Stanovení standardu pro kybernetickou bezpečnost fotovoltaických systémů

Rostoucí hrozby pro globální energetický sektor

V dnešním propojeném světě je energetický sektor hlavním cílem kybernetických hrozeb, které pocházejí z různých zdrojů. Tyto hrozby sahají od finančně motivovaných plánů kybernetických zločinců až po politicky motivované útoky organizované národními státy. Jen v roce 2023 vyplatily oběti kybernetických hackerů po celém světě (ze všech odvětví) po útocích ransomwaru obrovskou částku 1,1 miliardy dolarů - a to je jen to, co bylo nahlášeno*.

40 000

FV systémů nainstalovaných v holandských domácnostech a podnicích bylo nizozemskou vládou považováno za zranitelné vůči dálkovému ovládnutí (červenec 2022)

130 000

FV systémů od několika výrobců měničů bylo společností zabývající se kybernetickou bezpečností nahlášeno jako zranitelné vůči kybernetickým útokům (USA, červenec 2023)

200 milionů dolarů

Odhadované ztráty, které vznikly společnosti Target Corporation poté, co byla síť jejího poskytovatele HVAC napadena (USA, 2013).

Nezajištěné FV systémy představují kritická obchodní rizika

Solární energie je rychle rostoucí složkou globálního energetického mixu a tvoří významnou část celkové výroby energie v mnoha zemích, jako je Nizozemsko, Německo a USA. Již dnes je klíčovým zdrojem energie, který pomáhá snižovat náklady na elektřinu a zajišťovat kontinuitu podnikání mnoha společností. FV systémy sice nabízejí udržitelná energetická řešení, ale zároveň představují nové možnosti pro kybernetické hrozby. Srdcem každého systému je měnič, zařízení internetu věcí (IoT), které je obvykle připojeno k internetu a umožňuje monitorování a řízení systému. Díky tomu je mnohem náchylnější ke kybernetickým útokům ve srovnání s dobře chráněnou plynovou nebo uhelnou elektrárnou.

Solární energie se používá k napájení stále většího počtu lokálních energetických zařízení, jako jsou baterie, nabíječky elektromobilů a systémy HVAC, a bude tomu tak stále častěji, protože přecházíme do éry systémů řízení spotřeby energie. Nezabezpečený fotovoltaický systém ohrožuje nejen kontinuitu podnikání, ale může také sloužit jako nevědomá brána pro hackery k přístupu k energetické infrastruktuře podniku a také k širším digitálním platformám organizace, což má za následek další materiální, finanční a reputační škody.

* www.chainalysis.com/blog/ransomware-2024

Mezi běžná kybernetická rizika patří:

Únik dat a sankce

Hackeři mohou zneužít zranitelné fotovoltaické systémy ke krádeži soukromých dat uložených v interních sítích organizace. Za únik dat musí oběť platit vysoké pokuty.

Dálkové ovládnutí a odmítnutí služby (DoS)

Když se podnik stane obětí útoků DoS nebo dojde k dálkovému ovládnutí, musí čelit významným obtížím a škodám. Ransomware může držet kritická data jako rukojmí, zatímco dálkové ovládnutí a útoky DoS mohou zcela zastavit základní služby.

(Ne)soulad s dodržováním předpisů

V souvislosti se zaváděním nových kybernetických předpisů musí majitelé fotovoltaických elektráren přijmout proaktivní opatření, aby zajistili, že jejich systémy zůstanou v souladu s předpisy. V opačném případě hrozí riziko stažení výrobků z trhu nebo finanční sankce v případě narušení jejich sítí.

Připravují se nové kybernetické zákony a předpisy pro fotovoltaické systémy

FV systémy se staly kritickou energetickou infrastrukturou a jako takové přitahují vážnou pozornost regulačních orgánů. To je již vidět ve „vlně" připravovaných nových zákonů a předpisů.

UL 2941
Specializovaná mezinárodní norma pro kybernetickou bezpečnost chytrých měničů a distribuovaných energetických zdrojů.
(Očekáváno 2025)

„US Cyber Trust Mark" Program
Program certifikace a označování kybernetické bezpečnosti.
(Očekáváno 2025)

National Association of Regulatory Utility Commissions (NARUC/NASEO)
Základní principy kybernetické bezpečnosti pro elektrické distribuční soustavy a decentralizované zdroje energie.
(Očekáváno 2025)

Pracovní skupina IEEE P1547.10
Gateway platforms pro decentralizované zdroje energie.
(Probíhající práce)

UK PSTI (2023)
Zabezpečení produktů a telekomunikační infrastruktura.

RED 2014/53/EU
Evropská směrnice o rádiových zařízeních.

Cyber Resilience Act (Akt o kybernetické odolnosti)
Právní předpisy EU pro kybernetickou bezpečnost internetu věcí a připojených zařízení.
(Očekáváno 2026-2027)

Směrnice NIS 2
Směrnice pro dosažení vysoké úrovně kybernetické bezpečnosti v celé EU.
(Platí od října 2024)

SolarEdge - světový lídr v oblasti kybernetické bezpečnosti FV elektráren

Společnost SolarEdge je lídrem v oboru fotovoltaiky s celosvětovou působností a miliony připojených IoT zařízení.

Díky tomu má vynikající pozici pro rozpoznání rizik kybernetické bezpečnosti, kterým čelí majitelé fotovoltaických zařízení a energetické sítě.

Vaše bezpečnost je základem našeho podnikání

Vynaložili jsme značné investice na nábor specializovaného týmu odborníků, kteří vedou a neustále vyvíjejí naše kybernetické aktivity.

Pomáháme navrhovat mezinárodní regulační kybernetické normy

Společnost SolarEdge je aktivním účastníkem různých technických výborů a pracuje na tom, aby byl design všech výrobků v souladu s připravovanými předpisy.
Naše zařízení splňují standardy nejnovějších referenčních předpisů a norem kybernetické bezpečnosti pro decentralizované zdroje energie.

Produkty SolarEdge jsou prioritně vyvíjeny s ohledem na kybernetickou bezpečnost

Snažíme se, aby naši zákazníci byli neustále chráněni před neustále se vyvíjejícími kybernetickými hrozbami, a to zaváděním opatření v každém kroku návrhu našich produktů - napříč veškerým softwarem a hardwarem SolarEdge.

Maximalizujte svůj CyberEdge

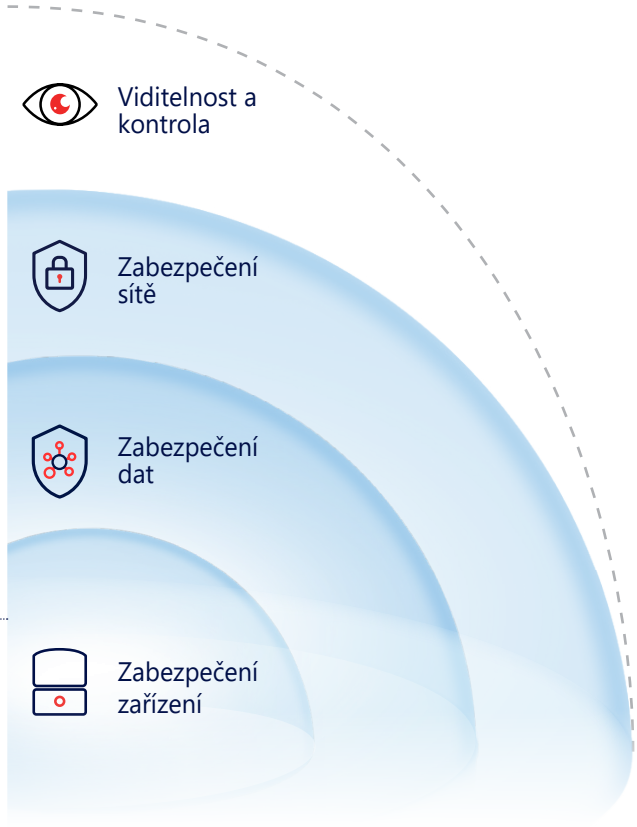
Partnerství se SolarEdge znamená, že získáte extra ochranu po celou dobu životnosti systému. Náš víceúrovňový přístup ke kybernetické bezpečnosti je zaměřen na ochranu integrity dat, komunikace a provozních operací od uvedení do provozu až po výrobu. Pro zabezpečení konektivity, funkčnosti a dat zákazníků se společnost SolarEdge řídí principem Cyber Informed Engineering (CIE) a do svých produktů začleňuje mechanismy zabezpečení informací již od počátečních fází návrhu. Neustále přizpůsobujeme a zdokonalujeme naše řešení tak, aby odpovídala vyvíjejícím se požadavkům a regulačním normám.

Upřednostňujeme potřeby bezpečnostních týmů našich zákazníků a navrhujeme naše produkty tak, aby byly nejen bezpečné, ale aby také zajišťovaly maximální přehled a kontrolu pro naše uživatele.

Energetická podsíť síť je strukturována tak, aby se bezpečně integrovala se sítěmi IT a OT vaší organizace.

Uživatelská data a údaje o spotřebě energie jsou bezpečně přenášeny a ukládány, což zajišťuje maximální soukromí dat a ochranu před kybernetickými hrozbami.

Měniče SolarEdge jsou srdcem fotovoltaického systému a spolu s dalšími zařízeními SolarEdge jsou navrženy tak, aby odhalily a zabránily kybernetickým útokům na celý fotovoltaický systém.



Požární i kybernetická bezpečnost jsou pro FV systémy zcela zásadní

Minimalizujte kybernetické riziko tím, že se rozhodnete spolupracovat se společností SolarEdge. Zajistěte, aby vaše podnikání zůstalo bezpečné a odolné vůči neustále se vyvíjejícím hrozbám.

O SolarEdge

Společnost SolarEdge Technologies je celosvětovým lídrem v oblasti technologií obnovitelných zdrojů energie. Využívá prvotřídní inženýrství a inovace k vytváření fotovoltaických řešení pro rezidenční, komerční a pozemní elektrárny. SolarEdge přináší optimalizovaný přístup k výrobě, skladování, správě a spotřebě energie. Společnost vyvíjí a vyrábí fotovoltaické měniče a optimizéry výkonu, řešení pro správu a optimalizaci energie, skladování energie a síťové služby. DC optimalizovaná technologie SolarEdge je nainstalována v milionech domácností ve více než 140 zemích světa a více než 50 % společností z žebříčku Fortune 100 má na svých střechách technologii SolarEdge. SolarEdge urychluje přechod k distribuovaným a udržitelným energetickým sítím, které budou optimalizovat energii všude.