



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

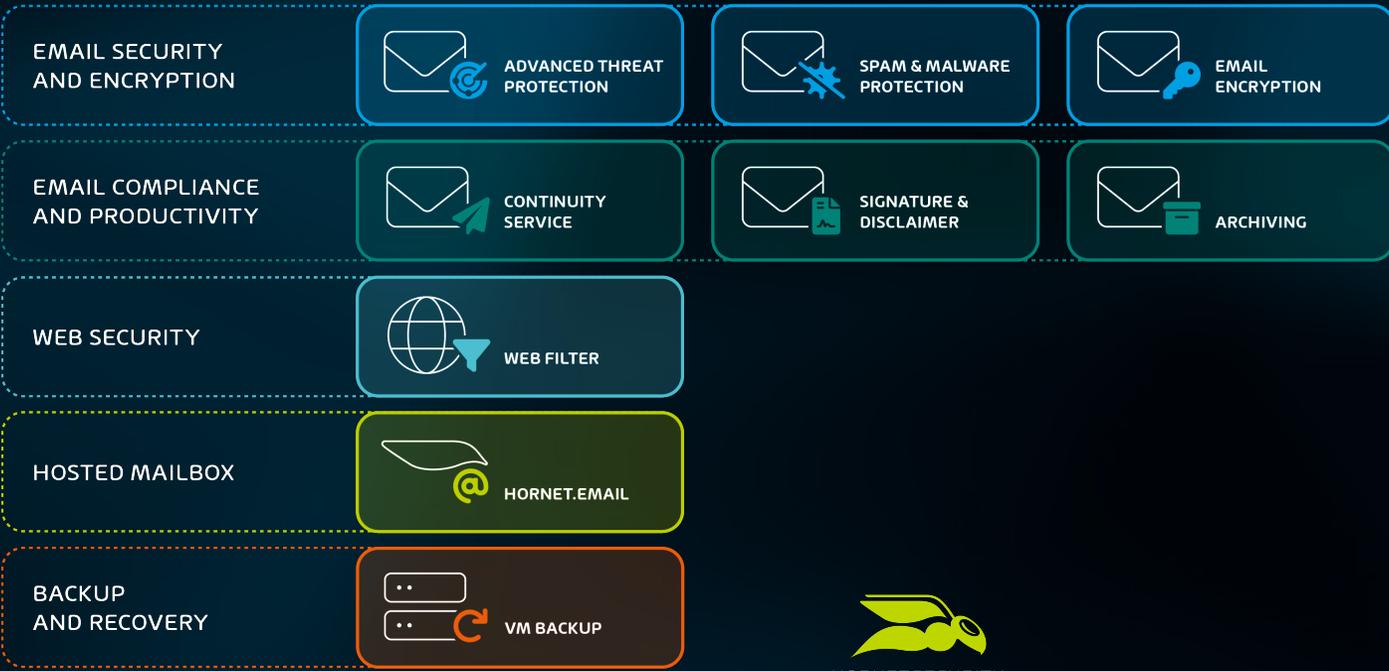


15
Services

CLOUD SECURITY SERVICES FOR MICROSOFT 365



SECURITY SERVICES



1 365 TOTAL PROTECTION BUSINESS (PLAN 1)

NEXT-LEVEL MICROSOFT 365 SECURITY

- SPAM & MALWARE PROTECTION
- EMAIL ENCRYPTION
- EMAIL SIGNATURES & DISCLAIMERS

2 365 TOTAL PROTECTION ENTERPRISE (PLAN 2)

PREMIUM NEXT-LEVEL MICROSOFT 365 SECURITY

- SPAM & MALWARE PROTECTION
- EMAIL ENCRYPTION
- EMAIL SIGNATURES & DISCLAIMERS

- ADVANCED THREAT PROTECTION
- EMAIL ARCHIVING
- EMAIL CONTINUITY

3 365 TOTAL PROTECTION ENTERPRISE BACKUP (PLAN 3)

SECURITY & BACKUP FOR MICROSOFT 365

- SPAM & MALWARE PROTECTION
- EMAIL ENCRYPTION
- EMAIL SIGNATURES & DISCLAIMERS

- ADVANCED THREAT PROTECTION
- EMAIL ARCHIVING
- EMAIL CONTINUITY

- BACKUP & RECOVERY OF MAILBOXES & TEAMS
- BACKUP & RECOVERY OF ONEDRIVE & SHAREPOINT
- BACKUP & RECOVERY OF ENDPOINTS

4 365 TOTAL PROTECTION COMPLIANCE & AWARENESS (PLAN 4)

SECURITY, BACKUP, COMPLIANCE & SECURITY AWARENESS FOR MICROSOFT 365

- SPAM & MALWARE PROTECTION
- EMAIL ENCRYPTION
- EMAIL SIGNATURES & DISCLAIMERS

- ADVANCED THREAT PROTECTION
- EMAIL ARCHIVING
- EMAIL CONTINUITY

- BACKUP & RECOVERY OF MAILBOXES & TEAMS
- BACKUP & RECOVERY OF ONEDRIVE & SHAREPOINT
- BACKUP & RECOVERY OF ENDPOINTS

- PERMISSION MANAGER
- PERMISSION ALERTS
- PERMISSION AUDIT

- SPEAR PHISHING SIMULATION
- CONTINUOUS AWARENESS TRAINING
- ESI® BENCHMARKING

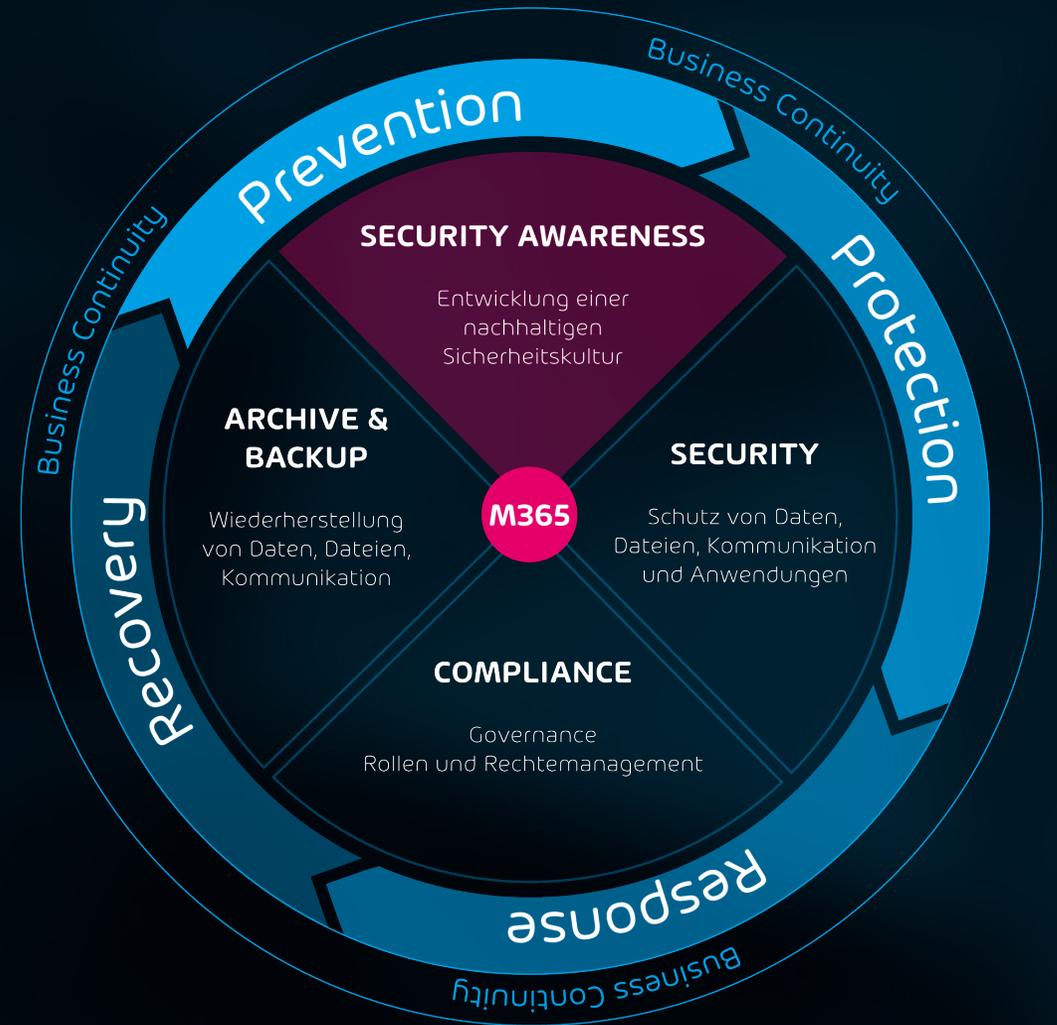
PRODUKT-ÜBERSICHT – DAS IST NEU!



HORNETSECURITY



**SECURITY
AWARENESS
TRAINING**



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% 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



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



Sehr geehrte Geschäftspartner,

die Gruppe ist Opfer eines kriminellen Cyberangriffes geworden. Unsere IT-Systeme sind standortübergreifend betroffen.

Allerdings sind große Teile unserer Produktion nach wie vor arbeitsfähig und laufen derzeit im Notbetrieb.

In unserer Erreichbarkeit sind wir aktuell jedoch noch stark eingeschränkt. Wir arbeiten mit Hochdruck an der Behebung der Situation und haben hierfür auch professionelle, externe Unterstützung hinzugezogen.

Vielen Dank für Ihr Verständnis sowie Ihre Unterstützung.

Geschäftsleitung

[Hinweis schließen](#)

DABW
ORHA
NVERI
Ws, Auto
meier Com



HORNETSECURITY

Die [redacted] 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.

[redacted] 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.



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
- Sicherheitsmeldekettchen
- 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



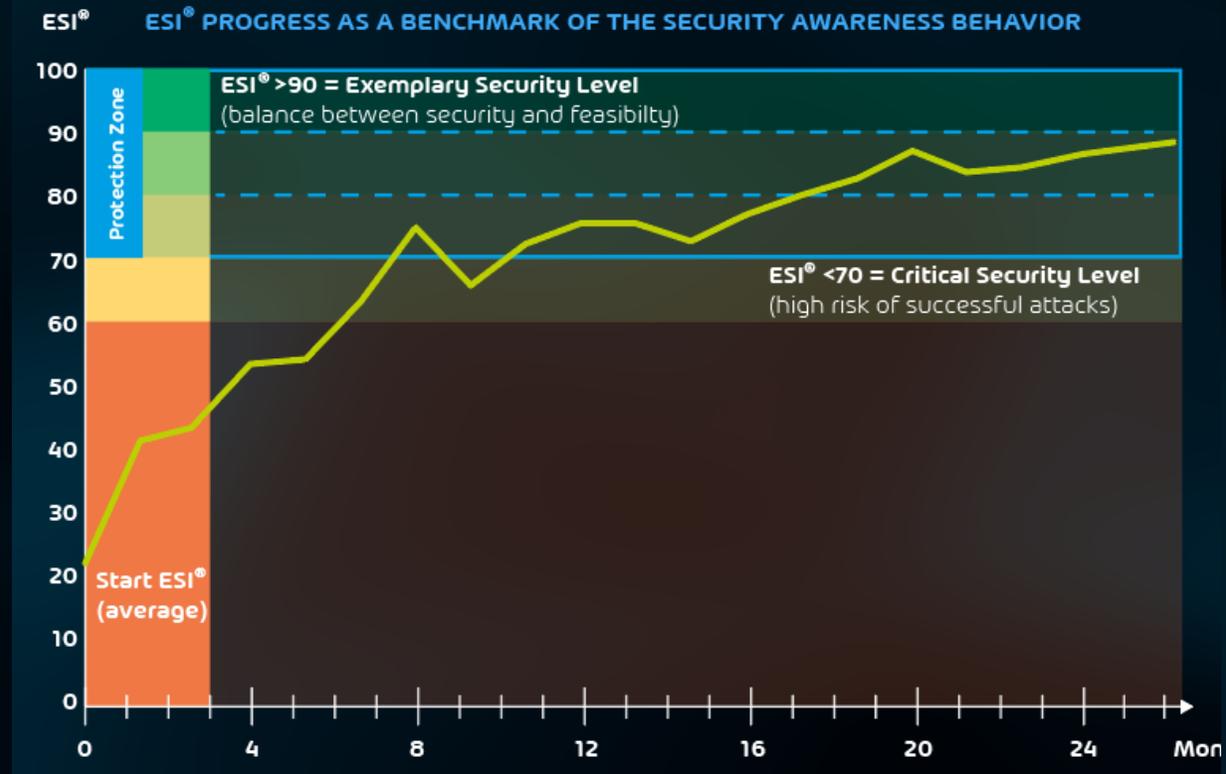
HORNETSECURITY

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.

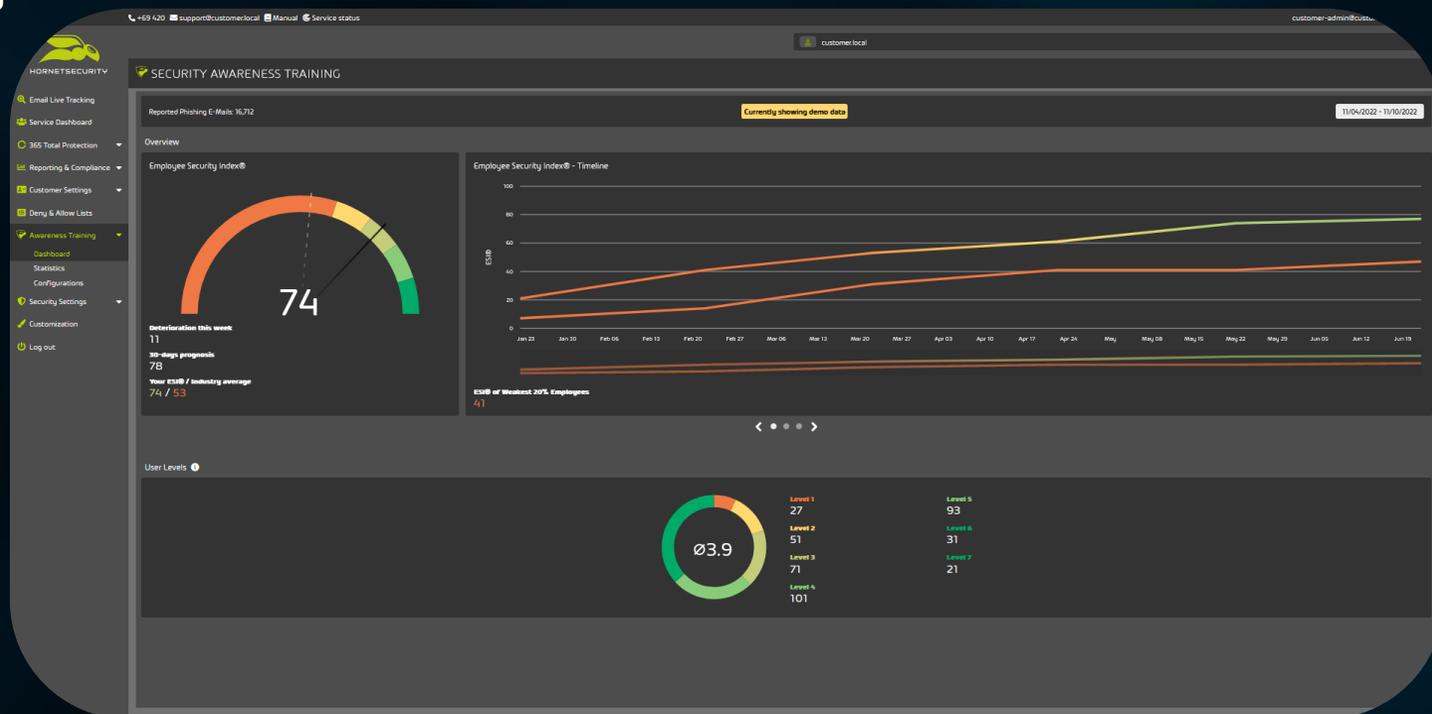


HORNETSECURITY



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



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.



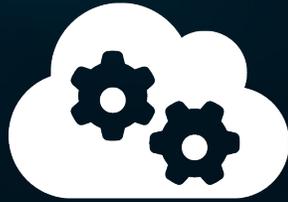
Die Awareness Engine identifiziert Nutzer mit besonderem Lernbedarf, die anschließend intensiver trainiert werden. Damit wird sichergestellt, dass Mitarbeiter mit zusätzlichem Lernbedarf nicht zu kurz kommen und weiterhin intensiv geschult werden.



HORNETSECURITY

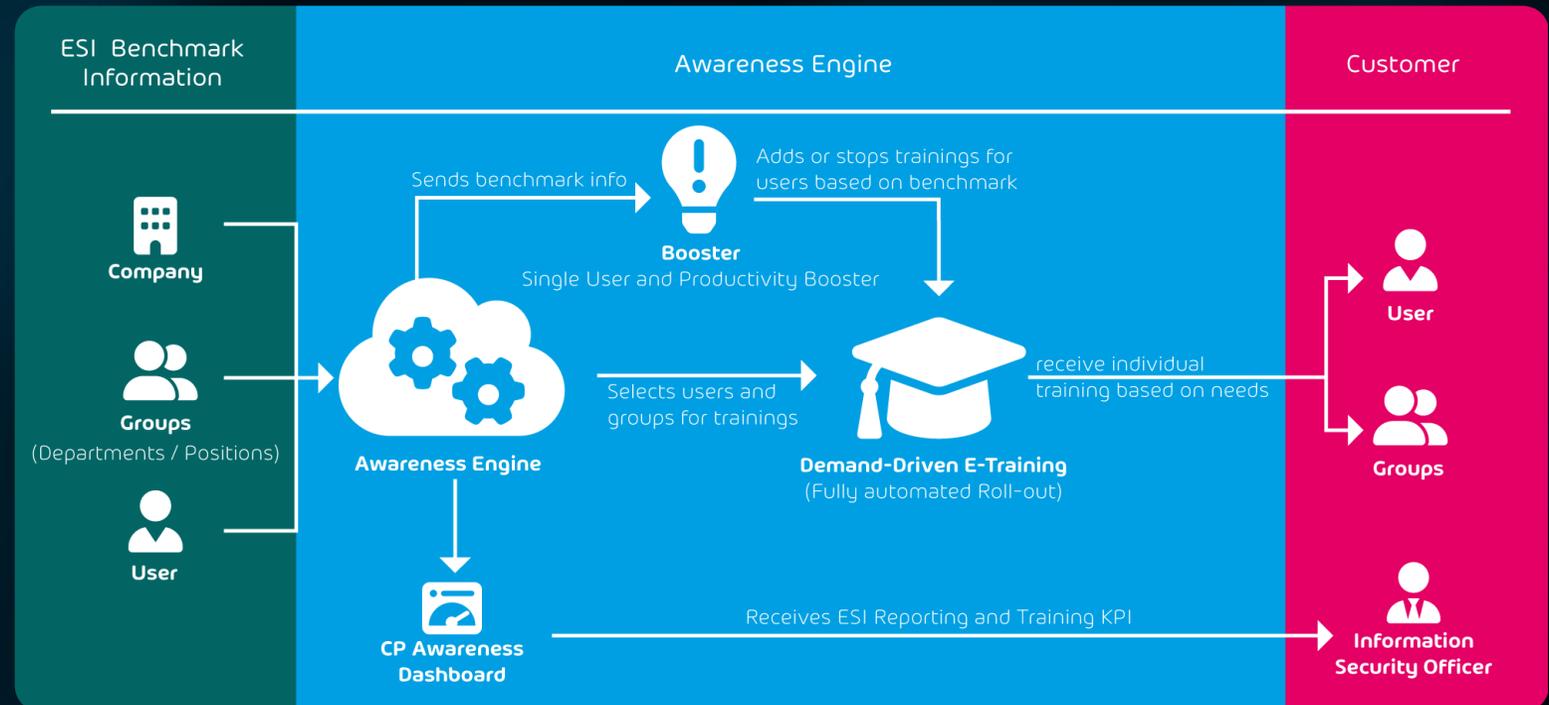
AWARENESS ENGINE

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



HORNETSECURITY

INDIVIDUALISIERUNG

kununu Let's make work better. Arbeitgeber eingeben

Arbeitgeber finden Gehaltscheck News Über kununu Für Arbeitgeber

Übersicht Bewertungen (143) Gehälter (33) Jobs Firmenkultur (25) Fragen

Was wir bieten

Benefits

Die folgenden Benefits wurden am häufigsten in den Bewertungen von 84 Mitarbeitern bestätigt.

- Mitarbeiter-Events** 71%
- Parkplatz** 71%
- Flexible Arbeitszeiten** 70%

✕ Änderungen verwerfen ✓ Speichern

Auswertung der Daten der Organisation auf Kununu

https://www.kununu.com/de/hornetsecurity3 ✓ Speichern

- Flexible Arbeitszeiten
- Mitarbeiter-Events
- Kantine
- Gute Verkehrsanbindung
- Diensthandy
- Betriebliche Altersvorsorge
- Internetnutzung
- Homeoffice
- Essenszulage
- Parkplatz
- Gesundheits-Maßnahmen
- Firmenwagen
- Barrierefrei
- Betriebsarzt
- Mitarbeiter-Beteiligung
- Coaching
- Kinderbetreuung
- Hund erlaubt
- Rabatte



HORNETSECURITY

INDIVIDUALISIERUNG



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



HORNETSECURITY

INDIVIDUALISIERUNG

Neue Benutzervorschriften



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

Donnerstag, 13. Oktober 2022 um 14:58

An: 🕒 Max Mustermann

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



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

PATENTIERTE SPEAR-PHISHING-ENGINE

VORGEHEN WIE EIN ECHTER ANGREIFER



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.

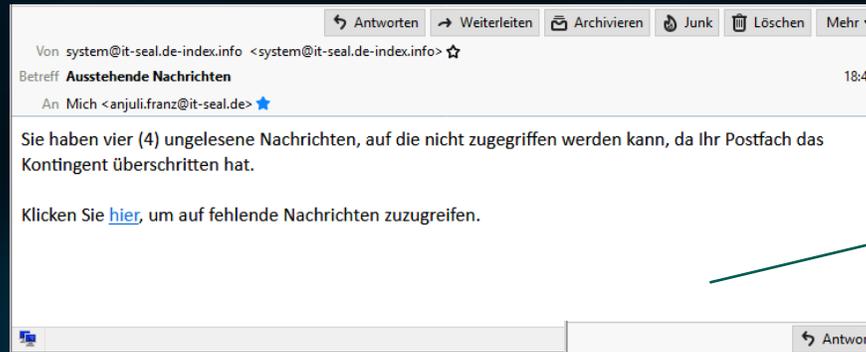


HORNETSECURITY

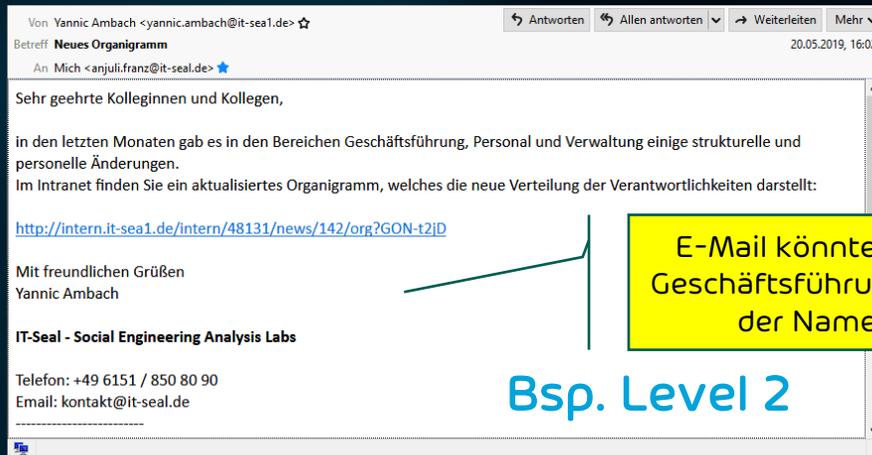
PATENTIERTE SPEAR-PHISHING-ENGINE

VORGEHEN WIE EIN ECHTER ANGREIFER

Bsp. Level 1

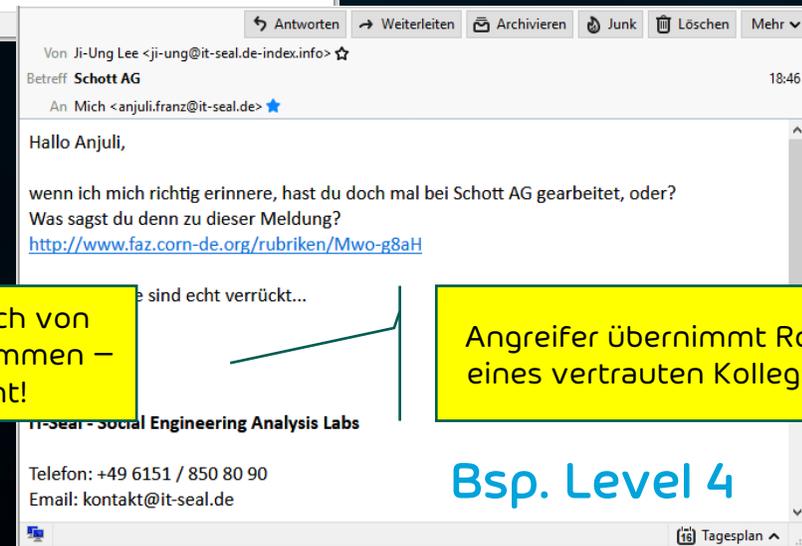


Autom. generierte System-E-Mail – könnte echt sein.



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

Bsp. Level 2



Angreifer übernimmt Rolle eines vertrauten Kollegen.

Bsp. Level 4



HORNETSECURITY

PATENTIERTE SPEAR-PHISHING-ENGINE

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



TEACHABLE MOMENT

PHISHING AWARENESS-TRAINING
EIN SERVICE FÜR IT-SEAL GMBH

GLÜCK GEHABT!
Das hätte eine Phishing-Mail sein können.

Drei einfache Schritte, wie Sie eine Phishing-Mail erkennen:

Jetzt ansehen ca. 3 Minuten

Ihre Teilnahme ist 100% anonym!
Niemand erhält Informationen darüber, wer welche E-Mail geöffnet oder welchen Link angeklickt hat. Das Training dient dazu, Sie im Umgang mit Betrugsversuchen zu schulen.

Schutz vor Cyber-Kriminellen
Cyber-Angriffe sind oft auf Ihre Organisation oder auf Sie persönlich zugeschnitten. Bleiben Sie wachsam, um sich und Ihre Organisation vor Betrug, Abzocke und weitreichenden Konsequenzen zu schützen.

AR | CS | DA | **DE** | EN | ES | FR | HI | HR | HU | IT | JA | NL | NO | PL | PT | RO | RU | SK | SR | TR | ZH



HORNETSECURITY

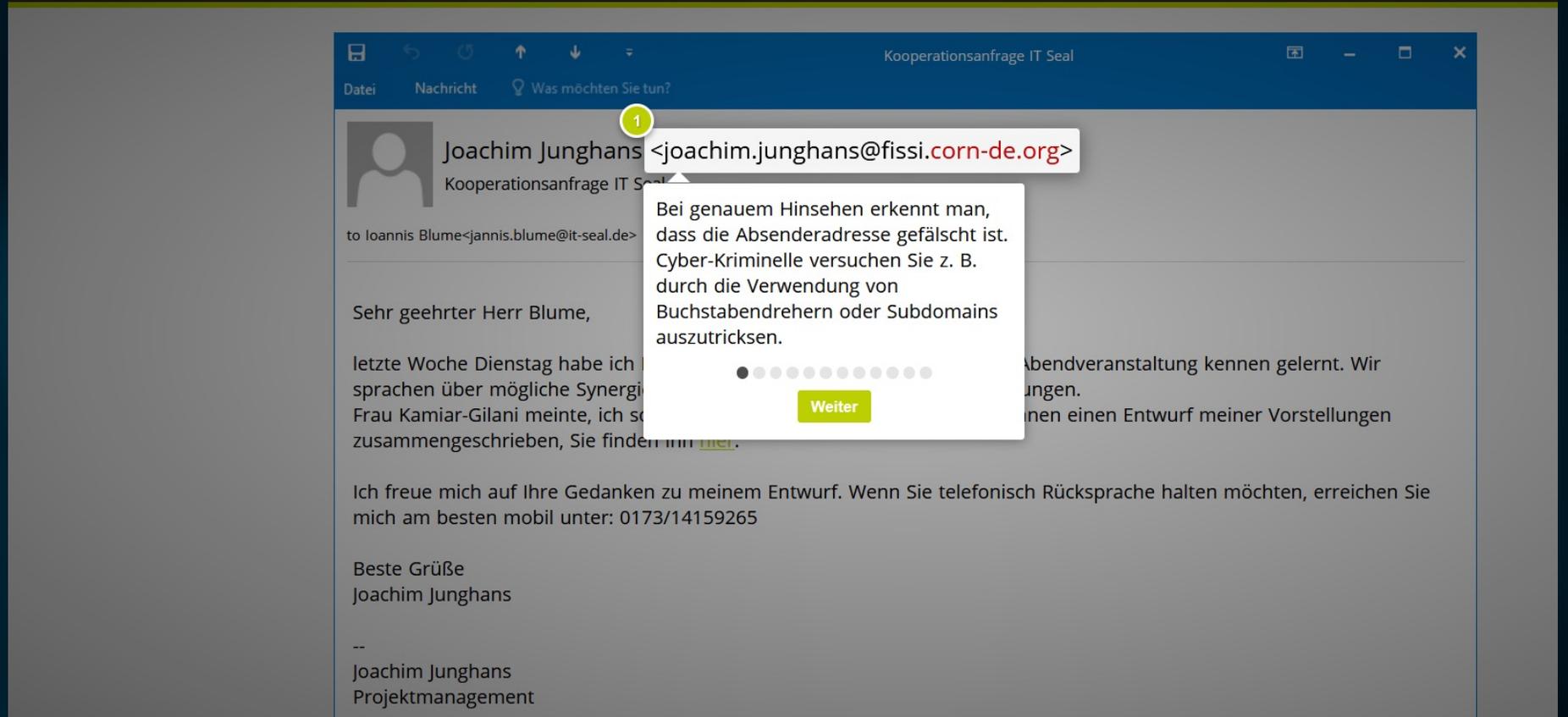
PATENTIERTE SPEAR-PHISHING-ENGINE

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

 TEACHABLE MOMENT

PHISHING AWARENESS-TRAINING

EIN SERVICE FÜR IT-SEAL GMBH



Kooperationsanfrage IT Seal

Datei Nachricht Was möchten Sie tun?

Joachim Junghans <joachim.junghans@fissi.corn-de.org>
Kooperationsanfrage IT Seal

to Ioannis Blume <jannis.blume@it-seal.de>

Sehr geehrter Herr Blume,

letzte Woche Dienstag habe ich ...
sprachen über mögliche Synergien ...
Frau Kamiar-Gilani meinte, ich soll ...
zusammengeschrieben, Sie finden mich [hier](#).

Ich freue mich auf Ihre Gedanken zu meinem Entwurf. Wenn Sie telefonisch Rücksprache halten möchten, erreichen Sie mich am besten mobil unter: 0173/14159265

Beste Grüße
Joachim Junghans

--
Joachim Junghans
Projektmanagement

Bei genauem Hinsehen erkennt man, dass die Absenderadresse gefälscht ist. Cyber-Kriminelle versuchen Sie z. B. durch die Verwendung von Buchstabendrehern oder Subdomains auszutricksen.

Weiter



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.



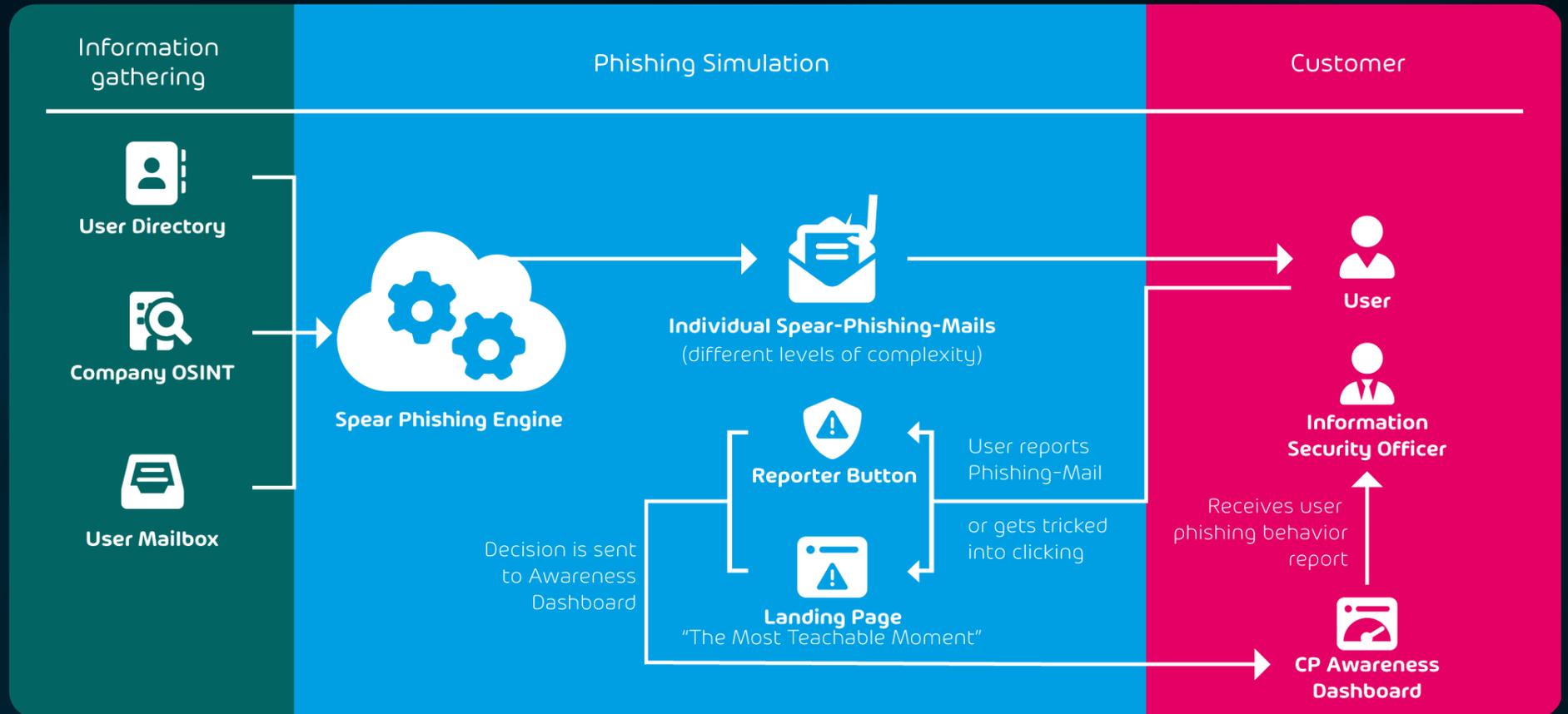
Kombination mit **Hornetsecurity 365 Total Protection** oder **Spam und Malware Protection** wird die Spear-Phishing-Engine sogar die individuellen User-Mail-Postfächer auslesen und in den Phishing-Szenarien Bezug zu Themen herstellen, die der Empfänger selbst gerade bearbeitet, z. B. ein Status-Update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



HORNETSECURITY

PATENTIERTE SPEAR-PHISHING-ENGINE

ABLAUF DER SPEAR-PHISHING-SIMULATION



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**

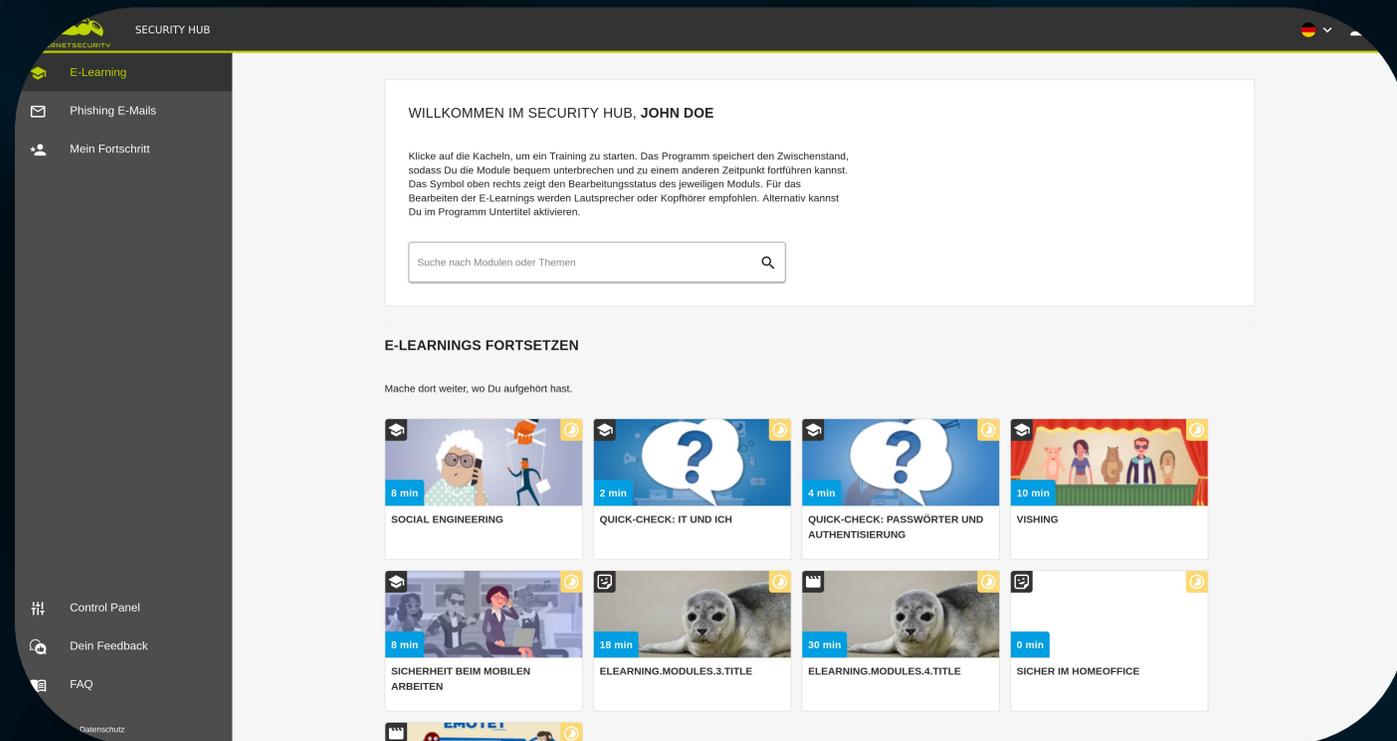


HORNETSECURITY

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



The screenshot displays the Security Hub interface. At the top, it says "SECURITY HUB" and "WILLKOMMEN IM SECURITY HUB, JOHN DOE". Below this is a welcome message in German: "Klicke auf die Kacheln, um ein Training zu starten. Das Programm speichert den Zwischenstand, sodass Du die Module bequem unterbrechen und zu einem anderen Zeitpunkt fortführen kannst. Das Symbol oben rechts zeigt den Bearbeitungsstatus des jeweiligen Moduls. Für das Bearbeiten der E-Learnings werden Lautsprecher oder Kopfhörer empfohlen. Alternativ kannst Du im Programm Untertitel aktivieren." Below the message is a search bar with the placeholder text "Suche nach Modulen oder Themen".

The main content area is titled "E-LEARNINGS FORTSETZEN" and includes the instruction "Mache dort weiter, wo Du aufgehört hast." Below this is a grid of e-learning modules:

Module Title	Duration
SOCIAL ENGINEERING	8 min
QUICK-CHECK: IT UND ICH	2 min
QUICK-CHECK: PASSWÖRTER UND AUTHENTISIERUNG	4 min
VISHING	10 min
SICHERHEIT BEIM MOBILEN ARBEITEN	6 min
ELEARNING.MODULES.3.TITLE	18 min
ELEARNING.MODULES.4.TITLE	30 min
SICHER IM HOMEOFFICE	0 min

The interface also features a sidebar with navigation options: "E-Learning", "Phishing E-Mails", "Mein Fortschritt", "Control Panel", "Dein Feedback", "FAQ", and "Datenschutz".



HORNETSECURITY

SECURITY HUB

SCHAFFEN SIE EINE MOTIVIERENDE LERNUMGEBUNG FÜR IHRE BENUTZER



HORNETSECURITY

← Zurück zu den E-Learnings



E-MAIL-SICHERHEIT

Die meisten Cyberangriffe werden über E-Mails initiiert. In Phishing-E-Mails geben sich Kriminelle als Kollegen, Vorgesetzte oder andere vertrauenswürdige Quellen aus und versuchen, Dich zur Übermittlung sensibler Unternehmensinformationen oder zur Installation von Schadsoftware zu bewegen. Lerne im E-Learning die Methoden der Cyberkriminellen kennen. Erfahre, wie Du Phishing-E-Mails, bösartige Anhänge oder Links sicher identifizieren kannst.

Inhalt:

- Was ist Phishing? Erklärung anhand prominenter Beispiele
- Wie erkenne ich das Ziel eines Links?
- Welche Dateianhänge sind gefährlich?

 Bearbeitungszeit: ca. 8 Minuten

 Das E-Learning verwendet Audio. Wenn Du eine Audioausgabe wünschst, aktiviere bitte Deine Lautsprecher oder Kopfhörer.

 Lernstatus: nicht begonnen

 Das E-Learning ist in folgenden Sprachen verfügbar:



Die Auswahl der Sprache erfolgt direkt im E-Learning.

E-LEARNING STARTEN

SECURITY HUB

SCHAFFEN SIE EINE MOTIVIERENDE LERNUMGEBUNG FÜR IHRE BENUTZER



Willkommen zum E-Learning. Bitte wählen Sie Ihre Sprache.

Welcome to the E-Learning. Please select your language.

Bienvenue à la formation en ligne. Veuillez sélectionner votre langue.



HORNETSECURITY

SECURITY HUB

SCHAFFEN SIE EINE MOTIVIERENDE LERNUMGEBUNG FÜR IHRE BENUTZER



Willkommen zum E-Learning. Bitte wählen Sie Ihre Sprache.

Welcome to the E-Learning. Please select your language.

Bienvenue à la formation en ligne. Veuillez sélectionner votre langue.



HORNETSECURITY

SECURITY HUB

SCHAFFEN SIE EINE MOTIVIERENDE LERNUMGEBUNG FÜR IHRE BENUTZER

The screenshot shows an interactive e-learning interface. At the top left is the HornetSecurity logo. The title 'IT und ich: Mein Beitrag zur Sicherheit' is centered at the top. On the right are icons for globe, help, and close. The main area is a light blue background with several fishing hooks hanging from the top. A yellow fish is on the left, a blue fish is in the center, and a brown fish is on the right. A white text box in the lower-left of the main area contains the text: 'Phishing = Cyberangriffe per E-Mail'. At the bottom left, it says 'IT-Security Modul 3 – E-Mail' and 'Was ist Phishing?'. In the bottom center is a progress indicator showing '7%'. At the bottom right are icons for volume, refresh, back, play, and forward.



HORNETSECURITY

SECURITY AWARENESS TRAINING KEY FEATURES IM ÜBERBLICK

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 zusätzlichem 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.



HORNETSECURITY

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