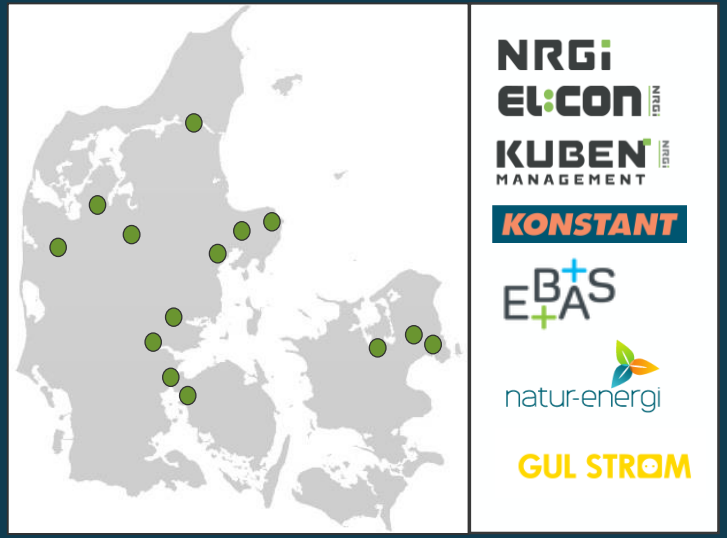
NRGi rammes af omfattende hackerangreb

Cybersikkerhed DI 2019

Cybersikkerhed DI 2019 – Hvem er NRGi?

- 210.000 andelshavere i det østjyske
- + 330.000 kunder
- 1.300 medarbejdere

- Elsalg
- Installation
- Rådgivning
- Elnet, kritisk infrastruktur
- Huseftersyn / tilstandsrapporter



- NRGi ejer andel i blandt andet Clever, Fibia og Energi Danmark

Cybersikkerhed DI 2019 – Hvem er jeg?

Michael Warrer

- CIO i NRGi, ansvarlig for 32 folk.
- 25 års erfaring
- IT-ledelse, drift, GDPR, udvikling og sikkerhed.
- Fokus på IT-strategi og forretningsudvikling i forhold til bedre udnyttelse af IT.
- Medlem af diverse IT-sikkerhedsgrupper, som er med til at udforme ”regelsæt” for kritisk infrastruktur i Danmark.

Uge 35 – 2015. NRGi rammes af omfattende hackerangreb

- Vores sikkerhed før den 28.8.2015: Fokus og tiltag var til stede, der var diverse IT sikkerhedspolitiker, PWC havde lige udgivet en rapport om energisektoren, gennemsnit var 2.5 ud af 5, vi var over gennemsnittet.
- Først opkald kl. 07. Beredskabsplan blev aktiveret. Alt lukkes ned og der ringes efter ekstern hjælp ☺
- 170 servere var blevet krypteret og NRGi blev afkrævet en løsesum i bitcoins. Noget der ligner 4 millioner, i alt eller pr. server ?
- Indsamling af data og så restore, restore og restore fra Veeam, 3Par snap og DPM. Vi har et godt backup system, som dog kan gøres endnu bedre. 170 servere genskabt på under 60 timer.
- Vores SQL / database backup var ramt.
- Hackerne har haft domæne administratoradgang relativt tidligt i angrebet, hvilket de udnyttede til at stoppe og nulstille log.
- De har brugt hackerværktøj, som de havde installeret på web serveren uden om alle vores overvågningssystemer. Desuden har de brugt teamviewer og installeret en virtuel pc.
- De har hentet hele AD'er, hvor de brød en stor del af brugernes passwords inklusiv domæneadministrator konti.
- Eksterne konsulenter mener at det lykkedes angriberne at kompromittere og få adgang til en web server via port 80, sandsynligvis via en fejl / sårbarhed i web serverens software.
- Der er i analysen ikke fundet spor efter om SCADA systemerne (el drift) er blevet kompromitteret. Det samme gør sig gældende for kundedata.
- IT sikkerhed er nu kommet på bestyrelsesniveau ☺

Hvad har vi gjort ?

- Fokus på infrastruktur og ikke den enkelte pc.
- Fokus på adfærd, awareness, ”den enkelte medarbejder” og arbejdet omkring.
- Fokus på servicekonti, lokale admin og sikkerhedsindstillinger på alle servere.
- 2 faktor validering af alle Domain admins.
- Second generation firewall, IPS/IDS / "intelligent" firewall. IPS / IDS på alle servere.
- Optimering af backup.
- Automatisk patch / opdateringer af servere.
- SCADA net total lukket.
- SIEM løsning med AI.
- Vigtig med en god og forståelig beredskabsplan.
- Træn beredskabsplan og restore
- National strategi for cyber- og informationssikkerhed.
- ”Skrivebordsarbejde” og procedure er ikke nok.

NRGi

IT-sikkerhed i fokus

IT-sikkerhed skal ikke blot være en forsikring, som man forhåbentlig ikke skal bruge, men skal også give værdi, så det ikke kun ses som en udgift.

- **IT sikkerhedskampagne / awareness ”styret” af koncernen**
  - **Info, info og info**
  - **Afsæt ressourcer**
  - **”Roadshow”.**
  - **Inddrag privat pc brug, ”sjove” og skræmme hændelser / historier.**
  - **Quiz.**
  - **Phishing mail.**
  - **Små og hyppige beskeder**
  - **Man kommer langt med sund fornuft og en god IT adfærd**

NRGi

IT-sikkerhed i fokus

- IT-sikkerhed på direktion og bestyrelsesniveau
  - IT sikkerhedstiltag skal gælde for hele koncernen og forankres i topledelsen. Fokus skal holdes hele tiden.
  - Det er vores fælles ansvar, at IT-sikkerheden er i orden, også selv om der benyttes ekstern bistand og samarbejde
  - Balance mellem sikkerhed, brugere, arbejdsgange og økonomi.
  - Vær åben og vis synlighed, så fokus kan holdes og der kan skabes bedre forståelse for IT-sikkerhed.
  - Lav bling-bling rapporter og dashboards. Pas med for meget teknik.
  - Det er direktionens / bestyrelsens ansvar. Jeg er rådgiver og skal opstille konsekvenser og risici. PAS på med ”følelser”.
  - GDPR er under IT-sikkerhed.

- Værdien ved udvidelse af IT-sikkerheds tiltag (SIEM, log mm) udover sikkerheden har fået et løft
  - Alt samles et sted, både sikkerhedshændelser og GDPR ”data”.
  - Hændelser og data kan bruges proaktiv og spores.
  - AI gør at andre udover IT sikkerhedsafdelingen kan hjælpe.

Der er ikke noget som er 100% sikkert.
Vi kan ikke vinde, men kan vi spille uafgjort er vi langt.

NRGi