
HORNETSECURITY

# Damals im Osten...


HORNETSECURITY

# Damals im Westen...

# Und heute...


3.67M
4K
174K
452K
16.2M
231M
167M
694M
2M
6M
66K
5.9M
46K
44M
575K
2.1M
20.8K
12.5K
EVERY
minute
OF THE DAY
LOCALiQ

# Größte Risiken im Geschäftsumfeld weltweit
# Allianz Risk Barometer 2024


Quelle: https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2024.pdf

# Wer sind „Die Hacker“?

HORNETSECURITY

# Wer sind „Die Hacker“?


HORNETSECURITY

# Top Ranking Hackergruppe LockBit


HORNETSECURITY

# Lockbit durch Ermittler zerschlagen - zwei Festnahmen

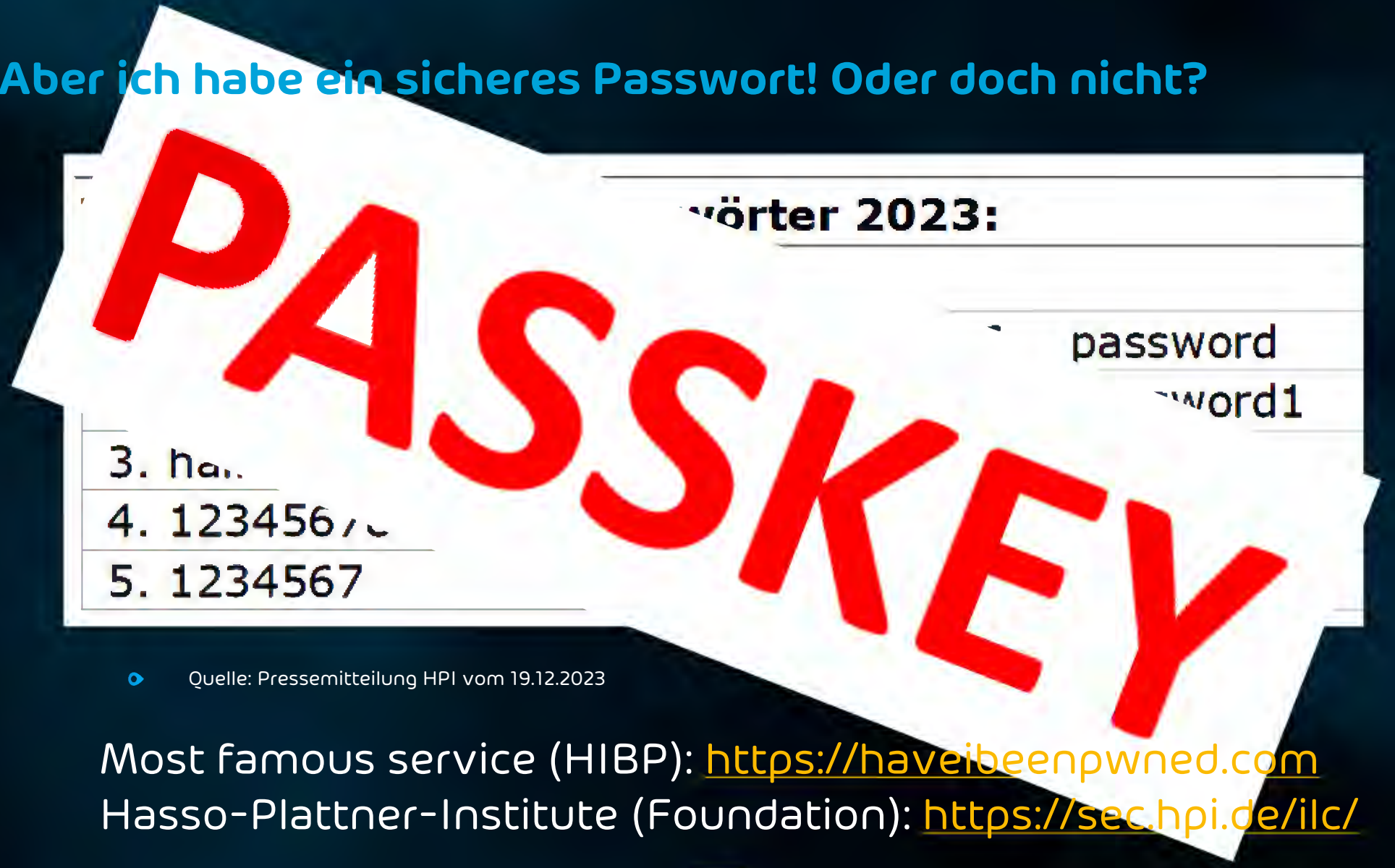

- Quelle: https://www.europol.europa.eu/

# Social Engineering Attacken auf Unternehmen

- wer ist CEO des Unternehmens
- welche Personen befinden sich in Führungspositionen?
- wer ist befugt Überweisungen zu tätigen?
- wann sind Entscheidungsträger im Urlaub oder auf Geschäftsreise?
- welche geschäftlichen Aktivitäten finden derzeit statt?

HORNETSECURITY

# Aber ich habe ein sicheres Passwort! Oder doch nicht?




- Quelle: Pressemitteilung HPI vom 19.12.2023

Most famous service (HIBP): https://haveibeenpwned.com
Hasso-Plattner-Institute (Foundation): https://sec.hpi.de/ilc/

HORNETSECURITY

# Statistiken Zur Cybersicherheit für 2024

- Im Jahr 2024 wird es weltweit **3,5 Millionen unbesetzte Stellen** im Bereich Cybersicherheit geben.
- Es wird prognostiziert, dass die gesamte globale Datenspeicherung bis 2025 **200 Zettabyte überschreiten** wird.
- Der Markt für Cybersicherheit wird jährlich um **15% wachsen**.

Wächst Ihr Budget auch?

HORNETSECURITY

Quelle: Top 10 Cybersecurity Predictions and Statistics For 2024 (cybersecurityventures.com)

# EINE FEHLENDE SICHERHEITSKULTUR FÜHRT ZU IMMENSEN SCHÄDEN

***„Ich werde sowieso nicht angegriffen."***
Maria (28) — HR Manager

***„Unsere IT kümmert sich bereits darum."***
Roland (41) — Controller

***„Ich habe wichtigere Dinge zu tun, als mich um die IT-Sicherheit zu kümmern."***
Gabi (54) — Head of Sales

**Die Arbeit von zu Hause aus wird sich weiter durchsetzen**

**95 % der Cybersicherheitsprobleme sind auf menschliches Versagen zurückzuführen**
[World Economic Forum: The Global Risks Report 2022]

**IT Security: Der Mensch ist Risikofaktor Nr. 1**

HORNETSECURITY

# DES HACKERS LIEBSTES TOOL...

E-Mail Kommunikation ist das größte Einfallstor für Cyberangriffe....

- leicht zu identifizieren
- keine Authentifizierung durch den Angreifer
- keine unternehmensspezifische Zugriffskontrollen
- am meisten genutzte Dienst für Unternehmen
- Mitarbeiter werden direkt kontaktiert
- Austausch sensibler Informationen
- personalisierbar und massenhafter Versand

**91%** aller Cyber-Attacken starten mit einer E-Mail

# Phishing ist größter Bedrohungsfaktor

HORNETSECURITY

# Shit happens!


ABO

WirtschaftsWoche

CYBER-ANGRIFF

## Wieso Unternehmen ihre IT-Sicherheit nicht in den Griff bekommen

von Sebastian Schug
20. April 2024

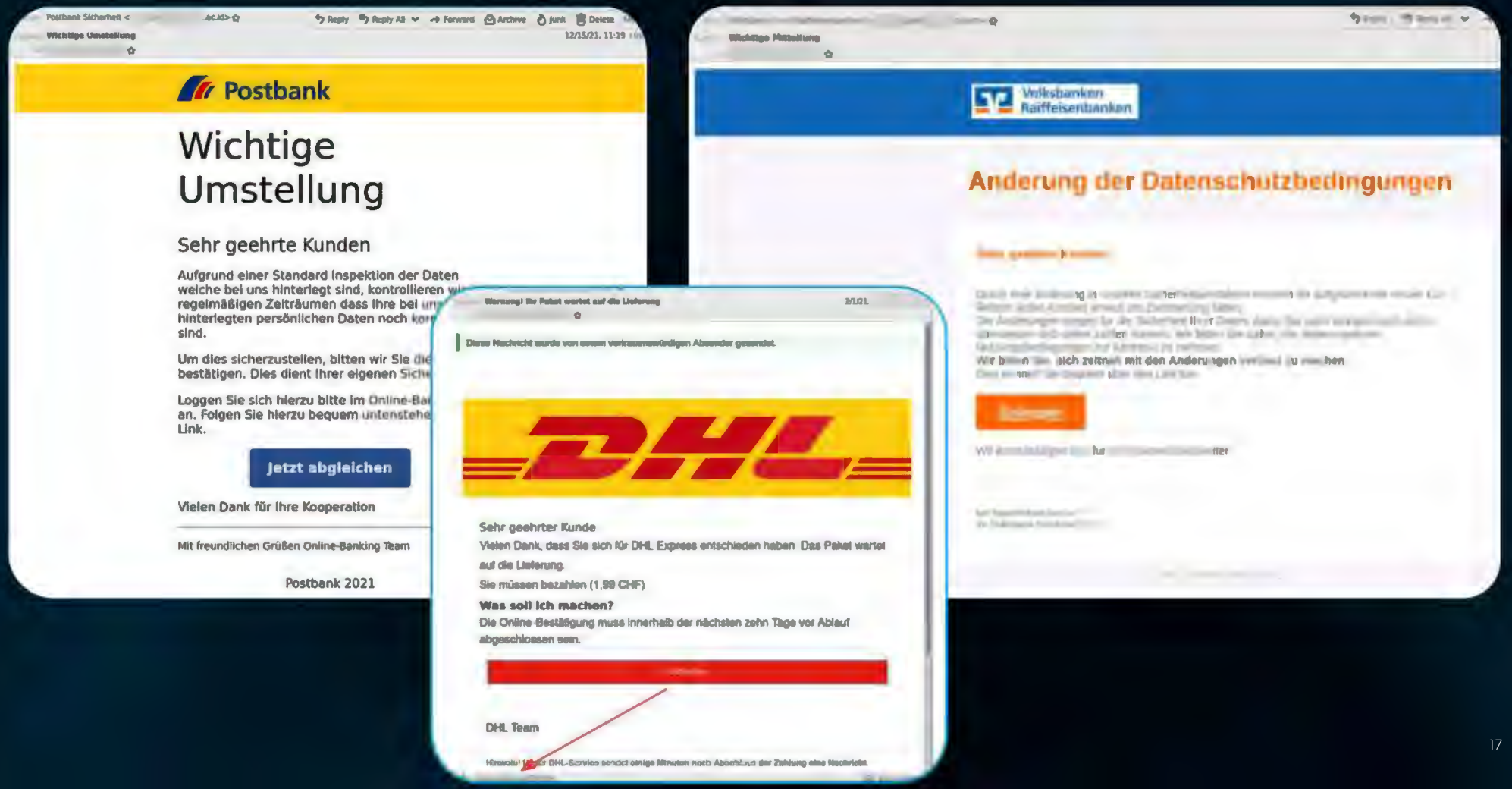


Netzwerkkabel stecken in einem Serverraum in München (Bayern) in einem Switch.
Bild: dpa

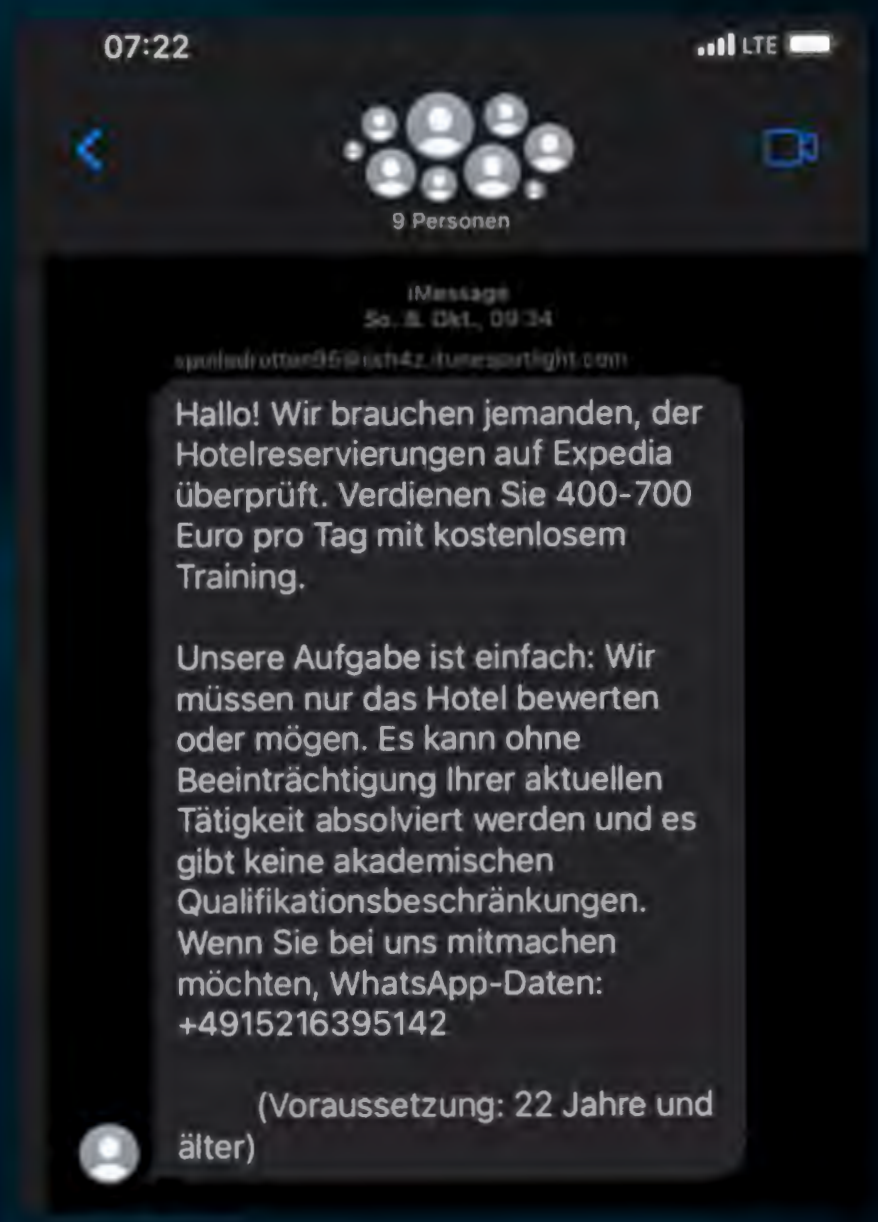
**Cyber-Angriffe auf Unternehmen sind ein wiederkehrendes Übel. Aber wieso eigentlich? Wie so oft in der IT, sitzt die Antwort vor dem Bildschirm.**

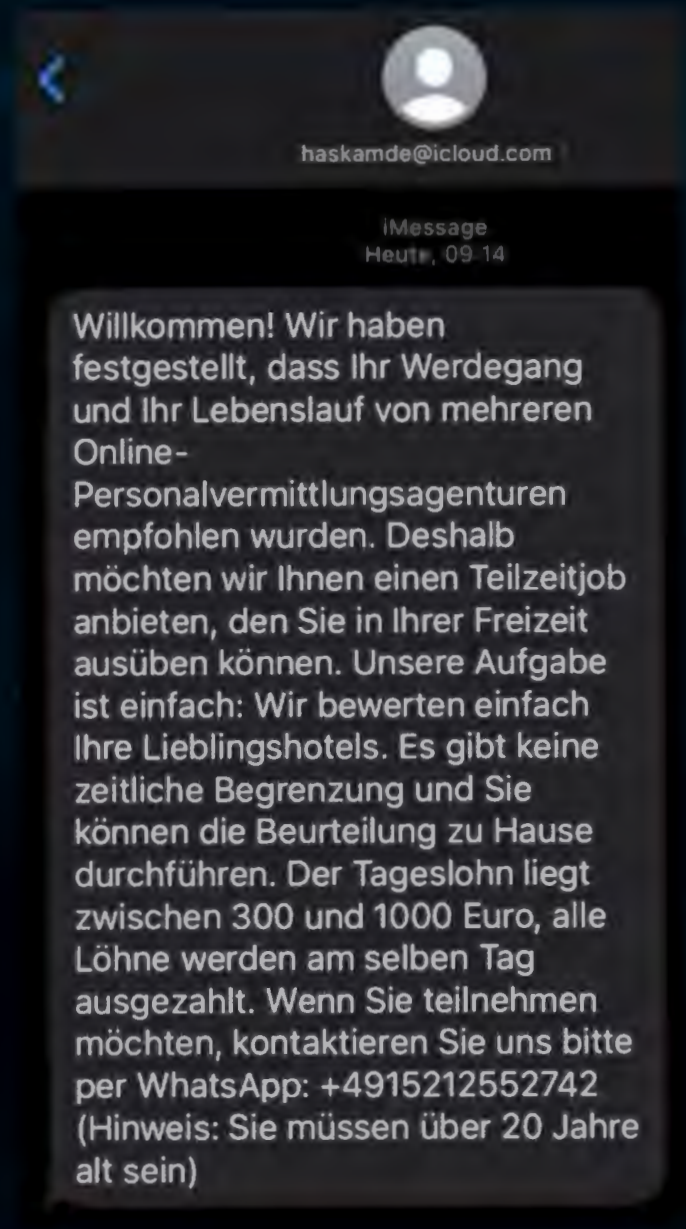
HORNETSECURITY

# BEISPIEL PHISHING MAIL



# SMISHING via WhatsApp oder SMS




HORNETSECURITY

# Phishing Attacken via QR Codes


Hornetsecurity erkennt QR Codes die in Bildern integriert sind.

```
qrs (master) ✗ du -h qr-mixed.png
.2M    qr-mixed.png
→ qrs (master) ✗ file qr-mixed.png
qr-mixed.png: PNG image data, 1500 x 843, 8-bit/color RGB, non-interlaced
→ qrs (master) ✗ ./qrs qr-mixed.png
Hurra! Task completed in 69.874459ms.

  QR Code ID ╪                                  Data
-------------*-------------------------------------------------------------------
           0 ╪ #hornetrocks
*------------*-------------------------------------------------------------------*
           1 ╪ https://www.hornetsecurity.com
*------------*-------------------------------------------------------------------*
           2 ╪ https://www.youtube.com/channel/UC7gf25rTAlVqv2acMQfCE0g/videos
*------------*-------------------------------------------------------------------*
           3 ╪ BEGIN:VCARD VERSION:3.0 N:Doe;John
             ╪ ORG: Example Inc  TITLE:Doctor
             ╪ EMAIL;TYPE=INTERNET:john.doe@example.com
             ╪ URL:https://en.wikipedia.org/wiki/John_Doe
             ╪ TEL;TYPE=CELL:9876543210 TEL:0123456789
             ╪ TEL;TYPE=FAX:0123498765 ADR:;; 123 Main
             ╪ Street;Anywhere;;12345;United States
             ╪ END:VCARD
-------------*-------------------------------------------------------------------
```


Cyberkriminelle senden Emails oder Bilder mit QR Codes die zu schadhaften Seiten oder Dokumenten führen.

In den QR Scan Ergebnissen werden unterschiedliche QR Codes analysiert (URLs, Texte und Kontakte). Dabei werden die Formate GIF, JPG, PNG und BMP unterstützt.

# Awareness in anderen Unternehmensbereichen

HORNETSECURITY


HORNETSECURITY

HORNETSECURITY

# VERHALTEN BEI IT-NOTFÄLLEN

**Ruhe bewahren & IT-Notfall melden**
**Lieber einmal mehr als einmal zu wenig anrufen!**

IT-Notfallrufnummer:

Wer meldet?

Welches IT-System ist betroffen?

Wie haben Sie mit dem IT-System gearbeitet?
Was haben Sie beobachtet?

Wann ist das Ereignis eingetreten?

Wo befindet sich das betroffene IT-System?
(Gebäude, Raum, Arbeitsplatz)

## Verhaltenshinweise

| Weitere Arbeit am IT-System einstellen | Beobachtungen dokumentieren | Maßnahmen nur nach Anweisung einleiten |
|---|---|---|

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik

www.bsi.bund.de

Allianz für Cyber-Sicherheit

www.allianz-fuer-cybersicherheit.de

klicksafe

www.klicksafe.de

# NEXT-GEN SECURITY AWARENESS SERVICE

HORNETSECURITY

SECURITY
AWARENESS
TRAINING

# 1 von 4

Unternehmen erleidet eine E-Mail-Sicherheitsverletzung

# 28,7 %

der Unternehmen schulen ihre Endbenutzer nicht darin, wie sie potenzielle Ransomware-Angriffe erkennen und melden können.

# 1,3 Mrd. €

Höhe der Geldbußen, die für Verstöße gegen die DSGVO allein in der ersten Hälfte des Jahres 2023 verhängt wurden, verglichen mit 800 Millionen Euro für das gesamte Jahr 2022.**

# 43 %

bestätigte Datenschutz-Verletzungen aufgrund von menschlichen Fehlern durch fehlgeleitete E-Mails*.

# 62 %

E-Mail-Sicherheits-verletzungen wurden durch kompromittierte Passwörter und Phishing-Angriffe verursacht.

# 15,2 %

der Unternehmen schützen ihre Backups nicht vor Ransomware.

Sources:

Hornetsecurity Research and Publications
* 2023 Data Breach Investigations Report,
** www.enforcementtracker.com

HORNETSECURITY

# VORAUSSETZUNGEN FÜR EINE NACHHALTIGE SICHERHEITSKULTUR

HORNETSECURITY

## MINDSET

**Motivation und offene Kommunikation**

- Verständnis für Bedrohungslage
- Eigenverantwortung betonen

**Kommunikationshilfen**
für alle Stakeholder

## SKILLSET

**Fähigkeiten und Wissen aneignen**

- Phishing-Simulation
- E-Learning
- Kurzvideos

**Awareness-Materialien**

## TOOLSET

**Aktiv ins Geschehen eingreifen**

- Live-Dashboard
- Sicherheitsmeldeketten

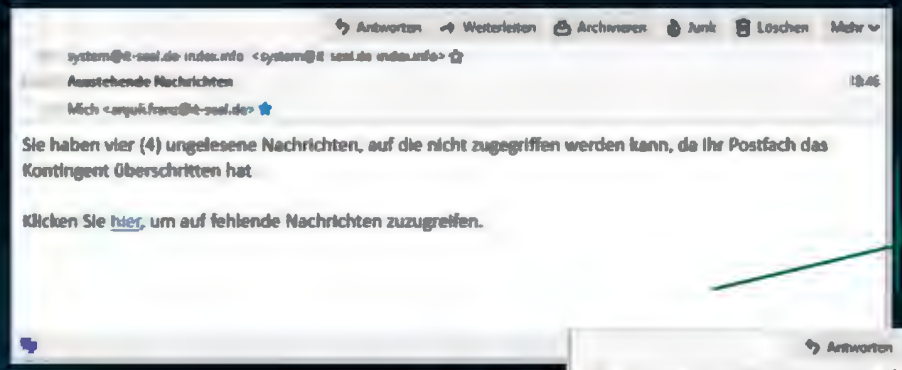
**Reporter-Button**
Outlook Add-In

# PATENTIERTE SPEAR-PHISHING-ENGINE

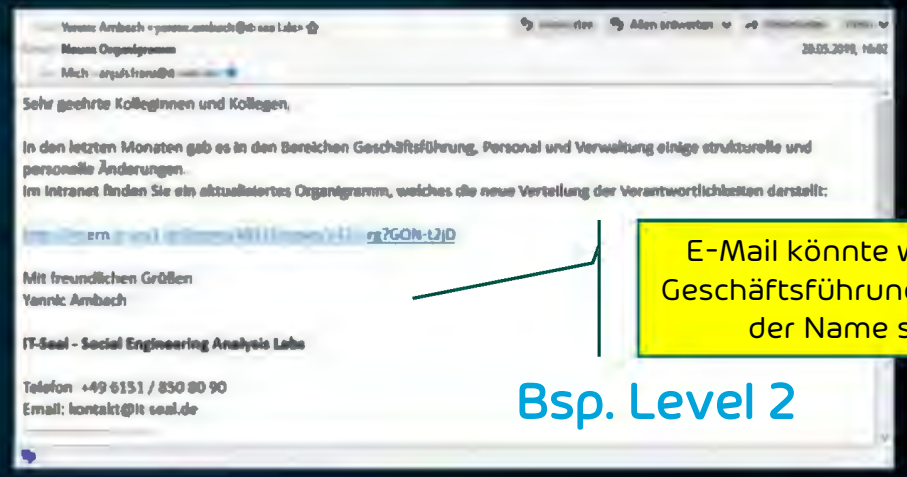
## VORGEHEN WIE EIN ECHTER ANGREIFER

HORNETSECURITY

Bsp. Level 1

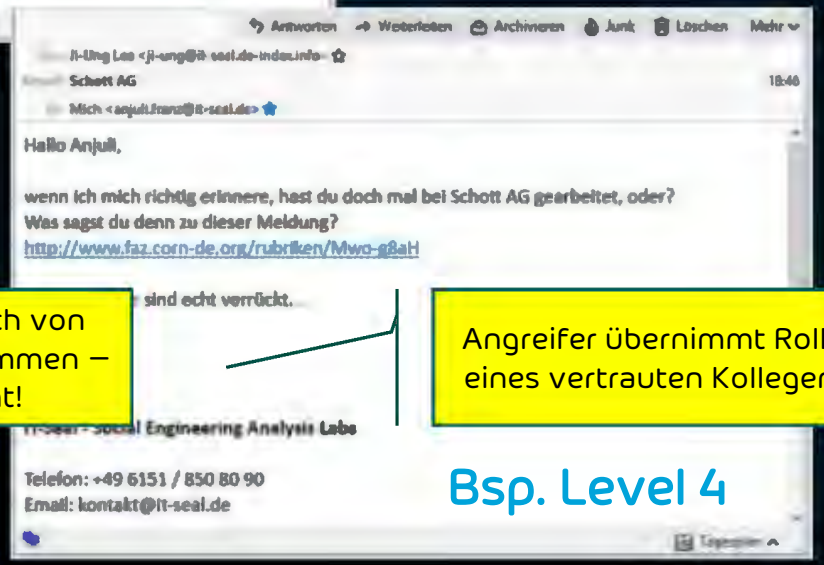



Autom. generierte System-E-Mail – könnte echt sein.




E-Mail könnte wirklich von Geschäftsführung stammen – der Name stimmt!

Bsp. Level 2




Angreifer übernimmt Rolle eines vertrauten Kollegen.

Bsp. Level 4

# Phishing Mails Beispiele

HORNETSECURITY

Ourobit

Sehr geehrte/r Tassilo Totzeck,

wir sind Ourobit - ein Unternehmen, das sich auf Highspeed-Internetausbau spezialisiert hat. Damit Sie und Ihre Kollegen mit schnelleren Internet noch bequemer im Homeoffice arbeiten können, ermöglichen wir zusammen mit Ihrem Arbeitgeber Highspeed-Internet für Sie zu Hause. Damit wir Ihnen die bestmögliche Internet-Lösung anbieten können, führen wir derzeit stichprobenartig Mitarbeiterumfragen durch, um zu erfahren, ob bei Ihnen und Ihren Kollegen Interesse an unserem **Highspeed-Internet-Kombipaket** besteht.

Unser Kombipaket umfasst den Ausbau Ihres Heimanschlusses und das Ihrer Kollegen für ein flüssigeres Arbeiten im Homeoffice.

Um sicherzustellen, dass Sie von unserem Angebot profitieren können, würden wir uns freuen, wenn Sie uns bei unserer Umfrage unterstützen. Die Umfrage wird nur wenige Minuten in Anspruch nehmen und wird uns helfen, Ihre Bedürfnisse besser zu verstehen.

**Zur Umfrage**

Vielen Dank im Voraus für Ihre Teilnahme an unserer Umfrage. Wir freuen uns darauf, Ihnen schon bald schnelleres Internet nach Hause zu bringen

Mit freundlichen Grüßen
Ihr Ourobit

Dietmar Ick
Leiter für Kundenzufriedenheit

Impressum Datenschutz Partner Nutzungsbedingungen

© Ourobit AG

Ihre Amazon.de-Bestellung "Canon PowerShot SX7..." wurde versandt!

Amazon <versandbestaetigung@amazon.de-index.info>

amazon.de

Versandbestätigung

Guten Tag

wir möchten Ihnen hiermit mitteilen, dass sich der letzte Artikel aus Ihrer Bestellung in Zustellung befindet. Alle weiteren Artikel aus dieser Bestellung wurden bereits versandt.

Ihre Sendung befindet sich nun auf dem Versandweg; eine Änderung durch Sie oder unseren Kundenservice ist nicht mehr möglich. Möchten Sie einen Artikel aus Ihrer Bestellung zurückgeben oder andere Bestellungen ansehen oder verändern, nutzen Sie bitte den Bereich Meine Bestellungen auf unserer Website Amazon.de.

Zustellung
08.04.2024

Tassilo Totzeck

Einzelheiten Ihrer Lieferung

- Canon PowerShot SX70 HS (20.3 MP, 65fach optischer Zoom, Dreh- und schwenkbares 7.5cm LCD, WLAN, 4K-Video) — EUR 485,99

| | |
|---|---|
| Zwischensumme | EUR 485,99 |
| Verpackung und Versand: | EUR 4,99 |
| Gratis Lieferung: | -EUR 4,99 |
| Zwischensumme ohne USt.: | EUR 393,65 |
| Umsatzsteuer: | EUR 92,34 |
| **Endbetrag inkl. USt.:** | **EUR 485,99** |
| Zahlung über Visa | EUR 485,99 |

Rücksendungen sind einfach. Besuchen Sie unser Online-Rücksendezentrum um

Wir freuen uns auf Ihren nächsten Besuch!
Amazon.de

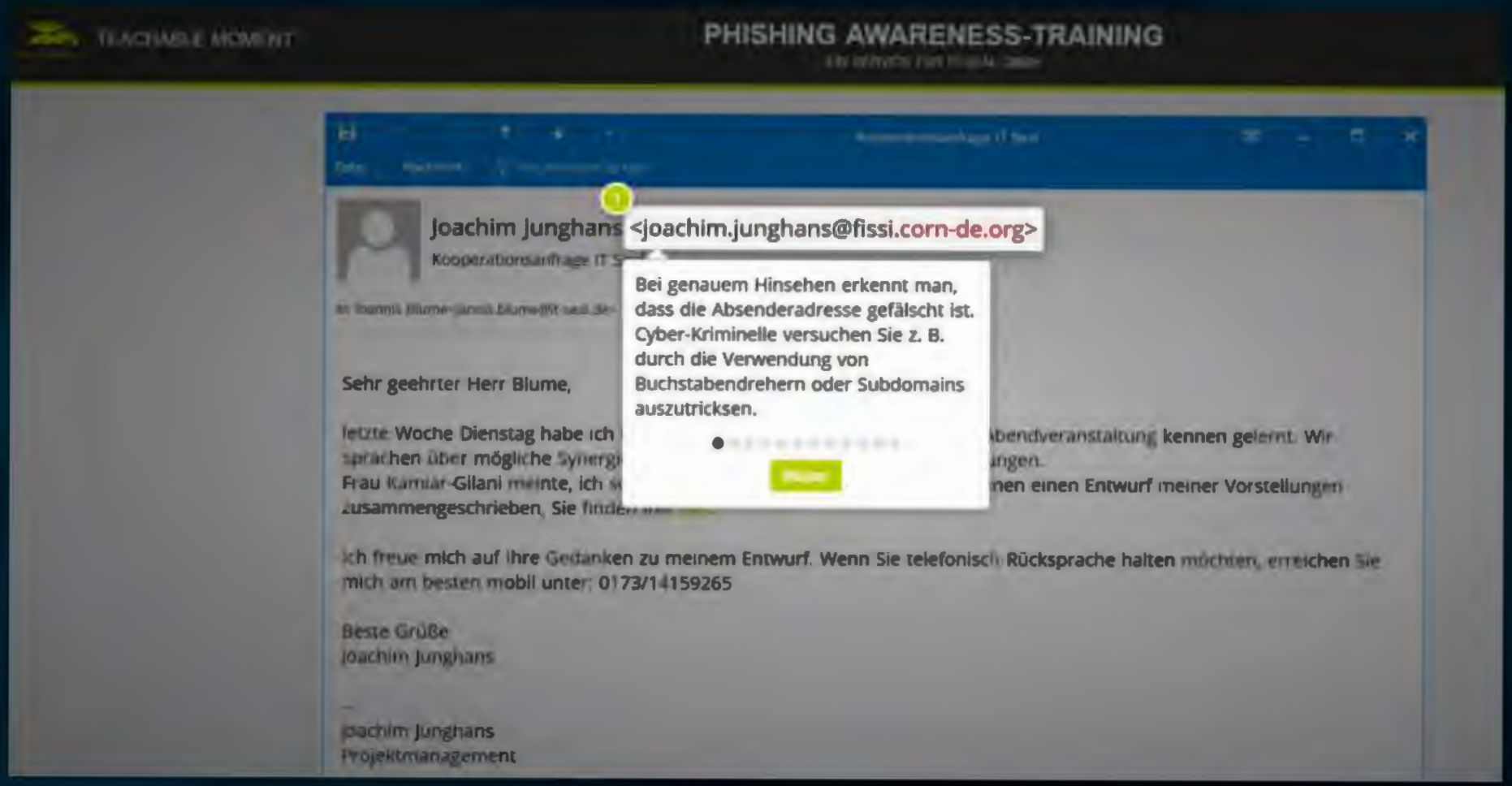
# PATENTIERTE SPEAR-PHISHING-ENGINE

Benutzer bei Klick auf Phishing-Mail aufklären: Most teachable moment

HORNETSECURITY

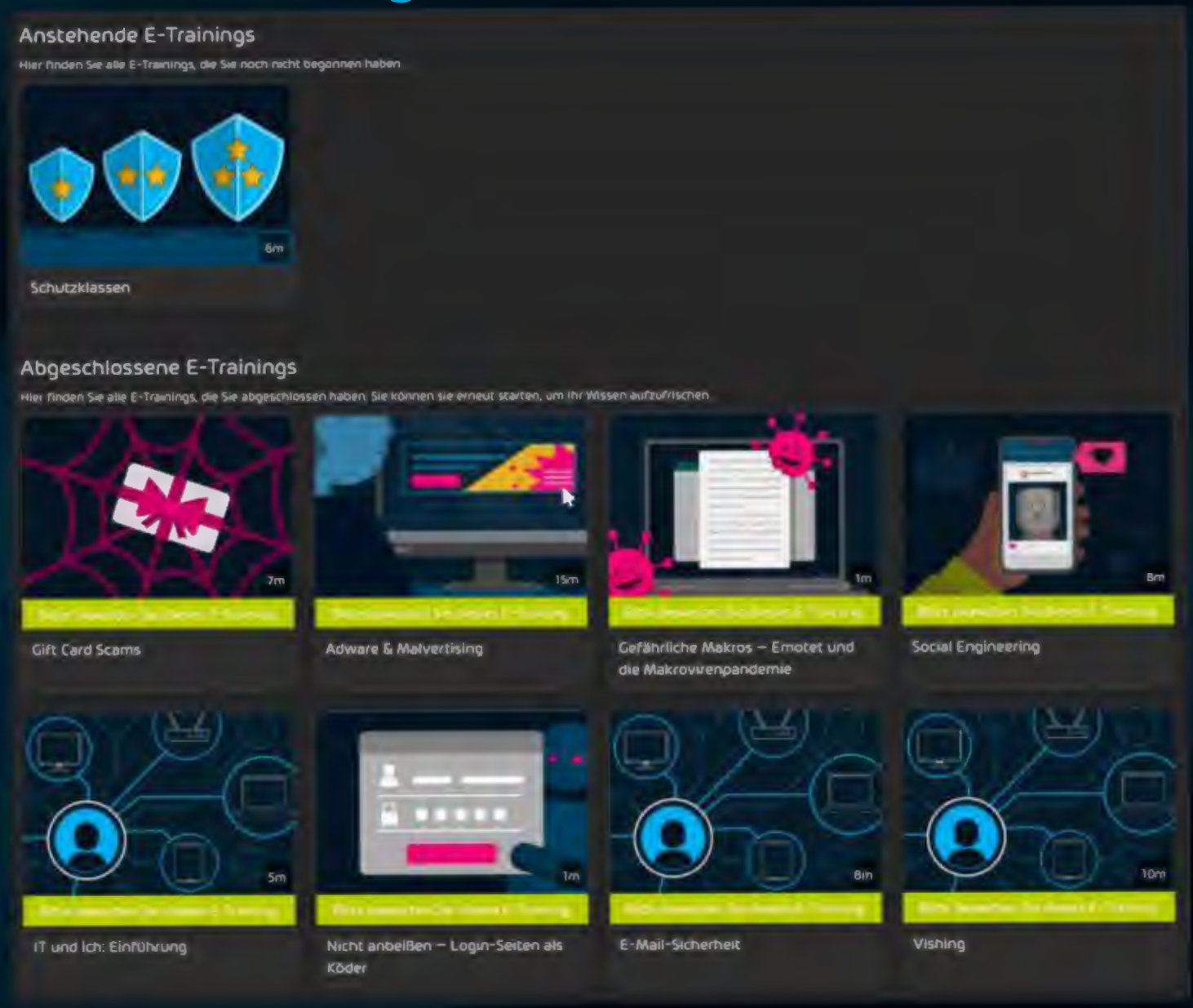
# PATENTIERTE SPEAR-PHISHING-ENGINE

Benutzer bei Klick auf Phishing-Mail aufklären: Most teachable moment




HORNETSECURITY

# Awareness Trainings Module




HORNETSECURITY

# Awareness / Phishing Simulator

HORNETSECURITY

# Machen!

- Cybersicherheit ist Chefsache
- Notfallplan erstellen
- Verhalten im Cybervorfall üben
- Updates & Patches immer aktuell halten
- Starke Passwörter, MFA
- Rollen- & Rechtemanagement
- Verschlüsselte Kommunikation
- Phase 1 Schwachstellenmanagement
- Phase 2 Pentesting
- Zeit und Geld in Sicherheit investieren

HORNETSECURITY

# 365 TOTAL PROTECTION

## NEXT-GEN MICROSOFT 365 SECURITY

HORNETSECURITY

| PLAN 1 | PLAN 2 | PLAN 3 | PLAN 4 |
|---|---|---|---|
| BUSINESS | ENTERPRISE | BACKUP | COMPLIANCE & AWARENESS |
| SPAM & MALWARE PROTECTION | ADVANCED THREAT PROTECTION | BACKUP & RECOVERY OF MAILBOXES, PLANNER & TEAMS | PERMISSION MANAGEMENT |
| EMAIL ENCRYPTION | EMAIL ARCHIVING | BACKUP & RECOVERY OF ONEDRIVE & SHAREPOINT | PERMISSION ALERTS |
| EMAIL SIGNATURES & DISCLAIMERS | EMAIL CONTINUITY | BACKUP & RECOVERY OF ENDPOINTS | PERMISSION AUDIT |

| PLAN 4 |
|---|
| PHISHING & ATTACK SIMULATION |
| SECURITY AWARENESS |
| ESI® REPORTING |

| PLAN 4 |
|---|
| COMMUNICATION PATTERN ANALYSIS |
| AI RECIPIENT VALIDATION |
| SENSITIVE DATA CHECK |

| PLAN 4 |
|---|
| DMARC REPORTING & MANAGEMENT |
| ENHANCED EMAIL REPUTATION & DELIVERY |
| EASY DNS MANAGEMENT & OPTIMISATION |

# NEUE WÖCHENTLICHE WEBINARE


Montags

11:00 Uhr

https://register.gotowebinar.com/rt/1465132659176518752?source=Ditpro


Donnerstags

11:00 Uhr

https://register.gotowebinar.com/rt/4668118882539976537?source=Ditpro


Donnerstags

11:00 Uhr

https://register.gotowebinar.com/rt/8193558884850603872?source=Ditpro

HORNETSECURITY

# Titeltext



HORNETSECURITY

# THANK YOU!

HORNETSECURITY