KYBERNETICKÉ HROZBY FV SYSTÉMŮ

Chystáte se na instalaci FV systému? Pokud ano, dbejte zvýšené pozornosti při výběru technologie, která zabezpečuje aktualizaci, přenos a zpracování informací o solární elektrárně. V případě FVE se jedná zejména o FV měnič, zařízení, které provádí konverzi z DC na AC, je připojeno k internetu (IoT zařízení), a které současně zabezpečuje i monitoring systému. Současné FV měniče jsou bohužel v drtivé většině kybernetické nezabezpečené a situaci lze přirovnat k bezpečnosti internetu v devadesátých letech. Měniče tak slouží nevědomky jako vstupní brána pro hackery a množství kybernetických útoků prostřednictvím IoT zařízení strmě roste. Alarmujícím příkladem z poslední doby je např. útok na nemocnice v Litvě právě skrze monitoring fotovoltaických elektráren. Co vlastníkům levných a nezabezpečených systémů hrozí? Jedná se o několik druhů rizik a ve výsledku i zmaření části nebo celé investice.

1. Geopolitická rizika a potenciální zákaz technologie, odpojení od internetu nebo od sítě
2. Napadení a dálkové ovládnutí systému, krádež citlivých dat, žaloby, pokuty a sankce
3. Nesoulad s přicházející kybernetickou legislativou

Geopolitická rizika - USA, Austrálie a se zpožděním i Evropa si uvědomily, že v jejich energetické síti je celá řada zařízení z nespolehlivých zemí, které ovládají obrovský agregovaný výkon (např. všechny FV instalace na RD, firmách a veřejných budovách), nejsou nikým regulovány a prostřednictvím internetu mohou velmi jednoduše mohou ohrozit energetickou síť daného státu nebo celou energetickou síť v EU. Z posledních studií plyne, že např. pro ohrožení stability sítě v Nizozemsku stačí ovládnout agregovaný výkon 3GW a kaskádovitým efektem je ohrožena celá evropská síť. Jen samotní výrobci měničů ovládají přes monitorovací platformy výkony v řádech desítek či stovek GW. EU se problémem intenzivně zabývá (např. Network Code on Cybersecurity) a je velmi pravděpodobné, že bude muset tzv. „non-traditional stakeholders" regulovat. V úvahu přichází např. odpojení daného zařízení od internetu nebo dokonce od sítě. Problémem se nyní také intenzivně zabývají rozvědky jednotlivých států (např. BIS, estonská rozvědka apod.) nebo český NÚKIB, které vydaly několik varování. Některé země již rozhodly od odpojení zařízení pocházející z nespolehlivých zemí od internetu (Litva, listopad 2024).

Dálkové ovládnutí systému - drtivá většina FV měničů postrádá absolutně základní kybernetické zabezpečení a slouží hackerům jako vstupní brána do interních podnikových sítí nebo do systémů úřadů. Důsledkem je ovládnutí systému nebo podnikových sítí, krádež citlivých dat, vydírání („ransomware"), žaloby a následné citelné sankce a pokuty. Nedávno ovládli desítky GW systémů asijských značek v Evropě tzv. etičtí hackeři (např. Vangelis Stykas) a tvrdí, že změnou FW mohou daná zařízení dokonce přivést ke vznícení.

Nová kybernetická legislativa - přicházející evropská kybernetická legislativa (např. Cyber Resilience Act) bude znamenat pro velkou většinu tzv. levných FV zařízení z nespolehlivých zemí značné potíže a nynější koupě levného a nezabezpečeného zařízení se může investorům v blízké budoucnosti prodražit. Hrozí značné investice do kybernetického zabezpečení nebo i odpojení takového zařízení od sítě (tak jako tomu bylo u některých IoT zařízení při zavedení první základní kybernetické legislativy v dubnu roku 2024 ve Velké Británii).

Doporučení: při výběru technologie FV měničů je vhodné zvolit výrobce sdružené v European Solar Manufacturing Council (ESMC).

Příklady úplně těch nejzákladnějších kybernetických problémů a přístup firmy SolarEdge.

STEJNÉ VÝCHOZÍ HESLO: Většina levných měničů vyjíždí z výroby s výchozím heslem, například (Uživatelské jméno: Admin, Heslo: 12345678). To je nebezpečné, protože hackeři mohou náhodně posílat příkazy na miliony náhodných IP adres (např. 192.0.0.2) a pokoušet se připojit pomocí výchozího hesla. Této metodě se říká „Spray and pray" a je hlavním důvodem napadení IoT zařízení. SolarEdge generuje silné náhodné a jedinečné heslo pro každý měnič, který vyjde z výroby, a toto jedinečné heslo vytiskne na měnič. To zvyšuje bezpečnost měniče a znemožňuje hackerům použít výchozí heslo a dálkově ovládnout systém.

VIDITELNÁ WI-FI SÍŤ (SSID) - do měniče, který má otevřený signál Wi-Fi (SSID), se mohou potenciálně nabourat procházející osoby nebo osoby v projíždějících vozidlech („Wardriving"), a to různými způsoby prolomení hesla. Většina levných střídačů má SSID „always on", ale měnič SolarEdge vysílá signál Wi-Fi pouze po dobu 15 minut, a to pro specifické účely, jako je instalace nebo servis. Tento bezpečnostní prvek znemožňuje útočníkům, kteří jsou fyzicky blízko, využít Wi-Fi jako útočnou platformu.

AKTUALIZAČNÍ SOUBORY VOLNĚ DOSTUPNÉ NA INTERNETU - přečtení zdrojového kódu je pro útočníka velmi dobrou zkratkou, když hledá způsoby, jak se do zařízení nabourat. Mnoho výrobců levných zařízení ponechává celý zdrojový kód v souboru s aktualizací firmwaru, nešifruje jej a nechává jej online ke stažení na svých webových stránkách. Společnost SolarEdge dbá na to, aby soubory firmwaru byly při instalaci do zařízení šifrovány a kryptograficky ověřovány (podepsány). Nejsou volně dostupné a jsou zasílány pouze v případě potřeby formou zabezpečené komunikace ze serveru SolarEdge do zařízení.

ZDROJOVÝ KÓD je totiž pro hackera něco jako „tahák". Přístup k nezašifrovanému zdrojovému kódu umožňuje hackerům zjistit, kde jsou v kódu chyby, a potenciálně tyto zranitelnosti zneužít. Je důležité, aby byl zdrojový kód skrytý a zašifrovaný. Jinak hackeři mohou potenciálně měnit firmware a instalovat poškozený firmware, který může narušit výkon zařízení nebo dokonce způsobit jejich požár (více např. ZDE).

KOMPATIBILITA S GDPR - GDPR je zákon, který musí dodržovat všechny společnosti působící v EU. Jeho dodržení není v zásadě kontrolováno, auditováno ani certifikováno. Čínští prodejci jej v obecné rovině dodržují, ale je na spotřebiteli, aby se rozhodl, zda důvěřuje tomu, že údaje evropských FVE jsou skutečně uchovávány pouze na půdě EU, jak GDPR vyžaduje. Společnost SolarEdge má fyzické datové centrum v německém Frankfurtu, kde uchovává svá data. Mezitím mnohé čínské společnosti oznámily strategická partnerství s poskytovateli cloudů, jako je např. AliBaba, kteří sídlí v Číně a podléhají čínským zákonům.

PROVĚŘOVÁNÍ HW a vlastní výroba kritických komponent. Prověřování hardwaru (vendor vetting process) znamená, že se ověřuje obchodní bezúhonnost společností, od kterých se nakupují elektronické komponenty, jako jsou mikročipy nebo komunikační čipy. Tím se snižuje riziko, že by do zařízení byla na hardwarové úrovni vložena zadní vrátka (tzv. backdoor). Existuje mnoho příkladů zadních vrátek nalezených prostřednictvím podobných „útoků na dodavatelský řetězec". Některé kritické komponenty si společnost SolarEdge navrhuje a vyrábí sama. Jedná se např. o ASICs, což je zjednodušeně řečeno elektronický čip, který je ústředním prvkem fungování hlavní počítačové desky měniče.

Doporučení pro tendry: základní požadavky kybernetického zabezpečení typu: „každý měnič musí mít své unikátní defaultní heslo" apod.

V případě dalších dotazů ohledně kybernetické bezpečnosti FV systémů kontaktujte prosím zástupce společnosti SolarEdge (Ing. Jindřich Stuchlý, Ph.D., jindrich.stuchly@solaredge.com , +420 725 882 477).