Version 0.9, 2020-09-24 16:47

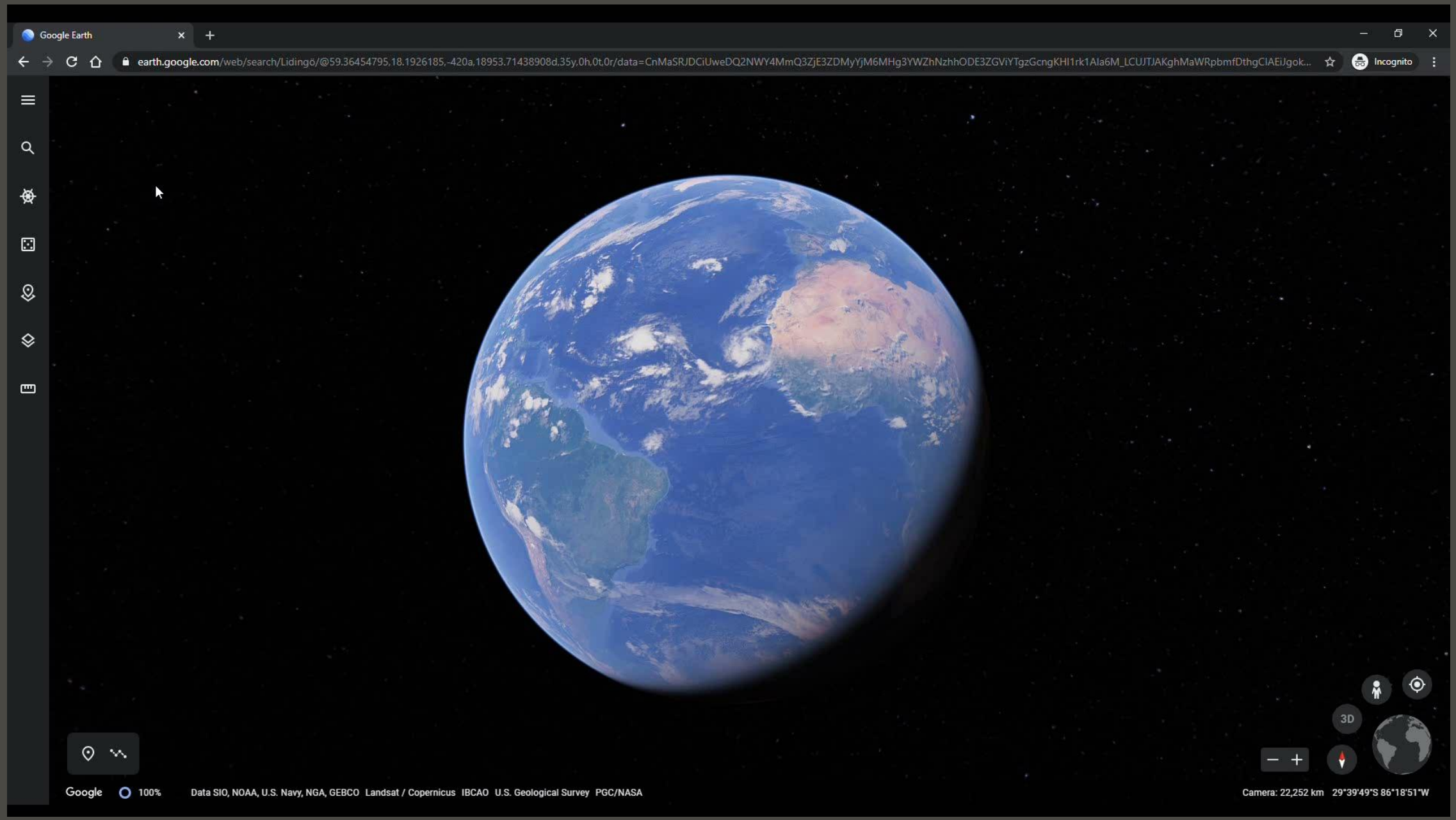
Årets digitaliseringskommun under attack

Per-Johan Gelotte, Lidingö stad

Myndigheten för samhällsskydd och beredskap

Mars 2018

Myndigheten för samhällsskydd och beredskap




Lidingö centrum
LIDINGÖ
Ropsten
STOCKHOLM CITY

Lidingö stad

- Antal invånare 48 200
- 3 200 anställda
- 10 772 belysningsstolpar

Per-Johan Gelotte

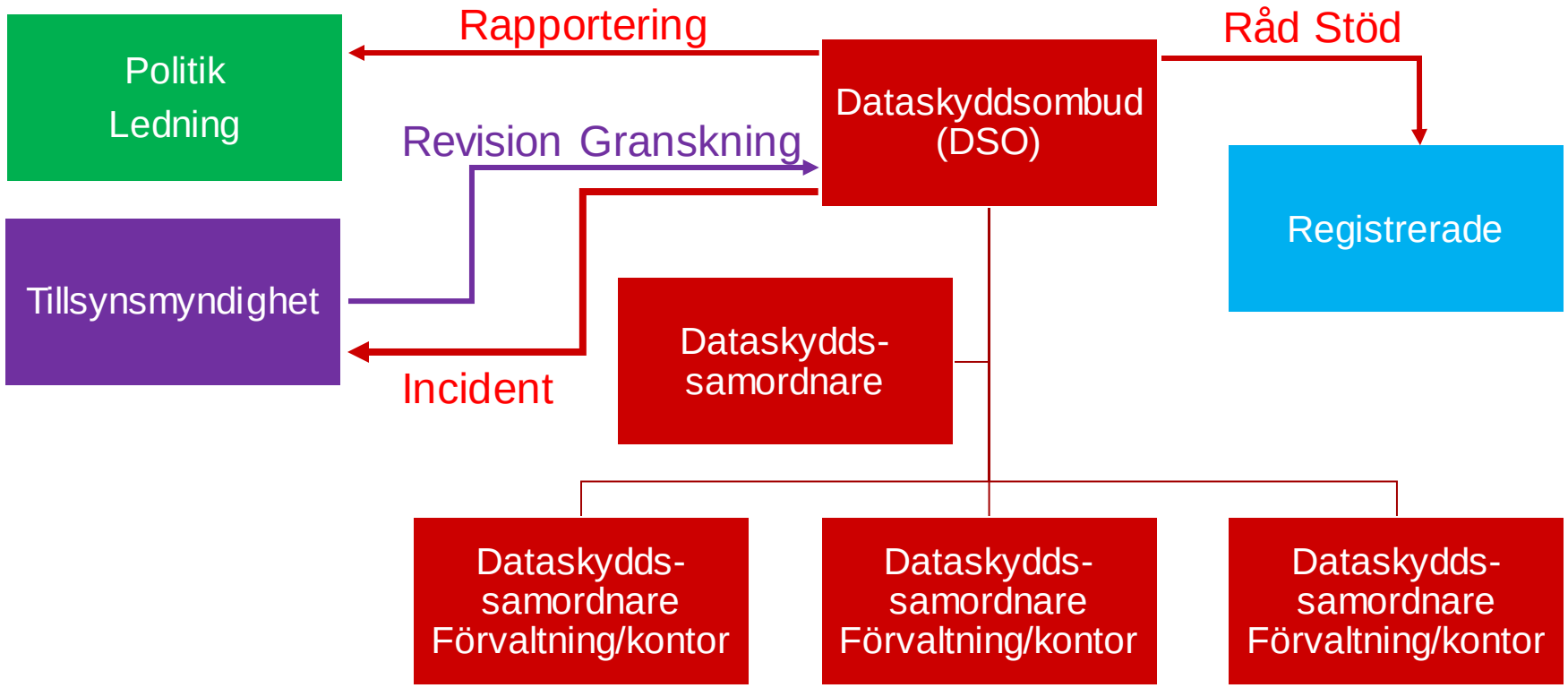
It-arkitekt, Lidingö stad

Kulturhuset Stadsteatern, Bitr IT-chef

Månskensbonde, Elfviks gård

https://www.linkedin.com/in/per-johan-gelotte/

Dataskyddsorganisation



SVERIGES DIGITALISERINGSKOMMUN 2019

Myndigheten för samhällsskydd och beredskap

Varför Sveriges Digitaliseringskommun?
Ledningsnivå

- Riktlinjer för digitalisering
  - Handlingsplaner för varje nämnd
- Aktivt stöd från politiken
- Utvecklingsfond
- Ledar- och medarbetarlyftet
- Digitalt först
- E-learning

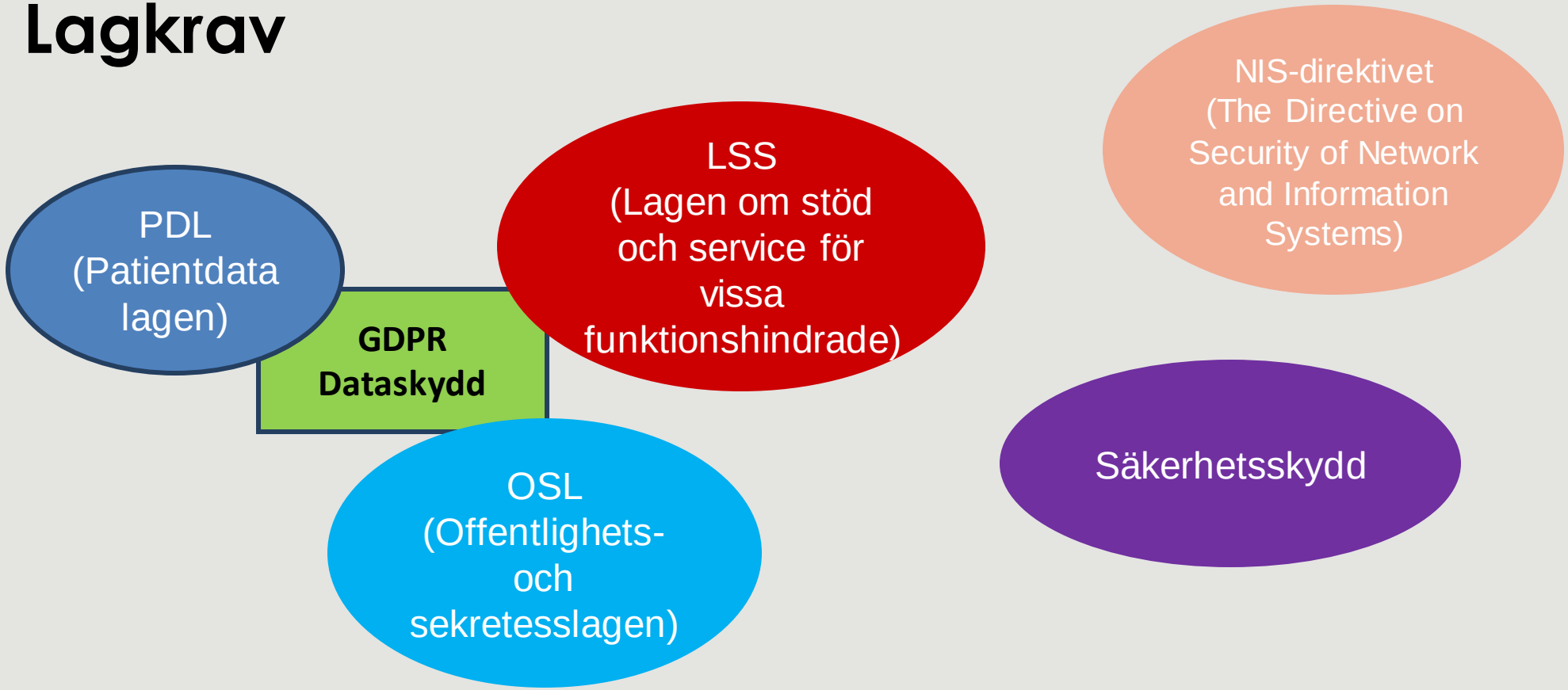
Varför Sveriges Digitaliseringskommun?
Operativ nivå

- Metodiska och effektiva it-upphandlingar
- It-enheten: Möjliggörare
- Tillåtande
- Hybridmiljö
- Delaktighet i Vinnovaprojekt
- Test av välfärdsteknik
- IoT-piloter

”Hej Google, töm alla vattentorn.”

Myndigheten för samhällsskydd och beredskap

Lagkrav

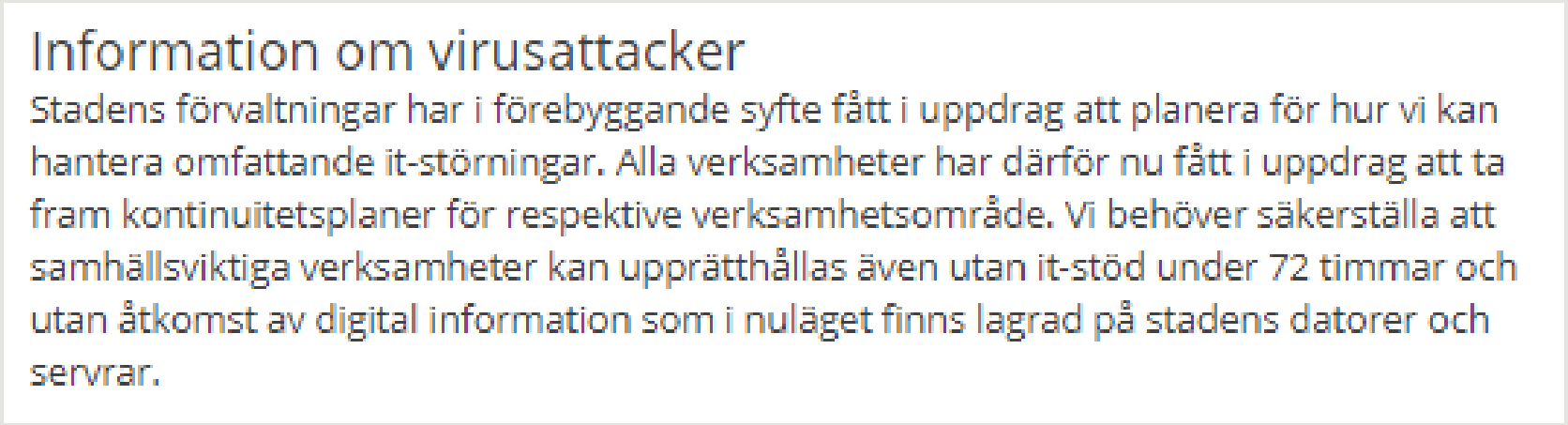

PDL
(Patientdata
lagen)
GDPR
Dataskydd
LSS
(Lagen om stöd
och service för
vissa
funktionshindrade)
NIS-direktivet
(The Directive on
Security of Network
and Information
Systems)
Säkerhetsskydd
OSL
(Offentlighets-
och
sekretesslagen)

”Pga GDPR, NIS, PDL och OSL får vi inte använda era namn … så kan den med syfilis gå till doktorn nu”.

Myndigheten för samhällsskydd och beredskap

Hygienfaktorer - organisationen

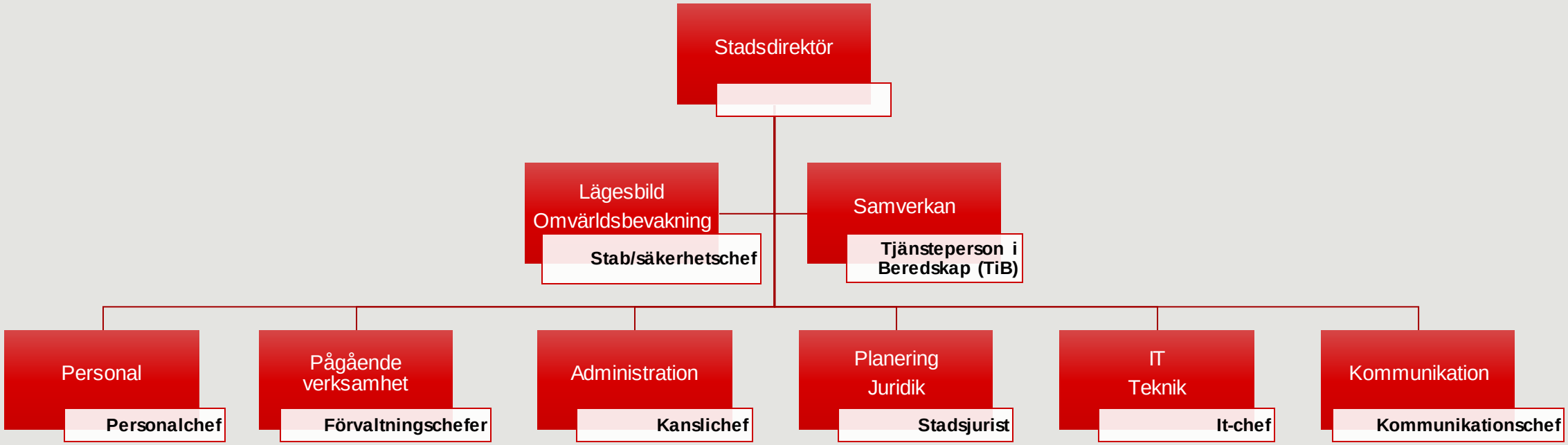
- KLASSA från SKR
  - Informationsklassificering enligt MSB:s metodstöd för informationssäkerhet
- Systemförvaltningsmodell
- Riskanalys
- Kontinuitetsplaner



Hygienfaktorer - It-enheten

- Prioritetsordning system (enligt KLASSA)
- Intern brandvägg
- Logg och avvikelsedetektering, brandväggslarm
- Segmentering
- haveibeenpwned.com, nvd.nist.gov
- Cert.se
- Härdning efter pentester
- Dubbla virusskydd
- Katastrofplaner – inkl kontaktlistor

Central krisledning



Lokaler för krishantering

- Kriskommunikationsgrupp
- Centrala krisledningsgruppen (CKL)
- Krisledningsstaben
- Vilorum

- Externt krisledningsrum

outlook.office.com/mail/deeplink?version=20200914002.05&popoutv2=1

Svara | Ta bort | Skräppost | Blockera | ···

199 emails on lidingo.se have been pwned in the Verifications.io data breach

Får du för mycket e-post? Avsluta prenumerationen

Översätt meddelandet till: Svenska | Översätt aldrig från: Engelska

H

Have I Been Pwned <noreply@haveibeenpwned.com>
Sön 2019-03-10 04:33
Till: Per-Johan Gelotte

An email on a domain you're monitoring has been pwned

You signed up for notifications when emails on **lidingo.se** were pwned in a data breach and unfortunately, it's happened. Here's what's known about the breach:

Breach:	Verifications.io
Date of breach:	25 Feb 2019
Accounts found:	763,117,241
Your accounts:	199
Compromised data:	Dates of birth, Email addresses, Employers, Genders, Geographic locations, IP addresses, Job titles, Names, Phone numbers, Physical addresses

E-post - Per-Johan Gelotte - Outlook - Google Chrome

outlook.office.com/mail/deeplink?version=20200914002.04&popoutv2=1

Svara | Ta bort | Skräppost | Blockera | ···

Ev pågående spam attack?

Till: Per-Johan Gelotte
Kopia:

Hej,

Är lite smått orolig över en viss trendvarning ifrån Microsoft 365 Security & Compliance – Threat management, så tänkte flagga lite för det.
Bör nämnas att det är så pass nyligen som det aktiverades så svårt att säga hur pass ovanligt det är, men vi har gått ifrån ca 7 tusen spam mail om dagen, till runt 316 tusen i går och i dag.

Det mesta verkar fastna i filter, men en del slinker nog igenom.

Onsdag 13/3 2019 vid hemgång

Security State

Endpoint Protection Client Status

Total active clients in this collection protected with Endpoint Protection: 97,1%

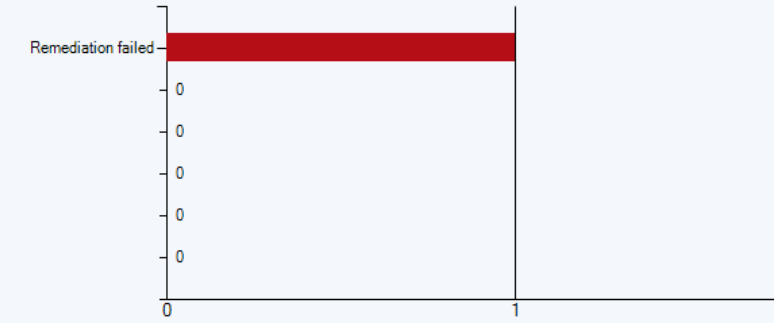
Endpoint Protection clients in this collection that are active: 1195

Active clients protected with Endpoint Protection: 1160

Active clients at risk: 35

Malware remediation status

1 /1472 affected by malware.



Myndigheten för samhällsskydd och beredskap

Torsdag 14/3 2019 morgon

Security State

Endpoint Protection Client Status

Total active clients in this collection protected with Endpoint Protection: 97,1%

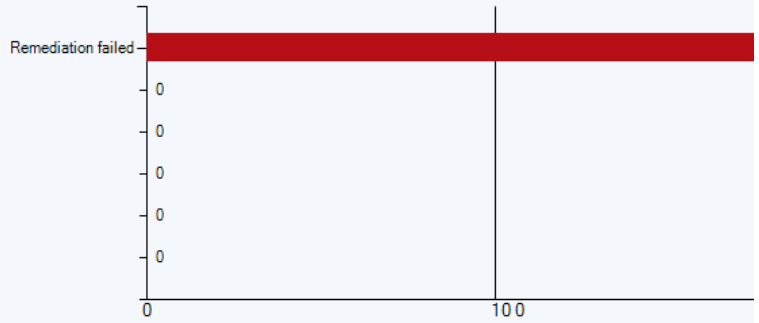
Endpoint Protection clients in this collection that are active: 1195

Active clients protected with Endpoint Protection: 1160

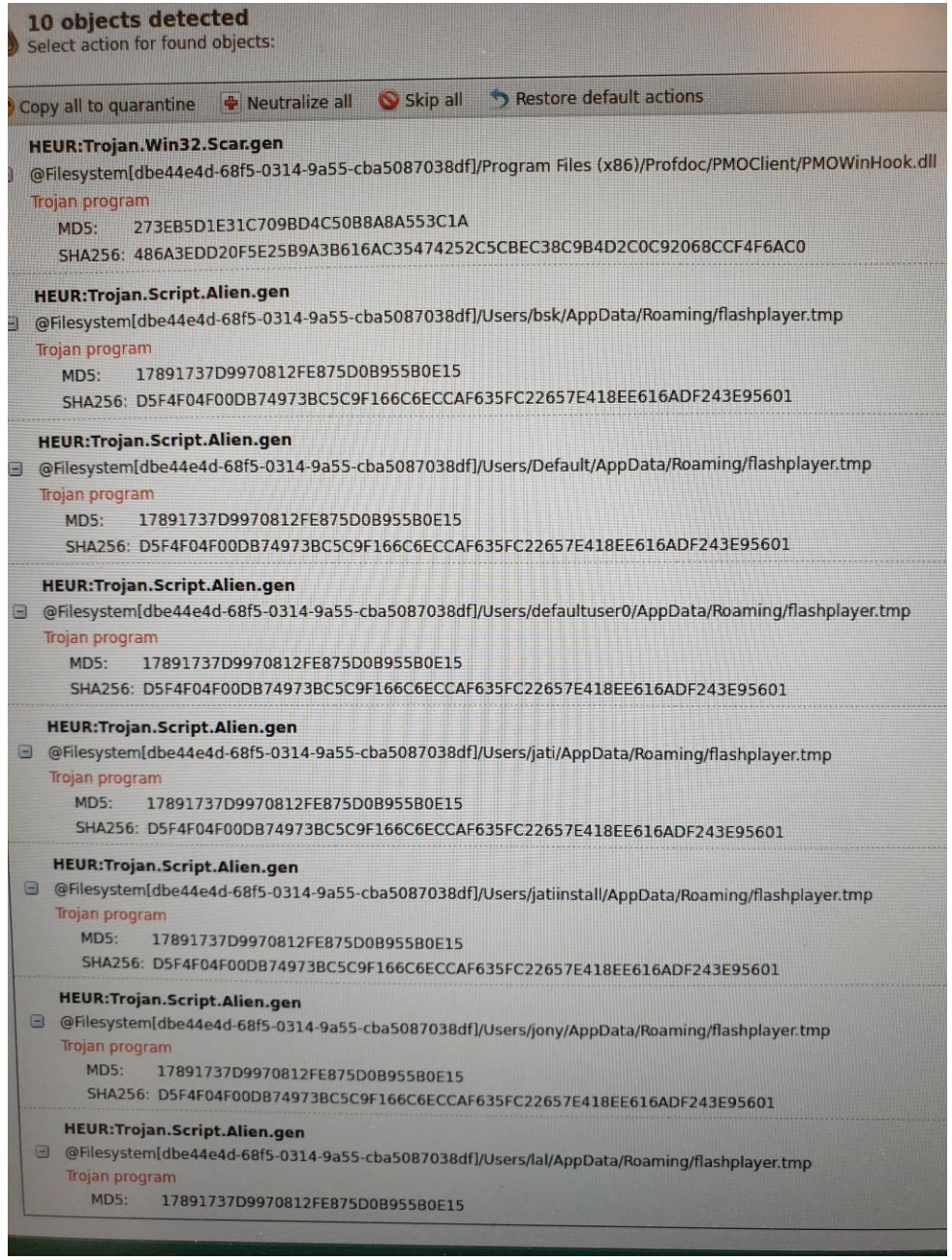
Active clients at risk: 35

Malware remediation status

471 /1472 affected by malware.



Myndigheten för samhällsskydd och beredskap



The shit has hit the fan

Myndigheten för samhällsskydd och beredskap

Incidenthantering från CKL

- Centrala krisledningen, CKL, samlas under torsdagskvällen och är aktiv under natten mot fredag
- Inkallade med 1,5 timmes inställelse
- Tjänsteperson i beredskap, TiB, leder till CKL finns samlad

Kommunikation

- Informationsskärmar
- SMS
- Fredagsfrukost

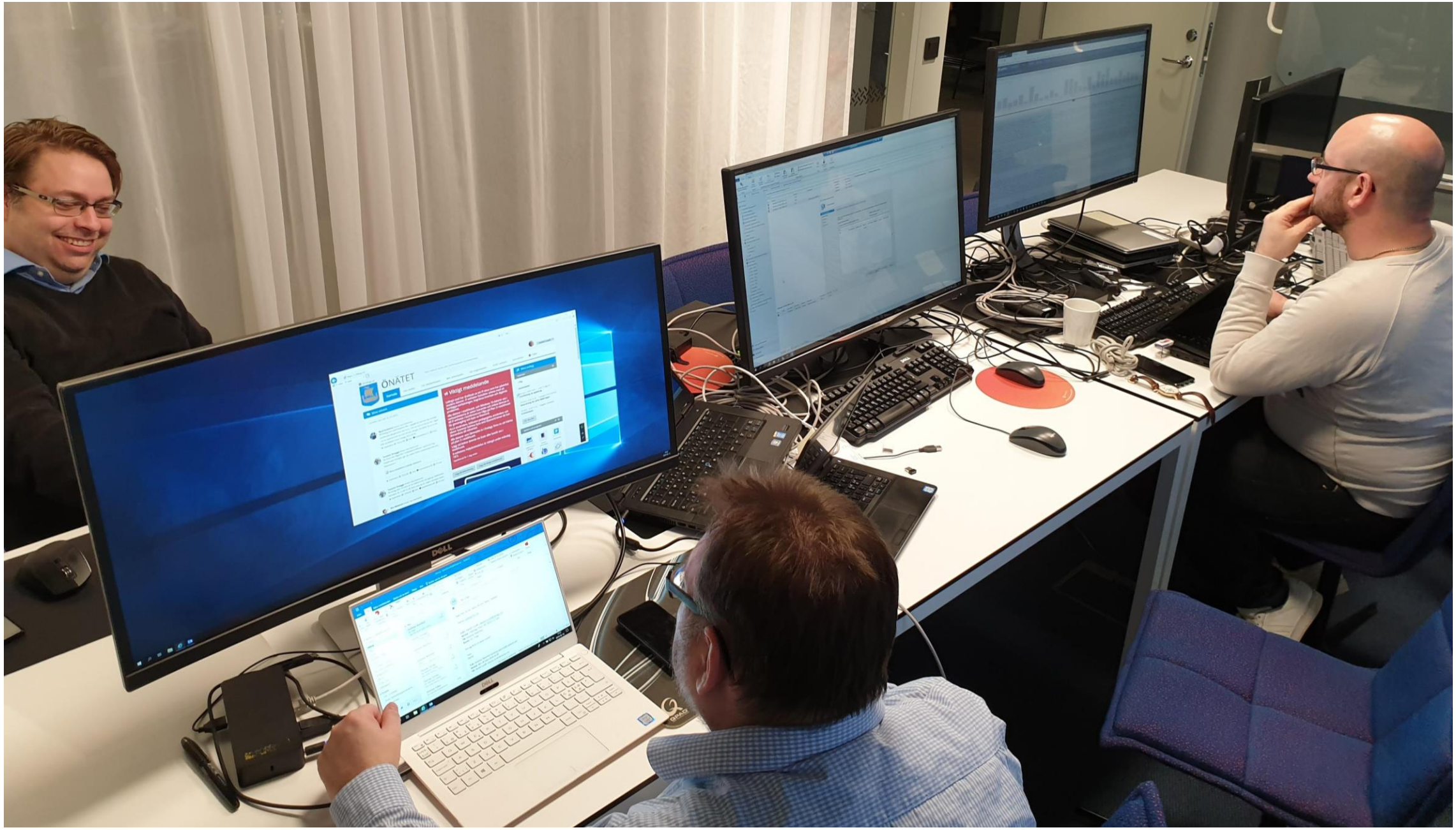
Myndigheten för samhällsskydd och beredskap


Här registrerar du dig

Vad gör it

- Isolering av infekterade datorer - ominstallation
- Stänger in/utgående i externbrandvägg
- DMZ-system stängs ner
- Klienter kan inte prata med varandra
- Tvingande lösenordsändring
- Samarbete med Microsoft (ATP)
- Cert.se – multipla offline-skydd
- Utökad loggning och övervakning DC och verksamhetskritiska system (enligt KLASSA) – håller interna brandväggen attacken stången?
- Extern granskare/rådgivare

- Vi passar på!



Myndigheten för samhällsskydd och beredskap

I incidentens öga har ”små” saker stor betydelse

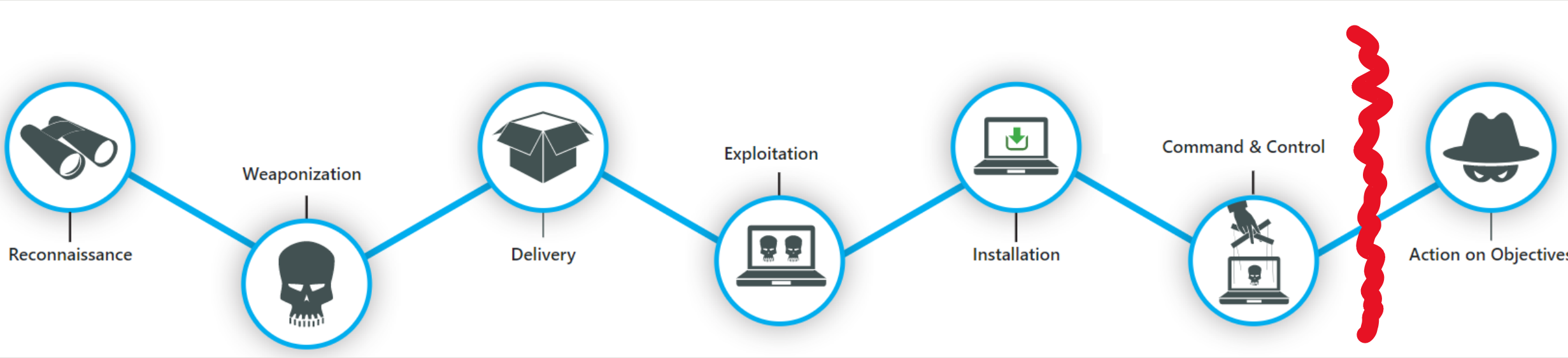
- Använd krishanteringens benämningar
- Använd kodnamn
- Näring

Myndigheten för samhällsskydd och beredskap

Jobba i fred

The kill chain

The kill chain



Resultat

- 900 datorer ominstallerade/kontrollerade
- 3 200 anställda och 8 000 elever bytte lösenord
- Incidentpersonal 900 tkr (1 278 timmar)
- Gick ur incidentläge efter dryga sju dagar.
- Tekniker på helspänn
- Höjd förståelse för it-säkerhet
- Samhörighetsskapande

SvD NÄRINGSLIV Nyheter Näringsliv Kultur Ledare Debatt Tidningen

Norsk Hydro utsatt för cyberutpressning

Norsk Hydro har angripits i en cyberattack. Arkivbild Foto: Fredrik Hagen NTB/Scanpix/TT

Norsk Hydro, en av världens största aluminiumtillverkare, är utsatt för en omfattande attack mot koncernens IT-system. De som ligger bakom kräver pengar för att stoppa attacken.

TT
Uppdaterad 2019-03-19
Publicerad 2019-03-19

– Efter angreppet har vi jobbat på att isolera och neutralisera viruset. Alla anläggningar är isolerade och det ser inte ut att ha drabbat oss utanför Norge, säger Norsk Hydros finansdirektör Eivind Kallevik på en presskonferens.

Enligt Kallevik har inga säkerhetsproblem uppstått till följd av angreppet, som dock slår ut datorer och försvårar administration och produktion.

NyTeknik

Premium / Automation / Digitalisering / Energi / Fordon / Startup / Ingenjörskarriär / Lediga j

ANNONS

SÄKERHET

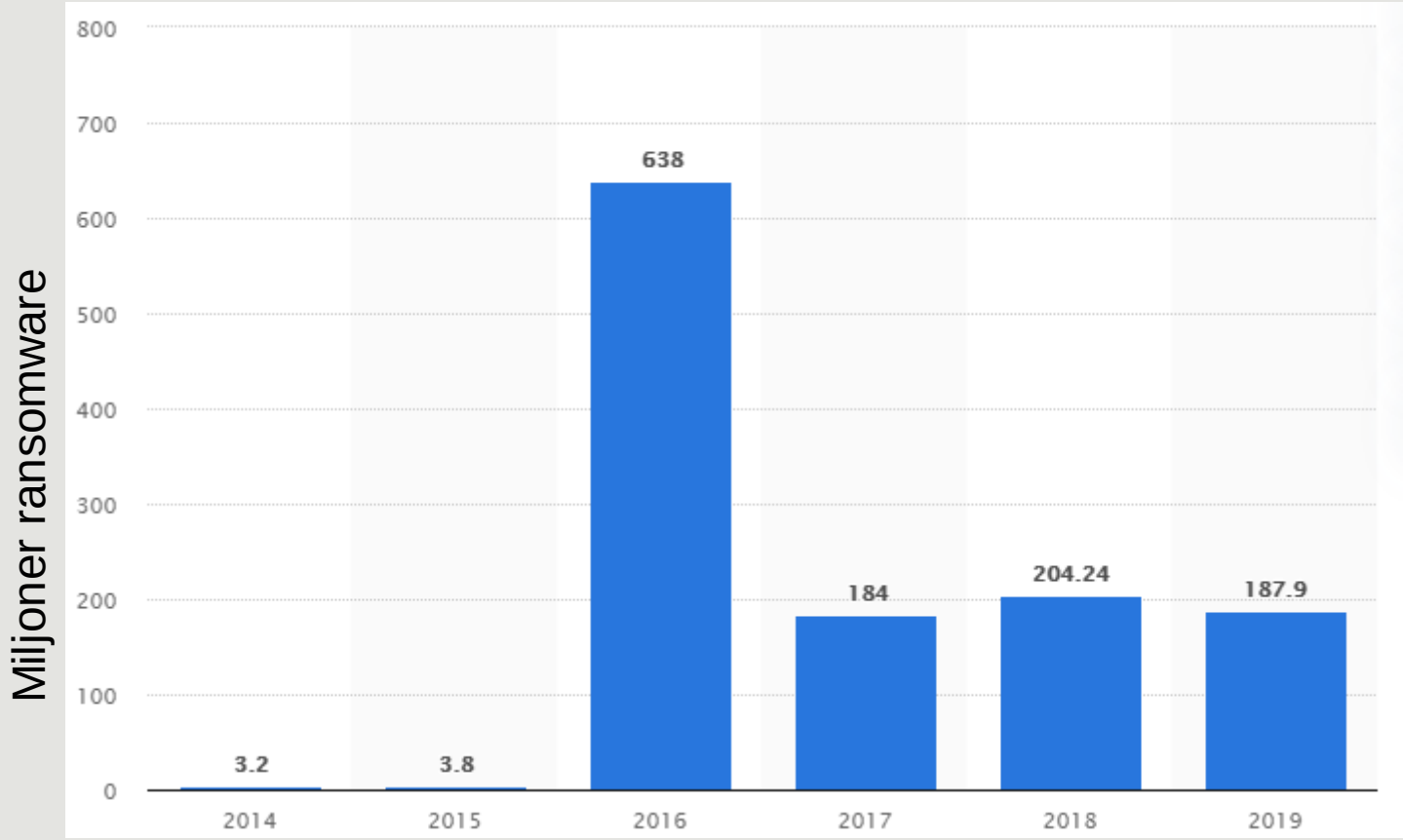
Addtechs it-system fortfarande utslagna efter hackerattack

2019-11-15 10:00 Av: Simon Campanello 1 kommentarer

För två veckor sedan drabbades teknikkoncernen Addtech av ett ransomwarevirus. Fortfarande har många av dotterbolagen stora problem, med försenade leveranser till följd.

Onsdagen den 30 oktober drabbades Addtech av ett omfattande cyberangrepp.

Alla är hela tiden under attack



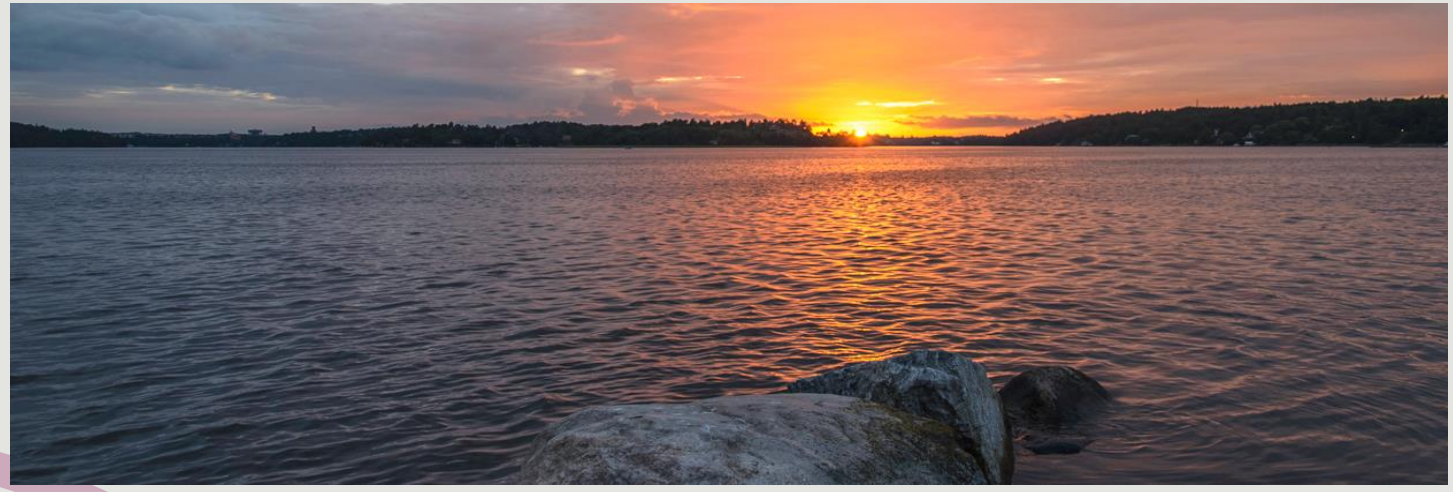
Källa: https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/

Vad har vi lärt oss?

- Veta att man är under attack är 70% av striden
- Utomstående ”second opinion” med kylan
- Tekniker som är tillfreds och därmed trogna
- Förhindra kommunikation mellan klienter
- Tjänsteleverantörs standardinställningar räcker inte

Välkommen till Lidingö




LIDINGÖ STAD

Myndigheten för samhällsskydd och beredskap