Experti Frank Bold i NÚKIB: Obce musí myslet na kyberbezpečnost při zadávání zakázek na obnovitelné zdroje

10.9.2025 - Markéta Bočková | Frank Bold

Už jen necelé dva měsíce mají obce s rozšířenou působností, aby se připravily na nové povinnosti v oblasti kybernetické bezpečnosti. S rozvojem obnovitelných zdrojů energie (OZE) a sdílení elektřiny se kyberbezpečnost stává klíčovým faktorem také při zadávání veřejných zakázek na obnovitelné zdroje energie. A to nejen v kontextu aktuálního varování Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) před používáním čínské techniky. Během workshopu organizovaného expertní skupinou Frank Bold odborníci z akademické sféry i praxe upozornili na rostoucí rizika kybernetických útoků na fotovoltaické elektrárny a další obnovitelné zdroje energie. Hackeři jimi mohou ohrozit stabilitu celé energetické sítě.

„Jednorázové vypnutí pouhých 10 GW výkonu fotovoltaických elektráren by podle zjištění expertů asociace Solar Power Europe stačilo k destabilizaci celoevropské energetické sítě s následným kaskádovým blackoutem. Přitom jen v roce 2024 bylo v Evropě instalováno 337 GW nových fotovoltaik," varovala **právnička Frank Bold Advokáti Anna Francová**. Zkušenosti podle ní ukazují, že je klíčové požadovat, aby komponenty FVE systémů pocházely od stejného, ideálně bezpečného výrobce. To zajišťuje jejich řiditelnost a vyšší bezpečnost.

„Zadavatelé mohou pro minimalizaci kybernetických rizik využít řady nástrojů, které jim dává zákon o zadávání veřejných zakázek – od nastavení technických požadavků přes smluvní podmínky až po předběžné tržní konzultace,“ popsala **Anna Francová.**

Vážnost situace podtrhuje i varování, které minulý týden vydal Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Ten varuje před používáním veškeré čínské techniky, která může odesílat data do Číny nebo která může být na dálku ovládána čínskými správci. Týká se to například mobilních telefonů, chytrých hodinek, bezpečnostních kamer, technologií pro solární elektrárny, elektroaut i zdravotnických přístrojů.

Zásadní změnu představuje také nová legislativa transponující evropskou směrnici NIS2. *„Od 1. listopadu 2025 vstoupí v účinnost nový zákon o kyberbezpečnosti, který rozšíří počet regulovaných subjektů v Česku ze 400 na přibližně 6000. Mezi nimi budou i obce s rozšířenou působností, které budou mít v souvislosti s výkonem veřejné správy či dalších regulovaných činností povinnost zavádět bezpečnostní opatření,“* vysvětlil **Ondřej Polák, analytik Národního úřadu pro kybernetickou a informační bezpečnost**.

V případě solárních elektráren a dalších obnovitelných zdrojů energie může jít mimo jiné o vhodné nastavení podmínek výběrového řízení: *„Každý zadavatel by měl provést důkladnou analýzu rizik a na jejím základě může v odůvodněných případech vyloučit rizikové dodavatele. To ve svém rozhodnutí ze začátku roku 2024 potvrdil i antimonopolní úřad,”* doplnil Polák.

Již nyní některé energetické projekty kyberbezpečnost v rámci zadávání zakázek řeší. *„V Jablonci nad Nisou připravujeme projekt solární elektrárny v hodnotě 240 milionů korun. Kybernetická bezpečnost byla od začátku klíčovou součástí zadávací dokumentace – stanovili jsme konkrétní technické požadavky na měniče, optimizéry i řídící systémy,*" přiblížil **Jaroslav Šída ze společnosti**

Jablonecká energetická.

O zabezpečení solárních elektráren by se měli starat i běžní uživatelé s několika fotovoltaickými panely na střeše. I jim totiž může útok hackerů způsobit potíže. *“Největším problémem u rezidenčních instalací je připojení střídače do cloudu výrobce, který často bývá velmi špatně zabezpečený. Napadení cloudu pak může mít dopad na všechny připojené domácnosti. Odstavení elektrárny z provozu se může stát nakonec tou nejmenší komplikací. Dalším rizikem tak může být například rozšíření kybernetického útoku do sítě domácnosti nebo fyzické poškození elektrárny,”* vysvětlila bezpečnostní výzkumnice ČVUT **Erika Langerová vedoucí týmu Kyberbezpečnost pro energetiku v Univerzitním centru energeticky efektivních budov.**

Podle aktuálních dat jsou obnovitelné zdroje již nyní pátým nejnapadanějším sektorem v energetice. Nejvíc slabých míst mají cloudové platformy pro monitoring. Například v roce 2024 napadli hackeři v Litvě systémy dodavatele technologií pro solární elektrárny a prodali přihlašovací údaje provozovatelů elektráren. Na Ukrajině jsou komerční solární elektrárny pravidelným cílem kyberútoků, přičemž některé útoky byly úspěšně a elektrárny zůstaly odstavené i několik dní. Je proto zásadní dobře vybrat výrobce technologií.

https://frankbold.org/pro-media/tiskova-zprava/experti-frank-bold-i-nukib-obce-musi-myslet-na-kyberbezpecnost-pri-zadavani-zakazek-na-obnovitelne-zdro