HORNETSECURITY

NEXT-GEN SECURITY AWARENESS TRAINING

STÄRKEN SIE IHRE MENSCHLICHE FIREWALL.
FÜR EINE NACHHALTIGE SICHERHEITSKULTUR.

HORNETSECURITY

ERFOLG IN ZAHLEN

HORNETSECURITY

>400
Mitarbeiter

3 Rechenzentren
In Deutschland

>50.000
Kunden

12
Büros

Security Lab

15
Services

CLOUD SECURITY SERVICES FOR MICROSOFT 365

PRODUCT SUITE FOR 365	365 TOTAL PROTECTION BUSINESS (PLAN 1)	365 TOTAL PROTECTION ENTERPRISE (PLAN 2)	365 TOTAL PROTECTION ENTERPRISE BACKUP (PLAN 3)	365 TOTAL PROTECTION COMPLIANCE & AWARENESS (PLAN 4)
BACKUP FOR 365	365 TOTAL BACKUP			
PERMISSION MANAGER FOR 365	365 PERMISSION MANAGER			
SECURITY AWARENESS	SECURITY AWARENESS SERVICE			

SECURITY SERVICES

EMAIL SECURITY AND ENCRYPTION	ADVANCED THREAT PROTECTION	SPAM & MALWARE PROTECTION	EMAIL ENCRYPTION
EMAIL COMPLIANCE AND PRODUCTIVITY	CONTINUITY SERVICE	SIGNATURE & DISCLAIMER	ARCHIVING
WEB SECURITY	WEB FILTER		
HOSTED MAILBOX	HORNET.EMAIL		
BACKUP AND RECOVERY	VM BACKUP		

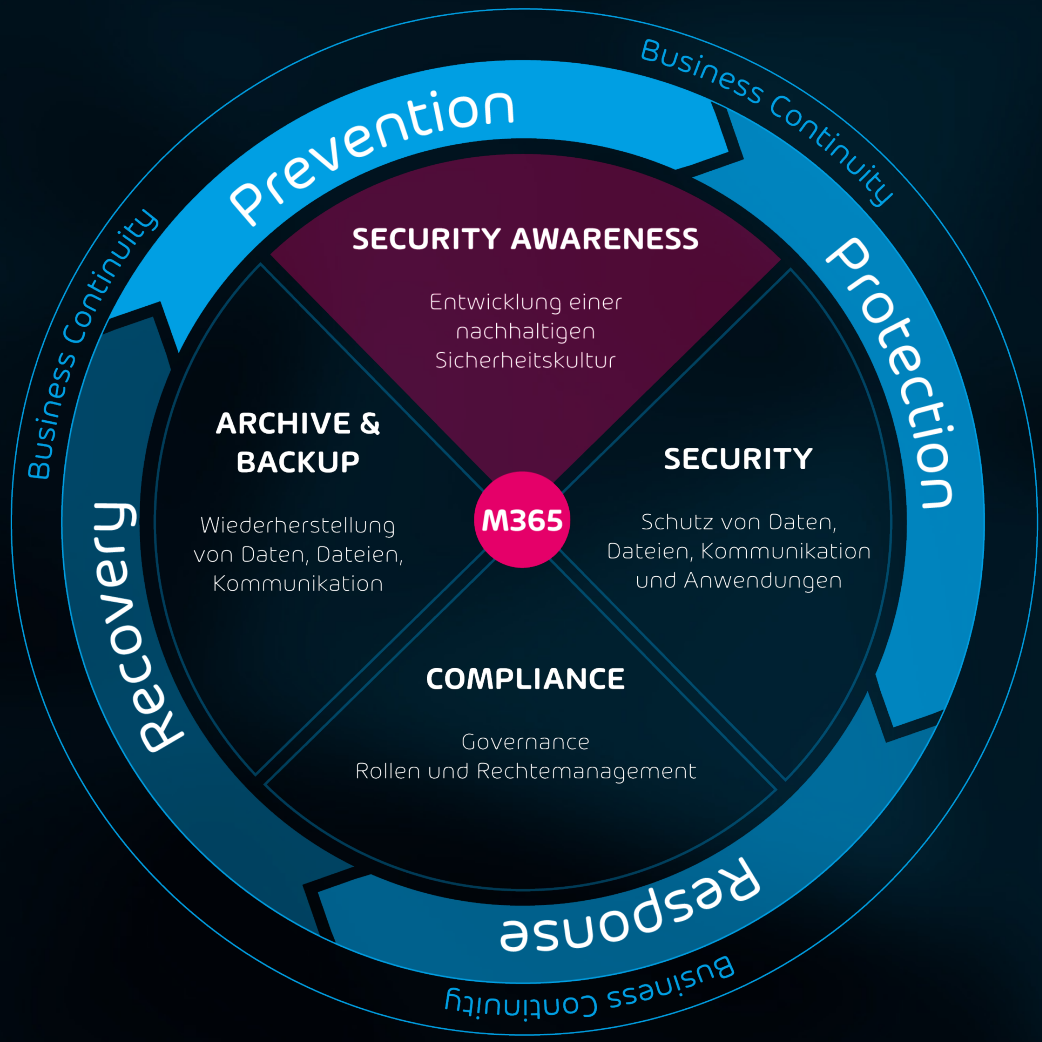
HORNETSECURITY

HORNETSECURITY

PRODUKT-ÜBERSICHT – DAS IST NEU!

HORNETSECURITY

SECURITY AWARENESS TRAINING



EINE FEHLENDE SICHERHEITSKULTUR FÜHRT ZU IMMENSEN SCHÄDEN

HORNETSECURITY

„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% aller Cybersicherheitsvorfälle sind auf menschliches Fehlverhalten zurückzuführen.

Quelle: World Economic Forum - The Global Risks Report 2022]

IT-Security: Der Mensch ist Risikofaktor Nr. 1

HORNETSECURITY

Wuppertal total

Cyberangriff - auch WZ und Wuppertaler Rundschau betroffen

Wie zahlreiche Medien am gestrigen Samstag, dem 17. Juni, berichtet haben, ist die Rheinische Post Mediengruppe Opfer eines Cyberangriffs...

vor 2 Tagen

Heise

Cyber-Angriff: IT der Deutsche Leasing seit Samstag offline

Bei Deutsche Leasing, einer großen Leasinggesellschaft zahlreicher Sparkassen, kam es am Samstag zu einem Cyber-Angriff.

vor 2 Wochen

Handelsblatt

AOK meldet Sicherheitslücke: 19 Millionen Versicherte betroffen

Die Krankenkasse AOK meldet einen Vorfall, durch den Unbefugte womöglich auf persönliche Daten von Versicherten zugreifen könnten.

vor 2 Wochen

Heise

Gesundheit Nord bestätigt Cyber-Angriff und Datenabfluss

Die Bremer Kliniken im "Gesundheit Nord"-Verband sind Opfer eines Cyber-Angriffs geworden, bestätigt der Verband jetzt.

vor 3 Wochen

Radio Zwickau

Nach Cyberangriff – Relaunch der TU Freiberg-Website

Nach dem Cyberangriff auf die Website der TU Bergakademie Freiberg wurde nun ein neuer Webauftritt aktiviert. Unter tu-freiberg.de wurde die...

vor 1 Stunde

Heise

Rheinische Post Mediengruppe: Noch immer Notbetrieb nach Cyber-Angriff

Die Webseiten der Medien der Rheinischen Post Mediengruppe sind immer noch lediglich eingeschränkt nutzbar. Auch die gedruckten Zeitungen...

vor 21 Stunden

Radio Chemnitz

Nach Cyberangriff – Relaunch der TU Freiberg-Website

Nach dem Cyberangriff auf die Website der TU Bergakademie Freiberg wurde nun ein neuer Webauftritt aktiviert. Unter tu-freiberg.de wurde die...

vor 1 Stunde

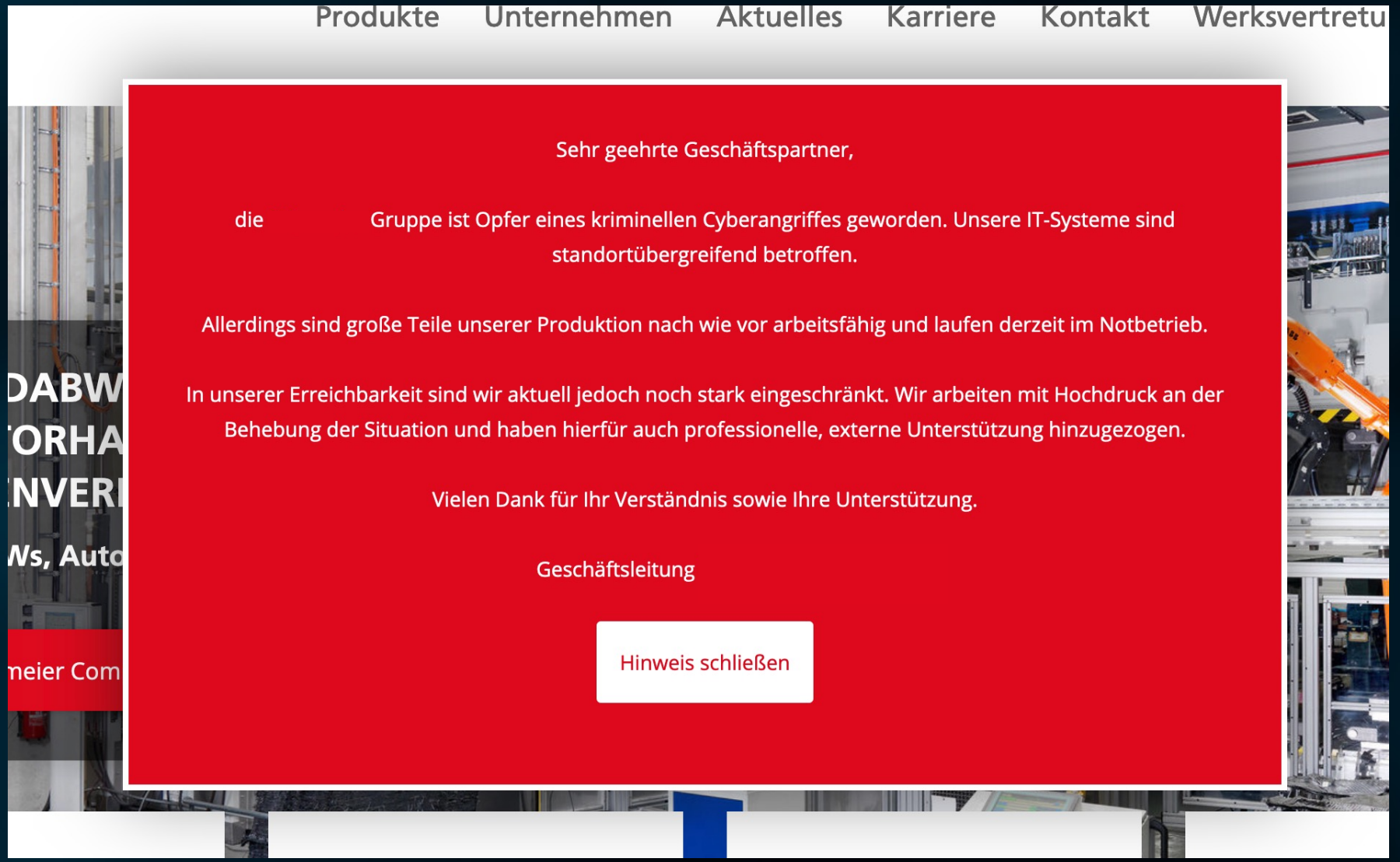
NDR

Medizinischer Dienst Niedersachsen nach Cyberangriff weiter offline

Der Medizinische Dienst Niedersachsen (MDN) ist nach einem Hackerangriff weiter nicht erreichbar. Der Gutachterdienst hat die Einstufungen...

vor 4 Tagen

HORNETSECURITY



Die Gruppe wurde Ziel eines organisierten Cyber-Angriffs. Die IT-Infrastruktur ist beeinträchtigt. Zum Schutz unserer Kunden, Mitarbeiter und Partner wurden unverzüglich die notwendigen Schritte unternommen, um dem Angriff mit gezielten Maßnahmen entgegen zu wirken.

Unser Team arbeitet gemeinsam mit externen Cyber-Security-Spezialisten mit Hochdruck daran, die Gefährdung zu beseitigen und den Normalbetrieb wiederherzustellen. Die zuständigen Ermittlungsbehörden sind eingeschaltet.

Group was target of an organized cyberattack. The IT infrastructure is affected. To protect our customers, employees and partners, the necessary steps were taken immediately to counter the attack with targeted measures.

Our team is working at full speed with external cybersecurity specialists and data forensics experts to eliminate the threat and restore normal operations. The relevant investigative authorities have been called in.

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
- Passwort-Manager

Reporter-Button
Outlook Add-In

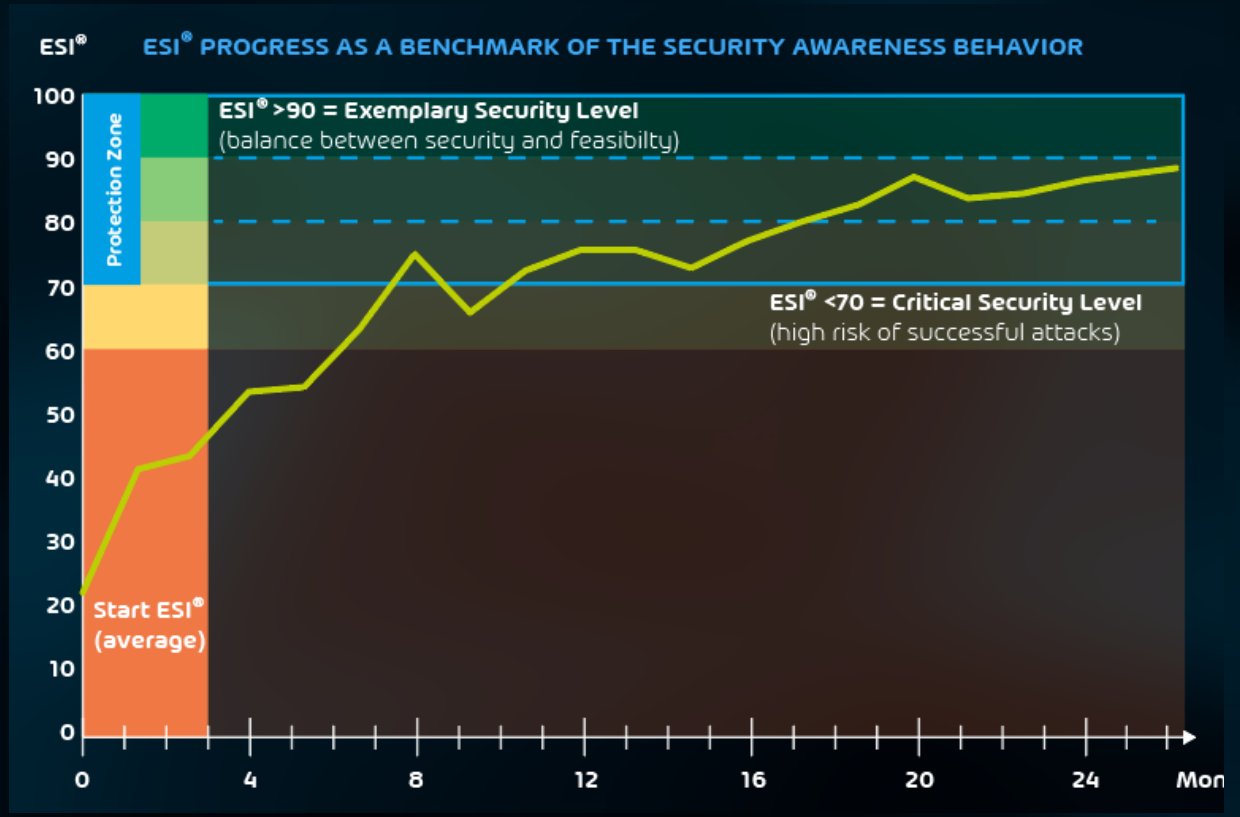
ENTSCHEIDENDE FAKTOREN FÜR EIN ERFOLGREICHES AWARENESS TRAINING

- Entscheidende Faktoren:
  - Messbar: für Ihren garantierten Erfolg
  - Effizient: Individuell und bedarfsgerecht
  - Realitätsnah: Vorgehen wie ein echter Angreifer
  - Wirksam: Selbstbestimmtes Trainieren & Lernen mit Fun Faktor

HORNETSECURITY

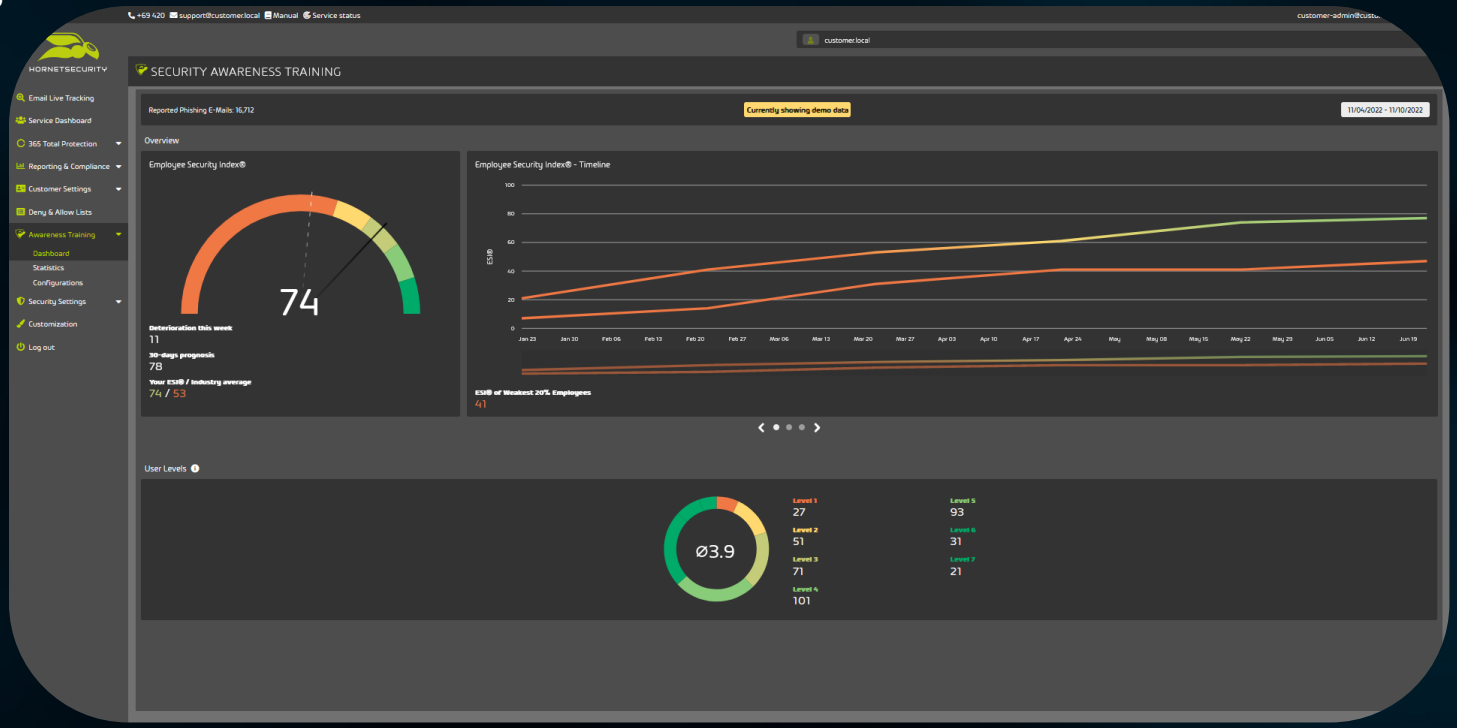
ESI® - EMPLOYEE SECURITY INDEX

- ESI® - Ein wissenschaftlich fundiertes und **patentiertes** Verfahren, um das Sicherheitsverhalten der Mitarbeiter messbar zu machen.
- Der ESI® Awareness-Benchmark ermöglicht eine **standardisierte, transparente Messung** und Steuerung des Sicherheitsverhaltens auf Unternehmens-, Gruppen- und User-Ebene.



AWARENESS DASHBOARD IM CONTROL PANEL

- Entwicklung des Security Awareness Trainings im Blick behalten
- ESI®-Reporting inkl. Historie und Forecast und Training KPIs
- Konfigurieren und passen Sie das Awareness Training an die Bedürfnisse Ihres Unternehmens an



HORNETSECURITY

ENTSCHEIDENDE FAKTOREN FÜR EIN ERFOLGREICHES AWARENESS TRAINING

- Entscheidende Faktoren:
  - Messbar: für Ihren garantierten Erfolg
  - **Effizient: Individuell und bedarfsgerecht**
  - Realitätsnah: Vorgehen wie ein echter Angreifer
  - Wirksam: Selbstbestimmtes Trainieren & Lernen mit Fun Faktor

HORNETSECURITY

AWARENESS ENGINE

SO VIEL TRAINING WIE NÖTIG, ABER SO WENIG WIE MÖGLICH

HORNETSECURITY

Bedarfsgerechtes Training für Mitarbeiter und Gruppen (z. B. Abteilungen). Jede Gruppe/jeder Mitarbeiter erhält hierbei das genau zu ihm passende Training. So wird **für jeden Mitarbeiter wertvolle Arbeitszeit und damit Kosten gespart**.

Als Training-Administrator brauchen Sie sich nicht mit der konkreten Steuerung und Umsetzung der Trainings beschäftigen. Die Awareness Engine **setzt Best Practices direkt um** und **spart die Ressourcen** Ihres IT-Security Teams.

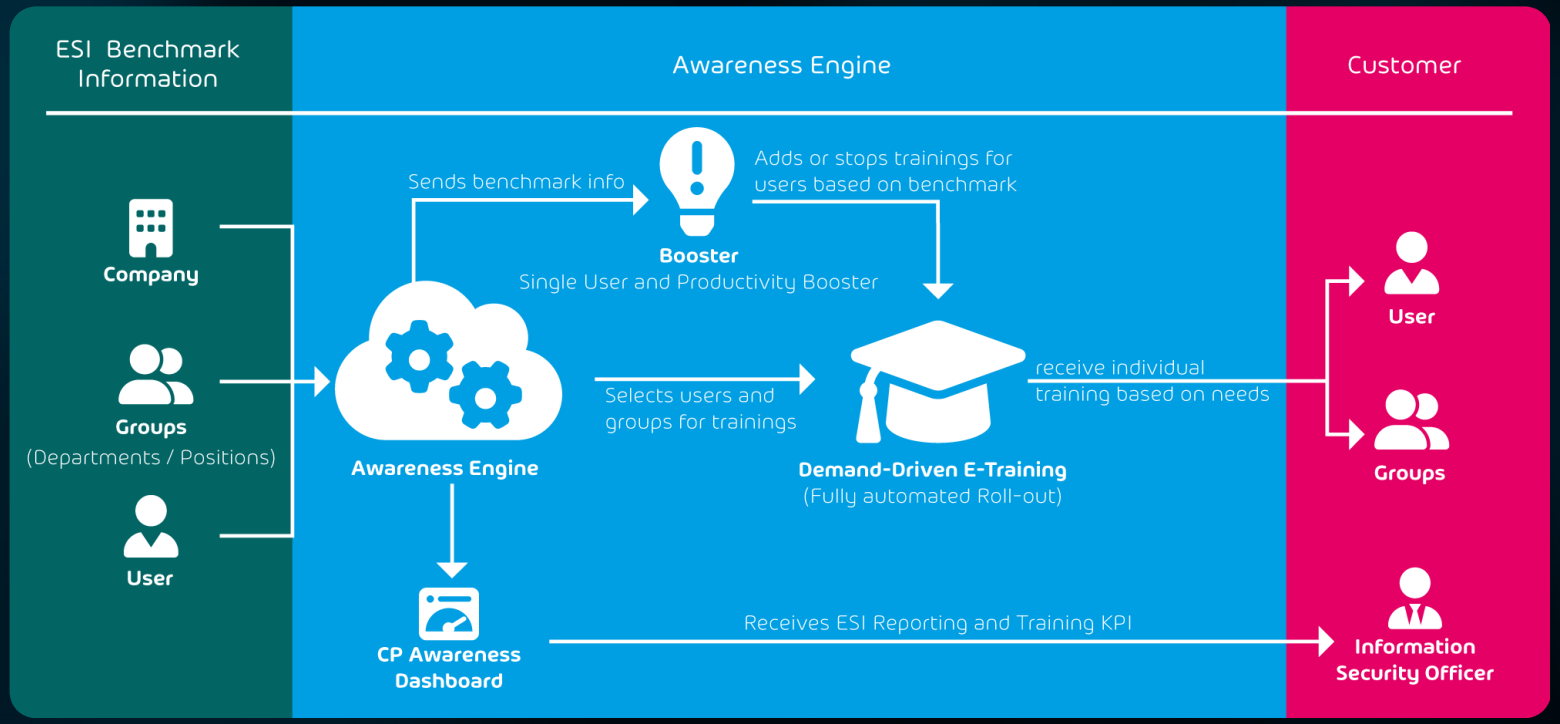
Die Awareness Engine identifiziert **Nutzer mit besonderem Lernbedarf**, die anschließend intensiver trainiert werden. Damit wird sichergestellt, dass Mitarbeiter mit zusätzlichem Lernbedarf nicht zu kurz kommen und weiterhin intensiv geschult werden.

AWARENESS ENGINE

SO VIEL TRAINING WIE NÖTIG, ABER SO WENIG WIE MÖGLICH

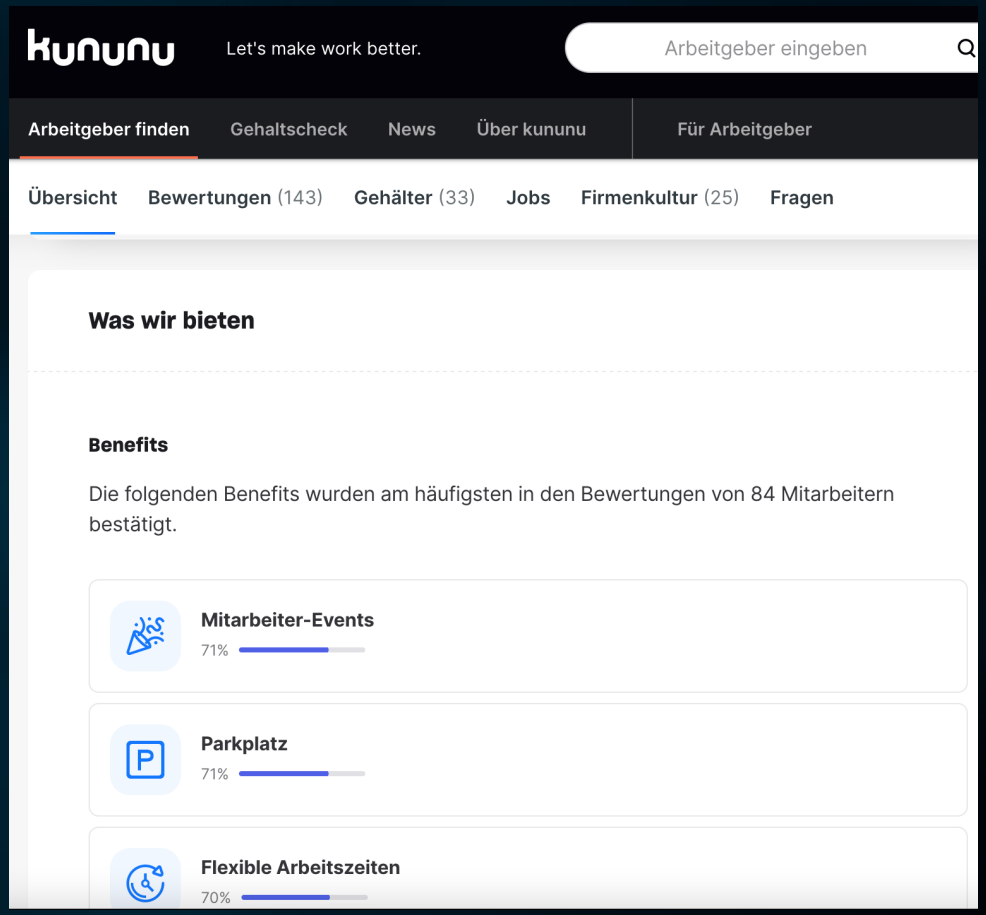
Einzigartig am Markt: Die Awareness Engine bietet kontinuierliches Awareness-Training im Autopiloten: bedarfsgerecht und ESI®-kennzahlenbasiert.

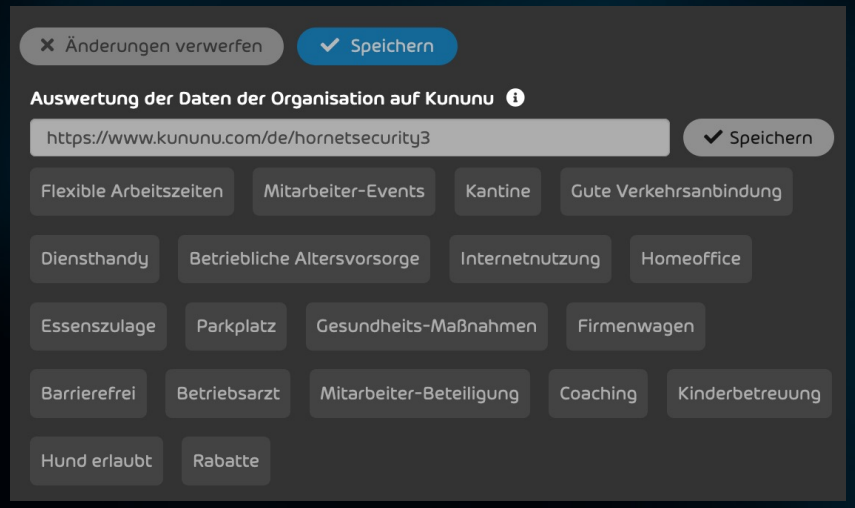
ABLAUF DES E-TRAININGS



INDIVIDUALISIERUNG

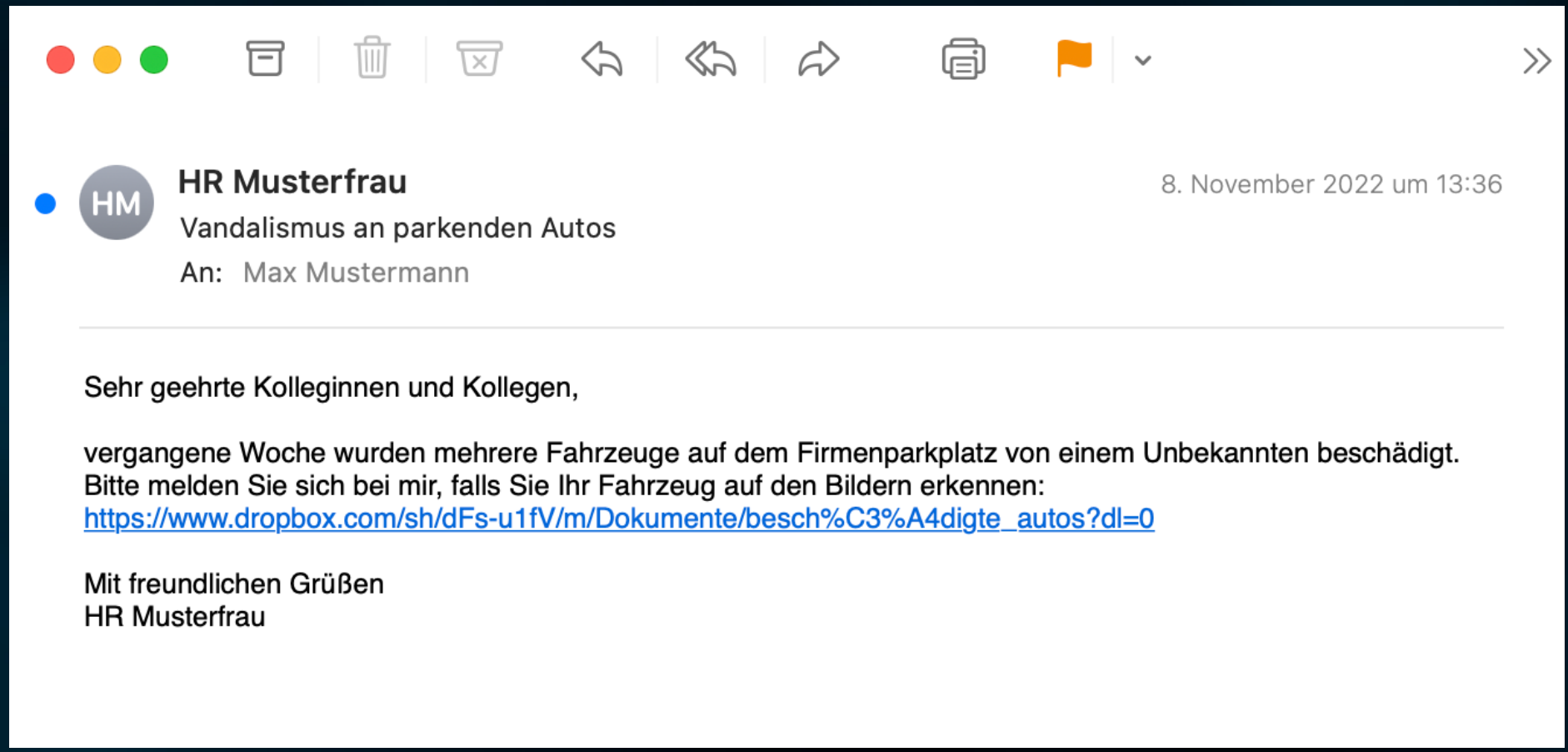
HORNETSECURITY





INDIVIDUALISIERUNG

HORNETSECURITY



HM

HR Musterfrau

8. November 2022 um 13:36

Vandalismus an parkenden Autos

An: Max Mustermann

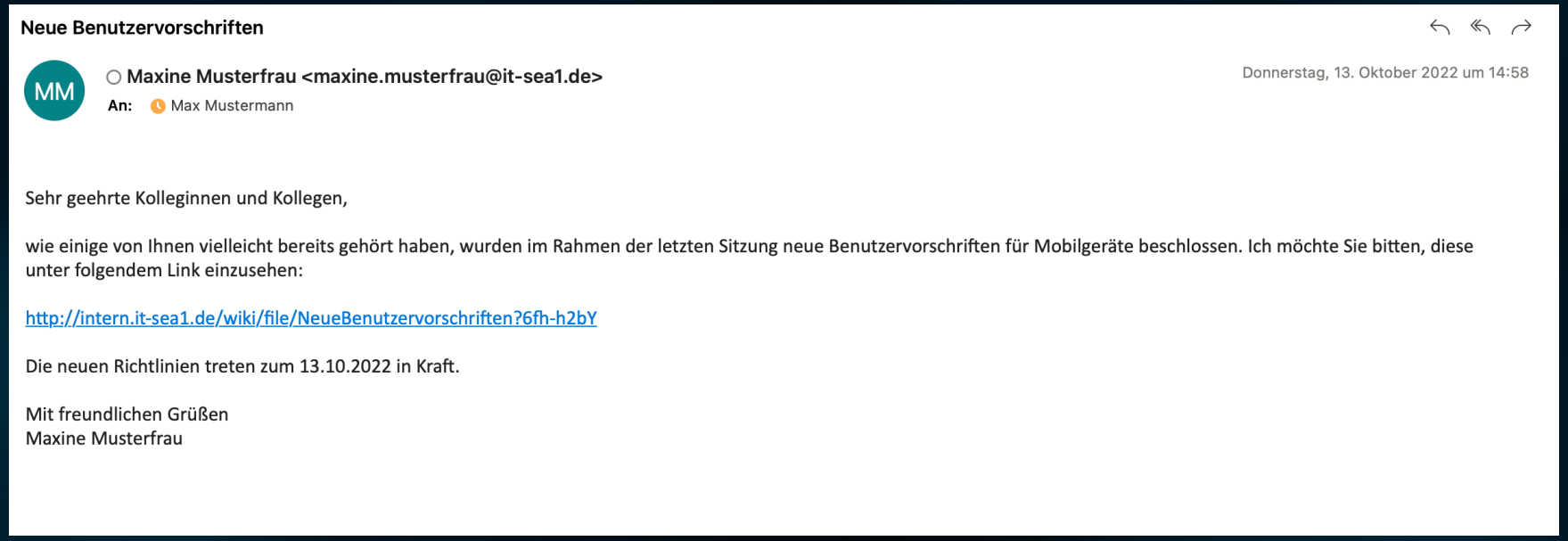
Sehr geehrte Kolleginnen und Kollegen,

vergangene Woche wurden mehrere Fahrzeuge auf dem Firmenparkplatz von einem Unbekannten beschädigt.
Bitte melden Sie sich bei mir, falls Sie Ihr Fahrzeug auf den Bildern erkennen:
https://www.dropbox.com/sh/dFs-u1fV/m/Dokumente/besch%C3%A4digte_autos?dl=0

Mit freundlichen Grüßen
HR Musterfrau

INDIVIDUALISIERUNG

HORNETSECURITY



Neue Benutzervorschriften

MM

Maxine Musterfrau <maxine.musterfrau@it-sea1.de>

An: Max Mustermann

Donnerstag, 13. Oktober 2022 um 14:58

Sehr geehrte Kolleginnen und Kollegen,

wie einige von Ihnen vielleicht bereits gehört haben, wurden im Rahmen der letzten Sitzung neue Benutzervorschriften für Mobilgeräte beschlossen. Ich möchte Sie bitten, diese unter folgendem Link einzusehen:

http://intern.it-sea1.de/wiki/file/NeueBenutzervorschriften?6fh-h2bY

Die neuen Richtlinien treten zum 13.10.2022 in Kraft.

Mit freundlichen Grüßen
Maxine Musterfrau

ENTSCHEIDENDE FAKTOREN FÜR EIN ERFOLGREICHES AWARENESS TRAINING

- Entscheidende Faktoren:
  - Messbar: für Ihren garantierten Erfolg
  - Effizient: Individuell und bedarfsgerecht
  - **Realitätsnah: Vorgehen wie ein echter Angreifer**
  - Wirksam: Selbstbestimmtes Trainieren & Lernen mit Fun Faktor

HORNETSECURITY

PATENTIERTE SPEAR-PHISHING-ENGINE

VORGEHEN WIE EIN ECHTER ANGREIFER

HORNETSECURITY

Die patentierte Spear-Phishing-Engine nutzt individuell zugeschnittene Spear-Phishing-Angriffe unterschiedlicher Schwierigkeits-Level.

Diese orientieren sich am Aufwand, die ein Angreifer zur Vorbereitung der Phishing-Mails benötigt: je mehr Zeit ein Angreifer in die Vorbereitung investiert, desto ausgeklügelter der Angriff und höher die Wahrscheinlichkeit, dass man auf eine Phishing-Mail reinfällt.

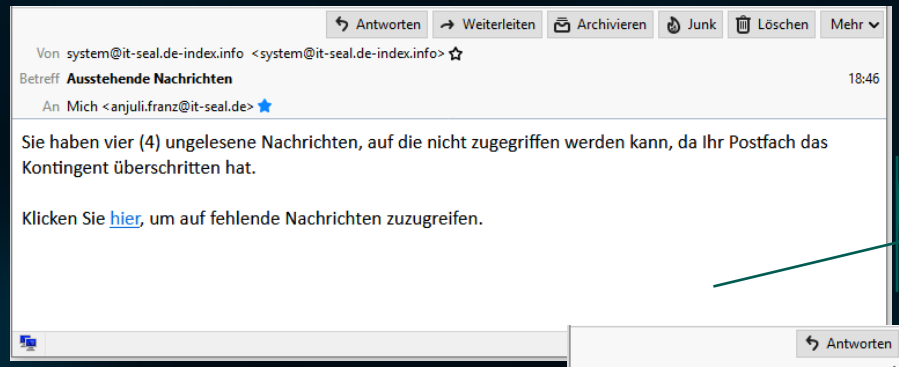
Die Erstellung und Versendung von Phishing-E-Mails wird von der Spear Phishing Engine zu individuellen Zeitpunkten vollautomatisch gesteuert.

PATENTIERTE SPEAR-PHISHING-ENGINE

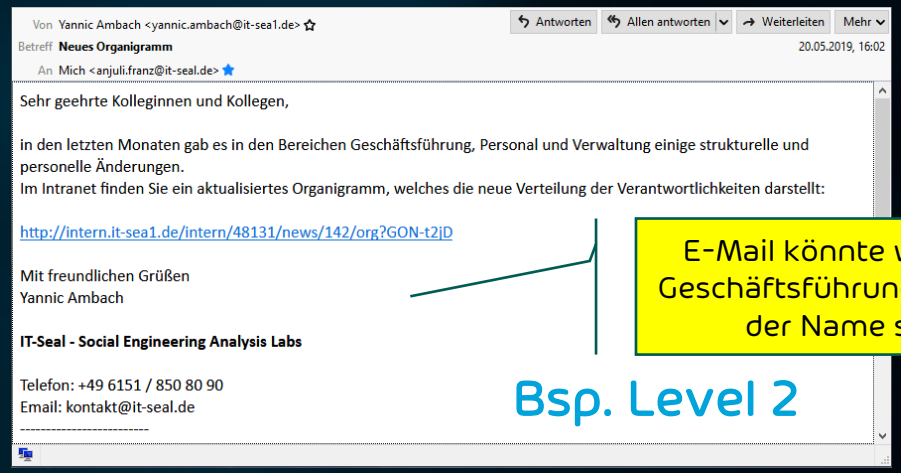
VORGEHEN WIE EIN ECHTER ANGREIFER

HORNETSECURITY

Bsp. Level 1

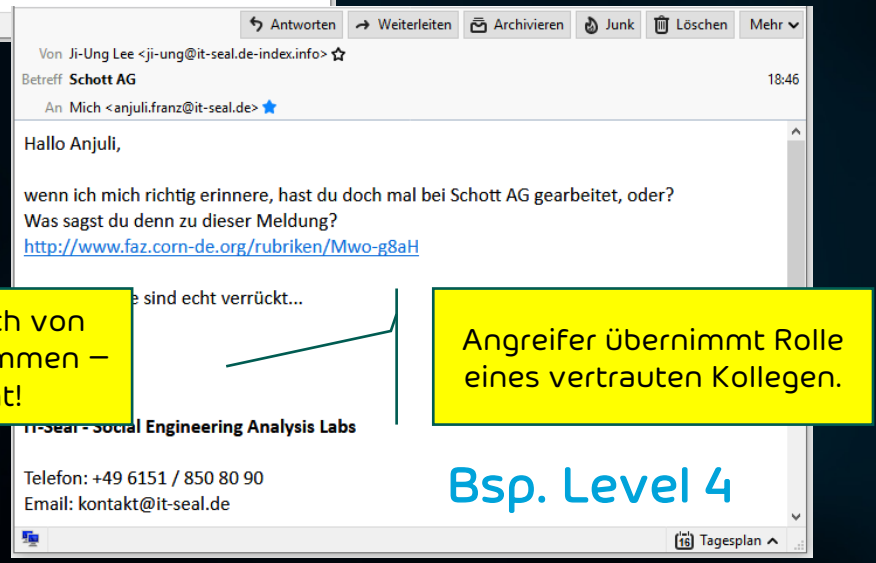


Autom. generierte System-E-Mail – könnte echt sein.



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

Bsp. Level 2



Angreifer übernimmt Rolle eines vertrauten Kollegen.

Bsp. Level 4

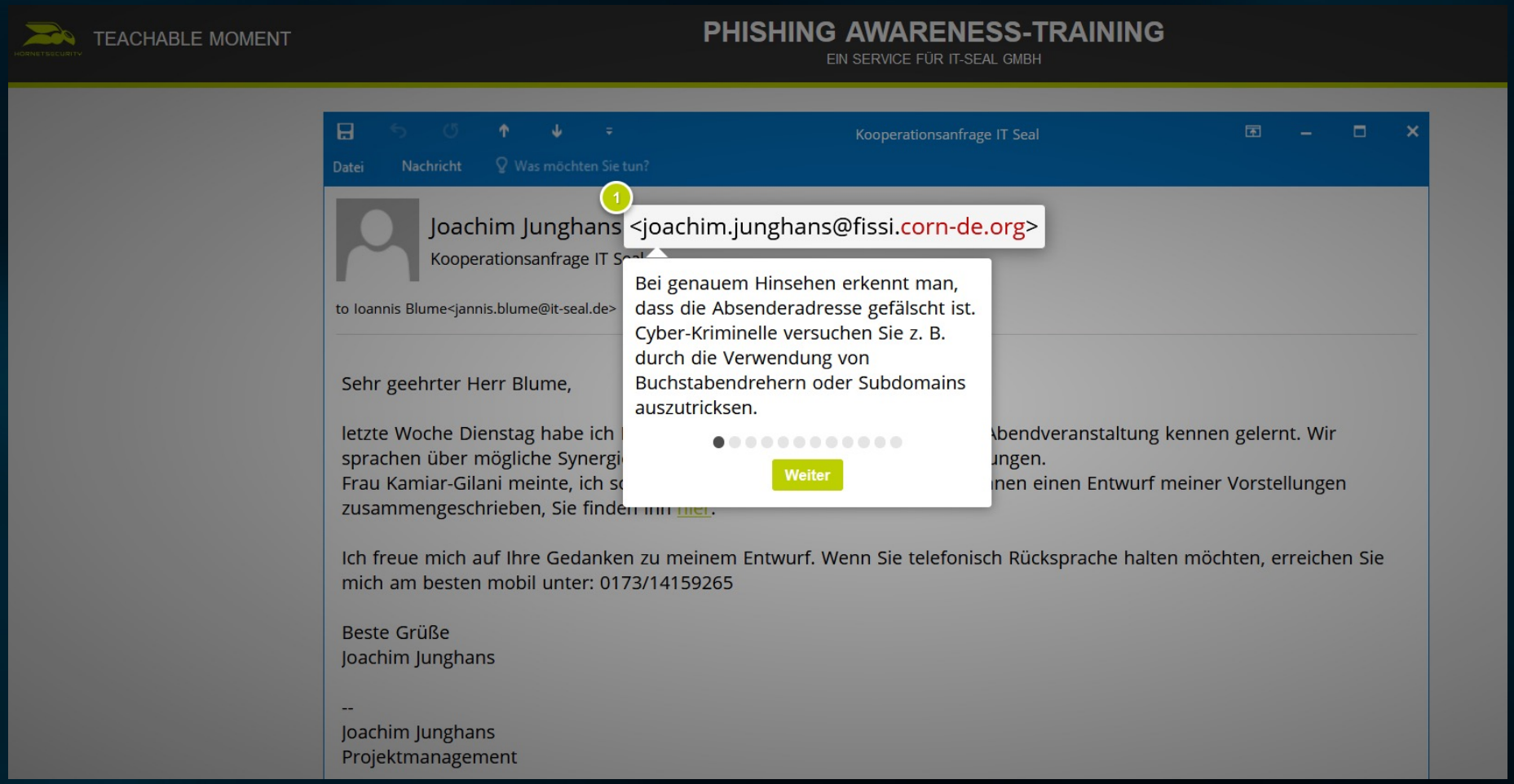
PATENTIERTE SPEAR-PHISHING-ENGINE

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

PATENTIERTE SPEAR-PHISHING-ENGINE

VORGEHEN WIE EIN ECHTER ANGREIFER

Die patentierte Spear-Phishing-Engine simuliert sogar ausgeklügelte Phishing-Angriffe, die einen realistisch-erscheinenden Antwortverlauf enthalten, wie es zum Beispiel der Fall sein könnte, wenn ein Geschäftspartner oder Kollege gehackt wurde.

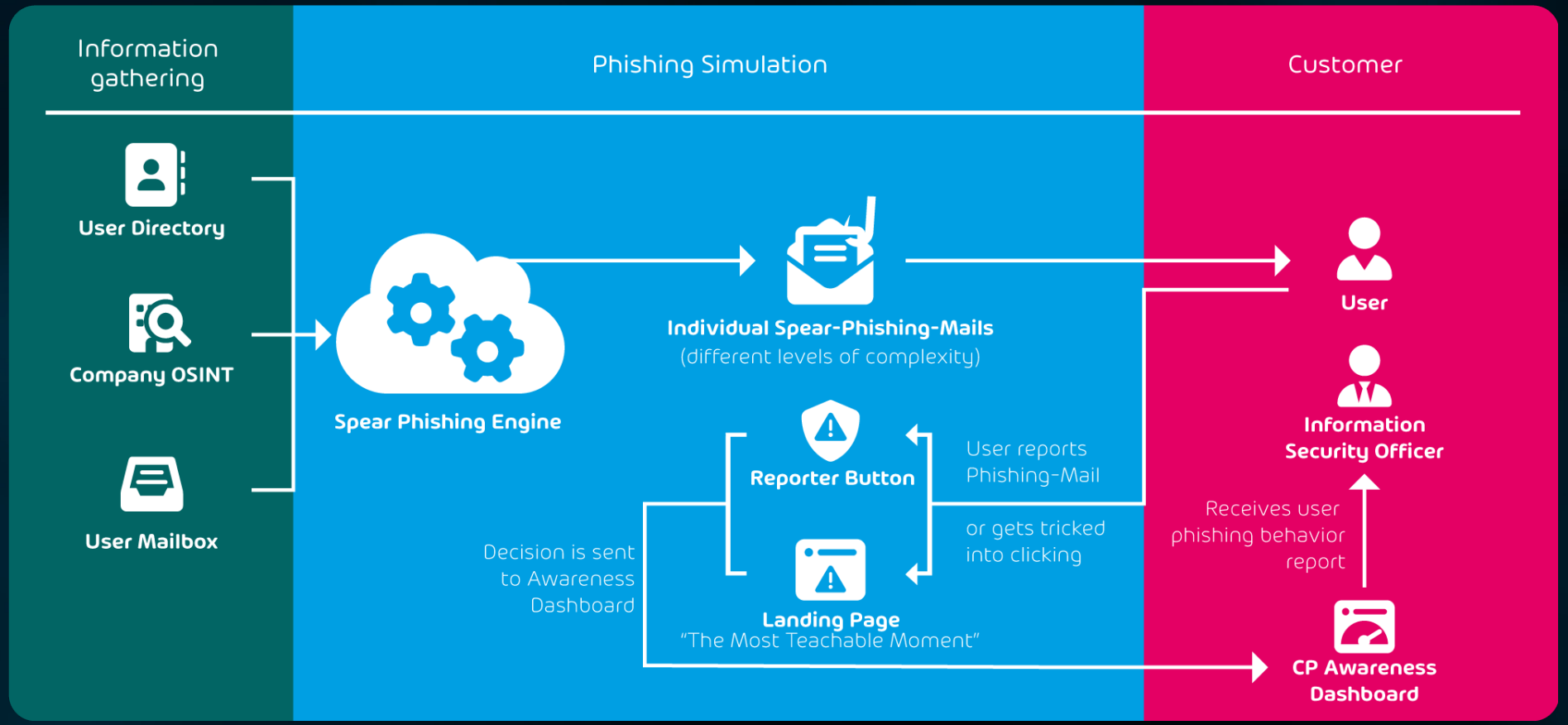
365 TOTAL PROTECTION

Kombination mit Hornetsecurity 365 Total Protection oder Spam und Malware Protection wird die Spear-Phishing-Engine sogar die individuellen User-Mail-Postfächer auslesen und in den Phishing-Szenarien Bezug zu Themen herstellen, die der Empfänger selbst gerade bearbeitet, z. B. ein Status-Update zu einem laufenden Projekt, an dem der Empfänger beteiligt ist.

HORNETSECURITY

PATENTIERTE SPEAR-PHISHING-ENGINE

ABLAUF DER SPEAR-PHISHING-SIMULATION



ENTSCHEIDENDE FAKTOREN FÜR EIN ERFOLGREICHES AWARENESS TRAINING

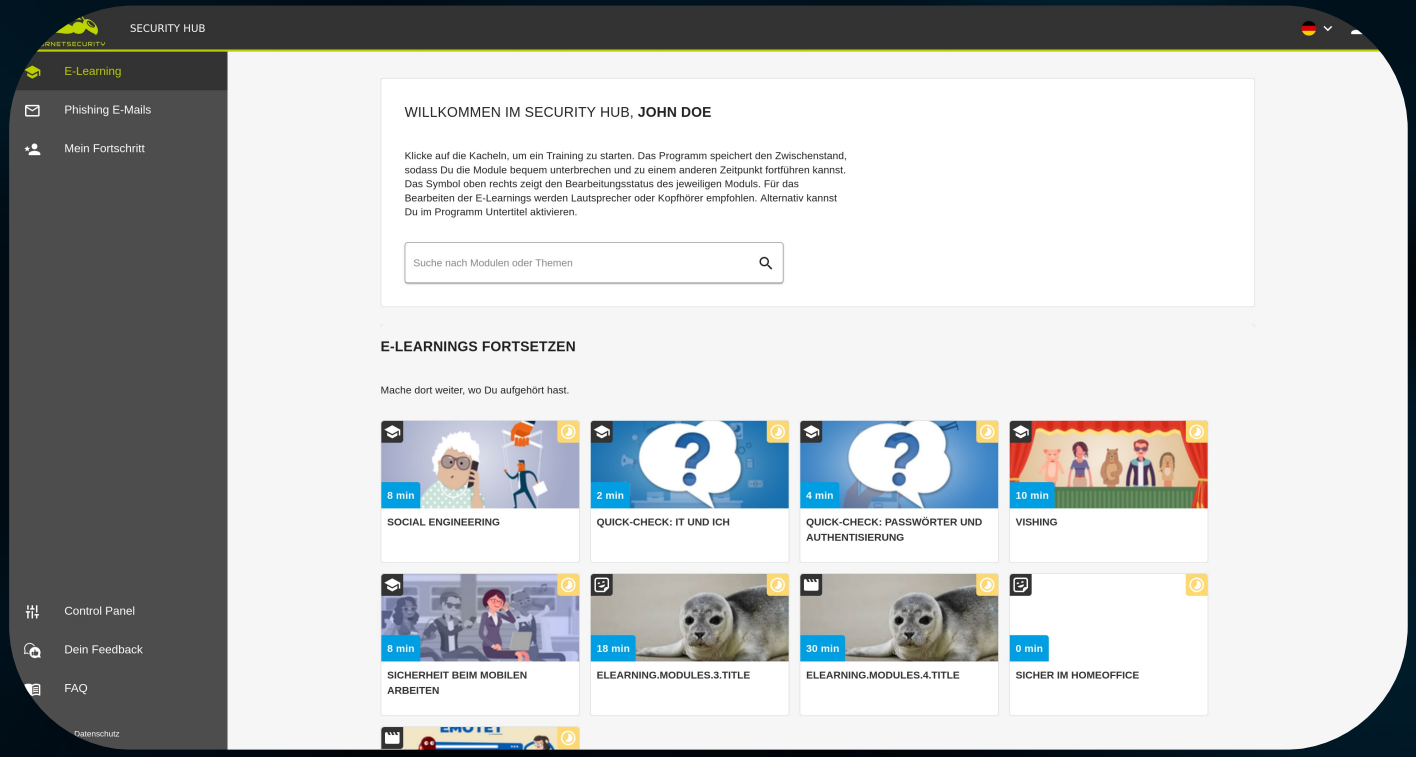
- Entscheidende Faktoren:
  - Messbar: für Ihren garantierten Erfolg
  - Effizient: Individuell und bedarfsgerecht
  - Realitätsnah: Vorgehen wie ein echter Angreifer
  - **Wirksam: Selbstbestimmtes Trainieren & Lernen mit Fun Faktor**

HORNETSECURITY

SECURITY HUB

SCHAFFEN SIE EINE MOTIVIERENDE LERNUMGEBUNG FÜR IHRE BENUTZER

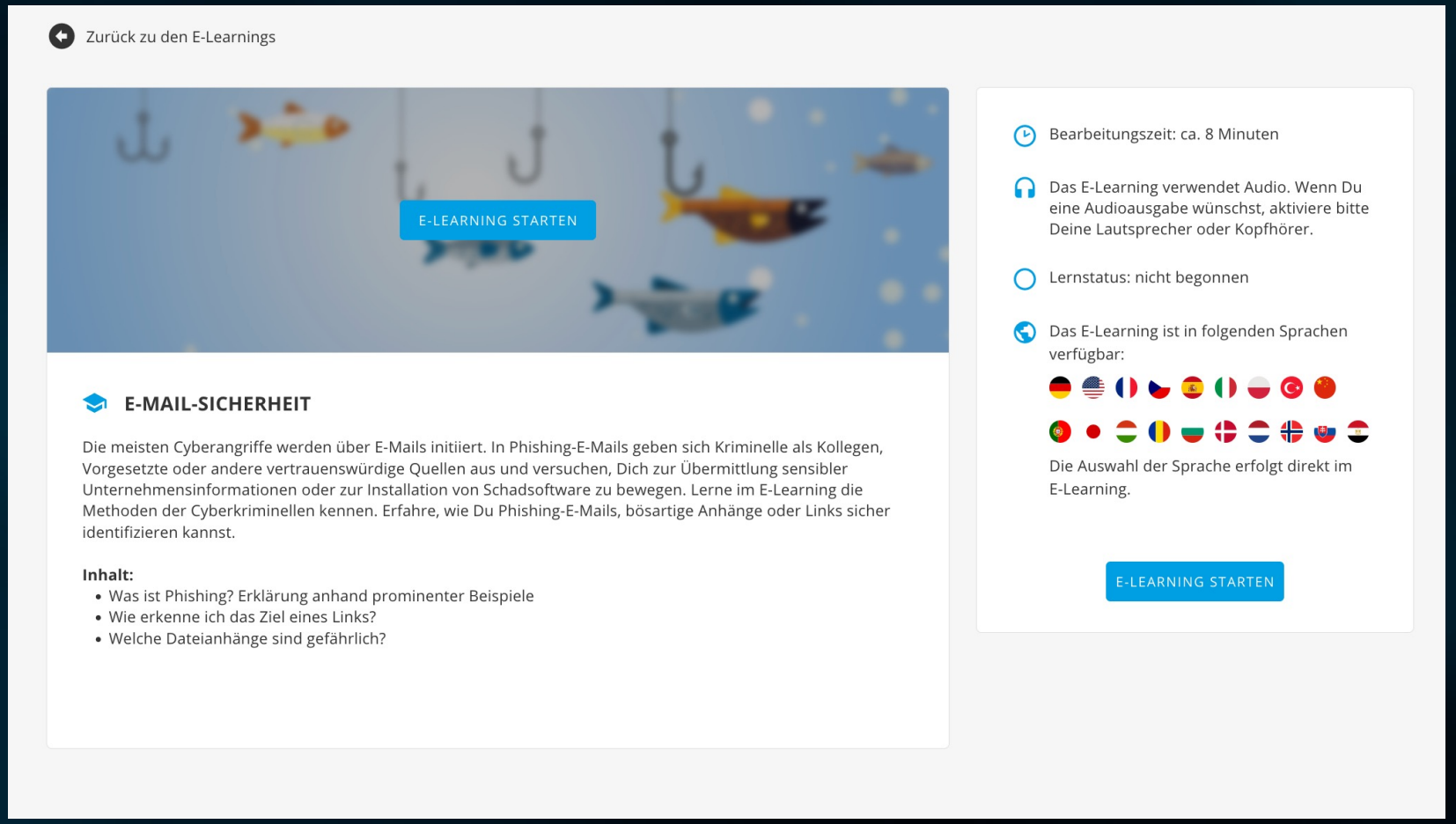
- Zentraler Zugriff auf alle Lerninhalte
- Auswertung der individuellen Phishing Simulation
- Gamification-Ansatz spornt Nutzer an, "ihr Bestes zu geben"
- Lerninhalte in mehreren Sprachen verfügbar



SECURITY HUB

SCHAFFEN SIE EINE MOTIVIERENDE LERNUMGEBUNG FÜR IHRE BENUTZER

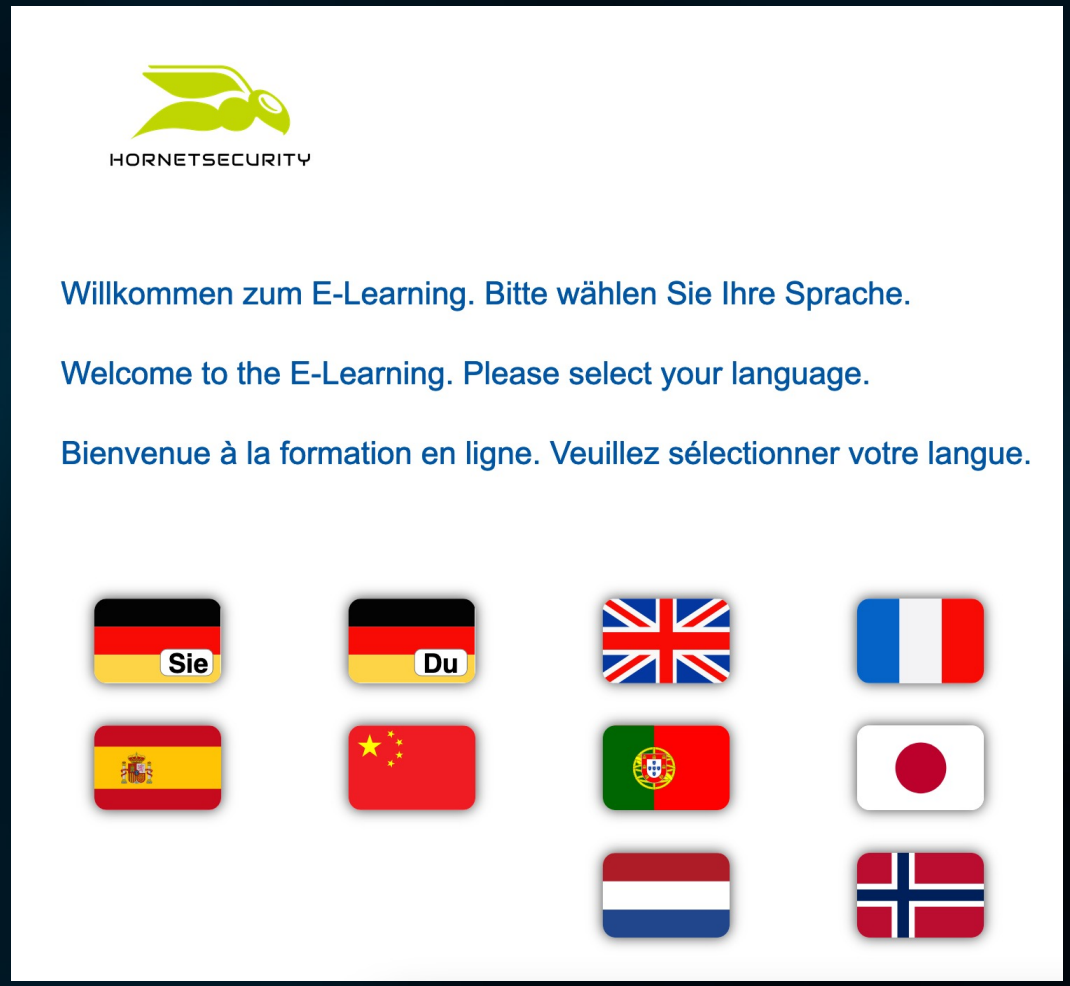
HORNETSECURITY



SECURITY HUB

SCHAFFEN SIE EINE MOTIVIERENDE LERNUMGEBUNG FÜR IHRE BENUTZER

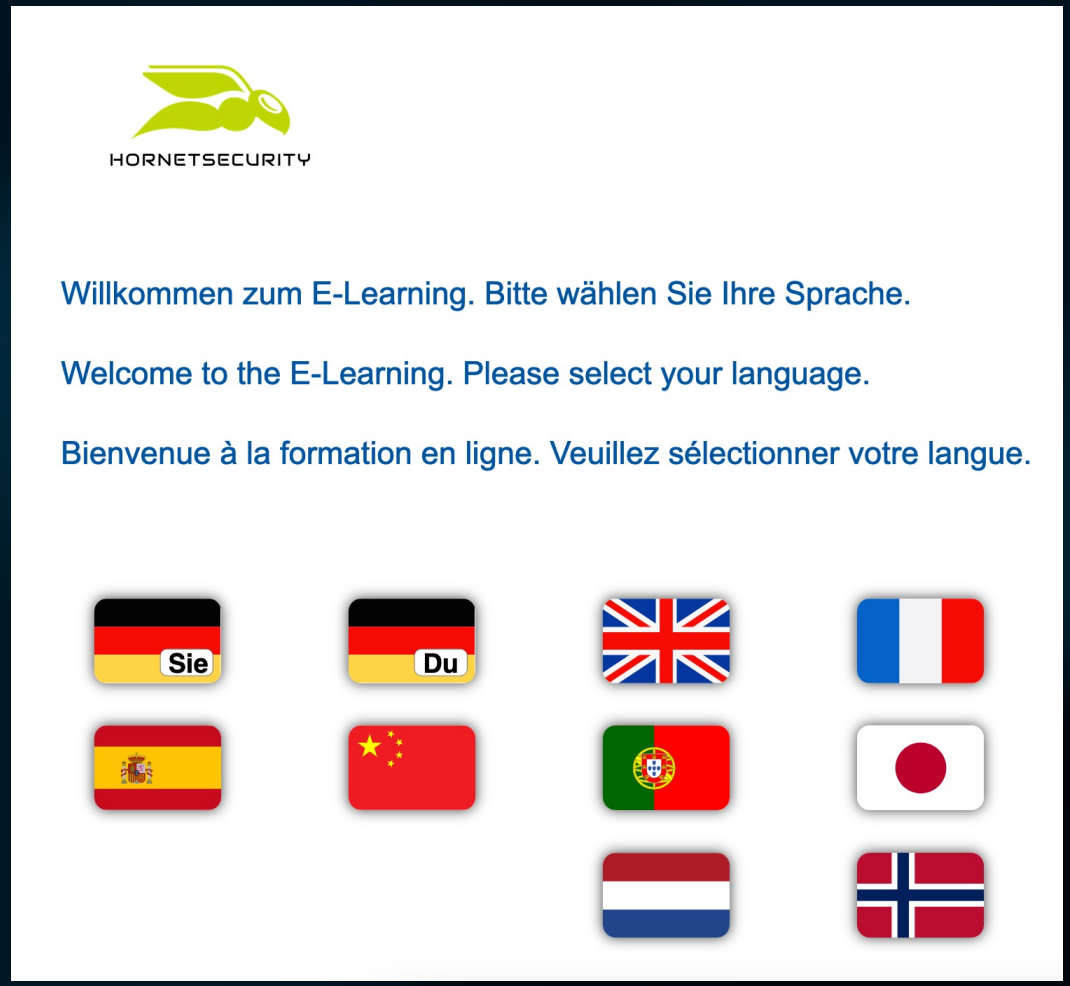
HORNETSECURITY



SECURITY HUB

SCHAFFEN SIE EINE MOTIVIERENDE LERNUMGEBUNG FÜR IHRE BENUTZER

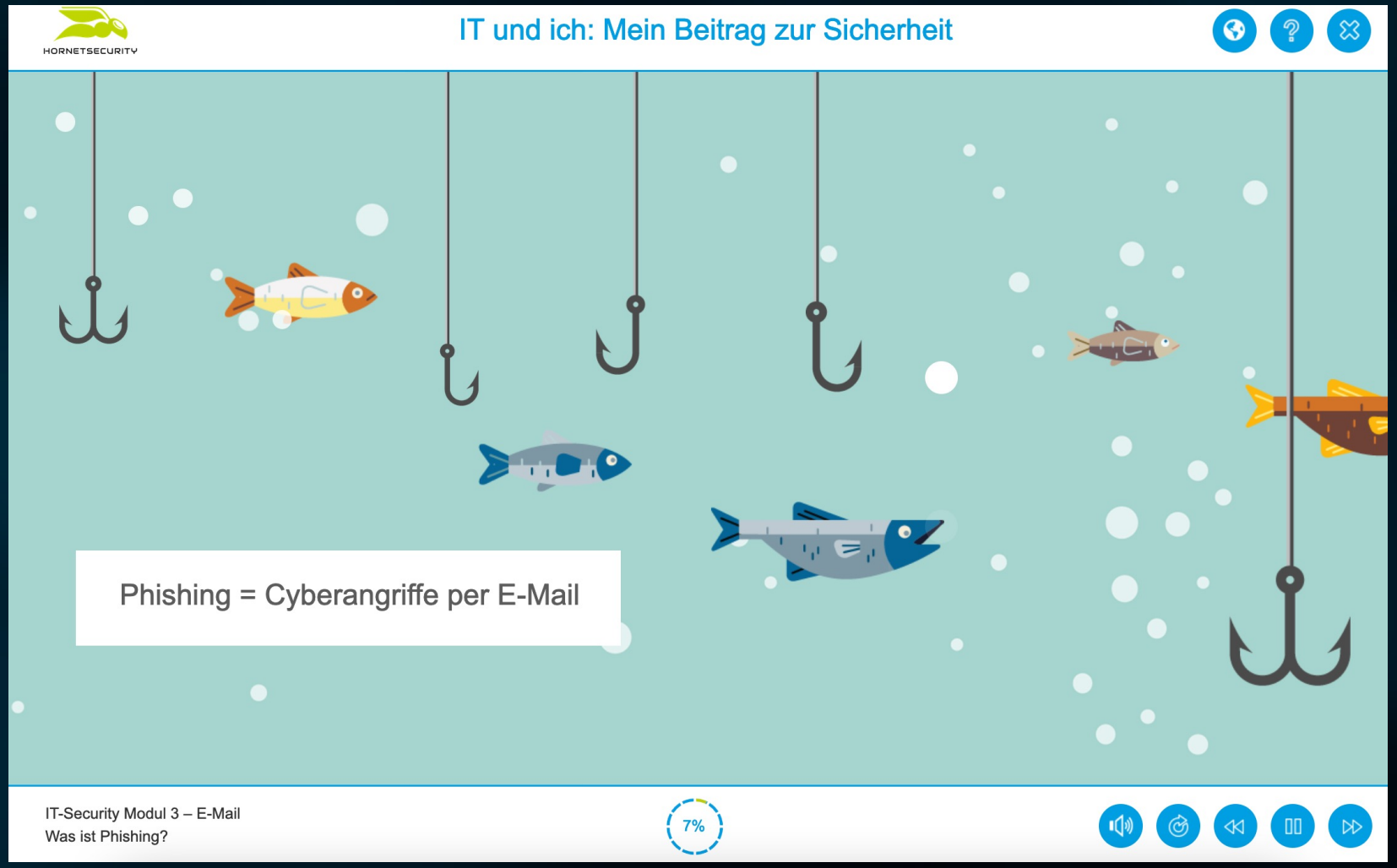
HORNETSECURITY



SECURITY HUB

SCHAFFEN SIE EINE MOTIVIERENDE LERNUMGEBUNG FÜR IHRE BENUTZER

HORNETSECURITY



SECURITY AWARENESS TRAINING
KEY FEATURES IM ÜBERBLICK

HORNETSECURITY

Awareness Engine – Key Features

- **Auto Training Mode: Die Lerninhalte werden automatisch und bedarfsgerecht an die User und Gruppen ausgerollt.**
- Single User & Productivity Booster: Benutzer mit zusätzlichen Lernbedarf werden intensiver trainiert; Benutzer auf einem sehr guten Sicherheitsniveau hingegen weniger.
- Automatisches Onboarding neuer User (setzt LDAP/AD Sync. voraus)
- Manual Training Mode: Es besteht die Option, Trainingsmodule manuell an die Gruppen und User auszurollen.

SECURITY AWARENESS TRAINING
KEY FEATURES IM ÜBERBLICK

Spear-Phishing-Engine – Key Features

Automatisiert generierte, individuell zugeschnittene Spear-Phishing-Angriffe mit unterschiedlichen Schwierigkeitsleveln. Inkl. gefälschte Login-Seiten und Dateianhänge mit Makros.

Level 7 – Inkl. Mitlesen des Postfachs	✓
Level 6 – Inkl. Antwort-Verlauf	✓
Level 5 – Inkl. Spoofing Domains	✓
Level 4 – Inkl. Job-Position + Abteilung	✓
Level 3 - Unternehmens-OSINT	✓
Level 2 - Spear-Phishing von GF	✓
Level 1 - Massen-Phishing	✓

✓ Level 6 & 7 Phishing-Szenarien für späteren Ausbau geplant.
Voraussetzung: Spam and Malware Protection oder 365 Total Protection erforderlich.

HORNETSECURITY

THANK YOU!

HORNETSECURITY

HORNETSECURITY