

Stärken Sie Ihre Human Firewall

Security Awareness Service by Hornetsecurity

AUTOMATISIERT. VERHALTENSBASIERT. KONTINUIERLICHER SERVICE.



Markus Todt

- Country Manager Austria
- todt@hornetsecurity.com



HORNETSECURITY



Muhammed Gülergüz

- Key Account Manager
- Muhammed.gueleryuez@hornetsecurity.com

HORNETSECURITY IN ZAHLEN



HORNETSECURITY



>420
Mitarbeiter



11
Rechenzentren



>60.000
Kunden



12
Büros



100 %
Channel



14
Services

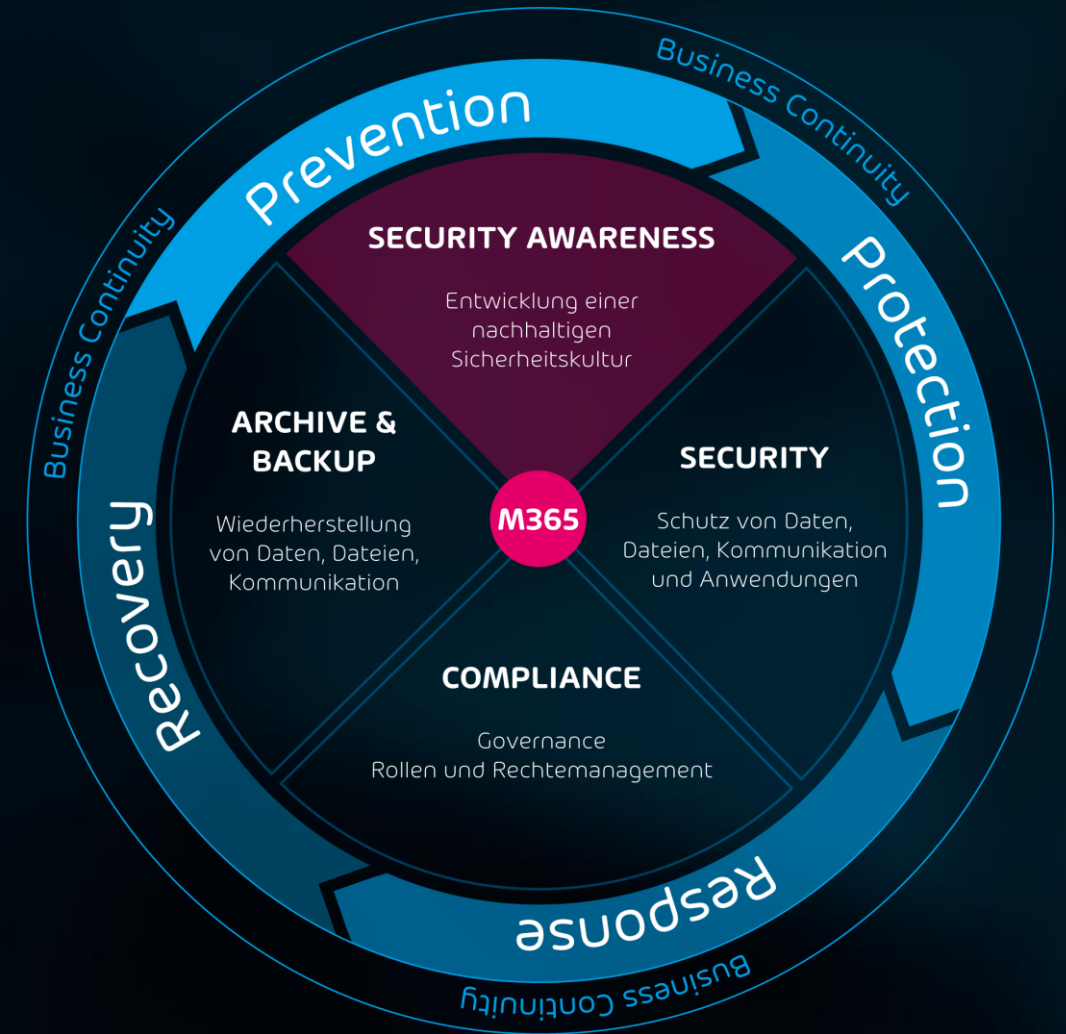
NEU: NEXT-GEN SECURITY AWARENESS SERVICE



HORNETSECURITY



**SECURITY
AWARENESS
SERVICE**



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
- Reports
- Sicherheitsmeldekettten



Reporter-Button
Outlook Add-In

ENTSCHEIDENDE FAKTOREN FÜR EIN ERFOLGREICHES AWARENESS TRAINING

👁 Entscheidende Faktoren:

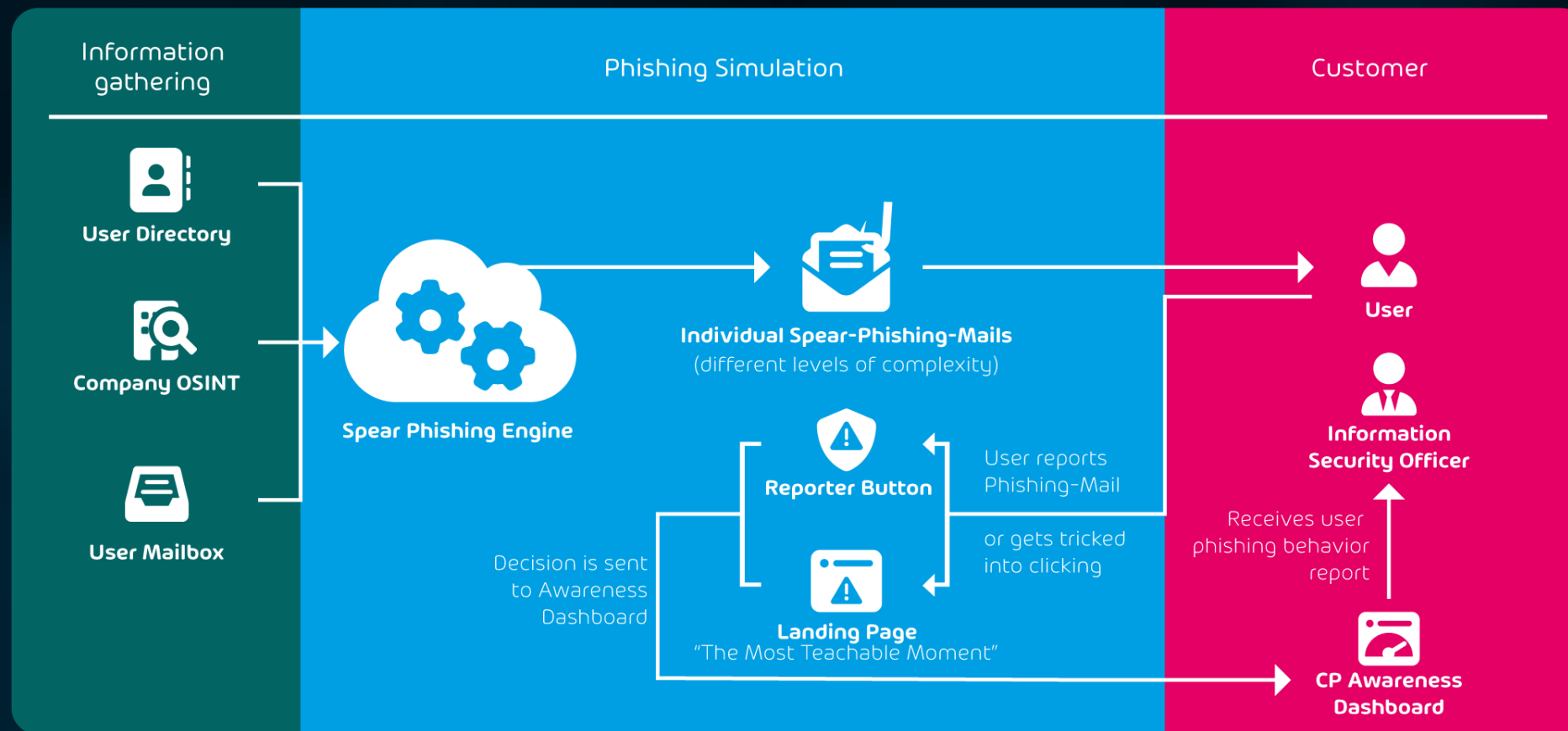
- 👁 **Realitätsnah:** Vorgehen wie ein echter Angreifer
- 👁 Messbar: für Ihren garantierten Erfolg
- 👁 Effizient: Individuell und bedarfsgerecht
- 👁 Wirksam: Selbstbestimmtes Trainieren & Lernen mit Fun Faktor



HORNETSECURITY

PATENTIERTE SPEAR-PHISHING-ENGINE

ABLAUF DER SPEAR-PHISHING-SIMULATION



HORNETSECURITY

PATENTIERTE SPEAR-PHISHING-ENGINE



Donnerstag, 1. Oktober 2020 um 13:49



○ Sofia pevnev <sofia.pevnev@it-seal.tr-login.org>

An: 🟢 Muhammed Gueleryuez

Hallo Muhammed,

wenn ich mich richtig erinnere, beschäftigst du dich doch recht gerne mit dem Thema Fußball, oder? Ich habe gestern eine Doku darüber gesehen und finde es auch sehr spannend. Ich würde mich gerne mehr damit beschäftigen und könnte dabei deine Hilfe und ein paar Tipps gebrauchen:

Was sagst Du dazu?

<http://www.amazon.safe-browsing.de/rubriken/671922Dwn-p6uD>

Mit freundlichen Grüßen

Sofia pevnev
IT-Seal GmbH

Hilpertstr. 31

64295 Darmstadt

PATENTIERTE SPEAR-PHISHING-ENGINE

Übernahme Vortrag Studentenbesuch

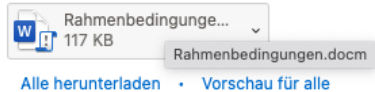


Dienstag, 5. Juli 2022 um 12:33



Sead Avdibasic <sead.avdibasic@it-seal.de>

An: Muhammed Gueleryuez



Hallo Muhammed,

am 19.07.2022 kommt uns eine Gruppe Studierender besuchen. Im Rahmen des Besuchs soll sich jede Abteilung im Unternehmen kurz vorstellen. Nun musste allerdings Jessica - eigentlich für die Aufgabe vorgesehen - aufgrund eines kurzfristigen Termins an dem Tag absagen. Könntest du bitte den Part übernehmen? Du kannst dir im Anhang mal die Rahmenbedingungen durchlesen.

Bitte sag mir bis zum 08.07.2022 Bescheid, ob du das übernehmen kannst - oder ob ich weitersuchen muss :-)

Viele Grüße
Sead



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](#)



PATENTIERTE SPEAR-PHISHING-ENGINE



SAB NetWeaver

Bitte mit Ihren Windows-Nutzerdaten anmelden.

User *

Password *

Logon Problems? [Get Support](#)

Copyright © SAB AG. All Rights Reserved.

PATENTIERTE SPEAR-PHISHING-ENGINE



Anmelden

jemand@example.com

[Sie können nicht auf Ihr Konto zugreifen?](#)

Weiter



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.

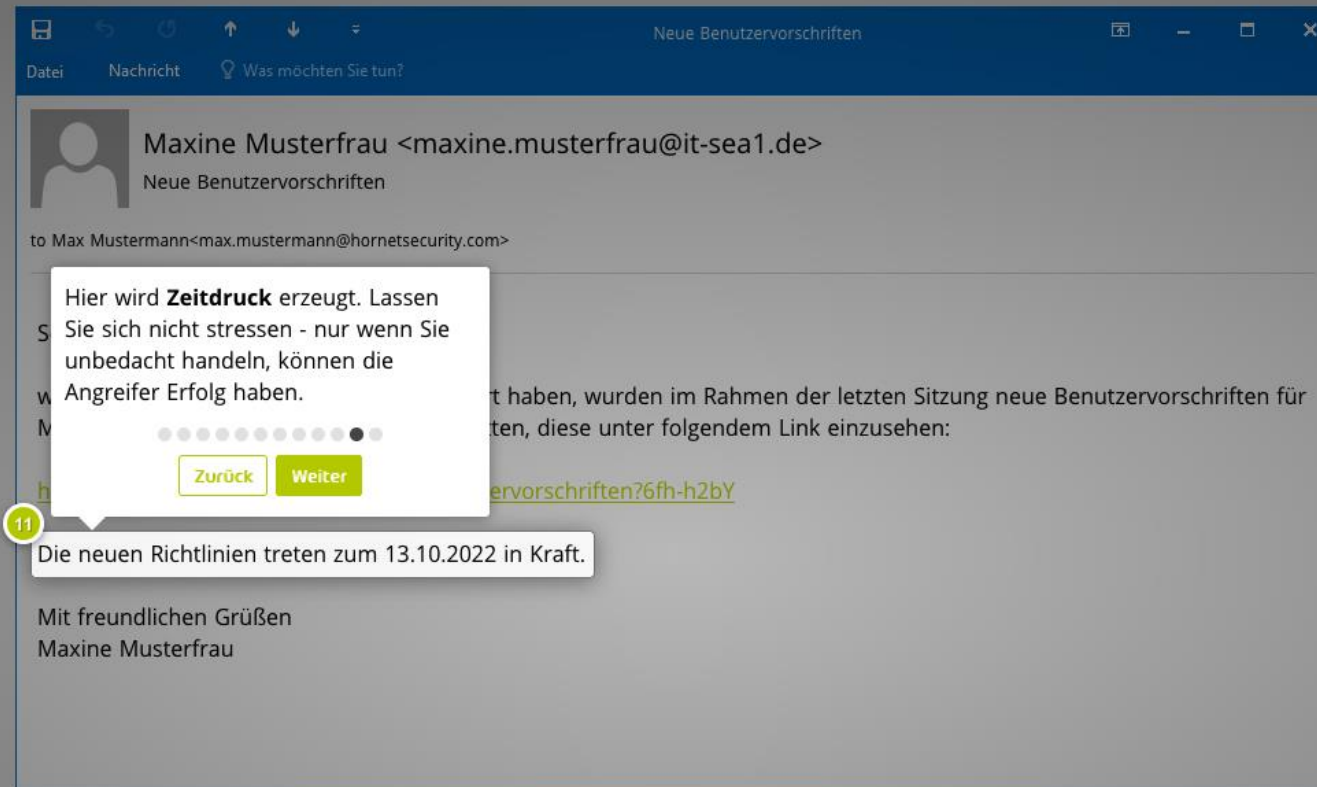
Schutz vor Cyber-Kriminellen

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](#)

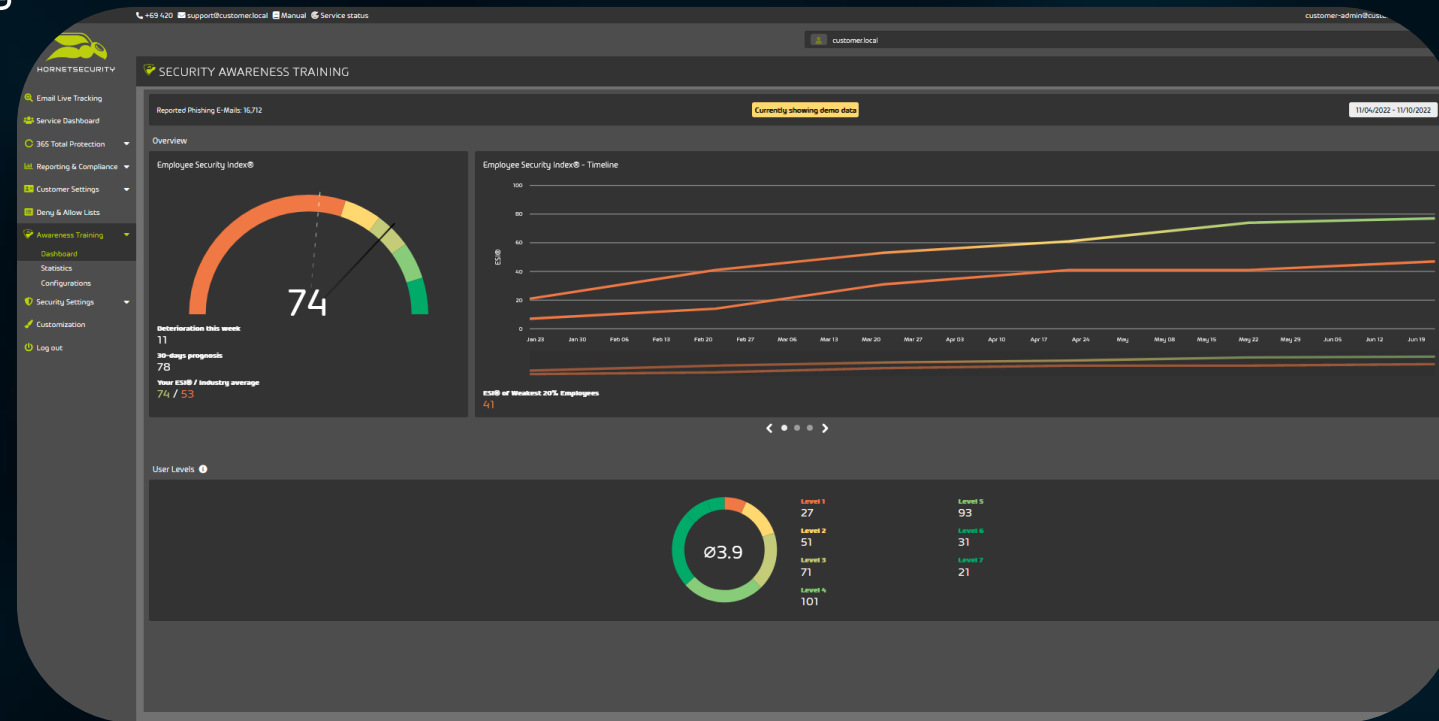


PATENTIERTE SPEAR-PHISHING-ENGINE



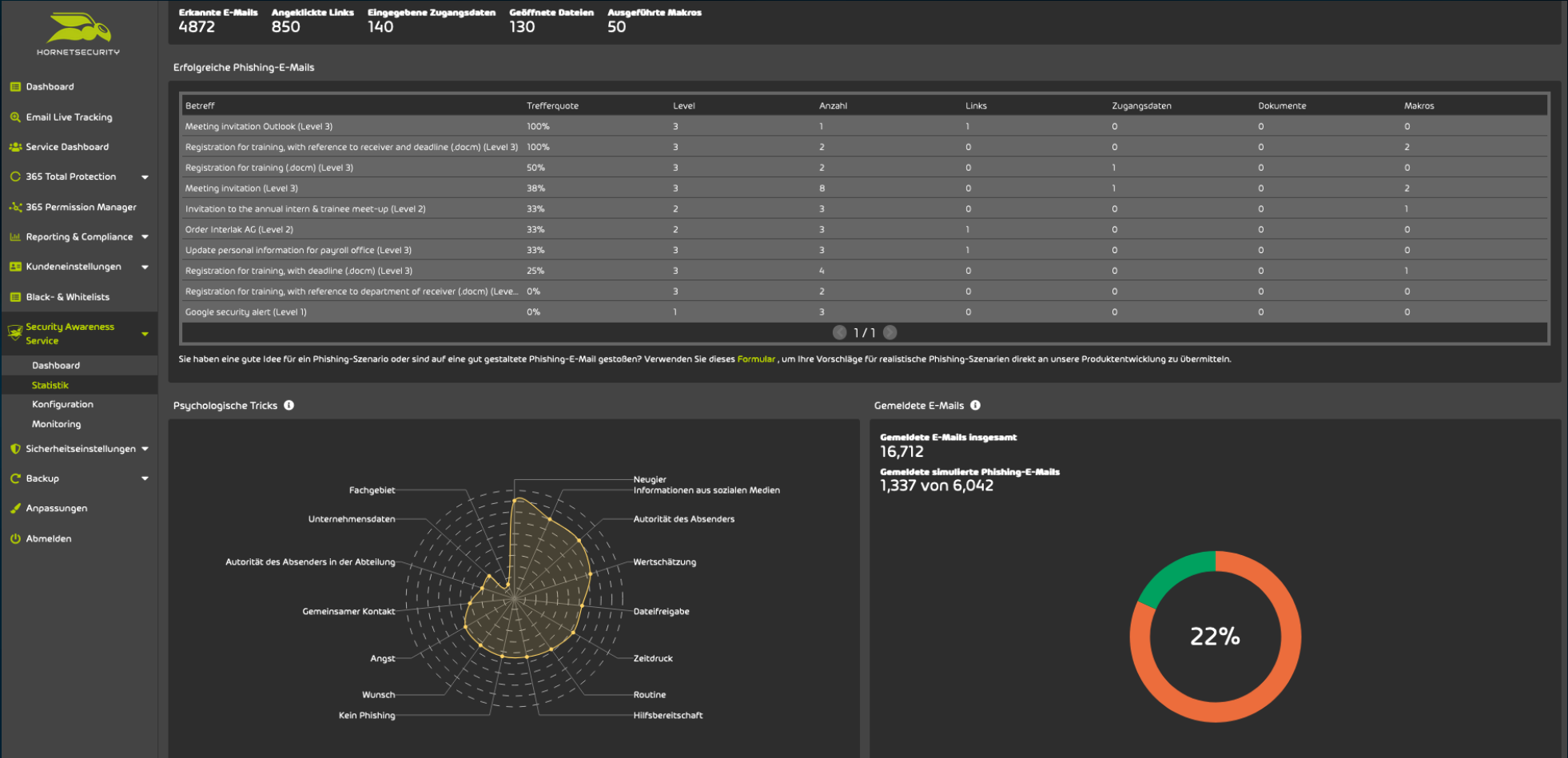
AWARENESS DASHBOARD IM CONTROL PANEL

- 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

AWARENESS DASHBOARD IM CONTROL PANEL



AWARENESS DASHBOARD IM CONTROL PANEL



HORNETSECURITY


HORNETSECURITY

Dashboard

Email Live Tracking

Service Dashboard

365 Total Protection

365 Permission Manager

Reporting & Compliance

Kundeneinstellungen

Black- & Whitelists

Security Awareness Service

Dashboard

Statistik

Konfiguration

Monitoring

Sicherheitseinstellungen

Backup

Anpassungen

Abmelden

SECURITY AWARENESS SERVICE - KONFIGURATION

Security Awareness Service aktivieren

Benutzer und Gruppen

Phishing-Simulation

E-Training

Phishing-Simulation aktivieren (inklusive patentierter Spear-Phishing-Engine)

Die Spear-Phishing-Engine versendet realistische und personalisierte Spear-Phishing-E-Mails mit steigendem Schwierigkeitsgrad. Wir empfehlen Ihnen, die Phishing-Simulation aktiviert zu lassen.

GRUNDLEGENDE EINSTELLUNGEN FÜR DIE PHISHING-SIMULATION

Beginn der Phishing-Simulation

10.05.2023

Frequenz der simulierten Phishing-E-Mails

Automatisch

Benutzerdefiniert

Niedrig (etwa 1 E-Mail pro Monat)

Allgemeine Einstellungen

Datenschutzmodus

Auswertung den Benutzern zur Verfügung stellen

Einstellungen des Phishing Reporters

Phishing Reporter

Herunterladen

Besondere Arten von simulierten Phishing-E-Mails

Anhänge

Makros

Phishing nach Zugangsdaten

Domain-Spoofing

Deaktivierte Simulationsszenarien

None

ORGANISATIONSEINSTELLUNGEN

Name

Anrede

Vorname

Sprache

Wählen Sie eine Sprache aus

Art der Organisation

Unternehmen

Behörde

Änderungen verwerfen

Speichern

Auswertung der Daten der Organisation auf Kununu

URL der Kununu-Seite ihrer Organisation

Speichern

KONFIGURATION DER INFRASTRUKTUR

Damit die Phishing-Simulation ordnungsgemäß funktioniert, darf die Infrastruktur des Kunden simulierte Phishing-E-Mails weder abfangen noch damit interagieren. Um zu prüfen, ob die Infrastruktur richtig konfiguriert ist, können Sie eine Test-E-Mail an einen Benutzer des Kunden senden. Die Konfiguration ist korrekt, falls keine Interaktion mit der Test-E-Mail stattgefunden hat, wenn sie vom Benutzer empfangen wird.

Erweiterte Zustellung von simulierten Phishing-E-Mails in Microsoft 365 Defender aktivieren

+ Test-E-Mail senden

E-Mail-Adresse	Datum und Uhrzeit	Gesendet	Empfangen	Interagiert
----------------	-------------------	----------	-----------	-------------

ENTSCHEIDENDE FAKTOREN FÜR EIN ERFOLGREICHES AWARENESS TRAINING

► Entscheidende Faktoren:

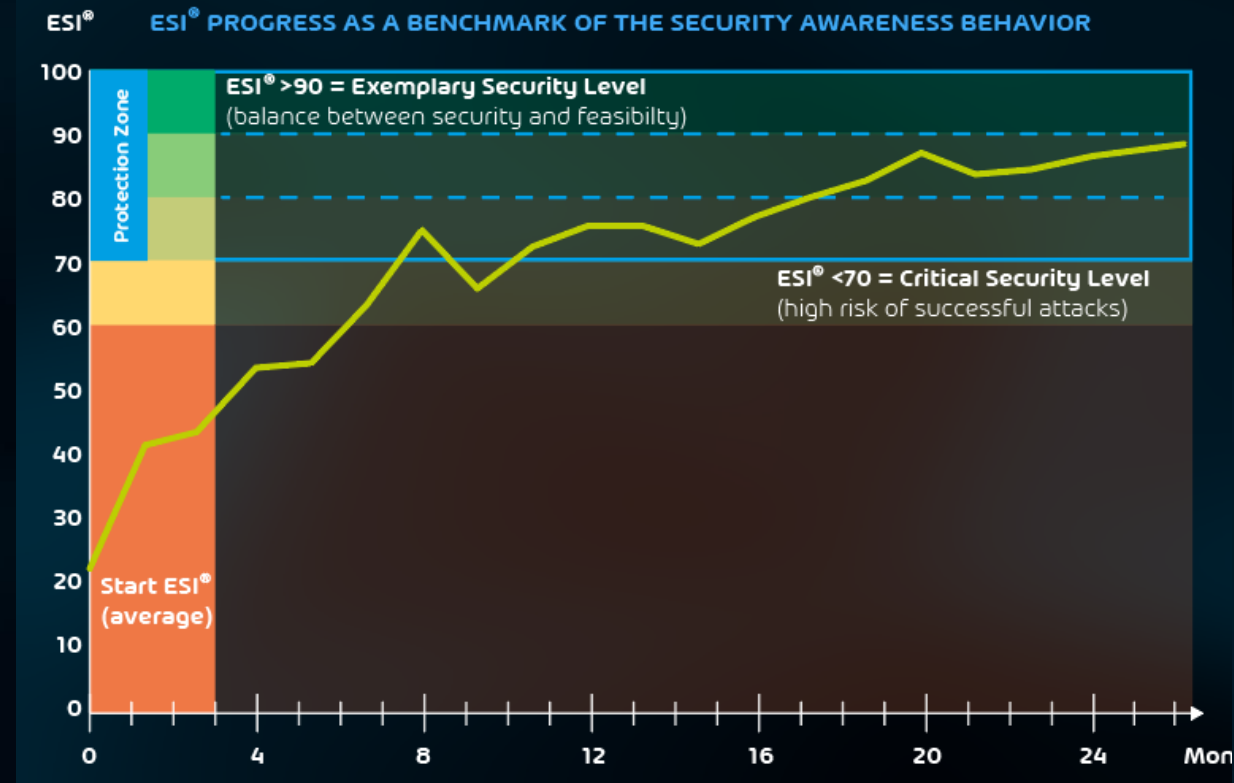
- Realitätsnah: Vorgehen wie ein echter Angreifer
- Messbar: für Ihren garantierten Erfolg
- Effizient: Individuell und bedarfsgerecht
- Wirksam: Selbstbestimmtes Trainieren & Lernen mit Fun Faktor



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.



ENTSCHEIDENDE FAKTOREN FÜR EIN ERFOLGREICHES AWARENESS TRAINING

👁 Entscheidende Faktoren:

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



HORNETSECURITY

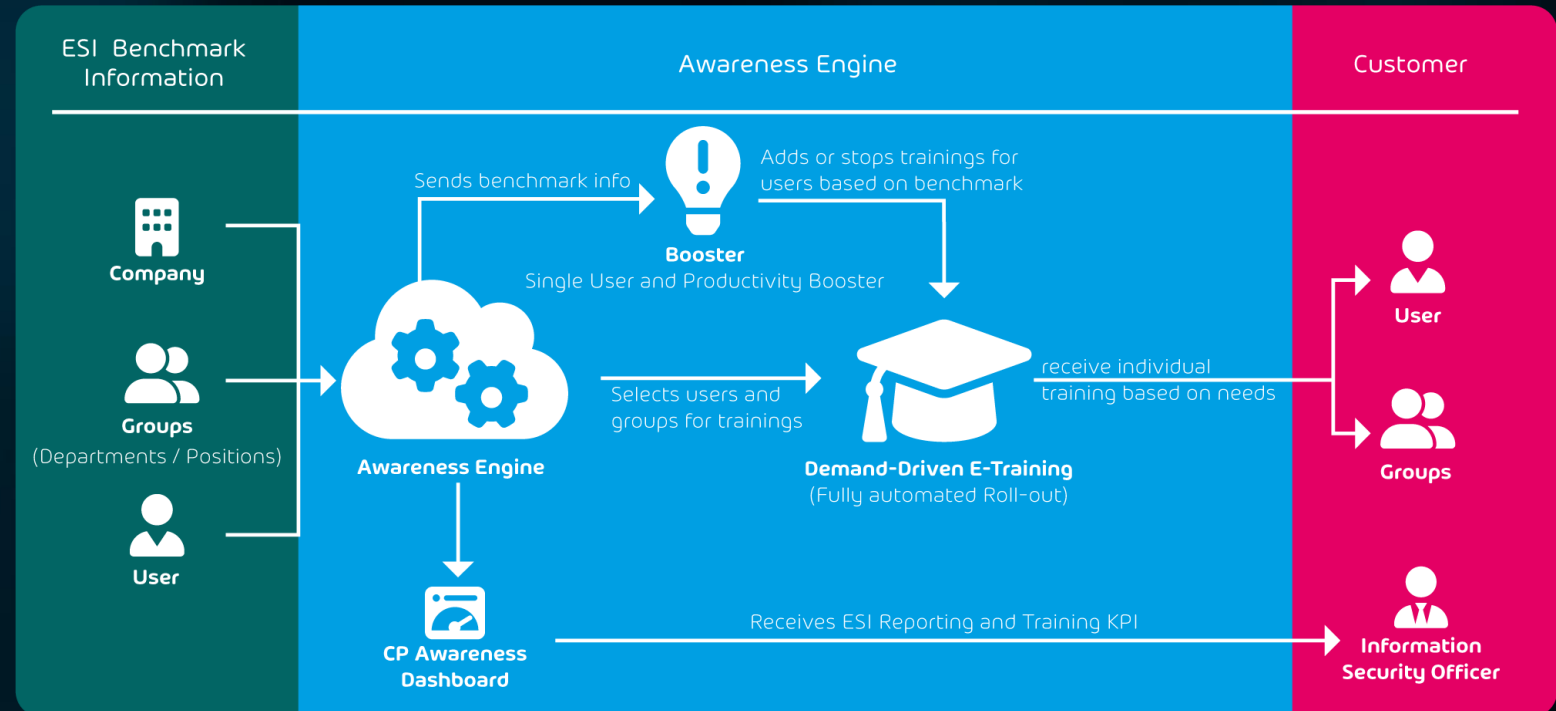
AWARENESS ENGINE

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



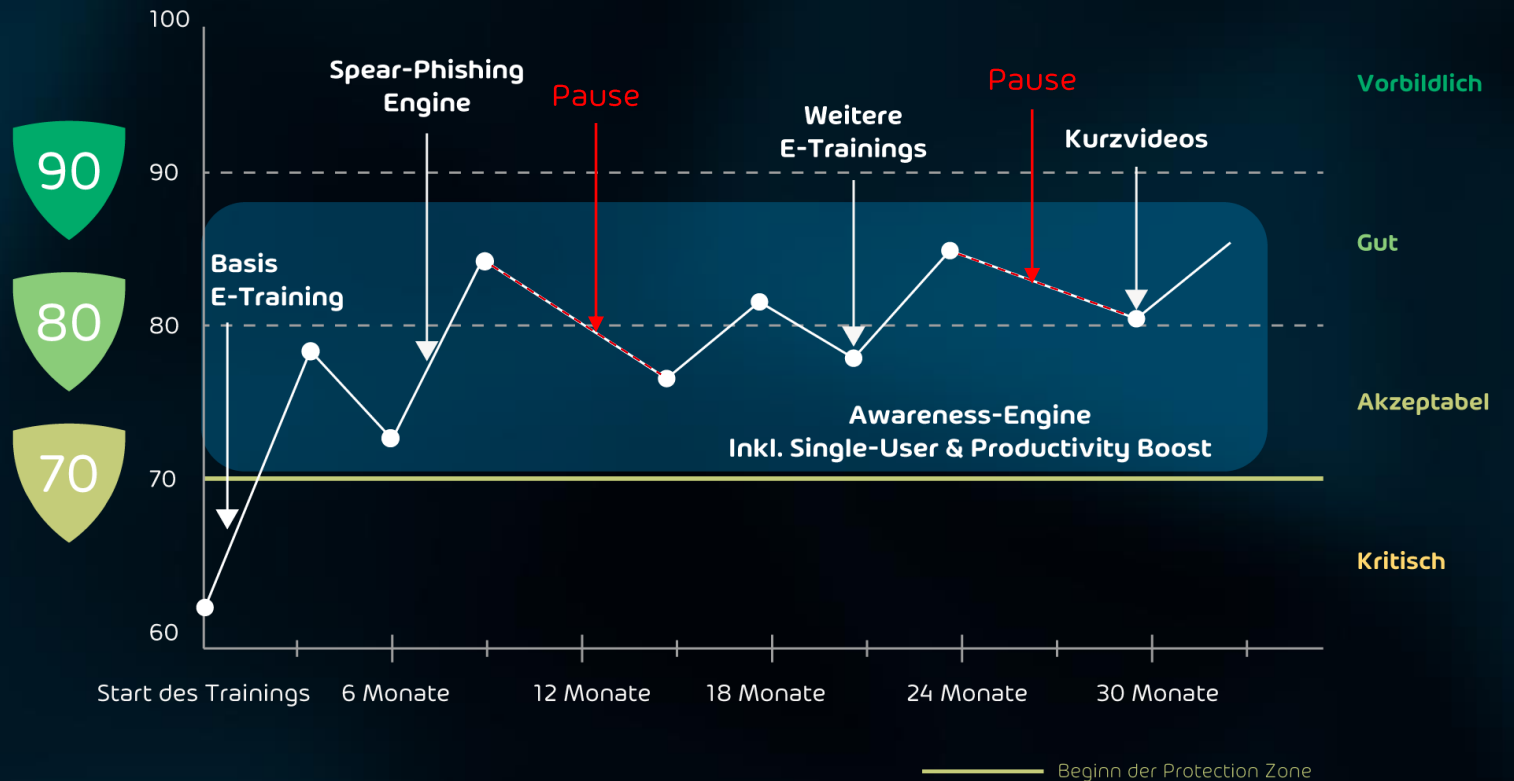
HORNETSECURITY

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.



ENTSCHEIDENDE FAKTOREN FÜR EIN ERFOLGREICHES AWARENESS TRAINING

► Entscheidende Faktoren:

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

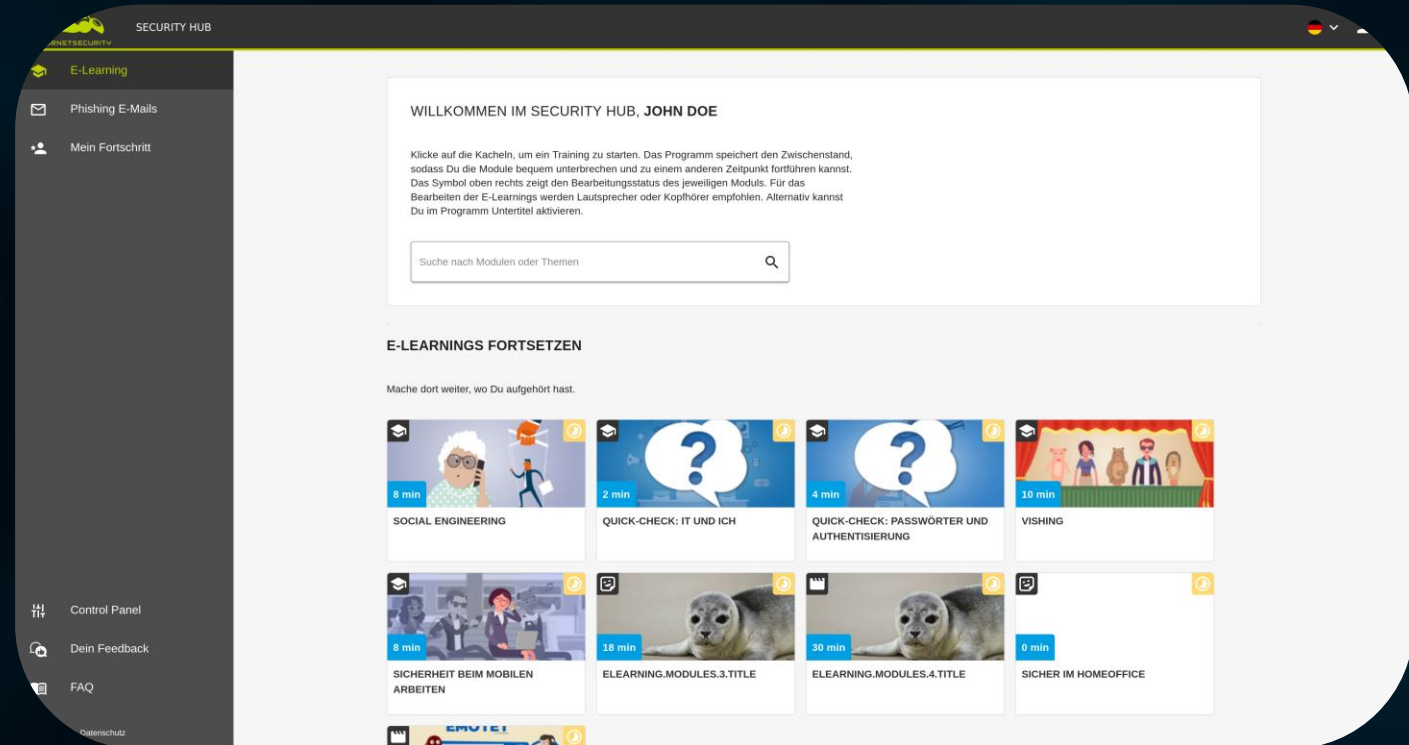


HORNETSECURITY

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



HORNETSECURITY

SECURITY HUB

SCHAFFEN SIE EINE MOTIVIERENDE LERNUMGEBUNG FÜR IHRE BENUTZER



HORNETSECURITY

 SECURITY HUB

 E-Learning

 Phishing E-Mails

 Control Panel

[Impressum](#) [Datenschutz](#)

PHISHING E-MAILS

Im Rahmen der Simulation wurden Dir eine oder mehrere Phishing-E-Mails zugeschickt. Welche hast Du *erkannt*, welche auch *gemeldet* und auf welche bist Du *hereingefallen*? Das siehst Du hier in der Übersicht.

PHISHING E-MAIL AUSWERTUNG

Wie viele Phishing-E-Mails wurden an Dich versandt? Und wie hast Du auf die E-Mails reagiert? Hier siehst Du die Zusammenfassung.

hereingefallen: 54

erkannt: 8

gemeldet: 0

62

Insgesamt versendete E-Mails

DEINE PHISHING E-MAILS

Hier siehst Du den Verlauf der Phishing-E-Mails, die im Rahmen der Simulation an Dich versandt wurden. Klicke auf einen Eintrag, um nähere Erläuterungen aufzurufen. Über den Filter kannst Du den Verlauf einschränken.

Filter

hereingefallen

erkannt

gemeldet

Januar 2023

 Versendet am: 16.01.2023

Pending messages



MANIPULATIVE TRICKS

Kriminelle versuchen Dich durch manipulative Tricks zur Reaktion auf Phishing-E-Mails zu bewegen. Auf welche Tricks bist Du besonders häufig hereingefallen? Klicke auf die Tricks für mehr Informationen.

18 Neugier

15 Zeitdruck

11 Angst

ENTSCHEIDENDE FAKTOREN FÜR EIN ERFOLGREICHES AWARENESS TRAINING

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



HORNETSECURITY

THANK YOU!



HORNETSECURITY



HORNETSECURITY