Kyberbezpečnost moderní elektrizační sítě

All for POWER | 5.3.2020 |
Rubrika: Elektrizační soustava | Strana: 66 | Autor: Doc. RNDr. Tomáš Pitner, Ph. D. | Téma: Masarykova univerzita, vysoké školy

S problematikou kyberbezpečnosti energetických řídicích systémů se nesetkáváme na stránkách All for Power poprvé. Integrace distribuovaných energetických zdrojů (DER), zejména obnovitelných, do inteligentní sítě zejména na úrovni distribuční soustavy se zrychluje a aktivity kolem využitelné flexibility (viz články k flexibilitě na stránkách tohoto časopisu), stejně jako nárůst specifické spotřeby vyvolané elektromobilitou napomohou ještě širšímu využití distribuovaných zdrojů.
Zařízení řídící distribuované zdroje energie, například inteligentní střídače pro fotovoltaiky či kontroléry řídící dobíjení elektromobilů doplňují již tak složitý systém měřicího a řídicího vybavení (SCADA) rozvoden a distribučních trafostanic, kde jde o jednotky RTU, koncentrátory AMM, měřící jednotky fázorů, ale také inteligentní transformátory, detektory zkratových proudů, dálkově řízené vypínače, a spoustu dalších komponent.
Co do rozsahu je velice významným krokem rozšíření inteligentních měřicích infrastruktur vč. koncových prvků (smart meterů) nad rámec relativně malých pilotních oblastí. To všechno jsou komponenty tvořící složité, a tudíž potenciálně zranitelné systémy, a výrazně rozšiřují perimetr potřebného zabezpečení nad rozměry obvyklé v běžných **IT** systémech jednoho provozovatele. Některé prvky, typicky smart metery, se nacházejí na místech nikoli fyzicky chráněných proti nepovolanému přístupu, a navíc v jejich bezprostředním sousedství nebo propojení fungují nebo budou fungovat řídicí systémy chytrých budov i obytných domů, které budou téměř vždy komunikovat nejen uvnitř lokálních domácích sítí, ale i po veřejném internetu a bude se k nim přistupovat prostřednictvím mobilních zařízení, tzn. přes veřejnou telekomunikační síť.
Pro komunikaci, tzn. výměnu dat a řízení, je používána řada protokolů, vzniklých často před desetiletími, kdy se kyberbezpečnostní hrozby z mnoha důvodů prakticky nevyskytovaly, mj. proto, že perimetr systémů byl omezený. Nejinak tomu bylo v průmyslu. Koncem 70. let se objevil doposud populární Modbus, schopný provozu na pomalých přenosových médiích (rádio, sériové linky a až později IP sítě). Sám o sobě nedisponoval žádným využitím kryptografie, tzn. bez rozšíření nebyl v podstatě odolný proti žádným hrozbám, a to ani kdyby bylo využito ověřování pomocí hesel. V řízení se dále široce používají protokoly DNP3 (Distributed Network Protocol 3.0), kde se rovněž objevují návrhy zabezpečení na úrovni protokolu až v posledních letech. Dosud používaný protokolem je rovněž průmyslový Profibus (PROces FIeld BUS), zejména na robustních sériových linkách RS-485, kde umožňuje přenosy na velké vzdálenosti. Rodiny protokolů specializované pro energetiku, jako jsou IEC 61850, umožňují zabezpečení díky nadstavbě v podobě IEC 62351.
Situace „na spodních vrstvách“ se tak postupně zlepšuje řadou opatření – protokoly při přenosech mimo fyzicky zabezpečené sítě používají k přenosu šifrované IP kanály (IPSec, sítě VPN) a u některých protokolů se používají vyšší (pokročilejší) varianty již disponující zabezpečením.
Systémy však zůstávají zranitelné takříkajíc „z opačného konce“, z dispečinků. Na začátku bývá člověk. Klasickým příkladem komplexního využití zranitelností distribuční soustavy je známý případ z Ukrajiny (1]. V prosinci 2015 zažil ukrajinský energetický systém rozsáhlý výpadek dodávek zasahující přibližně 225 000 zákazníků. Dle zveřejněné zprávy začal útok instalací malwaru phishingovými e-maily několik měsíců před vlastním výpadkem. Během „průzkumného“ období útočníci sledovali chování sítě a plánovali útok. V den D bylo napadeno rozhraní lidské obsluhy (HMI) a použito k vzdálenému odepnutí několika vypínačů, což přímo přerušilo dodávku zákazníkům. Proces obnovy byl výrazně zdržen tím, že byl současně masivním DoS (Denial of Service) útokem prakticky vyřazen telefonní systém a komunikační síť, takže callcentrum ani nemohlo přijímat zákaznické hovory. Malware na rozhraní HMI současně likvidoval software v systému, což provozovateli bránilo určit rozsah výpadků a dodávku obnovit.
Kyberútoky proti energetickým řídicím systémům se nevyhýbají ani západu. Konkrétně západ USA zažil v březnu loňského roku následně důkladně zdokumentovaný kyberútok (2]. Operátoři v centru řízení dodávek začali ztrácet komunikaci s „několika vzdálenými místy pro výrobu energie“ po dobu několika minut. Z nějakého důvodu se firewally připojené k internetu restartovaly a přecházely do offline režimu. Každé restartování sice přerušilo komunikaci mezi řízením a výrobou na nejvýše pět minut, ale stále se to opakovalo a trvalo celkem téměř 10 hodin. Naštěstí zafungoval plán reakce na kyberbezpečnostní incidenty a brzy se zjistila příčina – zvnějšku využitelná (známá!) zranitelnost

použitých firewallů. Dodavatel okamžitě aplikoval záplaty a řízení se obnovilo. Naštěstí se to celé stalo v méně významné části sítě, navíc v období bez zvýšené spotřeby – ani v zimě, ani v létě. Poučení zní: aktivní prvky poctivě záplatovat, mít co nejméně bodů propojení s internetem a nasadit vícevrstvou ochranu (např. ověřování přístupu ještě před firewallem). Rovněž redundance pomohla – tam, kde byly firewally duplikované a s vysokou dostupností, tam restarty tolik nevadily.
Závěr? Přirozeným řešením, jak zabránit rozsáhlým fatálním výpadkům, se zdá být dále zlepšovat technologie a eliminovat lidský faktor. Nicméně objevují se překvapivě protikladné přístupy – Národní kritická infrastruktura v USA včetně elektrorozvodných sítí chce dle schváleného senátního návrhu SEIA (Securing Energy Infrastructure Act) jít cestou posílení redundantních analogových, „low-tech“ nástrojů a lidské obsluhy, mimo jiné i na základě poučení z ukrajinského případu, kde škody mohly být ještě výrazně větší nebýt toho, že řízení bylo stále do značné míry manuální – a že personál byl dostatečně kvalifikovaný síť skutečně manuálně uřídit.
Americký koncept, který se má v následujících letech pilotně ověřovat, předpokládá, že bez manuální akce nebude možné provádět zásadní řídicí úkony, což by mělo eliminovat riziko celosystémových výpadků. Nicméně oponenti upozorňují, že to bude dražší o kvalifikovanou lidskou sílu a že je to nerealistický krok zpět. Uvidíme, možná i toto bude součást cesty k bezpečné síti. 1. SANS and Electricity Information Sharing and Analysis Center (E-ISAC): Analysis ofthe cyber attack on the Ukrainian power grid; 18. března 2016. http://www.nerc.com/pa/CI/ESISAC/Documents/EISAC_SANS_Ukraine_DUC_18Mar201 6.pdf 2. Sussman, B. Revealed: Details of 'First of Its Kind' Disruptive Power Grid Attack. SecureWorld 19. října 2019. https://www.secureworldexpo. com/industry-news/firstu. s.-power-grid-attack-details 3. O'Flaherty, K.: U. S. Government Makes Surprise Move To Secure Power Grid From Cyberattacks. Forbes 3. července 2019. https://www.forbes.com/sites/kateoflahertyuk/2019/07/03/u-s-governmentmakessurprise-move-to-secure-powergridfrom-cyber-attacks/#68165e123191

Foto popis|

O autorovi| Doc. RNDr. Tomáš Pitner, Ph. D. Masarykova univerzita, **Fakulta informatiky** 94@muni.cz