CONCLUSION
INTELLIGENCE

IHK München und Oberbayern

Pack ma's digital
Gemeinsam in die digitale Zukunft

# CYBERSICHERHEIT IM KI-ZEITALTER: WIE SICHERN SIE IHRE DATEN?

Erik Jan Hengstmengel

# AGENDA

CONCLUSION
INTELLIGENCE

- Daten sind überall (angreifbar)
- AI als Booster
- Die Aufgaben für Ihre Organisation
- Risiken minimieren
- Nach dem Ernstfall
- Unterschiede Deutschland – Niederlande: was kann man von einander lernen?

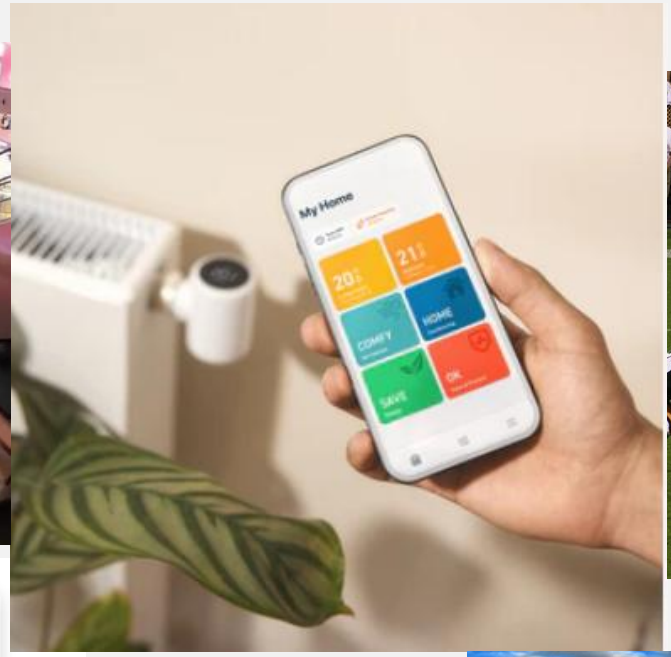
CONCLUSION
INTELLIGENCE

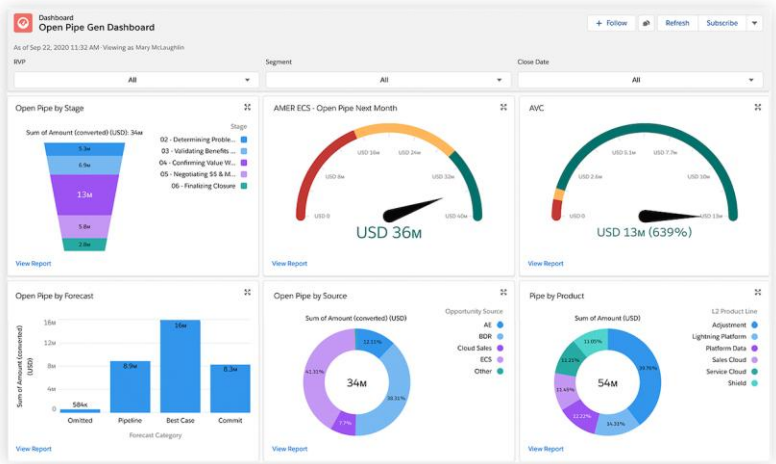
# CONCLUSION INTELLIGENCE IST DER DATEN- UND KI-SPEZIALIST, DER ENTSCHEIDUNGSFINDUNG, BETRIEBSEFFIZIENZ UND KUNDENINTERAKTION VERBESSERT

Ausgehend von Ihren geschäftlichen Herausforderungen arbeitet unser internationales Team mit Ihnen zusammen, um durchgängige Lösungen zu realisieren, die innovativ, bahnbrechend, verantwortungsvoll und vollständig auf Ihre Bedürfnisse zugeschnitten sind.

# DATEN SIND ÜBERALL

CONCLUSION
INTELLIGENCE





….angreifbar

# DAS GEFÄHR KOMMT AUS VIELEN ECKEN…

CONCLUSION
INTELLIGENCE

- Ransomware
- Social Engineering
- Data Diebstahl
- Kontinuität
- Wifi Angriffe
- Supply Chain, OT
- Aber natürlich auch: Sturm, Brand, Wasser….

# DIE 3 AUFGABEN IHRER ORGANIZATION:

CONCLUSION
INTELLIGENCE

Minimieren Sie das Risiko, Opfer eines Cybervorfalls zu werden:

- Systeme & Infrastruktur
- Menschen

Bereiten Sie sich auf den Ernstfall vor:

- Back Ups Data und Systeme
- Incident Response Prozessen
- usw.

Überzeugen Sie Ihre Kunden:

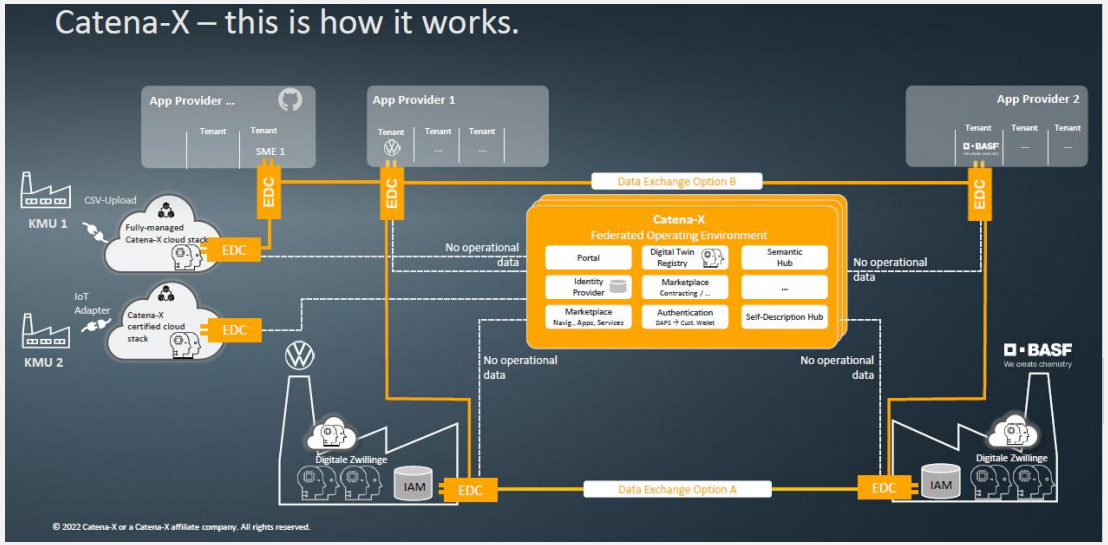
- Prozesse & Standards
- Zertifizierungen

# So you are a hacker

- Was wäre Ihr Ziel beim Hacken Ihrer Organisation?
- Welche Schwachstellen sehen Sie, die Sie ausnützen könnten?
- Wie würden Sie es angehen?

# SYSTEME UND INFRASTRUKTUR: WASS IST ZU KLÄREN?

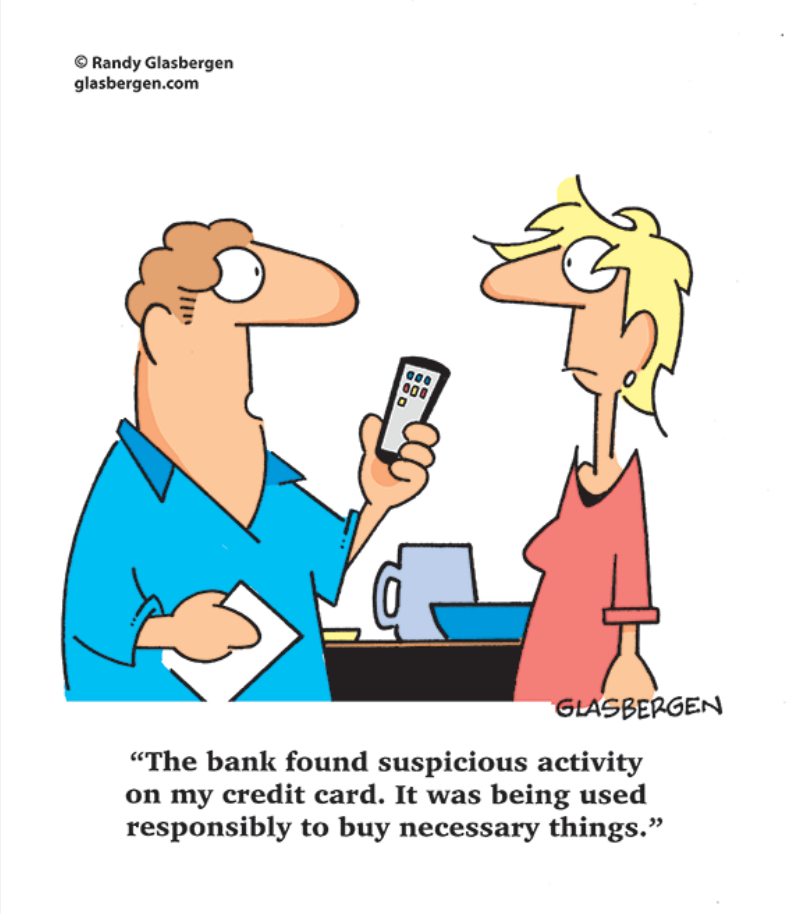
- Up to Date Technologie / Versionen
- Digitale Souveränität
- Managed Service Providers / SaaS
- BYOD
- Cloud oder On Premise
- Monitoring und Tracking
- Supply Chain und Data Spaces
- IoT und IT



# DER FAKTOR MENSCH

CONCLUSION
INTELLIGENCE

- Menschen machen Fehlern
- Kriminellen nützen die aus
- Human Risk Management
- Zero Trust Approach
- Erschießen Sie nicht den Boten



# AI MACHT ES NOCH KOMPLIZIERTER

CONCLUSION
INTELLIGENCE

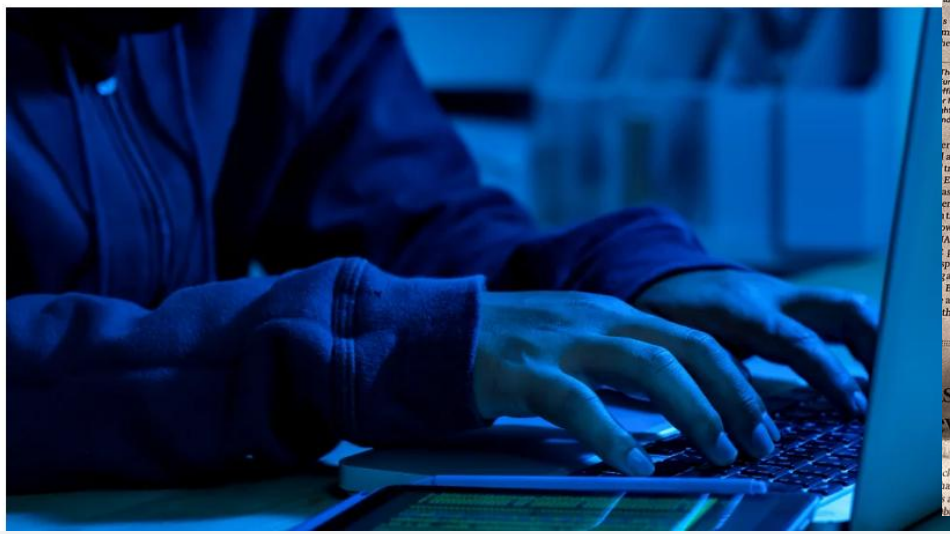
CNN World Watch Listen Live TV Sign in

World / Asia

## Finance worker pays out $25 million after video call with deepfake 'chief financial officer'

By Heather Chen and Kathleen Magramo, CNN

2 minute read · Published 2:31 AM EST, Sun February 4, 2024



China earnings – LEX

a tweet. I don't wake up to a strategy shift'

Denholm rejects criticism of governance at the business ahead of votes on chief's pay package and Texas move

TABBY KINDER AND STEPHEN MORRIS
SAN FRANCISCO

Robyn Denholm, Tesla's Sydney-based chair, is used to waking up to unexpected tweets from the carmaker's chief executive Elon Musk.

companies, including rocket builder SpaceX, brain implant technology group Neuralink, and X, has threatened to spend more time away from Tesla if he does not hold about 25 per cent of its

14 ★ FT Weekend 18 May/19 May 2024

COMPANIES & MARKETS

Technology

## Arup lost $25mn in fraudsters' deepfake video scam

*Money sent to Hong Kong accounts after conference with digitally cloned CFO*

CHENG LENG AND CHAN HO-HIM
HONG KONG

UK engineering group Arup lost HK$200mn ($25mn) after fraudsters used a digitally cloned version of a senior manager to order financial transfers during a video conference, the Financial Times has learnt.

Hong Kong police previously revealed what is one of the world's biggest known deepfake scams, but did not identify the company involved.

The FT has confirmed it was Arup, which employs around 18,000 people globally and has annual revenue of more than £2bn. Two people familiar with the matter told the FT this month that Arup had been the target of what Hong Kong police have classified as "obtaining property by deception".

The case highlights the threat posed by deepfakes — hyper-realistic video, audio or other material generated using artificial intelligence — when used by cyber criminals to target companies or governments. Asked about the case, Arup said it had "notified the police about an incident of fraud in Hong Kong" in January.

"We can confirm that fake voices and images were used," it said, declining to give details because the incident was still being investigated. "Our financial stability and business operations were not affected and none of our internal systems were compromised," it said.

Hong Kong police acting senior superintendent Baron Chan told local media in February that a member of staff in the targeted firm had received a message purporting to be from the company's UK-based chief financial officer regarding a "confidential transaction".

After a video conference joined by the company's digitally cloned CFO and other fake employees, Chan said, the staff member made 15 transfers to five Hong Kong bank accounts before discovering it was a scam after following up with the firm's headquarters.

A police spokesperson said an inquiry was continuing, with no arrests so far.

Arup's east Asia chair Andy Lee stepped down following the scam after just a year in the role. He was replaced by Michael Kwok, a former east Asia chair for the company. Lee said on his LinkedIn page that he had "decided to embark on a new opportunity". Lee did not respond to a request for comment made via LinkedIn. Arup declined to comment further on his departure.

The FT reported this month that international advertising agency WPP had been the target of an unsuccessful deepfake scam in which criminals used a voice clone and YouTube footage to set up a video meeting with executives. Liu Meng, an analyst with consultancy Forrester, said many companies, banks and legislators lacked awareness of new forms of scam, such as deepfakes.

"Corporates need to purchase more IT solutions to counter cyber security scams [and] banks need to alert their clients on suspicious payments when the money is about to be wired," Liu said, adding laws should be passed to ensure banks shared more in financial losses from fraud.

Arup's global chief information officer Rob Greig said in a statement that the number and sophistication of deepfake scams had been "rising sharply". "I hope our experience can help raise awareness of the increasing sophistication and evolving techniques of bad actors."

*Additional reporting by Gill Plimmer in London and Kaye Wiggins in Hong Kong*

Boss attempts to dig Anglo American out of a large hole

Spotlight

To head off a £34bn move from rival BHP, Duncan Wanblad this week unveiled a drastic set of sales and demergers that could raise $25bn

BUSINESS
WEEK IN REVIEW

Visa rules hit jobs

# AI unterstützt Cybersecurity: Beispiel Mobilfunkanbieter

CONCLUSION
INTELLIGENCE

- Intelligente Algorithmen scannen kontinuierlich nach anomalem Anrufverhalten und Nutzungsmustern und bieten so einen robusten Schutz vor betrügerischen Aktivitäten.
- Diese Systeme sind darauf ausgelegt, potenzielle Betrugsfälle in Echtzeit zu erkennen und zu melden, wodurch das Risiko von Umsatzeinbußen erheblich verringert wird.
- Mit der Implementierung dieser Algorithmen sichern wir den Betrieb und tragen so zu einem erheblichen Geschäftsvorteil bei.

# DATEN: WENIGER (ZUGRIFF) IST MEHR (SICHERHEIT)

CONCLUSION
INTELLIGENCE

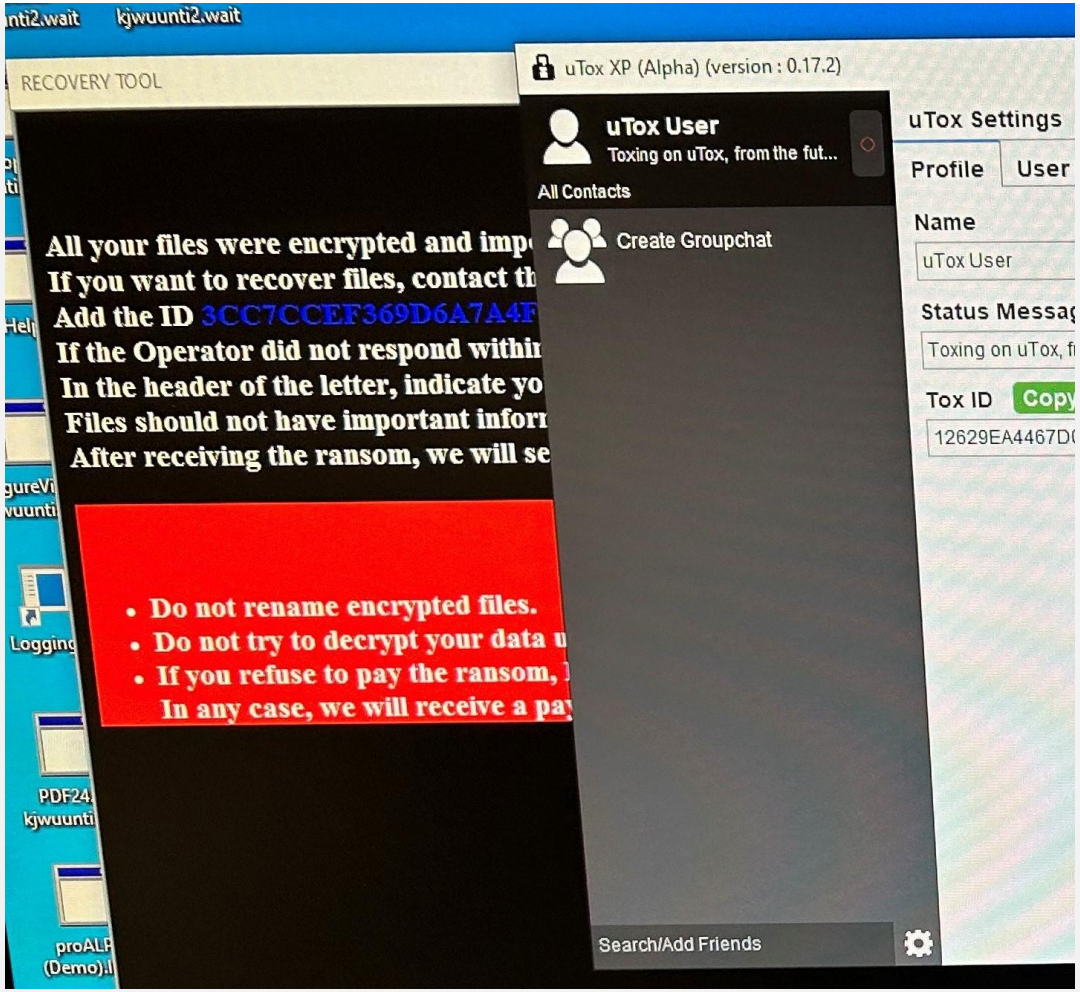
Stellen Sie sich selbst folgende Fragen:
- Wer
- Welche
- Wann
- Wofür
- Welche Rahmenbedingungen

# DER ERNSTFALL

CONCLUSION
INTELLIGENCE

- Incident Response- und Kontinuitäts-plan (auf Papier!)
- Daten Back Up
- Not-Infrastruktur
- Den Ernstfall Trainieren

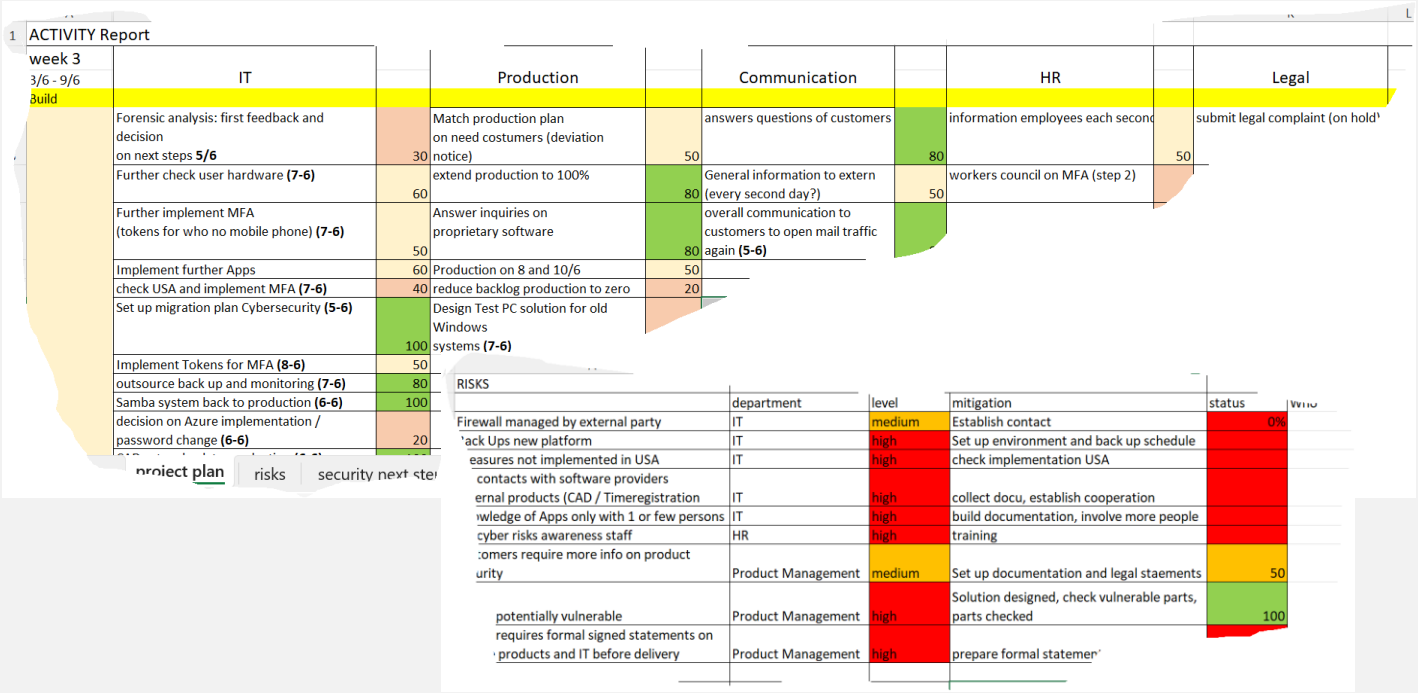
Was ist die schwierigste Herausforderung nach einem Hack?



# KRISEN MANAGEMENT

CONCLUSION
INTELLIGENCE

- Rollen vorab definieren
- Externe und interne Krisen Teams benennen
- Verhandeln oder nicht?
- Back Up Systeme
- Data Reintegration
- Drehbuch Kommunikation



ACTIVITY Report

| week 3<br>3/6 - 9/6<br>Build | IT | | Production | | Communication | | HR | | Legal |
|---|---|---|---|---|---|---|---|---|---|
| | Forensic analysis: first feedback and decision on next steps **5/6** | 30 | Match production plan on need costumers (deviation notice) | 50 | answers questions of customers | 80 | information employees each second | 50 | submit legal complaint (on hold |
| | Further check user hardware **(7-6)** | 60 | extend production to 100% | 80 | General information to extern (every second day?) | 50 | workers council on MFA (step 2) | | |
| | Further implement MFA (tokens for who no mobile phone) **(7-6)** | 50 | Answer inquiries on proprietary software | 80 | overall communication to customers to open mail traffic again **(5-6)** | | | | |
| | Implement further Apps | 60 | Production on 8 and 10/6 | 50 | | | | | |
| | check USA and implement MFA **(7-6)** | 40 | reduce backlog production to zero | 20 | | | | | |
| | Set up migration plan Cybersecurity **(5-6)** | 100 | Design Test PC solution for old Windows systems **(7-6)** | | | | | | |
| | Implement Tokens for MFA **(8-6)** | 50 | | | | | | | |
| | outsource back up and monitoring **(7-6)** | 80 | | | | | | | |
| | Samba system back to production **(6-6)** | 100 | | | | | | | |
| | decision on Azure implementation / password change **(6-6)** | 20 | | | | | | | |

project plan | risks | security next ste

RISKS

| | department | level | mitigation | status |
|---|---|---|---|---|
| Firewall managed by external party | IT | medium | Establish contact | 0% |
| ack Ups new platform | IT | high | Set up environment and back up schedule | |
| easures not implemented in USA | IT | high | check implementation USA | |
| contacts with software providers ernal products (CAD / Timeregistration | IT | high | collect docu, establish cooperation | |
| wledge of Apps only with 1 or few persons | IT | high | build documentation, involve more people | |
| cyber risks awareness staff | HR | high | training | |
| omers require more info on product urity | Product Management | medium | Set up documentation and legal staements | 50 |
| potentially vulnerable | Product Management | high | Solution designed, check vulnerable parts, parts checked | 100 |
| requires formal signed statements on products and IT before delivery | Product Management | high | prepare formal statemer | |

# DEUTSCHLAND – NIEDERLANDE
# WASS KÖNNEN WIR VON EINANDER LERNEN?


CONCLUSION INTELLIGENCE

GUARDIAN 360°

leitzcloud by vBoxx

# Die Gesetzlage

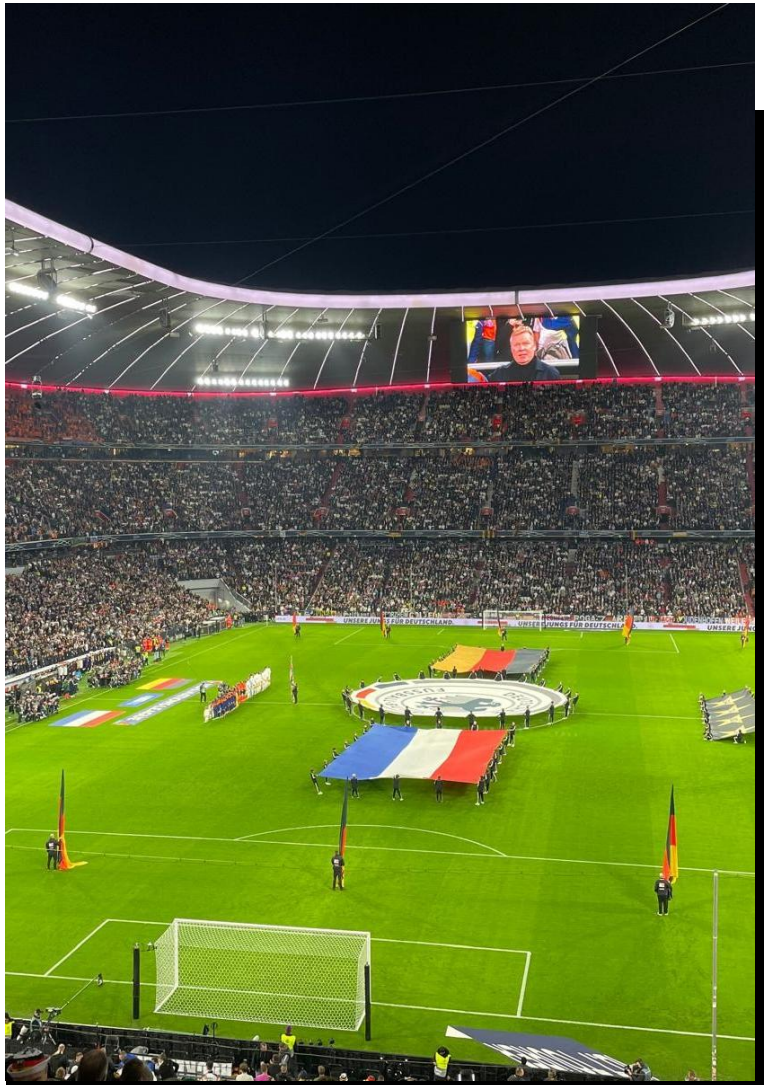
CONCLUSION
INTELLIGENCE

- D: Laut Strafgesetzbuch ist Hacken explizit verboten. Der sogenannte «Hackerparagraph» stellt jeden Versuch eines Eindringens in ein Datenverarbeitungssystem unter Strafe. Dabei ist es egal, ob ein Schaden angerichtet wurde, ob etwas geklaut wurde, oder ob die Hacker gute Absichten hatten.
- NL: Hacken ist nur strafbar, wenn es unrechtmäßig geschieht. Das heißt, wenn es gegen das Gesetz verstößt. Wenn das Hacken von Computern nicht rechtswidrig ist, spricht das Gericht den Hacker frei. In der Praxis wird davon ausgegangen, dass ethisches Hacking nicht rechtswidrig sein muss:
  - Wirkliche Interesse
  - Proportional
  - Subsidiär

# WASS KÖNNEN WIR VON EINANDER LERNEN?

CONCLUSION
INTELLIGENCE

- In Deutschland wird ein Betriebsrat schnell in die Implementierung von Informationssicherheitsdiensten einbezogen. Nicht nur, wenn es um die Sensibilisierung geht, an die wir in den Niederlanden auch in größeren Organisationen gewöhnt sind, sondern auch beim Scannen der Systeme der Benutzer
- Deutsche bevorzugen deutsche/europäische Lösungen, während wir in den Niederlanden schnell zu amerikanischen Produkten greifen
- In den Niederlanden ist die Einhaltung der Vorschriften eine Frage des „Ankreuzens“, während in Deutschland die Einhaltung der Vorschriften als sehr wichtig angesehen wird (wenngleich manchmal auch für die Buhne 😉 )
- Niederländer sind schnelle Entscheidungsträger, aber weniger loyal als Deutsche. Für die Informationssicherheit braucht man einen längeren Horizont, ein schneller Wechsel der Tools ist der Sicherheit nicht zuträglich



# WASS KÖNNEN WIR VONEINANDER LERNEN?

CONCLUSION
INTELLIGENCE

- Vertrauen und Formalität: In Deutschland ist es wichtig, dass alles formal korrekt abläuft – das heißt: Zertifizierungen, Abwicklungsvereinbarungen und klare Prozesse sind erforderlich, bevor es zu einer tatsächlichen Umsetzung kommt. In den Niederlanden hingegen sind die Abläufe meist informeller und schneller.
- Sicherheit durch Design: In Deutschland wird die Sicherheit häufiger direkt in die Vorgespräche einbezogen. In den Niederlanden erleben wir häufiger, dass sie später hinzugefügt wird, wenn etwas bereits in Gebrauch ist.
- Lokale Rechenzentren: Für deutsche Kunden ist der Standort der Datenspeicherung wirklich entscheidend. „In Deutschland gehostet“ macht einen großen Unterschied - während niederländische Kunden oft etwas flexibler sind, solange die Daten ordnungsgemäß gesichert sind.

# FRAGEN?

CONCLUSION
INTELLIGENCE

# VIELEN DANK!


www.conclusionintelligence.de

erikjan.hengstmengel@conclusionintelligence.de