MICHAEL WIESNER

LET‘S GET PHYSICAL

Eine Einführung in physische Penetrationstests

70. Infor Anwendertreffen, 13.11.2025

MICHAEL WIESNER

VORSTELLUNG

Michael Wiesner

- Informationssicherheit seit 1994
- Interim CISO & Trusted Advisor
- Red Teamer

MICHAEL WIESNER

EINLEITUNG

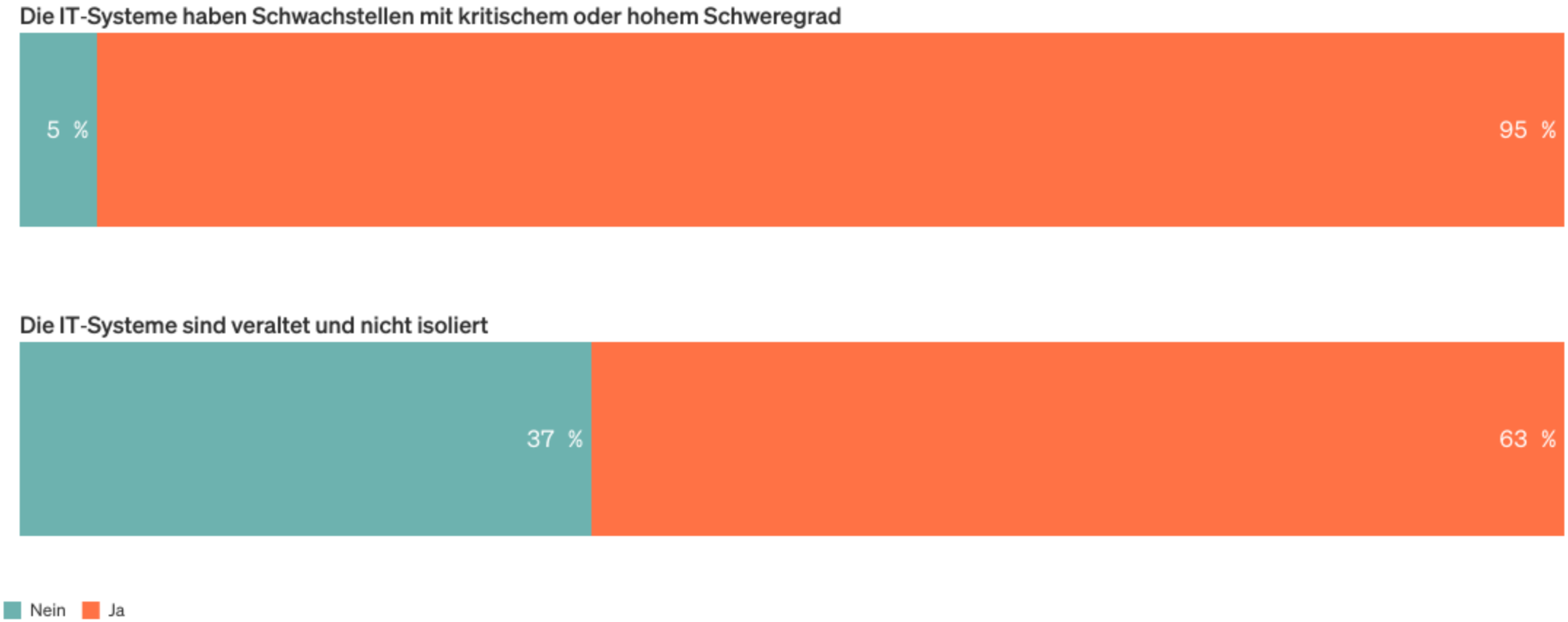
MICHAEL WIESNER

KLASSISCHE PENETRATIONSTESTS

- Klassische Penetrationstests zur Überprüfung der IT-Sicherheit betrachten i.d.R. keine physische Sicherheit
- Blind für physische Angriffsvektoren
- Oft mangelhafter Zutritts- und Netzwerkzugangsschutz

IT-Systeme

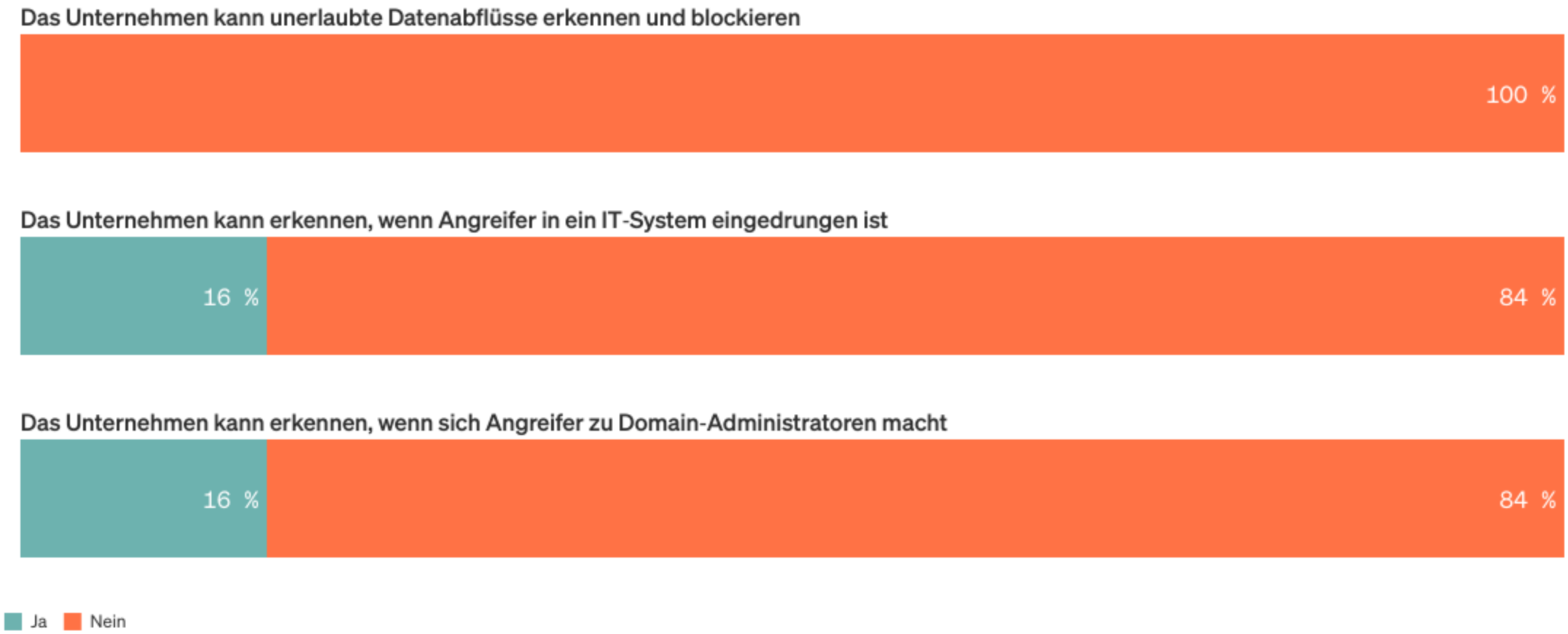
Hohes Risiko durch veraltete Software und viele Schwachstellen



Quelle: Michael Wiesner; Basis: IT-Sicherheitschecks bei 19 mittelständischen Einzelhandels-, Großhandels- und Transportunternehmen

Angriffserkennung

Angreifer und Datenabflüsse bleiben in aller Regel unerkannt



Quelle: Michael Wiesner; Basis: IT-Sicherheitschecks bei 19 mittelständischen Einzelhandels-, Großhandels- und Transportunternehmen

MICHAEL WIESNER

PHYSISCHE PENETRATIONSTESTS

- Ganzheitlicher Blick durch Betrachtung des physischen Angriffsvektors
- Simulation eines zielgerichteten Angriffs vor Ort
- Dediziert oder im Rahmen von Red Team Assessments

MICHAEL WIESNER

FRAGESTELLUNG

- Wo komme ich rein, ohne etwas kaputt zu machen?
- (Wo käme ich rein, wenn ich etwas kaputt machen würde?)
- Wie weit komme ich rein?
- Was kann ich von dort erreichen?

MICHAEL WIESNER

ZIELE

- Zutrittsschutz
- Besuchermanagement
- Netzwerkzugang
- Netzwerksicherheit
- Interne Schwachstellen

MICHAEL WIESNER

VORBEREITUNG

MICHAEL WIESNER

RAHMENBEDINGUNGEN

- Exakte Zieldefinition, Scope, Techniken
- Datenschutzbeauftragte/Betriebsrat einbinden
- So wenig Mitwissende wie möglich
- Kontaktdaten austauschen (insbesondere Mobilnummer)

MICHAEL WIESNER

RAHMENBEDINGUNGEN

- Haftung möglichst ausschließen (Vertrag, AGB, Versicherung)
- Auftrag mit detaillierter Ziel- und Leistungsbeschreibung; vom Topmanagement unterschrieben
- Hinweis geben auf potenzielle Störungen, Probleme, Datenverlust

MICHAEL WIESNER

VORBEREITUNG

- Aufklärung (vor Ort/remote)
- Vorgehen/Stories entwickeln
- Ausstattung zusammenstellen
- Gefälschte Identitäten vorbereiten: Verkleidung, Mitarbeiter-/Besucherausweise
- Legitimationsschreiben
- Gefälschtes Legitimationsschreiben ;)

MICHAEL WIESNER

GRUNDAUSSTATTUNG


GERBER
SUSPENSION


SUPERTAPE


LE
LE


TX10 TX15 TX20 TX30 HX4 HX5 NO.6 NO.8 PH1 PH2 3 5.5 TW1 TW2 TW3
PROXXON


Papierkorb
ThinkPad


renkforce
PEARL
EDITION BY
revolt


6COM
10/100TX 100/FX MONO
Fiber/T Converter
10/100TX 100/FX MULTI
Fiber/T Converter
Ethernet Converter 10/100M Auto-Negotiation
10/100/1000TX 1000/LX MONO
Fiber/T Converter
Ethernet Converter 10/100/1000M Auto-Negotiation
10/100/1000TX 1000/FX MULTI
Fiber/T Converter
Converter 10/100/1000M Auto-Negotiation

MICHAEL WIESNER

AUFKLÄRUNG

MICHAEL WIESNER

AUFKLÄRUNG (REMOTE)

- OSINT
- Internet/Social Media
- Shodan & Co.
- Interne IP-Adressen/Domains
- Mitarbeiter-/Besucherausweise
- Handelsregister
- Satellitenbilder, Google Streetview

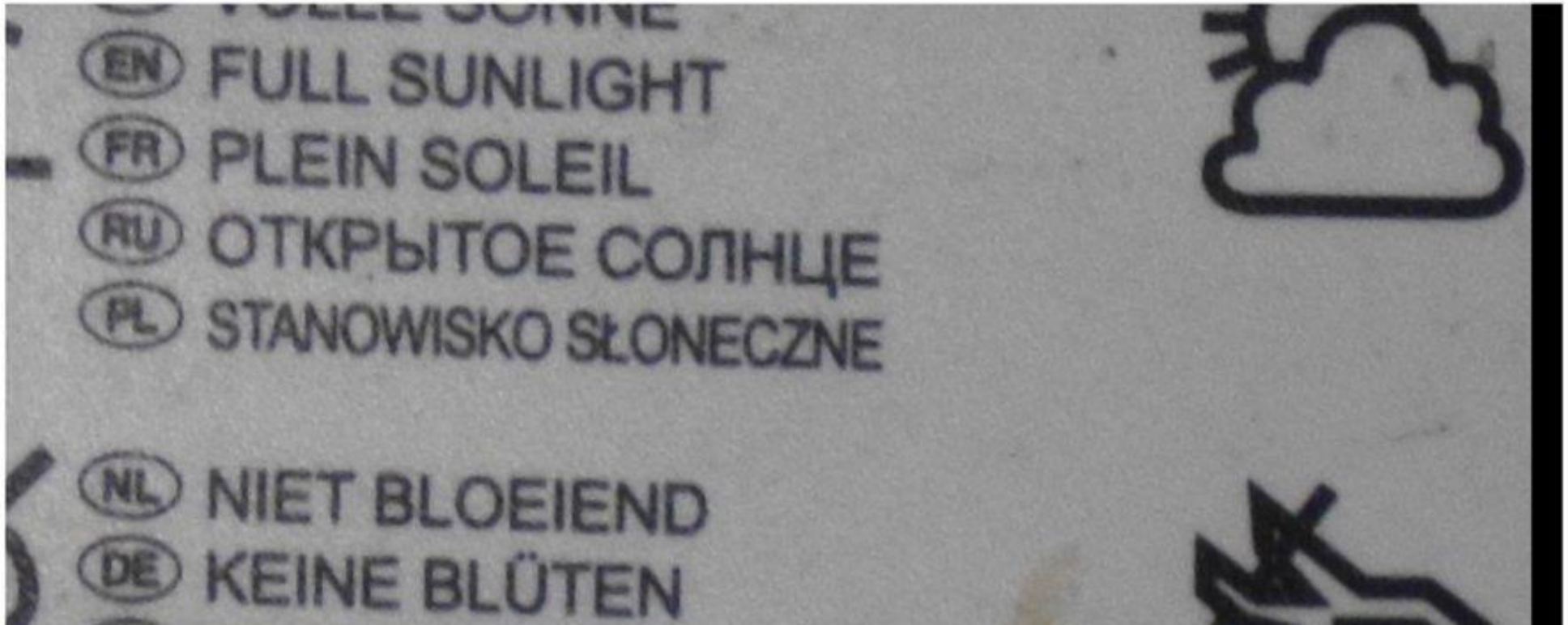
MICHAEL WIESNER

AUFKLÄRUNG (ON SITE)

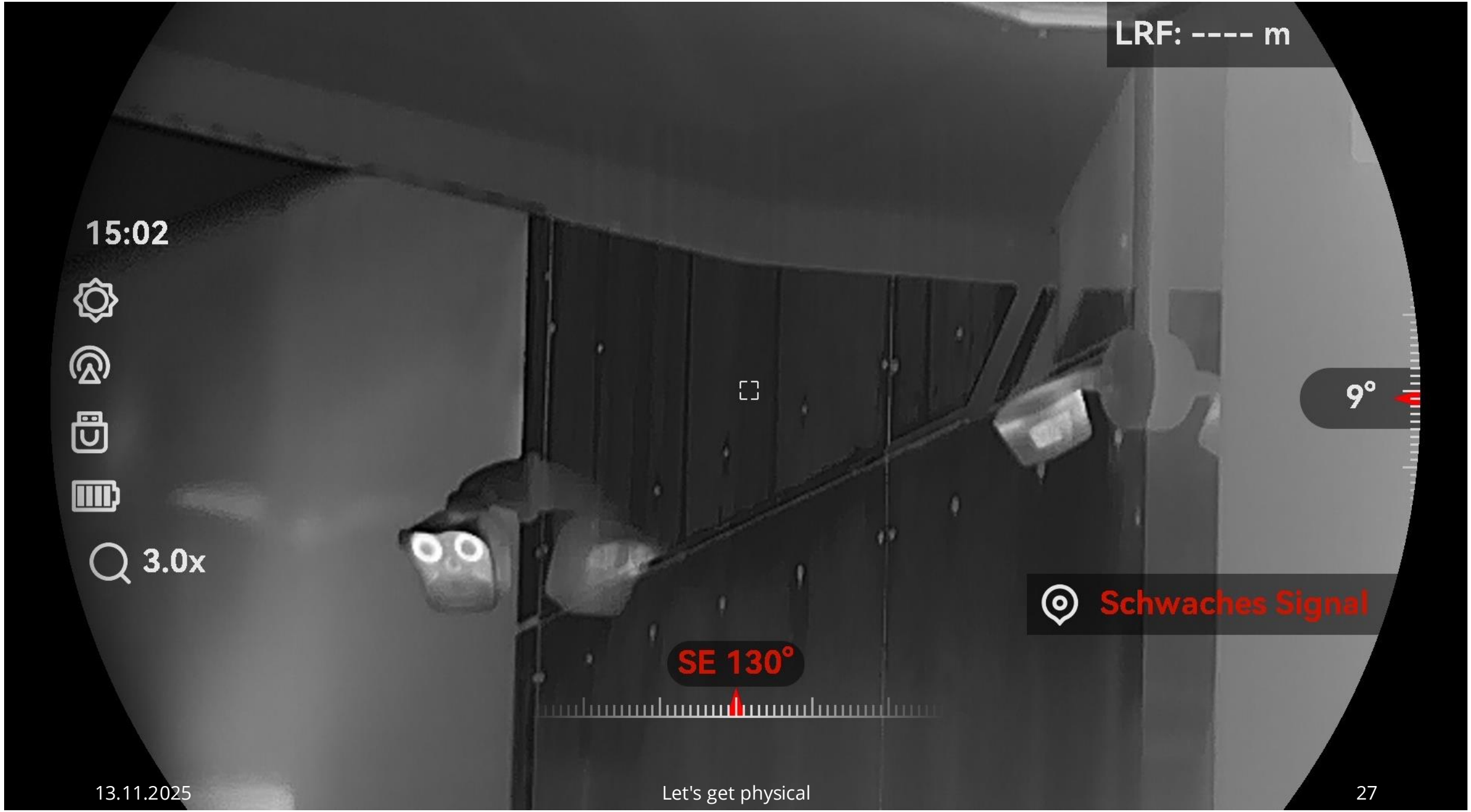
- Physische Gegebenheiten
- Werkschutz, Schlüsselrunde, Pförtner, Kameraüberwachung
- Verhalten von Mitarbeitern und Externen
- Antennen, Netzwerkzugangspunkte
- Mitarbeiter-/Besucherausweise


Nikon

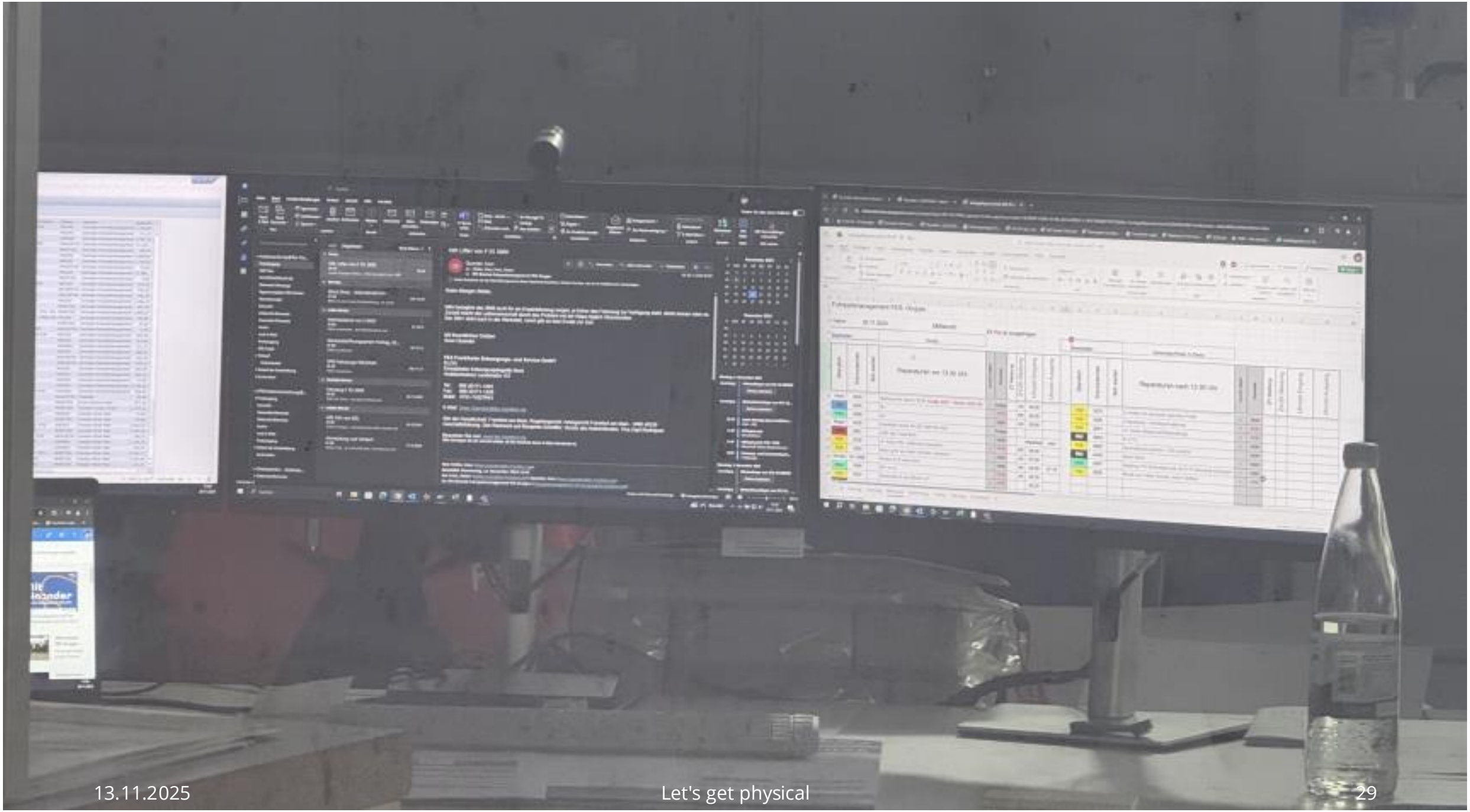

LEICA CAMERA
MADE IN GERMANY
NOCTIVID 10x42

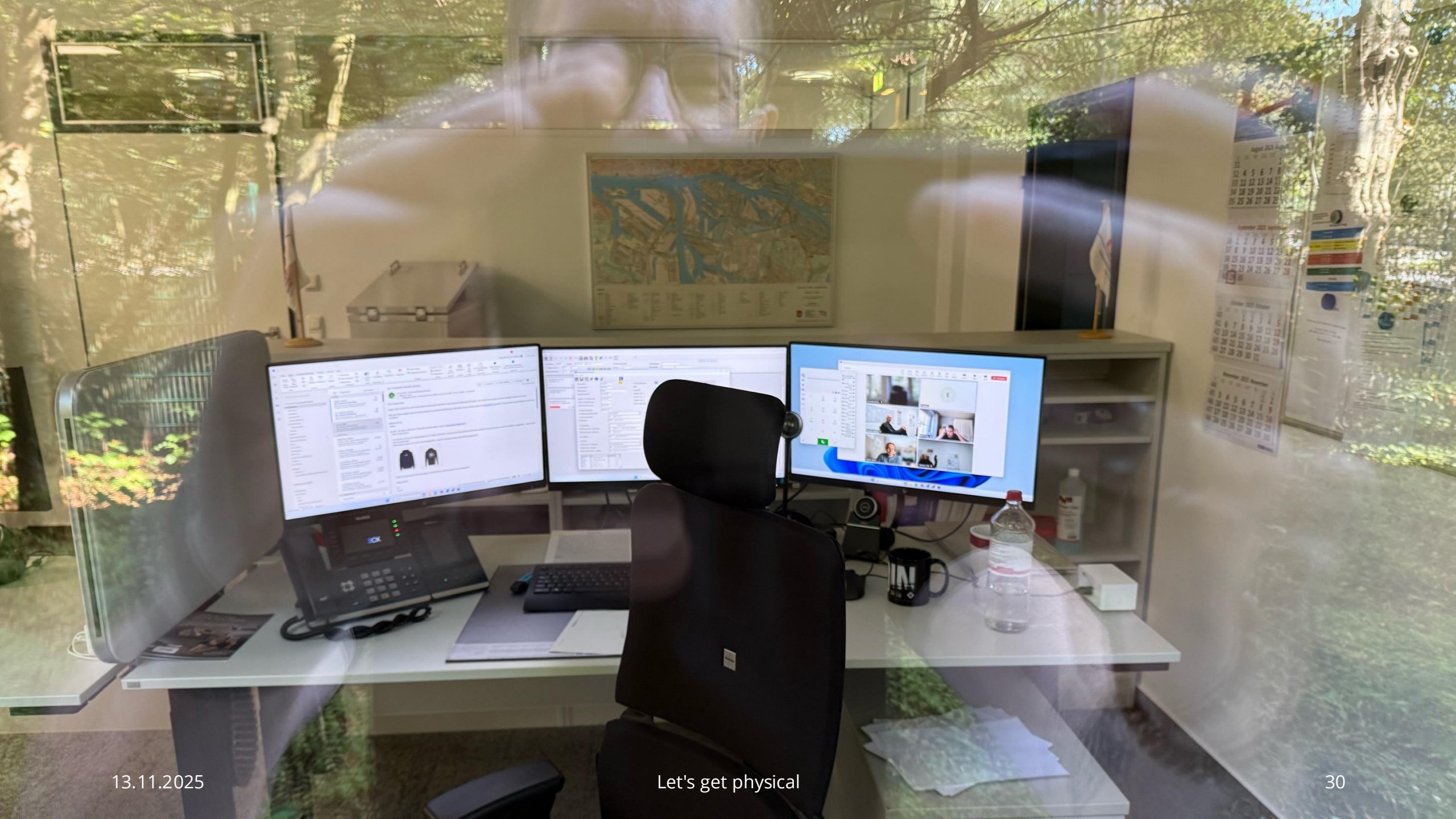

EN FULL SUNLIGHT
FR PLEIN SOLEIL
RU ОТКРЫТОЕ СОЛНЦЕ
PL STANOWISKO SŁONECZNE
NL NIET BLOEIEND
DE KEINE BLÜTEN

Let's g


LRF: ---- m
15:02
3.0x
9°
Schwaches Signal
SE 130°

Let's get physical






MINI 3 PRO

DURCHFÜHRUNG

MICHAEL WIESNER

DURCHFÜHRUNG

- In oder außerhalb Geschäftszeiten?
- Verkleidung, Ausweise
- „In Rolle schlüpfen“, selbstbewusstes Auftreten, Habitus anpassen

(Achtung: Social Engineering!)


AAA
Access All Areas
Michael Wiesner
Freundlicher Hacker
MITARBEITERAUSWEIS


DIENSTAUSWEIS
DEUTSCHER MESS- UND PRÜFDIENST
Wiesner
Name
Michael
Vorname
DMP
Institution
DMP230761
EMV
TCG
DMP-2018C-230761-DE
DMP-2018C-DE


KONICA MINOLTA
Wiesner
Name
Michael
Vorname
Service-Techniker
DMP-2018C-230761-DE


ROWE

MICHAEL WIESNER

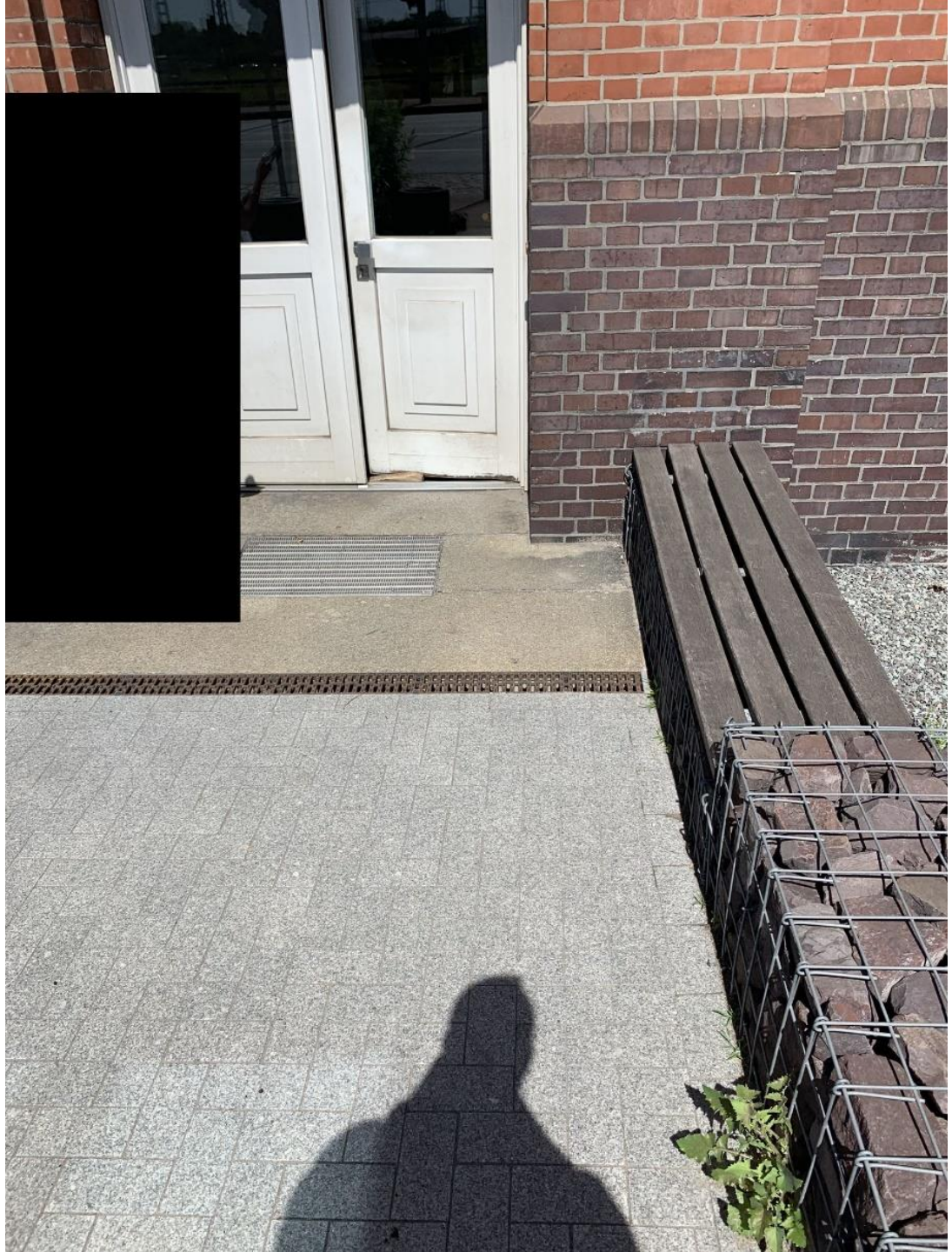
ZUTRITT VERSCHAFFEN (NICHT-DESTRUKTIV)

MICHAEL WIESNER

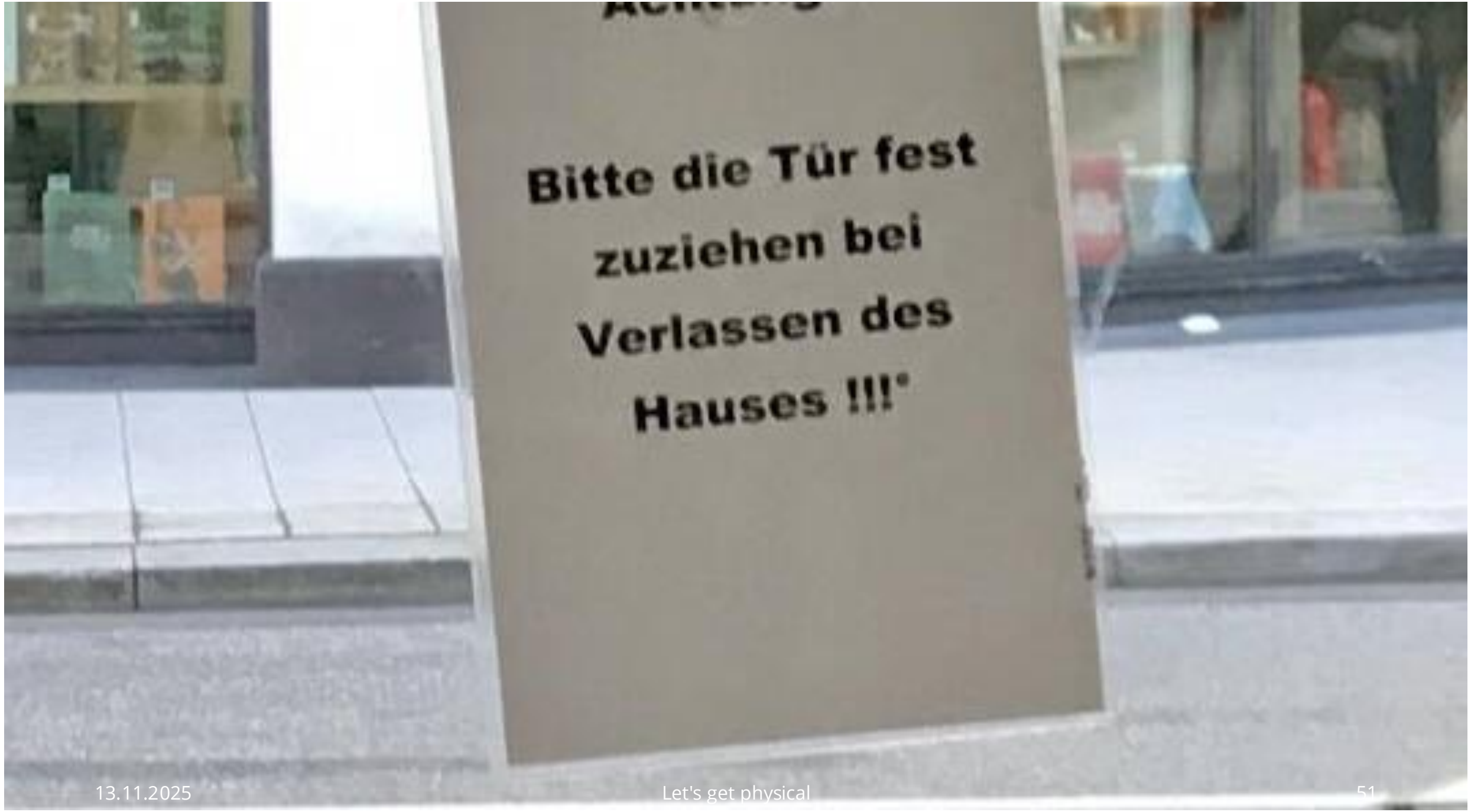
ZUTRITT VERSCHAFFEN

- Perimeter, Zäune, Tore
- Gebäude, Türen
- (Technik-)Räume
- Netzwerkschränke
- Verkabelung


ACHTUNG
Video-
überwachung!

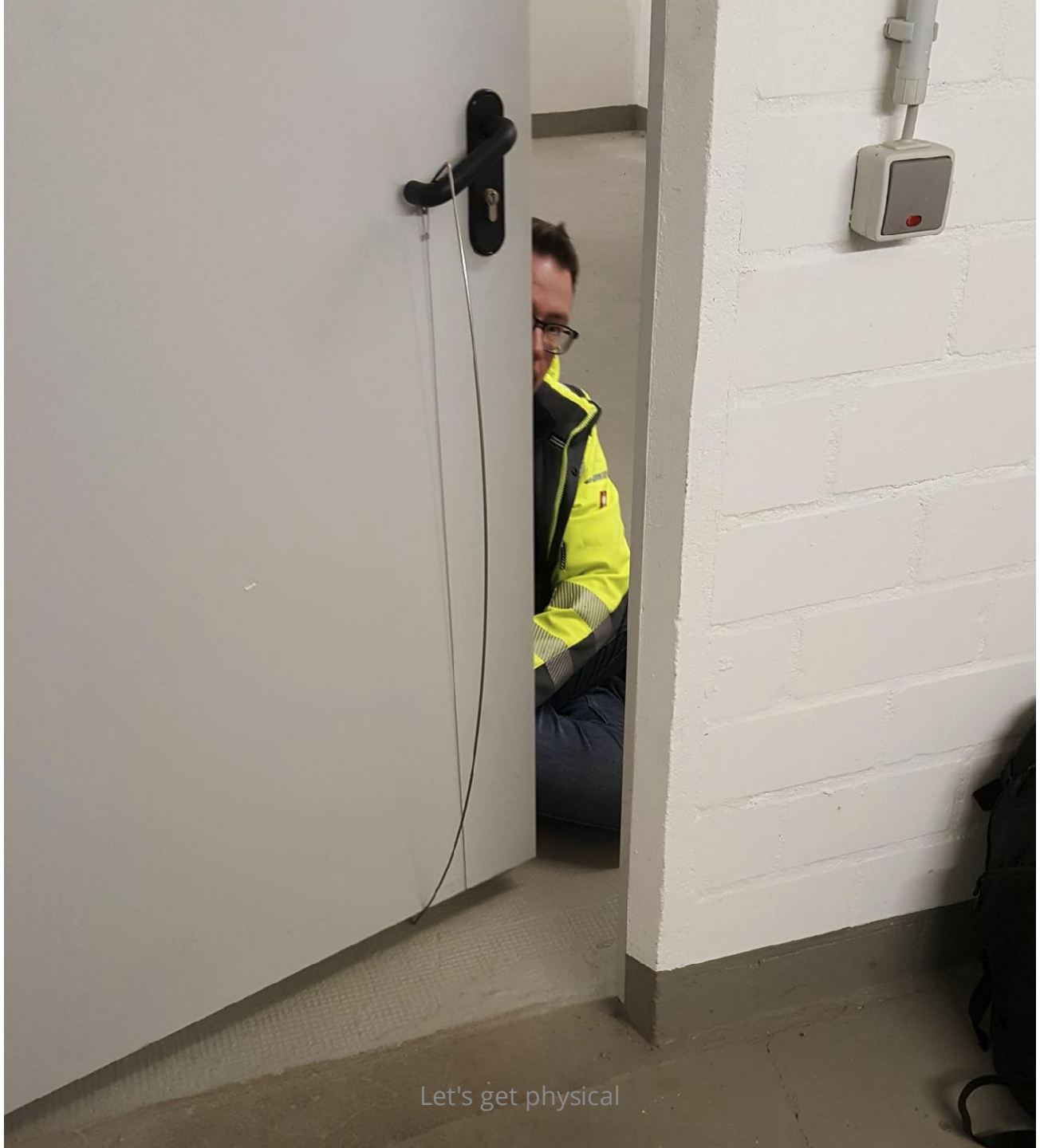


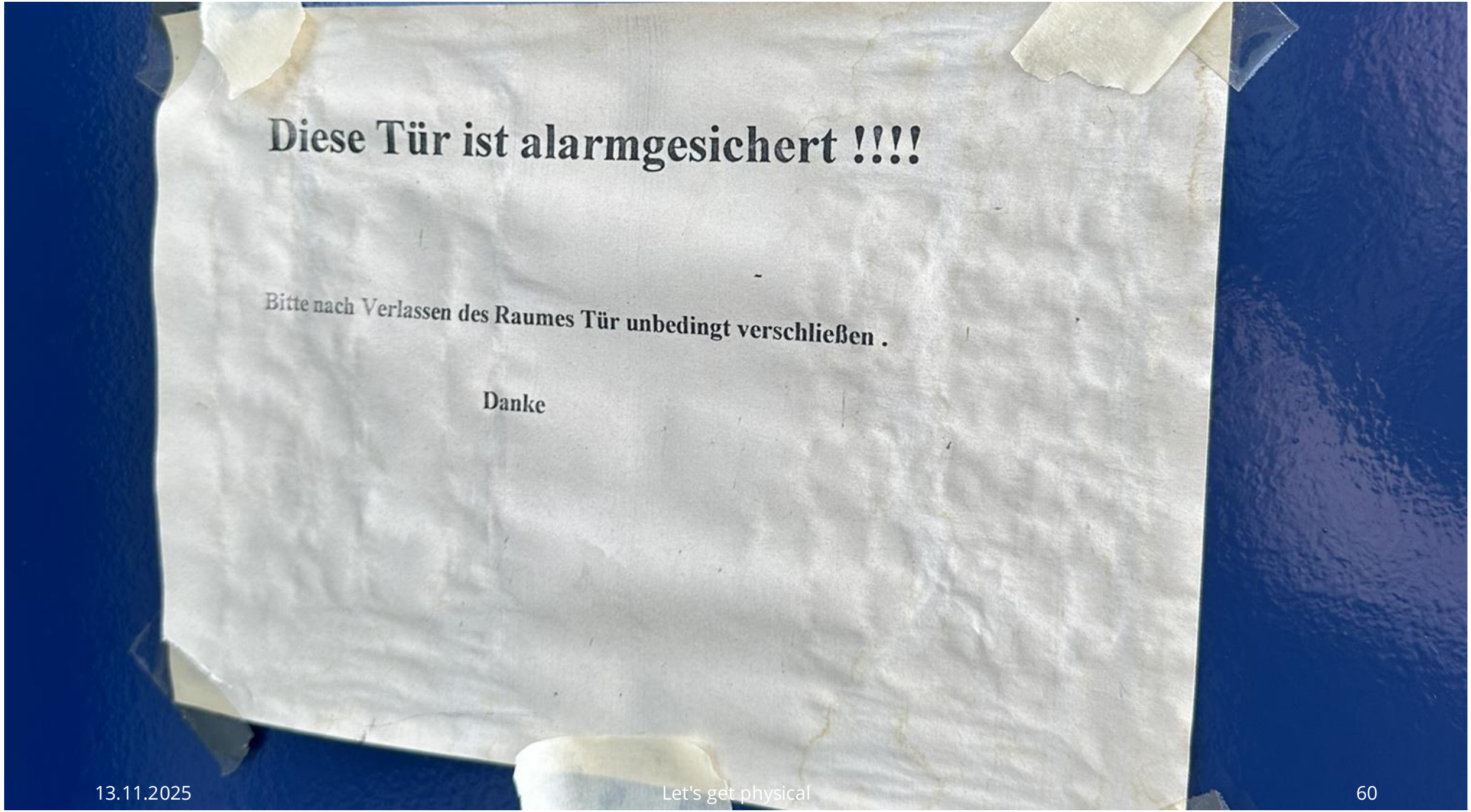

Tür zu !


Bitte die Tür fest
zuziehen bei
Verlassen des
Hauses !!!


Aus Sicherheitsgründen
bitte die Tür
immer abschließen.


7050K
OGRO




Diese Tür ist alarmgesichert !!!!
Bitte nach Verlassen des Raumes Tür unbedingt verschließen .
Danke


EK333


ENGLAND


2233


RITTAL
3524


CH 751


RITTAL

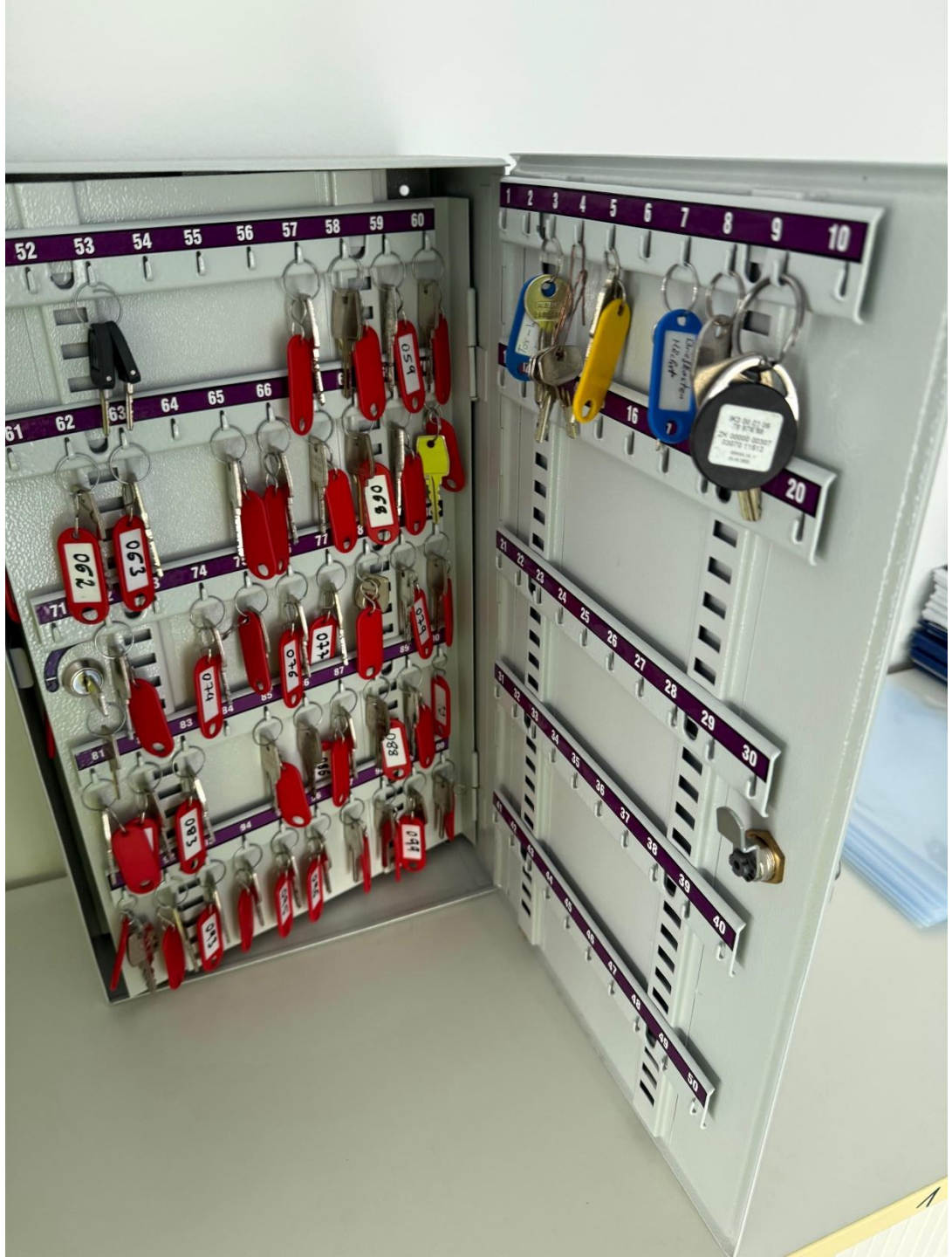

RITTAL


K2
K 2


IKON


1
2
3
4
5
6
7
8
9


1 2 3
4 5 6
7 8 9
c 0 *


52 53 54 55 56 57 58 59 60
61 62 63 64 65 66
71 74
1 2 3 4 5 6 7 8 9 10
16 20
21 22 23 24 25 26 27 28 29 30
31 32 33 34 35 36 37 38 39 40
41 42 43 44 45 46 47 48 49 50


Schlüsselkasten
Schlüssel


Auto Copy
MIFARE
DESFire
Frequency: 13.56MHZ
UID: 046C9402643680
SAK: 20 ATS: 067577+
Rescan
Read
OK
C/
S
R/W
EVVA


FLIR
1
2 abc
3 def
4 ghi
5 jkl
6 mno
7 pqrs
8 tuv
9 wxyz
0
OK

…ODER DOCH DESTRUKTIV?

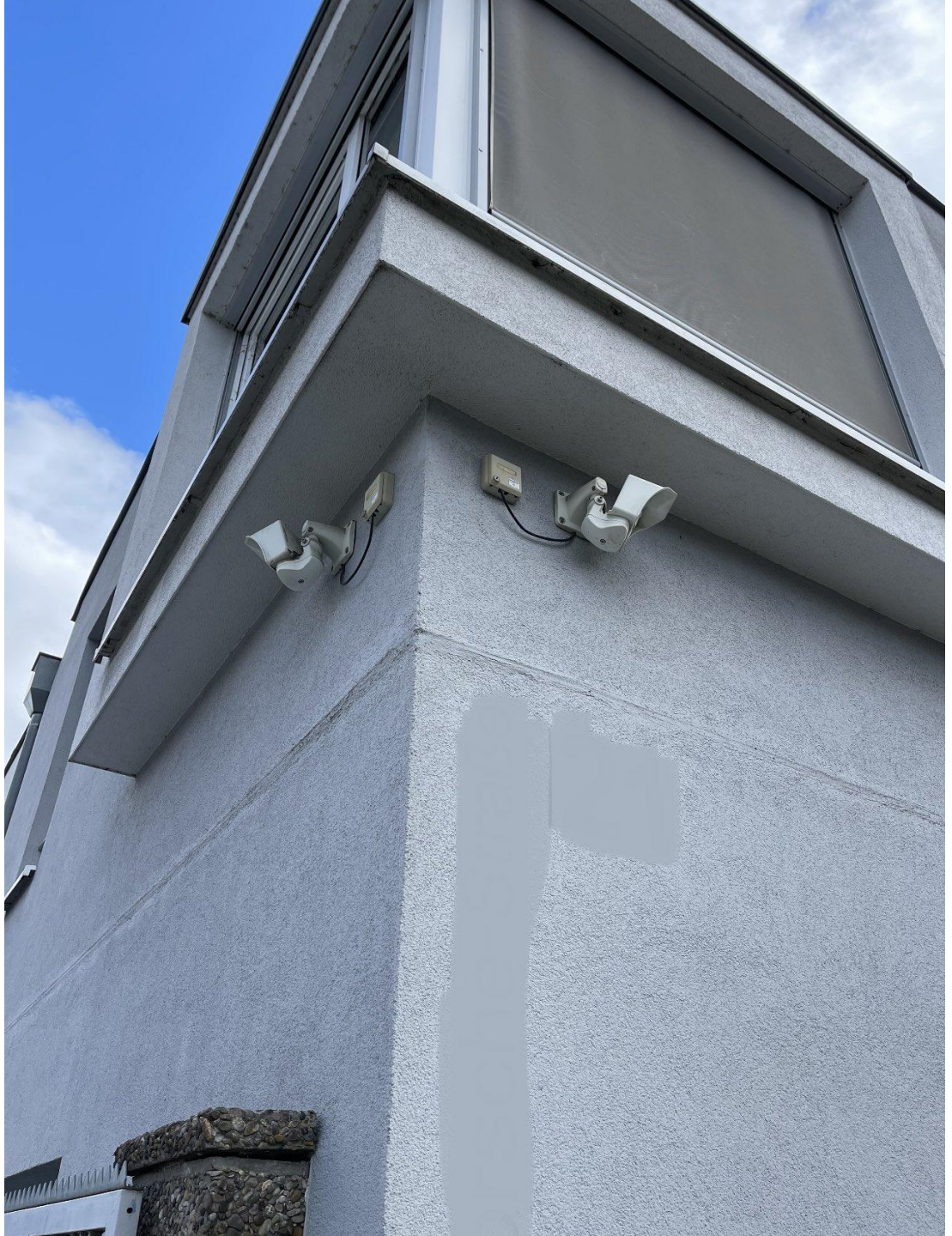

makita
LXT
makita
18V
LITHIUM-ION
GERMANY

(NETZWERK-)ZUGANG ERHALTEN

MICHAEL WIESNER

ZUGANG ERHALTEN

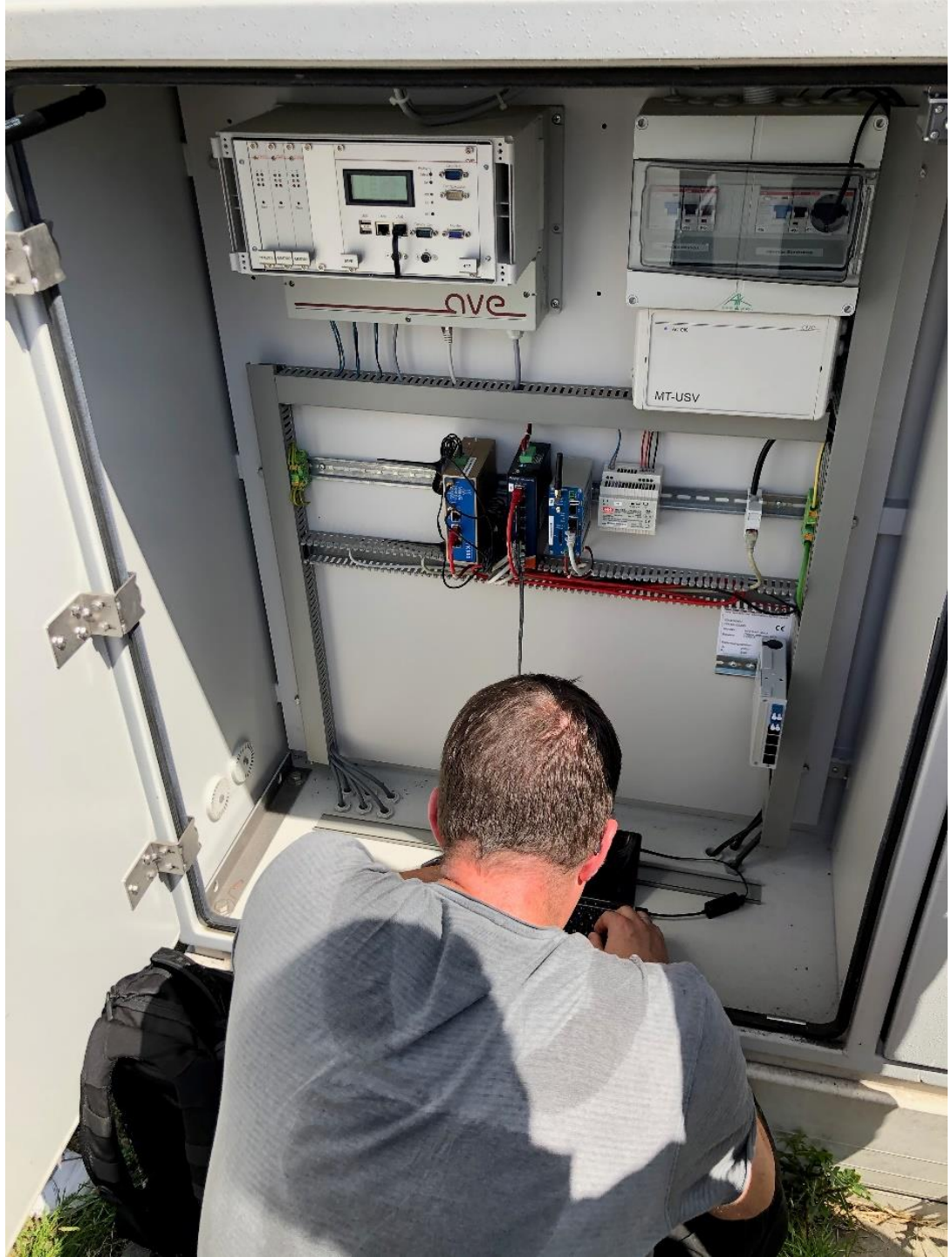
- Arbeitsplatzrechner
- Netzwerkdosen
- Drucker/Multifunktionsgeräte
- WLAN-Accesspoints
- Überwachungskameras
- Zeiterfassungsterminals
- Gegensprechanlage
- ...




M311 1.OG
M2 EG


MOBOTIX

CE 0682

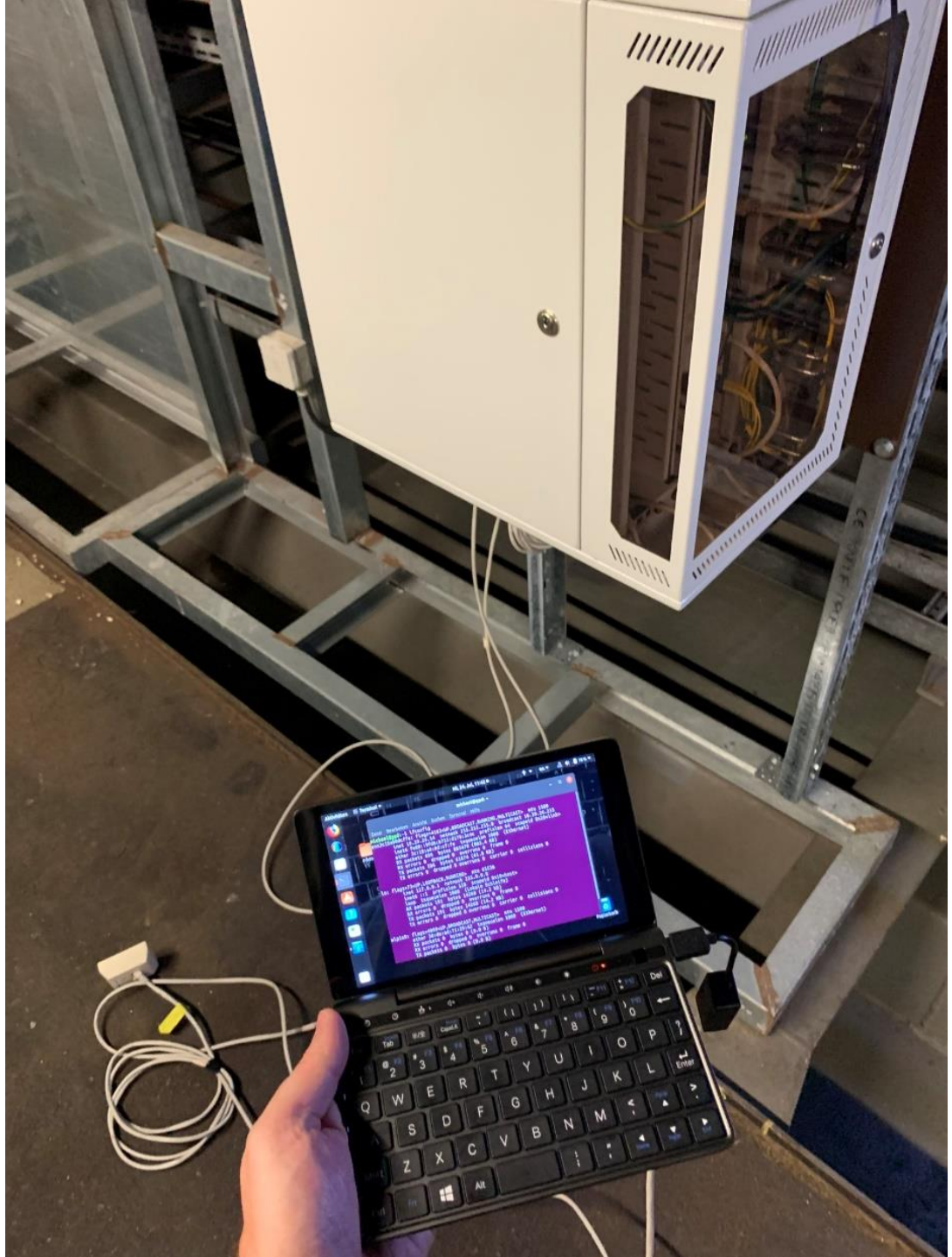

ave
MT-USV

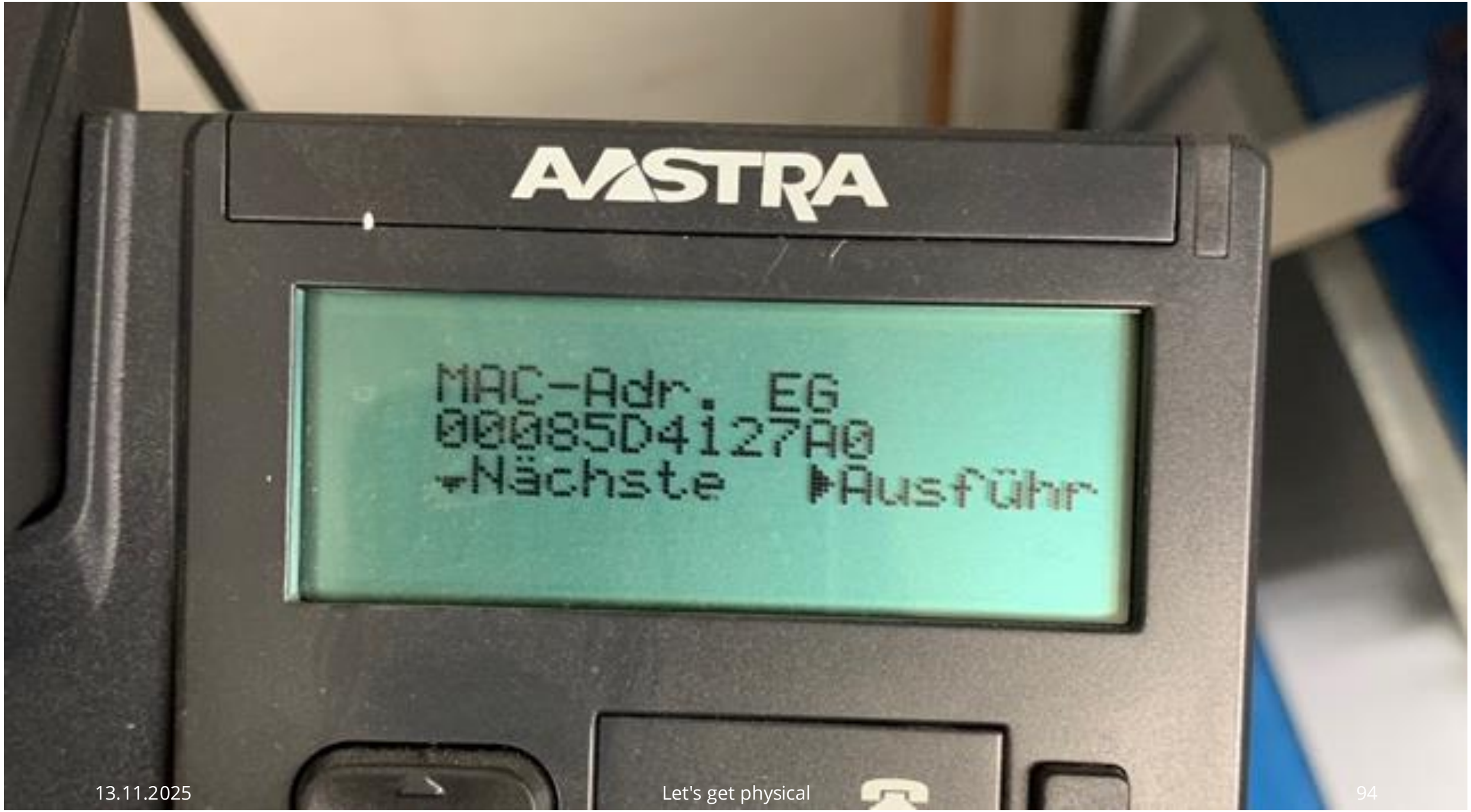

Aktivitäten
Terminal
pentest
packages
Papierkorb
pentest@pentest-t480: ~
pentest@pentest-t480:~$ ifconfig
enp0s31f6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.39.17.156 netmask 255.255.255.0 broadcast 10.39.17.255
inet6 fe80::ea8a:64ff:fe32:fced prefixlen 64 scopeid 0x20<link>
ether e8:6a:64:32:fc:ed txqueuelen 1000 (Ethernet)
RX packets 54 bytes 18002 (18.0 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 83 bytes 11359 (11.3 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device interrupt 16 memory 0xed200000-ed220000
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Lokale Schleife)
RX packets 535 bytes 39546 (39.5 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 535 bytes 39546 (39.5 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
wlp3s0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
ether dc:8b:28:4a:a8:0d txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
T480
ThinkPad

SI2
T1.6AL
250V
SI1
T1.6AL
250V
CCD Barcode
Reader
GND
12412
04041980001


SKINTASTIC
LEOCID SEPT P7
ThinkPad

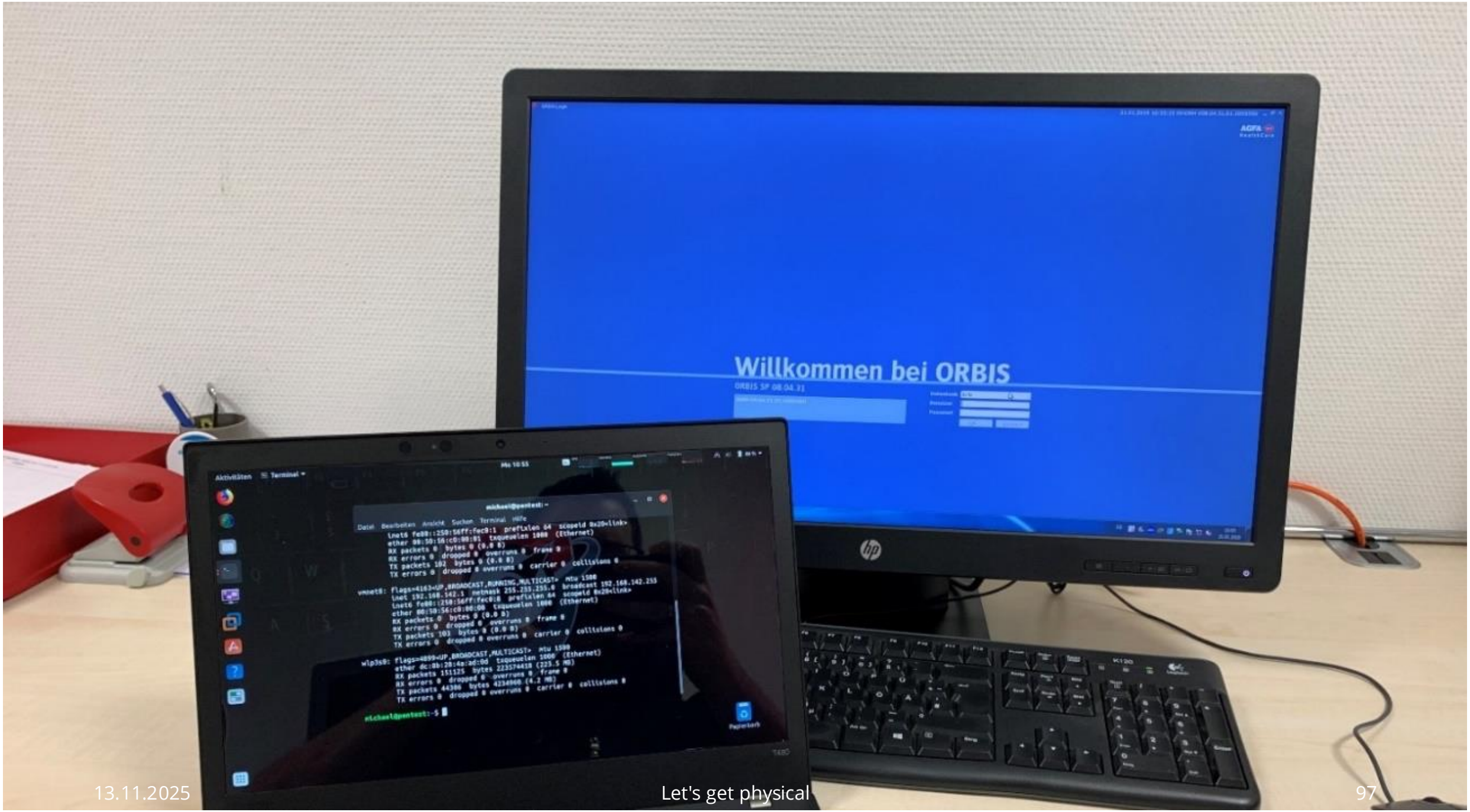

ABUS
85/50




AASTRA
MAC-Adr. EG
00085D4i27A0
▾Nächste ▸Ausführ


ResistTel IP2
NO
C
YES


NEC


Willkommen bei ORBIS
Aktivitäten
Terminal
Papierkorb

EINBRINGEN VON FREMDGERÄTEN


rmt
MADE IN CHINA
Cruzer Blade 16GB
FASTCHARGE
cellularline


TP-LINK
WPS/RESET
WAN/LAN
POWER
Nächster
Prüftermin


PENTEST DROPBOX
Pentest
Dropbox
PENTEST
DROPBOX
Property of Michael Wiesner GmbH
please call: +49 2773 81326230
UNAUTHORIZED ACCESS
PROHIBITED!
NUC22/i5/16/1000 (MAC:1c:69:7a:69:06:4a)
NICHT AUSSCHALTEN!
NICHT AUSSCHALTEN!

ESKALIEREN

MICHAEL WIESNER

PERSISTENZ

- Network Implant
- Call Home, C&C-Server
- Tunnel, WLAN, LoRa, 3G/LTE/5G
- Teamviewer / Anydesk / etc.

MICHAEL WIESNER

LATERAL MOVEMENT

- Active Directory
- Schwachstellenscans
- Exploiting

NACHARBEITEN

MICHAEL WIESNER

NACHARBEITEN

- Abschlussbericht
- Gesamtrisikobeurteilung
- Schwachstellen nach Risiko
- Chronologischer Ablauf
- Fotos/Videos
- Abschlussbesprechung

DOS & DON‘TS

MICHAEL WIESNER

DOS

- Zu zweit vor Ort, eine Person zur Unterstützung
- Ausreichend Zeit einplanen
- Optimalen Zeitpunkt wählen (wichtiges Ereignis, Montagmorgen, Mittagspause, warmer Sommertag, …)

MICHAEL WIESNER

DOS

- Aufklärung mit Grundausrüstung durchführen (unverhofft kommt oft!)
- Möglichst umfangreich/vollständig dokumentieren
- Immer einen „Plan B“ haben (z.B. bei geänderten Gegebenheiten oder Entdeckung)
- Behörden informieren!

DON‘TS


fensiveCon
8 Februar 2020 / c-base Berlin
KRITIS
I HEAR
BER
JUST
WANNACRY
NICHT FÜ
MILITÄRISCH
EM ROF SKROW

MICHAEL WIESNER

DON‘TS

- „Hacker-Style“, Tactical Rucksack, beklebtes Notebook
- Menschen bloßstellen, zu sehr unter Druck setzen
- Aggressives Auftreten, insb. gegen Sicherheitspersonal

BEHÖRDEN NICHT INFORMIEREN


POLIZEI

ZU WARM ANZIEHEN

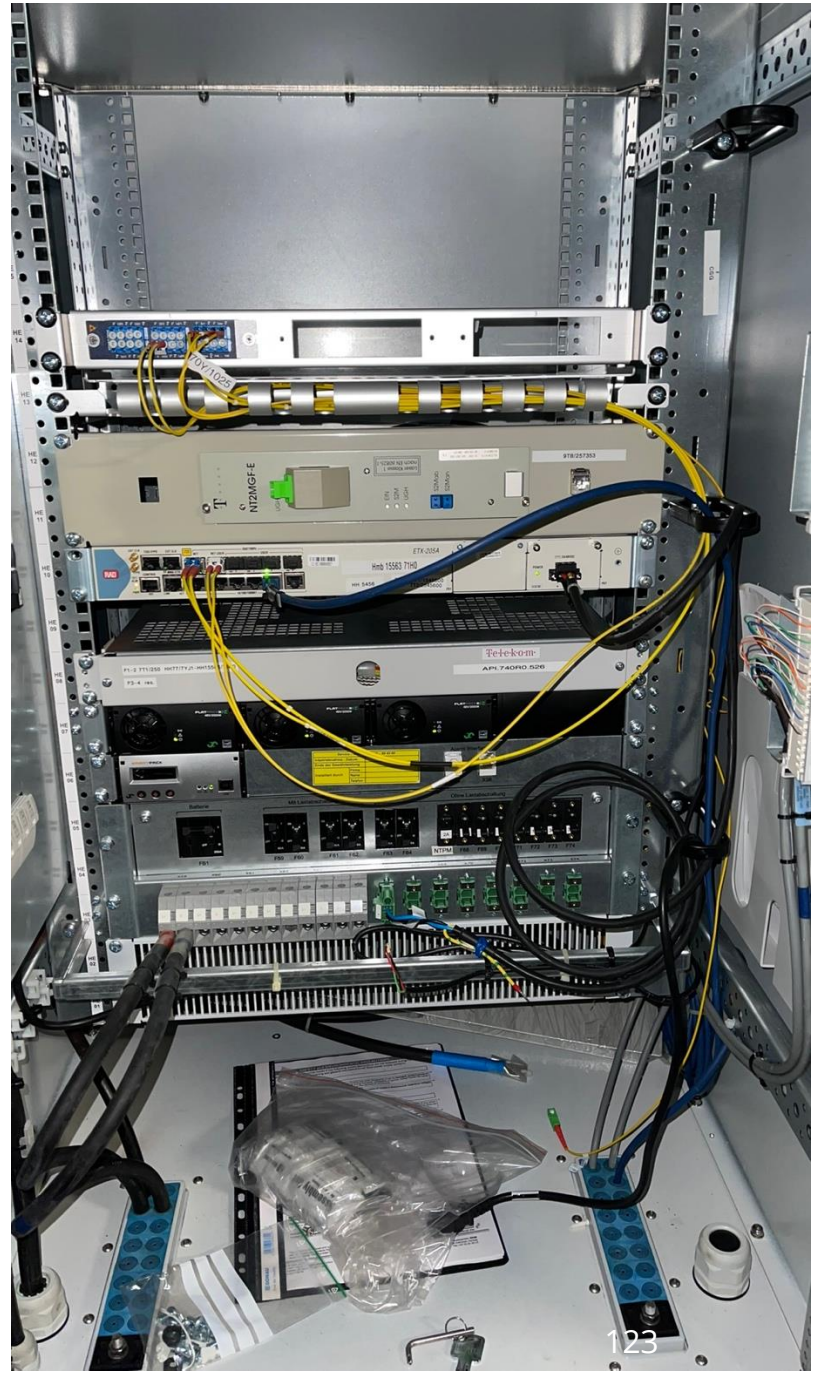

Gast
Visitor

STECKEN BLEIBEN

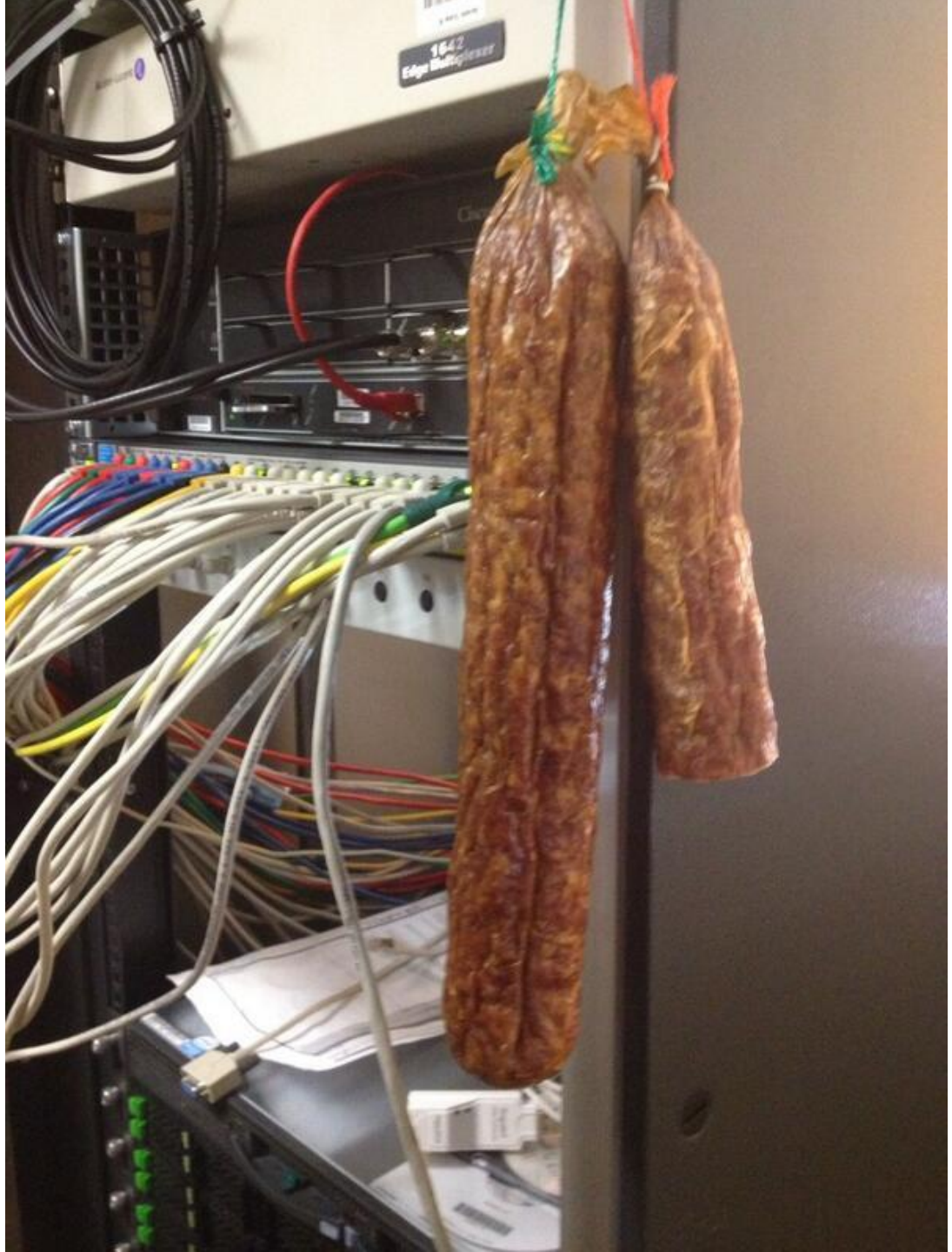
MICHAEL WIESNER

SCOPE VERLASSEN/ SICH HINREIßEN LASSEN


Headquarters: Eltek
8, 3036 Drammen, Norway
Fax: +47 32 20 32 10

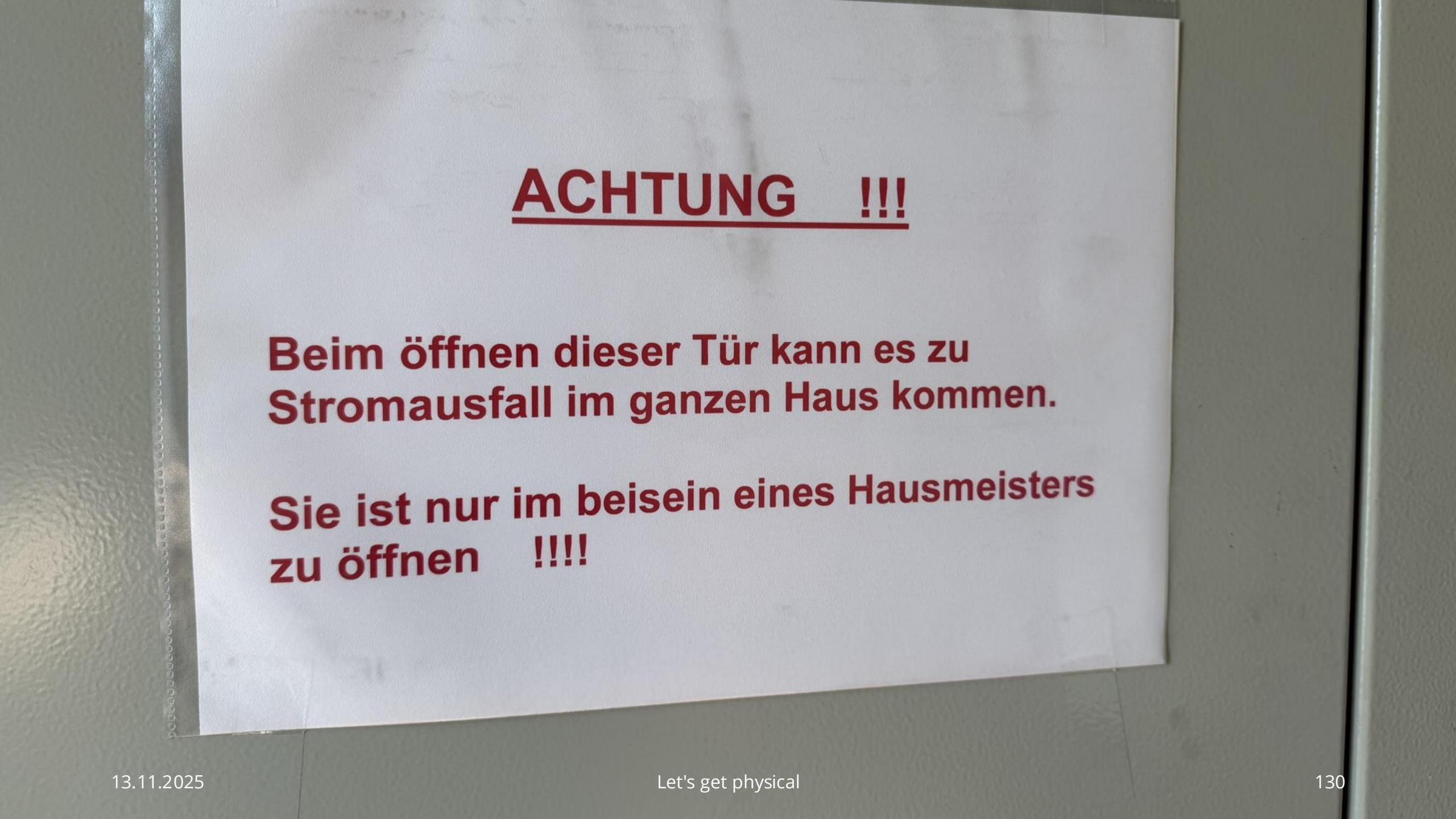

NT2MGF-E
Telekom

KURIOSES




Pilsner
4,9% vol


Sentinel
FORMATTED
CHANTRÉ
WEINBRAND
CHANTRÉ & CIE
KG mit beschränkter Haftung
D-6501 Nieder-Olm
0,1 l
36% vol
327 x 140 x 231
11 3/4-14


ACHTUNG !!!
Beim öffnen dieser Tür kann es zu Stromausfall im ganzen Haus kommen.
Sie ist nur im beisein eines Hausmeisters zu öffnen !!!!

VIELEN DANK! FRAGEN?

MICHAEL WIESNER

KONTAKT

Michael Wiesner GmbH

Am Flachsacker 4

35708 Haiger

T: +49 2773 8132623 0

M: mail@wiesner.eu

W: https://wiesner.eu