Cyberattack
Church of Sweden

- 5,5 million members
- 28 000 users
- a federation of 608 organizations
- outsourced IT
- 600 servers

Svenska kyrkan

How it all began 2023-11-23

- Our SOC (Security Operation Center) detects large-scale reboots and spontaneous encryption in the middle of the night

Svenska kyrkan

Milestones on the first morning

- Get help right away (Truesec)
- Turn off the back-ups
- Inform users what do/don’ts, knowing that the aggressor was “listening”

Svenska kyrkan

First couple of weeks – limit the damage

- Isolate the server hall = stop data theft centrally, threat actor cannot act
- Notify Police and the Swedish Authority for Privacy Protection (IMY)
- IT forensic investigation. How? Where? Infected? Backdoors? Verify not affected.
- 28,000 new passwords undigitally. 1.5 day plan + 1.5 day implementation
- Reinstall more than 4,000 computers (only 2200 computers were infected)
- Washing or new installation of about 600 servers

Svenska kyrkan

Week 3 to the end Feb- Recovery

- Expanding the SOC surveillance to all computers with Microsoft defender
- Relaunching our 500 IT systems again, one by one

Svenska kyrkan

How did it go?

- + Recovery with content
- + Limited data loss
- + Respect for not paying ransom

- - 28 000 people were 1 month almost completely without IT system, gradual recovery months 2-3.
- - Outcome over budget
- - It is not over yet…

Svenska kyrkan