Mezinárodní zkušenosti při zabezpečení zásobování velkoměst vodou

Bezpečnost technické infrastruktury měst a obcí

Praha, 16.5.2017

Ing. Bohdan SOUKUP, Ph.D., MBA

technický a provozní ředitel pro ČR a SR

koordinátor SMART řešení pro Zónu CEE

Zabezpečení zásobování vodou

- Legislativa zabezpečení zásobování vodou

- Zajištění bezpečnosti infrastruktury obecně

- Zabezpečení infrastruktury z pohledu kybernetické bezpečnosti

- Příklad zabezpečení fyzické bezpečnosti vodovodní sítě

Důležitost zásobování vodou

- Infrastruktura pro zásobování vodou – kritická infrastruktura –> POVINNOST ZABEZPEČENÍ
- Nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury
- Zákon č. 240/2000 Sb. Zákon o krizovém řízení a o změně některých zákonů (krizový zákon)
- Vyhláška č. 281/2001 Sb. Vyhláška MŠMT, kterou se provádí § 9 odst.3 písm. a) zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)
- Nařízení vlády č. 462/2000 Sb. Nařízení vlády k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)
- Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů
- Vyhl. 317/2014 Sb. Vyhláška o významn. informač. systémech a jejich určujících kritériích
- Vyhl. 316/2014 Sb. o bezpečnost. opatřeních, kyber. bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kyber. bezpečnosti (vyhláška o kyber. bezpečnosti)
- Zákon č. 101/2000 Sb. Zákon o ochraně osobních údajů a o změně některých zákonů
- SMĚRNICE EVROP. PARLAMENTU A RADY (EU) 2016/1148 z 6. 7. 2016 o opatřeních k zajištění vysoké společ. úrovně bezpečnosti sítí a informač. systémů v Unii (Directive on security of network and information systems (the NIS Directive))
- NAŘÍZENÍ EVROP. PARLAMENTU A RADY (EU) 2016/679 z 27. 4. 2016 o ochraně fyzic. osob v souvislosti se zpracováním osob. údajů a o volném pohybu těchto údajů – General Data Protection Regulation – implementace 25.05.2018

Safety first! Bezpečnost především!

- **Bezpečnost – komplexní záležitost:**
- **Fyzická bezpečnost – vloupání, požár, teroristické útoky...**
- **Informační bezpečnost – Důvěrnost (Confidentiality) (only authorised reading), Dostupnost (Availability) (only authorised access), Integrita (only adequate access – protection from unauthorised obstruction to access)**
- **Organizační bezpečnost – školení, kompetence**
- **Personální bezpečnost – prověřený personál**
- **Nařízení EU 2016/679 General Data Protection Regulation – plná implementace 25.05.2018**

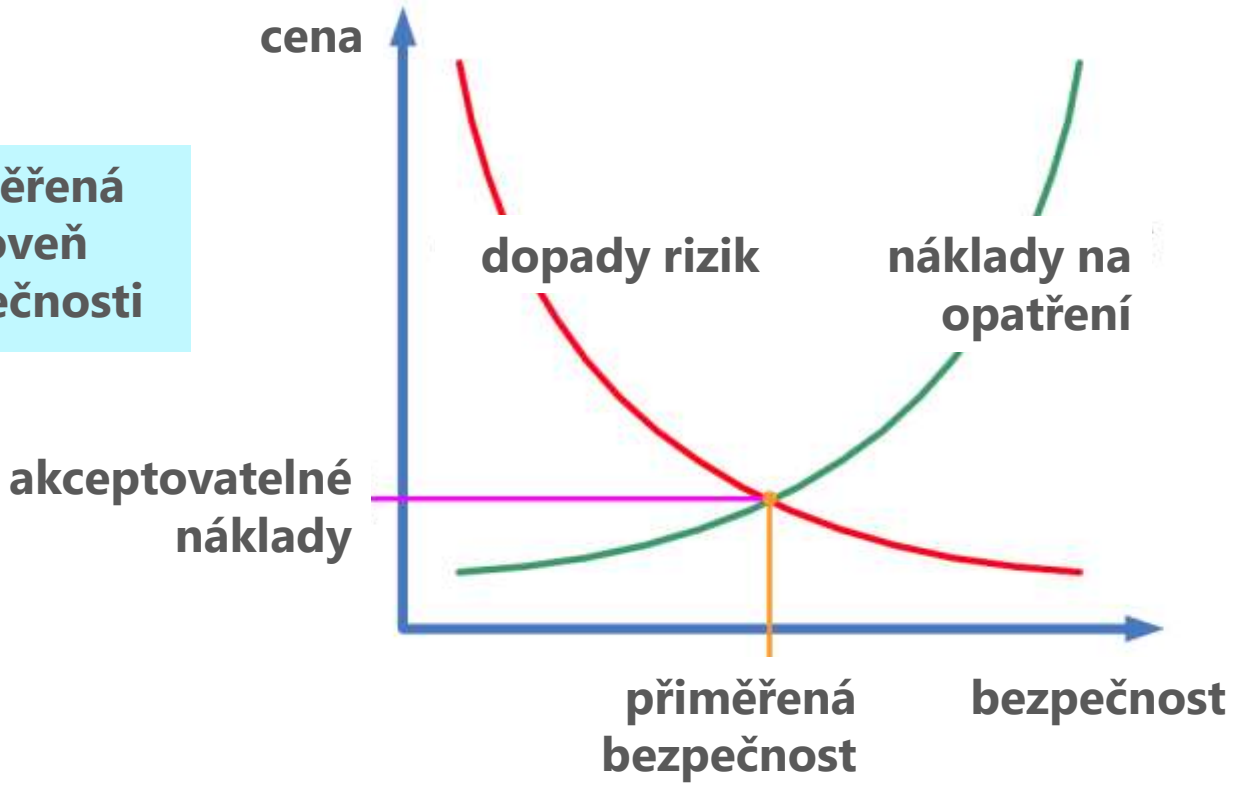
Vždy je třeba zvážit, jak vysoký stupeň ochrany si daná informace opravdu zaslouží. tj. jaký soubor opatření na úrovni organizační, logické a fyzické bezpečnosti je třeba přijmout.

Analýza rizik - cílem takové analýzy je identifikování informací, které společnost zpracovává a určení hrozeb, které by mohly ohrozit důvěrnost, integritu a dostupnost těchto informací.

Úroveň bezpečnosti

- Zajišťování bezpečnosti je nikdy nekončící proces hledání ochrany a volby bezpečnostních opatření
- Cílem je přiměřená úroveň bezpečnosti

Přiměřená úroveň bezpečnosti



Kyber útoky – odvrácená strana SMART světa

- Kyber útoky – rizika, vysoké náklady, ztráta dat, ztráta dobré pověsti...
- Podzim 2016 – první kyber útok na VaK okresní velikosti – výkupné
- Leden 2018 – novela Zák. o kyber bezpečnosti – nově součástí poskytovatelé základních služeb = VaKy přes 20 tis. obyvatel

Hackeři vítání – račte vstoupit

- Dveře do našich systémů a sítí
- PC
- Smart telefony
- Tablety
- Objekty připojené na IoT – lednička
- SCADA sítě
- dálkově ovládané ventily, klapky...

Nejčastější závady při security auditech

- Nedostatky ve fyzické bezpečnosti – chybějící plot, mříže...
- Přítomnost nízko kvalifikovaného personálu ve večerních hodinách
- Nedostatečné školení personálu (dáte klíče od auta pracovníkovi bez ŘP?)
- Slabá hesla
- „Živé“ porty na serverech
- Zanedbané aktualizace softwaru
- SCADA sítě na veřejných (nezabezpečených) wifi sítích
- Radio přenosy ze SCADA sítí bez záložní frekvence
- Neexistující disaster recovery

Strategie kyber bezpečnosti

- Stanovte si prioritní aktiva
- Bezpečnostní audit, nezapomeňte SCADA sítě
- Najděte slabá místa
- Uspořádejte priority
- Stanovte nápravná opatření a kdy je provést
- Formulujte postup
- Vyčleňte přiměřený rozpočet (některá opatření zdarma!)

- Nezapomínejte na disaster recovery
- Nezapomínejte, že bezpečnost je nekonečný proces – další audity, penetratční testy...
- Péče o bezpečnost se nedá plně internalizovat
- Péče o bezpečnost se nedá plně externalizovat

Reference skupiny Veolia

- SWiM Praha – PVK – od 2013
- SMART Kladno – od 2018
- Cvičení Geronimo – listopad 2015 – cvičení DCI / RAID / VEOLIA – simulace biologického teroristického útoku na vodovodní síť
- Konference COP21 – Paříž, prosinec 2015 – (po útocích v listopadu) – 50tis. účastníků, 195 ofic. delegací včetně prezidenta USA – globál. střežení vodovodní sítě – 15 dní

POLICE NATIONALE RAID

DCI

SYNDICAT DES EAUX D'ILE DE FRANCE

Klimatic. konference COP 21 Paříž – 12/2015

- *Zabezpečení události světového významu*

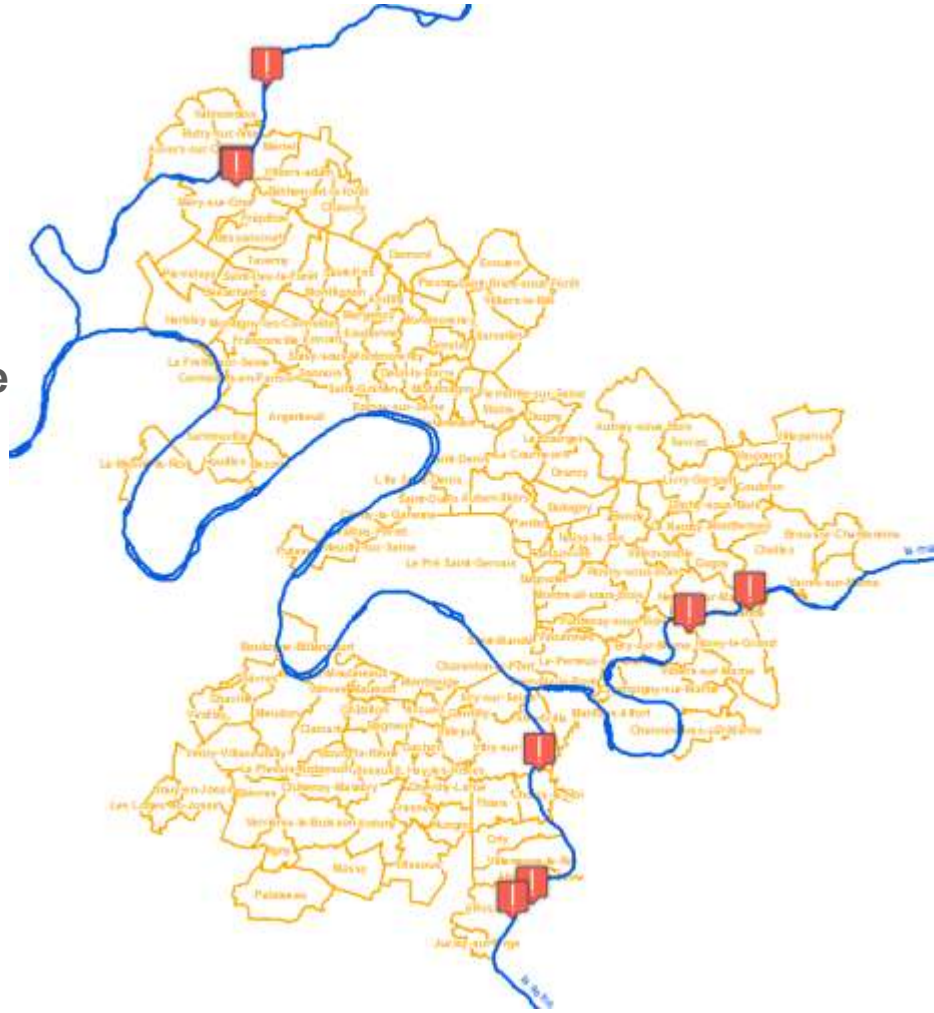
Širší kontext – Sedif Paříž

Základní data

- 4.5 milionu obyvatel zásobovaných pitnou vodou
- 149 obcí ve sdružení
- Největší síť pro dodávky pitné vody ve Francii, Top 5 v Evropě

Technické údaje

- Přibližně 8 000 km vodovod. sítí
- 3 hlavní ÚV s produkcí max. 2 mil. m3 PV / den
- 97 % produkce z povrchových vod



Použité řešení

Materiál

- 12 sond Kapta 3000 AC4 – sledování sítě
- 3 stálé sondy používané provozem pro zajištění bezpečnosti
- 9 přídavných sond pro kompletní přehled
- Automatický odečet každých 15 min., při alarmu ihned

9 smart měřičů

- Alarm při změně proudění v potrubí
- Sledování spotřeby vody na místě

Instalace sond proběhla 3 měsíce před konferencí

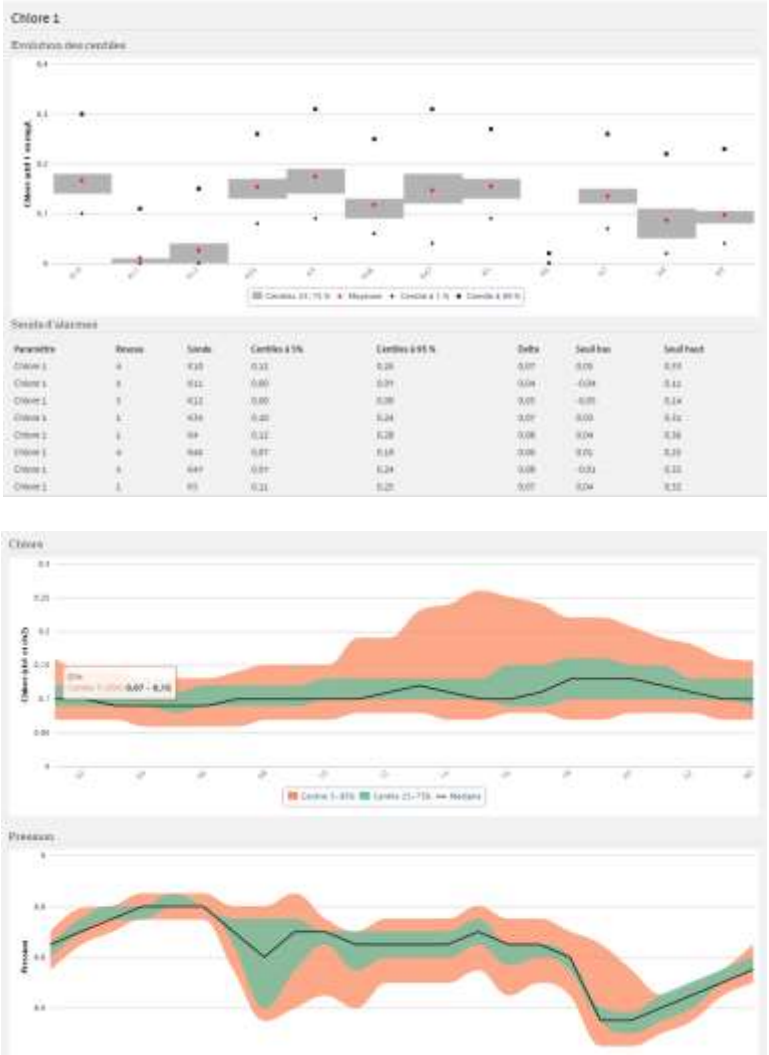
Činnost skupiny Veolia při COP 21

Před konferencí

- Strategie rozmístění sond ve spolupráci s bezpečnostními složkami
- Sběr dat historie každé sondy – typický datový profil pro každý měřený bod

V průběhu konference

- Sběr a integrace dat, analýza a vyhlášení alarmu v řádu minut od detekce kontaminace
- 24/24 7/7 střežení kvality vody při COP21
- Denní reporting pro policii (DCI-IT), municipalitu (SEDIF) a provozovatele



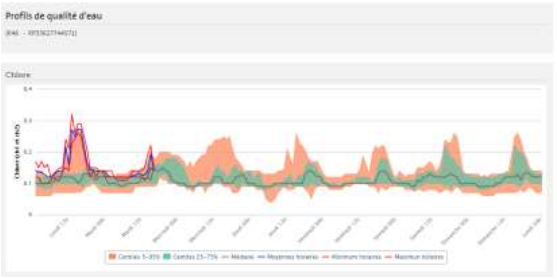
Detekované anomálie

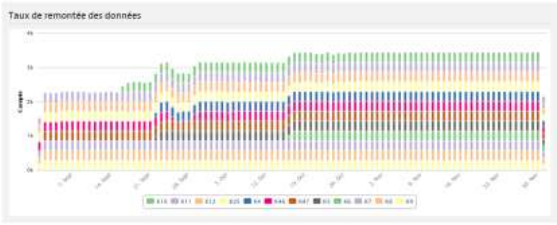
Před COP 21 (den D-15)

- Alarm 19.11., nízká hladina chloru. Příčina – porucha dochlorovací stanice Villetaneuse, vyprázdnění lahví s chlorem
- Alarm 19.11. – nízká hodnota konduktivity. Příčina – změna zdroje zásobování kvůli zvýšenému odběru vody

Zabezpečení během COP21

- Žádný „ostrý“ alarm, ale dvě mimořádné události:
- Pokles hladiny chloru po výměně lahve s chlorem (dochlorovací stanice v Bondy)
- Pokles tlaku po odstávce čerpací stanice (dodávka zajištěna jinou trasou)
- Pomalá změna kvality vody kvůli odstávce ÚV Mery (zvýšení doby zdržení, snížení zbytkového chloru)



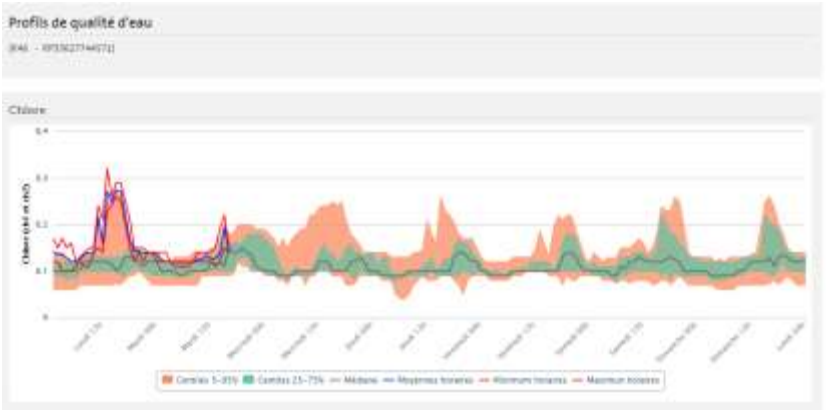


Názor SEDIF

- Vysoké uspokojení nad návrhem a provedením zabezpečení sítě PV, obzvláště po teroristických útocích z listopadu 2015 v Paříži.

- SEDIF ocenil know-how spočívající v kontinuálním sběru a analýze dat, které vede ke správnému vyhodnocení informací. Pro vyhlášení alarmu je nutné disponovat smart systémy.

- SEDIF zvažuje zvýšení počtu sond v sítích PV.



SYNDICAT DES EAUX D'ILE DE FRANCE

Děkuji za pozornost