VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2019 Martin Biolek

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

NÁVRH METODIKY TESTOVÁNÍ CHYTRÝCH SMART METERŮ SE ZAMĚŘENÍM NA INVAZIVNÍ TESTOVÁNÍ

DESIGN OF A SMART METER TESTING METHODOLOGY FOCUSING ON INVASIVE TESTING

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR
Martin Biolek

VEDOUCÍ PRÁCE
SUPERVISOR
Ing. Tomáš Lieskovan

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Informační bezpečnost**
Ústav telekomunikací

Student: Martin Biolek ***ID:*** 191382
Ročník: 3 ***Akademický rok:*** 2018/19

NÁZEV TÉMATU:

Návrh metodiky testování chytrých smart meterů se zaměřením na invazivní testování

POKYNY PRO VYPRACOVÁNÍ:

Cílem bakalářské práce je zpracovat analýzu aktuálního stavu a seznam doporučení a povinností vyplývajících z různých norem a standardů v oblasti informační bezpečnosti smart meterů. Zohlednit následující: Zákon o kybernetické bezpečnosti, Soubor norem ISO 27000, Standardy NERC-CIP a ISA S99 / IEC 62443. Práce by měla vyjmenovat a stručně popsat povinnosti a důležitá doporučení v oblasti informační bezpečnosti řídicích a monitorovacích systémů v energetice. Na základě těchto doporučení navrhněte komplexní metodiku pro testování komunikační bezpečnosti chytrých elektroměrů (minimálně dvou typů). Dále proveďte analýzu dostupných skenerů zranitelností a prakticky je ověřte na chytrých elektroměrech (minimálně dvou typů). Celkovým cílem je ověření komunikační bezpečnosti chytrých elektroměrů dle navržené metodiky jak z pohledu dokumentace, tak i praktických testů.

DOPORUČENÁ LITERATURA:

[1] BURDA, K. Bezpečnost informačních systémů. Brno: VUT v Brně, 2013. s. 1-152. ISBN: 978-80-214-4890- 2.

[2] Gilbert N. Sorebo, Michael C. Echols. Smart Grid Security: An End-to-End View of Security in the New Electrical Grid. December 5, 2011 by CRC Press, 328 stran. ISBN 9781439855874.

Termín zadání: 1.2.2019 ***Termín odevzdání:*** 27.5.2019

Vedoucí práce: Ing. Tomáš Lieskovan
Konzultant:

prof. Ing. Jiří Mišurec, CSc.
předseda oborové rady

ABSTRAKT

Bakalářská práce je zaměřena na problematiku penetračního testování chytrých elektroměrů. V rámci teoretické části jsou popsány dostupné standardy, kterými by se výrobci chytrého elektroměru měli řídit. Následuje pak praktická část zaměřená na testování dvou systémů chytrých elektroměrů a zjištění jejich nedostatků. Výsledkem práce je kompromitace jednoho systému, který potřebuje výrazné vylepšení pro nasazení do provozu v nové verzi. Popis nedostatků je zahrnut v praktické části práce.

KLÍČOVÁ SLOVA

chytrý elektroměr, informační bezpečnost, zákon o kybernetické bezpečnosti, penetrační testování, zranitelnost, útok

ABSTRACT

Bachelor thesis is focused on investigating the security deficits of smart meters through penetration testing. The theoretical part describes the standards that should be followed by smart meter manufacturers. This is followed by the practical part where the testing of two smart meter systems was conducted in order to discover their vulnerabilities. The result of the work is the exposure of one of the two systems of interest that requires significant security improvements before deployment of another version. A description of the vulnerabilities is included in the practical part of the thesis.

KEYWORDS

smart meter, information security, cyber security law, penetration testing, vulnerability, attack

BIOLEK, Martin. *Návrh metodiky testování chytrých smart meterů se zaměřením na invazivní testování*. Brno, 2018, 63 s. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: Ing. Tomáš Lieskovan

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Návrh metodiky testování chytrých smart meterů se zaměřením na invazivní testování“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autora

PODĚKOVÁNÍ

Chtěl bych poděkovat svému vedoucímu bakalářské práce Ing. Tomáši Lieskovanovi za odborné vedení, za pomoc a rady při zpracování této práce.

Brno ....

podpis autora

Obsah

Seznam obrázků

Úvod

V současnosti se smart metry stávají běžným elektrickým zařízením, které je součástí elektrického rozvaděče. Smart metr se může nacházet v domácnostech, v rámci výroby v průmyslu nebo v dobíjecích stanicích pro elektromobily.

Cílem teoretické části bakalářské práce je přiblížit čtenáři problematiku smart metru v systému informační bezpečnosti. Tato část se opírá o dostupné standardy a zákonné normy pro zajištění informační bezpečnosti. Na začátku jsou popsány základní vlastnosti a požadavky kladené na smart metr. Následuje výčet a popis druhů smart metrů na základě počtu fází či podle přenosové technologie. Mezi standardy, o které se bakalářská práce opírá, patří zákon o kybernetické bezpečnosti včetně prováděcí vyhlášky, rodina standardů ISO 27000, standardy NERC–CIP a v neposlední řadě standard ISA99 / IEC 62443. Stěžejní částí pro výrobce smart metrů je zákon o kybernetické bezpečnosti, jelikož splnění informační bezpečnosti je zákonnou povinností. Zároveň práce popisuje dostupné skenery zranitelností a jejich vlastnosti.

Praktická část je zaměřená na samotné testování dvou systémů smart metrů. Zejména pak na hledání nedostatků v zabezpečení, které je potřeba eliminovat před nasazením do provozu tak, aby bylo vyhověno normám popsaným v teoretické části a ztížili tak útočníkovi možnost kompromitovat systém. Testování je zaměřeno na bezpečnost síťových komponentů z pohledu síťové vrstvy a vyšších vrstev a nepojednává tedy o hardwarové části smart metru.

V části, kde je testován první typ smart metru je pouze obecná charakteristika, jelikož práce s tímto zařízením spadají pod Non-disclosure agreement a nelze tak uveřejňovat informace, které by mohly vést k identifikaci typu zařízení.

Závěrem jsou shrnuty výstupy z teoretické a praktické části bakalářské práce, společně s dalšími možnými cíli a rozšířením práce.

1 Definice a typy smart metrů

1.1 Definice

Jako smart metr byl původně označován elektroměr, který má možnost komunikace se zařízením pro svou vlastní správu. Hlavním benefitem je možnost dálkového odečtu, neboli odesílání dat o spotřebované elektrické energie pro fakturaci a odhalení černých odběrů. S tímto původním termínem budu pracovat.

V dnešní době je termín smart metr využíván pro zařízení, které měří určitou analogovou nebo digitální veličinu a mají možnost odesílat tato data nadřazenému systému. Komunikace musí být umožněna obousměrně. Momentálně lze tedy odečítat nejen stav elektrické energie, ale všechny možné veličiny, které lze uplatnit pro správu majetku. Jedná se například o stav vody, plynu a dalších.

Smart metry můžeme rozdělit do několika skupin podle technologie, se kterou komunikují, nebo podle počtu fází.

1.2 Dělení podle počtu fází

1.2.1 Jednofázové

Jednofázový smart metr měří okruh na jedné fázi. Tyto elektroměry nejsou standardně dodávány distributory elektrické energie, ale jsou nasazovány pro koncové uživatele, kteří chtějí mít přehled nad spotřebou energie v jednotlivých větvích své sítě. Další využití se nabízí v podobě samostatného okruhu pro nabíjení elektromobilů[1].

1.2.2 Třífázové

Tento typ smart metru je dodáván distributory elektrické energie pro vzdálenou správu a odečet. Slouží jako centrální prvek pro vstup elektrické sítě do domácnosti.

Elektroměr lze pořídit i vlastní za účelem kontroly energie uvnitř vlastní sítě. Například uvnitř továrny pro jednotlivé stroje a následnou fakturaci nákladů oddělením.

[1] Elektromobily mají možnost nabíjení i pomocí třífázového napětí.

1.3 Dělení podle přenosové technologie

1.3.1 PLC

PLC neboli Power Line Communication slouží pro přenos dat infrastukturou elektrického vedení. Elektroměry komunikují s lokálním centrálním prvkem (koncentrátorem), který je připojen pomocí jiné technologie do datové sítě, kde odesílá data za všechny smart metry dohromady.

1.3.2 Bezdrátový přenos

Přenos dat je realizován nejčastěji pomocí LPWAN (Low-Power Wide-Area Network). Mezi LPWAN sítě patří Sigfox, LoRa, Narrowband IoT. Tento typ sítě byl vytvořen pro IoT (Internet of Things) a má tyto charakteristické vlastnosti:

1. Nízký příkon vysílacího/příjímacího zařízení.
2. Dlouhá výdrž baterie.
3. Malá šířka pásma.
4. Omezený počet zpráv za den.

Ostatní datové sítě jsou vytvářeny pro objemný provoz v každé vteřině. Zařízení jako smart metr neklade tak velké nároky na přenos dat a stačí mu pár zpráv za den o malé velikosti. Využívání současných mobilních sítí by bylo neefektivní. Pro řešení tohoto problému byly vytvořeny právě LPWAN sítě.

1.3.3 Vlastní kabelové spojení

Poslední možností pro datové spojení je dovedení samostatného připojení přímo do smart metru, který obsahuje rozhraní uzpůsobené pro připojení. Příkladem může být připojení kroucené dvojlinky technologií xDSL k smart metru, který obsahuje modem pro kódování dat.

2 Aspekty bezpečnosti smart metru

U návrhu informačních systémů se smart metrem dochází k více bezpečnostním problémům. U „obyčejného“ elektroměru jediná možnost kontroly je při fyzickém kontaktu s elektroměrem a hlavní důraz je pouze na fyzické zabezpečení. Smart metry přináší nové bezpečnostní hrozby, se kterými si výrobce musí při implementaci poradit.

2.1 Fyzické zabezpečení

Jak pro klasický elektroměr (bez možnosti elektronické komunikace), tak pro smart metr je společné fyzické zabezpečení rozvaděče potažmo i samotného elektroměru. Nedostatečné fyzické zabezpečení dává možnost připojení domácnosti na černý odběr a elektroměr v podstatě ztrácí svůj význam.

Některé dnešní elektroměry, které zatím nedokáží komunikovat na delší vzdálenosti, již obsahují vlastní sériový port pro konfiguraci. Přístup k tomuto rozhraní by neměl být jednoduchý a pro autentizaci uživatele je vhodné nastavit dostatečně silné heslo[1].

2.2 Dostupnost služby

Při dálkovém odečtu je důležité, aby spojení mezi elektroměrem a systémem pro odečet nebylo závislé na kvalitě spojení a odeslaná zpráva byla i doručena. U smart meterů se nejedná o velké objemy dat (maximálně kB). Odeslání dat se provádí většinou jednou denně, a proto je důležité, aby byl implementován mechanismus pro zaručení doručení zprávy.

2.3 Autentičnost

Autentičností rozumíme stav, kdy aktiva IS (Informační systém) (tj. data, služby software, hardware) nebyla neoprávněně modifikována [1]. Komunikace mezi smart metrem a nadřazeným systémem nemohou být při přenosu přes nedůvěryhodný kanál změněna. Stejné pravidlo platí i pro opačný směr.

Pro zaručení autentičnosti se může využívat HMAC (Hash-based Message Authentication Code), popřípadě elektronický podpis. U obou algoritmů je využívána hashovací funkce, která bude podrobně probrána v kapitole 4.5.1.

[1] Existují seznamy uniklých hesel například: https://haveibeenpwned.com/Passwords.

2.4 Důvěrnost

Komunikace je důvěrná v případě, kdy k obsahu zprávy mají přístup pouze subjekty předem určené [1]. K dosažení důvěrnosti se využívá šifrování. Aplikovaní slabých nebo překonaných algoritmů šifrování nedává komunikaci dostatečnou důvěrnost. U informace šifrované překonaným šifrovacím algoritmem informace ztrácí na důvěrnosti a tím pádem je šifrování zbytečné.

Mezi překonané šifrovací algoritmy patří například DES (Data Encryption Standard). Pro zařízení s nižším výkonem může mít používání dostatečně silné šifry za následek značné zpomalení, proto vznikají nové šifry speciálně pro zařízení s procesorem s nižším výkonem. Jednou z takových je Adiantum, která byla vyvinuta společností Google pro operační systém Android [2]. Výrobce smart metru by měl uvážit možnost, že některé vzniklé šifry budou později odbornou veřejností prohlášeny za nedostatečné (šifra Speck). Nejlepší variantou zůstává využívání AES (Advanced Encryption Standard), jelikož smart metr si zpomalení v důsledku šifrování může dovolit (komunikace neprobíhá každou vteřinu).

3 Zákon o kybernetické bezpečnosti

Pro zajištění kybernetické bezpečnosti existují dva modely. První možností je taková kombinace technických a organizačních opatření, která ve výsledku zajistí identifikaci subjektu, jež způsobil kybernetický bezpečností incident. Tento model vyžaduje velký zásah do soukromí uživatelů. Je využíván v právních řádech států Jižní Ameriky. Mezi velké nedostatky patří i nutná mezinárodní spolupráce při identifikaci subjektů. [3]

Druhý model se snaží nezasahovat do soukromí subjektů[1], proto vytváří bezpečné kybernetické prostředí pomocí technických a organizačních nástrojů. Pro implementaci regulace není tak podstatná spolupráce na mezinárodní úrovni, avšak tato koncepce se uplatňuje napříč Evropou, kde Česká republika byla jedna z prvních, která legislativní implementaci provedla.[3]

3.1 Definice

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů upravuje práva a povinnosti pro kybernetický prostor, který sám vymezuje. Zákonu podléhá vše, co vytváří, zpracovává nebo umožňuje přenos dat v digitálním prostředí, mezi které smart metr spadá.

Podle §2 písmene i) se smart metr stává důležitý pro takzvanou základní službu, jejíž narušení může mít dopad v oblastech:

1. **energetiky**
2. dopravy,
3. bankovnictví,
4. infrastruktury finančních trhů,
5. zdravotnictví,
6. vodního hospodářství,
7. digitální infrastruktury,
8. chemického průmyslu.[4]

Pojem základní služba zavádí směrnice Evropského parlamentu ES (Evropská směrnice) č. 2016/1148, tzv. NIS (Network and Information System) směrnice. Česká implementace zákona rozšiřuje definici i o pojem kritická informační infrastruktura, kde síť[2] je důležitá pro národní bezpečnost, a proto se pojí na tento subjekt vyšší bezpečnostní nároky. Zůstává pak otázkou, jestli smart metr svým provedením může být bezpečností riziko pro celou síť nebo jen pro jednotlivé subjekty (koncové spotřebitele) v případě převzetí správy nad větším počtem zařízení.

[1] V porovnání s prvním modelem.

[2] Informační nebo komunikační síť.

Pokud páteřní elektrická síť není závislá na informačním systému s využitím smart metrů, tak se na smart metr nemusí uplatňovat vyšší bezpečnostní nároky, protože neohrožuje fungování základní služby. Příklad v části 3.5.

3.2 Bezpečnostní opatření

Podle zákona o kybernetické bezpečnosti je definován požadavek na zvolení povinných osob. Tyto osoby určí standard příslušných systémů nebo sítí formou organizačních nebo technických opatření [3]. Prováděné opatření se vztahuje na subjekty, které jsou povinné implementovat opatření do svého systému. Zákon rozlišuje provozovatele a správce systému, kde správce má systém nebo síť pod kontrolou na základě požadavku provozovatele.

3.2.1 Technické opatření

Zákon vyjmenovává několik prostředků na dosažení technických opatření, avšak nedává každému stejnou váhu a některé rozebírá do detailu, zatímco o některých pojednává všeobecně. Základním technickým opatřením je fyzická bezpečnost popsaná v kapitole 4.3. Dalšími opatřeními jsou například nástroje pro ochranu integrity komunikačních sítí, řízení přístupových oprávnění, ochrana před škodlivým kódem, či ověřování identity uživatelů.

3.2.2 Organizační opatření

Organizační opatření představují zavedení a řízení systému bezpečnosti informací. Příkladem může být správa rolí a funkcí v systému a administrativních záležitostí, týkající se udělování přístupu uživatelům k systému a druhu přístupu k systému (autorizace uživatele). Z formálního hlediska můžou být organizační opatření rozdělena na: řízení rizik, bezpečností politika, řízení aktiv, bezpečnost lidských zdrojů.

3.2.3 Bezpečnostní událost a incident

Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací [4].

Druhým termínem definovaným zákonem je kybernetický bezpečností incident, kdy rozdíl mezi těmito dvěma pojmy je ten, že při kybernetické bezpečnostní události nemusela být ohrožena bezpečnost systému, avšak u incidentu k narušení bezpečnosti systému reálně došlo.

Systém musí mít implementovány mechanismy pro detekci kybernetických událostí a incidentů. V případě jakéhokoliv bezpečnostního incidentu v síti provozující základní službu je provozovatel povinen neodkladně oznámit tuto skutečnost Úřadu pro kybernetickou bezpečnost. Úřad může na incident reagovat například vydáním varování, kdy je ostatním provozovatelům oznámeno zjištění o hrozícím narušení integrity důvěrnosti a dostupnosti dat.

3.3 Určení provozovatele základní služby

Doposud jsme používali termín základní služba, která je popsána v kapitole 3.1. Pojem základní služba neoznačuje všechny možné základní služby spadající do osmi subkategorií dle §2 písmene i) zákona 181/2014 Sb., ale pouze ty, jejíž fungování je závislé na informačních systémech nebo sítích.[3] Určení, kdo je povinen svůj systém ochránit, jak stanoví zákon pro základní službu, určuje Úřad pro kybernetickou bezpečnost na základě parametrů dopadu bezpečnostního incidentu. Základní služba se vztahuje na:

1. rozsah a kvalitu služby uživatelům, kteří jsou na ni závislí,
2. ekonomické a společenské činnosti a veřejnou bezpečnost,
3. vzájemnou závislost v odvětvích uvedených v kapitole 3.1.

V případě zjištění, že systém provozovatele má závažné nedostatky spojené s kybernetickým bezpečnostním incidentem, může úřad zakázat kontrolovanému subjektu používání tohoto systému, což může mít za následek i přerušení činnosti v odvětví, ve kterém se pohybuje. Toto je poslední krok, kterému předchází možnost pokuty za přestupky vyplývající z neplnění povinností tohoto zákona. Rozsah peněžité sankce je od 10 000 Kč až do 5 000 000 Kč. Samotnou sankci uděluje Národní úřad pro kybernetickou bezpečnost.

3.4 Prováděcí vyhláška

Zákon stanoví, že přesnější ustanovení týkající se bezpečnostních opatření bude upraveno prováděcí vyhláškou č. 82/2018 Sb. čímž se odstraní a doplní nedostatky vyhlášky č. 316/2014 Sb.

3.5 Aplikace zákona na smart metr

Podle definice kybernetického zákona implementace smart metru spadá pod základní službu. Samotný smart metr musí komunikovat nejen data vyplývající z provozu elektrické sítě, ale i data pro hlášení kybernetických událostí a incidentů nadřazenému

systému. Distributor elektrické energie musí mít organizačně definované subjekty, kteří mají pravomoc provádět vzdálenou správu smart metru.

Pro představu může nastat situace, kdy smart metr bude dodáván běžně ke spotřebitelům jako hlavní elektroměr pro fakturaci spotřebované energie v objektu. Komunikace mezi nadřazeným systémem a smart metrem je obousměrná a může se využívat pro vypnutí přívodu elektrické energie do objektu v případě nezaplacených účtů. Sám elektroměr obsahuje relé (popřípadě stykač), kterým přívod energie může řídit. V případě zneužití funkce útočníkem může být distribuční síť ochromena, pokud útočník převezme správu několika zařízení. V takovém případě není poškozena samotná páteřní síť, jako při výpadku vysokého napětí, ale důsledky jsou stejné. Na problém zneužití smart metru útočníkem, popřípadě správcem sítě, poukazuje článek s názvem „*Smart meters: can energy suppliers (or hackers) turn off my supply remotely?*“, jejímž autem je Sam Meadows [3].

Smart metr může být zajímavý pro útočníky nejenom jako nástroj pro ovládání elektrické energie, ale i jako prerekvizita k jinému útoku. V dnešní době jsou chytrá zařízení častým terčem útoků, kdy přihlašovací údaje jsou následně prodávány na internetu za několik dolarů. Důvod, proč útočníci pro svůj útok potřebují přihlašovací údaje, může být ten, že chytrá zařízení využijí jako botnet, přes který je samotný útok prováděn [5]. Použití české IP adresy pro útok v rámci České republiky je méně nápadné než využít IP adresu poskytovatele z Ruska.

[3] https://www.telegraph.co.uk/money/ask-a-money-expert/smart-meters-can-energy-suppliers-hackers-turn-supply-remotely/.

4 Prováděcí vyhláška k zákonu o kybernetické bezpečnosti

Samotný zákon je obecný a nemá specifikace v oblasti technických ani organizačních opatření. Dále neřeší role ve společnosti, která zákon implementuje. Původní a upravující tento stav byla vyhláška č. 316/2014 Sb., v roce 2018 jí nahradila nová prováděcí vyhláška č. 82/2018 Sb.

Hlavním důvodem vzniku nové vyhlášky je směrnice Evropského parlamentu a Rady EU 2016/1146. Vyhláška z roku 2018 již harmonizuje směrnici do našeho právního řádu.

4.1 Úvod

Vyhláškou se řídí všechny společnosti, které splňují kritéria vyhlášky a které provozují informační systém základní služby. Upravuje strukturu bezpečnostní dokumentace, hlášení bezpečnostních incidentů, rozsah a způsob bezpečnostních opatření a nebo i způsob likvidace dat.

Dále důležitým pojmem je primární aktivum, což je podle vyhlášky služba, kterou poskytuje informační systém. Pro systém využívající smart metr by primární aktivum byla služba distribuce elektrické energie. Samotný smart metr je pak technickým aktivem, kdy jeho selhání má dopad na systém z pohledu uživatele (zákazníka).

4.2 Organizační opatření

Organizační opatření nekladou tak velké nároky na výrobce smart metru, a z toho důvodu je tato část důležitá pro distributora elektrické energie. Organizace si zvolí povinnou osobu pro řízení bezpečnosti informací. Tato osoba má za povinnost:

1. stanovit cíle systému,
2. vytvářet bezpečností politiku,
3. zajistit provádění auditu kybernetické bezpečnosti,
4. řídit provoz bezpečnostních opatření.

Pověřená osoba stanoví metodiku, se kterou ohodnotí aktiva společnosti. Navrhne jakým způsobem se aktiva budou chránit, pravidla pro bezpečné sdílení a likvidaci dat. Pro naše zadání by aktivem mohly být údaje o spotřebě pro daného koncového uživatele nebo i další provozní údaje vzniklé na základě měření smart metru.

Dále pověřená osoba má povinnost nasazení bezpečností politiky pro správu zařízení a pro přístup k datům. Při porušení vzniklých politik musejí být implementovány mechanismy, které pokus ohlásí. V případě, že se jedná o bezpečnostní incident, pověřená osoba nahlásí incident Národnímu úřadu pro kybernetickou bezpečnost (NÚKIB).

Pověřená osoba postupuje podobně při určování důležitosti primárních aktiv. Pro systém se smart metrem jsou důležité pasáže, kdy bezpečnostní incident může ohrozit poskytování důležitých služeb, narušení běžné činnosti, nebo má dopad na bezpečnost a zdraví osob. Proto je třeba stanovit kritéria akceptovatelnosti zranitelností. Má 4 kategorie:

1. nízká
2. střední
3. vysoká
4. kritická.

Takto rozklíčované zranitelnosti je potřeba využít k opravě a předejít kybernetickým incidentům. Samotný úkon stanovení si zranitelností a rizik by měl probíhat jednou ročně.

4.3 Fyzická bezpečnost

Osoba povinná dle zákona musí zajistit, že po instalaci smart metru nebude možné elektroměr odcizit,poškodit nebo modifikovat. Není tedy možné instalovat smart metr do rozvaděče, který nemá možnost uzamčení. V dnešní době nejsou elektroměry zamykány pomocí individuálního klíče, ale pouze pomocí univerzální kličky, což pro znění zákona nemusí být dostatečné.

4.4 Důvěrnost

Důležitým opatřením je zabezpečení komunikace zařízením, kdy vyhláška stanovuje použití nepřekonaných kryptografických prostředků pro zajištění důvěrnosti dat, a to jak při přenosu dat, které smart metr odesílá pravidelně, tak pro vzdálený přístup. Zároveň má zařízení povinnost blokovat nežádoucí komunikaci.

V praxi to znamená, že pro odesílání dat a správu zařízení není možné využívat překonaných šifrovacích algoritmů pro zajištění důvěrnosti. Příkladem překonaného šifrovacího algoritmu je DES (Data Encryption Standard). Příkladem nepřekonaného algoritmu je AES (Advanced Encryption Standard), a to nejlépe pokud není použit mód ECB (Electronic Codebook), kdy je každý blok šifrován stejným nezměněným klíčem.[6]

Výhodnější je využití například módu PCBC (Propagating Cipher Block Chaining). U toho módu se před každým šifrováním bloku provádí `XOR` (Exclusive OR) s blokem předešlým před šifrováním a blokem předešlým po šifrování. U prvního bloku se využívá operace `XOR` s inicializačním vektorem.[7]

Inicializační vektor je náhodný řetězec přidávaný k prvnímu bloku šifrovaných dat, aby se docílilo větší náhodnosti výsledného zašifrovaného bloku. Vzniklá náhodnost se šíří i dalšími bloky a pro útočníka je dešifrování obtížnější.

Výrobce smart metru musí počítat s tímto zněním vyhlášky a při výběru aplikačního protokolu implementovat takový, který využívá nepřekonané šifrovací algoritmy, dále smart metr musí obsahovat firewall, kde bude moci koncový uživatel navolit svoje pravidla pro filtraci provozu.

4.5 Autentizace

Před zahájením aktivity spojené se správou smart metru je potřeba ověřit uživatele. Při ověřování uživatele by měl být smart metr podle vyhlášky odolný proti neoprávněnému odcizení přihlašovacích údajů. Pro výrobce smart metru to znamená, že přihlašovací údaje by neměly být uloženy ve smart metru v souboru běžně přístupném, a pokud jsou přihlašovací údaje přenášeny, měla by být vyžadována důvěrnost popsaná v kapitole 4.4.

Autentizační údaje jsou ukládány ve formě odolné proti offline útokům [8]. Tato věta z vyhlášky znamená, že autentizační údaje, zejména hesla, nelze ukládat ve formátu, kdy je lehké heslo získat, neboli heslo nelze ukládat jako prostý text. Pro ukládání hesel je potřeba využívat hashovací funkce a výsledné řetězce ukládat do souborů, ke kterým by útočník neměl mít přístup.

4.5.1 Hashovací funkce

Hashovací funkce je algoritmus, který z libovolně dlouhého řetězce vytvoří řetezec konstantní délky pomocí vnitřních pravidel funkce. Pro hashovací funkce je důležitá určitá náhodnost, jednocestnost a bezkoliznost. Náhodností se myslí stav, kdy malá změna na vstupu se projeví jako velká změna po provedení hashovací funkce. Výstup bývá označován jako hash nebo otisk. Jednocestnost znamená, že při získání výsledku hashovací funkce nelze na základě otisku získat zpětně původní řetězec. Příklad je zobrazen na obrázku 4.1a.

U těchto algoritmů je na začátku proměnlivý řetězec a výsledkem je řetězec konstantní délky. Je logické, že určité dva prvky, které jsou na počátku rozdílné, tak po provedení hashovací funkce mají stejný výsledek. Pro bezkoliznost platí,

(a) Znázornění jednocestnosti.

(b) Znázornění kolize.

Obr. 4.1: Znázornění jednocestnosti a kolize u hashovacích funkcí.

že nelze záměrně generovat dva prvky, které by měly výsledný otisk stejný. Příklad obrázek 4.1b. Takto záměrně lze generovat kolize u hashovací funkce SHA1 (Secure Hash Algorithm 1). Na webové stránce https://shattered.io/ lze zjistit, zda k Vámi vybranému souboru neexistuje kolize s dokumentem úplně jiným.

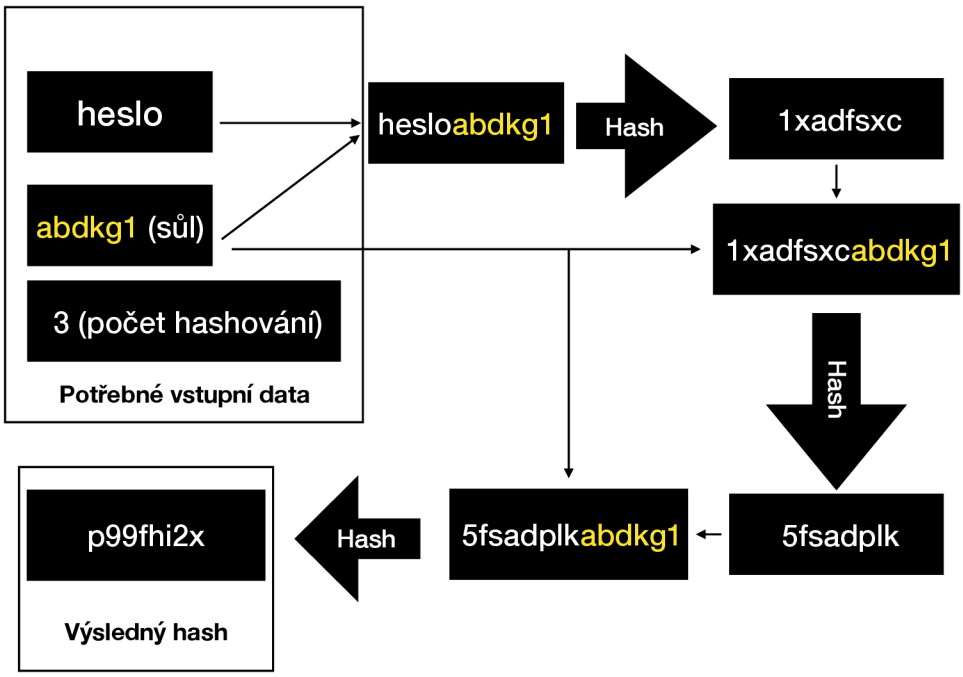
Pro ukládání hesel je lepší využít hashovací funkce, u kterých není možné využít výše popsaných slabin jako je například SHA512[1] nebo Argon2, která byla vytvořena pro ukládání hesel, jelikož je odolná proti útokům rainbow table. A to díky tomu, že v rámci svého algoritmu využívají solení hesel. Sůl je krátký, náhodně vygenerovaný textový řetězec, který se přidává k heslu, aby dvě stejná hesla neměla stejný výsledný otisk. Náročnost výpočtu hashe Argon2i (verze Argon2) lze ovlivnit nastavením následujících parametrů: počet vláken, časovou náročnost, pamět pro výpočet [9].

Dosažení odolnosti SHA512 proti útokům rainbow table lze docílit pomocí solení hesel před hashováním, opakovaným hashováním výstupu z funkce, nebo kombinací soli a počtem opakování hashování.

Příklad použití kombinace soli a počtu opakování je zobrazen na obrázku 4.2. Počet opakování a sůl byla vygenerována při vytváření hesla a tyto parametry jsou uloženy s výsledným hashem. Při přihlašování uživatele je proces proveden s heslem, které zadal a výsledek se porovná se záznamem uloženým pro daného uživatele, pokud se hashe rovnají, uživatel je autentizován.

Dostáváme se otázce, jak kvalitní ukládání hesel měl zákonodárce na mysli, když vytvářel vyhlášku. Pro splnění zmíněného paragrafu stačí využít kteroukoliv hashovací funkci, která doposud nebyla překonána z hlediska délky výsledného ře-

[1]Secure Hash Algorithms s výsledným otiskem dlouhým 512 bitů, ve standartu označováno jako SHA2.



Obr. 4.2: Znázornění hashování při použití soli a iterací.

tězce, jednocestnosti, nebo generování kolizí. Využití dalších mechanismů, jako je o solení a opakované hashování, z vyhlášky nevyplývá jako povinné.

4.5.2 Bezpečnostní nároky na hesla

Samotná vyhláška klade nároky na hesla používaná pro autentizaci. Pro autentizaci administrátorů se má využívat vícefaktorová autentizace s nejméně dvěma typy. Pokud to situace neumožňuje, má se dočasně používat autentizace pomocí kryptografických klíčů.

Pro vzdálenou správu smart metru pomocí dostupných aplikačních protokolů by se měly vybírat takové, které umožňují autentizaci pomocí kryptografických klíčů. Mezi takové patří například SSH (Secure Shell).

Pro uživatele jsou pak kladeny zejména nároky na hesla v případě, že kryptografické klíče nemohou být použity, nebo ještě nebyly implementovány. Nároky jsou dvojího typu v závislosti, zda se jedná o administrátora nebo „obyčejného“ uživatele.

Rozdíl je v délce hesla. Ostatní parametry jsou stejné. Pro administrátory platí pravidlo minimálně 17 znaků, u uživatelů 12 znaků. Heslo nemá omezení v počtu malých písmen, velkých písmen a speciálních znaků. Samotné zařízení musí umožnit

zadání hesla o délce minimálně 64 znaků a zamezit změny hesla v době 30 minut od poslední změny.

Při změně hesla musí zařízení zamezit volbu nejčastěji používaných hesel, a to i ty, kde se opakovaně opakuje jméno uživatele, e-mail nebo jméno systému. Změna by měla být povolena také, pokud heslo již bylo využíváno v posledních 12 heslech. Samotné zařízení by mělo vynucovat změnu hesla maximálně po 18 měsících.

V případě, že bylo vygenerováno heslo k obnovení přístupu, má uživatel možnost jej zadat pouze jednou do 60 minut po vygenerování a po autentizaci je vyzván ke změně hesla [8].

Pro výrobce smart metru to znamená, že tato pravidla musí implementovat do operačního systému, aby nemohla být eliminována a bylo zajištěno splnění podmínek vyhlášky.

4.6 Zaznamenávání událostí

Pokud je přistupováno k zařízení vzdáleně, musí být původce identifikován a záznam o aktivitě uložen. Záznam události musí obsahovat:

1. datum a čas,
2. typ činnosti,
3. účet, pod kterým byla akce prováděna,
4. identifikátor původce v komunikační síti,
5. výsledek úspěšnosti nebo neúspěšnosti úkonu.

Takto stanovený záznam je potřeba uložit vždy, když se přihlašuje a odhlašuje uživatel, když je prováděn jakýkoliv úkon administrátorem, odmítnutí akce z důvodu nedostatečných práv uživatele, pokus o manipulaci se záznamy nebo například chybové hlášení zařízení. Záznamy musí být synchronizovány alespoň každých 24 hodin se systémem, který události zaznamenává. Samotné záznamy se musí uchovat nejméně 18 měsíců.[8]

Jednou denně se musí přenést záznamy o událostech. Samotný smart metr dává možnost uchovávat záznamy alespoň 18 měsíců, v případě, že není využit externí logovací server.

4.7 Penetrační testování

Penetrační testování systému, v našem případě celého zařízení, je prováděno povinně před uvedením do provozu. Testování důležité pro o ochranu aplikací před neoprávněnou činností v systému. Test je prováděn také při významné změně v systému, kterou určí odpovědná osoba pro implementaci zákona.[8]

5 Rodina norem ISO/IEC 27000

Rodina standardů ISO/IEC (International organization for standardization/Internatinal electrotechnical commission) 27000 je neznámějším standardem, který poskytuje požadavky na systém řízení bezpečnosti informací, známý jako ISMS (Information security management system). ISMS je systém řízení informačních rizik, který zahrnuje bezpečnost lidských zdrojů, informačních systémů, efektivitu investic do bezpečnosti a jiné. Standard společně vydali a zastřešují organizace ISO (International organization for standardization), IEC (Internatinal electrotechnical commission).[10]

V rámci standardu bylo publikováno více norem s označením 27XXX, kdy každá část pojednává o jiném tématu v poskytování ISMS. Označení XXX přestavuje číslo jednotlivých norem z rodiny ISO/IEC 27000. Základní normou je ISO/IEC 27000, která uvádí přehled do problematiky a terminologie. Nejzmámější normou je ISO/IEC 27001, na kterou navazuje ISO/IEC 27002.

Zákon o kybernetické bezpečnosti vychází právě z tohoto standardu a přesně nedefinuje, jaké mechanismy se mají využít k dosažení zabezpečeného systému. Společnosti, které se musí řídit zákonem o kybernetické bezpečnosti, se často ucházejí o certifikaci ISO/IEC 27000. Zejména se chtějí vyhnout sankcím vyplývající z nedodržení zákona. Certifikace jim dává jistotu, že zákon implementovali do svého systému správně.

5.1 ISO/IEC 27001

Norma obsahuje výčet všech bodů, které musí organizace splnit k tomu, aby získala certifikaci. Forma dokumentace není specifikována – může to být interní webová stránka nebo může mít tištěnou i jinou podobu [11]. Obsahuje:

- výčet aktiv, spadající pod ISMS,
- nastavení politiky informační bezpečnosti,
- proces posuzování informačních rizik,
- proces nakládání s informačními riziky,
- výčet objektů zaručující informační bezpečnost,
- seznam kompetentních osob zaměřených na informační bezpečnost,
- ostatní dokumenty spojené s ISMS, které jsou potřebné pro společnost,
- dokumentace plánu a kontrol provozuschopnosti,
- výsledek posouzení informačních rizik,
- rozhodnutí týkající se nakládání s informačními riziky,
- evidence kontroly a měření informační bezpečnosti,
- interní ISMS audit a výsledky provedeného auditu,

- evidence ohodnocení vrcholového managementu ISMS,
- evidence zjištěných nedostatků a jejich náprava,
- implementace dalších nepovinných doporučení.

5.2 ISO/IEC 27002

Zatímco norma ISO/IEC 27001 je technicky neutrální, norma ISO/IEC poskytuje manuál bezpečného chování pro zajištění všech bodů z ISO/IEC 27001. ISO/IEC 27002 obsahuje usměrnění a doporučení postupů, které zajistí splnění požadavků na certifikaci. Prakticky je druhou částí ISO/IEC 27001. „Může být využita jako kontrolní seznam všeho správného, co je nutno pro bezpečnost informací v organizaci udělat.“[12]

Norma se tematicky dělí na 3 části: fyzické zabezpečení společně s informačním zabezpečením zdrojů, bezpečnost lidských zdrojů a řízení přístupu. Například uvádí, že pro dosažení autentizace a integrity dat se má využívat kryptografických prostředků. Jelikož poslední usměrnění normy vyšlo v roce 2015, je lepší využívat doporučení NÚKIB (Národní úřad pro kybernetickou a informační bezpečnost), kdy poslední verze je z podzimu 2018 a uvádí doporučené šifrovací algoritmy a minimální požadavky pro klíče.

Informační bezpečnost lidských zdrojů se vztahuje na všechny zaměstnance, a to i externí, jako jsou i dodavatelé. Tato opatření se musí zohlednit již před nástupem do zaměstnání, například jako dohody a povinnosti v oblasti bezpečnosti. Při ukončení zaměstnanecké smlouvy je potřeba vrátit informace a zařízení společnosti včetně přístupových práv. Vedoucí pracovníci jsou povinni informovat zaměstnance a dodavatele o povinnostech vztahujících se k informační bezpečnosti.

Poslední položkou je řízení přístupu, kde jsou definovány nároky na hesla a formát ukládání hesel. Stejně jako u kryptografických algoritmů, je dobré využívat hashovací funkce doporučené NÚKIB. Dále například definuje, jaká externí zařízení mohou být využívána uvnitř společnosti.[13]

5.3 ISO/IEC 27030

S nástupem IoT (Internet of Things) se vážou nová bezpečnostní rizika. Smart metr mezi zařízení IoT spadá. Aktuálně je vyčleněna norma ISO/IEC 27030, která se začala standardizovat v roce 2018 a je určena k zajištění informační bezpečnosti na zařízení označovaná jako IoT. Předpokládá se, že doba standardizace bude zhruba 4 roky. Společnost využívající chytré elektroměry, musí pamatovat na to, že po dokončení standardu bude muset elektroměr daný standard splňovat.[14]

6 NERC – CIP

NERC (North American Electric Reliability Corporation) je americká nezisková organizace, která se stará o bezpečnost elektrické rozvodné sítě v celé Severní Americe. Organizace vytváří a vynucuje dodržování bezpečnostních norem. Mezi vydané normy patří CIP (Critical Infrastructure Protection). CIP je komplexní soubor pravidel, které zvyšují bezpečnost elektrické rozvodné sítě tím, že slouží k zabezpečení fyzické a informační bezpečnosti aktiv. Stejně jako u norem již zmíněných je CIP založen na hierarchickém uspořádání aktiv a následném plánu zvládání rizik. Povinným subjektem je každý subjekt, který je identifikovaný společností NERC a vlastní nebo má ve správě část severoamerické elektrické sítě [15].

6.1 CIP standardy

První verze norem byla vydána v roce 2008, avšak aktuální je verze číslo 5. Předcházející verze NERC – CIP se zaobírá definováním a vymezením kritických aktiv, nejnovější verze je již hlavně změřena na komunikační zařízení. Verze 5 přináší vyšší důraz na informovanost zaměstnanců o informační bezpečnosti v organizacích a zvýšenou fyzickou bezpečnost než starší verze. Současná verze obsahuje 14 hlavních standardů. Standardy jsou označovány CIP-0XX, kde XX je konkrétní číselné označení normy [16].

- CIP-001 – Standard popisuje povinnost hlášení neobvyklých situací a incidentů.
- CIP-002 – Identifikace kritických informačních aktiv se změřením na ochranu elektrické rozvodné sítě.
- CIP-003 – Vymezení minimálních bezpečnostních mechanismů jako například určení pověřené osoby.
- CIP-004 – Řízení fyzického a elektronického přístupu ke kritickým aktivům.
- CIP-005 – Stanovení pravidel pro oddělení informační sítě pomocí firewallů.
- CIP-006 – Požadavky na fyzickou bezpečnost zahrnující monitorování vstupů a poplachů.
- CIP-007 – Standard pojednává o testování, monitorování a revizi všech částí systému.
- CIP-008 – Povinné vypracování plánu a popisu zvládání rizik.
- CIP-009 – Vypracování plánu obnovy, který zahrnuje možné nehody a incidenty.

- CIP-010 – Dokumentace plánovaných změn, díky níž lze odhalit neoprávněné změny v systému.
- CIP-011 – Zabezpečení integrity, důvěrnosti a dostupnosti dat pomocí kryptografie.
- CIP-012 – Používání zabezpečených komunikačních kanálů.
- CIP-013 – Dokumentace služeb zajišťované externími subjekty.
- CIP-014 – Fyzické zabezpečení prostorů elektrické infrastruktury, například instalací kamer, oplocení a další.

6.2 Sankce

NERC vykonává pravidelné kontrolní audity povinných subjektů, a proto je důležité, aby subjekty vykonávaly interní audity, monitoring a testování. Audit je proveden do 30 dní po nahlášení od NERC a bývá minimálně jednou za tři roky. V případě, že povinné subjekty nedodrží NERC – CIP, mohou být sankcionovány, anebo mohou být provedeny jiná opatření proti proviněné společnosti. Sankce nejsou jednotné, protože NERC je nadnárodní organizace, a jednotlivé sankce jsou definovány na úrovni jednotlivých států.[17]

7 ISA99 / IEC 62443

ISA99 / IEC 62443 (The International Society of Automation / International Electrotechnical Commission) je mezinárodní standard pro implementování bezpečnosti v průmyslové automatizaci. Standard byl vytvořen Mezinárodní společností pro automatizaci (ISA) a Mezinárodní elektrotechnickou komisí (IEC). Nelze ale přistupovat k standardu tak, že byl vytvořen ve spolupráci obou společností, jelikož IEC se podílela pouze na uspořádání ISA dokumentů, jejich následného označení podle norem Mezinárodní elektrotechnické komise a současně převzala její další vývoj. Norma vychází z ISO/IEC 27000, ale je jasně zaměřená na bezpečností problematiku průmyslových řídících systémů. Hlavním cílem standardu je usměrnění provozovatelů sítí průmyslových systémů, a to prostřednictvím požadavků a kontrol. Struktura standardu ISA99 / IEC 62443 se skládá ze čtyř kategorií: Obecné, Pravidla a procedury, Systémové požadavky a Požadavky na komponenty. První dvě kategorie obsahují výklad terminologie, metriku bezpečnosti a komplexního managementu bezpečnosti, včetně podmínek provozu bezpečného systému a opravy chyb.[18]

7.1 Požadavky na systém a komponenty

Jádrem standardu jsou systémové požadavky a požadavky na komponenty. Systémové požadavky se zaměřují na návrh a úpravu sítě zajišťující chod průmyslové výroby. Popisují přehled stávajících technologií sloužících pro zabezpečení sítě, hodnocení bezpečnostních rizik a následný návrh zabezpečené sítě. Při návrhu sítě je doporučeno segmentovat části sítě do zón, které mají podobnou funkci, a pomocí řízení přístupu do takto vytvořených zón lze omezit výskyt a šíření hrozeb. Současně vymezuje podrobné technické požadavky na zabezpečení systému: těmi jsou autentizace, důvěrnost dat a integrita systému. Poslední kategorie se zabývá vývojem komponentu, jehož cílem je snížení výskytu bezpečnostních chyb v systému sloužícím pro průmyslovou výrobu. Specifikuje technické požadavky na zabezpečení jednotlivých komponentů.[19]

Pokud chtějí manažeři výroby splnit tyto dvě kategorie, musí postupovat podle 4 základních kroků. Prvním krokem je sběr dat, který slouží k plnění výrobního cyklu linky. Mezi taková data patří soupis majetku nebo data o tom, jak spolu zařízení komunikují. Dalším krokem je posouzení bezpečnosti sítě, která navazuje na sesbíraná data, a to jejich analýzou. Na základě analýzy se vypracuje plán zvládání rizik. Na základě rizik se vystaví priority při tvorbě sítě a následné segmentace sítě do zón. Posledním krokem je nasazení provedených změn do každodenních cyklů.[20]

8 Skenery zranitelností

Skenery zranitelností jsou programy, které mají za úkol najít chybu v testovém systému a dát tak ve svém výsledku zpětnou vazbu k tomu, aby byla opravena. Samotné testování může zahrnovat chyby v rámci operačního systému a síťového spojení, nebo jenom na část služeb, které stanice poskytuje. Typicky jsou to webové aplikace.

Skenery obsahují zranitelnosti obsažené v databázích zranitelnosti, kde každá zranitelnost má přiřazené skóre, které reprezentuje míru nebezpečnosti při zneužití. Mezi takové databáze patří CVE (Common Vulnerabilities and Exposures)[1]. Databáze je vlastněna organizací NIST (National Institute of Standarts and Technology). Do databáze přispívá veřejnost, a je proto každým dnem aktualizována. Pro zajištění informační bezpečnosti je nezbytné pravidelné skenování zranitelností s využitím aktuálních skenerů, jelikož novější verze obsahuje větší množství známých zranitelností.

8.1 Skenery služeb

Každý síťový sken bez bližších informací začíná vyhledáním otevřených TCP (Transmission Control Protocol) a UDP (User Datagram Protocol) portů, na kterých skenovaná stanice naslouchá. Pro zjištění pouze otevřených portů a základních veřejných informací existuje aplikace Nmap. Tato aplikace je součástí Linuxové distribuce Linux Kali. Aplikace je spouštěna z příkazového řádku, popřípadě existuje i grafická verze Zenmap. Postupně jsou testovány porty a porovnány s databází známých aplikací, které na tomto portu naslouchají. Někdy je výsledkem i verze aplikace, která provozuje službu na skenovaném zařízením. Pro další testování je nezbytné znát služby poskytované do veřejné sítě. Pro samotný sken je už potřeba souhlas majitele stanice, která bude testována.

8.2 Skenery webových aplikací

Samostatnou skupinou jsou skenery webových aplikací, kdy se testuje nejenom webový server jako služba, ale i samotná aplikace, která často slouží ke správě zařízení, popřípadě obsahuje citlivá data. Skenery pracují tak, že posílají HTTP (Hypertext Transfer Protocol) požadavky a zkoumají, zda odpověď ze strany webové aplikace je předvídatelná, nebo server odpověděl nestandardně. Každý programátor webové aplikace má vlastní postup, proto je potřeba prozkoumat, zda nezanechal

[1] https://cve.mitre.org/.

v aplikaci známou chybu. Společnost OWASP (About The Open Web Application Security Project) vydává seznam nejčastějších chyb webových aplikací.[2] Samotná společnost vydává také vlastní skener zranitelností webových aplikací OWASP ZAP, dostupný zdarma na operační systémy Linux, macOS i Windows.[3]

Další skener webových zranitelností je Vega vytvořená společností Subgraph[4]. Samotný program je otevřený kód a lze si jej nainstalovat na stejné operační systémy jako OWASP ZAP. Obě aplikace pracují velice podobně a není mezi nimi velký rozdíl. Při tvorbě webových aplikací se často využívá databáze. Při nesprávném naprogramování aplikace je možné komunikovat rovnou s databází, a to i na informace, které neměly být součástí dotazu. Chyba se označuje obecně jako SQL injekce [21]. Výše zmíněné skenery kontrolují aplikace proti této chybě. Existuje i aplikace zaměřující se pouze na SQL injekce – jmenuje se Sqlmap[5] a je součástí Linuxové distribuce Kali. Současně s ní lze zjistit, zda webová aplikace neobsahuje SQL injekci a dokáže tuto chybu využít a data z databáze získat. Pro spuštění je potřeba pouze adresa a parametry dotazu na webovou aplikaci.

8.3 Komplexní skenery

Komplexní skenery seskupují skenery popsané doposud do jedné aplikace. Nejčastěji sken zahájí zjistěním otevřených portů. Na základě toho pak testují zranitelnosti z dostupných databází, jako je například CVE. Pokud zjistí, že na daném portu naslouchá webová aplikace, provedou test webové aplikace. Samotný proces je automatický. Pro spuštění testu je potřeba pouze adresa testované stanice. Pokud se jedná o celou síť, tak potom adresu sítě. Nejznámější je Nessus od společnosti Tenable. Samotný software je licencován, lze si zakoupit licenci na 1 až 3 roky, kdy cena za jeden rok je okolo 66 500 Kč. Před pořízením licence lze využít týdenní verzi zdarma.

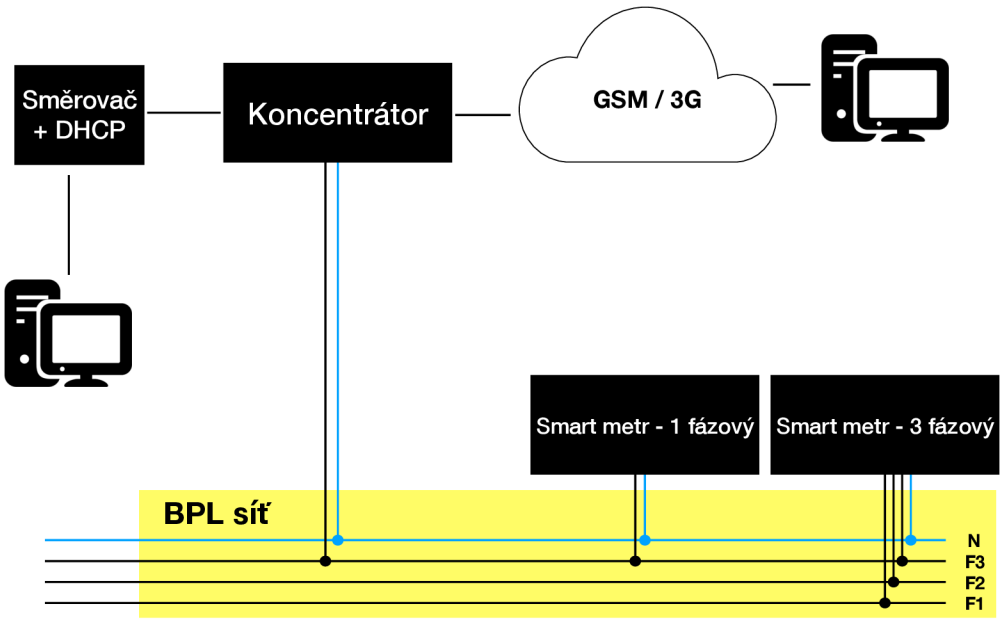
[2] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.
[3] https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
[4] https://subgraph.com/vega/
[5] http://sqlmap.org/

9 Testování v laboratoři

Pro vypracování praktické části bylo využito laboratoře na Ústavu telekomunikací. V rámci bakalářské práce jsou testovány smart metery od dvou výrobců. První je od výrobce, kterého budu v práci označovat jako Výrobce A, jelikož informace vedoucí k identifikaci typu výrobku podléhají Non-disclosure agreement. Druhý typ smart metrů je od výrobce ADD Group.

9.1 Výrobce A

Výrobce A využívá technologii BPL (Broadband over Power Lines) pro komunikaci mezi zařízeními. Pro připojení smart metru do komunikační sítě není potřeba zvláštního připojení, jelikož BPL je síť, která využívá stávající elektrické vedení pro zasílání elektronické komunikace [22]. Výrobce dodává smart metry pro měření spotřeby energie jedné fáze i tří fází. Aby bylo možné dostávat zprávy ze sítě BPL



Obr. 9.1: Zapojení sítě od výrobce číslo 1.

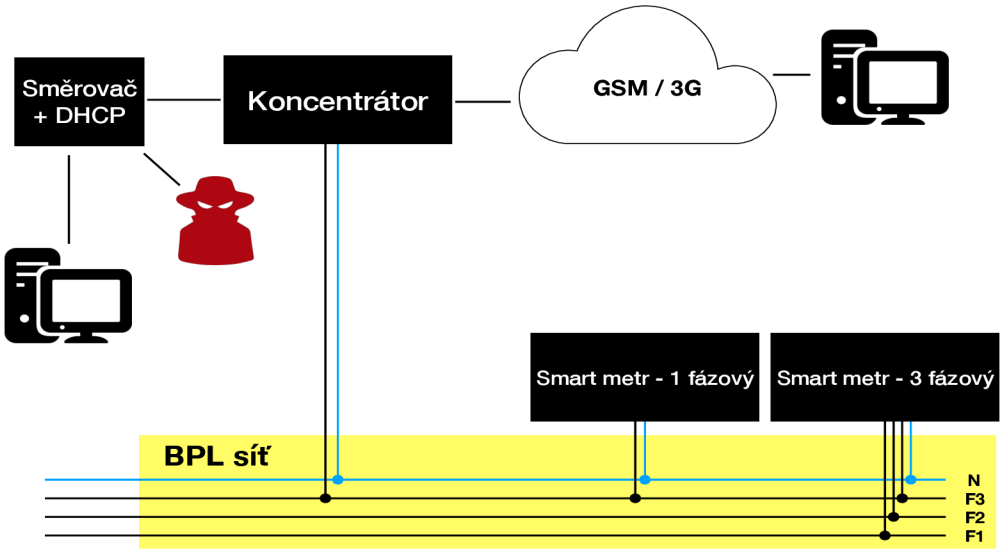
do sítě využívající jinou technologii, je potřeba mít součástí sítě koncentrátor od výrobce. Koncentrátor obsahující konektor SFP (Small Form factor Pluggable umožňuje spojení pomocí Ethernetu, popřípadě lze využít 3G mobilní síť, kterou podporuje po vložení SIM karty do slotu. Toto nejsou jediná rozhraní pro připojení ke

koncentrátoru. Dále obsahuje rozhraní RS232, RS485 a USB 2.0. Lze také využít BPL bránu, přes kterou lze pakety přeposílat do sítě BPL, tím lze vytvořit vlastní „koncentrátor“.

V laboratoři je vytvořena síť zobrazená na obrázku 9.1. Použití DHCP serveru není nutné a je možné využít ruční konfigurace IP adres. Samotný koncentrátor obsahuje webový portál pro správu a konfiguraci zařízení.

Samotný koncentrátor byl pro testování v laboratoři nastaven tak, aby veškerou komunikaci, která je směrována do sítě BPL, povolil a přeposlal požadavek. Pro testování tedy není potřeba BPL modem, jelikož lze takto využít samotný koncentrátor. Nastavení firewallu lze realizovat pomocí nástroje iptables. Při využití v reálném provozu je potřeba nadefinovat pravidla pro filtraci nežádoucího provozu. V laboratoři pro testování nebyla nastavena žádná pravidla a veškerý provoz byl povolen.

Pro testování systému Výrobce A existují dvě varianty, které může útočník využít. První možnost je zneužití zranitelnosti uvnitř BPL sítě. Druhá varinta je zneužití zranitelnosti koncentrátoru. Koncentrátor je vytvořen tak, aby byl dostupný z veřejné sítě a komunikace probíhala v ideálním případě pouze přes něj. Útočník může využít bezpečnostní zranitelnost koncentrátoru tak, že převezme správu nad celou BPL sítí. Další možností je odposlech komunikace, ke které by neměl mít útočník přístup. Útok z vnější sítě je zobrazen na obrázku 9.2. Pro splnění zákona a pro-



Obr. 9.2: Zobrazení útoku z veřejné sítě.

váděcí vyhlášky je potřeba zjistit, zda koncentrátor umožňuje blokaci nežádoucí komunikaci, která je do veřejné sítě šifrovaná a využívá nepřekonané algoritmy.

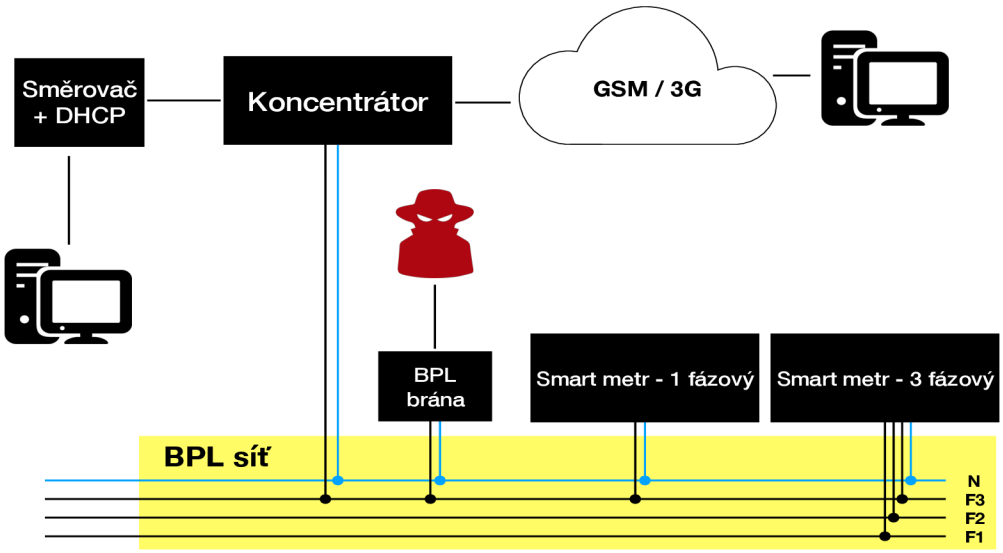
Koncentrátor v laboratoři je zároveň DHCP serverem pro BPL síť a pracuje jako NAT (Network address translation). Koncentrátor slouží jako perimetr mezi veřejnou částí sítě (internetem) a vnitřní BPL sítí. Při správné konfiguraci koncentrátoru je možné komunikaci filtrovat bez nutnosti přeposílání do sítě BPL.

Koncentrátor umožňuje i funkci síťového mostu. V takovém případě každý smart metr dostává přidělenou IP adresu z DHCP serveru mimo BPL síť a je tudíž dostupný i z veřejné sítě. Filtrování provozu tak zůstává na každém smart metru zvlášť.

9.1.1 Zneužití zranitelnosti uvnitř BPL sítě

Útočník disponující BPL bránou se může fyzicky připojit do BPL sítě a obejít koncentrátor. Situace je zobrazena na obrázku 9.3. Pro vnitřní síť platí podobné podmínky jako pro část veřejnou. Nelze se spoléhat na koncentrátor jako na hlavní bezpečnostní prvek a komunikaci uvnitř BPL sítě ponechat nešifrovanou, jelikož přístup k elektrickému vedení nemusí být dostatečně zabezpečen proti neoprávněné manipulaci, a to převážně z důvodu nedostatečného fyzického zabezpečení rozvaděčů. V dnešní době je využíván univerzální mechanismus pro zamykání rozvaděče u koncových spotřebitelů.

Nešifrovaná komunikace není jediný bezpečnostní problém, který se váže ke komunikaci uvnitř BPL sítě. Může to být také útok na dostupnost služeb a další potenciální zranitelnsoti, které budou testovány.



Obr. 9.3: Zobrazení útoku zevnitř BPL sítě.

9.1.2 Webová aplikace koncentrátoru

Na koncentrátoru je dostupných více služeb – jednou z nich je webová aplikace, která naslouchá na portu 8080 TCP (Transmission Control Protocol) a je dostupná pouze přes protokol HTTPS (Hypertext Transfer Protocol Secure). Pro návázání zabezpečeného připojení využívá TLS (Transport Layer Security) ve verzi 1.2, v současnosti je považována jako dostatečná, avšak bylo by dobré přejít na již dostupnou verzi 1.3, protože novější verze odstraňuje možnost využívat hashovací funkci MD5 (Message-Digest algorithm) a snižuje počet zpráv nutných k ustanovení šifrovaného spojení a díky tomu je navázání spojení rychlejší než u verze 1.2.

9.1.3 Certifikát webové aplikace

Certifikát webového serveru není prohlížeči vyhodnocen jako nedůvěryhodný, primárně kvůli doménovému jménu, které v laboratoři není využíváno (pouze IPv4 adresa). Druhý důvod je prošlá platnost certifikátu, která byla platná do 9. července 2015. Certifikát je podepsán sám sebou. Pro testování v laboratoři není nutné obstarávat podpis od důvěrné certifikační autority. Pro nasazení do provozu je dobré nechat si certifikát vystavit od společnosti, která zaručuje řetězec důvěry.

Podle doporučení NÚKIB (Národní úřad pro kybernetickou a informační bezpečnost) je pro certifikáty založené na RSA (Rivest–Shamir–Adleman) nutné využívat klíče minimální délky 3072 bitů a pro hashovací funkce se má využívat minimálně SHA2 (Secure Hash Algorithm 2) s minimální délkou výstupu 256 bitů. Jak je z obrázku v příloze A patrné, certifikát webové aplikace využívá podpis s hashovací funkcí SHA1 (Secure Hash Algorithm 1), což NÚKIB (Národní úřad pro kybernetickou a informační bezpečnost) v současnosti nebere jako bezpečnou hashovací funkci [23].

9.1.4 Vlastnosti webové aplikace

Aplikace beží na webovém serveru lighttpd ve verzi 1.4.11, což lze zjistit z hlavičky HTTP (Hypertext Transfer Protocol) odpovědi. Samotný back end je napsán v PHP verzi 5.4.14 a využívá framework CakePHP. Framework byl objeven na základě session cookie, která se jmenuje CAKEPHP. Front end využívá CSS knihovny Bootstrap a javascript knihovnu jQuery. Obě knihovny jsou stažené a vloženy do samotné webové aplikace. Není zde správně využíváno načítání knihoven přes HTTP protokol až z klientova PC, což by mohlo být zneužito pro Man-in-the-middle útok.

První stránka, která se načte, je přihlášení do aplikace. Políčka pro přihlášení jsou správně sanitována proti SQL injekcím. Testování proběhlo pomocí nástroje OWASP ZAP a SQL MAP.

9.1.5 Překonání přihlašování

Při hledání výsledku odpovědi 404 bylo zjištěno, že aplikace nezasílá standardní stránku s odpovědí, že stránka neexistuje. Současně se posílá HTML stránka, kde je lišta menu stejná jako při běžném přihlášení. Lišta obsahuje validní odkazy na stránky, které by měly být viditelné pouze po přihlášení (odpověď webové aplikace je zachycena v příloze B).

Odkazy, které nemění nastavení koncentrátoru, fungují a útočník má tedy přístup do sekce Analytics, částečně i Operations, a to bez jakékoliv znalosti hesla. Útočníkovi stačí pouze vyvolat stránku 404 a ihned získá přehled o adresářové struktuře webu a přístup na stránky, které neumožňuje změnu nastavení. V případě, že útočník přistoupí na stránku, která mění nastavení, je automaticky přesměrován na přihlašovací stránku.

Pokud útočník klikne na odkaz Analytics, dostane se k hlavní stránce, kde získá přehled o adresním rozsahu BPL sítě a všech připojených sítích. Zároveň se zobrazí posledních 15 logů, které koncentrátor vytvořil. V dolní části stránky se zobrazuje aktuální zatížení CPU (Centrální procesorová jednotka) a vytížení paměti. Pokud útočník má v úmyslu útočit na dostupnost služby, není pro něj problém otevřít právě kartu s Analytics a při spustění útoku sledovat, jak je vytížena paměť, potažmo i CPU. Poslední zajímavou položkou pro útočníka je seznam procesů, které jsou zrovna spuštěny na koncentrátoru, a to včetně PID (Process identifier). Z důvodu velkého počtu citlivých informací není stránka zobrazující Analytics součástí příloh.

Sledování systémového vytížení není poslední možností, jakou útočník disponuje. Pokud útočník klikne na stránku Operations a vybere z menu Metering, dostane se na seznam všech elektroměrů, které konkrétní koncentrátor spravuje. Může vidět jejich MAC (Media Access Control) adresu, datum registrace a sériové číslo. Může vybrat zařízení a provést přes webové rozhraní na něj ping, jeho deregistraci anebo otevřít telnet připojení na daný smart metr.

U posledních dvou variant se útočníkovi nabízí možnost zkusit zařízení deregistrovat od koncentrátoru a zamezit tak sbírání jeho dat. V případě, že zaškrtne vybraný elektroměr a variantu deregistrovat, je zařízení automaticky deregistrováno bez nutnosti zadávat přihlašovací údaje správce. Druhá varianta je, že si vybere elektroměr a klikne na tlačítko telnet. Útočníkovi se zobrazí nové pop–up okno webového prohlížeče, které je stejné, jako kdyby využíval terminálového klienta, a je automaticky přihlášen jako uživatel na vybraném elektroměru. Může vyčítat hodnoty, popřípadě se zkusit přepnout do administrátorského účtu, pokud zná heslo, nebo může vyzkoušet slovníkový útok. Samotné telnet spojení je jen mezi koncentrátorem a elektroměrem, na kterém běží služba telnet naslouchající na portu 40000. Koncentrátor komunikaci převádí do webové aplikace a plní funkci brány mezi BPL

sítí a ethernetem. Útočník tak ani nepotřebuje BPL modem, aby mohl komunikovat se zařízeními na elektrické síti. Stránka včetně otevřeného spojení na jeden z elektroměrů je v příloze C.

Jak je z přílohy C patrné, webová aplikace nenaslouchá na portu TCP 8080, jak zbytek webové aplikace, ale otevírá okno, kde naslouchá na vygenerovaném TCP portu. Tento port není otevřen pouze při stisknutí tlačítka pro připojení, ale naslouchá na něm neustále. Útočník pro příští přihlášení již nepotřebuje opakovat postup na webovém serveru, ale stačí mu pouze otevřít v prohlížeči adresu koncentrátoru a s dříve nalezeným TCP portem. Útočník si tak otevře telnet spojení rovnou na smart metr. Takto otevřené spojení není logováno, avšak ostatní události jsou logovány a jsou viditelné v záložce Dashboard.

9.1.6 Clickjacking

Clickjacking je typ útoku, kdy webová stránka je načtena do rámečku pomocí tagu iframe. Útočník pak využívá průhlednosti několika rámečků, kdy oběť neví, že nad rámečkem, kde se zobrazuje důvěryhodná webová stránka, je vložen průhledný rámeček, který může spouštět škodlivý kód.

Prohlížeče se brání tomuto útoku pomocí vložení restrikce do hlavičky HTTP odpovědi. Existují dva možné typy hlaviček, které tento útok znemožňují. První je X-Frame-Options a druhý je Content-Security-Policy. Pokud útočník načítá na svoji webovou stránku do iframe tagu a prohlížeč oběti zjistí, že součástí odpovědi je právě jeden z těchto tagů, nenačte stránku do rámečku.

Webový server nemá nastavenou ani jednu z možných odpovědí, a proto načtení webové stránky do rámečku je možné. Webová aplikace by měla odpovídat společně s jedním typem odpovědi, která zamezuje útok typu Clickjacking.

9.1.7 HSTS

Webová aplikace naslouchá pouze pomocí protokolu HTTPS. Sama aplikace ale klientovi nevnucuje využívání HTTPS protokolu jako jediný možný pro komunikaci se serverem. To dává útočníkovi možnost komunikaci degradovat spojení na HTTP protokol, který není šifrovaný a to umožňuje útočníkovi číst citlivé informace. Komunikace jde přes útočníka, kdy se oběť chce dotázat webového serveru pomocí zabezpečeného protokolu využívající TLS. Útočník vytvoří vlastní šifrované spojení mezi ním a webovou aplikací. Oběti zašle odpověď vydávající se za server. Odpověď již ale nevyužívá zabezpečené spojení pomocí TLS ale nijak nešifrovaná data pomocí protokolu HTTP, ze kterého může útočník vyčítat citlivé informace. Závisí pak na prohlížeči, jestli pro tuto webovou stránku není vynucováno pouze šifrované spojení.

Pro vyžadování HTTPS spojení je při odpovědi ze strany serveru do hlavičky přidána položka HSTS (HTTP Strict Transport Security), která nese informace, jak dlouho má vyžadovat pouze šifrované spojení, popřípadě i další informace, včetně spojení se subdoménami. Jediná možnost útoku je v době, kdy oběť navštěvuje danou stránku poprvé a nemá uložený HSTS tag ve své paměti [24].

Webový server ale položku HSTS vůbec neodesílá, a proto útočník může cílit i na oběti, které již na web přistupují poněkolikáté. Pro zajištění ochrany klientů by bylo dobré HSTS položku do odpovědí přidat.

9.1.8 Správa uživatelů

Prováděcí vyhláška zákona o kybernetické bezpečnosti udává povinné parametry pro hesla uživatelů. Webová aplikace umožňuje správu uživatelů, a to jak běžných uživatelů, tak i těch, kteří mají právo spravovat zařízení. Bohužel, nejsou splněny podmínky vyhlášky a heslo pro uživatele musí splnit jedinou podmínku, alespoň 5 znaků. Podle vyhlášky minimální délka znaků pro běžného uživatele je 12 a pro administrátory je 17. Dále lze zvolit heslo, které je v seznamu nejčastějších hesel, i heslo stejné, jako je jméno uživatele. V neposlední řadě lze heslo měnit bez jakéhokoliv časového omezení, což je v rozporu s vyhláškou, která definuje minimální časový odstup od poslední změny hesla na 30 minut.

Samotná webová aplikace neumožňuje obnovení hesla od uživatelů, kteří nejsou přihlášení a nebo nemají dostatečné práva. Hesla uživatelům tedy může měnit uživatel typu administrátor. Změněné heslo není taktéž časově omezeno a uživatel po přihlášení není vyzván, aby heslo změnil. Samotný uživatel typu admin může smazat účty jakéhokoliv jiného uživatele, a to i typu administrátor.

V případě, že útočník získá heslo jednoho z administrátorů, může smazat všechny uživatele a změnit heslo administrátorovi, kterému heslo bylo odcizeno. Takto se stává jediný možný administrátorem na zařízení. V takovémto případě je potřeba mít zálohu systému, jinak koncentrátor bude muset být obnoven do továrního nastavení a veškerá důležitá data mohou být nenávratně ztracena. Další možností je ukládání provozních dat na externí paměťové zařízení.

9.1.9 SSH

Koncentrátor naslouchá na připojení pomocí protokolu SSH (Secure Shell) na portu TCP 22. Jako server je využita aplikace Dropbear ve verzi v2015.55. Samotná aplikace do verze v2016.74 obsahuje kritické chyby, které umožňují spuštění kódu pod právy uživatele root. Jedná se o 4 chyby ohodnocené jako kritické, které jsou blíže popsané v CVE–2016–7406 až CVE–2016–7409. Ke všem chybám existuje v databázích zranitelností pouze krátký popis možných dopadů, avšak chybí popis, jak

je možné zranitelnost zneužít. V současné době není dispozici exploit zneužívající tuto chybu. Po krátkém popisu závažnosti chyby následuje doporučení aktualizovat SSH server – alespoň na verzi v2016.74.

9.1.10 Webový server smart meteru

Každý smart metr, jak třífázový, tak i jednofázový, naslouchá pomocí protokolu HTTP na portu TCP 80. Webová stránka obsahuje pouze nadpis, a to slovo Marvell. Samotná odpověď ze strany serveru neobsahuje žádné informace ve hlavičce, ani jméno stránky. Služba žádné takové informace neposkytuje a není tedy žádný důvod k tomu, aby služba měla být aktivní a naslouchat na portu.

9.1.11 Telnet

Smart metr má otevřen port TCP 40000 a zde naslouchá telnet server. Telnet slouží ke vzdálené správě zařízení, stejně jako SSH. Hlavní slabinou telnetu je, že data zasílá mezi zařízeními nejsou nijak šifrována, narozdíl od SSH. V případě, že útočník se připojí do BPL sítě pomocí svého modemu, je veškerá komunikace proudící přes BPL síť dostupná i pro útočníka. Při přihlášení uživatele na smart metr pomocí telnetu, může útočník zachytit jméno i heslo. Pro splnění vyhlášky zákona o kybernetické bezpečnosti není možné využívat telnet službu. Doporučuje se ji nahradit službou SSH a pro přihlašování nevyužívat jméno a heslo, ale nahradit přihlašování RSA klíči.[25]

Pro přihlášení na smart metr není vyžadováno žádné heslo, automaticky je uživatel přihlášen jako user, který nemá veškerá práva, ale již si může prohlížet určitá nastavení pomocí příkazů, která smart metr umí. Veškerý soupis příkazů lze zjistit pomocí příkazu *ls*. Pro přístup do administrátorského účtu je potřeba již heslo administrátora. Připojení pomocí telnetu není logováno v koncentrátoru ani v rámci události, kterou si koncentrátor stahuje ze samotných smart metrů.

9.1.12 Získání administrátorského účtu smart metru

Smart metr od Výrobce A obsahuje relé, které slouží pro přívod a elektrické energie. Pokud majitel nemovitosti neplatí za účty, může být odpojen od energie. Funkce vzdáleného odpojení a připojení má velké uplatnění v oblastech, kde je obtížné se fyzicky dopravit. Pro Českou republiku se může jednat o chatové oblasti v horském prostředí. Rozepnutím relé bude nemovitost odpojena od přívodu elektrické energie. Relé je největším chráněným aktivem ve smart metru [26].

Pro ovládnutí administrátorského přístupu smart metru útočník potřebuje BPL modem připojen na stejnou fázi, na které komunikují všechny smart metry spadající

pod koncentrátor. Útočník začně záchytem provozu v síti BPL. Dalším krokem je, že útočník přistoupí na webovou aplikaci na koncentrátoru. Zde útočník vyvolá chybovou odpověď serveru typu 404. Koncentrátor loguje odpověď typu 404 i IPv4 adresu, která způsobila tuto odpověď. Z toho důvodu je vhodné využít další zařízení, které je připojené do internetu a pro vyvolání chyvébo stavu využít VPN (Virtuální privátní síť), pro skrytí veřejné IP adresy útočníka.

Po vyvolání HTTP odpovědi typu 404 uvidí menu i s odkazy. Dostane se na stránku Metering, kde je výpis všech zaregistrovaných zařízení a možnost otevření telnet spojení. Ve skutečnosti se neotevírá telnet stejně jak z příkazového řádku, ale startuje službu, která zprostředkovává spojení se smart metrem. Tato služba se jmenuje Shell In A Box. Úočník se dostane k menu, kde si vybírá podle možností, a po stistknutí klávesy volby se provede příkaz. Některé fungují v režimu běžného uživatele. Pokud útočník vybere například možnost 2, což je příkaz pro přečtení fyzické adresy smart metru, následuje série příkazů, které nejprve přepnou do režimu administrátora, pak se zadá příkaz pro vyčtení fyzické adresy zařízení a poslední příkaz je pro přepnutí zpět mimo administrátorský mód do menu s výběrem možností. Při přihlášení pomocí obyčejného příkazového řádku je při výběru možnosti 2 potřeba heslo k administrátorskému účtu. Situace je zachycena v příloze D. Z toho je patrné, že samotná služba Shell In A Box má uložené administrátorské heslo v čistém textu tak, aby mohla provést sérii příkazů za uživatele.

Pokud má útočník připojené zařízení do BPL sítě a zapnuté zachytávání paketů, heslo je pro administrátora přenášeno právě přes telnet, tedy jako nešifrovaný text. Útočník tedy nemusí čekat až se administrátor přihlásí, aby získal jeho přihlašovací údaje. Kvůli chybě na webovém portálu akci může vykonat za něj. Zachycené heslo je v příloze E. Takto útočník získá administrátorské heslo ke smart metru. Dalším krokem je již telnet připojení na zařízení. Po připojení je uživatel přihlášen jako běžný uživatel. Pokud zadá příkaz ls, vypíší se mu všechny dostupné příkazy pro daného uživatele a v dané složce. Utočník využije příkaz *mode admin* pro přepnutí do pozice administrátora. Zde si opět může vypsat všechny dostupné příkazy. Pokud si vybere příkaz *sd*, dostane se do složky, kde lze manipulovat se všemi relé. Příkazy pro vypnutí relé:

```
#admin@/scheduleDebug/>tt 17 s 0 0
relay1 0 relay 2 1
OK
#admin@/scheduleDebug/>tt 17 s 1 0
relay1 0 relay 2 0
OK.
```

9.1.13 Administrátorské heslo v textové podobě

Jak je z předešlého útoku patrné, heslo pro zvýšení práv na smart metru je přenášeno bez zadání uživatele, a proto na koncentrátoru musí být uloženo v textové podobě. Heslo je uloženo ve stejné složce jako samotná služba. Jedná se o složku:

`/usr/local/wui2/scripts.`

Zde je soubor jak samotné služby Shell In A Box, tak i podpůrný soubor pojmenován wuishell.sh. V samotném souboru je nadefinované menu příkazů. Uživatel si číslicí vybírá příkaz pro vykonání. Kromě přímého spojení telnetu a ukončení Shell In Box možnosti jsou veškeré příkazy vykonány až po příkazu LOGINCMD. Tento příkaz je definován:

```
LOGINCMD="echo \"mode admin\"; sleep 1;echo \"********\"; sleep 1".
```

Heslo je uloženo jako text a využíváno aplikací, avšak podle vyhlášky nesplňuje odolnost vůdči offline útokům, kdy uložené heslo nesmí být dostupné jako čitelný text, popřípadě využívat slabé hashovací funkce. Bezpečné hashovací funkce pro ukládání hesel jsou vyjmenovány v doporučení NÚKIB. V tomto případě je uloženo v textové podobě, aby mohlo poskytnout dostupné informace administrátorovi, aniž by musel heslo zadávat. Je zde uloženo jediné heslo, které bude využito pro připojení na jakékoliv zařízení. Proto veškeré smart metry kontrolované jedním koncentrátorem musí mít stejné heslo pro přístup do administrátorského režimu. Útočník zjištěním hesla pro jeden smart metr získává heslo ke všem dalším, bez nutnosti opakování útoku pro zjistění administrátorského hesla na další smart metr.

9.2 ADDAX Metering Solution

Druhým typem smart metrů testovaných v laboratoři je řešení od společnosti ADD Group. Tato společnost vytváří systém, který pojmenovali ADDAX Metering Solution. ADDAX zastřešuje více typů výrobků typu smart metr. Jeden typ výrobků je určen pro distributory elektrické energie a je to, stejně jako u předešlého výrobce, koncentrátor, který zprostředkovává komunikaci mezi smart metry a jinými sítěmi.

Dalším typem je smart metr určen primárně pro arabský trh. Fakturace není nastavena po spotřebě elektrické energie zpětně, ale zavádí systém předplacených karet, které při přiložení ke smart metru dobijí konto smart metru. Využívá technologii NFC (Near Field Communication), což je druh bezdrátové komunikace na velice krátkou vzdálenost. Pro evropský trh je určen primárně smart metr z řady Classic, který nevyžaduje systém předplacených karet. V České republice jsou tyto smart metry nasazovány do domácností, kde je distributorem elektrické energie Pražská energetika. Podle oficiálních stránek skupiny ADD Group do České republiky

bylo dodáno a nasazeno okolo 22 000 smart metrů. Jedná se o smart metry měřící spotřebu na jedné fází nebo na třech fázích. Pro komunikaci mezi smart metrem a koncentrátorem je využito stávající infrastruktury elektrického vedení. Využívá technologii PLC (PowerLine Communication), což představuje úzkopásmovou komunikaci, kdežto BPL je širokopásmová. Výhoda PLC je vyšší přenosová rychlost, jelikož technologie pracuje v pásmu 150 – 500 kHz.

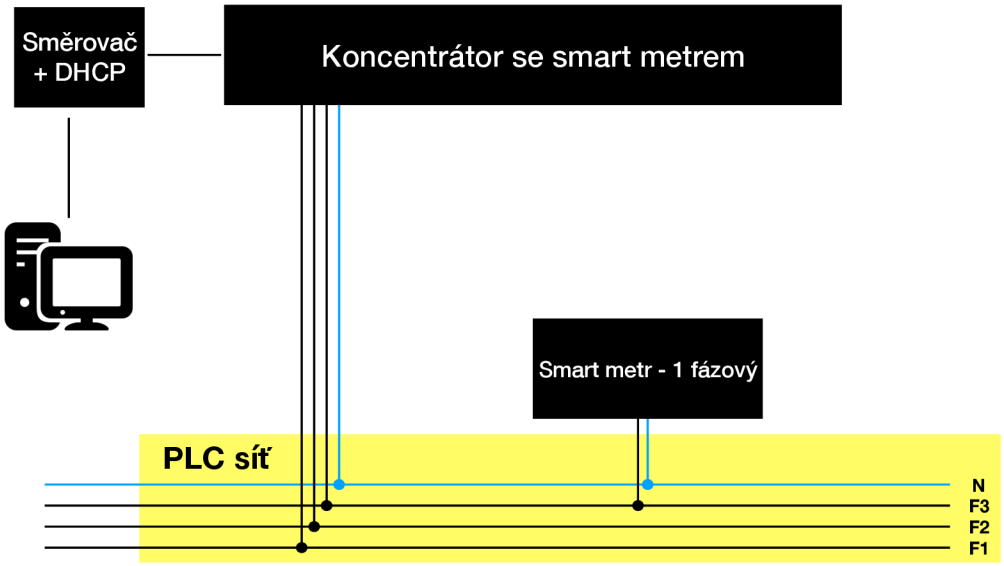
Na rozdíl od společnosti Výrobce A je v řešení ADDAX více typů koncentrátorů. Prvním typem je koncentrátor, který nespojuje PLC síť s dalším typem sítě a netvoří tak bránu, ale pouze ukládá informace do své paměťové karty. Druhým typem je koncentrátor umožňující komunikaci i mimo PLC síť, který obsahuje možnost komunikace pomocí Ethernetu, USB, optické sondy nebo RS-485. Jedná se o podobný typ, který dodal Výrobce A. Posledním typem je koncentrátor a zároveň smart metr. Jedná se o smart metr třífázový. Výhodou posledního typu je možnost umístit tento smart metr před smart metry v domácnostech. Takto umístněný smart metr plní funkci koncentrátoru a zároveň měří celkovou spotřebu. Pokud se významně liší rozdíl spotřeby celkové a součet spotřeby odběrných míst, může se jednat o poruchu a možné technické ztráty na vedení, nebo netechnické ztráty, a tím pádem i černého odběratele elektrické energie. Tento poslední typ koncentrátoru je v laboratoři na testování.

9.2.1 Zapojení laboratoře

V laboratoři lze zapojit řešení ADD Group na stejnou fázi jako je i řešení od Výrobce A. Oba využívají elektrické vedení jako přenosové médium, avšak technologie BPL a PLC se navzájem neovlivňují. Lze tedy využít pouze jednu fázi. Zapojení ADDAX Metering Solution je zachyceno na obrázku 9.4. Hlavní rozdíl oproti již testovanému výrobci číslo 1 spočívá ve vnitřní PLC síti. Koncentrátor neumožňuje směrování zpráv do PLC sítě, a nemůže tak být modemem pro útočníka. Znemožnění směrování je dobrým krokem pro lepší segmentaci sítí. V tomto případě zbývají útočníkovi dvě možnosti, jak realizovat útok: ovládnout koncentrátor a získat přístup do vnitřní sítě, nebo se připojit do PLC sítě pomocí svého modemu a komunikovat se smart metry přímo bez koncentrátoru. Bohužel v době testování nebyl na ústavu dostupný PLC modem a testování vnitřní sítě nebylo provedeno.

9.2.2 Webová aplikace

Koncentrátor naslouchá na portech TCP 80 a 443, kdy na portu 80 je webová aplikace poskytována pomocí protokolu HTTP a na portu 443 pak aplikace poskytuje stejnou aplikaci přes protokol HTTPS. Webová aplikace je spouštěna a provozována pomocí serveru nginx/1.10.1. Tuto informaci lze zjistit díky hlavičce HTTP odpovědi



Obr. 9.4: Zapojení sítě od výrobce ADD Goup.

serveru. Doporučení pro administrátora je zamezit posílání této informace v hlavičce odpovědi. Back end je napsán pomocí skriptovacího jazyku PHP, lze ji zjistit na základě session cookie, který se jmenuje PHPSESSID. Není využito žádné nadstavby PHP v podobě frameworku jako u Výrobce A. Tyto informace jsou dostupné pro útočníka bez přihlášení. První načtená stránka je právě přihlašovací stránka, avšak nenachází se v souboru *index.php*, jak se by se dalo očekávat, ale v souboru *login.php*. Po načtení stránky je uživatel přesměrován na stránku *login.php* pomocí HTML (HyperText Markup Language) tagu:

```
<meta http-equiv="REFRESH" content="0;url=/login.php">
```

Výsledkem tohoto požadavku je okamžité přesměrování stránky na login.php. Po přihlášení je načtena stránka, která již obsahuje rozšíření pro front end. Jedná se o javascript framework Backbone.js ve verzi 1.2.3 a další dvě javascript knihovny: jQuery 2.0.3 a Underscore.js 1.8.3. Webová aplikace obsahuje menu z tří částí. Data z koncentrátoru o stavu smart metrů v síti, nastavení PLC sítě a údržby. U smart metrů lze vidět pouze jejich MAC adresa. Firewall umožňuje definování povolených, zakázaných adres a povolení source NAT, ale již nelze nastavit port forwarding pro přístup k službám uvnitř PLC sítě. Lze povolit SNMP (Simple Network Management Protocol) pro určitou IPv4 adresu, ale již není nikde definováno, jaká verze SNMP je využita.

9.2.3 Certifikát webové aplikace

Samotné parametry certifikátu splňují doporučení NÚKIB pro asymetrické protokoly a i pro hashovací funkce. Certifikát je vystaven pro využití RSA s délkou klíče 4096 bitů, což je více než je potřeba podle doporučení NÚKIB a hashovací funkce pro podpis je SHA2 s výstupem 256 bitů. Certifikát je zobrazen v příloze F.

Při připojení pomocí protokolu HTTPS je využit TLS ve verzi 1.2. Tato verze je dostatečná a prohlížeče ji podporují, doporučuje se však postupně přejít na novější verzi 1.3. Spojení s koncentrátorem není prohlížečem shledáno jako důvěryhodné, a to hlavně z důvodu, že certifikátu chybí doménové jméno a je podepsán sám sebou. Pro využití v provozu by certifikát byl vystaven na doménové jméno a podepsán certifikační autoritou, která je ve výchozím nastavení již součástí kořenových certifikačních autorit.

9.2.4 Nedostatky webové aplikace

Webová aplikace využívá protokol HTTPS, který posílá data přes TLS, jsou šifrována, avšak pokud uživatel přistoupí na webovou aplikaci pomocí protokolu HTTP, není automaticky přesměrován na protokol HTTPS. Uživatel, který si nevšimne, že nepřistoupil do administrace koncentrátoru pomocí zabezpečeného protokolu, může své přihlašovací údaje poskytnout útočníkům po cestě, kteří pak jsou schopni zachytit přihlašovací údaje v otevřené podobě. Pro zajištění důvěrnosti dat je potřeba zakázat naslouchání přes protokol HTTP, nebo přesměrovávat provoz na zabezpečený protokol.

Stejně jako u webové aplikace Výrobce A chybí HSTS tag i v řešení ADDAX. Pokud chce administrátor webové aplikace zaručit, že se uživatel nestane obětí degradace HTTPS spojení na HTTP, je potřeba přidat HSTS tag do hlavičky odpovědi. Aktuálně není parametr zasílán u žádné z načítaných stránek. To není jediný společný nedostatek webových aplikacích obou typů koncentrátorů, i u řešení ADDAX chybí hlavička HTTP odpovědi serveru, která zamezuje technice Clickjacking, více v kapitole 9.1.6.

9.2.5 SSH

Koncentrátor umožňuje připojení na zařízení pomocí SSH. Pro připojení je potřeba jméno a heslo stejné jako do webové aplikace. Pro přihlašování by pro splnění vyhlášky mělo být využito přihlašování pomocí jména a hesla až v poslední variantě, kdy nelze realizovat přihlášení asymetrické kryptografie. U běžné Linuxové distribuce lze tuto variantu nakonfigurovat a stejně tomu je i u Výrobce A. Po přihlášení pomocí SSH koncentrátor ADDAX nenabízí celkovou správu zařízení, ale pouze systémové

menu s možností výběru a provedení akce. Uživatel tedy vybírá pouze číselné hodnoty pro interakci se zařízením. Lze vyčíst záznamy událostí, informace o zařízení, restartovat službu, případně i rozhraní. Nemůže ale jakkoliv měnit nastavení nebo procházet souborový systém. Lze stáhnout zálohu systému s nastavením. Vzniklý soubor má příponu .backup a obsahuje pouze nečitelná data v binární podobě. Zavedení menu s možnostmi je dobrý bezpečnostní prvek, který zamezuje uživateli poškodit systém, avšak přihlašovací údaje jsou zde stejné jako do webové aplikace, kde je možné definovat více nastavení systému. Pokud uživateli budou odcizeny přihlašovací údaje k SSH, automaticky musí počítat i s možností změny nastavení přes webovou aplikaci, kde lze změnit heslo, definovat firewall a další možnosti, které přes SSH nejsou možné.

9.2.6 Testování zranitelností

Zranitelnosti smart metru byly testovány pomocí nástroje Nessus a Metasploit. Pro testování byla využita distribuce Linux Kali ve verzi 2019.1. Tato verze byla vydána v únoru 2019. Hlavní novinkou je právě databáze zranitelností Metaspoit, která je zde součástí operačního systému ve verzi 5.0. Databáze zranitelností byla využita pouze na útok proti koncentrátoru, jelikož koncentrátor neumožňuje směrování do vnitřní sítě a v době testování se na ústavu nenacházel PLC modem, který by umožnil se připojit přímo do sítě se smart metry. V databázi zranitelností se nenacházela žádná zranitelnost, která by mohla být zneužita pro převzetí správy zařízení.

9.2.7 Dostupnost služby

Pokud se útočníkovi nepodaří převzít kontrolu nad koncentrátorem, může se pokusit vyřadit koncentrátor z provozu alespoň pro legitimní uživatele pomocí útoku na dostupnost služby. Tento útok spočívá v zahlcení koncentrátoru nelegitimními požadavky, aby legitimní provoz nemohl být zpracován. Útoky lze realizovat z jednoho místa, jedná se o DoS (Denial of Service), nebo z několika zařízení a má označení DDoS (Distributed Denial of Service). Samotný koncentrátor nemá potřebnou funkci pro rozpoznání útoku na dostupnost služby, proto je důležité zjistit, jak koncentrátor bude reagovat, když bude vystaven různým druhům zahlcení.

Prvním testem byla závislost doby odpovědi webového serveru při odesílání několika požadavků zároveň. Tento test bude v provozu ovlivněn kapacitou linky, která bude hrát zásadní roli. V případě, že v aktivním prvku po síti nastane hromadění požadavků do fronty, může nastat situace, kdy požadavky budou zahazovány bez rozdílu, zda se jedná o legitimní požadavek, či nikoli. Při testování byl kladen

důraz na koncentrátor, proto aktivní prvky nehrály v testu hlavní roli a byla testována výkonnost webového serveru. Pro měření doby odpovědi byl využit program Apache JMeter [1]. Nelegitimní požadavky byly zasílány pomocí virtuálního stroje Linux Kali za pomocí programu ApacheBench. Test začínal odesíláním 10 požadavků současně. Graf doby odpovědi je zobrazen v příloze G. Následně se počet zvyšoval a končil odesíláním 200 požadavků současně, zobrazeno v příloze H. Doba zpoždění sice narůstala, ale i tak bylo zaručeno, že se uživateli stránka po nějakém čase načte, jelikož nebyla překročena mezní hodnota časovače prohlížeče. Každý prohlížeč má samostatně definovaný čas, po který čeká na odpověď ze strany serveru.

Druhý test byl zaměřen na vyčerpání prostředků, které koncentrátor alokuje pro vyřízení požadavku. Pokud uživatel vytvoří TCP spojení, je možné posílat data požadavku velice pomalu. To je dáno vlastností HTTP protokolu, který se snaží zajistit službu i uživatelům s pomalým připojením. Při vytvoření spojení mezi klientem a serverem je alokována paměť pro vyřízení žádosti. Útok typu Low and Slow využívá této vlastnosti. Útočník vytváří velké množství spojení, které posílají požadavky velice malou přenosovou rychlostí, a tím se snaží serveru vyčerpat prostředky pro legitimní uživatele. Výsledkem tohoto testu je, kolik otevřených spojení musí útočník vytvořit, aby koncentrátor neodpovídal legitimnímu uživateli. Pro útok Low and Slow byl využit program slowloris.py [2]. Hraniční počet spojení dosáhlo hodnoty 763, při tomto počtu spojení server sice odpovídá legitimnímu uživateli, ale odpovědí typu 500 (Internal Server Error). Pokud se zvýší počet nelegitimních pomalých spojení na 764, z toho důvodu není navázáno spojení se serverem a webová aplikace se stává pro legitimního uživatele nedostupná.

Koncentrátor ale nealokuje veškeré prostředky pro webový server. V případě útoku na webový server pomocí Low and Slow má stále legitimní uživatel možnost připojit se na koncentrátor pomocí SSH. Proces si tedy nemůže alokovat veškeré prostředky pro sebe. Situace, kdy je webový server pod útokem a zároveň se lze připojit pomocí SSH, je zobrazena v příloze I.

9.2.8 Rozdíly mezi výrobci

Hlavním rozdílem, který je mezi dodavateli řešení, je koncept smart metru. Společnost ADD neumožňuje správu relé na jednotlivých smart metrech. Nelze tak odpojit domácnost od elektrické energie pomocí vzdálené správy. Koncentrátor pouze slouží k měření. Nelze otevřít spojení na smart metr z webové aplikace, tak jak je to u výrobce číslo 1. Lze říci, že ADD se snaží vytvořit uzavřené řešení, které klade nároky na bezpečnost.

[1] https://jmeter.apache.org/

[2] https://github.com/gkbrk/slowloris

Přičemž ADD má nedostatky ve filtrování provozu oproti Výrobce A. U ADD lze filtrovat spojení pouze pomocí IP adres, nelze již definovat pravidla pro vyšší vrstvy. Útočník může provést sken zařízení, a to i z veřejné sítě. U Výrobce A lze definovat pravidla pomocí nástroje Iptables, pravidla po restartu zařízení jsou smazána, ale lze vytvořit skript, který definovaná pravidla po každém restartu nahraje zpět do firewallu.

10 Závěr

Tato bakalářská práce měla poskytnout pohled na problematiku smart metru. Neodmyslitelnou součástí této problematiky jsou bezpečnostní aspekty smart metru, které jsou nepřímo vymezeny v zákoně o kybernetické bezpečnosti. Důvodem je skutečnost, že smart metr může být prvkem systému, kterým je poskytována základní služba, konkrétně v oboru energetiky. Proto nároky na zabezpečení mohou být vyšší než u jiných infrastruktur.

V teoretické části bylo pojednáváno o aktuálních normách, které se týkají smart metrů. Hlavní závaznou normou je zákon o kybernetické bezpečnosti, který vychází z rodiny standardu ISO 27000. Do budoucnosti je potřeba pamatovat na aktuálně rozpracovanou podobu standardu ISO 27030, jelikož se týká zařízení internetu věcí, mezi než se smart metr řadí.

Cílem praktické části pak bylo testování dvou systémů od různých výrobců. Výsledkem jsou značné nedostatky u Výrobce A. Nedostatky vedou k možnosti převzetí kontroly nad smart metrem. Další verze smart metru by měla zjištěné nedostaky odstranit, a předejít tak možnému zneužití. Následkem zneužití nedostatků může být domácnost odpojena od elektrické energie. Výhoda těchto nedostatků je, že se jedná pouze o softwarové vady, které lze opravit novou verzí systému.

Daleko méně chyb a nedostatků z pohledu informační bezpečnosti obsahoval smart metr výrobce ADD Group oproti smart metru od Výrobce A. Vyšší informační bezpečnost jde ruku v ruce s nižší funkcionalitou, protože smart metr neobsahuje veškeré funkce smart metru od výrobce číslo 1. Tento typ neobsahoval závažné chyby, které by vedly k převzetí kontroly nad smart metrem. Pro případ rozšíření práce se nabízí testování vnitřní PLC sítě. Dále bych navrhoval testování hardwarových částí smart metrů.

Literatura

[1] BURDA, Karel *Bezpečnost informačních systémů.* ISBN: 978-80-214-4890-2, 2013 [online]. Dostupné z URL: <https://www.vutbr.cz/www_base/priloha.php?dpid=81244>.

[2] CROWLEY, Paul a Eric BIGGERS. *Adiantum: length-preserving encryption forentry-level processors* [online]. Google, 2018 [cit. 13-12-2018]. Dostupné z URL: <https://eprint.iacr.org/2018/720.pdf>.

[3] POLČÁK, Radim. *Právo informačních technologií.* Praha: Wolters Kluwer, 2018. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7598-045-8.

[4] Zákon č. 181/2014 Sb. [online] *O kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).* [cit. 20-10-2018]. Dostupné z URL: <https://nukib.cz/download/kii-vis/ZKB_uplne_zneni.pdf>.

[5] *Hacked smart devices are being user to launch web attack* [online]. Vector Choise, 2016 [cit. 2018-11-11]. Dostupné z URL: <https://www.vectorchoice.com/2016/10/14/hacked-smart-devices-are-being-used-to-launch-web-attacks/>.

[6] *Kryptografie, kódování dat* [online]. [cit. 4-11-2018]. Dostupné z URL: <http://www.zaachi.com/cs/print/kryptografie-kodovani-dat.html>.

[7] *What are the Counter and PCBC Modes?* [online]. WILMINGTON: X5 Networks [cit. 4-11-2018]. Dostupné z URL: <https://x5.net/faqs/crypto/q84.html>.

[8] Vyhláška č. 82/2018 Sb. [online]. *Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).* [cit. 27-10-2018] Dostupné z URL: <https://nukib.cz/cs/nova-vkb>.

[9] *Password Hashing Competition* [online]. 2015 [cit. 4-11-2018]. Dostupné z URL: <https://password-hashing.net>.

[10] ISO/IEC 27001 Information security management: ISO/IEC 27000 family - Information security management systems. *International Organization for Standardization* [online]. Švýcarsko, 2019 [cit. 2019-03-23]. Dostupné z URL: <www.iso.org/isoiec-27001-information-security.html?fbclid=IwAR0ba8sx8unyh-OI02B4iWoSiAedTf7O3M3Ht-Ce1iFu9nMwj7O_dXBsR0s>.

[11] CALDER, Alan. *INFORMATION SECURITY&ISO27001* [online]. IT Governance.co.uk, 2018,10 [cit. 2019-03-23]. Dostupné z URL: <https://www.itgovernance.co.uk/files/Infosec_101v1.1.pdf>.

[12] ISO/IEC 27002:2013. *Risk Analysis Consultants* [online]. Praha, 2019 [cit. 2019-03-23]. Dostupné z URL: <http://www.iso27000.cz/rac/homepage.nsf/CZ/27002>.

[13] ISO/IEC 27002:2013. *ISO27k information security* [online]. New Zeland: IsecT, 2019 [cit. 2019-03-23]. Dostupné z URL: <http://www.iso27001security.com/html/27002.html?fbclid=IwAR3S_iPUxTHAUCwwDatLit0VTku3DEBSNszXLqDNPu9emzbA4Hm-aShZ6BY>.

[14] ISO/IEC 27030. *ISO27k information security* [online]. New Zeland: IsecT, 2019 [cit. 2019-03-23]. Dostupné z URL: <http://iso27001security.com/html/27030.html>.

[15] NERC CIP Compliance Consultants: Compliance analysis and certification, we can help. *Cybersecurity Services & Managed Network Security Services - RSI Security* [online]. San Diego, 2019 [cit. 2019-03-23]. Dostupné z URL: <https://www.rsisecurity.com/compliance-advisory-services/nerc/>.

[16] Cybersecurity Blog - Network Security Blog | RSI Security. *NERC CIP STANDARDS: WHAT YOU NEED TO KNOW* [online].San Diego: RSI Security, 2018 [cit. 2019-03-23]. Dostupné z URL: <https://blog.rsisecurity.com/nerc-cip-standards-what-you-need-to-know>.

[17] *In: Standard CIP-001-1 — Sabotage Reporting: Sabotage Reporting*[online]. Atlanta: The North American Electric Reliability Corporation, 2006 Dostupné z URL: <https://www.nerc.com/files/CIP-001-1.pdf>.

[18] ISA/IEC 62443 (ISA-99). *The International Society of Automation*[online]. 2012 [cit. 2019-04-04]. Dostupné z URL: <https://www.isa.org/templates/two-column.aspx?pageid=124560>.

[19] BYRES, Eric. Using ANSI/ISA-99 Standards for SCADA Security (plus White Paper). *Tofino Industrial Security Solution*[online]. 2017 [cit. 2019-04-04]. Dostupné z URL: <http://isaeurope.com/iec62443/>.

[20] ANDERSON, Erin. A Four Step Guide to Secure Your ICS Network Using ISA 99/IEC 62443. *SecurityMatters* [online]. San Jose: SecurityMatters Americas, 2017 [cit. 2019-04-04]. Dostupné z URL: <https://www.tofinosecurity.com/blog/using-ansiisa-99-standards-scada-security-plus-white-paper>.

[21] FORMÁNEK, David. *Zranitelnosti typu injekce: SQL injekce* [online]. www.root.cz, 11-10-2018 [cit. 2019-05-23]. Dostupné z URL: <https://www.root.cz/clanky/zranitelnosti-typu-injekce-sql-injekce/>

[22] PRAVDA, Ivan *Nové trendy v elektronických komunikacích PLC, BPL - Využívání silnoproudových vedení a sítí pro přenos zpráv* [online]. Praha: České vysoké učení technické v Praze [cit. 07-12-2018]. Dostupné z URL: <https://publi.cz/books/256/Cover.html>.

[23] Národní úřad pro kybernetickou a informační bezpečnost. *Minimální požadovky na kryptografické algoritmy*, doporučení v oblasti kryptografických prostředků Verze 1.0, platná ke dni 28.11.2018 [online]. [cit. 2-3-2019]. Dostupné z URL: <https://www.govcert.cz/download/uredni-deska/Kryprografické%20prost%C5%99edky/Kryptograficke_prostredky_doporuceni_v1.0.pdf>.

[24] HODGES, Jeff, Adam BARTH a Collin JACKSON. *RFC 6797 – HTTP Strict Transport Security*. IETF Tools [online]. Carnegie Mellon University, 2008, 2008 [cit. 2019-03-29]. Dostupné z URL: <https://tools.ietf.org/html/rfc6797#page-16>.

[25] Národní úřad pro kybernetickou a informační bezpečnost. *BEZPEČNOSTNÍ DOPORUČENÍ NCKB PRO ADMINISTRÁTORY 2.0*, [online]. [cit. 2-4-2019]. Dostupné z URL: <https://www.govcert.cz/download/doporuceni/container-nodeid-1259/NUKIB_doporuceni_admin_2.0_cernobile.pdf>.

[26] SOREBO, Gilbert N. a Michael C. ECHOLS. *Smart Grid Security: An End-to-End View of Security in the NewElectrical Grid*. CRC Press, 2011. ISBN 9781439855874.

Seznam symbolů, veličin a zkratek

LPWAN	Low-Power Wide-Area Network
IoT	Internet of Things
kB	Kilobyte
HMAC	Hash-based Message Authentication Code
DES	Data Encryption Standard
AES	Advanced Encryption Standard
IS	Informační systém
NIS	Network and Information System
ECB	Electronic Codebook
PCBC	Propagating Cipher Block Chaining
SHA1	Secure Hash Algorithm 1
ISO/IEC	International organization for standardization/Internatinal electrotechnical commission
ISMS	Information security management system
ISO	International organization for standardization
IEC	Internatinal electrotechnical commission
NERC – CIP	North American Electric Reliability Corporation – Critical Infrastructure Protection
NERC	North American Electric Reliability Corporation
CIP	Critical Infrastructure Protection
ISA99 / IEC	The International Society of Automation / International Electrotechnical Commission
ISA	The International Society of Automation
TCP	Transmission Control Protocol
CVE	Common Vulnerabilities and Exposures
NIST	National Institute of Standarts and Technology
OWASP	About The Open Web Application Security Project
ZAP	Zed Attack Proxy
SQL	Structured English Query Language
UDP	User Datagram Protocol
BPL	Broadband over Power Lines
SFP	Small Form factor Pluggable
NAT	Network Address Translation
HTTPS	Hypertext Transfer Protocol Secure
TLS	Transport Layer Security
MD5	Message-Digest algorithm
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost

RSA	Rivest–Shamir–Adleman
SHA2	Secure Hash Algorithm 2
HTTP	Hypertext Transfer Protocol
CPU	Centrální procesorová jednotka
MAC	Media Access Control
PID	Process identifier
HSTS	HTTP Strict Transport Security
SSH	Secure Shell
VPN	Virtuální privátní síť
NFC	Near Field Communication
PLC	PowerLine Communication
HTML	HyperText Markup Language
NAT	Network address translation
SNMP	Simple Network Management Protocol
IPv4	Internet Protocol version 4
DoS	Denial of Service
DDoS	Distributed Denial of Service

Seznam příloh

A Certifikát webové aplikace u výrobce číslo 1

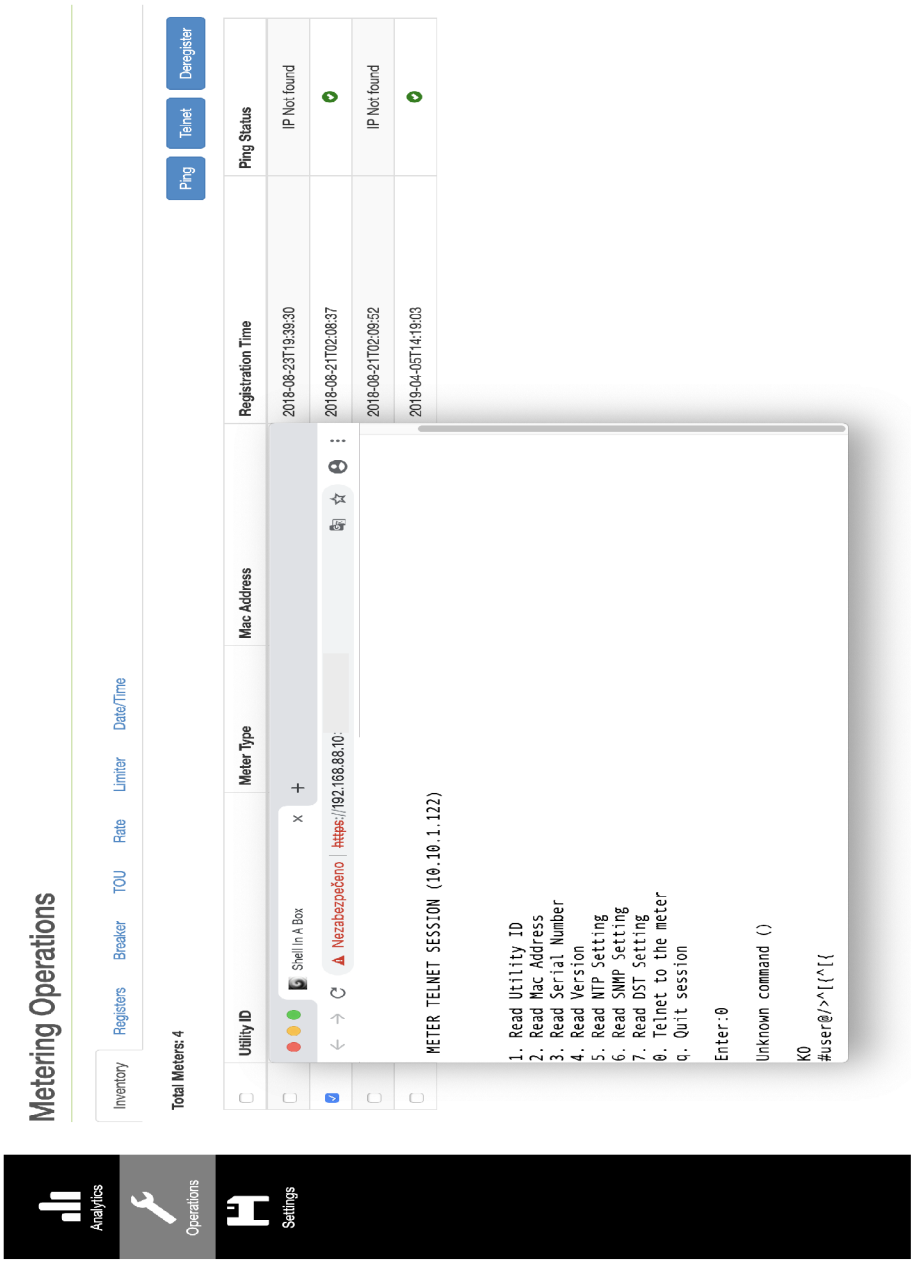
Algoritmus podpisu	SHA-1 se šifrováním RSA (1.2.840.113549.1.1.5)
Parametry	Žádný
Neplatné před	středa 9. července 2014 17:08:49 Středoevropský letní čas
Neplatné po	čtvrtek 9. července 2015 17:08:49 Středoevropský letní čas
Informace o veřejném klíči	
Algoritmus	Šifrování RSA (1.2.840.113549.1.1.1)
Parametry	Žádný
Veřejný klíč	128 bajtů : D1 4C E0 41 F2 E5 78 AA ...
Exponent	65537
Velikost klíče	1 024 bitů
Použití klíče	Jakékoli
Podpis	128 bajtů : 3B AF A9 3A B7 D8 A7 1D ...
Rozšíření	Základní omezení (2.5.29.19)
Kritické	NE
Certifikační autorita	ANO
Rozšíření	Identifikátor klíče subjektu (2.5.29.14)
Kritické	NE
ID klíče	D4 6E 15 83 36 24 93 BA 12 25 D5 C9 16 63 67 71 CB 7D 15 EA
Rozšíření	Identifikátor klíče autority (2.5.29.35)
Kritické	NE
ID klíče	D4 6E 15 83 36 24 93 BA 12 25 D5 C9 16 63 67 71 CB 7D 15 EA
Otisky	
SHA-256	D3 E5 1E 83 A6 6F 88 CD 3D EE 02 38 19 3A 55 4A E3 43 9F F0 84 7E 8C 6E E7 1B 9E CB 7F CE 5F 6F
SHA-1	A3 BD 67 3B 71 59 8B 18 03 B4 33 DF F1 A6 2A 00 28 2C 73 A3

B Odpověd webové aplikace typu 404

Not Found

Error: The requested address **'/dsafasdgasfd?url=%2Fdsafasdgasfd'** was not found on this server.

C Stránka Metering



D Služba Shell In A Box s možností 2

```
 METER TELNET SESSION (10.10.1.122)


1. Read Utility ID
2. Read Mac Address
3. Read Serial Number
4. Read Version
5. Read NTP Setting
6. Read SNMP Setting
7. Read DST Setting
0. Telnet to the meter
q. Quit session

Enter:2
2
execute echo "sys mac g"; sleep 1
FIRMWARE VERSION

 running
Compiled on Tue Oct 10 01:49:44 CEST 2017


Entering character mode
Escape character is '^]'.

          ---------------------
            Type 'h' for help
          ---------------------

Password:


Entering line mode
Escape character is '^C'.

OK
MAC Address:

OK
#admin@/>

1. Read Utility ID
2. Read Mac Address
3. Read Serial Number
4. Read Version
5. Read NTP Setting
6. Read SNMP Setting
7. Read DST Setting
0. Telnet to the meter
q. Quit session

Enter:
```

E Zachycené administrátorské heslo

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.0.1	10.10.1.158	TCP	74	53281 → 40000
2	0.095964	10.10.1.158	10.10.0.1	TCP	64	40000 → 53281
3	0.096155	10.10.0.1	10.10.1.158	TCP	54	53281 → 40000
4	0.096566	10.10.0.1	10.10.1.158	TCP	65	53281 → 40000
5	0.112884	10.10.1.158	10.10.0.1	TCP	64	40000 → 53281
6	0.112962	10.10.1.158	10.10.0.1	TCP	67	40000 → 53281

Wireshark · Follow TCP Stream (tcp.stream eq 0) · biolek.c

```
mode admin
Password:.....


OK

#admin@/>.....sys mac g

MAC Address:

OK
#admin@/>quit
```

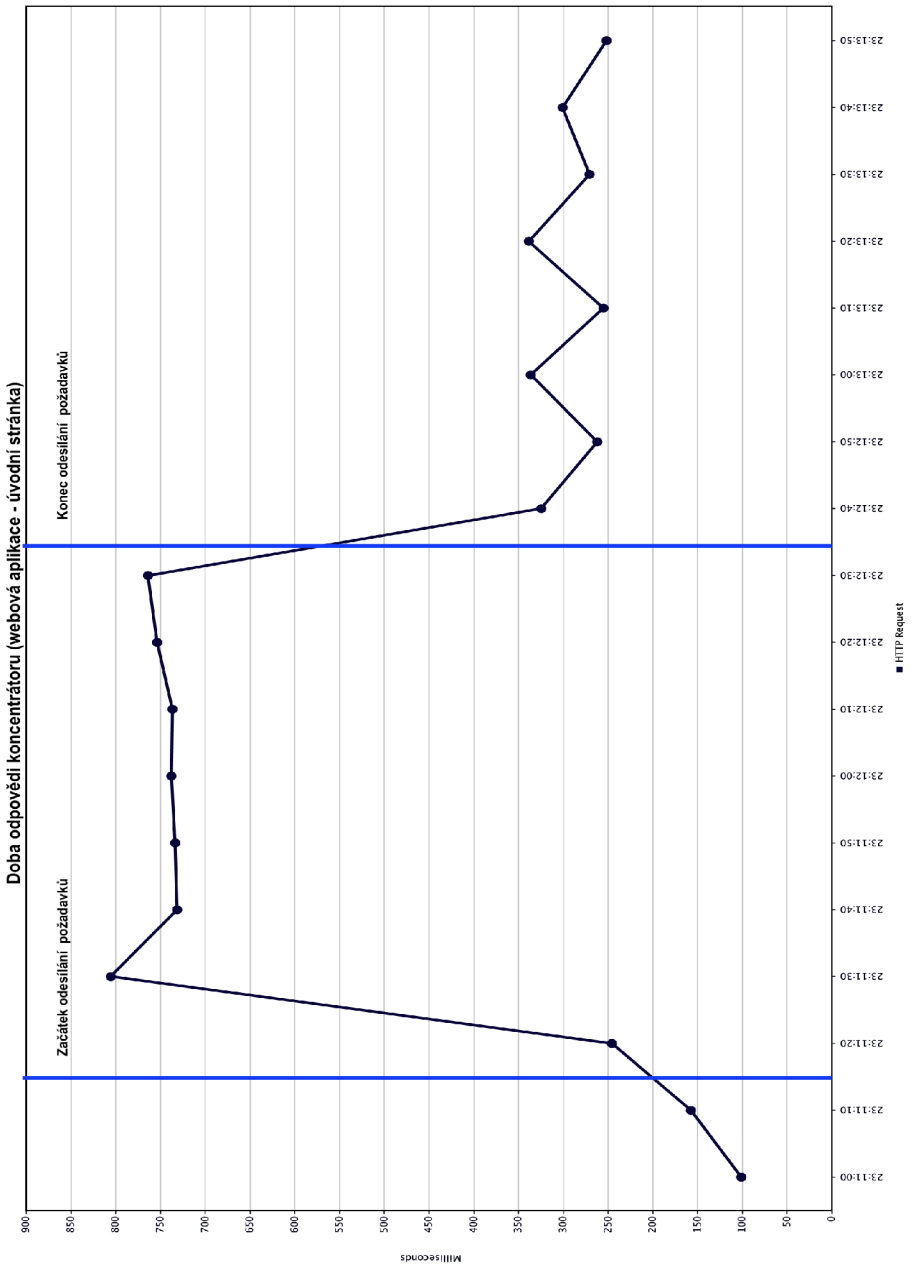
F Certifikát webové aplikace ADD Group

Router8
Kořenová certifikační autorita
Platnost vyprší: sobota 9. května 2026 10:58:13 Středoevropský letní čas
Certifikát „Router8“ není důvěryhodný

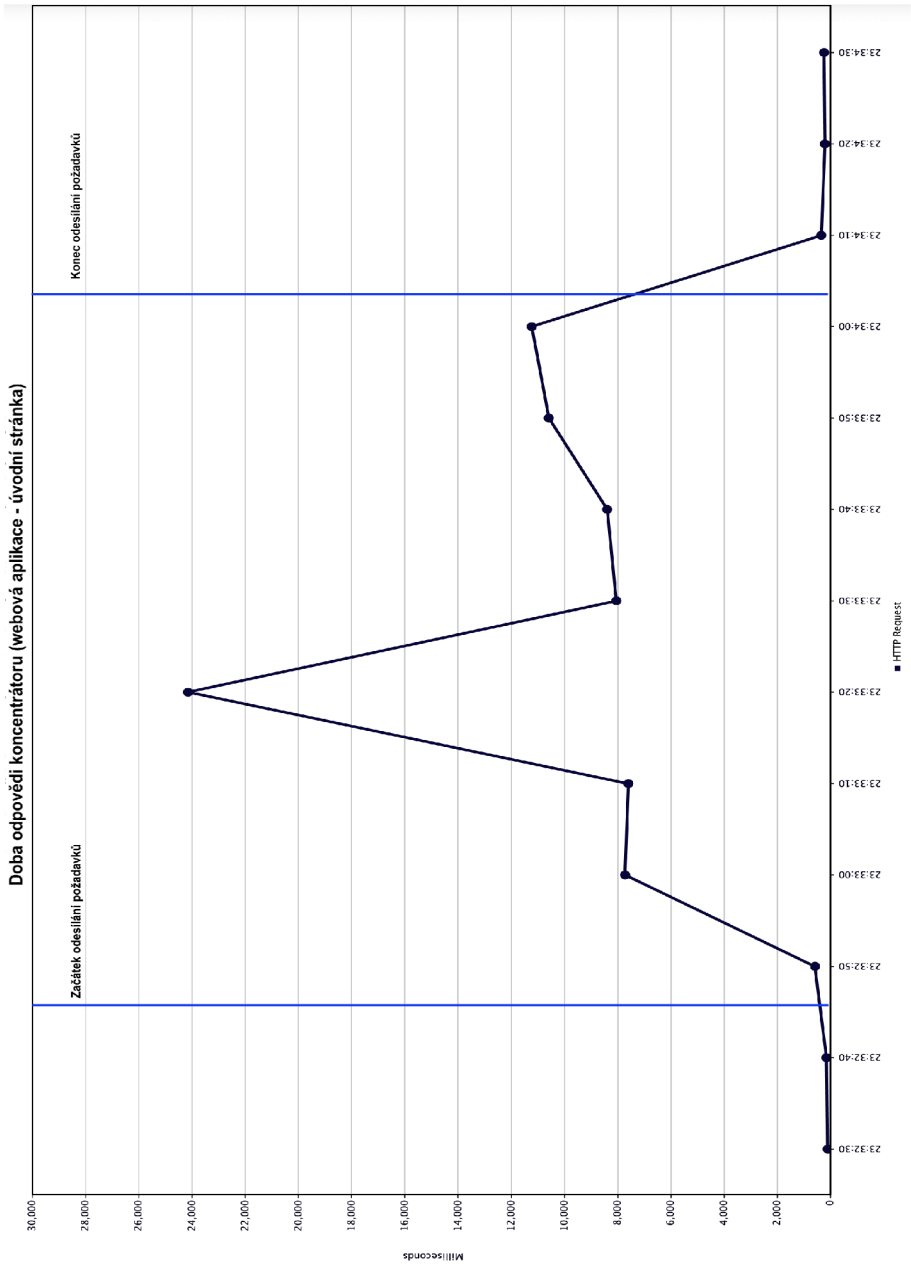
▼ **Podrobnosti**

Název subjektu	
Země/oblast	MD
Stát/kraj	Chisinau
Lokalita	Chisinau
Organizace	ADD-Technology SRL
Jednotka organizace	R&D Department
Obecný název	Router8
E-mailová adresa	service@addgrup.com
Název vystavitele	
Země/oblast	MD
Stát/kraj	Chisinau
Lokalita	Chisinau
Organizace	ADD-Technology SRL
Jednotka organizace	R&D Department
Obecný název	Router8
E-mailová adresa	service@addgrup.com
Sériové číslo	00 C1 E7 35 23 FB 76 00 76
Verze	3
Algoritmus podpisu	SHA-256 se šifrováním RSA (1.2.840.113549.1.1.11)
Parametry	Žádný
Neplatné před	středa 11. května 2016 10:58:13 Středoevropský letní čas
Neplatné po	sobota 9. května 2026 10:58:13 Středoevropský letní čas
Informace o veřejném klíči	
Algoritmus	Šifrování RSA (1.2.840.113549.1.1.1)
Parametry	Žádný
Veřejný klíč	512 bajtů : D1 D2 F0 4B 94 9E 4E 44 …
Exponent	65537
Velikost klíče	4 096 bitů
Použití klíče	Jakékoli
Podpis	512 bajtů : 52 A8 67 40 FC 0C 21 84 …
Rozšíření	Základní omezení (2.5.29.19)
Kritické	NE
Certifikační autorita	ANO
Rozšíření	Identifikátor klíče subjektu (2.5.29.14)
Kritické	NE
ID klíče	67 B6 2C EF 8A 47 FE B4 19 3F F3 38 C6 CD 51 48 6E B0 3D 17
Rozšíření	Identifikátor klíče autority (2.5.29.35)
Kritické	NE
ID klíče	67 B6 2C EF 8A 47 FE B4 19 3F F3 38 C6 CD 51 48 6E B0 3D 17
Otisky	
SHA-256	F0 D7 D5 2B 11 A2 B7 51 1B 56 EB EF 54 74 0A 13 4C 83 8E 47 38 B9 70 93 05 E0 D6 CF 81 6E 37 7D
SHA-1	7A C0 48 AD FA 7C 6B 6A 20 2B BD EB B3 D6 95 71 5F 1F 77 68

G Graf 10 požadavků současně



H Graf 200 požadavků současně



I Alternativní spojení při Low and Slow