ICZ

SCADA SYSTÉMY

Agenda

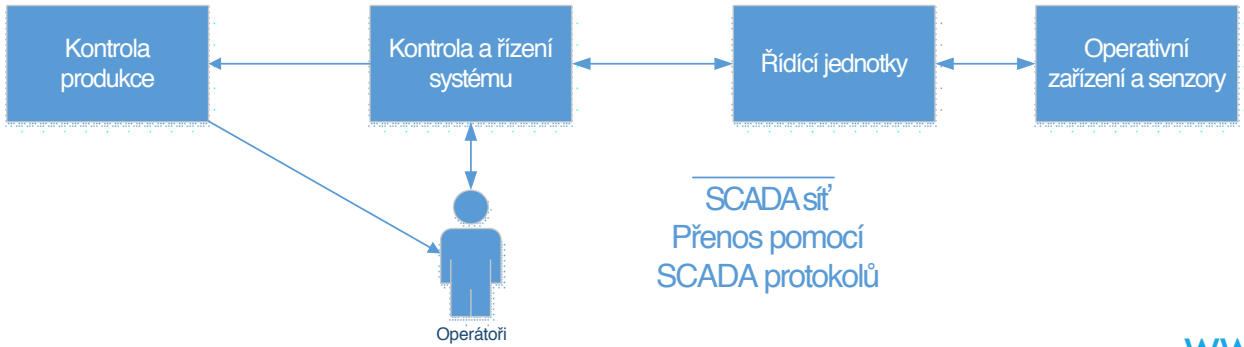
- Představení ICZ
- Úvod do SCADA systémů
- Bezpečnostní rizika SCADA systémů
  - Příklady prolomení bezpečnosti
- Ochrana SCADA systémů
  - SCADA Firewally

Představení skupiny ICZ

- Dodavatel komplexních ICT řešení
- Významný systémový integrátor
- Společnost založena roku 1997
- Sídlo společnosti v Praze
- Kolem 550 zaměstnanců

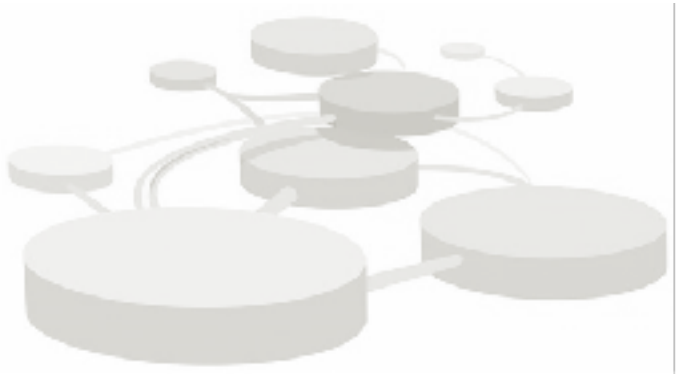
SCADA

- „Supervisory Control And Data Acquisition“
- Software, který centrálně řídí a monitoruje technická zařízení
- Využití v průmyslu
- Často součástí kritické infrastruktury státu



Generace SCADA architektur

- Jednolitá
- Distribuovaná
- Síťová
- Internet věcí (IoT)



Bezpečnostní rizika

- Důraz na funkčnost, ale ne na bezpečnost
- V návrhu SCADA systému chybí bezpečnostní prvky
  - Chybí kontrola přístupů
  - Chybí šifrování a kontrola integrity provozu
  - Někdy i nezměnitelná hesla
- SCADA síť není fyzicky zabezpečená
- Do SCADA sítě jsou připojována nezabezpečená zařízení
- Absence logování
  - Pomalé útoky
- Obsluha systémů

Případy prolomení bezpečnosti

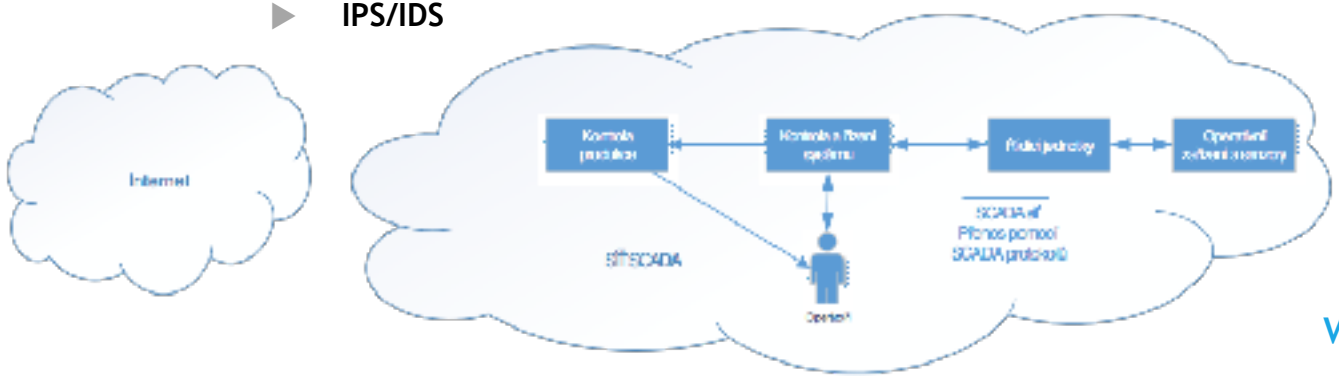
- Stuxnet (2010)
  - Měnil výstupní frekvenci měničů v jaderných elektrárnách
  - Primární cíl elektrárna Búšehr (Írán)
- BlackEnergy (Vánoce 2015)
  - DDOS útok na ukrajinské elektrárny
  - 6 hodin výpadku
- Industry, Havex, Shamoon
- Útok na německou ocelárnu (2014)
  - Obsluha nemohla vypnout vysokou pec
  - Útok založený na social engeneeringu

Základní ochrana SCADA systémů

- Oddělení SCADA sítě od internetu
- Změna defaultního nastavení
  - Změna hesel
- Aplikace bezpečnosti fyzických portů (USB)
- Používání anti-malware
- Provádění penetračních testů
- Vzdělávání obsluhy SCADA systémů

SCADA Firewally

- Kontrolují, kdo komunikuje s jakou částí SCADA systému
- Omezují komunikaci na úrovni jednotlivých příkazů použitého SCADA protokolu
- Mohou poskytovat vyšší stupně ochrany
  - Ochrana proti DDOS útoku
  - Behaviorální analýza sítě
  - IPS/IDS



www.i.cz

GDPR, DPIA a cloud

GDPR

- **Nařízení (EU) č. 2016/679** přijato Evropským parlamentem a Radou 27. 4. 2016 po čtyřleté přípravě; účinné od **25. 5. 2018**
- **Buzzword** roku 2017, prakticky **plošný dopad** na organizace v EU (i mimo ní)
- Evoluce i revoluce
  - posílení práv osob/subjektů údajů
  - náročnější pravidla pro správce a zpracovatele
  - snaha o rovnováhu mezi správci/zpracovateli a subjekty
  - vyšší pokuty

- **A co cloud?**

Studie – otázky …

- Studie: **Modelová DPIA a analýza rizik pro zpracování osobních údajů v Microsoft Office 365** (SharePoint, Exchange, Skype)
- Zadavatel Microsoft ČR, dodavatel S.ICZ, leden – březen 2017
- Otázky:
  - Je možné zpracovávat osobní údaje (včetně zvláštní kategorie) ve službách Office 365 ?
  - Jaká technická a organizační opatření bude nutné nasadit ?
  - Jak by mohla vypadat požadovaná DPIA včetně posouzení rizik ?
- Na posouzení právních aspektů spolupracovala advokátní kancelář PIERSTONE s.r.o.

Studie – … odpovědi …

- **Shrnutí studie**
- Nebyly identifikovány případy, kdy by zpracování osobních údajů v cloudu nebylo principiálně **v souladu s GDPR**
- Bezpečnostní opatření v prostředí Office 365
  - Bezpečnostní opatření jsou implementována, zdokumentována a auditována
  - Organizační opatření na straně provozovatele defaultní
  - Technická opatření jak defaultní, tak i volitelná (např. RMS)
- Správce
  - Vhodný výběr technických opatření
  - Podpora ze strany vlastních opatření

Studie - … a DPIA

- **DPIA - „Posouzení vlivu na ochranu osobních údajů“** resp. „Data protection impact assessment“
- Nejedná se o GAP analýzu (analýza pokrytí požadavků GDPR)
- Týká se pouze vybraného zpracování
- Definovaný obsah (4 body), mj.
  - Posouzení rizik pro práva a svobody subjektů údajů
  - Plánovaná opatření k řešení těchto rizik …
- Posouzení rizik ≈ Analýza rizik
  - Např. podle principů uvedených ve vyhlášce č. 316/2014 Sb.
  - Nutné upravit vodítka (dopady na subjekt údajů ≠ dopady na správce)

www.i.cz