ale zároveň nové hrozby **kybernetických útoků**.

Výrobny OZE jsou často **slabě softwarově zabezpečené**, případně je problém již v jednotlivých **komponentech (hardwaru)**, a to někdy i úmyslně způsobený. Srdcem každé solární elektrárny je její **měnič**, obvykle připojený k internetu a umožňující monitorování a řízení zdroje. Právě tyto vlastnosti způsobují náchylnost ke kybernetickým útokům.

Nezabezpečená fotovoltaická elektrárna (FVE) ohrožuje nejen kontinuitu výroby elektřiny, může se ale také pro hackery stát **nevědomou přístupovou bránou k energetické infrastruktuře obce** a k digitálním platformám samosprávy a jejích úřadů.

Jaká jsou kybernetická rizika?

Únik citlivých dat a následné pokuty

Dálkové ovládnutí nebo vypnutí zdroje

Systémový výpadek dodávek elektřiny (blackout)

Evropská energetická síť je zranitelná. Včetně Česka a Slovenska

Kybernetické útoky jsou blíže, než by se mohlo zdát. Zkušenosti už s nimi má i Česká republika, příkladem budiž hackerský útok na strojírenský závod ve Středočeském kraji **s vyčíslenou škodou 750 milionů korun.** Na Slovensku zase proběhl hackerský útok na katastr nemovitostí. Hackeři tam požadovali výkupné 300 milionů korun a nápravy škod budou Slovenko stát **minimálně 400 milionů korun**.

10 GW výkonu fotovoltaik

Tolik stačí podle reportu přední evropské solární asociace Solar Power Europe[1] **jednorázově vypnout** pro destabilizaci celoevropské energetické sítě s následným kaskádovým **blackoutem** (výpadkem dodávky elektřiny). Přitom jen v roce 2024 bylo v Evropě instalováno 337 GW výkonu nových fotovoltaik.

Přes 80 % měničů pochází od čínských výrobců, jejichž produkty mohou postrádat kyberbezpečnostní ochranu, nebo si naopak záměrně ponechávají zadní vrátka. Je tak v podstatě možné energetické zdroje vzdáleně ovládat či dokonce cíleně vypnout. To může mít obzvlášť v celoevropském měřítku **fatální následky**.

Energetická přenosová a distribuční síť je v mnoha evropských zemích považována za **kritickou infrastrukturu** a proto podléhá zvýšené ochraně.

[1] *Solar Power Europe, „Řešení pro kybernetická rizika fotovoltaiky a stabilitu sítě"*, duben 2025

Řešení? Zadávání veřejných zakázek

Zadávání veřejných zakázek představuje **nástroj, jak může obec regulovat kybernetickou bezpečnost svých OZE**. Zákon o zadávání veřejných zakázek umožňuje veřejným zadavatelům jako jsou obce, kraje či organizační složky státu požadovat zajištění kybernetické bezpečnosti OZE v rámci zadávacího řízení. Samosprávy se tak mohou chránit před riziky kybernetických útoků.

Současný zákon o zadávání veřejných zakázek sice přímo s kyberbezpečností nepracuje, obsahuje však ustanovení, která mohou být využita k dosažení vyššího zabezpečení OZE. Požadavky na kyberbezpečnost OZE může zadavatel veřejné zakázky **zohlednit v rámci podmínek účasti dodavatelů** v zadávacím řízení.

Jaké podmínky účasti v zadávacím řízení může obec stanovit?

Kvalifikační

- Profesní (odborná) způsobilost dodavatele, technická kvalifikace
- Referenční obdobné zakázky, certifikace od výrobce technologie

Technické

- Použití určité technologie jako referenčního standardu, odkaz na technické normy
- Zákaz využití určitých komponent

Obchodní nebo smluvní

- Podmínky v návrhu smlouvy na veřejnou zakázku (smlouvy o dílo)

Zvláštní podmínky plnění

- V oblasti vlivu předmětu veřejné zakázky na životní prostředí, sociálních důsledků či inovací

Jak připravit zadávací řízení s ohledem na kyberbezpečnost OZE?

Využijte předběžnou tržní konzultaci

Ještě před zahájením zadávacího řízení **můžete komunikovat s potenciálními dodavateli a odborníky**. To vám pomůže definovat, co přesně můžete po dodavateli FVE z hlediska kyberbezpečnosti požadovat a jaké jsou aktuální možnosti na trhu. Více o předběžné tržní konzultaci se dozvíte na stránkách Ministerstva pro místní rozvoj.[2]

Stanovte jasné podmínky účasti dodavatelů

Požadavky na kyberbezpečnost OZE můžete zohlednit v rámci podmínek účasti dodavatelů v zadávacím řízení ve smyslu § 37 odst. 1 písm. a) až d) zákona o zadávání veřejných zakázek. Jako nejvhodnější se jeví využít **technická kritéria**, která jasně vymezí předmět veřejné zakázky (instalaci FVE) právě z hlediska kybernetické bezpečnosti.

Konkrétní kritéria, která lze při zadávání veřejné zakázky využít, **najdete na následující stránce brožury**.

Vždy dodržujte zásadu přiměřenosti a zásadu rovného zacházení

„Pokud budete jako zadavatel veřejné zakázky např. stanovovat určité technické požadavky, musíte být schopen odůvodnit, proč a na základě čeho jste je stanovil. Stejně tak musí podmínky stanovené pro účast dodavatele vždy souviset s předmětem veřejné zakázky (instalací FVE).“

Jan Bakule, právník Frank Bold

[2] *www.portal-vz.cz/instituty/predbezne-trzni-konzultace/*

Příklady technických kritérií s důrazem na kyberbezpečnost

Technický parametr
Systém řízení informační bezpečnosti výrobce měničů je certifikován dle ISO/IEC 27001:2022 – doložit certifikátem
FVE měniče musí být v rámci kybernetické bezpečnosti ve shodě s ETSI 303 645 – doložit certifikátem
FVE měniče musí být v rámci v kybernetické bezpečnosti certifikovány dle RED 2014/53/EU - doložit certifikátem
Výrobce technických nebo programových prostředků (HW a SW vybavení měničů) není klasifikován jako hrozba v oblasti kybernetické bezpečnosti a NÚKIB nevydal před použitím těchto prostředků varování
Každý měnič FVE systému, popř. gateway musí mít z výroby své unikátní přístupové heslo, tzn. nesmí být použito stejných nebo defaultních hesel
Data o výrobě, spotřebě a systémové informace musí být uložena na evropských serverech

Další doporučená kritéria
V souladu s politikou udržitelného rozvoje a ESG musí výrobce doložit, že k výrobě svého produktu nevyužívá dětskou práci, moderní otroctví, obchodování s lidmi aj.
Kybernetická bezpečnost FVE měničů a systému musí být potvrzena nezávislým certifikačním subjektem
Výrobce FVE měničů musí pocházet ze zemí Evropské unie, Evropského hospodářského prostoru nebo Organizace pro hospodářskou spolupráci či Severoatlantické aliance

Příklad úspěšné praxe

Jablonec n. Nisou

Jako teplárenská společnost 100% vlastněná statutárním městem **dlouhodobě řeší kybernetickou bezpečnost svých energetických zařízení** (zejm. teplárenských technologií). Rozšíření kybernetické ochrany i na plánovaný projekt fotovoltaik je tak pro Jablonecku energetickou logickým krokem. Další motivací bylo také plnění povinností vyplývajících z evropského nařízení „NIS II".[3]

O jaký projekt jde?

Městská společnost je hlavním hybatelem projektu komunitní energetiky **Planeta Jablonec**[4]. V rámci něj plánuje investovat do komunitní fotovoltaiky o souhrnném výkonu **až 3,6 MWp**, která bude umisťována na budovách města a jeho příspěvkových organizací. Cílem je větší stabilita a soběstačnost města díky čistému zdroji.

Co udělali v Jablonci jako první?

V první fázi se rozhodli využít **předběžnou tržní konzultaci**.[5] Cílem bylo připravit zadávací podmínky veřejné zakázky tak, aby odpovídaly požadavkům projektu i zadavatele a umožnily co nejširší účast dodavatelů v zadávacím řízení.

Zadavatel oslovil celkem 8 dodavatelů, vyjádřilo se 5. S jednotlivými účastníky vedl konzultace odděleně, přičemž je vyzval k vyplnění písemného dotazníku. **Ověřil tak technické podmínky i kvalifikační kritéria** pro návazné zadávací řízení.

Jak nastavili zadávací podmínky?

V zadávacím řízení stanovili **podmínky kyberbezpečnosti jako nepřekročitelné** - musel je tedy splnit každý potenciální dodavatel FVE. Podmínky byly vymezeny zejména v technických požadavcích na technologii, a to například:

- Ukládání dat z fotovoltaického systému **pouze na evropském serveru** (cloudu) a splnění norem **ISO 27001:2022** pro systém řízení informační bezpečnosti
- **Zabezpečený protokol pro přenos dat z FVE** do dalších systémů organizace
- **Certifikace výrobce střídače** dle RED 2014/53/EU
- **Aktualizace** zařízení pouze systémem OTA (over-the-air)

„Pro zadávací řízení jsme zvolili formu otevřeného řízení. U žádného z dodavatelů zajištění kyberbezpečnosti nepředstavovalo problém a tyto požadavky se nepromítly ani do ceny zakázky."

Jaroslav Šída, manažer energetických projektů

Jak to všechno dopadlo?

V srpnu 2025 byl vybrán vítězný dodavatel celé zakázky. Ten je schopen zajistit i kyberbezpečnost OZE. K postupné instalaci na více jak 50 budovách města má dojít v horizontu dalších dvou let, první instalace začnou už na podzim 2025.

---

[3] *https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32022L2555*

[4] *https://jeas.cz/komunitni-energetika/*

[5] *https://nen.nipez.cz/verejne-zakazky/detail-zakazky/N006-25-P00000059*

Obraťte se na nás

Problematice kyberbezpečnosti OZE a hlavně **zadávání veřejných zakázek na kvalitu** se ve Frank Bold Advokáti dlouhodobě věnujeme.

Postaráme se o to, abyste při zadávání veřejné zakázky na obnovitelné zdroje postupovali správně.

Pomůžeme vám vše nastavit tak, aby váš obnovitelný zdroj odolal kybernetickým hrozbám a zároveň zajistíme, že podmínky zadávacího řízení budou nastavené **neprůstřelně, nediskriminačně** a zajistí co nejširší účast potenciálních dodavatelů.

Petr Jelínek
senior konzultant
Frank Bold Advokáti

petr.jelinek@fbadvokati
+420 778 111 866

www.fbadvokati.cz

Chcete se dozvědět víc o tématu kyberbezpečnosti OZE?

Přečtěte si podrobnější právní analýzu Frank Bold

Kyberbezpečnost OZE a veřejné zakázky
Jan Bakule, Anna Francová (Frank Bold), Jindřich Stuchlý (SolarEdge)
Konzultace: Jaroslav Šída
Editace a sazba: Martin Vérteši

Publikace je součástí projektu „Města a obce odolná vůči změnám klimatu“, financovaného Evropskou unií v rámci Národního plánu obnovy.

frank bold

solaredge

Financováno Evropskou unií NextGenerationEU

NÁRODNÍ PLÁN OBNOVY

Ministerstvo životního prostředí

STÁTNÍ FOND ŽIVOTNÍHO PROSTŘEDÍ ČESKÉ REPUBLIKY

frank bold