Erfaringer med cybersikkerhet i VA-sektoren

Bjørn T. Tveiten,
Daglig leder

Kommune-CSIRT

Innhold

- Intro/om oss
- Kommunale verdier og risiko
- Digitalisering/automasjon
- Trusler og sårbarheter
- Egne erfaringer og mottiltak

Kommune-CSIRT

Kommune-CSIRT er den eneste

non-profit

organisasjonen som leverer

én-til-én operativ rådgivning

og støtte innen

digital sikkerhet

til norske kommuner og fylkeskommuner i

hele kommunens oppgavebredde

– og som samtidig deltar fullverdig *i*

NSMs sektorsamarbeid SRM (Sektorvise ResponsMiljø).

Status per oktober 2023

- Ca. 60 medlemmer, hvorav seks fylkeskommuner og tre rene VA-foretak
- Medlemmer fra hele landet, fra Hammerfest i nord til Sola i sør
- Store og små, Eidfjord den minste, Oslo den største
- Fullt samarbeid i SRM-nettverket hvor NSM er vertskap
- Benyttes som kommunenes representant ved nasjonal varsling
- Har gjennomført onboarding med de fleste medlemmene, og tettet mange sikkerhetshull
- Medlemsmøter er gjennomført med erfaringsutveksling og aktuelle sikkerhetstema
- Trusseletterretning, varsler (1-2 egenproduserte per uke) og rapporter produseres løpende. Vårt siste «Digitalt situasjonsbilde» ble sendt ut 31. oktober.

Kommunale oppgaver* – KCSIRT støtter i hele oppgavebredden

Undervisning
- barnehage/grunnskole/SFO
- spesialundervisning

Helse og sosial
- primærhelsetjenesten
- barnevern
- hjemmehjelp og hjemmesykepleie
- alders- og sykehjem
- helsevern for psykisk utviklingshemmede
- sosialhjelp

Transport og tekniske oppgaver
- lokale veier
- brannvesen
- vann, avløp og renovasjon (VAR)
- forvaltning/eiendom og planmyndighet
- lokalt miljøvern

Kultur og fritid
- fritidsklubber
- kulturskole
- folkebibliotek

Underliggende virksomheter

*ikke uttømmende liste

Risikoelementene knyttet til cyberangrep

- Verdi
  - Graderte data, personopplysninger/helse, IP (IE), forskning, konkurransesensitivitet ++
  - Krav om oppetid/tilgjengelighet, sikring av dataintegritet og konfidensialitet
  - Økonomi/kostnader
  - Leveranse av rene og uskadelige produkter iht behov
- Sårbarheter
  - Kontinuerlig rekke sårbarheter i programvare (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)

Aktuelle hendelser

Dataangrep på deler av Volues virksomhet

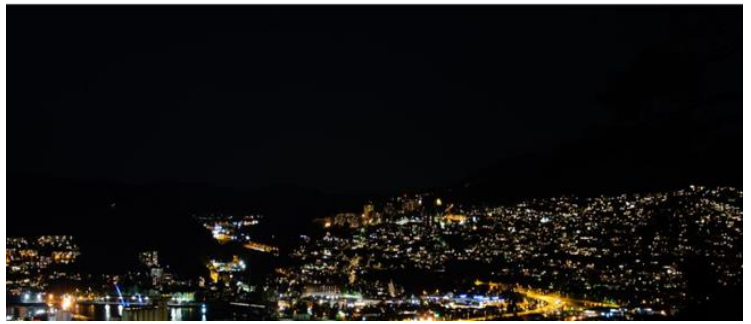
Onsdag ble deler av Volues virksomhet utsatt for dataangrep. Utover kvelden onsdag ble det klart at dette i første rekke påvirket Volue Technology, tidligere Powel. Det er snakk om et løsepenger-angrep.

Vadsø kommune utsatt for dataangrep

UTSATT FOR ANGREP: Vadsø kommune jobber for å finne ut hvordan angriperne har kommet seg inn i systemene. Foto: Illustrasjonsfoto

HACKERANGREP MOT DRAMMEN KOMMUNE

Politiet etterforsker hackerangrep mot vann- og avløp i Drammen kommune



U.K. Water Supplier Hit with Clop Ransomware Attack

Author:
Elizabeth Montalbano

August 16, 2022
/ 10:30 am

3 minute read

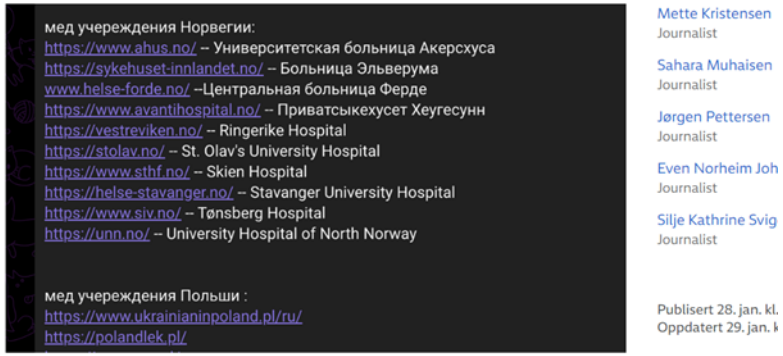
Write a comment

Share this article:

The incident disrupted corporate IT systems at one company while attackers misidentified the victim in a post on its website that leaked stolen data.

Norske sykehus trues av russiske hackergrupper

Russiske hackergrupper truer lørdag sykehus og helseinstitusjoner i Norge og flere vestlige land.



мед учереждения Норвегии:
https://www.ahus.no/ -- Университетская больница Акерсхуса
https://sykehuset-innlandet.no/ -- Больница Эльверума
www.helse-forde.no/ --Центральная больница Ферде
https://www.avantihospital.no/ -- Приватсыкехусет Хеугесунн
https://vestreviken.no/ -- Ringerike Hospital
https://stolav.no/ -- St. Olav's University Hospital
https://www.sthf.no/ -- Skien Hospital
https://helse-stavanger.no/ -- Stavanger University Hospital
https://www.siv.no/ -- Tønsberg Hospital
https://unn.no/ -- University Hospital of North Norway

мед учереждения Польши :
https://www.ukrainianinpoland.pl/ru/
https://polandlek.pl/

Mette Kristensen
Journalist

Sahara Muhaisen
Journalist

Jørgen Pettersen
Journalist

Even Norheim Joh
Journalist

Silje Kathrine Svig
Journalist

Publisert 28. jan. kl.
Oppdatert 29. jan. k

SYKEHUS TRUES AV RUSSISKE HACKERE: Dette er listen over helseforetakene som skal være utsatt for hacking.

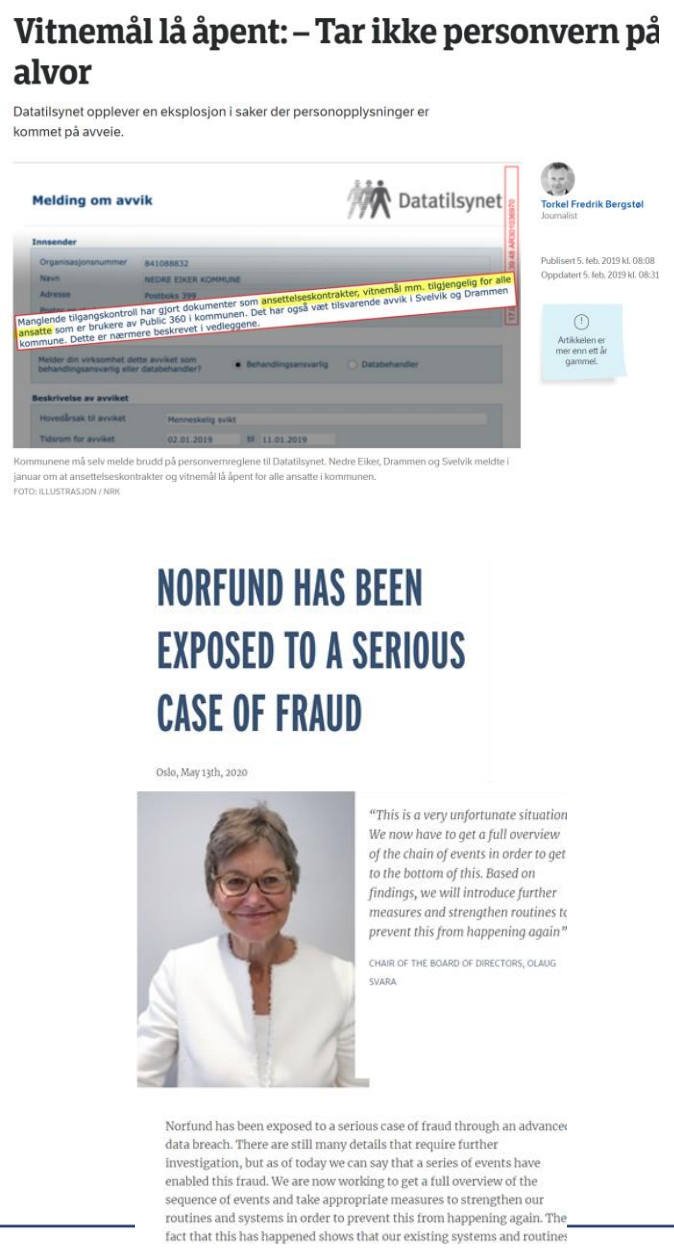
Rørledningen Colonial Pipeline ble angrepet via bortglemt konto

Passordet ble delt på den mørke weben.

Noen konsekvenser av cyberangrep og sikkerhetsbrudd

- Brudd på personvernet
- Krypterte data og løsepengekrav (Østre Toten, Hydro, Volue, Drammen VA, Amedia m.fl)
- Utfall/sabotasje av drifts-, kontroll- og kommunikasjonssystemer
- Cyberspionasje
- Fakturasvindel/BEC (Ref. NorFund-saken)
- Kompromittering som del av kriminelt nett
- Lekkasjer og sikkerhetsglipper – tap av tillit/renommé

Personvern – operativ evne – helse – økonomi – tillit/renommé – rikets sikkerhet



Vitnemål lå åpent: – Tar ikke personvern på alvor

Datatilsynet opplever en eksplosjon i saker der personopplysninger er kommet på avveie.

Melding om avvik

Datatilsynet

Manglende tilgangskontroll har gjort dokumenter som ansettelseskontrakter, vitnemål mm. tilgjengelig for alle ansatte som er brukere av Public 360 i kommunen. Det har også vært tilsvarende avvik i Svelvik og Drammen kommune. Dette er nærmere beskrevet i vedleggene.

Torkel Fredrik Bergstøl
Journalist

Publisert 5. feb. 2019 kl. 08:08
Oppdatert 5. feb. 2019 kl. 08:31

Artikkelen er mer enn ett år gammel.

Kommunene må selv melde brudd på personvernreglene til Datatilsynet. Nedre Eiker, Drammen og Svelvik meldte i januar om at ansettelseskontrakter og vitnemål lå åpent for alle ansatte i kommunen.
FOTO: ILLUSTRASJON / NRK

NORFUND HAS BEEN EXPOSED TO A SERIOUS CASE OF FRAUD

Oslo, May 13th, 2020

"This is a very unfortunate situation We now have to get a full overview of the chain of events in order to get to the bottom of this. Based on findings, we will introduce further measures and strengthen routines to prevent this from happening again"

CHAIR OF THE BOARD OF DIRECTORS, OLAUG SVARA

Norfund has been exposed to a serious case of fraud through an advanced data breach. There are still many details that require further investigation, but as of today we can say that a series of events have enabled this fraud. We are now working to get a full overview of the sequence of events and take appropriate measures to strengthen our routines and systems in order to prevent this from happening again. The fact that this has happened shows that our existing systems and routines

Vannforsyning/vannverk er

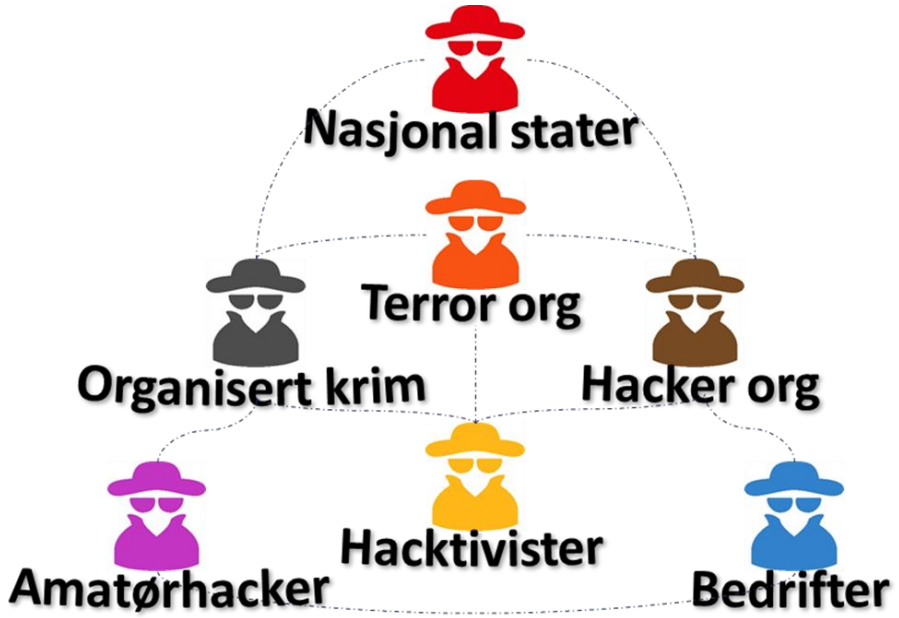
- kritisk tjeneste for innbyggere, offentlige forvaltning og virksomheter
- (og dermed også) kritisk infrastruktur
- grunnleggende nasjonal funksjon (GNF)
- definert som kritisk tjeneste av EU (NIS/GDPR)
- kommunenes ansvar

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

Trusselaktører

- Kategorisering av aktør:
  - Amatører
  - Insidere
  - Hactivister
  - Organisert kriminalitet
  - Terrororganisasjoner
  - Statssponset aktør
- Hvor er de hjemmehørende ?
  - Org. krim/ransomware: Mest i Russland + tidl. Sovjetstater
  - Industrispionasje: Mest Kina
  - Insidere – lokale eller gjester fra utlandet
  - Statssponset: Russland, Nord-Korea, Iran, Kina
  - Kriminelle org også i Europa og USA.
- Hvor opererer de fra? Internett…



Twisted Spider angrepskjede og teknikker

(Kilde: Analyst1)

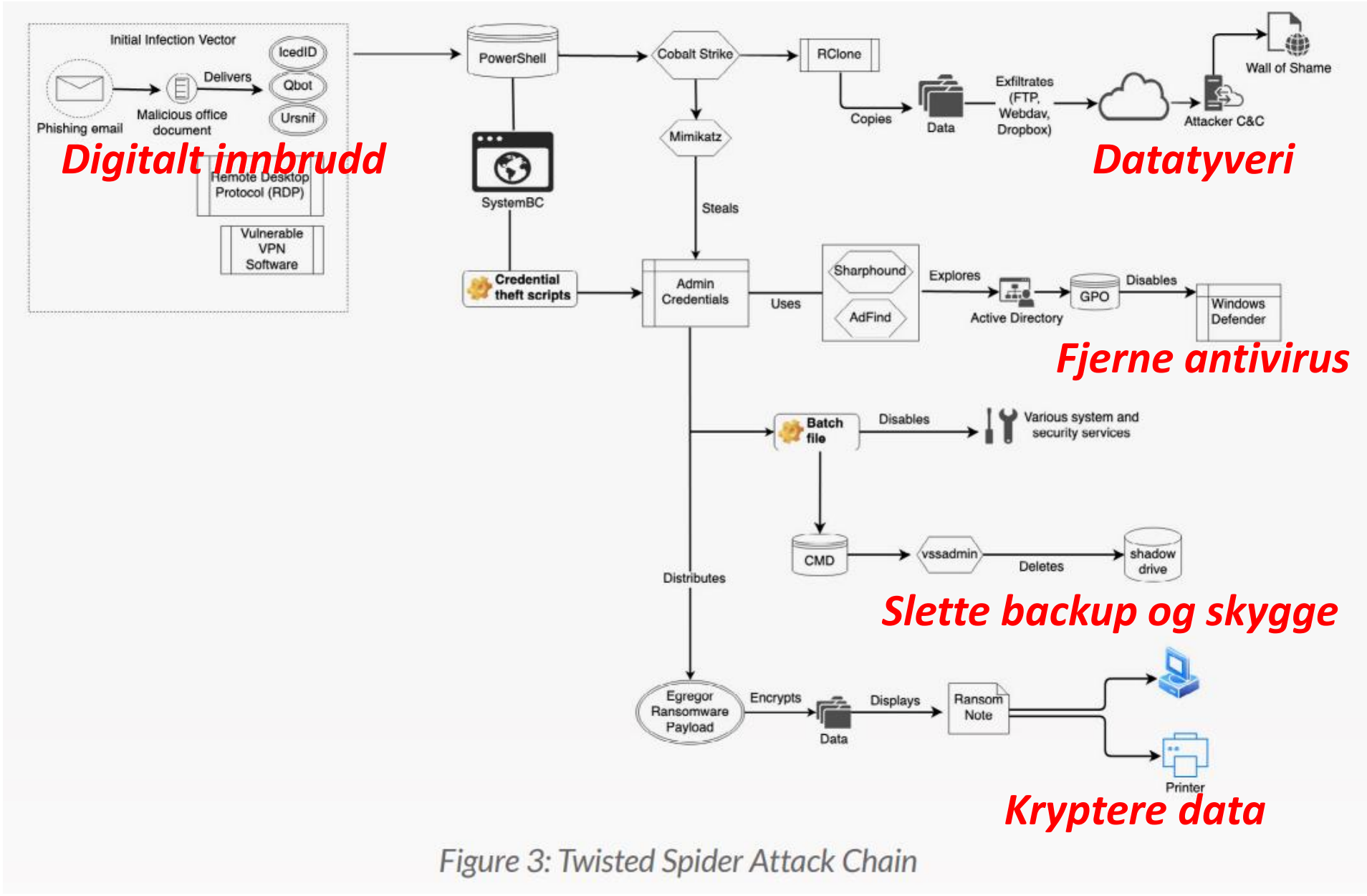


Figure 3: Twisted Spider Attack Chain

Verdikjede-betraktning

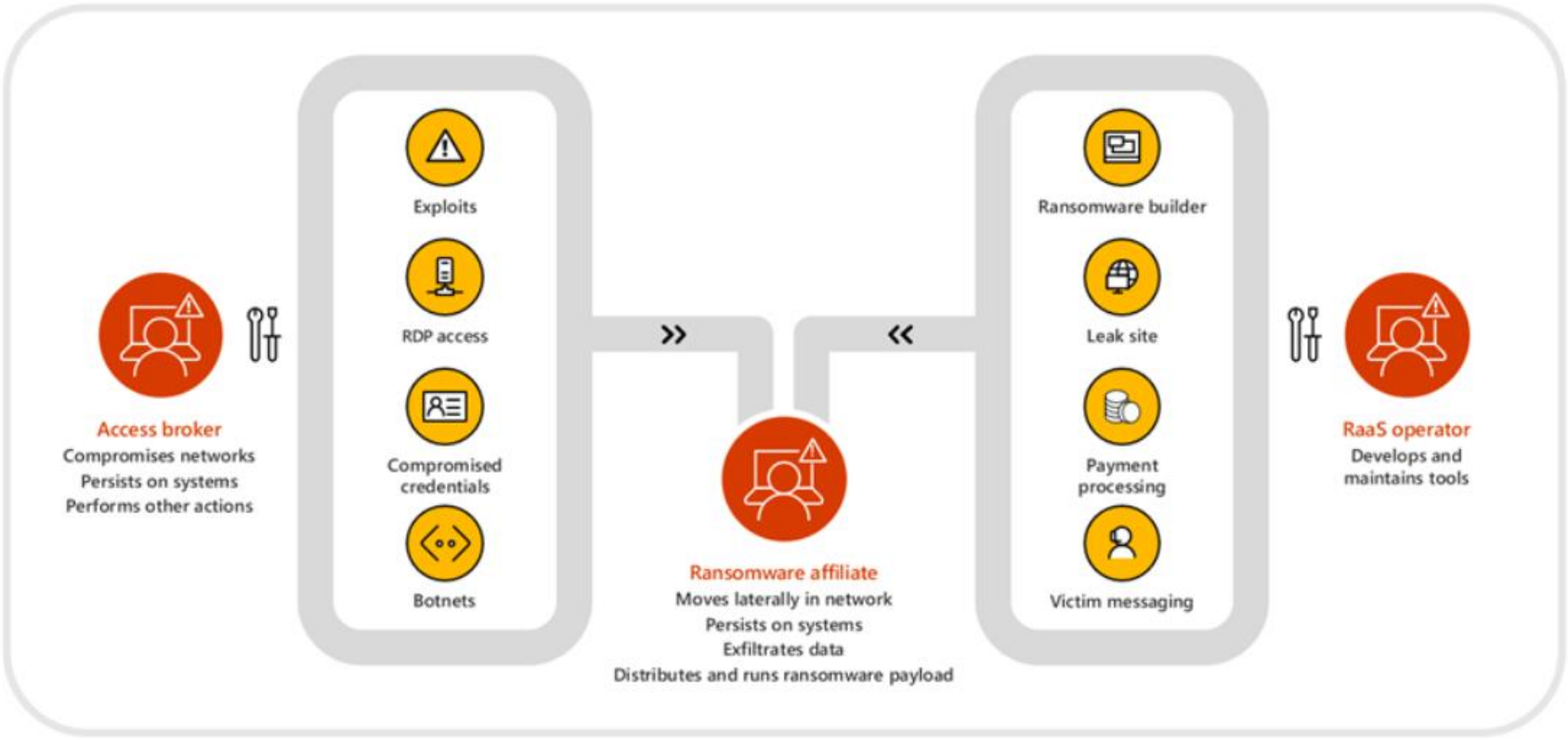
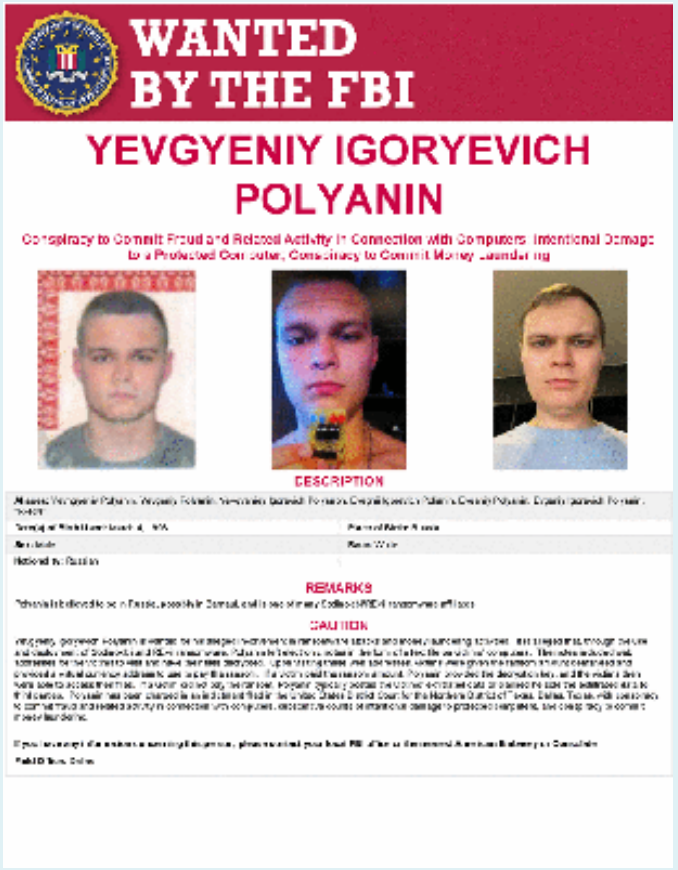


Figure 6. The underground economy of ransomware gets malicious actors going

REvil: Noen blir arrestert, andre blir etterlyst!

REvil hacker arrestert: Jaroslav Vasinski, Ukraina



REvil hacker etterlyst, og arrestert: Jevgeni Poljanin, Russland

Etterlyst!


Cyber's Most Wanted
Select the images of suspects to display more information.
Filter by
Filter by:
Filter by title, description, category...
Year
Filter
Sort by:
New
Results: 106 Items
IRANIAN INTERFERENCE IN 2020 U.S. ELECTIONS
YEVGYENIY IGORYEVICH POLYANIN
APT 40 CYBER ESPIONAGE ACTIVITIES
MUJTABA RAZA
MOHSIN RAZA
PARK JIN HYOK
KIM IL
JON CHANG HYOK
GRU HACKERS' DESTRUCTIVE MALWARE AND INTERNATIONAL CYBER ATTACKS
YURIY SERGEYEVICH ANDRIENKO
SERGEY VLADIMIROVICH DETISTOV
PAVEL VALERYEVICH FROLOV
ANATOLIY SERGEYEVICH KOVALEV
ARTEM VALERYEVICH OCHICHENKO
PETR NIKOLAYEVICH PLISKIN
APT 41 GROUP
ZHANG HAORAN
TAN DAILIN
QIAN CHUAN
FU QIANG
JIANG LIZHI
IRGC CYBER ACTORS
SAID POURKARIM ARABI
MOHAMMAD REZA ESPARGHAM
MOHAMMAD BAYATI
MEHDI FARHADI
HOOMAN HEIDARIAN
MARWAN ABUSROUR
BEHZAD MOHAMMADZADEH
CHINA MSS GUANGDONG STATE SECURITY DEPARTMENT HACKERS

Sårbarheter i IT og OT

- ‘Vanlig’ IT – en strøm av sårbarheter
- Mange leverandører også i OT
- Leverandører kan også hackes!
- Benytter 20 % egen kode og 80 % gjenbruk
- Nettverk/komm spesielt sårbart
  - 2020: Amnesia 33 (33 sårbarheter)
  - 2021: INFRA:HALT (14 sårbarheter)
  - 2022: IceFall (56 sårbarheter)
- Komponentene har ofte (for) lang levetid!

PLCS ARE USED IN A WIDE RANGE OF INDUSTRIAL PROCESSES AND CRITICAL INFRASTRUCTURE, INCLUDING BRIDGES. IMAGE: ALEXANDER GRIGORYEV VIA UNSPLASH

Jonathan Greig
February 15th, 2023

Government | Malware | Nation-state | News | Technology

The return of ICEFALL: Two critical bugs revealed in Schneider Electric tech

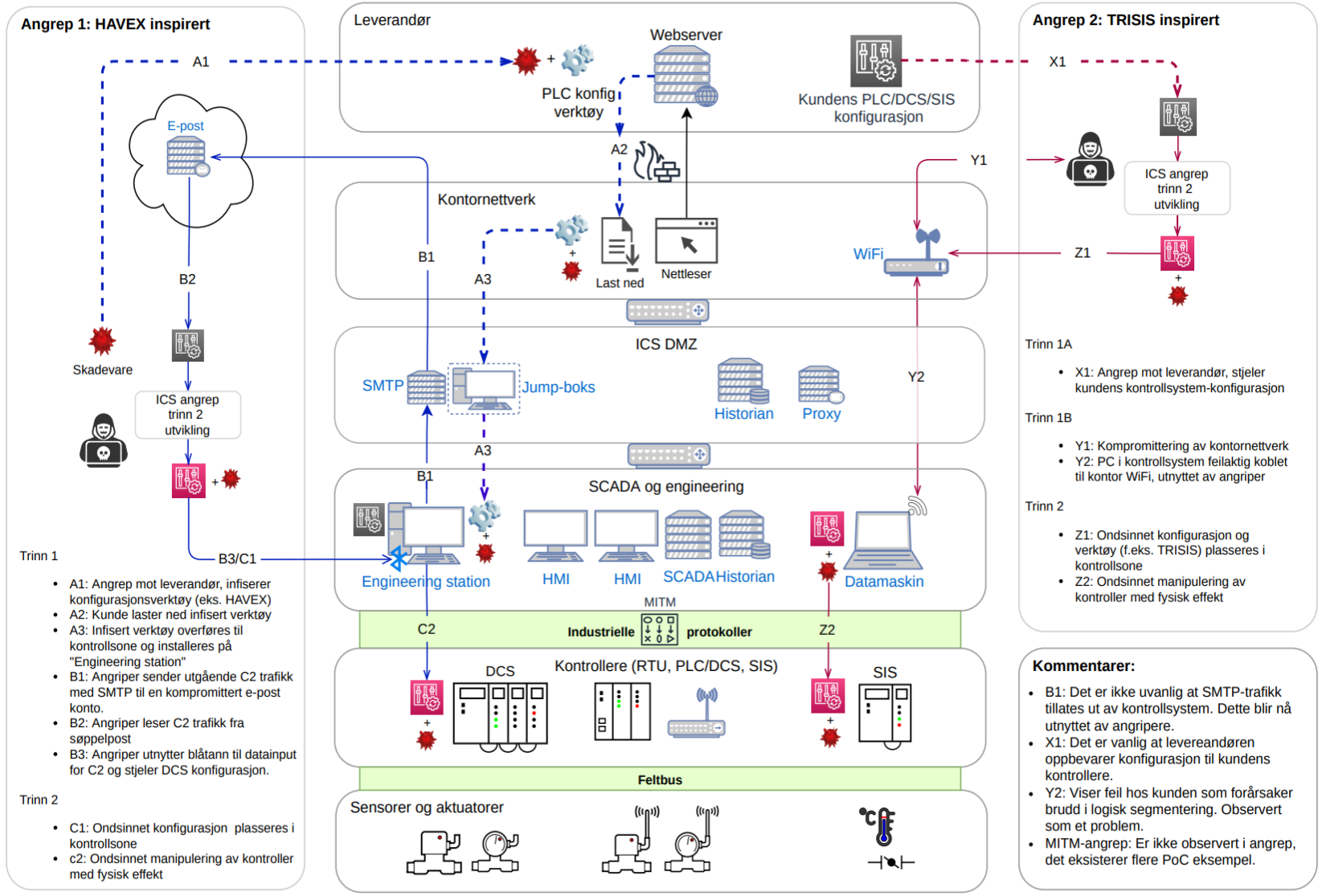
Researchers have announced two critical vulnerabilities in some operational technology systems made by the digital automation giant Schneider Electric.

The announcement comes just months after researchers at Forescout and the U.S. Cybersecurity and Infrastructure Agency (CISA) disclosed some 56 bugs affecting a roster

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)
- Industroyer 2 (mot Ukraina i 2022, etter krigsutbruddet)

Eksempel på angrep med skadevare mot kontrollsystem



Våre funn/observasjoner

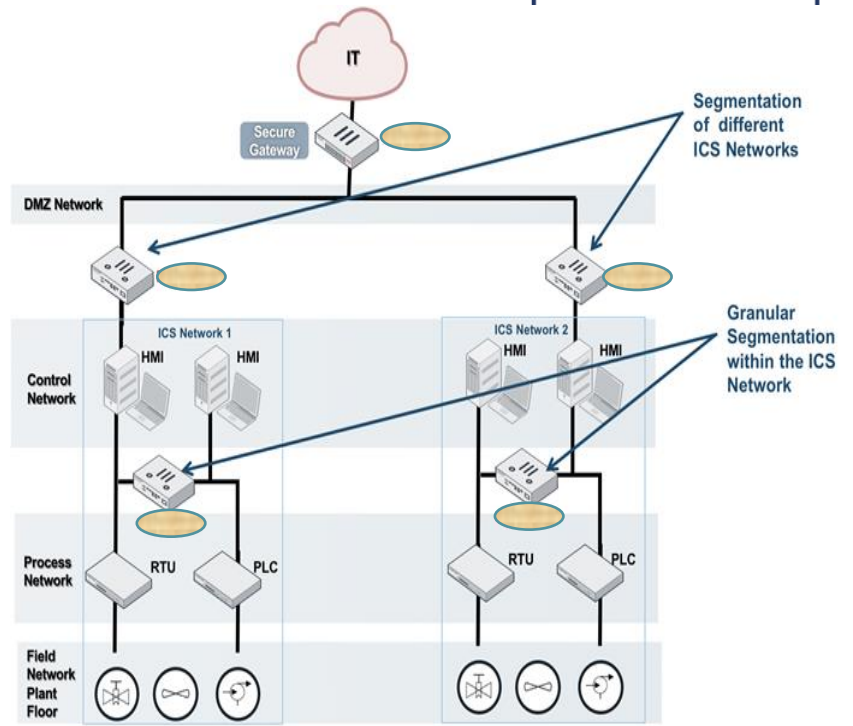
- Kommune A: Manglende sikkerhetskontroll for ekstern pålogging
  - Ikke MFA ved tilgang utenfra
  - Svake/gjenbrukte passord og RDP-pålogging
  - Oppdatering for sjeldent (hver 6. måned)
- Kommune B: For gamle systemer – ikke oppdaterbare:
  - Ikke MFA ved tilgang utenfra
  - 10-14 år gamle systemer (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…?)

Våre funn/observasjoner (forts)

- 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 **(inkl. leverandører!)**
- Sørg for gode passord som ikke deles, og ikke bruk default fra leverandør!
- Vær oppdatert – bygg et effektivt og raskt oppdatering/patcheregime
- Segmentér de ulike delene – tilgang, applikasjon og driftskontroll
- Fjern utrangert utstyr – disse er alltid en sikkerhetsrisiko
- Sørg for reell offline backup
- Kriseøvelse/beredskapsplan – kan systemet driftes manuelt i en periode og er det øvet?
- Kontinuerlig opplæring og øvelse av brukere i operativ informasjonssikkerhet – sikkerhetsbevissthet fra toppledelse til vanlig ansatte
- Vær forberedt!
    - Opprett, vedlikehold og tren på planer for å svare på et angrep og gjenopprette driften etter en krise
- + gjennomgang av K-CSIRT kontrollskjema (se neste slide)



Eksempel spørreskjema fra K-CSIRT

Kommune-CSIRT: Cybersikkerhetsspørsmål for tekniske installasjoner og V

Kommune - avd _____

Ansv. kommunen _____

E-post _____

Dato for svar _____

Ansv. Kommune-CSIRT _____

Spørsmål	Svar	Kategori	Følges opp
1. Hvilke IP-adresser og DNS-navn (tjenestenavn) er eksponert mot internett? Vi ønsker en liste over disse slik at vi kan gjøre et eksternt skann av disse.	(denne ønskes mottatt før vi møtes om de andre spørsmålene, sendes til csirt@kommunecsirt.no – kan krypteres i MS 365)	Eksp infrastr og tjenester	
2. Hvordan er VA/teknisk drift organisert med hensyn til ansvar? Teknisk og organisatorisk.		Org/drift/vedl.	
3. Hvem drifter infrastrukturen? For OT*? For IT?		Org/drift/vedl.	
4. Hvem har ansvar for digital sikkerhet? Rolle/person.		Org/drift/vedl.	
5. Hvordan håndteres/kravstilles informasjonssikkerhet mot leverandørens løsning(er)?		Org/drift/vedl.	
6. Avtale med leverandør: Beredskapsavtale? Driftsavtale? Support?		Avtaler/beredskap	
7. Hvilke leverandører har dere egne avtaler med? Navn og funksjon på komponenter, programvare og leverandør		Avtaler/beredskap	
8. Rapportering: Når rapporteres digitale sikkerhetshendelser, og til hvem?		Org/drift/vedl.	
9. Hvordan skaffer driftsansvarlig og sikkerhetsansvarlig seg kunnskap om sårbarheter og kritiske oppdateringer?		Org/drift/vedl.	
10. Norsk Vann og andre ekspertorganer anbefaler tre soners segmentering (tilgang, applikasjon og DKS**). Hva har dere, og hva kan leveres? Planer?		Org/drift/vedl.	
11. Er det operative backup-prosedyrer av systemet? Administrative systemer, SCADA og driftskontroll. Hvis nei, hvorfor ikke?		Org/drift/vedl.	
12. Kan styringssystemene nås fra kommunens administrative nett? Hvis ja, hvordan er tilgangen sikret?		Eksp infra og tilgang	
13. Beskriv eventuell trådløs kommunikasjon mot eller fra for		Kommunikasjon	

Takk for oppmerksomheten.

Spørsmål?

https://kommunecsirt.no

bjorn@kommunecsirt.no

T. 90 85 00 42