Ransomware Nightmares

and how to wake up...

20. SRT – 31.Oct.2023

Alex Diekmann
Director Corporate Security
u-blox

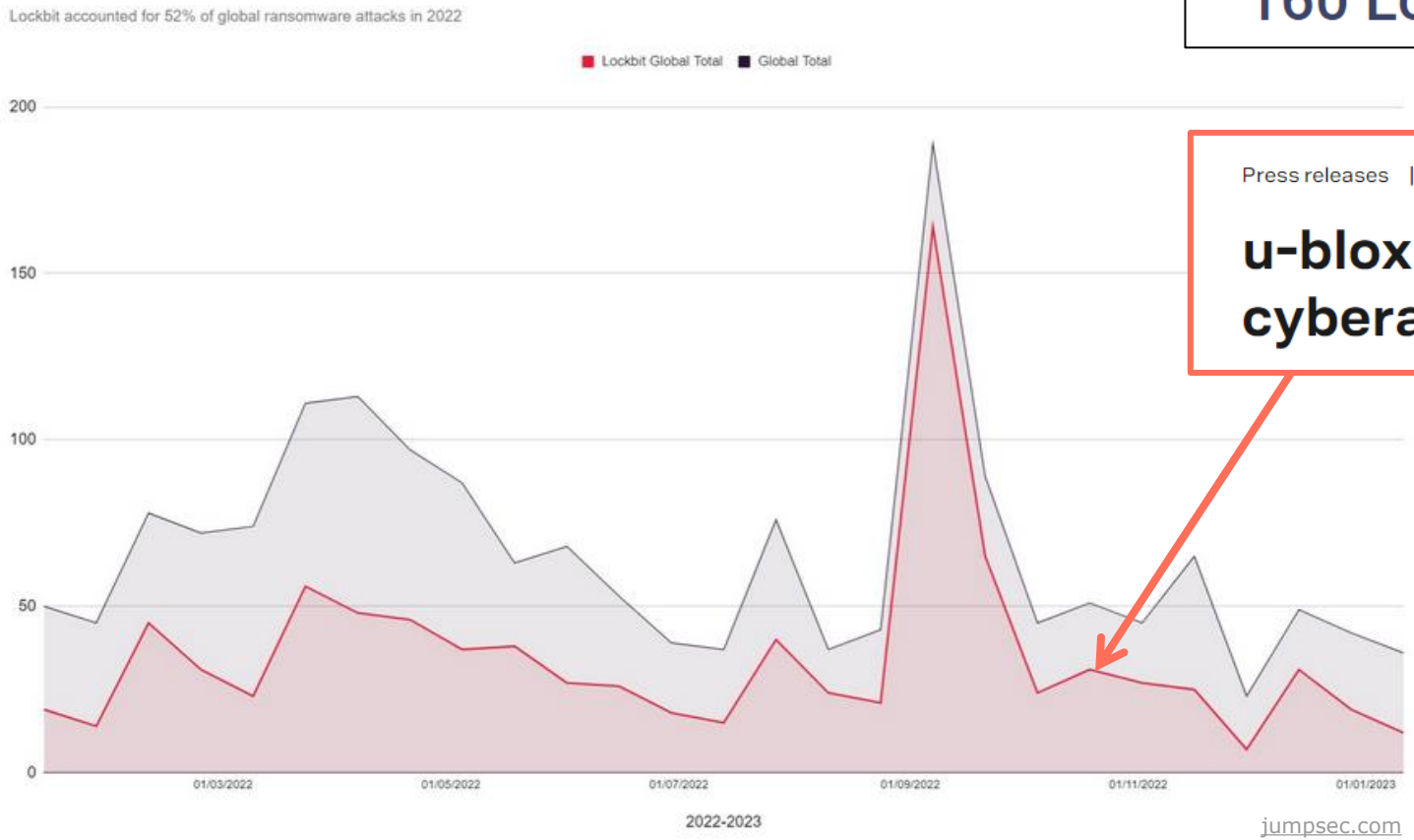
A nightmare based on a true story

Fall 2022…

Auch Schweizer Konzern betroffen

IT-Markt.ch

160 Lockbit-Opfer im Oktober



Press releases | 28 Oct 2022

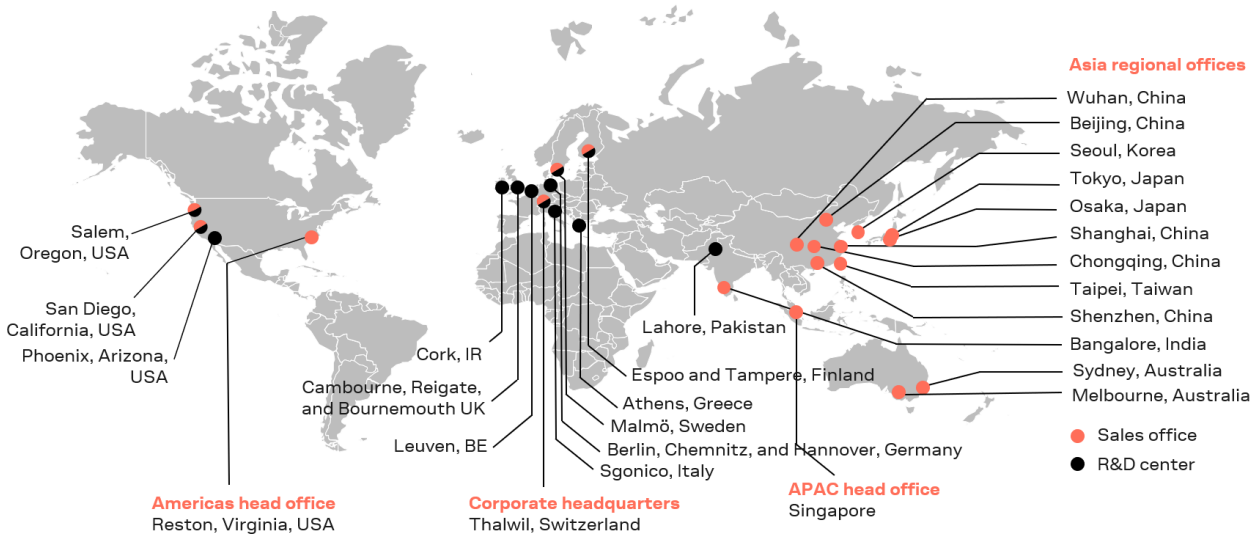
u-blox fends off ransomware cyberattack

u-blox.com

About u-blox

Positioning and wireless connectivity for billions of smart devices

The company



332m Revenue in H1 2023 **in CHF**	**3** Core markets	**1997** Founded as a spin-off from **ETH Zurich**	**18%** of revenue invested into **R&D**
>100M Chips & Modules **sold in 2022**	**1300** Employees **66% in R&D**	**2007** IPO and listed **SIX:UBXN**	**15%** Growth (CAGR) **2007...2022**

The Megatrends and our Products

u-blox solutions are comprised of chipsets, modules, and data services

Services

To make it simple to connect and locate everyThing

Positioning	**Cellular connectivity**	**Short range connectivity**
To locate the source of information	To connect over a wide area	To connect over short distances

About the presenter

Alex Diekmann

Director Corporate Security at u-blox

leading the central organization for

- Information Security
- Business Continuity Management
- Product Cybersecurity
- Site Security
- Supply Chain Security

Lecturer Product Cybersecurity at HSLU Lucerne University of Applied Sciences and Arts

- B.Sc. Information & Cyber Security, Module SPREN
- Lecturing on Product SDLC, Risk Management, *Supply Chain Security,* Post-Launch Security
- Grading Bachelor Thesis

Past Experience

Various roles related to Medical Device Security at Roche

- Built up and lead the Diagnostics Product CERT
- Medical Device Security Expert, Process Manager, Service Manager & Project Lead
- Internal Auditor QMS

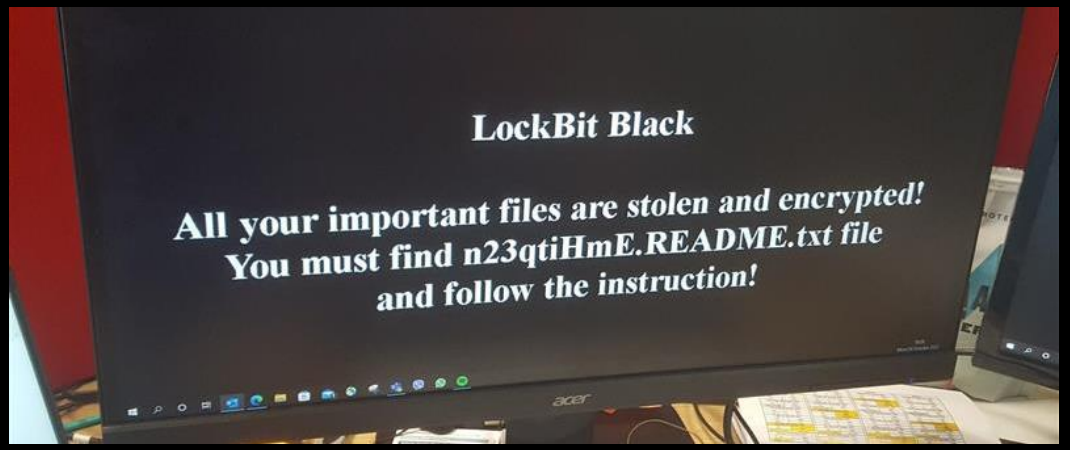
Education

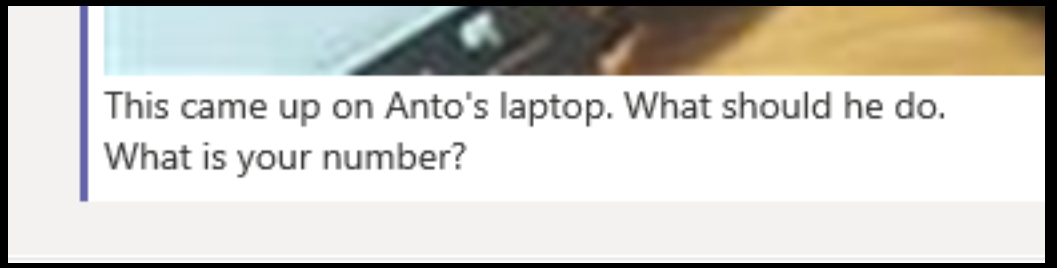
B.Eng IT, CISA, CISM, ISO27001 Lead Auditor, ISO27032 Lead Cybersecurity Manager, ISO21434 Automotive Cybersecurity Red Belt, SEI Software Architecture Professional, CCSK, ISO13485 Internal Auditor

The Nightmare Begins...

24.Oct.2022 - The eMail

From Russia with love?



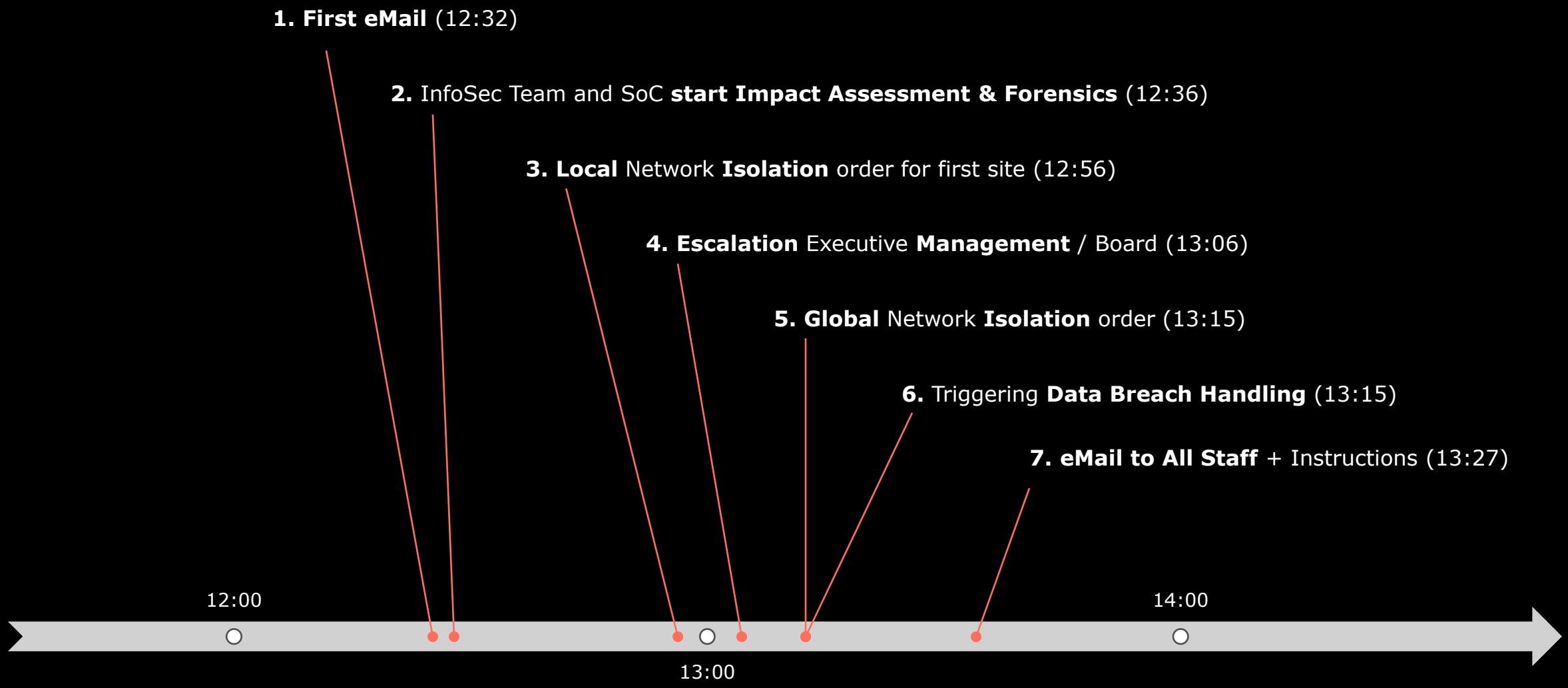



```
All your important files are encrypted!
Any attempts to restore your files with the thrid-party software will be fatal for your files!
RESTORE YOU DATA POSIBLE ONLY BUYING private key from us.
There is only one way to get your files back:

| 1. Download Tor browser - https://www.torproject.org/ and install it.
| 2. Open link in TOR browser - http://lockbitks2tvnmwk.onion/[redacted]
        This link only works in Tor Browser!
| 3. Follow the instructions on this page


 ###  Attention! ###
 # Do not rename encrypted files.
 # Do not try to decrypt using third party software, it may cause permanent data loss.
 # Decryption of your files with the help of third parties may cause increased price(they add their fee to our).
 # Tor Browser may be blocked in your country or corporate network. Use https://bridges.torproject.org or use Tor Browser over VPN.
 # Tor Browser user manual https://tb-manual.torproject.org/about

!!! We also download huge amount of your private data, including finance information, clients personal info, network diagrams, passwords and so on.
Don't forget about GDPR.
```

And thus it began…

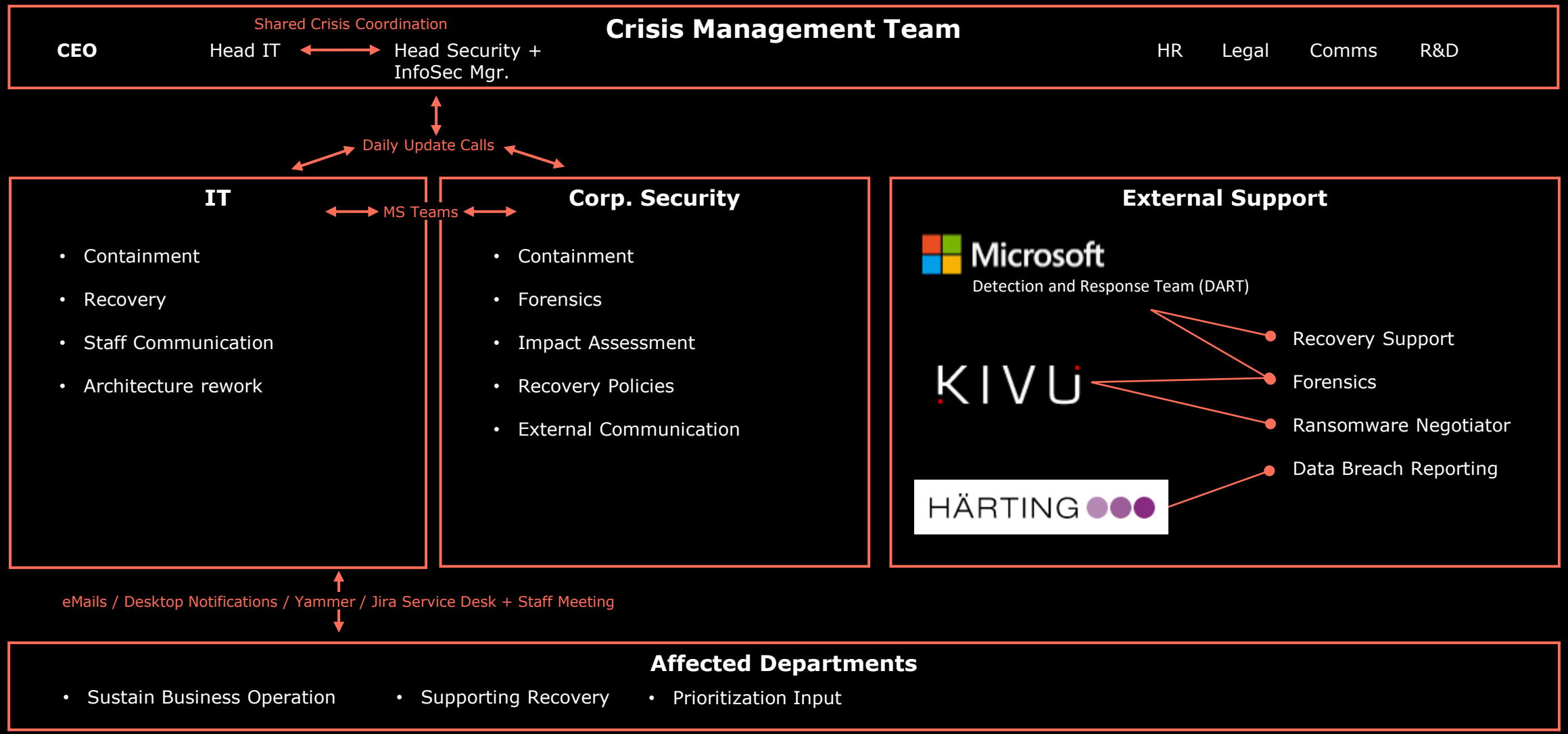
The clock's ticking...

24-Oct-22 – The first hour

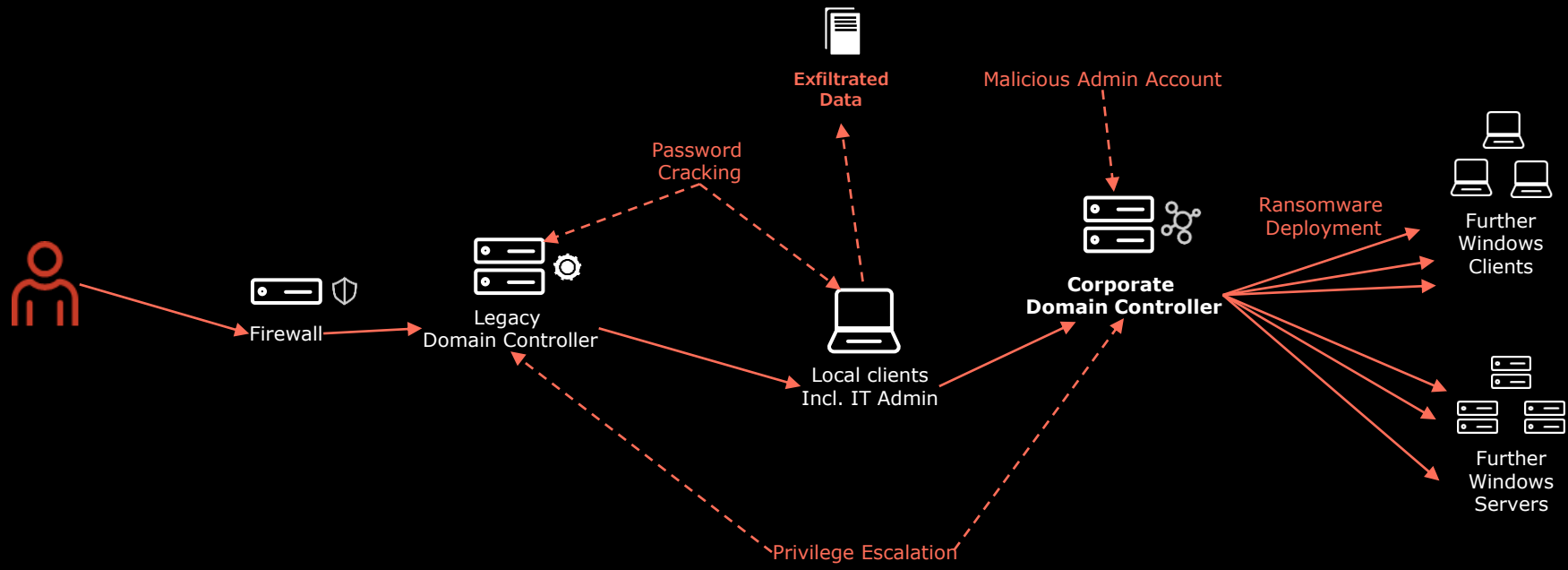


Crisis Management

Setup & Internal Communication



Attack Path & Impact



What **they got**

- **Encrypted clients & servers**
- **Manually** Exfiltrated data
  - (unconfirmed) User Data from **Active Directory**
  - **Passwords** from certain users' browser password stores
  - Some **IT documentation**
- **Network & system downtime**

What they **didn't get**

- No outage of **communication**
- No compromise of
  - **Customer-** or **supplier data** or systems
  - u-blox **business data** or **product data**
  - **Customer Services** (as properly segregated on AWS)
  - **Cloud** services, **Linux** infrastructure & **production** infrastructure
  - **Backups**

External Communication

Breach Reporting

Reported to

- **Police** of Canton Zurich / Public Prosecutors (Criminal Complaint)
- **NCSC**
- **EU Data Protection Authorities** (All Countries with u-blox Site, within 72h thanks to Härting)

Report details

- Affected sites
- Type of affected data
- Number of affected individuals
- Measures taken

Questions back (UK, Italy, Ireland, Berlin)

- Copy of notification to affected individuals
- Details on affected data
- u-blox IT Architecture & Security Measures
- Forensics reports

Customers

- Direct notification (Impacted customers)
- Q/A Sessions
- Covered in customer audits

Suppliers

- Direct notification
- Collaboration on containment and recovery

Public

- Statement on Website
- Annual Report
- Corporate Sustainability Report

Auditors

- Covered in financial audits
- Covered in ISO9001 audit

How to wake up…

Response

Lessons Learned

Attack

- **Ransomware** is the **last attack step**
- **Don’t Pay Ransome** (may even be illegal)
- Still **Negotiate** (to learn & buy time)
- **Ransomware Gangs**
  - Are available **as a service**
  - Love working during the **weekend**
  - **Double-extort**
  - have **limited resources** and make **mistakes**

Response

- **Isolate first**, shut down internet connectivity
- **Prevent re-infections**
  - **Stop** infections through **File shares, USB flash drives**
  - **Don’t just restore** old vulnerable state
  - Enforce **password change**
- **Always assume Data Breach**
  - **Involve DPO** immediately
  - Start **forensics** immediately
  - Get **external legal support** for **Breach Reporting**
- **Keep Monitoring** for ongoing attacks and data disclosure

Response
Lessons Learned

Communication

- **Communicate quickly** and **transparently**
  - Response & Recovery Roles & Responsibilities
  - Clear instructions & rules for all staff
  - Early, controlled external communication
- **3rd Parties care**
  - Customers & Suppliers
  - Law Enforcement
  - Data Protection- & Cyber Authorities
  - Financial Auditors

Recovery

- **Prioritize your Assets** (Data, Systems, Owners, Criticality)
- **Know your Shadow IT**
- **Have your plans ready**
  - Overarching Business Continuity Plan
  - Disaster Recovery Plan
- **Exercise Response & Recovery**

Detection

Lessons Learned

Technology

- Keep your **network** under **control**
  - Central Management
  - Broad-coverage NDR
  - **Deploy EDR** on all endpoints!
- **Monitor** your networks for
  - **Admin** Account **activity**
  - **Data flows** to 3rd party systems and non-business countries
  - **Hacking tool activity** (e.g. password crackers) (especially on the weekend)
  - **Access** to critical systems **outside office hours**

People & Processes

- **Awareness is key**
- **Clear SOC Instructions**
  - Highlight **critical systems**
  - Instruct to **Isolate first** (non-production-critical)
  - Instruct to **Alert immediately**
- **Blind-test** your **SOC**
- **Exercise** incident detection & reporting

Prevention

Lessons Learned

Technology

- Reduce **blast radius**
  - Network Segregation
  - Hardening & Patching
  - Least Privilege
- **Decommission legacy** infrastructure
- **Technological Diversity** can increase resilience
- **Shift to (Multi-)Cloud** helped keep critical systems online

People & Processes

- **Prioritize Clean Up** over launching new systems
- **Protect your backups** and test them regularly
- Apply **strict governance** on **critical systems**
  - 4-eye principle
  - Enforced Testing before go-live

Questions?

Ask now or get in touch later…

Contact me

Alex Diekmann

Director Corporate Security

u-blox AG, Zürcherstrasse 68, CH-8800 Thalwil

Phone: +41 44 722 9609

eMail: alex.diekmann@u-blox.com

Threema: 7SBWM9V7

PGP Fingerprint: 419B B106 204F 4703 2D22 131C 938C 2158 DF6D 2A2D

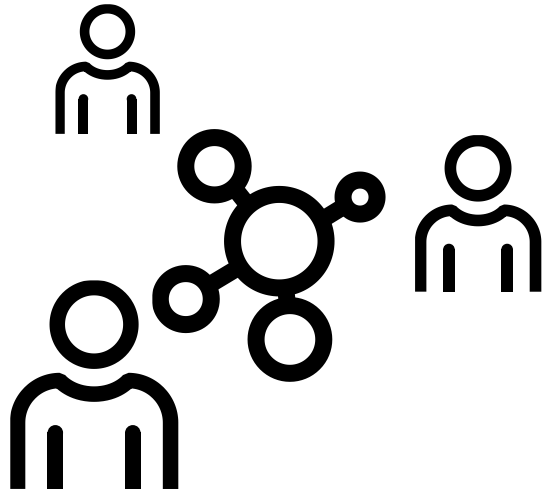
Contact u-blox Corporate Security

u-blox Corporate Security

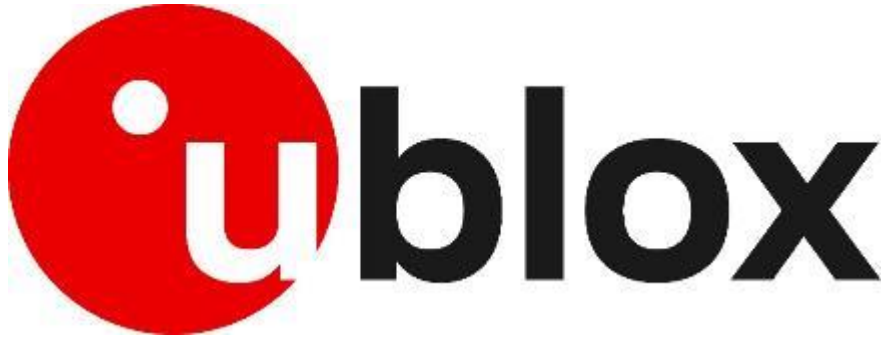
u-blox AG, Zürcherstrasse 68, CH-8800 Thalwil

Web: https://www.u-blox.com

Mail: security@u-blox.com



Thank you
for your attention!



Technology for engineers