

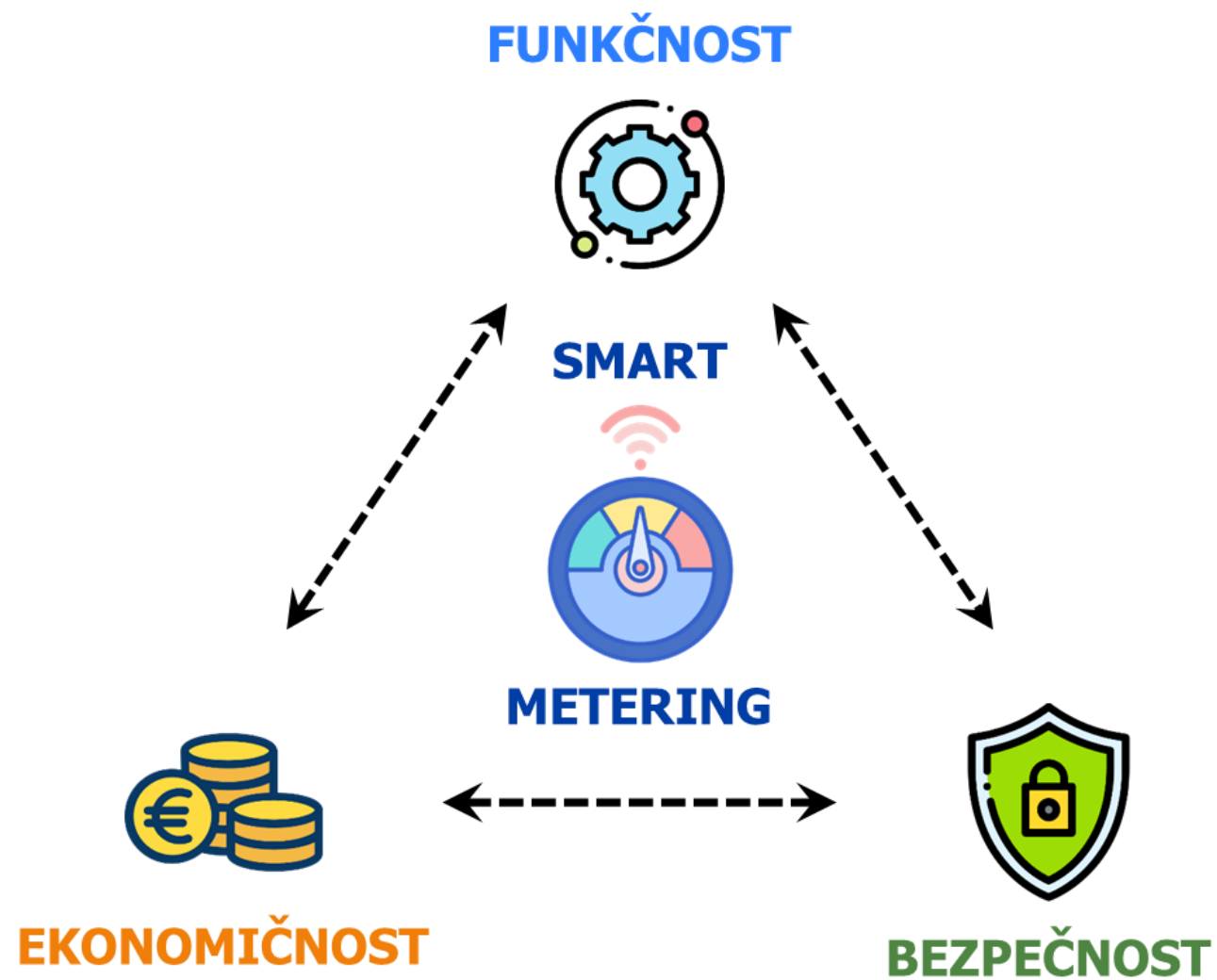
# Dopady kybernetické bezpečnosti na regulované oblasti smart meteringu

Petr Mlýnek, Radek Fujdiak

20.5.2021

## Dopady kybernetické bezpečnosti na regulované oblasti smart meteringu

- **Doba řešení:** 10/2020 – 12/2021
- **Uchazeči:** VŠB Ostrava a VUT v Brně
- **Řešitelé:** Miroslav Vozňák, Petr Mlýnek, Radek Fujdiak, Ján Sláčík
- **Aplikační garant:** Energetický Regulační Úřad (ERÚ)
  
- **Výsledky projektu:** Vyhodnocení praktických dopadů kybernetické bezpečnosti na regulované oblasti smart meteringu (0 - Ostatní)



## Bezpečnost

- Specifikace bezpečnostních požadavků
  - příloha č. 4 k vyhlášce č. 359/2020
- Komerčně dostupná řešení chytrých elektroměrů s DLMS Security Suite 1

## Komunikace

- Uvažování úzkopásmových řešení - PLC a NB-IoT
  - Výběrové osazování – NB-IoT; LTE Cat. M1 (3GPP v 14)
- Postupné ukončování HDO
- Komunikace až k zákazníkovi, zapojení zákazníka do trhu, flexibilita

## Bezpečnost

- Minimální požadavky a pouze na bezpečnost příloha č. 4 k vyhlášce č. 359/2020
  - Zvýší cenu a je nutné striktně kontrolovat/testovat – tech. požadavky 15 a 16 vyhlášky

15	Vzdálená aktualizace bezpečnostních funkcionalit a kryptografických primitiv
16	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 (M43 studie NAP SG)

- Měli bychom chtít výrazně více než DMLS SS 1 a 2
  - VPN, IPSec, SSL/TLS
  - FIPS-140 – key management system

## Komunikace

- Širokopásmové technologie pro AMM (LTE Cat. M1)
- Obousměrná zabezpečená komunikace „skoro“ v reálném čase k zákazníkovi (1 min frekvence, reakční doba do 10s)
  - Jednání Think Tanku NAP SG 18. 1.2021..... ochrana soukromí a osobních údajů zákazníků

## Dopady nedostatečné či nesprávné bezpečnosti

- Finanční a regulační
- Strategický
- Jméno firmy a vliv na zákazníka

## Cena

- Dražší elektroměr – HW (M43 studie NAP SG a 15,16 vyhláška)
- Key Management Systém (FIPS-140)
- Vyšší objem dat (certifikáty, měření VUT)
- Školení, kvalifikace, procesy

## Proč?

- CBA Smart Metering: Cena Security pro ČR: **XX Eur**/odběrné místo (4 Eur v 2015)
- Gordon-Loeb Model: „on average we should spend no more than 37% of our potential loss“
  - Z celkové investice (strategický dopad) nebo studie uvádějí 50 mil. EUR

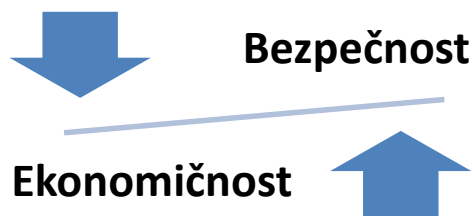
## Příklady útoků:

- United Kingdom (May 2020)
- Portugal (April 2020)
- ENTSO-E (March 2020):
- Ireland (August 2017)
- Ukraine (December 2015)

*Zdroj: Connecting the dots: Distribution grid investment to power the energy transition, 2020 Deloitte*

- Testování před nasazením, certifikace
- Uvažování řešení pro očekávané změny (výrazný posun (HDO), zapojení zákazníka, flexibilita)
- Centrála, KMS - nezávislé na technologii
- Personál- kvalifikace, školení, problematika instalace elektroměru
- GDPR
  - identifikována nejednoznačně zodpovězená otázka GDPR
  - definice podstaty zasílaných dat
  - problematika otázky ochrany dat a soukromí uživatele chytrého elektroměru
  - vlastnictví dat a přístup třetích stran
- Budoucí uvažování technologií + bezpečnostních požadavků pro
  - ostrovní provozy
  - P2P obchodu s elektřinou
  - demand response management
  - Blockchain
  - Flexibilita, obchodník, agregátor

- DLSSM Security Suite 2 není dostačující
  - Nedefinuje technické požadavky
  - Nad 2036 nejsou algoritmy a klíče bezpečné
- BSI profil (Německo)
  - Jiný model a uvažování (Gateway)
  - TLS a IPSec – naddimenzované, vysoká cena
- NCSC (VB)
  - Národní **certifikační rámec** pro chytré elektroměry
  - Jiný model (předplacené tarify, huby)
- ENCS (NL)
  - Specifikace přímo pro chytré elektroměry → **testovací laboratoř**
- **Závěr:**
  - Bezpečnostní požadavky z NAP SG → Příloha č. 4 k vyhlášce č. 359/2020
  - Certifikace (doporučuje i EU, SGTF EG2 / Cybersecurity June 2019)
  - Testovací laboratoř v ČR pro nalezení kompromisu bezpečnost/funkčnost

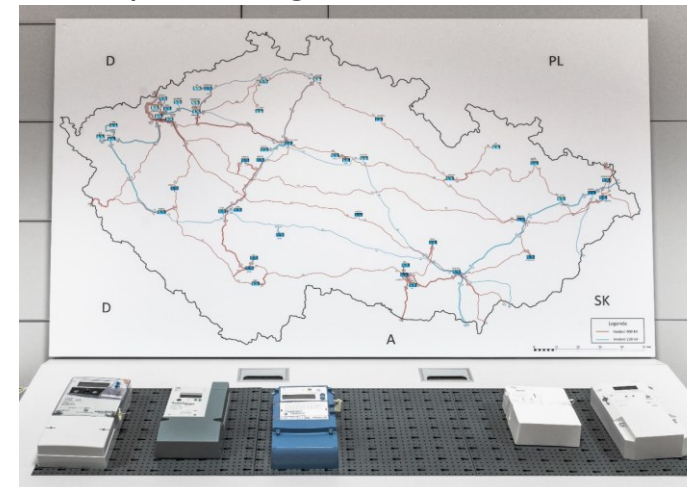


## Ukázky testovacích prostor VUT

- Certifikace v procesu



Cyber Range



3GPP v. 14 a vyšší





# Děkuji za pozornost.

Petr Mlýnek, Radek Fujdiak

20.5.2021