A Real Experience

“From Business as Usual to NO Business at all”

Lars André – ELKA:a Konsult AB

doc
We make it simple.

MultiCom
SOFTWARE

Powered by
COMMVAULT®

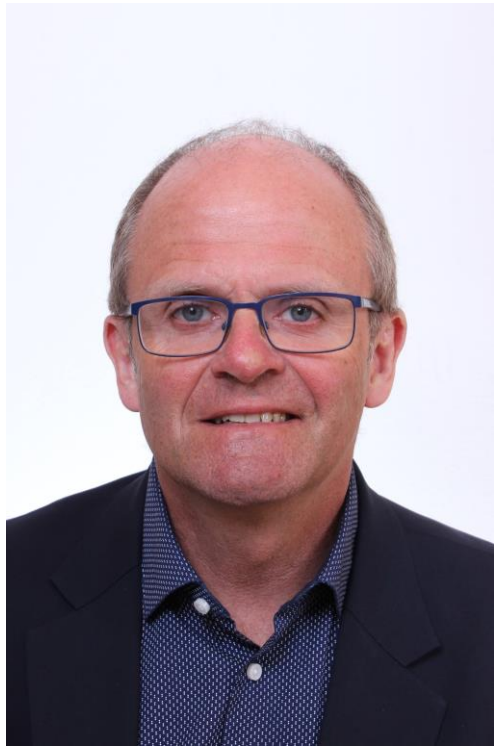
ELKA:a

Lars André

- Experience from ABB, Ericsson and Essnet
- VP-roles in IT at Nasdaq (OMX), TeliaCompany
- CIO att Codan/Trygg-Hansa
- Interims CIO in an European Financial Company in Receivables Management

- Building strong teams
- Transformation
- Information Security

} Main focus in all roles



Lars André, phone: +46-70-5905022, mail: larsjandre@gmail.com, LinkedIn: www.linkedin.com/in/larsjandre

Agenda

- Background
- What happened
- Business impact
- Time lines
- Recovery
- Lessons learned
- Outcomes
- Questions

ELKA:a

Background

- An European company in the financial business based in Germany built on a large number of acquisitions
- Approx 1400 employees spread over 10+ offices
- Operating profit of 100 mEur
- A traditional IT estate with a mix of in-house and outsourced IT services
- IT Security suffering from years of budget cuts
- A penetration test was performed approx. 6 months before the attack
- A cyber security insurance in place

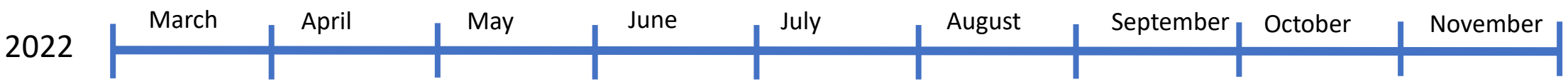
What happened

- End of March 2022 all systems got locked by encryption
- Backups were deleted
- Messages on some screens with clear information what had happened
- BCM team gathered at head quarter

Business impact

- All users were unable to access systems
- All networks had to be shut down
- Business telephony did not work
- Suspicions that data had been stolen
- Internal communications had to rely on traditional text messaging (sms)

Time lines



Infra recovery

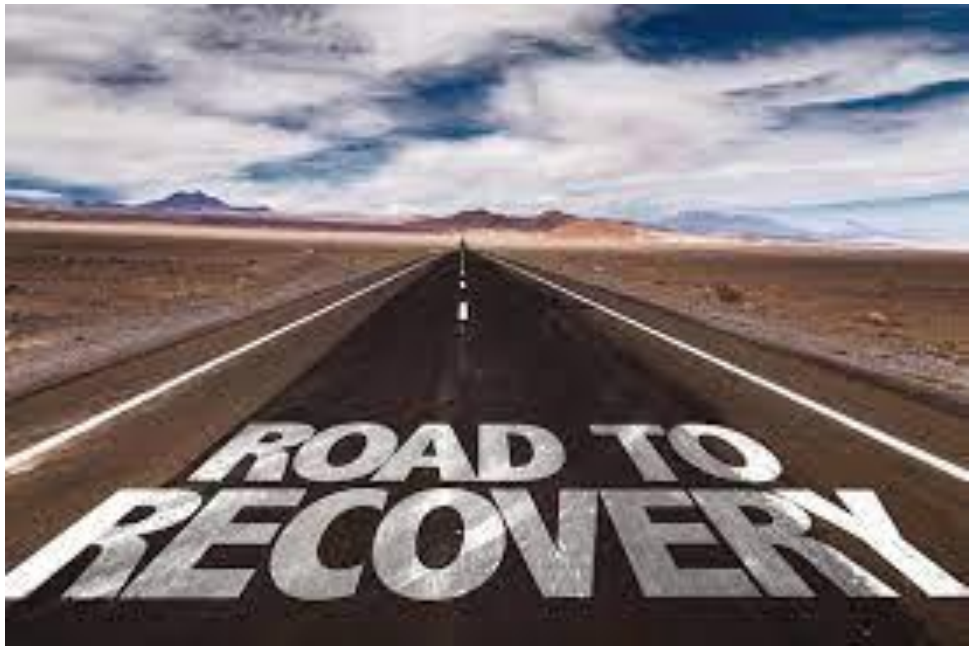
Application recovery

Process improvements

Initial business recovered

Recovery - Infra

- IT staff divided the tasks into a number of workstreams with defined leader for each
- All external access shut down initially
- All hardware run through a cleaning process
- External consulting expertise from IT security partners, Sygnia (an Israelean company) contributed greatly
- It was observed that hackers were sniffing around during recovery
- The IT landscape was very fragmented due to history => challenging recovery
- Very time consuming due to the great variety of old and new HW/SW and a multitude of business applications



ELKA:a

Recovery - Applications

- Not possible initially, had to wait for infrastructure
- Telephony systems priority 1 to be able to resume and continue customer dialogues
- Key individuals incl architects engaged to plan the road to recovery
- Strong co-operation between IT and business to focus on what matters the most
- Access to customer data for sales staff was prioritized
- Time consuming activity due to an unconsolidated environment

ELKA:a

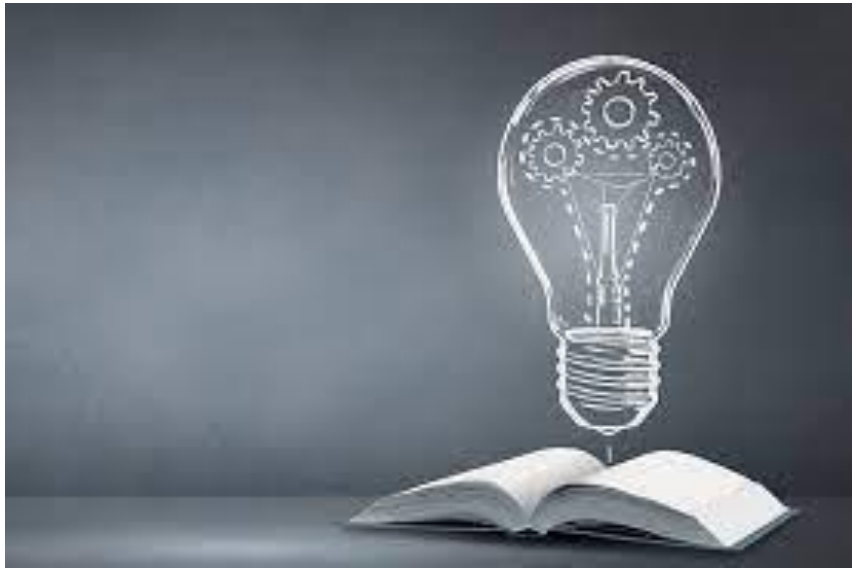
Recovery - Business

- Recovery was divided into three phases
  - Breathing – access to data and telephony
  - Drinking – reaching customer systems across the estate
  - Eating – being able to get back to normal
- Starting were damage was smallest (not encrypted) as well as were business was most profitable but always focusing on being able to provide customer support
- Intense communication with customers and authorities due to possible data leakage
- Most customers very understanding and amazingly patient. Many could move business to other vendors temporarily and then move back

ELKA:a

Lessons learned

- Improve security awareness in the wider organisation (phishing etc). 91% of all IT attacks starts with a phishing-mail according to Deloitte
- The cost of not being prepared is extremely high
- A fragmented IT landscape makes recovery very challenging
- Be on-top of patching schemes
- You can always be hacked but with good organisation and preparations you can get out of it “alive”
- Don’t underestimate the need for investments in your IT environment
- Have a well defined crisis management structure incl. alternative communication solutions in place



Outcomes

- Migration from legacy was speeded up and completed ahead of plan
- A great team-building exercise
- Architecture has been more IT security focused since the event
- Better processes in place now
- A common view in the organisation on what to prioritize

Questions ?

Thank You