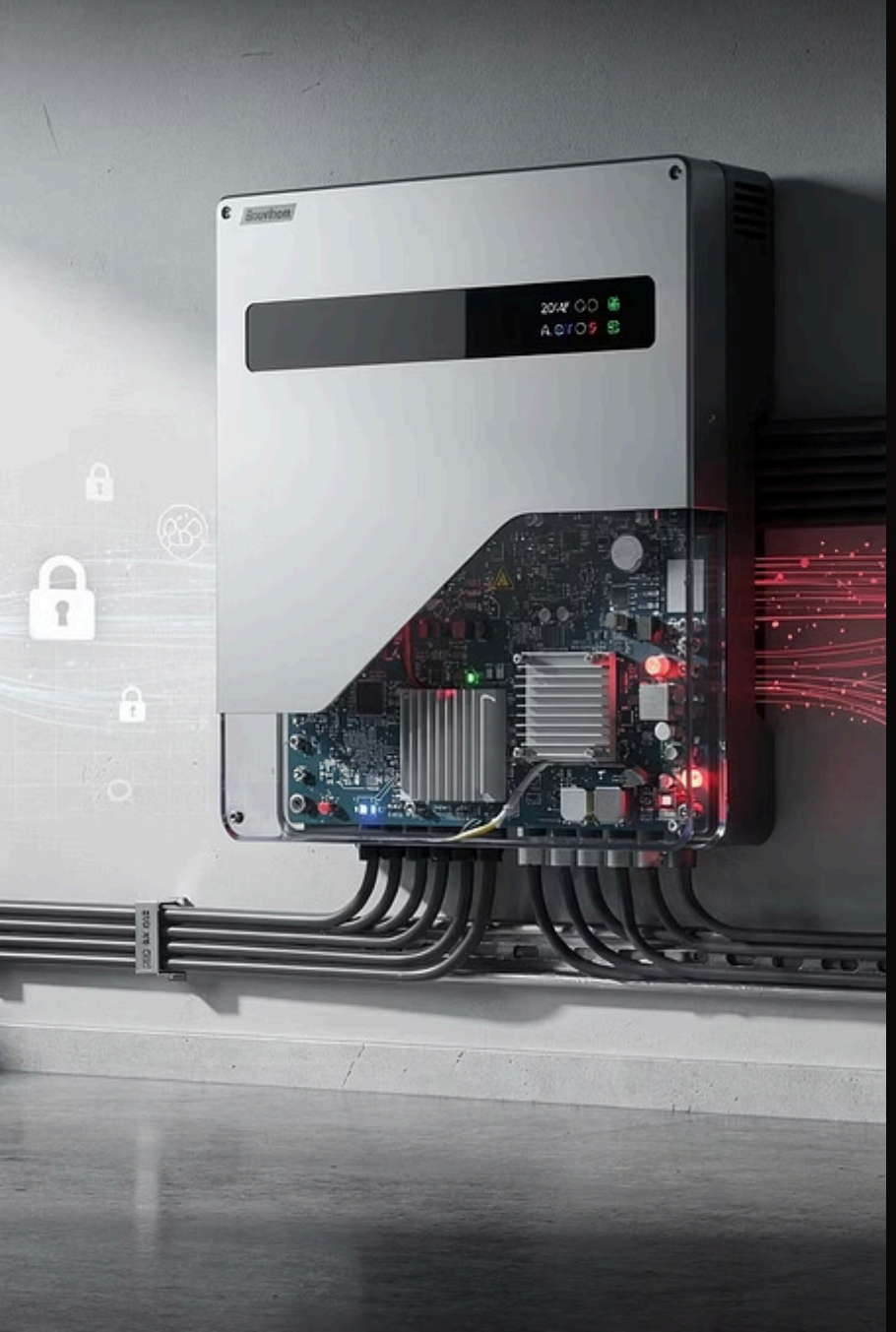


Když se střídač stane vstupní branou

Dnes je střídač více než jen převodník energie – je to kritický bod, který propojuje váš systém FVE s digitálním světem. To z něj činí jak páteř funkčnosti, tak potenciální slabinu.

Michal Vyskala

Marketing Manager, SOLSOL

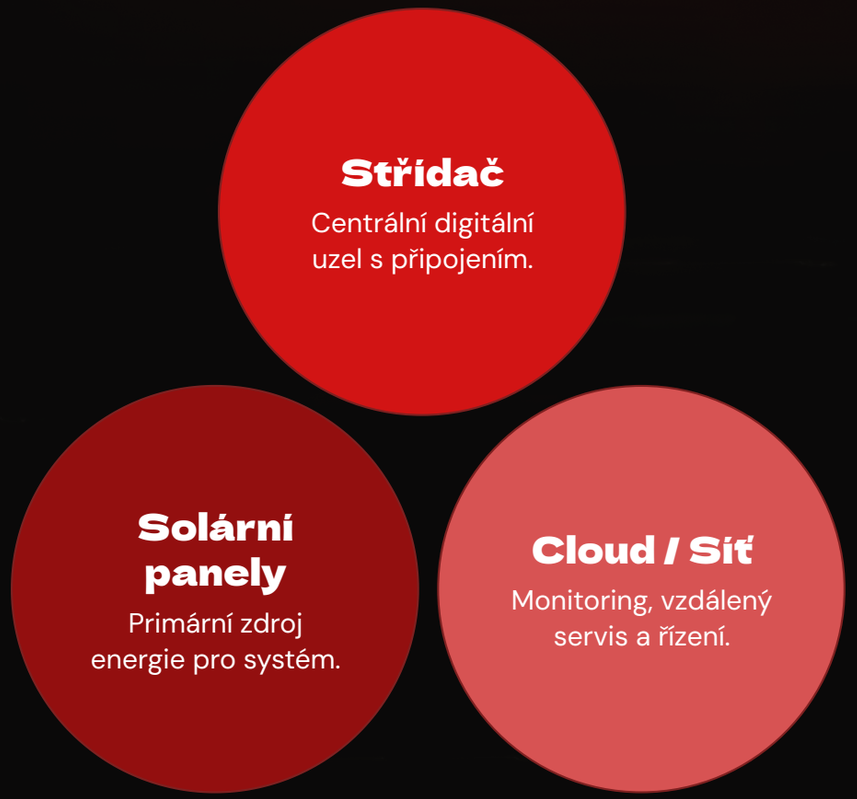
Působím jako marketing manažer ve společnosti **SOLSOL**, která je největším distributorem fotovoltaických technologií v České republice.

- Profil LinkedIn
- Web SOLSOL

Proč je střídač vstupní branou

FVE KYBERNETICKÁ BEZPEČNOST

FVE už není jen zdroj energie — je to **digitálně řízený systém**. Střídač dnes zajišťuje připojení k internetu, cloudový monitoring, vzdálený servis a řízení dalších prvků. Stává se tak centrálním digitálním uzlem celého ekosystému.



Každý měnič, bateriové úložiště nebo vzdálená platforma rozšiřují útočnou plochu. **Čím více konektivity, tím větší závislost na kybernetické odolnosti.**

Případová studie: Polsko 12/2025

Když útok na komunikaci přeroste v systémové riziko

V Polsku došlo ke koordinovanému kybernetickému útoku, který odhalil kritickou zranitelnost v energetické infrastruktuře.

Cíl útoku

Komunikační vrstva mezi distribuční soustavou a více než 30 větrnými, solárními farmami a teplárnami.

Dopad incidentu

Ohrožení dodávek tepla pro 500 tisíc obyvatel a reálné riziko celonárodního výpadku elektřiny.

Důsledek a reakce

Urychlení prací na polském zákoně o národní kybernetické bezpečnosti a zdůraznění strategického významu energetické kyberbezpečnosti.

Tento případ ukazuje, že zranitelná komunikace mezi sítí a zdroji může proměnit lokální incident v národní problém.

Kdo útočí a proč

Motivace útočníků se liší — slabiny systémů jsou však často stejné.

💰 Finanční motivace

Vydírání, ransomware, neoprávněný přístup do sítě nebo krádež provozních dat.

🌐 Geopolitická motivace

Průzkum infrastruktury, vliv na distribuci energie, strategické narušení provozu.

⚡ Oportunistické zneužití

Slabě zabezpečená IoT zařízení automaticky skenovaná a zneužívaná ve velkém měřítku.

⚠ Nejčastější cesta útoku není sofistikovaná — stačí **ukradené účty, slabá hesla, otevřený vzdálený přístup nebo zranitelný firmware**. Útočník nemusí být geniální. Stačí, aby systém byl levný, rozšířený a špatně zabezpečený.

Co je ve hře

Kybernetický incident ve FVE není jen technická závada. Jeho dopady sahají daleko za hranice strojovny.

Omezení výroby

Odstavení nebo narušení výrobního provozu elektrárny.

Ztráta kontroly

Převzetí řízení zařízení neoprávněnou stranou.

Vstup do sítě

Laterální pohyb do firemní nebo veřejné infrastruktury.

Únik dat

Kompromitace provozních nebo citlivých obchodních dat.

Reputační škoda

Ztráta důvěry u klientů, partnerů a veřejnosti.

Dodatečné náklady

Audit, retrofit nebo výměna technologie — vše ex post a draho.

Co na začátku vypadá jako **levnější nákup**, se může změnit v nákladný provozní a bezpečnostní problém. Ve hře není jen výkon elektrárny, ale **kontinuita provozu, důvěra a budoucí náklady**.

Od lokálního incidentu k systémovému riziku

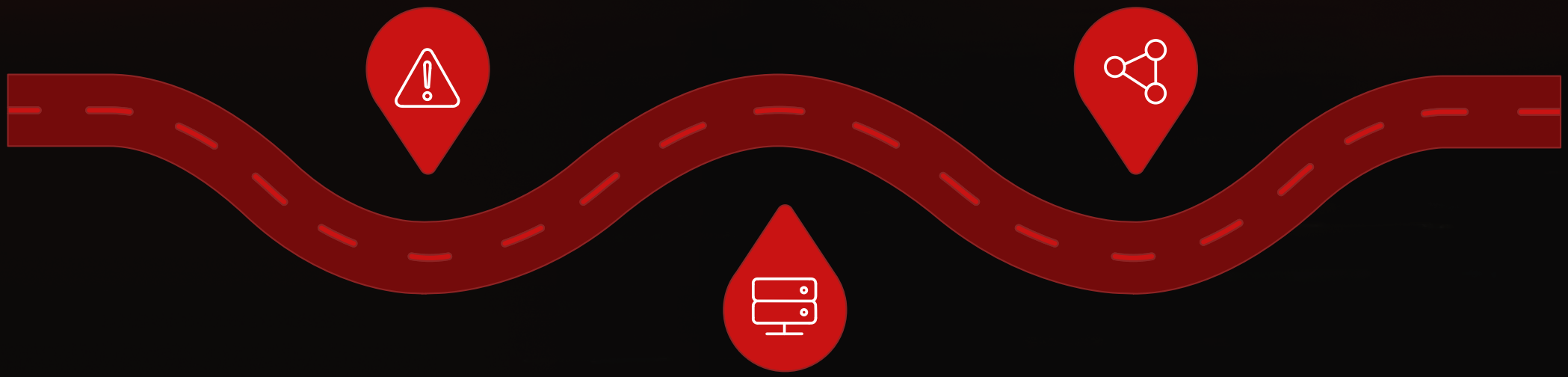
Jeden zranitelný střídač je provozní problém. Tisíce stejných střídačů na stejných platformách jsou **infrastrukturní riziko**.

Lokální incident

Jeden zařízení,
omezený dopad

Systémové riziko

Tisíce zařízení,
koordinovaný útok



Více instalací

Desítky zařízení,
podobné zranitelnosti

Technický detail

Zařízení napojená na stejné cloudové platformy, používající podobný firmware a sdílející obdobné slabiny, umožňují koordinovaný útok s rozsáhlým dopadem na distribuci energie.

Strategické téma

Riziko neroste jen **počtem zařízení**, ale mírou jejich **společné ovladatelnosti**. Zde se z technického detailu stává téma pro firmy, municipality i stát.

Regulace a právní rámec

Kyberbezpečnost FVE přestává být doporučením — stává se **vymahatelnou povinností**.

1

RED / ETSI EN 303 645

1. srpna 2025 — Kybernetické požadavky na rádiová zařízení; baseline bezpečnostní standard pro IoT (unikátní hesla, bezpečné aktualizace).

2

ZoKB č. 264/2025 Sb.

1. listopadu 2025 — Nový český zákon o kybernetické bezpečnosti promítající NIS2; rozšiřuje okruh povinných organizací.

3

NIS2 (průběžně)

Řízení rizik, odpovědnost vedení a **povinné hlášení incidentů**. Platí pro provozovatele kritické a důležité infrastruktury.

4

Cyber Resilience Act

11. prosince 2027 — Horizontální požadavky na bezpečnost digitálních produktů během celého životního cyklu (v účinnosti od 10. 12. 2024).

⚠ **Kdo dnes vybírá technologii bez kybernetických parametrů**, může zítra narazit na compliance problém, povinný retrofit nebo neobhajitelný provoz.

Na co dbát při výběru technologie

Při výběru FVE technologie a dodavatele jsou toto **minimální bezpečnostní parametry**, které musí být součástí zadání, smlouvy a SLA.

🔑 Unikátní výchozí hesla

Každé zařízení musí mít jedinečné heslo — žádné sdílené tovární výchozí hodnoty.

🔄 Bezpečné aktualizace firmware

Podepsané a auditovatelné aktualizace s jasným procesem dodávky a ověření.

🔒 Řízený vzdálený přístup

Auditovatelný přístup s minimálními oprávněními a logovatelností každé relace.

📊 Transparentní práce s daty

Jasné vymezení, kde jsou data uložena, kdo k nim má přístup a za jakých podmínek.

✅ Doložitelný bezpečnostní proces

Výrobce i dodavatel musí být schopni prokázat svůj přístup ke kybernetické bezpečnosti.

📋 Promítnutí do smlouvy a SLA

Všechny bezpečnostní požadavky musí být smluvně závazné — ne jen deklaratorní.

Bezpečnost nesmí být doplněk. Musí být součástí zadání. V další části se podíváme na praktické řešení, jak ochrannou vrstvu do FVE doplnit.