VŠB TECHNICKÁ UNIVERZITA OSTRAVA

T A
Č R

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Výzkumná zpráva (O - Ostatní)

Číslo projektu: **TK03010091**
Název projektu: **Dopady kybernetické bezpečnosti na regulované oblasti smart meteringu**

Název hlavního řešitele: Vysoká škola báňská - Technická univerzita Ostrava
17. listopadu 2172/15
Ostrava-Poruba 708 00

Další účastník projektu: Vysoké učení technické v Brně
Antonínská 548/1
Brno-střed 601 90

Aplikační garant projektu: Energetický regulační úřad
Masarykovo Nám. 5
Jihlava 586 01

VŠB TECHNICKÁ UNIVERZITA OSTRAVA

T A
Č R

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Obsah

Manažerské shrnutí

Kapitola 1 analyzovala regulační rámec v rámci kybernetické bezpečnosti. Z pohledu projektu byla jako hlavní regulační oblast označena "Regulace cen, ochrana zájmů zákazníka a spotřebitelů", jedná se především o regulaci cen, kde vstupují do ceny informační či komunikační technologie, kde je kybernetická bezpečnost součástí. Dále se jedná o ochranu zájmů zákazníka a spotřebitele, kde kybernetická bezpečnost jasně ovlivňuje tyto zájmy mj. z pohledu soukromí. **Doporučení pro ERÚ:** Vzhledem k nutnosti zapojení zákazníka k chytrému elektroměru, podporovat/regulovat předávaní dat na zákaznickém rozhraní elektroměru v zabezpečené podobě.

Kapitola 2 jen souhrnně uvedla komunikační technologie, kdy pro nadcházející rollout jsou uvažovány bezdrátové technologie na principu bod-bod. **Doporučení pro ERÚ:** Chybí definice sekundárních technologií pro zákaznické rozhraní. Byl představen konsensus distribučních společností v rámci NAP SG, ale nepromítl se do legislativy. Výrobci a trh tedy nemají jasné noty a specifikaci (viz diskutované napájení na zákaznickém rozhraní).

Kapitola 3 se zabývala analýzou kybernetických rizik elektroměrů. **Doporučení pro ERÚ:** Z pohledu spotřebitele je zde stále nevyřešena otázka soukromí, osobních či citlivých údajů, kdy chybějící analýza a jasná direktiva/legislativa v ČR chybí. Prozatím doporučujeme se opírat obecně o GDPR, tedy aby elektroměru nebylo možné vyhodnotit chování zákazníka (např. že není doma – možnost krádeže).

Kapitola 4 Analýza ekonomických dopadů pomocí ekonomického modelu čisté současné hodnoty vyčíslila ekonomické dopady na regulované oblasti (cenu chytrého elektroměru vzhledem ke kybernetické bezpečnosti). Na základě požadavků na kybernetickou bezpečnost chytrých elektroměrů a související infrastruktury (vyhláška, DLSM SS a NAP SG) je zřejmé, že současné elektroměry (nasazované v posledních 10 letech bez zabezpečení či jen s DLMS SS 0) nebude možné využít a je nutný HW a SW redesign. Tuto problematiku dopadu vlivu kybernetické bezpečnosti na cenu elektroměrů analyzuje kapitola 4 s těmi to závěry:

- Z výstupů ekonomického modelu čisté současné hodnoty (NPV) lze vidět, že by cena nových chytrých elektroměrů s DLMS SS2 musela být více než dvojnásobná oproti stávajícím elektroměrům, aby byl model negativní/záporný.
- Výrazný dopad do ceny mají datové tarify, kdy datový objem na základě reálných měření bude až o 50 % vyšší a to způsobí snížení NPV o 1-2 mil. EUR.
- Klíčovým bodem ekonomického modelu je stanovení přínosů eliminace rizik a útoků souvisejících s kybernetickou bezpečností. Pro náš definovaný model lze konstatovat, že pokud by přínosy odvrácení rizik kybernetické bezpečnosti (např. útoků) byly nižší než 3mil EUR byla by čistá současná hodnota NPV záporná a tím investice nerentabilní.

Na základě analýzy ekonomických dopadů lze stanovit tyto doporučení pro ERÚ:

- Naplnění bezpečnostních požadavků vzhledem k rizikům útoků a narušení vyžaduje testování a ověřování splnění bezpečnostních požadavků nezávislými autoritami před nasazením (např. testy VUT při výběrovém řízení Smaragd pro E.ON, certifikační schéma, nutnost testování kvůli problematice Čínských dodavatelů).
- Rizika související s nedodržením požadavků na kybernetickou bezpečnost definovaná v ekonomickém modelu jako finanční přínosy zcela pokryjí zvýšené náklady na implementaci bezpečnosti.
- Klíčovým bodem nasazení chytrých elektroměru a související infrastruktury je reálné laboratorní testování naplnění požadavků kybernetické bezpečnosti nezávislou autoritou v rámci výběrového řízení. VUT v kooperaci se všemi distributory v rámci NAP SG definovaly 45 požadavků a postupů testování pro bezpečnost chytrých elektroměrů, tyto testy je nutné provést před samotným nasazením, jinak hrozí možná rizika definovaná v modelu (finanční ztráty, porušení legislativy či GDPR, poškození zákazníka, jména firmy či odpojení zákazníka).
- Cena testování kybernetických požadavků jednoho výrobce se pohybuje v řádu stovek tisíc korun, což vzhledem k výši investice (pořízení stovky ticích elektroměrů za stovky miliónů) je zcela zanedbatelná a přidaná hodnota výsledků je obrovská (reálné zkušenosti s testováním VUT-E.ON).
- VUT doporučuje testovat všechny požadavky, klíčové požadavky které mají dopad 80 % jsou:
  - Minimální kryptografické požadavky dle vyhlášky.
  - Vzdálená aktualizace kryptografických pověření.
  - Dostatečné budoucí prostředky (RAM, flash a výpočetní výkon) pro aktualizaci bezpečnostních funkcionalit a kryptografických primitiv po celou dobu životního cyklu elektroměru.
  - Vzdálená aktualizace bezpečnostních funkcionalit a kryptografických primitiv.

Kapitola 5 provedla analýzu legislativního rámce pro kybernetickou bezpečnost chytrých elektroměrů. **Doporučení pro ERÚ:** Příloha č. 4 k vyhlášce č. 359/2020 Sb. definovala požadavky na kryptografické a technické požadavky elektroměrů, tím vznikl český standart/doporučení a jasné pravidla. Toto je vzor i pro další oblasti (např. zákaznické rozhraní, definice primární komunikační technologie, datový model).

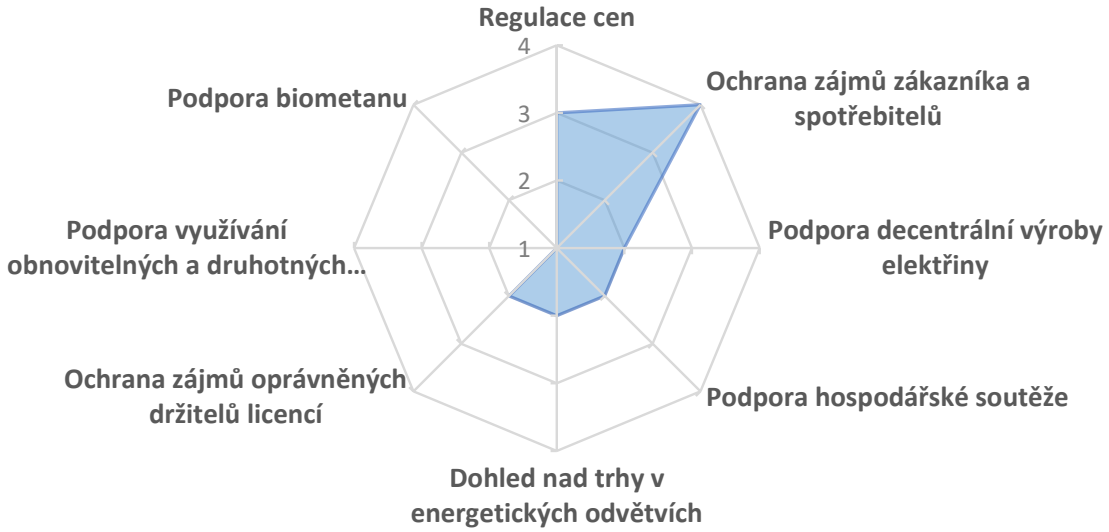
1 Stanovení základního regulačního rámce v rámci kybernetické bezpečnosti

I přes jasnou definici působnosti ERÚ v čase, místě i oblasti, bylo nutné definovat jednotlivé oblasti působnosti ERÚ z důvodu napojení na nově přicházející oblast kybernetické bezpečnosti v energetice a kritické i nekritické energetické infrastruktuře. Identifikace jednotlivých oblastí resp. regulačních nástrojů a jejich navázání na kybernetickou bezpečnost by měla následně dopomoci k lepšímu pochopení jednotlivých vazeb kybernetické bezpečnosti na operační i kapitálové náklady či obecně vliv kybernetické bezpečnosti na regulovanou i neregulovanou část ceny elektrické energie, společně s pochopením pozice ERÚ v rámci kontroly splnění požadavků zákona a běžné bezpečnostní praxe.

Z tohoto důvodu byla provedena analýza legislativy a příbuzných směrnic i doporučení v rámci ČR a EU, kde byl identifikován základní regulační rámec, který vychází z podstaty Energetického regulačního úřadu ČR (ERÚ). Samotná působnost ERÚ pak vychází z čl. 79 odst. 1 ústavního zákona č. 1/1993 Sb. Ústavy ČR, kde hlavní působnost pak vymezuje par. 17 odst. 4 energetického zákona, společně se zákonem č. 458/2000 Sb. (a dalších zákonů mj. č. 165/2012 o podporovaných zdrojích energie a o změně některých zákonů, č. 552/1991 Sb. o státní kontrole; č. 320/2001 Sb. o finanční kontrole ve veřejné správě. resp. č. 211/2011 Sb.; a dalších). Základní regulační rámec je definován dle jednotlivých rolí v rámci hlavních oblastí působnosti:

- Regulace cen,
- ochrana zájmů zákazníka a spotřebitelů,
- podpora decentralizované výroby elektřiny,
- podpora hospodářské soutěže,
- dohled nad trhy v energetických odvětvích,
- ochrana zájmů oprávněných držitelů licencí,
- podpora využívání obnovitelných a druhotných zdrojů energie,
- podpora biometanu.

Z pohledu projektu byla jako hlavní regulační oblast označena "Regulace cen, ochrana zájmů zákazníka a spotřebitelů". Dále jako vedlejší oblast "Podpora hospodářské soutěže, dohled nad trhy v energetických odvětvích, ochrana zájmů oprávněných držitelů licencí". Okrajově se pak projekt dotýká oblasti "Podpora decentralizované výroby elektřiny". V neposlední řadě pak projektem není zastoupena regulační oblast "Podpora využívání obnovitelných a druhotných zdrojů energie, podpora biometanu". Z tohoto pohledu pak lze vidět na grafu níže propojení jednotlivých regulačních oblastí veřejné správy s obsahem projektu.



Obrázek 1: Identifikovaná úroveň souvislosti projektu a jeho případného dopadu na jednotlivé regulované oblasti

Hodnocení bylo provedeno semi-kvantitativní metodou pro kybernetickou bezpečnost a jednotlivé oblasti působnosti ERÚ dle hodnocení:

- 1 b. - Není součástí regulované oblasti. *Kybernetická bezpečnost má minimální či žádný vliv na regulační nástroje či regulovanou oblast,* např. v rámci oblasti podpory biometanu je zřejmý mizivý efekt projektu.
- 2 b. - Nepřímá součást regulované oblasti či její části. *Kybernetická bezpečnost není přímou součástí a její vliv je převážně pasivní (nepřímý),* např. v oblasti podpory hospodářské soutěže je nutno dodržet jasná minimální pravidla pro kybernetickou bezpečnost pro dodržení rovných tržních podmínek.
- 3 b. - Přímá (klíčová) součást dílčí části regulované oblasti. *Jedná se o případy, kdy kybernetická bezpečnost není hlavní oblastí zájmu, ale i přesto svým účinkem aktivně vstupuje do ovlivnění dané oblasti*, např. se jedná o regulaci cen, kde vstupují do ceny informační či komunikační technologie, kde je kybernetická bezpečnost součástí.
- 4 b. - Přímá (klíčová) součást regulované oblasti. *Jedná se o oblasti, kde je jasná přímá souvislost s hlavní náplní oblasti,* např. se jedná o ochranu zájmů zákazníka a spotřebitele, kde kybernetická bezpečnost jasně ovlivňuje tyto zájmy mj. z pohledu soukromí.

2 Analýza a výzkum komunikačních technologií a přenosových technologií

V rámci komunikačních protokolů se lze setkat s následujícími: Modbus, DLMS/COSEM a IEC-60870-5-104 či IEC-60870-5-101. V rámci primární komunikace je uvažována převážně technologie DLMS/COSEM, kde pro sekundární rozhraní lze použít ostatní technologie - seriovou Modbus RTU či IEC-60870-5-101 či TCP/IP spojení v rámci Modbus TCP či IEC-60870-5-104.

Komunikační protokoly přímo nespecifikují použití určitého přenosového media a komunikační technologie. V rámci přenosových technologií byla provedena analýza využívaných technologií v rámci Evropy. Identifikovány byly v rámci chytrého měření pro primární rozhraní následující technologie uvedené v tabulce níže.

Typ	Technologie	Standardizace
Optika	OM1, OM2, OM3, OM4	Ano
Kabel	10/100/1000/2.5G/5G/10G/25G/40G Base	Ano
PLC (Broad)	Homeplug 1.0, Homeplug AV, Homeplug, Green PHY, HD-PLC, UPA Powermax, IEEE1901, ITU-T G.hn	Ano
PLC (Narrow)	G3-PLC, PRIME, IEEE P1901.2, ITU-T G.hnem, IEC61334, ANSI/EIA 709.1.2	Ano
Serial	RS232, RS485, m-bus	Ano

Tabulka 1: Kabelové přenosové technologie využívané/uvažované v rámci Evropy pro chytré měření.

Typ	Technologie	Standardizace
Celulární	2G (GSM, GPRS, GPRS+, EDGE)	Ano
	3G (UMTS, HSDPA, LTE)	Ano
	4G (LTE A, NB-IoT, LTE Cat M)	Ano
	5G (5G-NR)	Ano
802.15	ZigBee, 6LoWPAN, Bluetooth	Ano
802.11	IEEE 802.11n, Enhanced WiFi, WiFi	Ano
802.16	WiMAX	Ano
LPWA	LoRaWAN, Sigfox	ne
Ostatní	RF MESH, Wireles-m-bus, Wimax	Částečně

Tabulka 2: Bezdrátové přenosové technologie využívané/uvažované v rámci Evropy pro chytré měření.

2.1 Komunikační technologie

V ČR je nad rámec ostatních technologií specifikum HDO v rámci chytrých sítí, v rámci chytrého měření pak je to z pohledu komunikačních technologií celkově jednoznačná situace, kde je hlavním volba protokol DLMS/COSEM pro primární rozhraní. Z bezpečnostní analýzy provedené v rámci NÚKIB a NIST pro protokol DLMS/COSEM lze doporučit využívání následujících úrovní bezpečnosti.

Druh autentizace	Mechanism_id
HLS s využitím GMAC	5
HLS s využitím SHA-256	6
HLS s využitím EC-DSA	7

Tabulka 3: Doporučené úrovně využívání High Level Security (HLS) DLMS / COSEM.

Security Suite	Autentizované šifrování	Digitální podpis	Ustanovení klíče	Hash Hash	Přenos klíče
1	AES-GCM-128	ECDSA P-256	ECDH P-256	SHA-256	AES-128 key wrap
2	AES-GCM-256	ECDSA P-384	ECDH P-256	SHA-384	AES-256 key wrap

Tabulka 4: Doporučené úrovně DLMS Security Suite.

2.2 Přenosové technologie

Pro Českou republiku jsou v rámci chytrého měření nejčastěji uvažovány **celulární technologie** (převážně pak GPRS, GPRS+, EDGE, UMTS, HSDPA, LTE, LTE A a NB-IoT), příp. ve specifických případech pak i LPWA (konkrétně LoRaWAN). Tyto technologie jsou aktuálně z dostupných zařízení nejvyspělejší a jsou testovány v reálně praxi – produkční provoz mobilními operátory. Z pohledu zákaznického (sekundárního) rozhraní pak lze uvažovat převážně sériové rozhraní RS-232 a RS-485 či např. i (wireless) m-bus.

Přenosové technologie ve většině případů neposkytují bezpečnost typu konec-konec (end-to-end), kdy je nutno nad rámec vlastních bezpečnostních algoritmů vytvořit vždy nadstavbu v rámci komunikační technologie či poskytnout nejlépe aditivní ochranu prostřednictvím dostupných bezpečnostních prvků (např. zabezpečení na vyšších vrstvách komunikace).

Z pohledu odběratele je pak zajištění plné kybernetické bezpečnosti velmi složitou otázkou - převážně pak z pohledu soukromí, jelikož samotný uživatel nebude mít nikdy pod svou správou např. kryptografické klíče v rámci komunikace elektroměru a primárního rozhraní (prakticky nelze zabezpečit kvůli vlastnictví a zodpovědnosti distributora), tedy nemá ani pod kontrolou přímo "svá"data, která jsou elektroměry sbírána. Z tohoto důvodu je nutné zabývat se otázkou GDPR z pohledu elektroměrů, otázkou soukromí a vlastnictví měřených dat, stejně jako otázkami životního cyklu těchto dat – tedy od jejich sběru, uložení, množení či smazání.

3 Analýza a výzkum kybernetických rizik elektroměrů

Pokud uvažujeme pouze stranu distributora elektrické energie (provozovatele), pak lze přistoupit k definici aktiv v rámci chytrého měření následovně [1]:

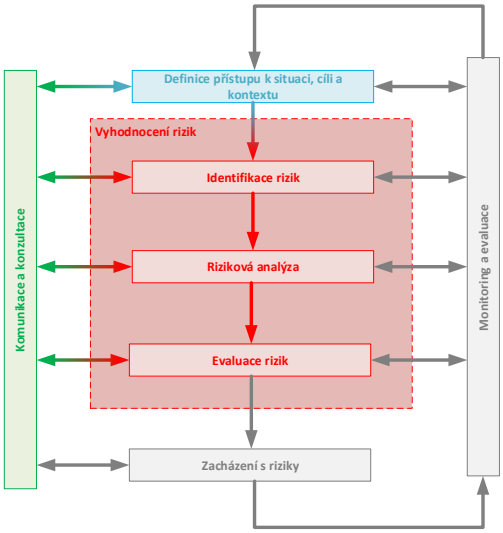
- Hlavní aktivum: Plná funkčnost vzdáleného odečtu.
- Funkcionality odečtu: Jedinečné ID elektroměru, časová značka, naměřená hodnota spotřeby.
- Funkcionality řízení: Jedinečné ID elektroměru, kód zprávy.
- Hlavní požadavky: CIA triáda, tedy Důvěrnost (Pouze autorizovaná osoba může číst data), Integrita (Pouze autorizovaná osoba může měnit data), Dostupnost (Většina požadavků míří k 99,5 % či 99,5 % a výše).
- Nejkritičtější požadavek: Integrita.

Z pohledu vyhodnocení rizik je nutno přistoupit k problematice komplexně. Z tohoto pohledu byla provedena analýza dostupných obecných metod vyhodnocení rizik se zaměřením na vhodnost pro oblast Smart Metering (SM). Z tohoto pohledu je poskytnuto know-how vlastností jednotlivých metod a doporučeno průběžné vyhodnocování externích i interních rizik v rámci SM. Vize viz tabulka níže [1].

	CRAMM	IS1	RiskSafe	NIST SP800-30	OCTAVE Allergo	IT-Grundschutz
Původ	UK	UK	UK	US	US	DE
Hodnocení	Kval.	Kval.	Kval.	Kval.	Semi-Kvan.	Kval.
Expertiza	Velmi Vysoká	Vysoká	Střední	Střední	Střední	Střední
Jazyk	AJ, CZ	AJ	AJ	AJ	AJ	AJ, NJ
Cena	Placen	Zdarma	Placen	Zdarma	Zdarma	Zdarma
Standard	ISO/IEC IS 17799	ISO 27001	ISO 27001, ISO 27005	-	-	ISO/IEC IS 17799/27001
Aktuálnost k	2003	2012	2012	2002	2007	2005
Detail	Vysoký	Nízký	Vysoký	Střední	Střední	Vysoký
Vhodnost pro SM	NE	ANO	ANO	ANO	ANO	ANO

Tabulka 5: Analýza dostupných metod pro vyhodnocení rizik.

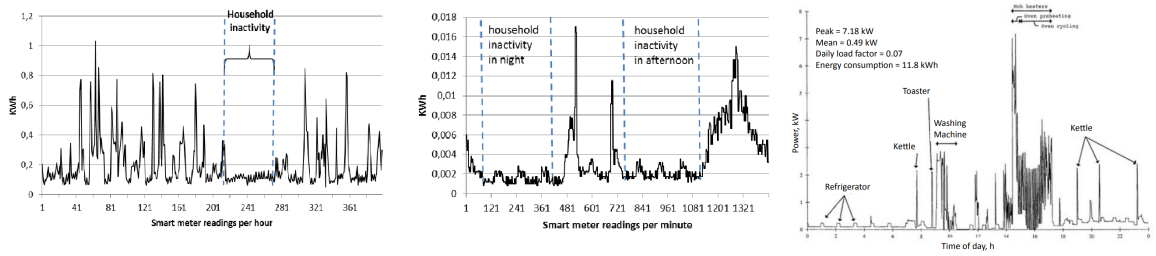
RiskSafe dle ISO/IEC 27005 a IEC 27001 se jeví jako ideálním kandidátem vzhledem k aktuálnosti metodiky, vysoké míře detailu analýzy a potřebné pouze střední odbornosti pro vyhodnocení rizik. Nicméně samotná metodika je placená, kde vyžadování tímto směrem by bylo nutno vždy zahrnout do nákladů. S přihlédnutím k předpokladu nutnosti průběžné analýzy rizik, díky měnícímu se prostředí, hrozbám a dalším. Obecně však dle ISO/IEC 27005 lze postupovat podle navržené metodiky níže.



Obrázek 2: Navržená metodika rizikové analýze dle ISO/IEC 27005 pro oblast Smart Meteringu

Metodika je rozdělena na pět hlavních částí: (i) Mopnitoring a evaluace, (ii) Definice přístupu k situaci, cíli a kontextu, (iii) Vyhodnocení rizik, (iv) Komunikace a konzultace a (v) Zacházení s riziky. Takto sestavená metodika by měla být dostačující k provedení základního přehledu rizik. Samotná výsledná riziková analýza pak může být provedena kterýmkoliv vhodným prostředkem uvedeným v tabulce výše. **Z pohledu regulátora by měla být požadována riziková analýza vždy ve chvíli, kdy jsou požadovány úhrady nákladů z pohledu bezpečnosti či mitigace rizik, tedy tak, aby náklady byly obhajitelné a hrozba, kterou náklady mitigují skutečná.** Ideálním stavem v tomto případě je, pokud bude regulátor tlačit na vytvoření legislativy pro rizikovou analýzu vyhodnocující kybernetická rizika v rámci chytrého měření.

Z pohledu aktuálních dostupných doporučení mj. v rámci "Bezpečnostních požadavků na měřidla a související infrastrukturu"[2] z pohledu distributora (provozovatele) lze tvrdit, že většinu kritických rizik lze mitigovat pomocí kryptografických funkcí, které jsou mj. doporučovány i v rámci NAP SG. **Nicméně je nutno se soustředit například i na problematiku Smart Meteringu - chytrých elektroměrů z pohledu spotřebitele. Zde je stále nevyřešena otázka soukromí, osobních či citlivých údajů, kdy chybějící analýza a jasná direktiva/legislativa v ČR chybí. Prozatím se doporučení opírají o obecné GDPR, nicméně problematiku např. vyhodnocování chování, viz obrázky níže. chybí.**



Obrázek 3: Analýza běžné domácnosti a vyhodnocení aktivity [3, 4].

4 Analýza ekonomických dopadů

4.1 Manažerské shrnutí

Na základě požadavků na kybernetickou bezpečnost chytrých elektroměrů a související infrastruktury (vyhláška, DLSM SS a NAP SG) je zřejmé, že současné elektroměry (nasazované v posledních 10 letech bez zabezpečení či jen s DLMS SS 0) nebude možné využít a je nutný HW a SW redesign. Tento redesing má výrazný dopad do ceny řešení, což diskutují a analyzují následující kapitoly s těmito hlavními závěry:

- Současné elektroměry na trhu a související infrastruktura (komunikace a centrála) nejsou připraveny pro plné nasazení bezpečnostních požadavků – vyžaduje vývoj a tím zvýšení ceny.
- Naplnění bezpečnostních požadavků vzhledem k rizikům útoků a narušení vyžaduje testování a ověřování splnění bezpečnostních požadavků nezávislými autoritami před nasazením (např. testy VUT při výběrovém řízení Smaragd pro E.ON, certifikační schéma, nutnost testování kvůli problematice Čínských dodavatelů).
- Rizika související s nedodržením požadavků na kybernetickou bezpečnost definovaná v ekonomickém modelu jako finanční přínosy zcela pokryjí zvýšené náklady na implementaci bezpečnosti.
- Klíčovým bodem nasazení chytrých elektroměru a související infrastruktury je reálné laboratorní testování naplnění požadavků kybernetické bezpečnosti nezávislou autoritou v rámci výběrového řízení. VUT v kooperaci se všemi distributory v rámci NAP SG definovaly 45 požadavků a postupů testování pro bezpečnost chytrých elektroměrů, tyto testy je nutné provést před samotným nasazením, jinak hrozí možná rizika definovaná v modelu (finanční ztráty, porušení legislativy či GDPR, poškození zákazníka, jména firmy či odpojení zákazníka).
- Cena testování kybernetických požadavků jednoho výrobce se pohybuje v řádu stovek tisíc korun, což vzhledem k výši investice (pořízení stovky ticích elektroměrů za stovky miliónů) je zcela zanedbatelná a přidaná hodnota výsledků je obrovská (reálné zkušenosti s testováním VUT-E.ON).
- VUT doporučuje testovat všechny požadavky, klíčové požadavky které mají dopad 80 % jsou:
  - Minimální kryptografické požadavky dle vyhlášky.
  - Vzdálená aktualizace kryptografických pověření.
  - Dostatečné budoucí prostředky (RAM, flash a výpočetní výkon) pro aktualizaci bezpečnostních funkcionalit a kryptografických primitiv po celou dobu životního cyklu elektroměru.

  - Vzdálená aktualizace bezpečnostních funkcionalit a kryptografických primitiv.

- Z výstupů ekonomického modelu čisté současné hodnoty (NPV) lze vidět, že by cena nových chytrých elektroměrů s DLMS SS2 musela být více než dvojnásobná oproti stávajícím elektroměrům, aby byl model negativní/záporný.
- Výrazný dopad do ceny mají datové tarify, kdy datový objem na základě reálných měření bude až o 50 % vyšší a to způsobí snížení NPV o 1-2 mil. EUR.
- Klíčovým bodem ekonomického modelu je stanovení přínosů eliminace rizik a útoků souvisejících s kybernetickou bezpečností. Pro náš definovaný model lze konstatovat, že pokud by přínosy odvrácení rizik kybernetické bezpečnosti (např. útoků) byly nižší než 3mil EUR byla by čistá současná hodnota NPV záporná a tím investice nerentabilní.

4.2 Dopad kybernetické bezpečnosti na cenu elektroměrů a systému AMM

Následující kapitoly v krátkosti shrnou vstupy pro ekonomický model, hloubková analýza níže uvedených podkapitola je dostupná ve studii NAP SG A17 a P12 [1]

4.2.1 Definice vstupních dat

- Vyhláška o měření elektřiny, resp. její příloha č. 4 k vyhlášce č. 359/2020 Sb. obsahující:
  - Minimální kryptografické požadavky,
  - technické požadavky.
- Device Language Message Specification (DLMS) - Security Suite - resp. jednotlivé úrovně zabezpečení definované standardem.
- Národní akční plán pro chytré sítě 2019-2030 (NAP SG) - bezpečnostní požadavky stanovené v rámci NAP SG.

4.2.2 Příloha č. 4 k vyhlášce č. 359/2020 Sb.

Požadavky jsou rozděleny na dvě základní části a to (i) minimální kryptografické požadavky (viz Tabulka 6) a (ii) technické požadavky (viz Tabulka 7).

[1] Studii lze nalézt zde.

Tabulka 6: Přehled min. kryptografických požadavků z Přílohy č. 4 k vyhlášce č. 359/2020 Sb.

Security Suite	**Autentizované šifrování**	**Digitální podpis**	**Ustanovení Klíče**	**Hash**	**Přenos klíče**
0	AES-GCM-128	X	X	X	AES-128 key wrap
1	AES-GCM-128	ECDSA P-256	ECDH P-256	SHA-256	AES-128 key wrap
2	AES-GCM-256	ECDSA P-384	ECDH P-256	SHA-384	AES-256 key wrap

Tabulka 7: Přehled technických požadavků z Přílohy č. 4 k vyhlášce č. 359/2020 Sb.

#	**Požadavek**
1	Bezpečné zotavení po chybě, výpadku či poruše.
2	Spolehlivá časová synchronizace.
3	Návod na bezpečnou instalaci, inicializaci a provoz dodávaný společně se zařízením.
4	Validace dat před jejich použitím - ochrana vstupů.
5	Ochrana před záplavami (DoS) pomocí filtrace provozu či segmentace sítě, management zdrojů.
6	Minimalizace rozhraní - deaktivace všech nepotřebných služeb.
7	Bezpečnostní události musí být zaznamenány a reportovány, log musí být chráněn proti modifikaci a smazání, velikost min. pro 1000 bezpečnostních záznamů.
8	Každé zařízení musí být jednoznačně identifikovatelné.
9	Data ve zprávách musí být šifrována.
10	Zprávy musí mít chráněnou integritu.
11	Provedení příkazů musí být potvrzováno.
12	Přístup do prvků zpracovávajících citlivé údaje vyžaduje proniknutí bezpečnostním perimetrem s plombou.
13	Kryptografická pověření musí být pro elektroměr unikátní a bezpečně uložena, nesmí po zcizení způsobit snížení bezpečnosti jiného elektroměru.
14	Oddělení funkcionalit měření a komunikace.
15	Vzdálená aktualizace bezpečnostních funkcionalit a kryptografických primitiv.
16	Vzdálená aktualizace kryptografických pověření.

4.2.3 DLMS Security Suite

Bezpečnost přenášených dat je v DLMS zajištěna úrovněmi tzv. Security Suite. Číslo Security Suite udává úroveň šifrování, autentizace, typ digitálního podpisu, metodu ustanovení klíče, typ hashe a způsob přenosu klíče, viz tab. 8.

Tabulka 8: Parametry jednotlivých úrovní zabezpečení v rámci DLMS Security Suite.

Security Suite	Autentizované Šifrování	Digitální Podpis	Ustanovení Klíče	Hash	Přenos Klíče
0	AES-GCM-128	X	X	X	AES-128 key wrap
1	AES-GCM-128	ECDSA P-256	ECDH P-256	SHA-256	AES-128 key wrap
2	AES-GCM-256	ECDSA P-384	ECDH P-256	SHA-384	AES-256 key wrap

4.2.4 NAP SG bezpečnostní požadavky

V rámci studie[2] NAP SG A17 a P12 byla realizována na VUT v Brně studie zákonných požadavků a legislativy ČR a EU k zajištění kybernetické bezpečnosti AMM. Výstupem jsou kryptografické a technické požadavky, které odpovídají legislativě a všem uznávaným doporučením a standardům. Z těchto požadavků byla tvořena Příloha č. 4 k vyhlášce č. 359/2020 Sb (je nutné zdůraznit, že požadavky NAP SG jsou přísnější a komplexnější). Studie navíc specifikovala postupy pro ověření definovaných technických požadavků (komplexní testovací metodiku).

4.2.5 Současný stav - situace na trhu

V současné době k Q3 2021 nejsou zcela komerčně dostupné elektroměry naplňující přílohu č. 4 k vyhlášce č. 359/2020 Sb, ale probíhá intenzivní vývoj. Objevují se řešení představující implementaci DLMS Security Suite 2, ale chybí pilotní ověření. Jsou částečně dostupné elektroměry s DLMS Security Suite 1 a probíhá vývoj Security Suite 2.

4.3 Dopady kybernetické bezpečnosti Smart Meteringu na cenu

Pro naplnění nejvyšších kryptografických a technických požadavků dle NAP SG byla provedena cenová analýzy na základě zkušeností z vývoje komunikační jednotky k elektroměru, která naplňuje nejvyšší bezpečnostní požadavky dle NAP SG, tedy i vyhlášku. Důvody, které zvyšují cenu řešení chytrého elektroměru kvůli implementaci bezpečnosti a souvisejících požadavků:

[2]Studii lze nalézt zde.

- Napájení,
- datové objemy,
- mikroprocesor,
- bateriové napájení.

4.3.1 Napájení

Při uvažovaní kybernetické bezpečnosti a bezdrátových technologií pro současně uvažované výběrové osazování je na základě zkušeností špičkový příkon až 10 W, kdy odhad špičkové spotřeby procesoru je 4 W, špičkový příkon modemové části například pro NB-IoT je 1,9 W (reálně měřený, proudové špičky až 300 mA po dobu max. 1 s) a je také potřeba započítat ostatní periferie a rezervu. Proto je nutné uvažovat AC/DC měnič napájený z podružných svorek elektroměrů a do finálního provedení integrované komunikační jednotky upravit elektroměr. Současné elektroměry AMM elektroměry mají napájení větev 3,3–5 W, což je nedostatečné pro komunikační modem s plnou bezpečností a bezdrátovou technologií pro výběrové osazování.

4.3.2 Datové objemy

Vzhledem k uvažování moderních mobilních technologií pro výběrové osazování je nutné uvažovat zvýšení datových objemů a tím zvýšení datových tarifů a nárůstu ceny, které je nutné platit mobilnímu operátorovi. Příklad reálného odečtu 27 objektů DLMS protokolem s TLS 1.2 s AES_256_GCM a porovnání bez zabezpečení:

- Jednorázový odečet: 21,5 kB *(Separátní odečet z objektů – dotaz na každý objekt zvlášť)*.
- S zabezpečením: 36,7 kB *(TLS 1.2 s AES_256_GCM)*. Narůst objemu dat o 41,4 % .

Zdůvodnění nárůstu objemu dat – protokol TLS vnáší tyto režie nutné pro zabezpečení:

- Režijní data – zvýšený datový objem každého paketu v závislosti na algoritmu a na počtu navazování nebo ukončování spojení.
- Pro TLS 1.2 s AES_256_GCM je režie následující:
  - TLS header 5 B,
  - Explicit Nonce 8 B,
  - GMAC 16 B.
- TLS handshake je 4-7 kB.

Vzhledem k vyhlášce, konkrétně technickému požadavku č. 7, je nutné také reportovat bezpečností logy, což vede k dalšímu nárůstu objemu dat (uvažujeme tedy nárůst objemu dat o 50 % .).

4.3.3 Bateriové napájení

Úprava konstruovaného HW (dimenzování záložního napájení), aby disponoval záložním bateriovým napájením pro realizaci funkcionality „poslední výdech“, která má za cíl úspěšně provést definovanou operaci při výpadku energie (odeslání informace výpadku do centrály apod.).

4.3.4 Řídící mikroprocesor

Uvažování výkonného procesorového modulu z důvodů:

- Logování bezpečnostních událostí viz Příloha č. 4 k vyhlášce č. 359/2020 Sb. Obsahující - Technické požadavky.
- Zpracující asymetrické algoritmy.

Dále musí být zabezpečen dostatečný výpočetní výkon pro obsluhu dalších (nově implementovaných) funkcí:

- Pokud výpočetní výkon nedostačuje:
  - Výpočetní výkon je v elektroměru dimenzován pouze pro obsluhu funkcí elektroměru.
  - Omezené možnosti budoucích funkcí pro implementaci kvůli sdílenému výkonu (společný procesor pro všechny funkce měřidla).
- Pokud výpočetní výkon dostačuje:
  - Stále se jedná o sdílený výkon, hranice omezení pro další funkce stále existuje.
  - Nutné doplnit o prvky řízení v připojené síti přes sekundární rozhraní -– implementace funkcí do firmware elektroměru.
- Nejen výpočetní výkon, ale i datová paměť:
  - Elektroměr musí mít prostor pro uchovávání dat nad rámec měřených dat, např. data která elektroměr přenáší z připojených zařízení (vyrovnávací paměť) a také prostor pro uchovávání získaných dat pro nové funkce.
  - Paměť by měla také sloužit pro rozšiřující funkce (firmware) jako jsou autonomní algoritmy pro řízení, např. optimalizace výroby, či dynamické vyrovnání zátěže při nabíjení elektromobilů apod.

4.3.4.1 Možnost rozsahu implementovatelnosti

V rámci analýzy vlivu bezpečnostních požadavků na funkcionalitu systému byly provedeny měření náročnosti kryptografických algoritmů na výpočetní prostředky poskytované hardwarem AMM systémů. Z pohledu výkonu je nejvíce omezeným zařízením elektroměr, koncentrátor i centrála v naprosté většině případů disponují stejným či vyšším výpočetním výkonem. Jak vyplývá z dokumentů výrobců mikrokontrolérů[3] i z diskuzí s výrobci zařízení dodávaných na český trh, nejpoužívanějším jádrem v elektroměrech je ARM Cortex M3. Pokud není použit žádný akcelerátor či TPM (Trusted Platform Module) modul, musí toto jádro být schopné šifrovat, počítat autentizační kódy a digitální podpisy. Autentizační kódy jsou ve většině případů založeny na konstrukci HMAC, tedy jsou výstupem hash zprávy a symetrického klíče. Rychlost hashování „nejnáročnějšími" funkcemi SHA-2 512 a SHA-3 512, které jsou dle kryptografických požadavků bezpečné i nad rok 2036, jsou uvedeny v Tabulka 9.

Tabulka 9: Rychlost hashování na platformě ARM Cortex M3.

	SHA-2 512	**SHA-3 512**
Rychlost [kB/s]	341	93

Šifrování je nejčastěji realizováno pomocí blokové šifry AES s délky klíčů 128, 192 či 256 bitů. Rychlosti implementace na uvažovaném mikrokontroléru jsou uvedeny v Tabulka 10.

Tabulka 10: Rychlost šifrování na platformě ARM Cortex M3.

	AES 128	**AES 192**	**AES 256**
Rychlost [kB/s]	152	126	108

Výpočetně nejnáročnější operací je digitální podpis dat a asymetrické ustanovení klíče. Tyto operace jsou nejčastěji realizovány z důvodu omezeného paměťového prostoru pomocí kryptografie eliptických křivek. Pro algoritmy ECDH (ustanovení klíče) a ECDSA (digitální podpis) s velikostí parametrů 256 bitů (dle požadavků bezpečné do roku 2036) jsou naměřené hodnoty uvedeny níže v Tabulka 11.

[3] Více lze nalézt zde.

Tabulka 11: Doba nutná pro ustanovení klíče a dig. podpis na platformě ARM Cortex M3.

	ECDH-256	**ECDSA-256**
Doba výpočtu [ms]	880	762

Vzhledem k uvažovaným objemům přenášených dat v systému AMM na primárním rozhraní a požadovaným rychlostem nepovažujeme kryptografické požadavky za omezující faktor pro funkčnost celého systému měření. Zejména asymetrická kryptografie, která je používána pouze pro ustanovení klíče a zabezpečení kritických zpráv, nepředstavuje z důvodu nízké četnosti těchto operací výraznější omezení. Lze také předpokládat, že hardware používaný v současnosti bude v budoucnu nahrazován výkonnějšími prvky umožňující hardwarovou akceleraci operací, tedy výpočetní zátěž bude dále snižována.

4.4 Rozšiřování a náhrada HDO

Vzhledem k HAN rozhraní (rozhraní elektroměru na zákazníka) je nutné uvažovat zvýšení ceny kvůli:

- Implementaci zabezpečení i pro rozhraní na zákazníka, doposud nezabezpečená komunikace přes optickou sondu.
- Rozšíření počtu výstupů (spínaní či řízení) vzhledem k FVE a wallboxům (náhrada HDO a příprava obchodování elektrické energie, obchodníka, flexibilitu a vstupu třetích stran).

Aktuální stav elektroměrů z pohledu předávání dat zákazníkovi a řízení jeho spotřeby je následující:

- Využití sekundárního HAN rozhraní na zákazníka pro přímé ovládání spotřeby a výroby (nad rámec blokování TUV a el. vytápění).
- Využití sekundárního HAN rozhraní na zákazníka pro připojení přídavného zařízení pro ovládání, blokování či automatizaci spotřeby a výroby.
- Možností rozšíření elektroměru o další relé či náhrady HDO v kombinaci s elektroměrem (náhrada pro zamyšlené utlumení celého HDO systému).

Jedním z možných řešení je přídavné zařízení k elektroměru, jehož cílem je rozšířit současný počet relé elektroměru především pro blokování FVE a dobíjecích stanic elektromobilů. Cílem tohoto zařízení je v kombinaci s elektroměrem nahradit funkcionality HDO (zamyšlené utlumení HDO systému). Jedná se o jednoduché zařízení, které implementuje pouze funkce připojení a odpojení výstupů relé a je závislé na připojení s elektroměrem. Další možnosti řešení je

využití přímého ovládání externích zařízení (automatizace a blokování), např. FVE a dobíjecí stanice, přes sekundární HAN rozhraní elektroměru na zákazníka. Pro počáteční vývoj/nasazení uvažovat Relé box v rozšířeném provedení – s obousměrnou zabezpečenou komunikací. Tento koncept umožňuje základní implementace pro řízení relé – DLMS PUSH mód (obousměrně i jednosměrně) a umožní jednoduché přidání funkcí do zařízení změnou FW a díky přípravě v podobě HW slotů (modulární řešení) umožní snadné rozšíření pro navazující pokročilejší funkce a zajištění plné kybernetické bezpečnosti (nutno uvažovat budoucí obchodování a flexibilitu).

4.5 Analýza ekonomických dopadů – ekonomický model

4.5.1 Model rizik – nedodržení bezpečnostních požadavků v AMM

Bezpečnost informací představuje vytvoření bezpečného informačního systému, ve kterém je zajištěna ochrana dat, která systém zpracovává a skladuje tak, aby nedocházelo k únikům nebo manipulaci neoprávněnými osobami. Tato rizika lze simulovat v teoretickém modelu pro hodnocení rizik, například Gordon-Loeb modelem [5]. Porušení bezpečnosti se v praxi rozděluje a hodnotí ve třech hlavních vrstvách (atributech) podle triády CIA (Confidentiality, Integrity, Availability) [6] a ty jsou:

4.5.2 1. Zajištění důvěrnosti

Tento atribut zajišťuje, aby data nebyla zpřístupněna nebo odhalena neautorizovaným osobám nebo entitám. Do této kategorie patří zejména zaručení důvěryhodnosti citlivých informací. Předchází se tak neautorizovanému fyzickému přihlášení například do elektroměru, v případě, kdy útočník zachytává komunikaci mezi elektroměrem a centrálou za účelem odchycení hesla. V tomto případě je hlavní riziko únik dat o spotřebě, o změňte firmware, manipulace s registry a tarify, nebo jednotlivé nebo hromadné odpojení elektroměrů.

4.5.3 2. Zajištění dostupnosti

Musí být zajištěna schopnost být aktivně k dispozici v případě žádosti autorizované entity. Dostupnost je časová charakteristika, která vyjadřuje závislost mezi požadavky řízeného systému a plněním těchto požadavků [7]. Tento atribut obsahuje rizika týkající se nedostupnosti komunikace, tedy neschopnost navázat komunikaci. Zabraňuje se tak útokům na dostupnost komunikace mezi klientem a serverem.

4.5.4 3. Zajištění integrity

Integrita zajišťuje stav bezpečnosti, přesnosti a úplnosti aktiv. Čtená data jsou totožná s uloženými daty, což znamená, že během přenosu a ukládání dat nedošlo ke změnám.

Rizika spojená s provozem systémů pro zpracování dat od zákazníků, ať už měřených nebo fakturačních, se soustřeďují především u provozovatele distribuční soustavy, který tato data získává, zpracovává, archivuje a vyhodnocuje. Rizika, která jsou pro DSO relevantní, lze shrnout do následující struktury:

- finanční rizika,
- regulační rizika,
- provozní a organizační rizika,
- rizika poškození jména firmy a vliv na zákazníka.

Kvantifikace rizik je patrná z tabulek 12 až 15, které jsou na svislé ose rozděleny do vrstev podle poskytování bezpečnostních atributů a horizontální osa dělí tyto tři vrstvy podle času, ve kterém se riziko uplatňuje. Časy uvedené v tabulkách udávají časový rámec, ve kterém musí být proces obnoven, aby se společnost nedostala do fáze, ve které je z krátkodobého nebo dlouhodobého hlediska ohrožena její schopnost přežít. Tyto časy se interpretují jako doba potřebná k tomu, aby se zkoumaný proces dostal na minimální požadovanou úroveň. Tato úroveň představuje také zabezpečení funkčnosti procesu tak, aby společnosti nevznikaly žádné další škody. Parametry a kvantifikace čtyř různých rizikových oblastí byly vypracovány na základě konzultací s distribučními společnostmi a po posouzení potenciálních rizik spojených s provozem inteligentních měření.

4.5.5 Finanční rizika

Jaké jsou finanční důsledky v případě přerušení procesu?

Finanční dopad na základě snížení tržeb a pokut vyplývajících z právních závazků. Úrovně dopadu lze rozdělit na:

1. **Mírný** dopad – do 1 mil. Eur.
2. **Střední** dopad – do 15 mil. Eur.
3. **Vysoký** dopad – do 50 mil. Eur.

Tabulka 12: Finanční rizika.

Vrstvy	24 hod.	3 dny	7 dnů	14 dnů
Důvěrnost	1	2	3	3
Dostupnost	1	2	2	3
Integrita	2	2	3	3

4.5.6 Regulační rizika

Jaký právní nebo regulační dopad může mít přerušení procesu?

Distribuční společnosti jsou subjektem regulace v síťových odvětvích. Slovenská republika – ÚRSO, Česká republika – ERÚ.

1. **Mírný** dopad – porušení s menšími následky, nízkými kompenzacemi.
2. **Střední** dopad – porušení s většími následky, více civilních žalob.
3. **Vysoký** dopad – porušení s vážnými následky, vysoké pokuty anebo kompenzace, pozastavení činnosti.

Tabulka 13: Regulační rizika.

Vrstvy	24 hod.	3 dny	7 dnů	14 dnů
Důvěrnost	1	2	3	3
Dostupnost	1	2	2	2
Integrita	1	2	3	3

4.5.7 Provozní a organizační rizika

K jakému zhoršení plnění úloh může dojít v případě přerušení procesu?

Provoz distribuční soustavy, interní a procesní komplikace.

1. **Mírný** dopad – je ovlivněno vícero oddělení v organizaci, proces vykazuje menší zpoždění, malé množství ovlivněných projektů.
2. **Střední** dopad – je ovlivněno vícero oddělení v organizaci, proces vykazuje podstatná zpoždění, velké množství ovlivněných projektů.
3. **Vysoký** dopad – pozastavení hlavních aktivit, zpozdění většiny projektů, fungování jiných procesů je rovněž pozastaveno.

Tabulka 14: Provozní a organizační rizika

Vrstvy	24 hod.	3 dny	7 dnů	14 dnů
Důvěrnost	2	3	3	3
Dostupnost	3	3	3	3
Integrita	3	3	3	3

4.5.8 Rizika poškození jména firmy a vliv na zákazníka

Jaký může mít dopad na vnímání společnosti/jména společnosti/na zákazníka případné přerušení procesu?

Provoz distribuční soustavy, interní a procesní komplikace.

1. **Mírný** dopad – domácnosti, firmy: malý počet klientů – postižených méně než 5 % zákazníků, regionální resp. lokální negativní publicita.
2. **Střední** dopad – domácnosti, firmy: 5 až 10 % postižených zákazníků, národní negativní publicita.
3. **Vysoký** dopad – domácnosti, firmy: 10 až 25 % postižených zákazníků, intenzivní národní negativní publicita, přechod do mezinárodní negativní publicity.

Tabulka 15: Rizika poškození jména firmy a vliv na zákazníka.

Vrstvy	24 hod.	3 dny	7 dnů	14 dnů
Důvěrnost	1	2	3	3
Dostupnost	1	2	3	3
Integrita	2	2	3	3

4.5.9 Tvorba ekonomického modelu založeného na NPV

Cíle modelu a NPV

Na základě dostupných informací z jiných zemí a od distribučních společností bylo provedeno ekonomické zhodnocení nákladů a přínosů využití funkcionalit kybernetické bezpečnosti.

Model je založen na metodice diskontovaných peněžních toků, která spočívá v ocenění projektu pomocí časové hodnoty peněz. Jedná se o výnosovou metodu, při které jsou budoucí peněžní toky diskontovány tak, aby byla stanovena čistá současná hodnota – NPV (Net Present Value). Výsledná hodnota NPV je součet diskontovaných přínosů a rozdílu výdajů za hodnocené období. Ve výpočtu je uvažována diskontní sazba 5,65 % . Hodnocené období se skládá z realizační fáze

a provozní fáze. Realizační fáze je samotná instalace chytrých elektroměrů. Ve zhodnocení bude uvažována realizační fáze 7 let.

Uvažované modely - rozdíly způsobené bezpečnosti

Při zhodnocovaní vlivu kybernetické bezpečnosti na provozní, ekonomické a uživatelské aspekty byly uvažovány dva modely:

První model reprezentuje **minimální úroveň zabezpečení** takzvanou LLS strukturu, kde neexistuje systém přidělovaní kryptovaných hesel Key Management Systém. Hardware elektroměrů neumožňuje nasadit algoritmy a metody kybernetické bezpečnosti (např. DLMS SS2), jde tedy o elektroměry nasazované v posledních 15 letech bez zabezpečenínebo jen s DLMS SS0. Komunikace centrály s elektroměrem v tomto případě probíhá v otevřené formě prostým ověřením hesla, které se nachází v měřidle (nebo je využito jen šifrování).

Druhý model reprezentuje **optimální úroveň zabezpečení**, kterého součástí je Key Management System, hardware elektroměru umožňuje zabezpečenou komunikaci HLS (High Level Security). Druhý model s optimální úrovní zabezpečení se oproti prvému modelu liší:

- Elektroměr s rozdílným hardwarem pro naplnění požadavků z Přílohy č. 4 k vyhlášce č. 359/2020 Sb. a dle požadavků NAP SG.
- zřízení systému na přidělovaní hesel – Key Management System,
- komunikaci mezi centrálou a elektroměrem využívá symetrické a asymetrické algoritmy - narůst objemu dat
- provozování systému si vyžaduje personál s vyšší kvalifikaci.

Vstupy modelu - náklady

Tabulka 16 zobrazuje seznam vstupních parametrů použitých na výpočet NPV.

CAPEX náklady tvoří cena za elektroměry (počet elektroměrů * cena), náklady na instalaci elektroměrů, náklady za pořízení centrály a KMS. OPEX náklady tvoří údržba elektroměru, náklady na komunikaci (datové přenosy) a náklady na údržba centrály.

Počet elektroměrů (CAPEX) Dle nové vyhlášky musí distribuční společnosti do roku 2027 nainstalovat chytré elektroměry zákazníkům, kteří mají roční spotřebou přesahující 6 MWh. To představuje například pro ČEZ instalovat do roku 2026 až 600 tisíc chytrých elektroměrů, pro EG.D cca 500 tisíc chytrých elektroměrů a pro PRE okolo 100-200 tisíc chytrých elektroměrů. Osazování na odběrná místa s roční spotřebou přesahující 6 MWh předurčuje k výběrovému selektivnímu osazování. Proto nejsou vhodné doposud uvažované technologie PLC a radio MESH, které jsou postaveny na nutnosti vybudovat plošně komunikační síť s opakovači. Pro výběrové osazování se z principu komunikace hodí point-point komunikační technologie na bázi rádiové komunikace či mobilní operátorské technologie. Pro určité lokality bude samozřejmě vhodné selektivní roll-out rozšířit na plošný.

Tabulka 16: Tabulka vstupných parametrů modelu.

Vstupní parametry

Parametr	**Hodnota**
Diskontní sazba (WACC)	5,65 %
Počet elektroměrů	110 000 kusů
Předpokládaná životnost měřidla	12 roků
Předpokládaná životnost centrály	12 roků
Předpokládaná životnost KMS	12 roků
Počet roků rolloutu	7 roků
Údržba KMS	20,00 %
Údržba měřidel optimálního zabezpečení	2,00 %
Údržba měřidel minimální zabezpečení	1,80 %
Cena elektroměru – minimální zabezpečení	60 Eur
Cena elektroměru – optimální zabezpečení	80 Eur
Náklady na instalaci elektroměru	16 Eur
Jednotková cena za SIM a datový přenos – minimální zabezpečení	1,80 Eur
Jednotková cena za SIM a datový přenos – optimální zabezpečení	2,20 Eur

Pro výpočet bylo zvoleno 110 000 elektroměrů, které by představovaly nasazení pro určitou lokalitu a jednu distribuční společnost (jedna komunikační technologie = jedno výběrové řízení).

Předpokládaná životnost elektroměru Dobu platnosti elektroměru definuje legislativa. Pro model byla stanovena na 12 roků.

Předpokládaná životnost centrály a Key Management Systému Na základě diskuzí a "best practice"byla životnost pro model stanovena na 12 roků.

Počet roků rolloutu Počet roků rolloutu představuje čas, za který společnost osadí všechny předurčené odběrné místa. Pro model bylo uvažováno postupné nasazování po dobu 7 let.

Údržba Key Management systému, centrály a elektroměrů (OPEX) Náklady na údržbu byly stanovené procentem z investičních prostředků, které byly vynaložené v dané oblasti.

Cena elektroměru (CAPEX) Průměrná cena elektroměru pro minimální model z pohledu zabezpečení byla stanovena na 60 Eur a průměrná cena elektroměru pro optimální model zabezpečení a s vyššími hardwarovými parametry byla stanovena na 80 Eur. Cena elektroměrů byla konzultována s distribučními společnostmi.

Náklady na instalaci elektroměru (CAPEX) Náklady na instalaci zahrnují podíl hodinové sazby montéra, který vykoná montáž elektroměru. Tyto náklady jsou zahrnuté v kapitálových výdajích.

Jednotková cena za SIM a datové přenosy (OPEX) Cena za nákup SIM karet a platby za datové tarify.

Vstupy modelu - přínosy

Evropská komise (EK) doporučením č. 2012/148/EÚ *Commission Recommendation on preparations for the roll-out of smart metering systems* doporučila strukturu a způsob kvantifikace přínosů AMM.

V modelu uvažujme tyto přínosy:

Přínosy pro zákazníka:

- Na základě informací z AMM může zákazník přesunut část svojí spotřeby do časových pásem/tarifů, kde je cena elektřiny nižší.
- Na základě informací z AMM může zákazník přesněji predikovat svoji spotřebu a tím pádem se vyhnout nákladům za zpodobené odchylky v spotřebě (hlavně průmysloví zákazníci).
- Na základě informací z AMM může zákazník optimalizovat/snižovat svojí spotřebu.
- Snižováním spotřeby se snižuji také technické ztráty u zákazníka.

Přínosy pro distribuční společnosti:

- Přínosy z nahrazení manuálního odečtu elektroměru, automatizovanými odečty.
- Přínosy plynoucí z většího množství dostupných informací a jejich vyšší přesnosti pro dispečerské řízení.
- Měření kvality elektřiny a přecházení stížnostem od zákazníků.
- Nižší netechnické ztráty (lepší identifikace krádeží).
- Poskytování dat třetím stranám.
- Přesnější znalost podmínek a technických parametrů v distribuční soustavě (elektroměry poskytují kromě spotřeby také další elektrické veličiny jako U, I, $\cos\phi$) čímž je umožněno i přesnější plánování obnovy a investic do distribuční soustavy.

Přínosy pro obchodníka:

- Citlivější elektroměry, méně obchodních zrát.
- Přínosy souvisící s přesnějšími náměrnými daty, méně stížností, reklamací, snížení pohledávek.
- Přínosy z různých tarifních struktur v prodeji elektřiny.

Přínosy pro odvrácení rizik kybernetické bezpečnosti (např. útoků):

- Zajištění důvěrnosti,
- zajištění dostupnosti,
- zajištění integrity,
- finanční a regulační rizika,
- provozní a organizační rizika,
- poškození jména firma a vliv na zákazníka.

Výsledky

Výsledkem modelu je NPV pro:

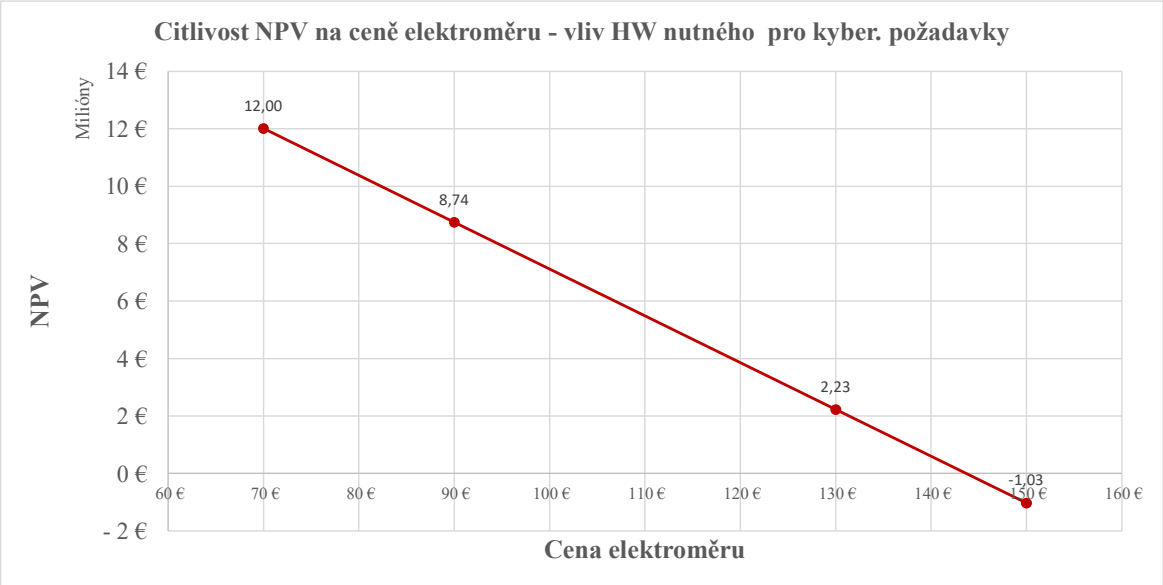
- Scénář s minimálním zabezpečením s výslednou NPV 1,25 mil EUR.
- Scénář s optimálním zabezpečením s výslednou NPV 12,19 mil EUR.

Tyto hodnoty nejsou klíčové pro posouzení dopadů kybernetické bezpečnosti Smart Meteringu na cenu, proto byly provedeny citlivostní analýzy na aspekty, které ovlivňují cenu z pohledu pouze kybernetické bezpečnosti. Byly provedeny tyto citlivostní analýzy:

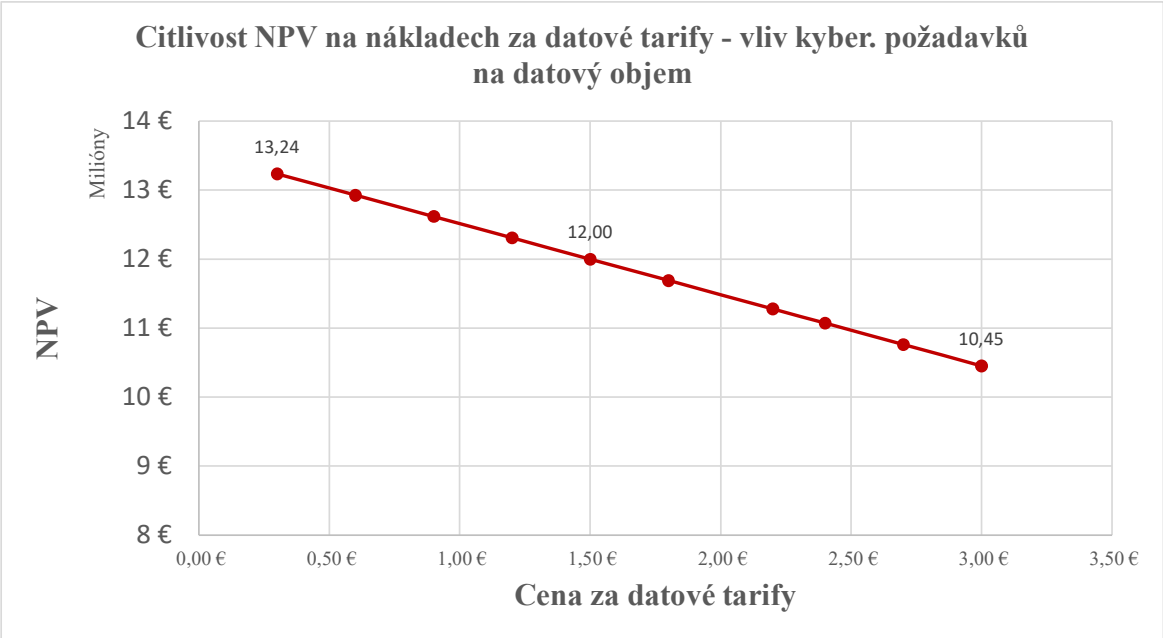
- Citlivost NPV na ceně elektroměru - vliv nových nebo dražších HW komponent pro naplnění kybernetických a technických požadavků vyhlášky
- Citlivost NPV na nákladech za datové tarify - vliv kyber. požadavků na datový objem
- Vztah NPV na výšce přínosů eliminace rizik

Obrázek 4 zobrazuje citlivostní analýzu pro různou cenu elektroměru ovlivněnou kybernetickou bezpečností – citlivostní analýzy pro 70–150 EUR/ elektroměr. Cena elektroměru je ovlivně kybernetickými požadavky a nutností využít pokročilejší a dražší HW, zdůvodnění je popsáno v předcházejících kapitolách. Pro cenu elektroměru vyšší než 143,6 EUR začíná být čistá současná hodnota záporná. Vzhledem k přínosům pro odvrácení rizik kybernetické bezpečnosti (např. útoků), viz teoretický model rizik spojených s porušením kybernetické bezpečnosti, má zvýšení cena HW elektroměru kvůli požadavkům kybernetické bezpečnosti vliv na čistou současnou hodnotu, ale nezpůsobí zápornou NPV (pro uvažovaný model by cena stávajících elektroměrů oproti novým chytrým elektroměrům s DLMS SS2 musela být více než dvojnásobná).

Obrázek 5 zobrazuje citlivostní analýzu zvýšeného datového objemu způsobeného kybernetickou bezpečností – citlivostní analýzy pro 0,3–3 EUR/ datový tarif za elektroměr. Zvýšení kybernetické bezpečnosti přináší zvýšení objemu přejásaných dát (viz předchozí kapitola až o 50 % .). Nárůst datové objemu o vypočtených a změřených 50 % má výrazný vliv na NPV, kdy pro současné



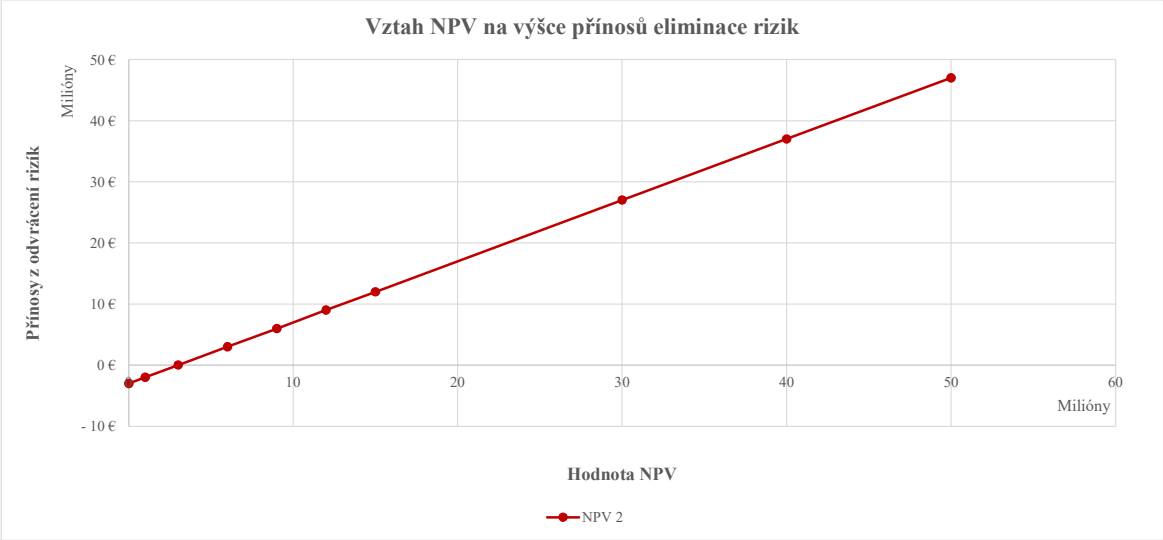
Obrázek 4: Citlivost NPV na ceně elektroměru - vliv HW pro kyber. požadavky



Obrázek 5: Citlivost NPV na nákladech za datové tarify - vliv kyber. požadavků na datový objem

odečty se uvažuje okolo 1,5EUR a nárůst způsobí 3 EUR/elektroměr. Tato změna bude mít propad o 1,55 mil EUR v čisté současné hodnotě.

Obrázek 6 zobrazuje vztah NPV na výšce přínosů eliminace rizik. Tento průběh je důkazem toho, že stanovení výšky investic do kybernetické bezpečnosti, jejich správné použití a minimalizace rizik z odvracení možných kybernetických útoků je kritickým vstupným parametrem. Pro náš definovaný model lze z průběhu vidět, že pokud by přínosy odvrácení rizik kybernetické bezpečnosti (např. útoků) byly nižší než 3mil. EUR byla by čistá současná hodnota NPV záporná a tím investice nerentabilní.



Obrázek 6: Vztah NPV na výšce přínosů eliminace rizik

Porovnání

Z výsledků předešlých kapitol je jednoznačné, že stanovení ekonomického rámce kybernetické bezpečnosti, který můžeme použit na stanovení hraničních podmínek pro výdaje na kybernetickou bezpečnost je obzvlášť důležitý krok. Tento předpoklad se potvrdil také v již existujícím modelu *Gordon-Loeb Model* [5], kde byl vyčíslený procentuální poměr možných ztrát, které jsou definované v tomto dokumentu jako bezpečnostní přínosy. Uvedený model stanovil hranici investic do zvýšení bezpečnosti na maximálně 37 % z celkových potenciálních ztrát vyplývajících z hrozeb.

5 Analýza legislativního rámce

V rámci studie NAP SG A17 a P12 byla realizovala VUT v Brně studie zákonných požadavků a legislativy ČR a EU k zajištění kybernetické bezpečnosti, především byly uvažovány:

- **Směrnice NIS** (Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii) [CR.4],
- **Nařízení GDPR** (Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)),
- **Zákon o kybernetické bezpečnosti** (Zákon č. 181/2014 Sb.),
- **Vyhláška o kybernetické bezpečnosti** (Vyhláška č. 82/2018 Sb.),
- **Doporučení v oblasti kryptografických prostředků**,
- **Veřejná vyhláška: Opatření obecné povahy**.

Dále byly postupně analyzovány požadavky ostatních autorit a institucí. Jedná se o:

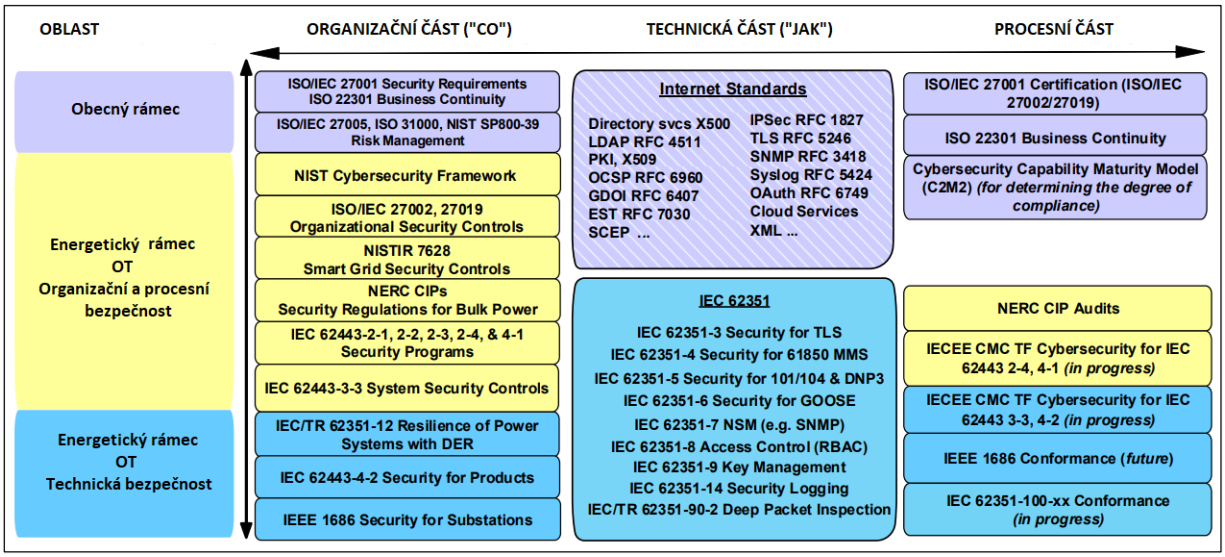
- Evropskou agenturu pro bezpečnost sítí a informací (ENISA),
- britské Národní centrum kybernetické bezpečnosti (NCSC),
- americký Národní institut standardů a technologie (NIST),
- nizozemskou laboratoř European Network for Cyber Security (ENCS) a
- nizozemský Companion Standard (CS).

Výstupem této studie byl průnik požadavků na kryptografické mechanismy a soubor technických požadavků, které jsou promítnuty v legislativě ČR (Příloha č. 4 k vyhlášce č. 359/2020 Sb. o měření elektřiny). Z pohledu zahraničních doporučení a pravidla významných institucí je možné pro AMM v ČR uvažovat:

- **NCSC**: National Cyber Security Centre (VB),
  - Proč NCSC? Zatím jediný komplexní národní certifikační rámec, který funguje.
  - Proč nepřevzít přímo? Odlišná architektura systému (předplacené tarify, huby x koncentrátory, . . .).

- **ENCS**: European Network for Cyber Security (Nizozemí - EU)
  - Požadavky ENCS obdobně jak NCSC jsou na rozdíl např. od českých národních požadavků NÚKIBu cíleny přímo na oblast smart meteringu.
  - Požadavky vycházejí z DLMS Security Suite, což dle výsledků studie VUT není bezpečné nad 2036 (podloženo NIST).
- **DLMS**: Standard definující komunikační protokol pro smart metering.
  - Nedefinuje technické požadavky, ale pouze kryptografické algoritmy a klíče.
- **BSI profil** (Německo)
  - V Německu je model AMM odlišný a uvažují se Smart Meter Gateway, které musí splňovat nejpřísnější požadavky z celé EU (BSI guidelines). Ty lze zjednodušeně naplnit pouze zabezpečením na vyšších vrstvách pomocí TLS a IPSec a dostatečně dimenzovaným HW pro naplnění technických požadavků.

Výsledkem výše uvedené analýzy je, že pro ČR jsou definovány kryptografické a technické požadavky, které odpovídají legislativě a všem uznávaným doporučením a standardům. Dalším krokem je inspirace ve Velké Británii a realizace národního certifikačního rámce, ale s uvažováním pouze požadavků nezbytných pro ČR, viz Příloha č. 4 k vyhlášce č. 359/2020 Sb. V rámci kybernetické bezpečnost však nevznikají požadavky jen na technické úrovni a z tohoto důvodu budeme vycházet z většího koncepčního rámec identifikovaného v rámci této studie, viz obrázek níže (zdroj Xanthus Consulting International).



Obrázek 7: Identifikovaný rámec kybernetické bezpečnosti na nadnárodní úrovni pro oblast energetiky

V neposlední řadě pak na národní i mezinárodní úrovni byla identifikována nejednoznačně zodpovězená otázka GDPR, definice podstaty zasílaných dat a problematika otázky ochrany dat a soukromí uživatele chytrého elektroměru, stejně jako např. vlastnictví dat.

Reference

[1] Till E., "Ict risk assessment of smart electricity meters," 2014.

[2] Vysoké učení technické v Brně, "Bezpečnostní požadavky na měřidla a související infrastrukturu," 2020.

[3] Zabkowski T., Gajowniczek, K., "Smart metering and data privacy issues," 2013. Vol. 2 (3) 239–249.

[4] Gunduy, D., Kalogridis, G., Mustafa, A.M., "Privacy in smart metering systems," 2015.

[5] TODOR, "Cybersecurity economics: What the cio/ciso must know." [online]. [vid. 31.12.2021]. Dostupné z: `https://www.cybervelocity.com/cybersecurity-economics-for-cio-and-ciso/`.

[6] CertMike, "Confidentiality, integrity and availability – the cia triad." [online]. [vid. 31.12.2021]. Dostupné z: `https://www.certmike.com/confidentiality-integrity-and-availability-the-cia-triad/`.

[7] Hennzezova, K., Gerhatova, G., "Bezpečnostné aspekty spracovania informácií." [online]. [vid. 31.12.2021]. Dostupné z: `https://spu.fem.uniag.sk/mvd2016/proceedings/sk/articles/hennyeyova_gerhatova.pdf`.