TVIS
sammen om varmen

Cyberforsvar mod en usikker verden

- Der er et behov for øget Cybersikkerhed

- NIS2/CER direktiver – Marts 2025
- Udmøntes i Lov om styrket beredskab

- Ikke omfattet < 50 TJ dvs. ca. 1000 varmekunder

Formålet med NIS2-direktivet er at yderligere styrke og ensarte cybersikkerheden og modstandsdygtigheden overfor cybertrusler på tværs af EU for virksomheder inden for en lang række sektorer og for offentlige myndigheder, som anses for at være kritisk for økonomien og samfundet
– Center for Cybersikkerhed

Millioner af login-forsøg: Cisco advarer om massiv hackerkampagne mod VPN-tjenester

Energi

Elektricitetsvirksomheder
Distributionssystemer
Producenter
Fjernvarme eller fjernkøling
Olierørledningsoperatører
Forsyningsvirksomheder
Naturgasvirksomheder
Brintproduktion og -lagring

Fremstilling

Virksomheder inden for fremstilling og samling af:
Computere, telefon og dataudstyr
Elektroniske motorer, transformere og generatorer
Pumper, kompressorer, kugle og rullelejer
Biler, busser mv.
Skibe, fly mv.

Fødevarer

Fødevarevirksomheder, som beskæftiger sig med engrosforhandling og industriel produktion og tilvirkning

Forsyning

Leverandører og distributører af drikkevand (undtagen hvis ikke væsentlig del)
Virksomheder, der indsamler, bortskaffer eller behandler spildevand fra by, hus og industri

Der er eksempler nok..

Firma regner med at gå konkurs efter stort hackerangreb

I sidste uge var der et stort hackerangreb på OUH.
Foto: Mads Claus Rasmussen/Ritzau Scanpix

Af **Casper Fauerholdt**

Odense Universitetshospital blev i sidste uge udsat for et stort hackerangreb, som nu viser sig at få store konsekvenser.

Det skriver DR.

Angrebet gik ikke ud over patienter, men derimod den eksterne leverandør IT-hotellet, som har servere stående i en gammel bunker ved Fruens Bøge i Odense.

På sin hjemmeside skriver firmaet, at man hverken har de nødvendige interne ressourcer eller økonomiske muligheder for at få ryddet op.

- Det er derfor også vores forventning, af IT-hotellet lukker eller går konkurs som følge af dette angreb, står der.

Hackerangrebet var også voldsommere, end man først vurderede:

- Efter vi har fået gennemgået de enkelte systemer og fået et overblik over angrebets omfang, er det blevet tydeligt for os, at angrebet er langt mere omfattende end først vurderet og har ramt så mange systemer at det ikke umiddelbart kan inddæmmes, skriver IT-Hotellet.

Vand skal der til, og vandforsyningen er kritisk infrastruktur. Derfor tages det også meget alvorligt, når der er hackere, der går efter vand og spildevand. Arkivfoto: Mads Claus Rasmussen/Ritzau

For IT-chef John Gravesgaard og konstitueret direktør for Tønder Forsyning, John Pies Christiansen, har hacker-angrebet i december været noget af et mareridt, som forsyningsvirksomheden internt fortsæt mærker følgerne af. Foto: Tønder Forsyning