SCADA-system
Erfarenheter och hot

Per Anth, FRA/ISA
per.anth@fra.se

Allmänt tillstånd

- Gamla protokoll utan säkerhet
- Påklistrad TCP/IP
- Sköra IP-stackar
- Standard nätverkskomponenter
- Vanliga operativsystem, ofta föråldrade
- Standardkonton med standardlösen
- Separata fjärranslutningar för leverantörer

Allmänt tillstånd

- Långa omsättningstider
- Funktionalitet framför allt
- Skapade utan tanke på IT-säkerhet

Allmänt tillstånd

- SCADA-näten svåra att ändra
- Krav på färsk driftinformation i kontorsnätet
- Enkel ihopkoppling av SCADA- och kontorsnät

Kontorsnätet

- Internet på arbetsdatorer
- Sårbarheter i webbläsare och dokumentläsare
- Gemensamma filareor

- Innehåller information om SCADA-nätet
- Har en ingång till SCADA-nätet

Intrång

- Klientattacker vanliga
- Användaren ”gör jobbet”
- Enkelt första steg, utan given uppgift
- Fjärrstyrd
- Laddar ner olika funktioner

Angrepp

- Kartläggning av nätverk och information
- Nedladdning av valda delar
- Vidare angrepp internt – system, webb, SCADA
- Eskalerar behörigheter

- Målet – administratör med höga behörigeter

Behåller kontroll

- Flyttar till servrar

- Kan vara inaktiv långa perioder

- Tillgång till både kontors- och SCADA-näten om de är ihopkopplade

Hotbilden

- Spam bots m.m.
- Statliga aktörer
- Hacktivister - nya spelare.

- Automatiserade verktyg
- ”Forskare” utanför industrin
- Hårdvara från eBay

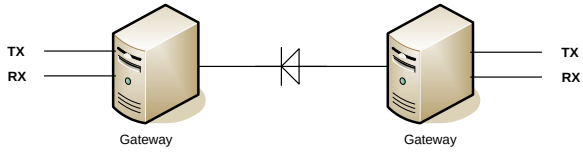
SCADA-nätet

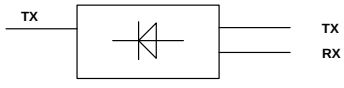
- Kontorsnätet avskiljt från SCADA-nätet.
  - Även på lokalkontor
- Normalt stängda serviceportar och modem.
  - Både för leverantörer och egna tekniker.
- Trådlös access jämställt med distansarbetsplats.
- Tydlig policy för USB-minnen
- Säker arkitektur i nya delar

Separation med datadiod

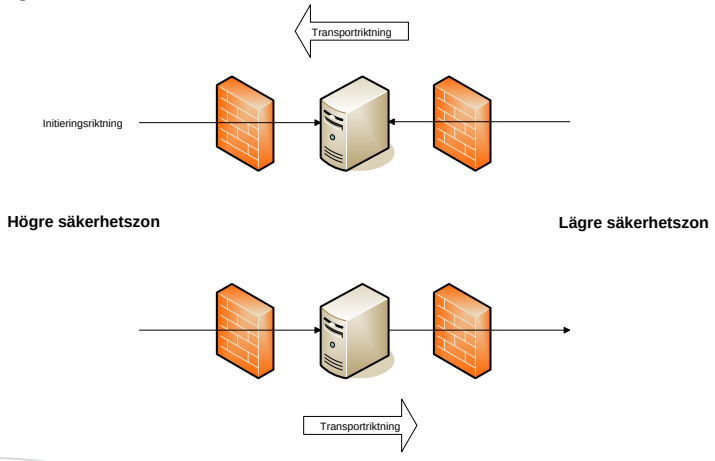
- Enkelriktad datatrafik
  exempelvis statistik eller loggning.
- Kontinuerligt flöde möjligt
- Särskild teknisk lösning

Separation med datadiod





Separation med Datasluss



Separation med Datasluss

- Automatiserad enkelriktad filtransport
- SCADA-sidan initierar all trafik.

- Använder standardkomponenter
- Statisk konfiguration
- Tål konfigurationsmissar

Kontorsnätet

- Avskilj SCADA-delen, fullständigt om möjligt
- Säkerhet i flera lager
- Högt allmänt säkerhetsmedvetande
- Mobila enheter aktuellt problem

Sammanfattning

- Ihopkoppling av SCADA- och kontorsnät kan vara motiverat men mycket sårbart
- Metoder finns för att göra det på ett kontrollerat sätt

Guidelines

- För SCADA
  - MSB:s Vägledning till ökad säkerhet i industriella kontrollsystem (2009)
    http://www.msb.se/ribdata/filer/pdf/25548.pdf
- För kontorsnät
  - 20 Critical Security Controls
    http://www.sans.org/critical-security-controls
  - Manageable Network Plan
    http://www.nsa.org/ia/_files/vtechrep/ManageableNetworkPlan.pdf