Schwachstelle Mensch – Layer 8 im ISO/OSI-Modell

KNF-KONGRESS 2024

Roland Wagner

ISO/OSI-Schichtenmodell

Layer	Name	Example protocols
7	Application Layer	HTTP, FTP, DNS, SNMP, Telnet
6	Presentation Layer	SSL, TLS
5	Session Layer	NetBIOS, PPTP
4	Transport Layer	TCP, UDP
3	Network Layer	IP, ARP, ICMP, IPSec
2	Data Link Layer	PPP, ATM, Ethernet
1	Physical Layer	Ethernet, USB, Bluetooth, IEEE802.11

7 Application

6 Presentation

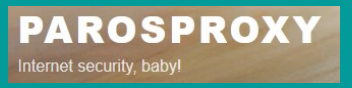
5 Session

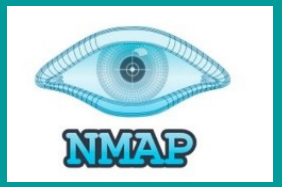
4 Transport TCP/UDP

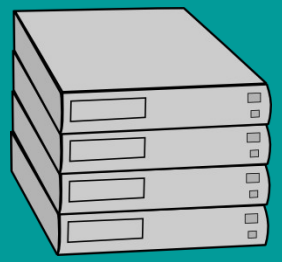
3 Network IP

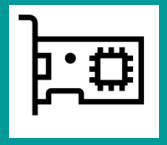
2 Data Link

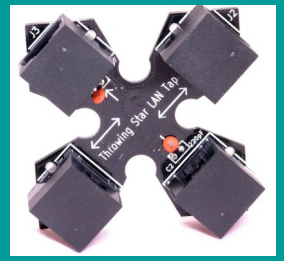
1 Physical











Agenda

1. Awareness
2. Begriffe
3. Sensibilisierung
4. Schulung
5. Gefahren
6. Deep Fake
7. Rubber Ducky
8. Schutzmaßnahmen
9. Do‘s and Dont‘s
10. Konzept
11. ABC
12. Produkte
13. Lernplattform
14. Gamification
15. VTC
16. Veranstaltungen
17. Podcast
18. Experience Desk
19. Gegenmaßnahmen
20. Ausblick

… so viele Folien …

… schon wieder …

langweilig !!!

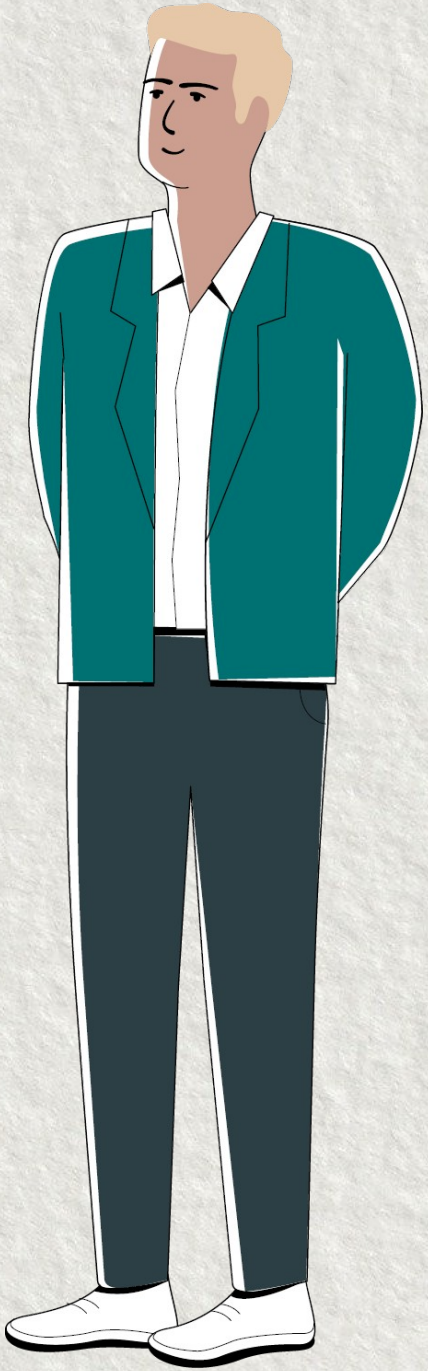
Die Handlung ist frei erfunden. Etwaige Ähnlichkeiten mit tatsächlichen Begebenheiten oder mit lebenden oder verstorbenen Personen wären rein zufällig.

Lena Maier

- Firma Öko-Pharma Wiesbaden
- Department HR
- Recruiterin
- Langjährige Erfahrung im Bewerbermanagement

Andi Schmidt

- Firma PI-Consult
- Department HR
- Recruiter



Szenario:

- Freitag Abend nach Messeschluss
- Treffpunkt „After Work Party“

Sorry, ist hier noch Platz?


Ja klar, ist wirklich voll hier.

„Lena Maier von diesem Pharma-Unternehmen in Wiesbaden? Richtig? Hab Deinen Vortrag gesehen, war echt klasse!


Oh Danke! Das Unternehmen heißt „Öko-Pharma Wiesbaden“

Ja richtig! Ich bin übrigens Andreas Schmidt von PI-Consult, oder einfach nur Andi.


Ja, ich weiß, habe auch deinen Vortrag heute gesehen – aber nur kurz – musste dann weg.

Da hast Du aber was verpasst.

Ihr seid vermutlich auch auf der Suche nach neuen Mitarbeitern . so wie fast alle hier – ist echt schwierig! Wie ist es denn diese Woche gelaufen – wenn man fragen darf?


Naja, hatte mir mehr erhofft – bin schon froh um jeden einzelnen, der am Stand war und mir seine Kontaktdaten gegeben hat. Überprüfe gerade nochmal meine Liste mit den letzten Kandidaten. Und wie liefs bei Dir?

Auch so ähnlich – meine Liste könnte auch länger sein.

Oh da fällt mir ein ich sollte die Liste lieber noch auf einen USB-Stick sichern. Das letzte mal ist mir das Notebook abgeraucht. Alle Daten waren weg! Mein Cheffin war nicht gerade „amused“ darüber …


Gute Idee, dann mach ich auch noch schnell eine Sicherung auf USB-Stick.

Erläuterungen zu Szene 1

- Was ist in diese Szene passiert:
- Freitag Abend nach Messeschluss treffen sich zwei Recruiter
- Sie haben sich nach der Messe ausgetauscht. Man hat Kontakte geknüpft, Informationen, Telefonnummern ausgetauscht.
- Bisher ein netter Abend für beide Akteure
- Ein ganz normaler Vorgang, nicht außergewöhnliches ist passiert

- Zeitsprung bis Montag Morgen
- Neuer Ort: Das Büro von Lena Maier


PRIVACY
SECURITY

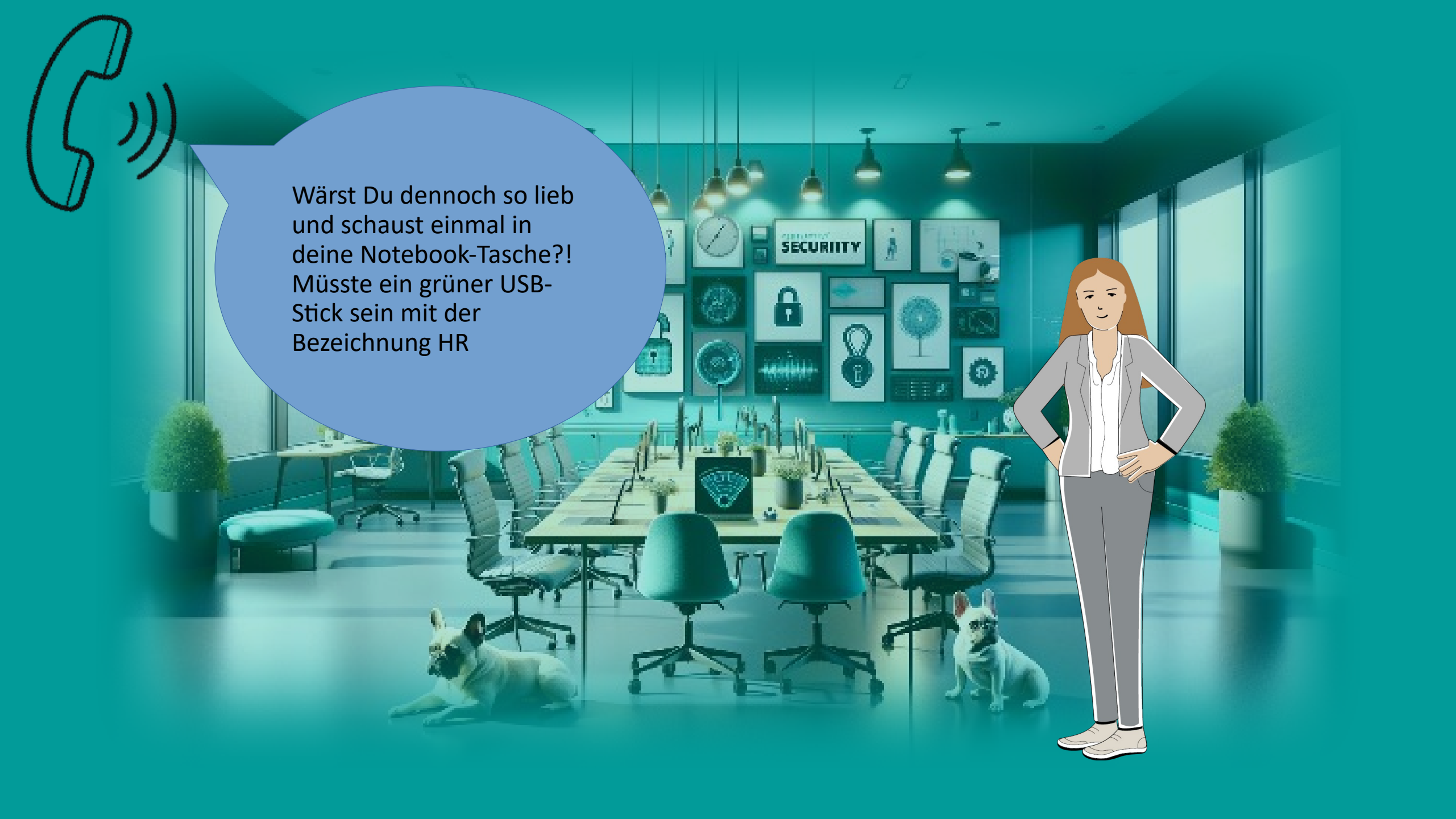

Hallo Lena, Andi Schmidt hier. Ich hoffe Du erinnerst Dich noch?
SECURITY


Ja klar doch, war ein netter Abend. Hab nicht damit gerechnet, so bald von Dir zu hören. Sagtest Du nicht Du hättest diese Woche viel zu tun? Und warum rufst Du über die Telefonzentrale an? Du hast doch meine Mobile-Nummer?
PRIVACY

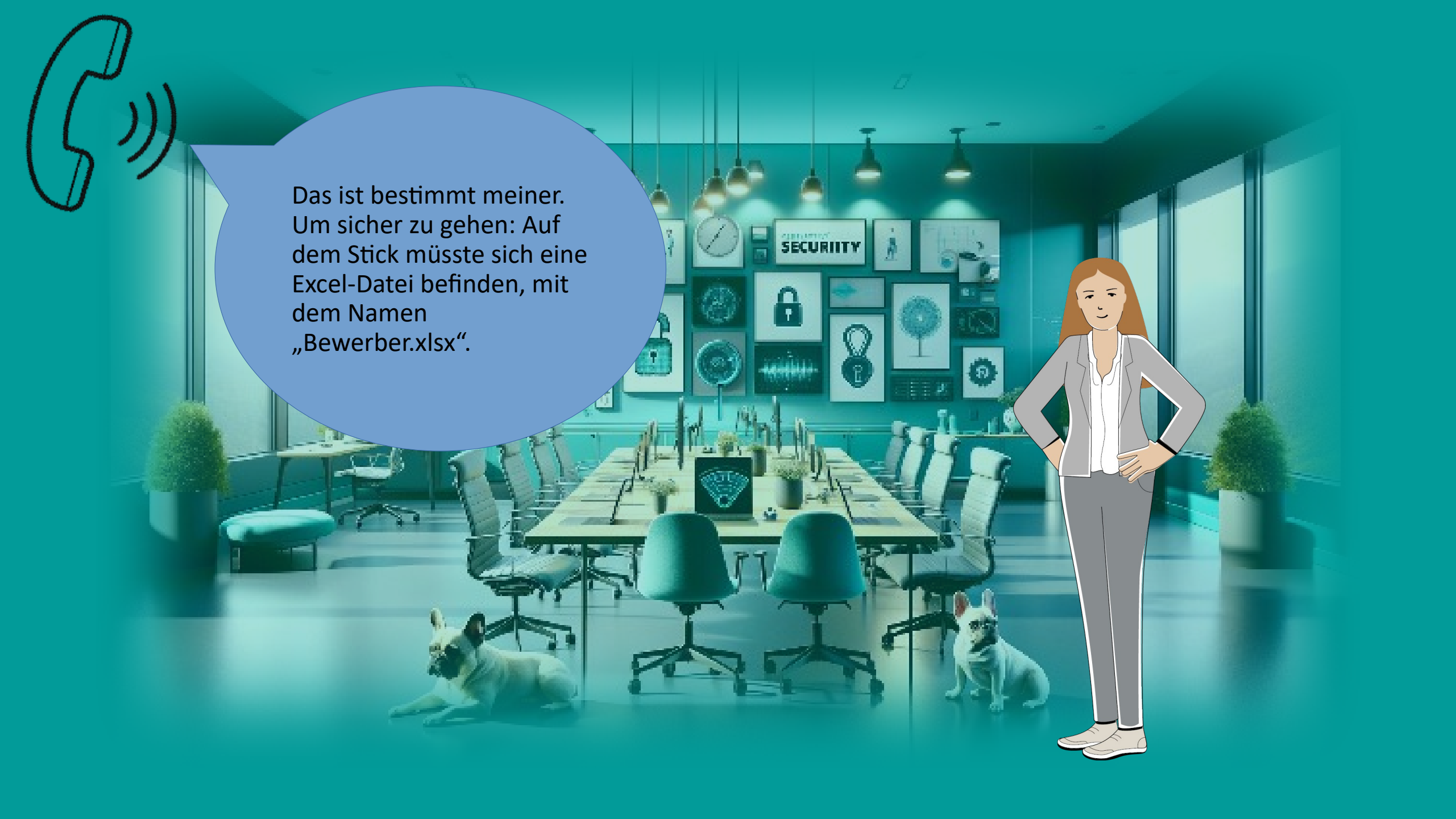

Richtig, muss auch gleich auf ein Meeting. Ich habe auf die Schnelle Deine Mobile-Nummer nicht gefunden, da bin ich über die Telefonzentrale gegangen.
SECURITY


Ich rufe nur kurz an, da ich meinen USB-Stick nicht mehr finden kann. Kann es sein, dass er am Freitag in Deine Tasche gefallen ist?
SECURITY


Kann ich mir nicht vorstellen.
PRIVACY
SECURITY


Wärst Du dennoch so lieb und schaust einmal in deine Notebook-Tasche?! Müsste ein grüner USB-Stick sein mit der Bezeichnung HR
SECURITY


Tatsächlich, da ist ein grüner USB-Stick der gehört mir nicht?!
PRIVACY
SECURITY


Das ist bestimmt meiner. Um sicher zu gehen: Auf dem Stick müsste sich eine Excel-Datei befinden, mit dem Namen „Bewerber.xlsx“.
SECURITY


Könntest Du mal schnell nachsehen, ob das der richtige Stick mit der richtigen Datei ist? Du wirst mir schon nicht meine Bewerber abwerben ...
SECURITY


OK, aber nur weil
Du es bist – Ja die
Datei ist da !
PRIVACY
SECURITY


OK, super! Vielen Dank, war echt lieb von Dir. Kannst Du noch mal schnell in Deine Notebook-Tasche schauen ob sich die Visitenkarten meiner Bewerber auch in Deiner Tasche befinden?
SECURITY


Die habe ich am Freitag Abend zusammen mit dem USB-Stick auf dem Tisch liegen gehabt.
SECURITY


Moment …
Nein, tut mir leid, Visitenkarten finde ich keine.
PRIVACY
SECURITY


OK, kein Problem, Hauptsache Du hast den USB-Stick. Hm, was machen wir mit dem Stick? Ich vertraue Dir den USB-Stick an. Oh, ich muss auch gleich weiter. Ich melde mich die Woche noch mal – vielleicht können wir uns ja auch treffen – bis dann
SECURITY


Bis dann ...
PRIVACY
SECURITY

Erläuterungen zu Szene 2

Ein normaler Telefonanruf von zwei Personen, die sich vor einigen Tagen kennengelernt haben – Andi hat Lena um Hilfe gebeten - Lena kennt ja Andi und hat ihm bereitwillig geholfen

In der Firma Öko-Pharma ist die Verwendung von unbekannten USB-Sticks an Firmenrechner verboten. Lena fühlt sich dabei etwas unbehaglich. Muss sie das jetzt melden? Aber es ja nichts passiert.

Einige Tage später wird plötzlich ein großer Teil der Clients und Server von Öko-Pharma Wiesbaden durch Ransomware verschlüsselt.

Was ist passiert? War Andi doch nicht so freundlich?

„Der“ Andi Schmidt von PI-Consult hat nicht wirklich bei Lea angerufen!

Es gibt da noch einen dritten Protagonisten in der Szene!

Hacker UX24

- 29 Jahre alt
- „Freier Mitarbeiter“ der Hackergruppe XOR
- Wohnort: unbekannt
- Spezialist für „hardwarenahe Angriffe“

Was ist wirklich passiert?

Back in Time:

Freitag Abend:

- UX24 beobachtet Lena und Andi
- Vorbereitete USB-Sticks


HR


Personal-
abteilung

Technische Skizzen

Passwörter


Bilanzen

Was ist wirklich passiert?

Back in Time
Freitag Abend:

- UX24 beobachtet Lena und Andi
- Vorbereitete USB-Sticks
- „umgekehrter Diebstahl“
- Stimme von Andi wird aufgezeichnet

Wochenende:

- UX24 trainiert seine KI mit der Stimme von Andi

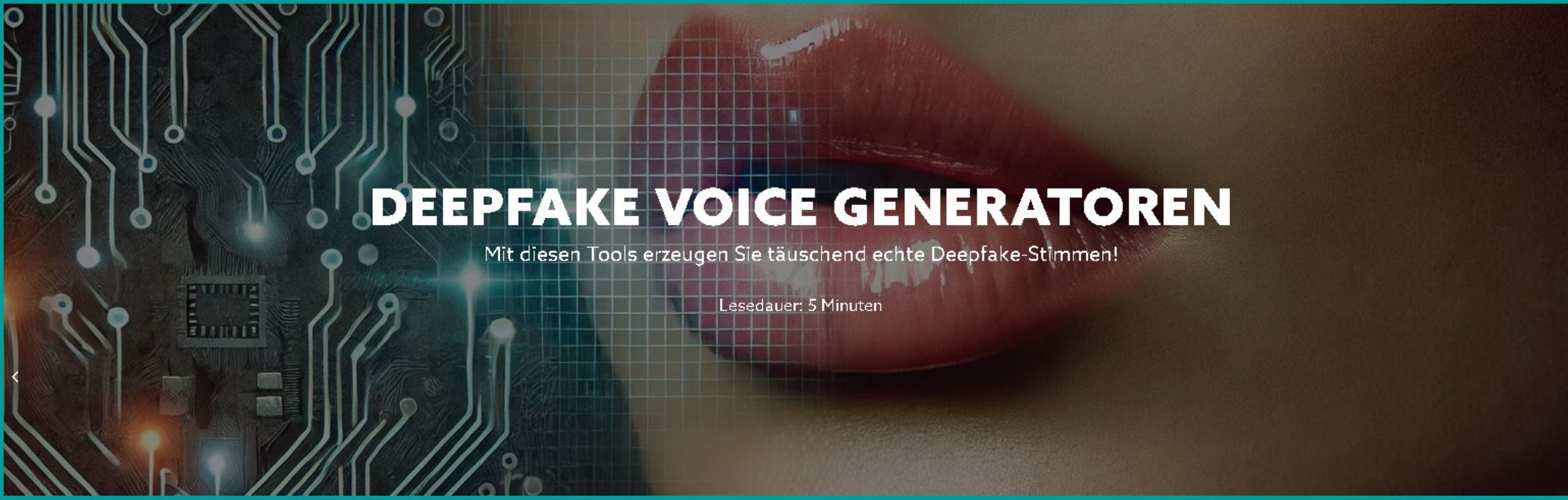
Montag Morgen:

- Anruf von UX24 bei Lena mit KI-Stimme
- Vertrauen aufbauen
- Zeitdruck
- Ablenkung

Die Handlung ist fr[illegible]n.
Etwaige Ähnlic[illegible]mit
tatsächli[illegible]benheiten oder
mit l[illegible]oder verstorbenen
Pers[illegible]wären rein zufällig.

Science Fiction ?

Was ist Deep Fake ?



Was ist Deep Fake ?

Was ist Deep Fake ?

Alexa kann künftig mit der Stimme von Toten sprechen

Von t-online, jnm

Aktualisiert am 23.06.2022
Lesedauer: 2 Min.

Lautsprecher Amazon Echo mit dem Alexa Voice Service: Bald soll Alexa auch die Stimme von Verstorbenen imitieren können. (Quelle: Franziska Gabbert/Archiv./dpa)

News folgen

Amazons Sprachassistentin Alexa könnte bald einen unheimlichen Trick beherrschen: Sie soll die Stimme von Verstorbenen nachahmen – und mit dieser dann Geschichten vorlesen.

Was ist Deep Fake ?

- https://youtu.be/N2X-GHnijKs
- https://youtu.be/1h-yy3h1u04
- https://youtu.be/6sUO2pgWAGc

Rubber Ducky?

USB RUBBER DUCKY

$79.99

NEW VERSION OF THE BEST SELLING HOTPLUG

With a few seconds of physical access, all bets are off...

USB RUBBER DUCKY	PRO BUNDLE	ELITE BUNDLE
$79.99	$99.99	$129.99

Accessories

Advanced DuckyScript Online Course	USB Rubber Ducky Textbook	Payload Studio Pro
$59.99 USD	$39.99 USD	$79.99 USD
USB Rubber Ducky Multi-Color Cases	USB Rubber Ducky Pocket Guide	Morale Patch USB Rubber Ducky
$14.99 USD	$9.99 USD	$3.50 USD

SAVE $10

1 ADD TO CART

Pay in 4 interest-free installments of **$19.99** with shop Pay Learn more

Ships in 1-3 business day worldwide • Free US Shipping on orders >$250

All orders protected against loss, damage & theft

[USB Rubber Ducky - Hak5]


BitBox02
Bitcoin-only edition


O.MG ELITE

Wo lag der Fehler?- **Do‘s and Dont‘s**

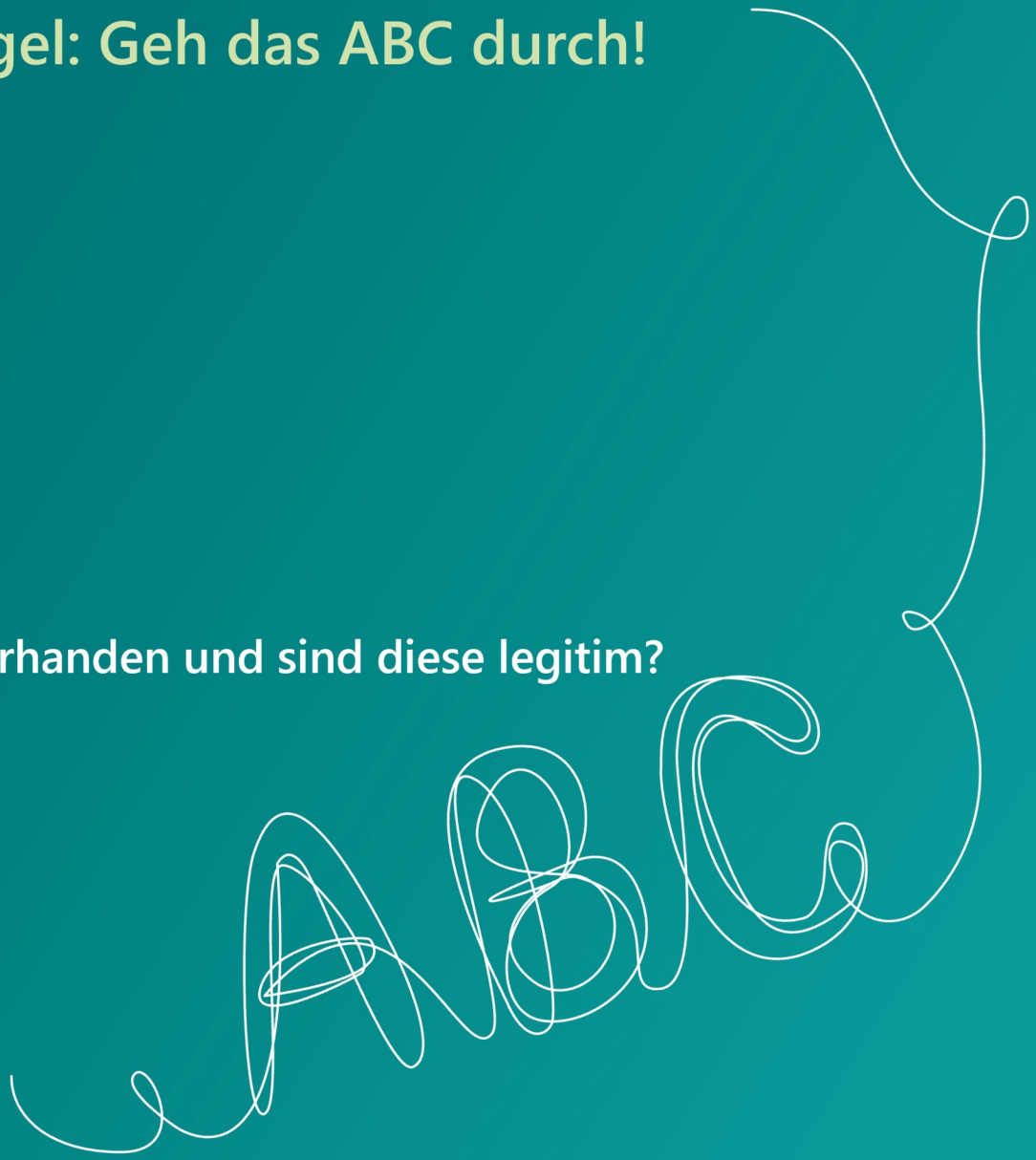
- Niemals einfach (fremde) USB Sticks an den eigenen Laptop/PC stecken
- Autoplay deaktivieren
- Sicherheitssoftware installieren und aktualisieren
- Nicht mit Admin-Rechten arbeiten
- USB-Sperrsoftware /physische USB-Sperren
  - Kaufsoftware / freie Software (keyboard-guard, USBGuard)
  - Bordmitteln (Intunes, /etc/udev/rules.d)
- Zurück rufen
- Verdachtsfälle melden
- Regelmäßige Backups

Schützen kann man sich mit dieser Faustregel: Geh das ABC durch!

A **Absender:** Prüfe immer, woher die Nachricht kommt!
Ist der Absender verifizierbar?

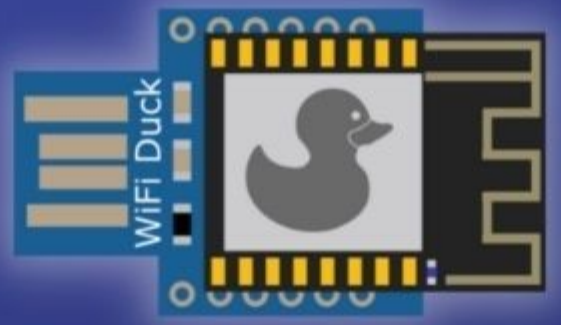
B **Betreff:** Was ist der Betreff der Nachricht?
Gibt es einen berechtigten Anlass?

C **Content:** Was ist der Inhalt der Nachricht?
Sind Anhänge, Links oder Forderungen vorhanden und sind diese legitim?



Rubber Ducky

Demo



WIFI DUCK

Wireless BadUSB

Connect

SSID: wifiduck

Password: wifiduck

Script

URL: wifi.duck

IP: 192.168.4.1

Control

Emulate a keyboard and run scripts

Super WIFI DUCK

Wireless BadUSB on ONE chip

Connect

SSID: wifiduck

Password: wifiduck

Script

URL: wifi.duck

IP: 192.168.4.1

Control

Emulate a keyboard and run scripts

Super WiFiDuck

Super WiFiDuck -- Ready

Status

Storage: 8192 byte used (99% free)

FORMAT STOP RECONNECT

Scripts

File	Byte	Actions
calc-slow	60	EDIT RUN
calc	45	EDIT RUN
ps-fast	96	EDIT RUN
ps-slow	130	EDIT RUN
ps	150	EDIT RUN

/ CREATE

Editor

/calc-slow | DELETE | DOWNLOAD | ENABLE AUTORUN

```
DEFAULTDELAY 200
WINDOWS r
DELAY 1000
STRING calc.exe
ENTER
```

Output: saved

SAVE | RUN | STOP

Editor

/ps-slow | DELETE | DOWNLOAD | ENABLE AUTORUN

```
DEFAULTDELAY 1000
WINDOWS r
DELAY 5000
STRING powershell
ENTER
STRING Slow Kezboard
ENTER
DELAY 5000
STRING EXIT
DELAY 1000
ENTER
```

Output: saved

SAVE | RUN | STOP

Fragen?

Fragen?

Was passt nicht (in der Geschichte)?

USB-Geräteklassen

Klasse	Verwendung	Beschreibung	Beispiele
00_h	Gerät	Composite Device	Die Klasse wird auf Ebene der *Interface-Deskriptoren* definiert
01_h	Interface	Audio	Lautsprecher, Mikrofon, Soundkarte, MIDI
02_h	*sowohl als auch*	Kommunikation und CDC-Steuerung	Modem, Netzwerkkarte, Wi-Fi-Adapter
03_h	Interface	Human Interface Device	Tastatur, Maus, Joystick etc.
05_h	Interface	Physical Interface Device	Physikalisches Feedback, etwa für Force-Feedback-Joysticks
06_h	Interface	Bilder	Digitalkamera, Scanner
07_h	Interface	Drucker	Laserdrucker, Tintenstrahldrucker
08_h	Interface	Massenspeicher	USB-Stick, Festplatten, Speicherkarten-Lesegeräte, MP3-Player
09_h	Gerät	USB-Hub	Full-Speed-Hub, Hi-Speed-Hub
$0A_h$	Interface	CDC-Daten	diese Klasse wird zusammen mit Klasse 02_h verwendet
$0B_h$	Interface	Chipkarte	Chipkarten-Lesegerät
$0D_h$	Interface	Content Security	Fingerabdruckscanner
$0E_h$	Interface	Video	Webcam
$0F_h$	Interface	Personal Healthcare	Pulsuhr
10_h	Interface	Audio/Video Devices	AV-Streaming-Geräte
DC_h	*sowohl als auch*	Diagnosegerät	*USB-Compliance*-Testgerät
$E0_h$	Interface	kabelloser Controller	Bluetooth-Adapter
EF_h	*sowohl als auch*	Diverses	ActiveSync-Gerät, RNDIS
FE_h	Interface	softwarespezifisch	IrDA-Brücke
FF_h	*sowohl als auch*	herstellerspezifisch	der Hersteller liefert einen Treiber mit

Quelle: https://de.wikipedia.org/wiki/Universal_Serial_Bus#Ger%C3%A4teklassen