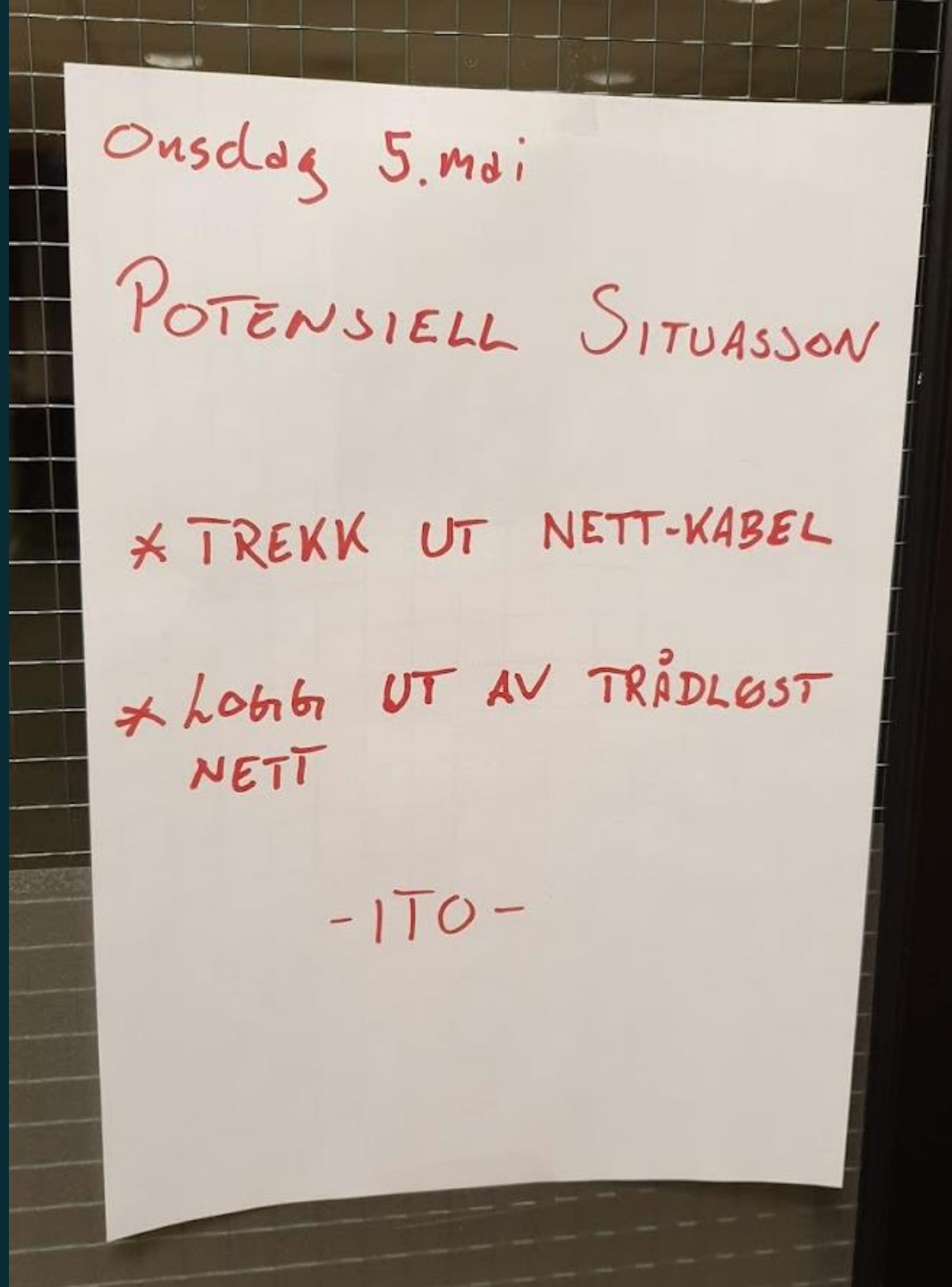
volue

volue

Cyberattack on Volue

The incident in short

- Ryuk Ransomware on Volue Technology infrastructure
- Opportunistic & financially motivated
- Attacker used stolen customer credentials to gain initial access
- Total attack duration approx. 12 hours
- Technical response team from Volue IT and ATEA IRT
- 2 months of massive effort to restore and recover fully
- We released a Post mortem-report and engaged PwC to conduct an external audit on our incident handling



volue

Preparation & incident response

- Volue Technology is ISO 27001 certified
- ISMS and our Contingency plan was key for quick and efficient alerting and setup of the correct teams
- ATEA IRT agreement ensured quick response with the right skillset
- Cyber insurance as a financial safety net

volue

Visibility & information

Having a large number of logs available enabled us to provide a clear and detailed picture of the incident

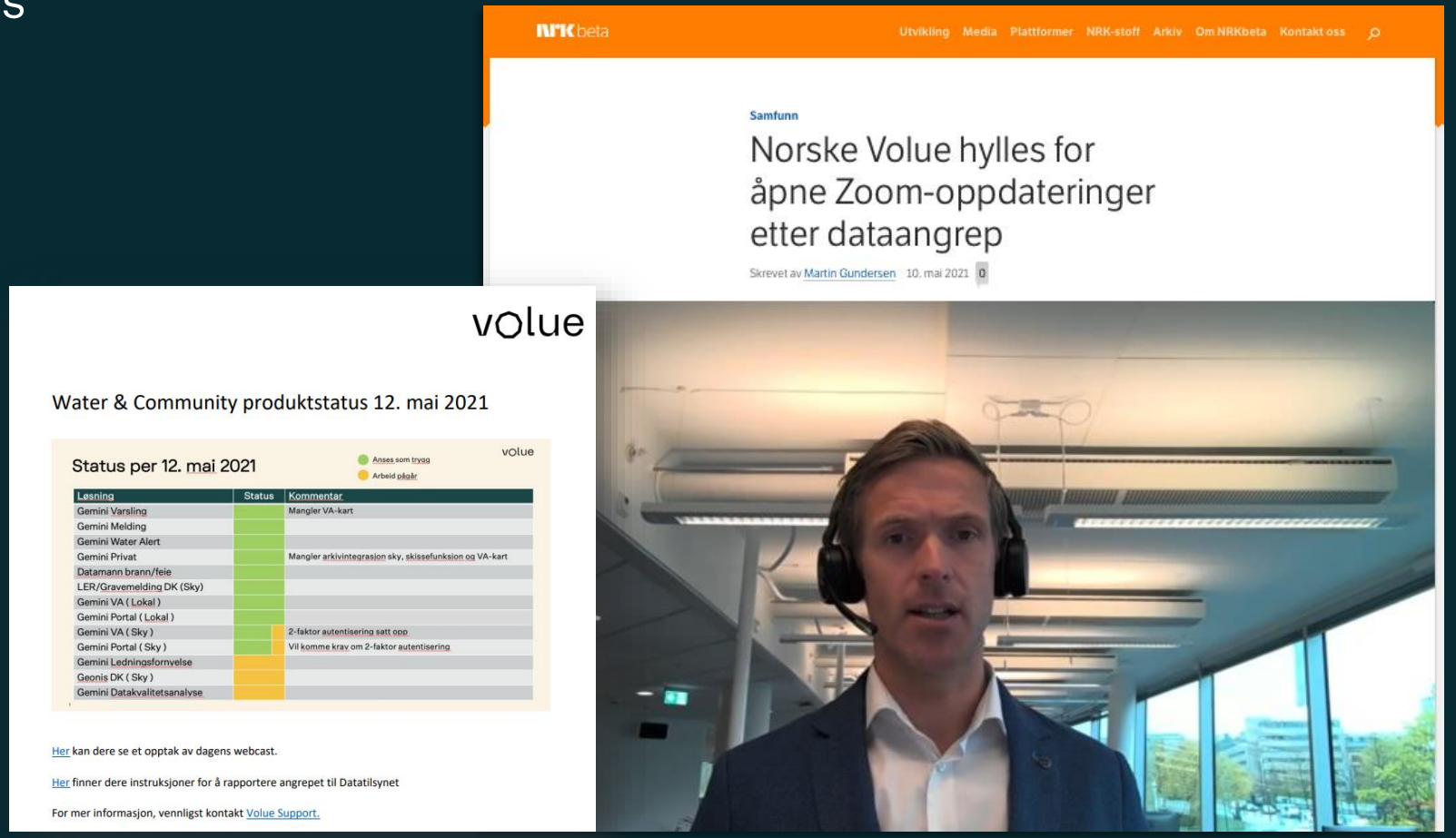
Being able to give our customers confident answers regarding potential data theft was crucial with regards to trust

“Thorough investigations of logs revealed no indications of data exfiltration”

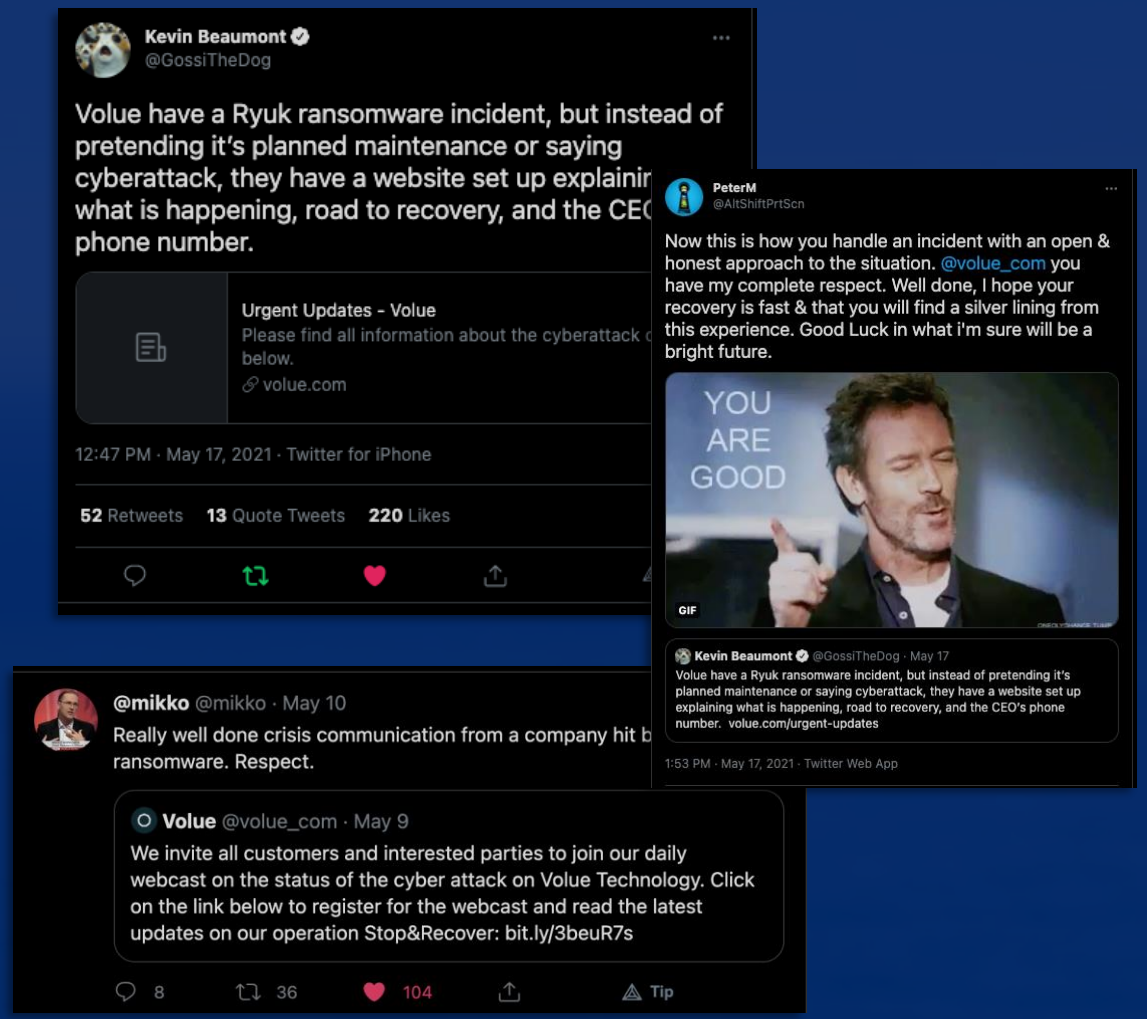
Information control

We had good control on information sharing through a dedicated team and a framework for customer meetings

Having strict control of how we communicated helped us avoid misunderstandings, rumors or conflicting messages



Demonstrate transparency



"Is it just technical issues, or are they hacked?"

We decided to be open and transparent about the incident.

If the fear of reputation loss after cyber incidents decreases, it will leave better possibilities for more companies to choose to make the same decision

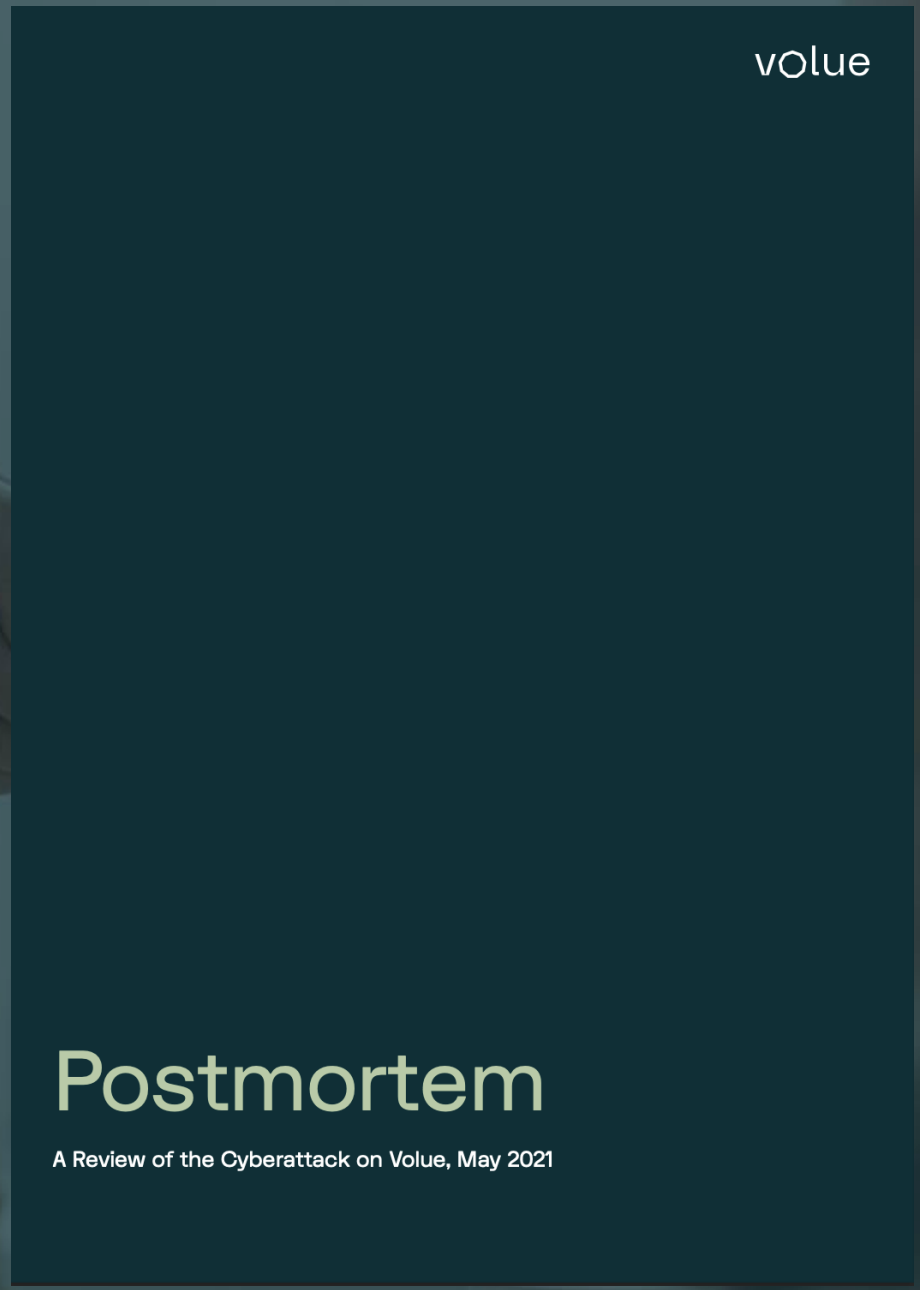
More focus leads to more knowledge, change of attitude and ultimately better security and awareness

Partner up

We teamed up with ATEA IRT to get 24/7 security response and the right skillset to work with us during the incident.

Our cooperation with KraftCERT helped spread technical information and IOC’s to other CERT’s and to customers who requested this.

Thank you

- Postmortem, a review of the cyberattack on Volue, released including:
  - Timeline of the attack
  - Incident management
  - Communications
  - Evaluation and further initiatives
  - Build back better
- Request the report on volue.com

Brynjar Larssen-Aas
Head of IT Operations
Volue ASA
48164617 - brynjar.larssen-aas@volue.com