Kommune-CSIRT

Erfaringer med cybersikkerhet i VA-sektoren

Bjørn T. Tveiten, Kommune-CSIRT

KiNS, 20. april 2022

Kommune-CSIRT så langt (april-21)

- 50 medlemmer, inkludert to fylkeskommuner og to VA-org
- Deltar fullt ut i SRM-samarbeidet (NSM er vertskap)
- Onboardingsprosess i gang for alle
- Leverer rapporter, varsler, trusseletterretning, rådgivning og situasjonsbilde
- Medlemsmøte med erfaringsutveksling 2-3 ganger per år
- Deltar i KS sitt utvidet fagråd for informasjonssikkerhet og personvern - sammen med KiNS!

Vannforsyning/vannverk er

- kritisk tjeneste for innbyggere, offentlige forvaltning og virksomheter
- (og dermed også) kritisk infrastruktur
- grunnleggende nasjonal funksjon (GNF)
- definert som kritisk tjeneste av EU (NIS/GDPR)
- kommunenes ansvar

Kommune-CSIRT

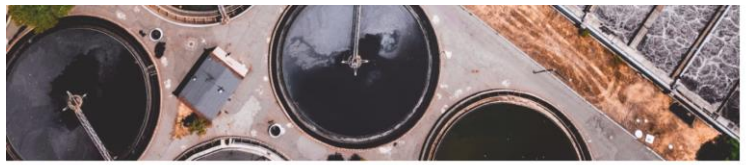


IMAGE: IVAN BANDURA

Martin Matishak
January 27, 2022

Government News

Biden administration launches initiative to protect U.S. water systems from cyberattacks

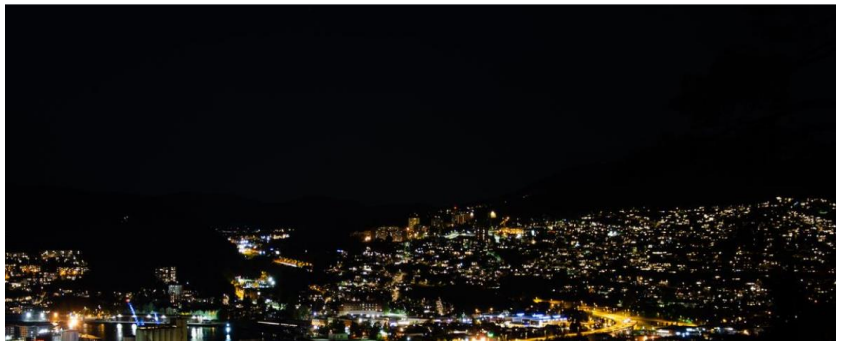
The Biden administration on Thursday will kick off an effort to protect the country's water sector from cyberattacks, the latest attempt by the federal government to strengthen the digital defenses of the nation's critical infrastructure.

The administration will formally extend President Joe Biden's "Industrial Control Systems Cybersecurity Initiative" — which was established last year and already includes the country's electric system and natural gas pipelines — to encourage owners and operators of water and wastewater systems to improve their capabilities for identifying cyber threats to their networks. The 100-day effort is also intended to promote information sharing about such threats with the government.

"There is absolutely inadequate cyber resilience across the water sector," a senior Biden administration official told reporters on Wednesday. "The threshold of resilience is not what it needs to be to meet threats today."

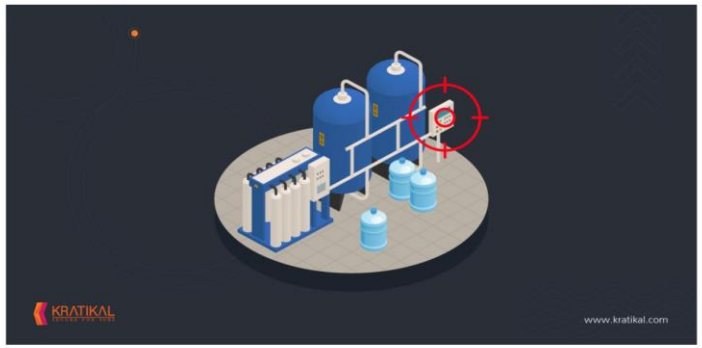
HACKERANGREP MOT DRAMMEN KOMMUNE

Politiet etterforsker hackerangrep mot vann- og avløp i Drammen kommune



Cyber Attack Haunts a Public Water Supply System. Again!

by Rishi Khemani on April 26, 2021



In my previous blog, I had described how and why it is important for critical agencies to ensure that they are secure from cyber threats lurking around. If you have not read the blog then I strongly suggest you should. The reason being that another cyber attack has taken place, where a malicious actor has targeted critical infrastructure, and this time it is Ellsworth Water Plant at Kansas.

Breached water plant employees used the same TeamViewer password and no firewall

Shortcomings illustrate the lack of security rigor in critical infrastructure environments.

DAN GOODIN - 2/10/2021, 11:59 PM

Enlarge

157

The Florida water treatment facility whose computer system experienced a potentially hazardous computer breach last week used an unsupported version of Windows with no firewall and shared the same TeamViewer password among its employees, government officials have reported.

Dataangrep på deler av Volues virksomhet

Onsdag ble deler av Volues virksomhet utsatt for dataangrep. Utover kvelden onsdag ble det klart at dette i første rekke påvirket Volue Technology, tidligere Powel. Det er snakk om et løsepenger-angrep.

UTPRESSINGSVARE

Rørledningen Colonial Pipeline ble angrepet via bortglemt konto

Passordet ble delt på den mørke weben.

Digitalisering av teknisk sektor og VA

- Parallelle digitaliseringsløp i kommunen
- Uavhengighet/selvråderett
- VA er ingeniørdrevet med høy faglig stolthet
- Ofte ikke synkronisert med IT-avd på cybersikkerhetsområdet
- Kraftig økning av den digitale kompleksiteten og automatiseringen (SCADA, kartverk, alarmsystemer, målinger, kontinuerlig rapportering)
- Leverandører og automatikere har ofte ekstern tilgang og høyeste mulige rettigheter

Risikoelementene knyttet til cyberangrep

- Verdi
  - Leveranse av rene og uskadelige produkter iht behov
  - Graderte data, personopplysninger/helse, IP (IE), forskning, konkurransesensitivitet ++
  - Krav om oppetid/tilgjengelighet, sikring av dataintegritet og konfidensialitet
  - Økonomi/kostnader
- Sårbarheter
  - Kontinuerlig rekke (nye produkter, mer komplekse, mer integrasjon, på alle enheter ++), *svake rutiner, manglende digital sikkerhetsbevissthet og -kultur*
- Trusler
  - Mer avanserte. Flere. Raskere. -> Økende fare.

Risiko = Trusler x Sårbarheter x Verdi (Konsekvens/skadeomfang)

Trusselaktørenes angrepskjede og teknikker

(Kilde: Analyst1)

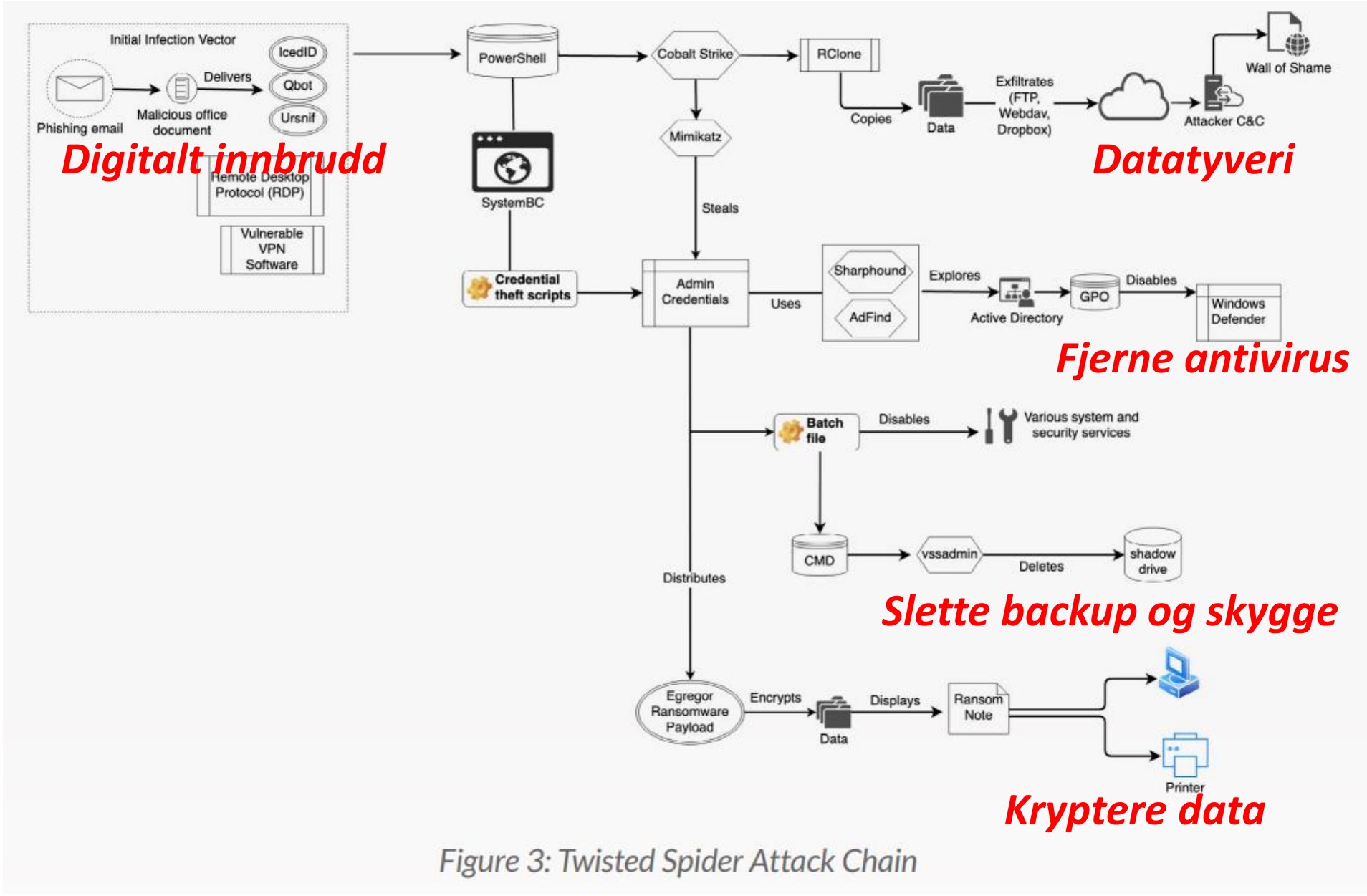


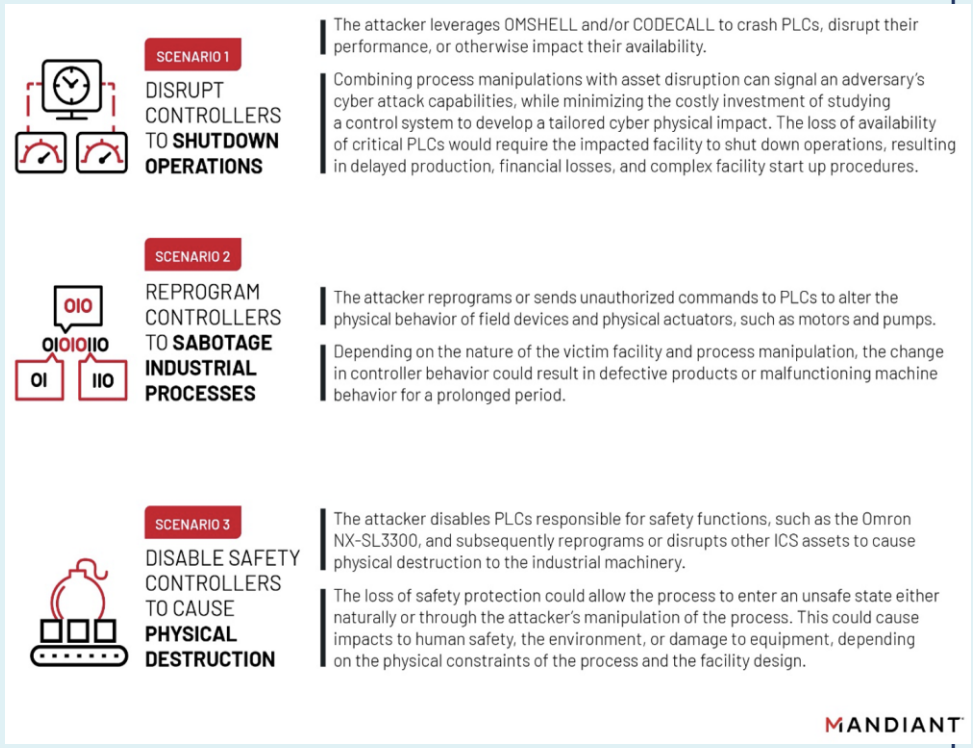
Figure 3: Twisted Spider Attack Chain

Sårbarheter i IT og OT

- IT kjenner de fleste til
- Mange leverandører også i OT
- Leverandører kan også hackes!
- Benytter 50 % egen kode og 50 % gjenbruk
- Nettverk/TCP spesielt sårbart
  - Amnesia 33 (33 sårbarheter)
  - INFRA:HALT (14 sårbarheter)
  - ++
- Komponentene har ofte (for) lang levetid!

Skadevare brukt mot DKS/SCADA

- Stuxnet (2010, mot Irans atomprogram)
- BlackEnergy (2007, 2010, 2015 - Ukrainsk kraftproduksjon)
- Industroyer (2016 mot Ukrainsk kraftproduksjon)
- HAVEX (2013++, mot USA/Europa)
- Triton/Trisis (2017, «morderisk skadevare», Saudi-Arabia)
- April 2022: Ny skadevare (INCONTROLLER) rettet mot driftskontrollsystemer (PLC) avdekket: FBI/CISA/Mandiant har analysert ny skadevare som går mot PLC-er fra Siemens, OMRON og Schneider.

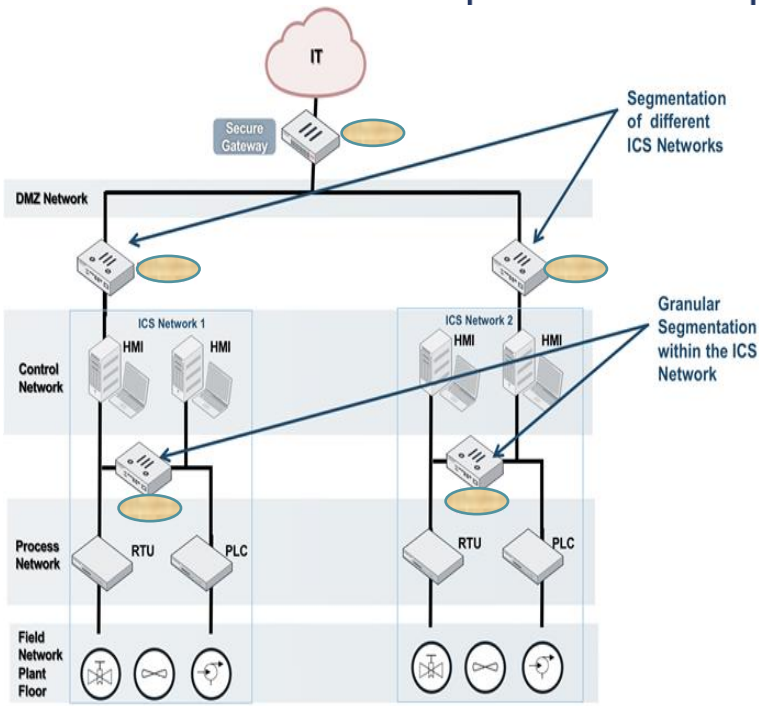


Våre funn/observasjoner

- Kommune A: Manglende sikkerhetskontroll for ekstern pålogging
  - Ikke MFA ved tilgang utenfra
  - Svake/gjenbrukte passord og RDP-pålogging
  - Oppdatering for sjeldent (hver 6. måned)
- Kommune B: For gamle systemer - ikke oppdaterbare:
  - Ikke MFA ved tilgang utenfra
  - 10-14 år gamle systemer (eller enda eldre for DKS)
  - PLS-programmering kunne kun gjøres på en XP PC
- Kommune C: Admin-rettigheter
  - For mange med Domain Admin-rettigheter
  - For mange av dem var eksterne brukere
  - Mange upersonlige admin-brukere (hvem gjorde hva…?)
- Kommune D: Leverandører har for høye rettigheter
  - Leverandører har høyere rettigheter enn driftsoperatør
  - Ikke MFA for alle leverandører
- Kommune E: Teamviewer permanent åpen
  - Ikke MFA ved tilgang utenfra
  - Teamviewer stod åpen for leverandør nærmest permanent
  - Gjenbruk av passord på tvers av infrastrukturkomponenter

Mottiltak

- Bruk multifaktor-autentisering for ***all*** tilgang utenfra
- Sørg for reell offline backup
- Segmentér de ulike delene - tilgang, applikasjon og driftskontroll
- Vær oppdatert - bygg et effektivt og raskt oppdaterings/patcheregime
- Fjern utrangert utstyr
- Vær forberedt!
  - Opprett, vedlikehold og tren på planer for å svare på et angrep og gjenopprette driften etter en krise
  - Bygg/anskaff cybersikkerhetskompetanse
- Kontinuerlig opplæring og øvelse av brukere i operativ informasjonssikkerhet - sikkerhetsbevissthet fra toppledelse til vanlig ansatte



Utfordring fra Norsk Vann: Hvem hjelper kommunalt VA? Kommune-CSIRT? KraftCERT?

Takk for oppmerksomheten.

Spørsmål?

http://kommunecsirt.no

bjorn@kommunecsirt.no

T. 90 85 00 42