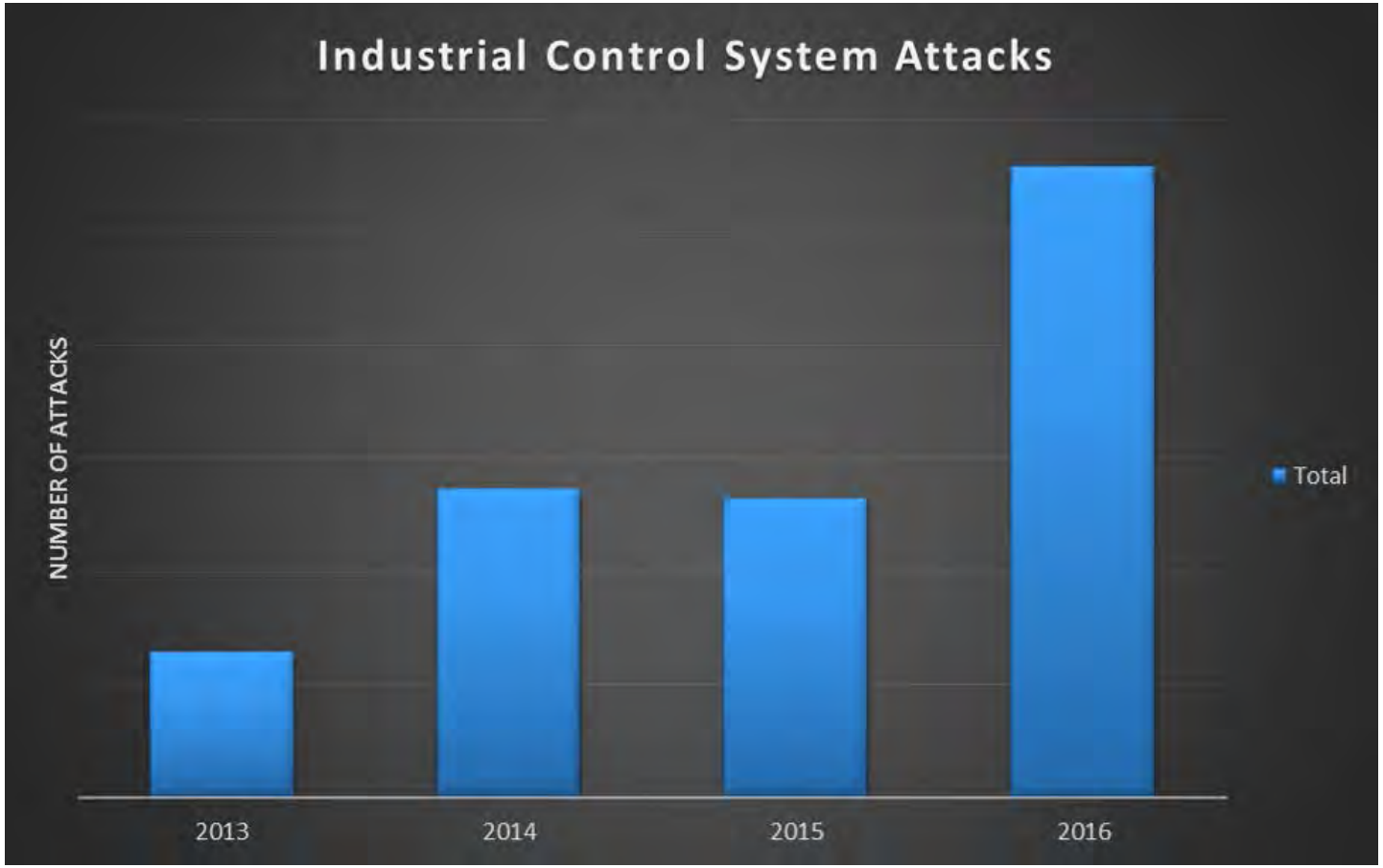
GUARD

IT-sikkerhet

Magnus Rundhaug
Teamleder IT

Angrep mot driftskontrollsystemer øker



Kilde: IBM X-Force
https://securityintelligence.com/attacks-targeting-industrial-control-systems-ics-up-110-percent/

Angrep mot driftskontrollsystemer øker

«Industrial Control Systems: Next Frontier for Cyber Attacks?»
TripWire, 22.06.2016

«The Growing Threat of Cyber-Attacks on Critical Infrastructure»
The Huffington Post, 24.05.2016

«Industrial control systems a growing target for cyber attack»
ComputerWeekly, 29.01.2016

«SCADA Vulnerability on the Rise»
EETimes, 24.09.2015

«SCADA cyber attacks double over the last year»
DatacenterDynamics, 15.04.2015

«Hackers exploit SCADA holes to take full control of critical infrastructure»
Computerworld, 15.01.2014

«Telvent Hit by Sophisticated Cyber-Attack, SCADA Admin Tool Compromised»
SecurityWeek, 26.09.2012

«FBI Admits Attackers Compromised SCADA Systems in Three U.S. Cities»
eWeek, 01.12.2011

"Kemuri Water Company"

- Et pseudonym for et spesifikt vannbehandlingsanlegg som be hacket i 2016. Bruddet ble rapportert av Verizon, et eksternt sikkerhetsselskap som ble hyret inn for å utføre en sikkerhetsanalyse.
- Hackerne fikk tilgang via en webserver som kjørte en kundeportal, og som hadde en integrasjon mot driftskontrollsystemet.
- Driftskontrollsystemets interne IP-adresse og administratorpassord ble funnet i en tekstfil på webserveren.
- Hackerne tuklet med ventiler og kjemikaliedosering i 60 dager før sikkerhetsbruddet ble oppdaget.

Teknisk eller menneskelig svikt?

- 93 % av suksessfulle sikkerhetsbrudd i 2015 kan tilskrives «menneskelig svikt»
- I snitt brukes bare 9 % av IT-budsjettet på IT-sikkerhet
- Av dette brukes bare 4 % på sikkerhetsopplæring av brukere

Kilde: Sans, Ponemon, PwC

Hvilke metoder benyttes i angrep?

- «Zero day»-sårbarheter
- Sosial manipulasjon
- Penetrasjonstesting

Drikkevannsforskriften 2017

§ 10. Forebyggende sikring

Vannverkseieren skal sikre at vannbehandlingsanlegget og alle relevante deler av distribusjonssystemet er tilstrekkelig fysisk sikret, og at alle styringssystemer er tilstrekkelig sikret mot uautorisert tilgang og bruk.

Mattilsynets «Veiledning til drikkevannsforskriften»

Dere skal sikre alle styringssystemene mot dataangrep.

Som vannverkseiere har dere ansvar for at digitale styringssystemer er tilstrekkelig sikret mot dataangrep. Her er eksempler på spørsmål som kan avdekke om styringssystemene er sikret godt nok:

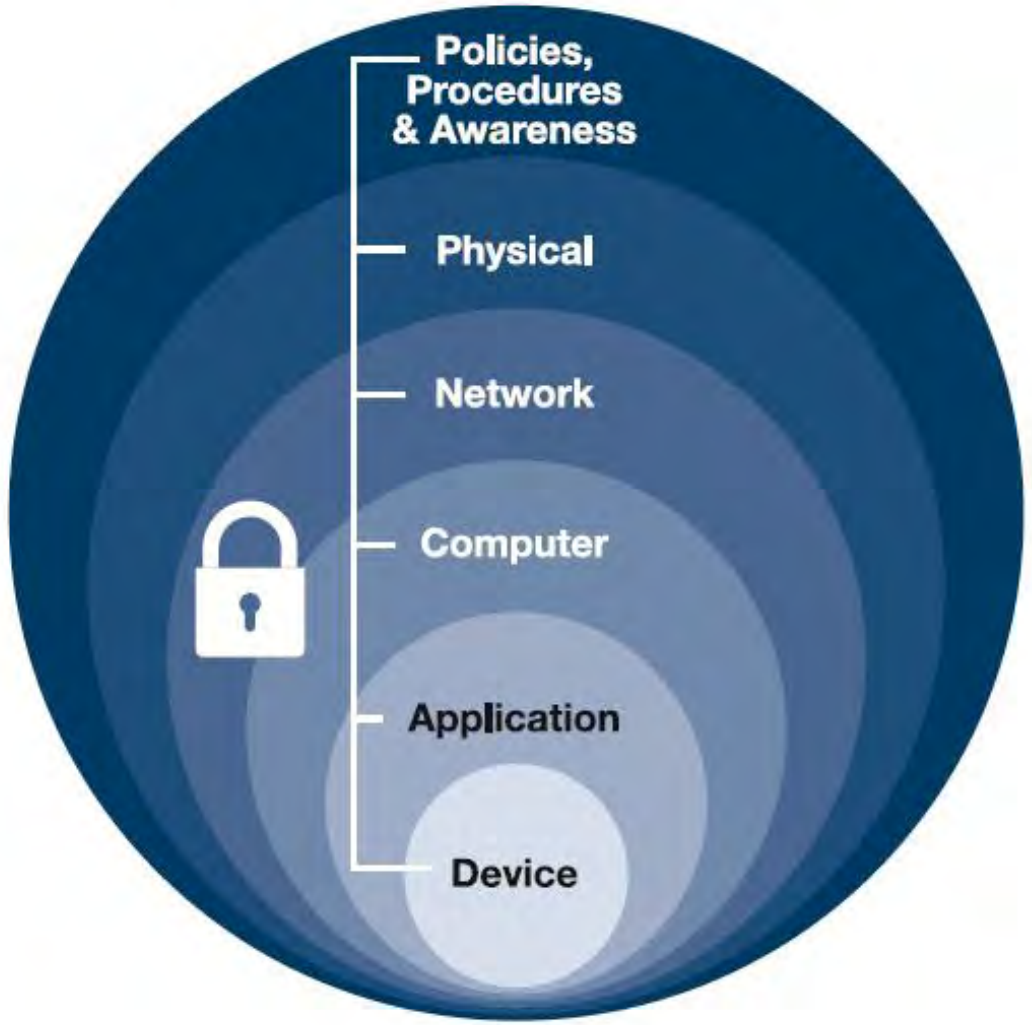
- Er styringssystemene koblet opp via internett?
- Hvilke sikkerhetsbarrierer ligger i programmerbare logiske styringsenheter?
- Hvor unike er passord for pålogging?
- Hvor ofte skiftes passord, og hvem har tilgang til dem?
- Hva ligger åpent på internett av kartdata og tekniske opplysninger?
- Hvilken grad av sikring ligger i elektroniske reserveløsninger?

Sikkerhet i flere lag

Alle skivene har hull…

Sikkerhet i flere lag

> Prosedyrer, opplæring, sikkerhetskultur
> Fysisk tilgang (kontorer og anleggsområder)
> Nettverk
> Servere og klienter
> Driftskontrollsystemet
> PLS / frekvensomformere / motor



Bilde: rockwellautomation.com

God sikkerhet betinger en plan

- Hvor er vi?
- Hvor skal vi?
- Hvilke tekniske administrative tiltak bør gjøres?
- Hvordan håndteres et angrep?
- Søk bistand!

GUARD

guard.no