Lessons Learned from 10 years of Incident Response

JOHANN STOCKINGER

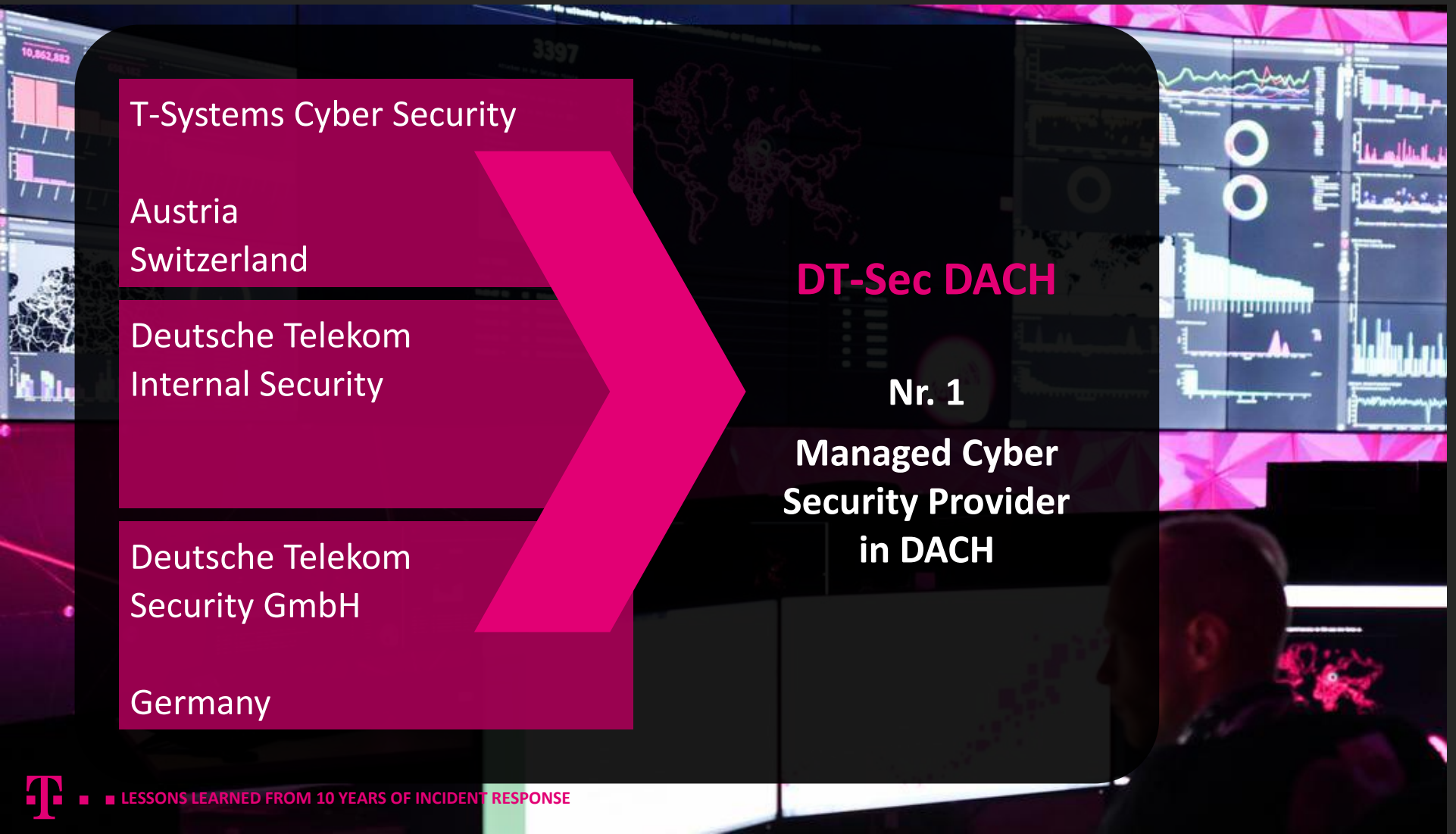
Who am I?

T · · Systems ·

Johann Stockinger
Senior Security Analyst & Incident Responder

T-Systems ALPINE
Rennweg 97-99
1030 Vienna, Austria
stockingerj@t-systems.com

Deutsche Telekom Security



T-Systems Cyber Security

Austria
Switzerland

Deutsche Telekom
Internal Security

Deutsche Telekom
Security GmbH

Germany

DT-Sec DACH

Nr. 1

Managed Cyber Security Provider in DACH

We have
more than
1,500 specialists
in operations
DACH +
Nearshore Center HU and SK

WE‘RE HIRING!

Most attacks share similarities

The vast majority of incidents…

- originate from malicious mails, unpatched applications, or leaked credentials,
- are amplified by wide-spread domain admin usage and missing network segmentation,
- and are often difficult to investigate due to a lack of visibility.

The typical top 5 lessons learned

1. Missing/ineffective vulnerability & patch management
2. Domain admin accounts being used too freely
3. Missing/ineffective network segmentation
4. Limited visibility (infrastructure, endpoints, network)
5. No centralized logging / unable to “look into the past”

But you've heard this before

We want to share some of the slightly less known but still common lessons we've seen over the past decade

- Based on some very real cases we've worked on
- Disclaimer: no, we are obviously unable to name any customers

Victim was an intergovernmental organization

- Many member countries & partner organizations worldwide
- “Distributed infrastructure”

Attack conducted by state-sponsored actor

- Connected to military intelligence agencies
- Victims include governments (and related organizations), various armed forces, news agencies, …
- Primarily espionage, sometimes sabotage

Case 1

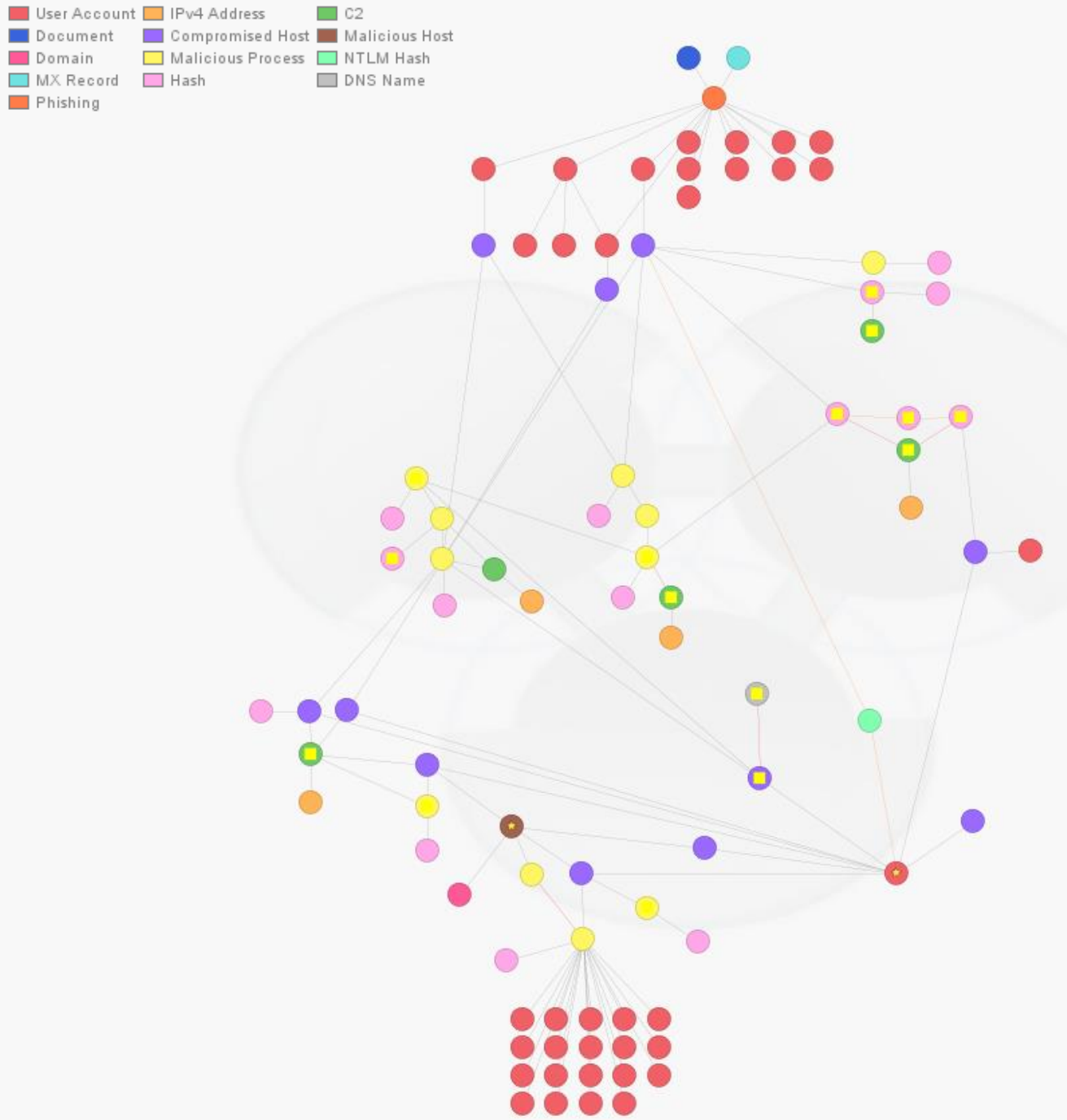
Out-of-band communication should remain so

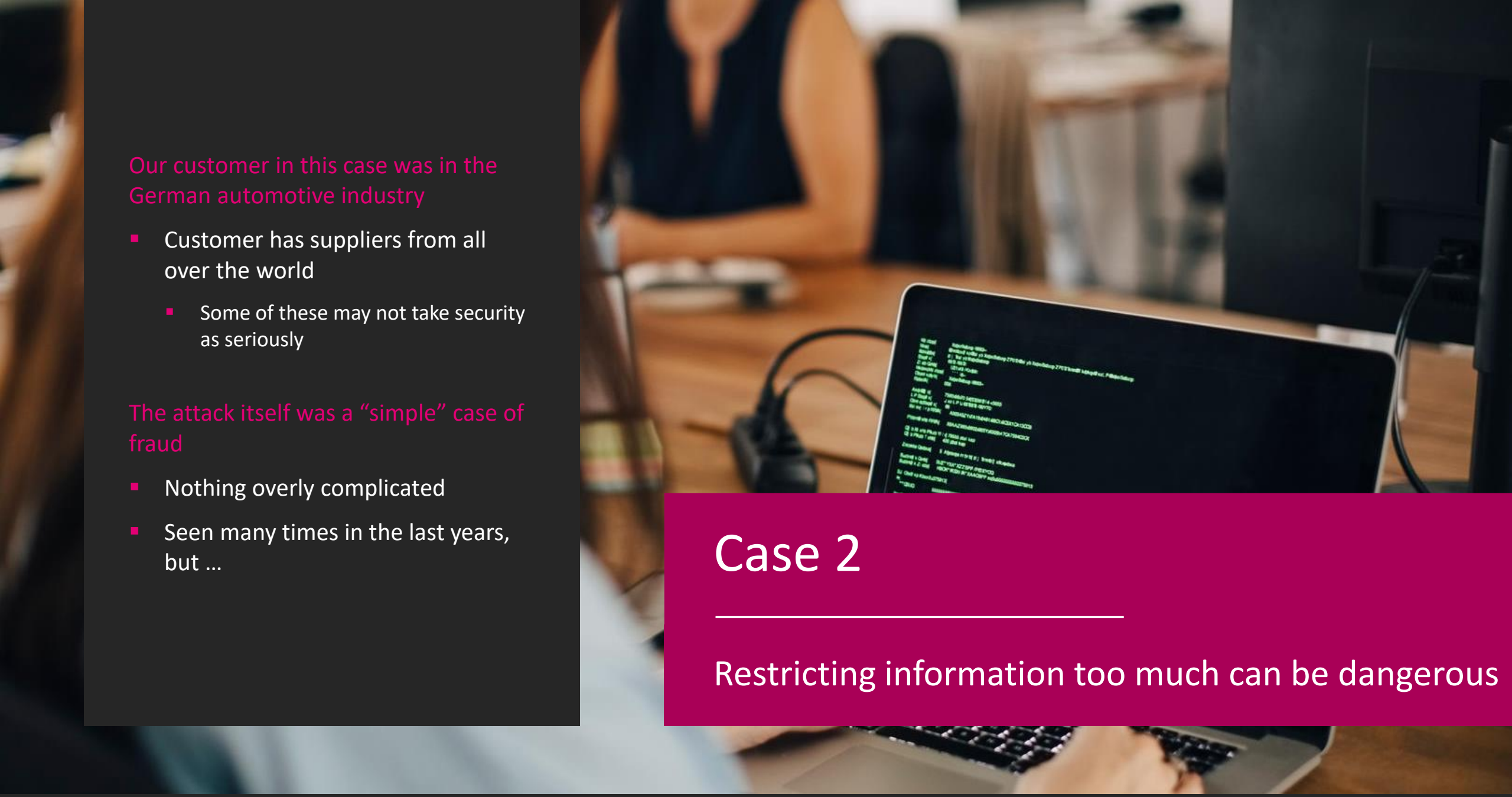
A sophisticated attack

- Initial infection via e-mail attachment
  - Well executed, fit perfectly into the recipient's workflow
- Attacker moved slowly and stealthy – undiscovered for months & very sophisticated
  - Full AD compromise
  - Firmware level attacks
  - …
- We established an out-of-band communication with our customer
  - Exchange compromised as well!
  - Access only for selected users on dedicated hardware…

Tales of exfiltrated data

- Attackers dumped data from Exchange
  - We found remnants …
  - … that included our IR status reports
- Turns out: customer forwarded these internally using (the compromised) Exchange
- Many lessons, but three stick out:
  - Out-of-band communication should remain so
    - Pro-Tip: Don’t put all your security incidents into your ITSM tool!
  - (Some) attackers absolutely do read and exploit sensitive stuff
  - Don’t put your own name in IR reports





Our customer in this case was in the German automotive industry

- Customer has suppliers from all over the world
  - Some of these may not take security as seriously

The attack itself was a “simple” case of fraud

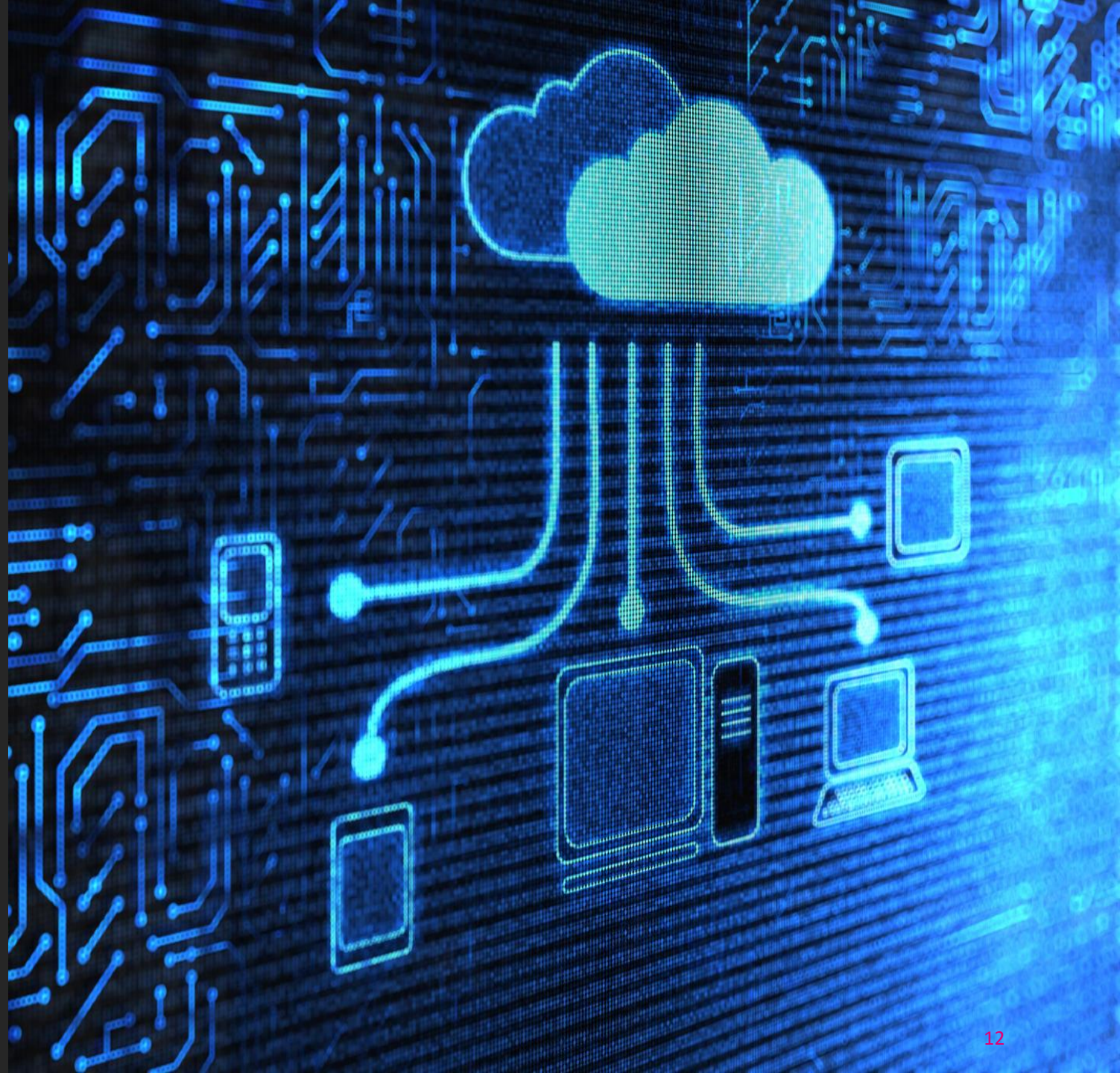
- Nothing overly complicated
- Seen many times in the last years, but …

Case 2

Restricting information too much can be dangerous

A fraudulent invoice

- A fraudulent invoice was sent from one of their suppliers
  - Somewhat well done, similar to how legitimate invoices were sent
  - Supplier was very likely compromised
  - Procurement even asked for additional confirmation (via the same e-mail channel ;-))
- So, payment was made…
  - …and the customer decided to keep this incident confidential
  - Very confidential
  - Confidential from procurement…
  - See where this is going?



A second invoice

- A second (fraudulent) invoice, sent from the same supplier
- Payment was made
  - Obviously, as procurement was unaware of the initial fraud!

- One lesson here is to keep raising awareness
  - You've heard this before, but, well… :-)

- The second lesson: restricting information too much can be as harmful as sharing too much

- And finally: make sure your suppliers take security seriously as well

Remember Hafnium?

- Unauthenticated RCE against Exchange servers (March/April 2021)
- Wide-spread deployment of web-shells
  - Bit of a mess

Many organizations were affected

- But for most, nothing happened post web-shell deployment
- i.e., web-shells deployed but no further attacks
  - At first…

Case 3

Asset management is important

Did we forget something?

- One engagement sticks out
- Customer is a service provider themselves
- ~25 Exchange servers for individual customers
  - Approx. 50% had web-shells, but no further compromise

- Customer happy, case closed?
  - Almost… received a fun call about two weeks later

- Turns out, they had forgotten one Exchange server
  - We found more web shells than legitimate .aspx files
  - Amazingly, still no further compromise!

Well…

- Everyone knows the lesson here: keep track of your assets
- And yet, stuff like this keeps happening
- Constantly, some examples from the past 6 months:
  - A Win7 machine no one knows about, reachable from the Internet via RDP
  - Multiple test/dev applications that were forgotten but remain reachable from the internet
  - DMZs that… aren't
  - Hundreds of AV alerts that are being ignored because they weren't forwarded
  - And many, many more…

When things go wrong people often panic

- When an incident occurs it typically gets rather stressful
- There may be outages, other people breathing down your neck, etc.
- Often there is no time to properly analyze the situation
  - People just assume the worst, often a breach and an active attacker
  - But the reality is often different
- Enter: headless-chicken-mode
  - We have a lot of stories about this one…

(Not a) Case 4

Not everything is a security incident

A ghost in the machine

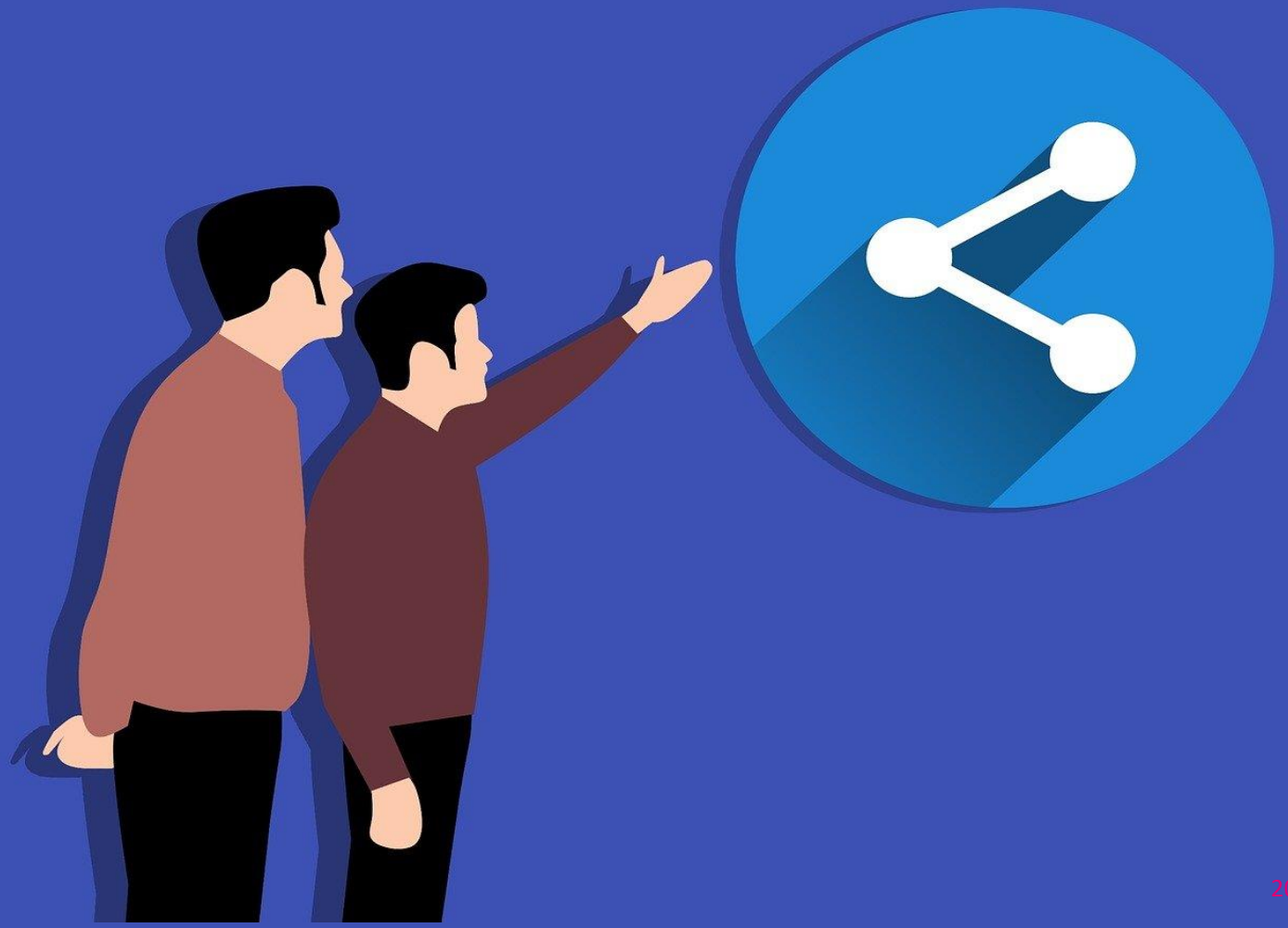
- Imagine you're called to an incident…
  - Where your customer tells you, that late last night, his notebook started talking to him
  - And told him that he had X days before… something
- On the flipside, we were called to an incident where…
  - "Random text" appeared while customer was writing an e-mail
  - Something the customer certainly did not copy/paste
- Text-to-speech/Speech-to-text
  - It can sometimes be hard to stay serious

Malware detected

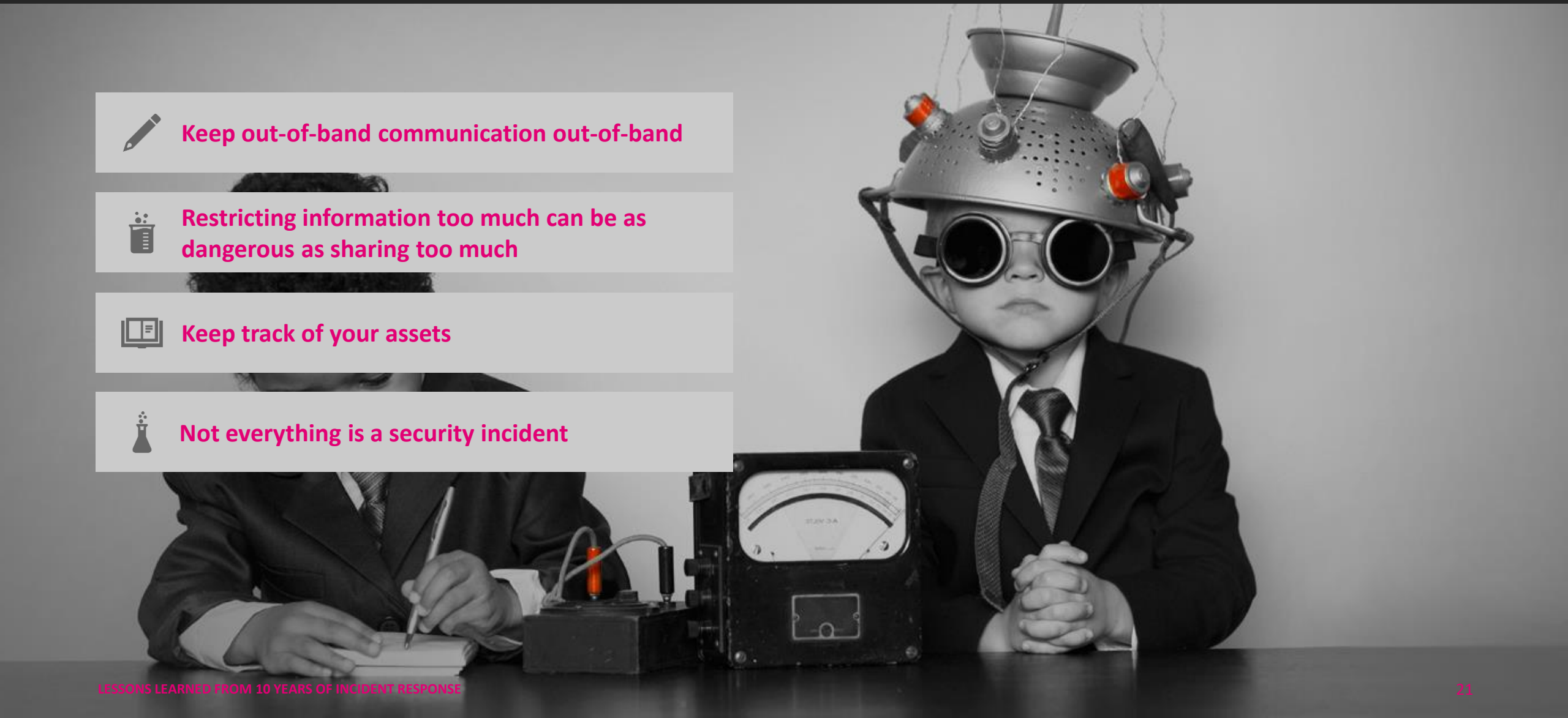
- Incident: internet-exposed server A started sending malicious requests to different internal server B
  - THOR scanner also detected malware on internal server B
  - Sounds like an incident, right?
- Except when you consider…
  - Server A is a reverse proxy, and proxies for server B
  - The malicious requests were simply common exploitation attempts
- What about the malware on server B?
  - Found in “localhost_access_log.txt”…
  - Matched an exploitation string…

Sharing is caring

- Customer was just hit by ransomware
  - Currently in the process of getting everything up and running again
  - Everyone was on edge, sensitive data was exfiltrated…
- A sensitive document appeared on a private Facebook account
  - Is everything, including private phones still compromised and is the attacker actively trying to build pressure?
- Or…
  - Were scanners still offline and users resorted to taking photos…
  - …and hitting “share with” by mistake?



To recap



- Keep out-of-band communication out-of-band
- Restricting information too much can be as dangerous as sharing too much
- Keep track of your assets
- Not everything is a security incident

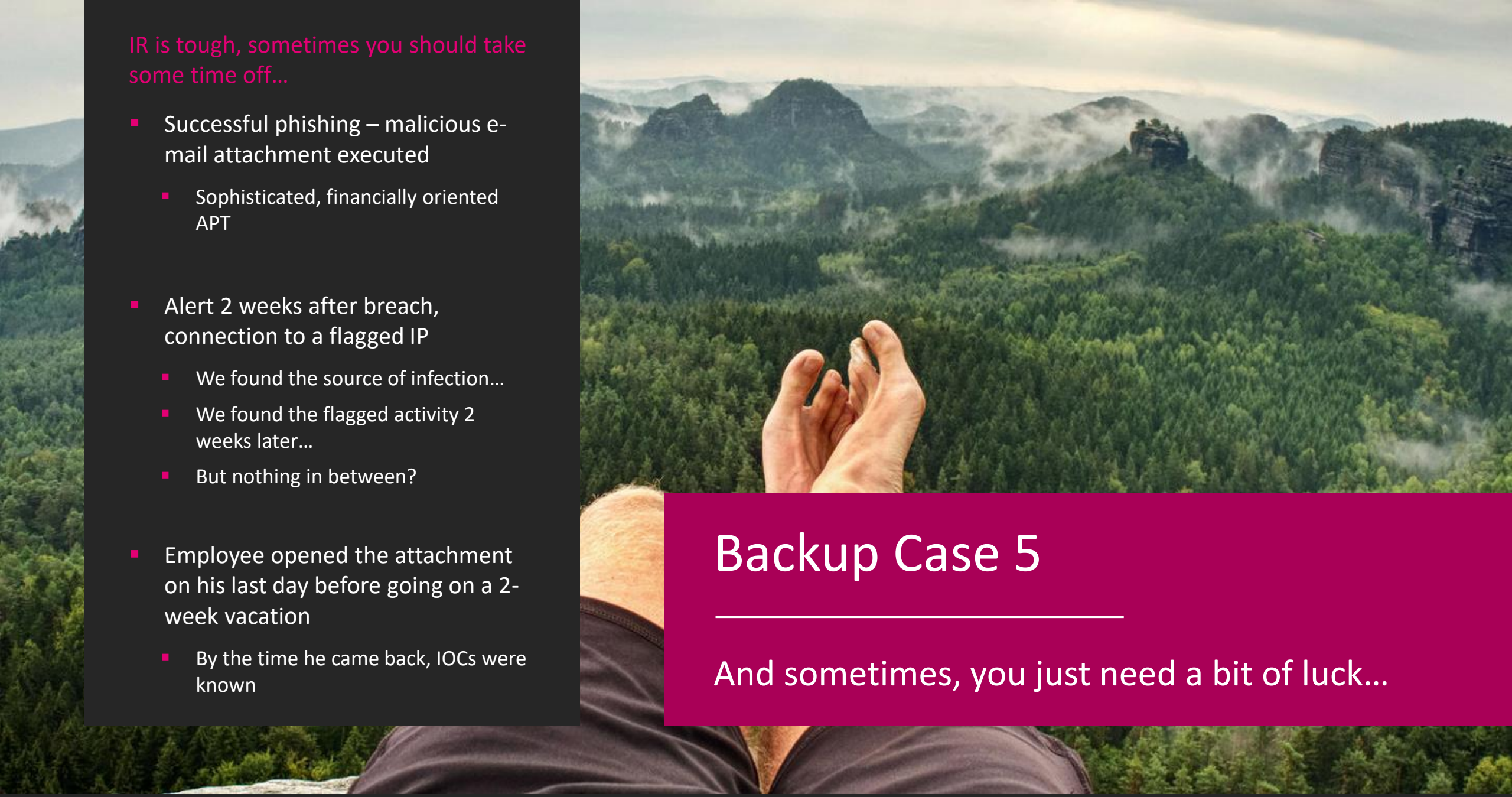
But just to repeat this one…

1. Missing/ineffective vulnerability & patch management
2. Domain admin accounts being used too freely
3. Missing/ineffective network segmentation
4. Limited visibility (infrastructure, endpoints, network)
5. No centralized logging / unable to “look into the past”

Thank You!

IR is tough, sometimes you should take some time off…

- Successful phishing – malicious e-mail attachment executed
  - Sophisticated, financially oriented APT
- Alert 2 weeks after breach, connection to a flagged IP
  - We found the source of infection…
  - We found the flagged activity 2 weeks later…
  - But nothing in between?
- Employee opened the attachment on his last day before going on a 2-week vacation
  - By the time he came back, IOCs were known



Backup Case 5

And sometimes, you just need a bit of luck…