Security Awareness

Sicherheitsbewusstsein im digitalen Zeitalter

Günther Rohrecker
Chief Sales Officer
g.rohrecker@conova.com
+43 676 83050 343

Markus Todt
Country Manager Austria
todt@hornetsecurity.com
+43 664 1114071

CONOVA

HORNETSECURITY

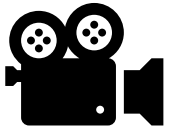
Herzlich Willkommen bei conova communications!

CONOVA

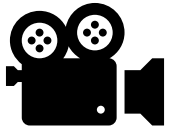
CONOVA – MEHR ALS EIN RECHENZENTRUM

Wir betreiben Ihre **Server und Applikationen hochverfügbar und sicher** in unseren **eigenen Rechenzentren** oder in einer Public Cloud.

Unternehmenspräsentation



Imagevideo



DCs Hallein

CONOVA


>110
Spezialisten
EN50600
zertifizierte
Data Center
>30
Jahre
am Markt
>90.000
Echtzeitwerte
im Monitoring
2
starke
Eigentümer
100%
Rechenzentrum
Verfügbarkeit
bis zu
100%
Datenhaltung
in Österreich
+24
Mio. Umsatz
>1.000
aktive Kunden
24x7
Service
ISO27001
zertifiziertes
Unternehmen
CONOVA

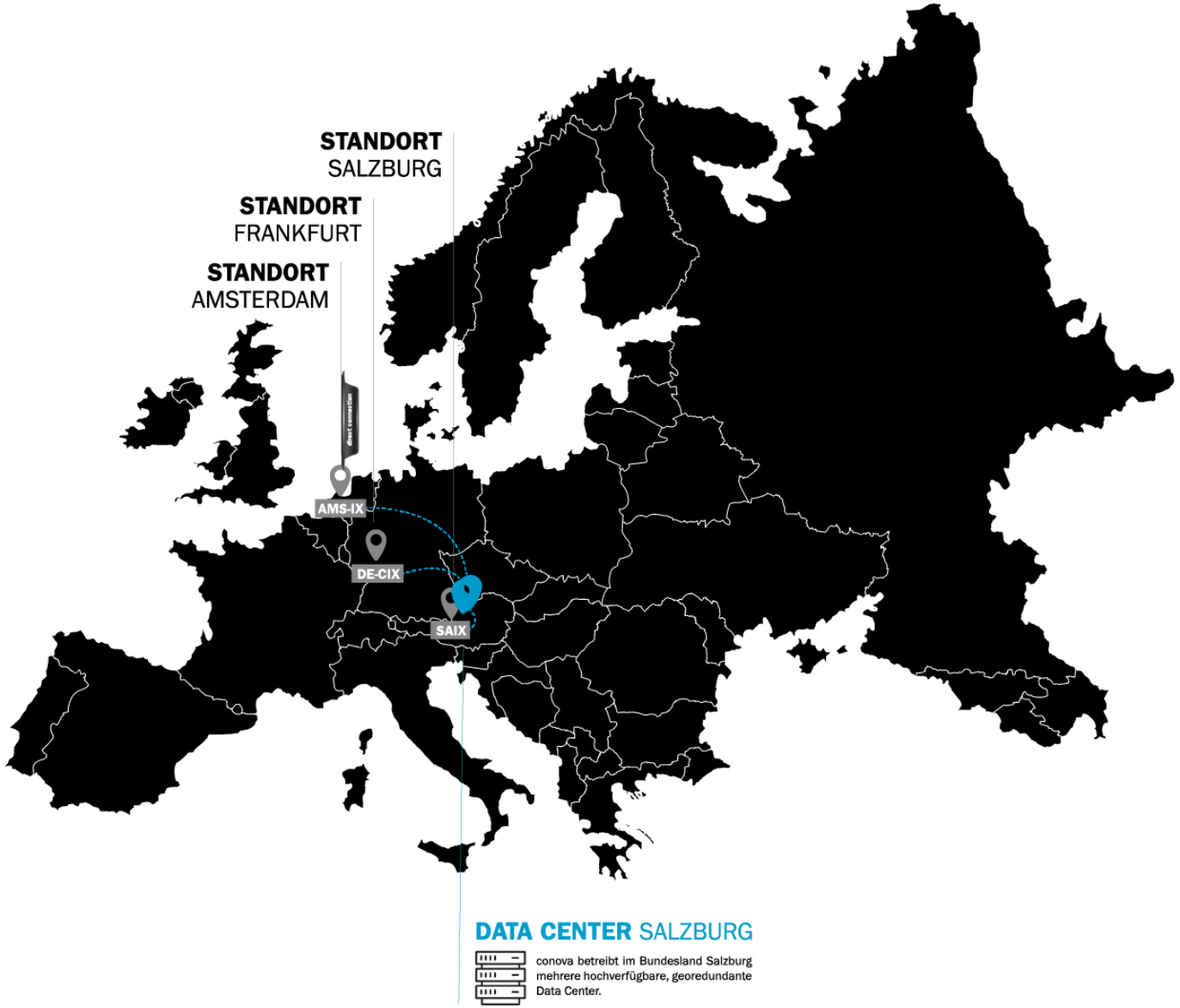
STANDORTE – vollständige Georedundanz

Salzburg City: Data Center 4 & 5 in Maxglan

Salzburg South: Data Center 6 & 7 in Hallein

CONOVA

WEITERE STANDORTE



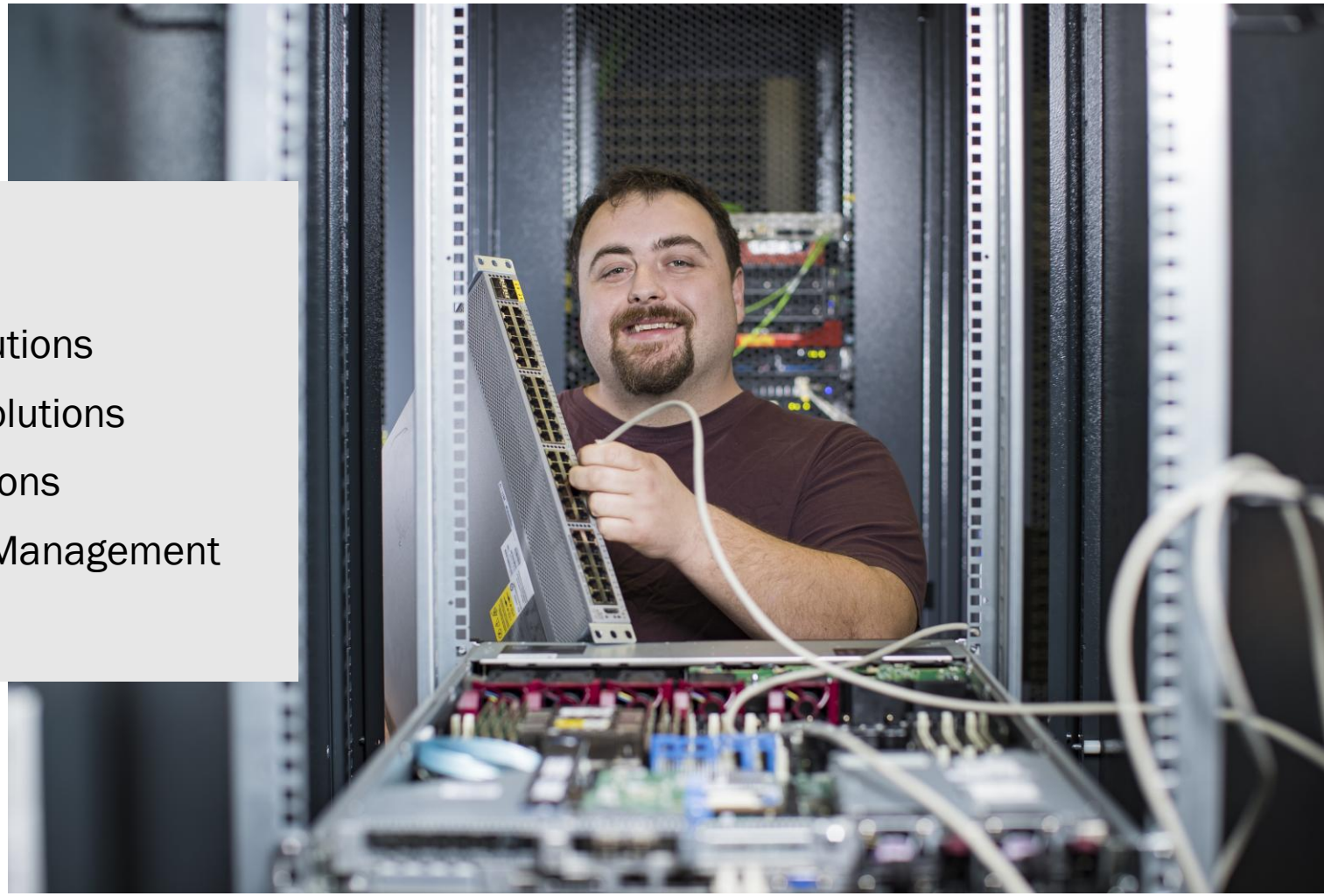
DATA CENTER SALZBURG

conova betreibt im Bundesland Salzburg mehrere hochverfügbare, georedundante Data Center.

CONOVA

KOMPETENZ^5

- Microsoft & Datacenter Solutions
- Linux & Open Technology Solutions
- Network & IT Security Solutions
- Service Level & Availability Management
- IT Helpdesk

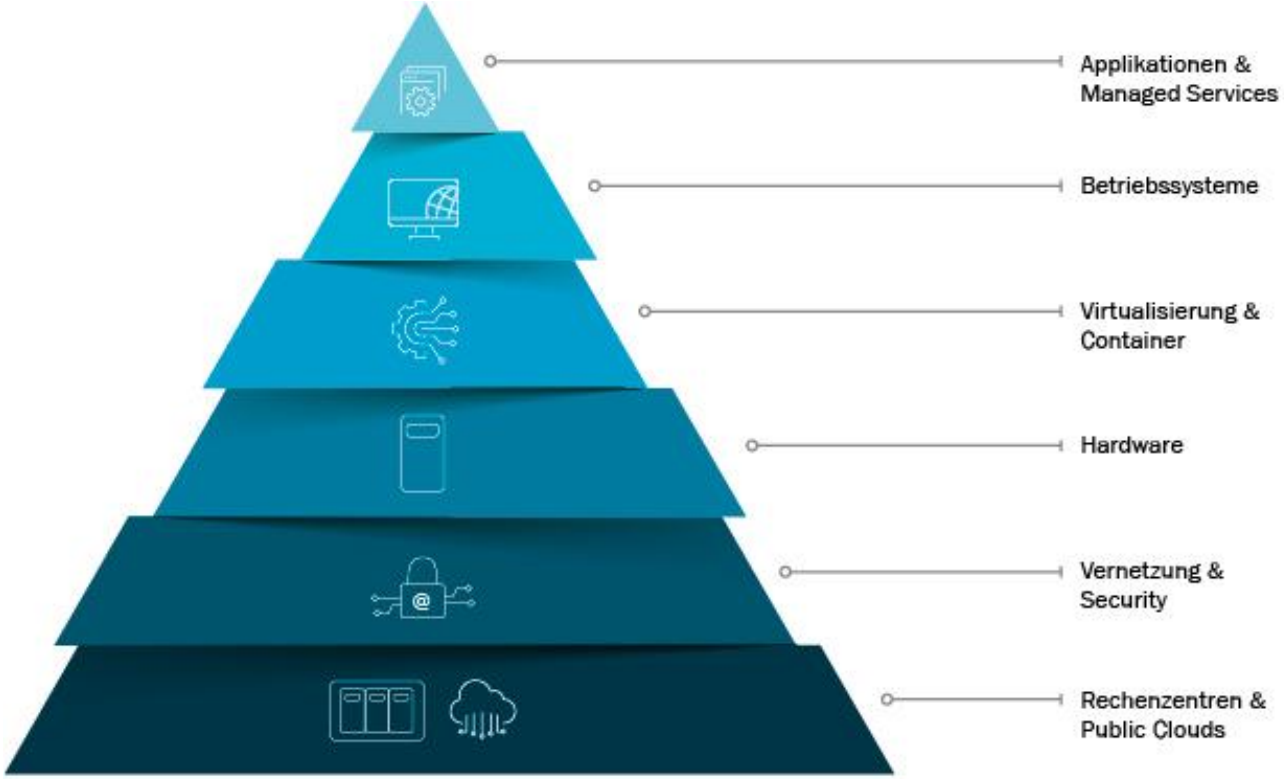


CONOVA

UNSERE DIENSTLEISTUNGSPYRAMIDE

FULL STACK

- Infrastructure as a Service
- Platform as a Service
- Software as a Service



CONOVA

Mail Security Services

- Premium Spam- und Virenschutz
- Advanced Threat Protection
- E-Mail Signatur / Verschlüsselung
- Revisionssichere E-Mail Archivierung
- Business Continuity Lösung

- **für M365/Hosted/On-Premise Mailserver**

TopAwareness
powered by Hornetsecurity

CONOVA

Zusammenarbeit conova - Hornetsecurity

- conova schließt Partnervertrag mit Hornetsecurity im Jahr 2009 (**vor 16 Jahren**!)
- Ablöse des eigenen Mail Security Produktes durch Spam- und Virenschutz von Hornetsecurity
- Know-how Transfer in beide Richtungen
- Einziger österreichischer Partner mit eigenen SV Appliances in den conova Rechenzentren
- Größter österreichischer Partner und einziger **Platinum Partner** in Österreich

CONOVA

GEMEINSAME REFERENZEN IM BUNDESLAND SALZBURG

- Porsche (37.000 User TopAwareness)
- EMCO
- Windhager (beide)
- ROCO Modelleisenbahnen
- Landeszahnärztekammer
- Voglauer Möbel
- Gebr. Limmert
- Sport Bründl
- Salzburger Land Tourismus

PORSCHE INFORMATIK

emco group
Designed for your profit

WINDHAGER HOME & GARDEN

windhager
BEST HEATING TECHNOLOGY

VOGLAUER

FLEISCHMANN Roco

Bründl SPORTS

Gebrüder LIMMERT Aktiengesellschaft

CONOVA

Stärken Sie Ihre Human Firewall

Security Awareness Service by Hornetsecurity

AUTOMATISIERT. VERHALTENSBASIERT. KONTINUIERLICHER SERVICE.

Markus Todt

- Country Manager Austria
- todt@hornetsecurity.com

HORNETSECURITY

Prok. Mag. Günther Rohrecker

- Chief Sales Officer
- g.rohrecker@conova.com

HORNETSECURITY ERFOLG IN ZAHLEN

700+
Mitarbeiter

3
Rechenzentren in Deutschland

75.000
Kunden in **120** Ländern

17
Büros

B2B
Channel Business

100%
DSGVO-konform

AKTUELLE MARKTLAGE

CYBER SECURITY MARKTLAGE

MICROSOFT 365 WÄCHST STETIG

Über 4 Millionen Unternehmen nutzen Microsoft Office 365**

400 Millionen zahlende Abonnenten im Jahr 2024*

Millionen von potenziellen Zielen für Cyberkriminelle

Microsoft haftet nicht für Schäden

z.B. Nutzungsausfall, Datenverlust oder entgangenem Gewinn.***

HORNETSECURITY

* office365itpros.com **statista.com/statistics/983321/worldwide-office-365-user-numbers-by-country ***Microsoft Services Agreement – https://www.microsoft.com/en-us/servicesagreement

CYBER SECURITY MARKTLAGE

MICROSOFT 365 WÄCHST STETIG

HORNETSECURITY

* office365itpros.com **statista.com/statistics/983321/worldwide-office-365-user-numbers-by-country ***Microsoft Services Agreement – https://www.microsoft.com/en-us/servicesagreement

CYBER SECURITY REPORT 2025

KLASSIFIZIERUNG VON UNERWÜNSCHTEN MAILS

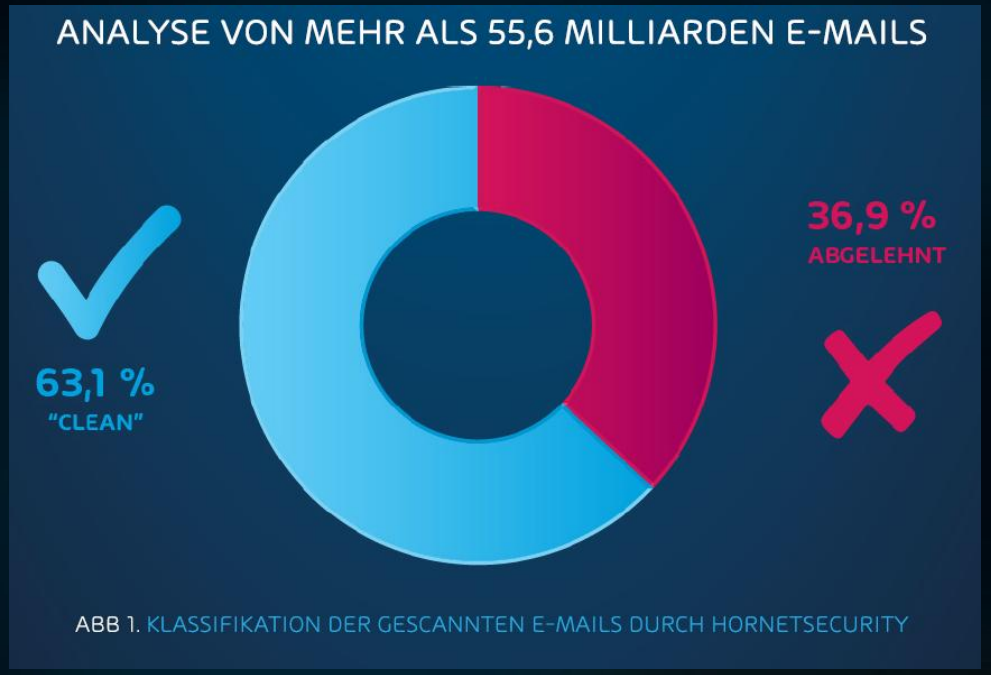


ABB 1. KLASSIFIKATION DER GESCANNTEN E-MAILS DURCH HORNETSECURITY

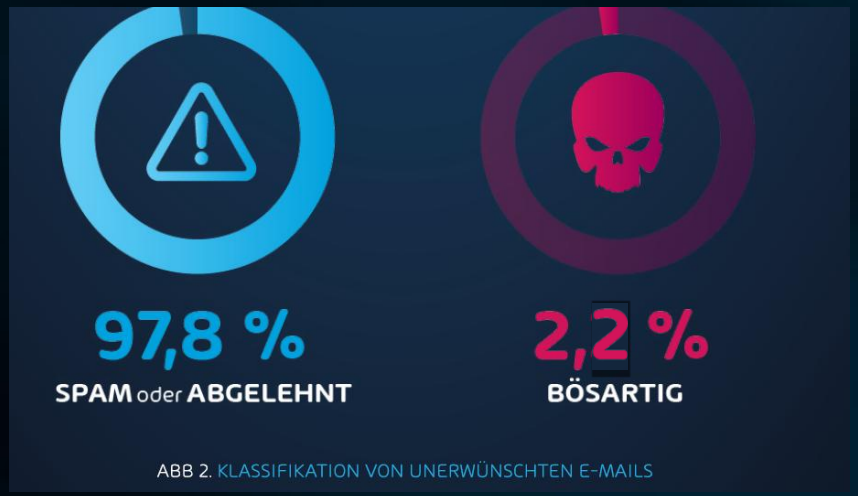


ABB 2. KLASSIFIKATION VON UNERWÜNSCHTEN E-MAILS

HORNETSECURITY

* office365itpros.com **statista.com/statistics/983321/worldwide-office-365-user-numbers-by-country ***Microsoft Services Agreement - https://www.microsoft.com/en-us/servicesagreement

CYBER SECURITY REPORT 2024

ERFOLGREICHE ANGRIFFSARTEN

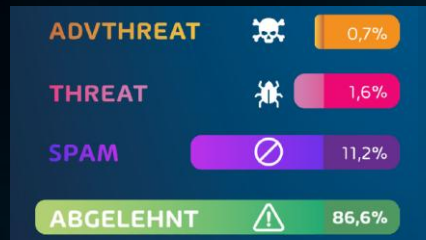
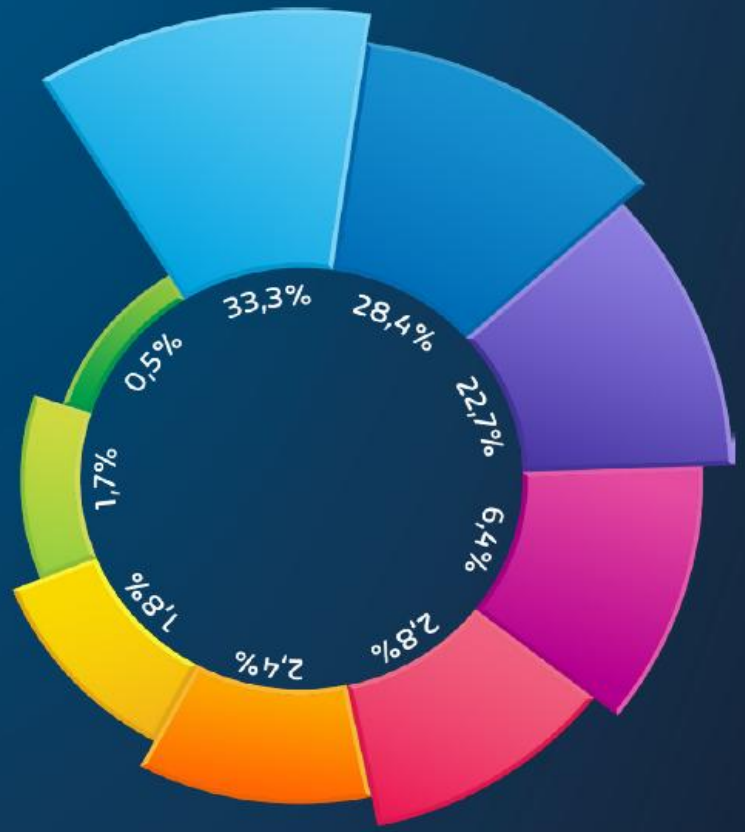


ABB 4. 2024 UNERWÜNSCHTE E-MAILS NACH KATEGORIE

KATEGORIE	BESCHREIBUNG
Spam	Diese E-Mails sind unerwünscht und enthalten oft Werbung oder betrügerische Inhalte. Die E-Mails werden gleichzeitig an eine große Anzahl von Empfängern gesendet.
Threat	Diese E-Mails enthalten schädliche Inhalte, z. B. bösartige Anhänge oder Links, oder sie werden zu kriminellen Zwecken wie Phishing verschickt.
AdvThreat	Advanced Threat Protection hat in diesen E-Mails eine Bedrohung erkannt. Die E-Mails werden für illegale Zwecke verwendet und beinhalten ausgeklügelte technische Mittel, die nur mit fortschrittlichen dynamischen Verfahren abgewehrt werden können.
Abgelehnt	Unser E-Mail-Server lehnt diese E-Mails direkt bei der ersten Verbindung vom sendenden E-Mail-Server aufgrund äußerer Merkmale wie der Identität des Absenders ab, und die E-Mails werden nicht weiter analysiert.



ANGRIFFSTECHNIK

PHISHING	33.3%
„ANDERE“	28.4%
URL	22.7%
VORKASSEBETRUG	6.4%
ERPRESSUNG	2.8%
.EXE IN DISK IMAGE / ARCHIV	2.4%
IDENTITÄTSDIEBSTAHL	1.8%
HTML	1.7%
MALDOC	0.5%

ABB 5. ANGRIFFSTECHNIKEN BEI E-MAIL-ANGRIFFEN IM JAHR 2024

HORNETSECURITY

* office365itpros.com **statista.com/statistics/983321/worldwide-office-365-user-numbers-by-country ***Microsoft Services Agreement - https://www.microsoft.com/en-us/servicesagreement

CYBER SECURITY PHISHING 2025

ERFOLGREICHE ANGRIFFSARTEN

kaernten ORF.at

Kärnten-News | Radio Kärnten | Fernsehen | Landesstudio | Bachmannpreis | Volksgruppen | Ganz Österreich

CHRONIK

Zehntausende Euro an Betrüger überwiesen

Eine Firma aus dem Bezirk Klagenfurt-Land ist Onlinebetrügern aufgesessen. Mehrere zehntausend Euro wurden laut Polizei an eine rumänische Firma überwiesen. Wie sich später herausstellte, handelte es sich um eine Betrugsmasche, mit der noch mehr Geld von der Firma herausgelockt werden hätte sollen.

Online seit gestern, 19.34 Uhr

Teilen

Anfang März erhielt die Firma per E-Mail eine Rechnung von der rumänischen Firma über bestellte Ware im Wert von mehreren zehntausend Euro. Weil von dieser seit Jahren regelmäßig Ware bestellt wird fiel der Schwindel zunächst nicht auf.

Imago Images/Imaginechina-Tuchong

Polizei warnt vor „Phishing-Fallen“ in ganz Österreich

Eine österreichweit agierende Tätergruppe dürfte Anfang Jänner mit „Phishing-Fallen“ wohl gleich mehrere Männer und Frauen über den Tisch gezogen haben.

31. Jänner 2025, 14.40 Uhr

Teilen

APA/ZB/Jens Büttner

Unter den Opfern ist auch eine 36-jährige Südoststeirerin: Sie hatte am 7. Jänner angezeigt, dass sie über eine SMS auf eine täuschend echt aussehende Internetseite ihrer Bank gelockt wurde und mittels QR-Code persönliche Daten eingab. Danach wurde von Wien aus von ihrem Konto Geld behoben, hieß es am Freitag seitens der Polizei.

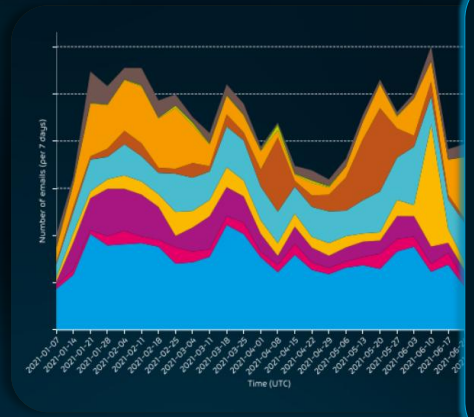
Mit QR-Code in die Falle gelockt

Es stellte sich heraus, dass die Steirerin wohl nicht das einzige Betrugsopfer der Tätergruppe gewesen sein dürfte: Gleich gelagerte Fälle wurden auch in Wien, Oberösterreich und Salzburg gemeldet. Ein Zusammenhang könnte bestehen, so die Ermittler. Es wird davon ausgegangen, dass es noch weitere Fälle in Österreich geben könnte. Mit Bildern aus Überwachungskameras jener Bankautomaten, wo Geld von den Opfern behoben wurde, wird nun nach den Verdächtigen gesucht.

red, help.ORF.at/Agenturen

HORNETSECURITY

HORNETSECURITY SECURITY LAB



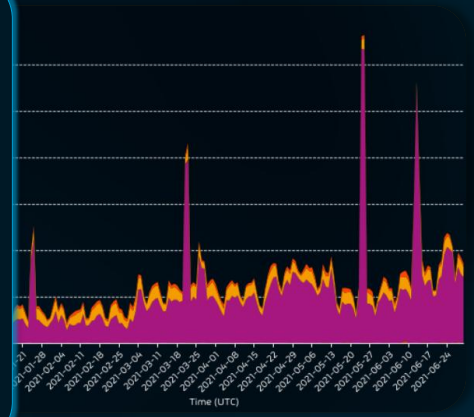
Exklusive Zahlen & Fakten

2,3 Milliarden E-Mails pro Tag analysiert

12,996 Ransomware-Angriffe pro Stunde

361 "komplexe" Phishing-Angriffe pro Minute

8 Multi-Vektor-Betrugsangriffe pro Minute



>50
Mitarbeiter in Hannover

24/7
Überwachung der Erkennungs-mechanismen

Team aus internationale IT-Security Spezialisten

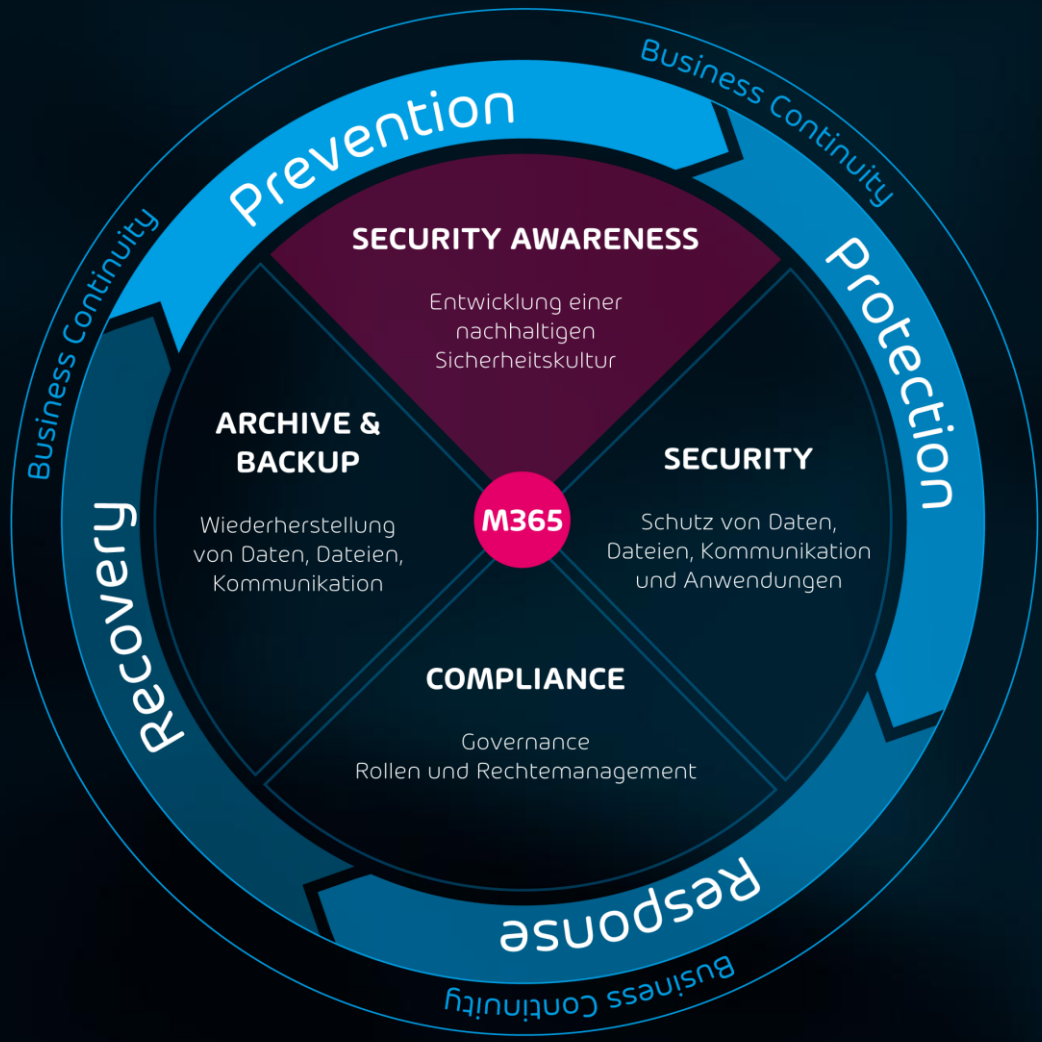
Monthly Threat Report & Security Trends

Abb. 1 & 2: Grafiken zu unterschiedlichen E-Mail Bedrohungen aus dem Hornetsecurity Security Lab

NEU: NEXT-GEN SECURITY AWARENESS SERVICE

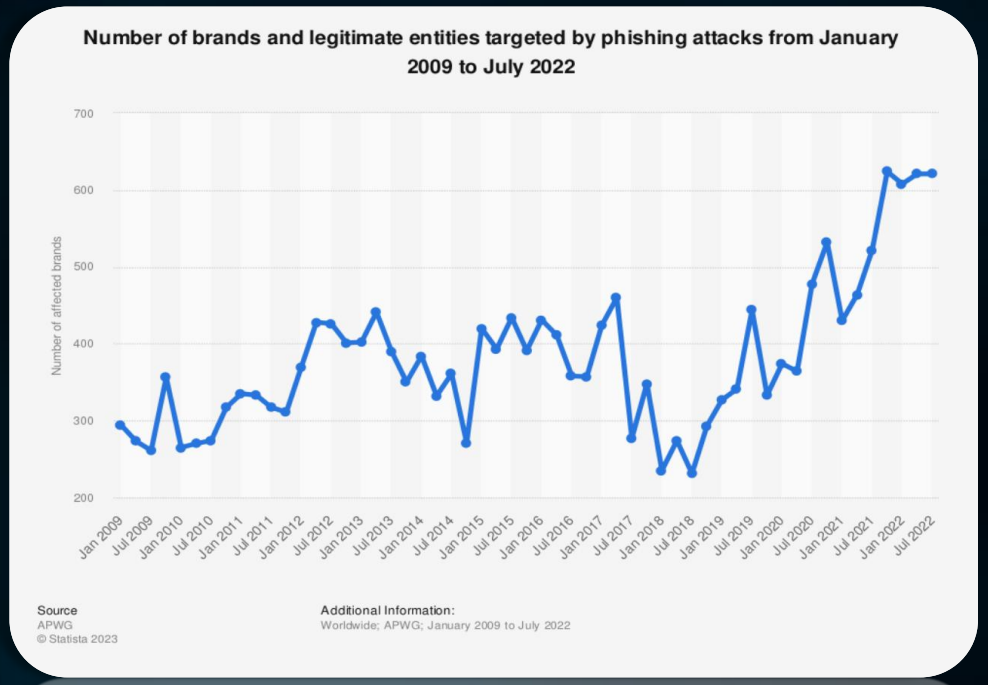
HORNETSECURITY

SECURITY AWARENESS SERVICE



PHISHING BLEIBT GRÖSSTER

RISIKOFAKTOR



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

95% aller Cybersicherheits-vorfälle sind auf menschliches Fehlverhalten zurückzuführen

HORNETSECURITY

WARUM IST SECURITY AWARENESS SO WICHTIG?

DESHALB REICHEN REIN TECHNISCHE MASSNAHMEN ALLEIN NICHT AUS. Einige Beispiele:

- Mitarbeiter greifen auf Geschäftsanwendungen über eigene, unzureichend gesicherte Geräte und Räumlichkeiten zu, z. B. im Home-Office

HORNETSECURITY

- Sie nutzen geschäftliche Geräte, um privat im Netz zu surfen oder E-Mails abzurufen
- Sie erhalten Phishing-Anrufe und werden auf sozialen Netzwerken von Fake-Profilen kontaktiert
- Sie überschätzen ihre eigenen Fähigkeiten, sich vor Cyber-Angriffen zu schützen

- Sie wissen nicht, was sie tun sollen, wenn sie einen Sicherheitsvorfall beobachten

PLAN 4

SECURITY AWARENESS SERVICE

NACHHALTIGE SICHERHEITSKULTUR

MINDSET

Motivation und offene Kommunikation

- Verständnis für Bedrohungslage
- Eigenverantwortung betonen

SKILLSET

Fähigkeiten und Wissen aneignen

- Phishing-Simulation
- E-Learning
- Kurzvideos
- Quizze

TOOLSET

Aktiv ins Geschehen eingreifen

- Live-Dashboard
- Reporter-Button
- Weiterleitungsfunktion

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

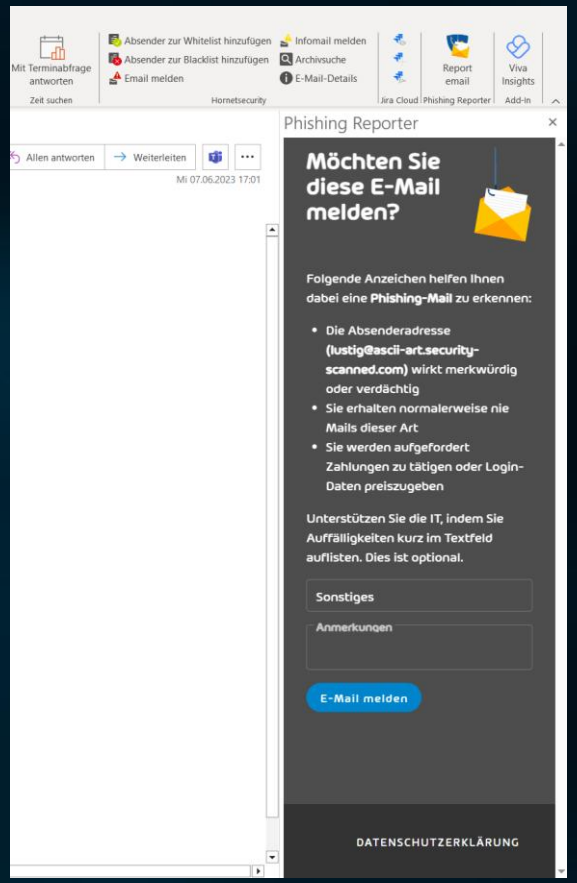
Cyber-Angriffe auf Unternehmen sind ein wiederkehrendes Übel. Aber wieso eigentlich? Wie so oft in der IT, sitzt die Antwort vor dem Bildschirm.

HORNETSECURITY

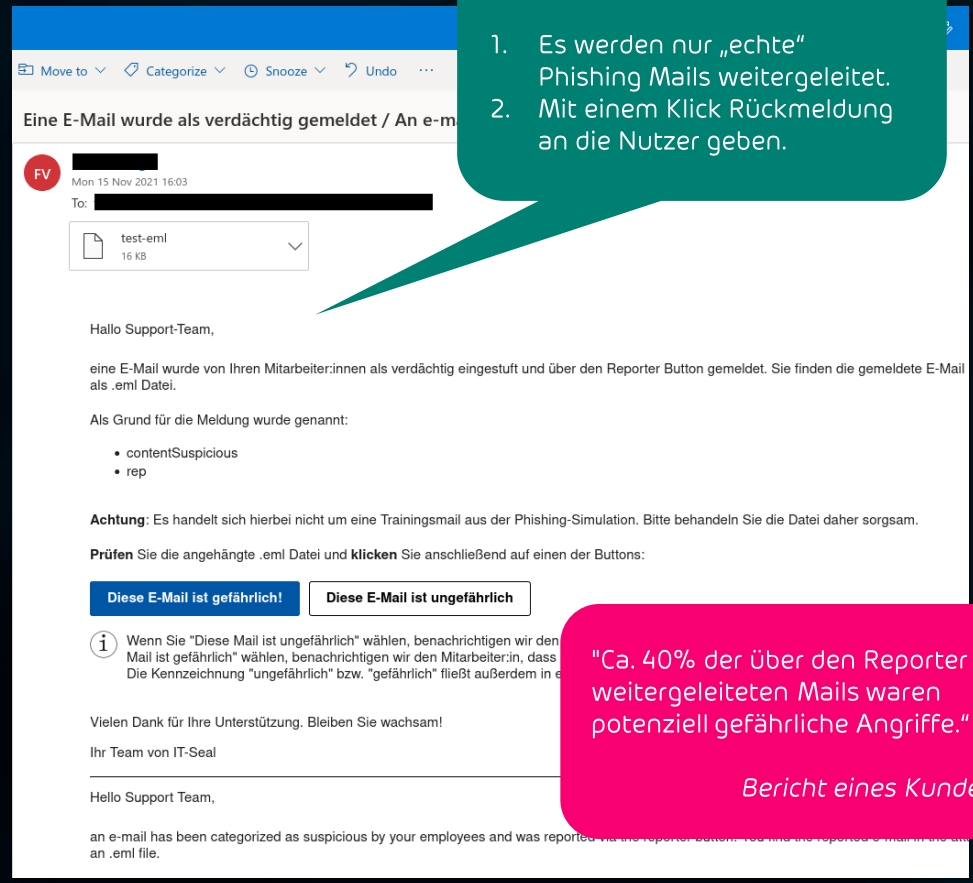
REPORTER BUTTON (OUTLOOK-ADD-IN)

HORNETSECURITY

Benutzer



IT-Support



Spart der IT doppelt Zeit:

1. Es werden nur „echte“ Phishing Mails weitergeleitet.
2. Mit einem Klick Rückmeldung an die Nutzer geben.

"Ca. 40% der über den Reporter weitergeleiteten Mails waren potenziell gefährliche Angriffe."

Bericht eines Kunden

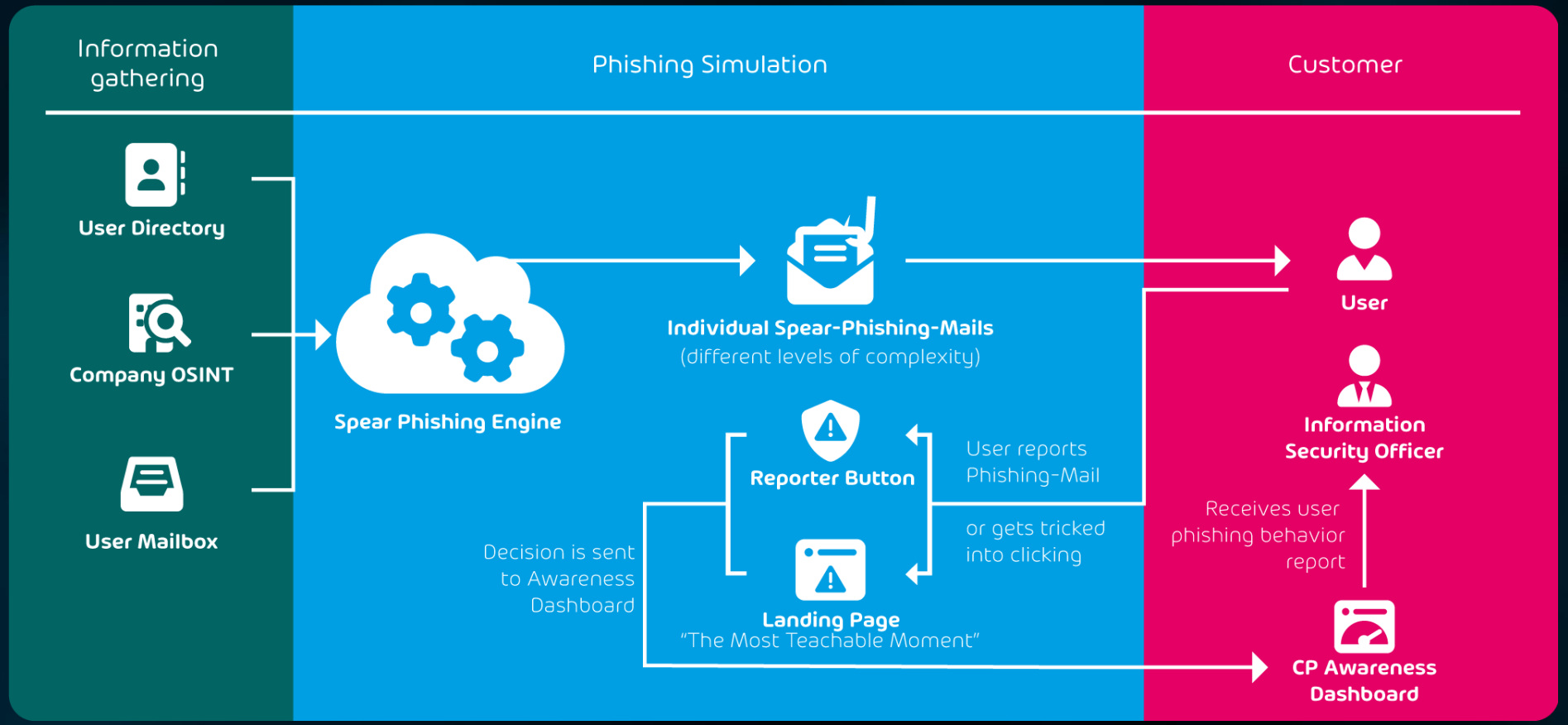
ENTSCHEIDENDE FAKTOREN FÜR EIN ERFOLGREICHES AWARENESS TRAINING

- 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

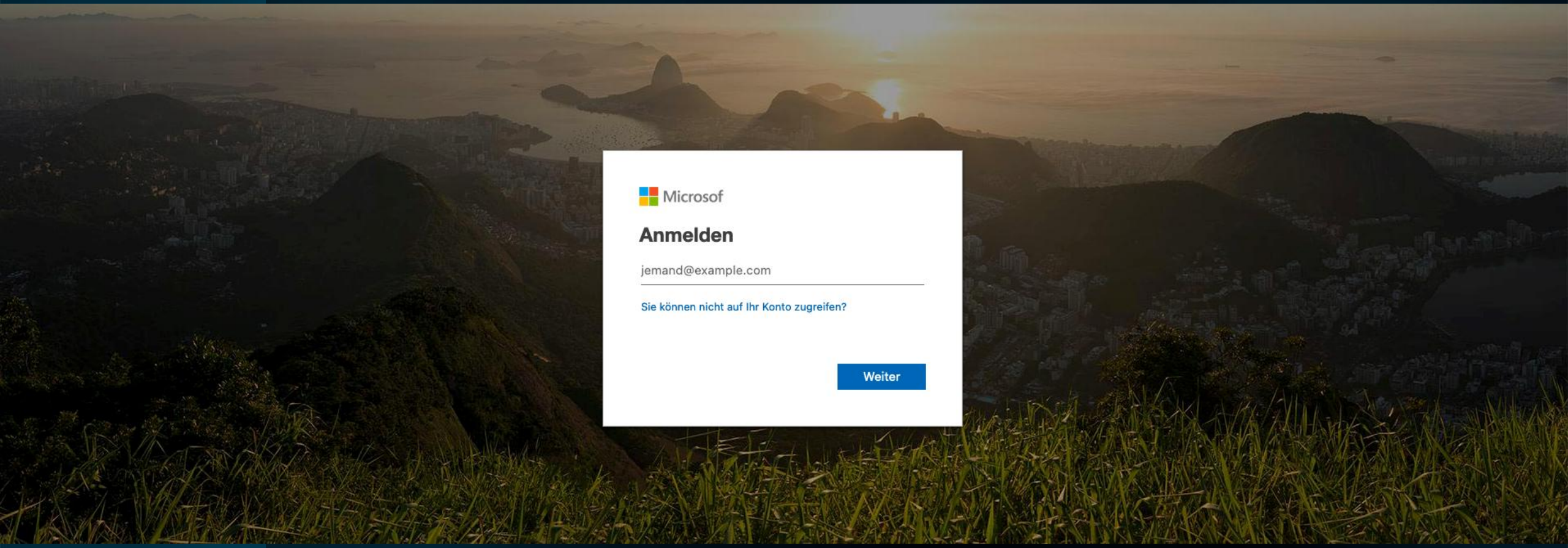
PATENTIERTE SPEAR-PHISHING-ENGINE

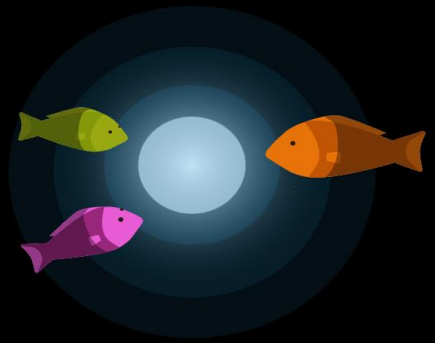
ABLAUF DER SPEAR-PHISHING-SIMULATION



PATENTIERTE SPEAR-PHISHING-ENGINE

PATENTIERTE SPEAR-PHISHING-ENGINE





THAT WAS LUCKY!

This could have been a phishing email!

Three easy steps for recognising a phishing email:

Watch now

approx 30 seconds

Your participation is 100% anonymous!

Nobody receives any information about who opened which email or clicked on which link. The training serves to teach you about how to deal fraud attempts.

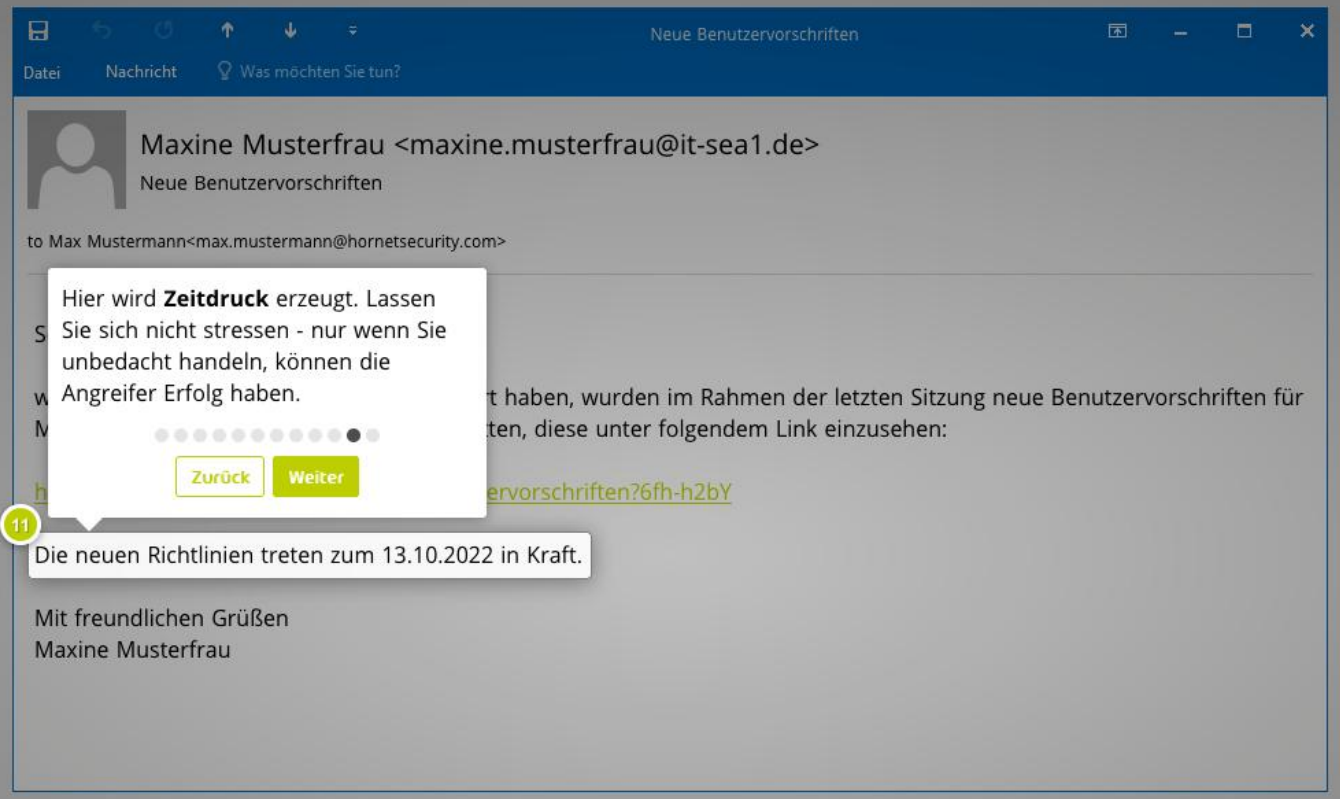
Protection against cyber-criminal

Cyber-attacks are often tailored to your organisation or to you personally. Stay alter to protect yourself and your organisation from fraud, swindles and far-reaching consequences.

The logo of a third party that might be used in the phishing simulation is only used for illustrative or didactic purpose. There is no connection with the trademark owner.

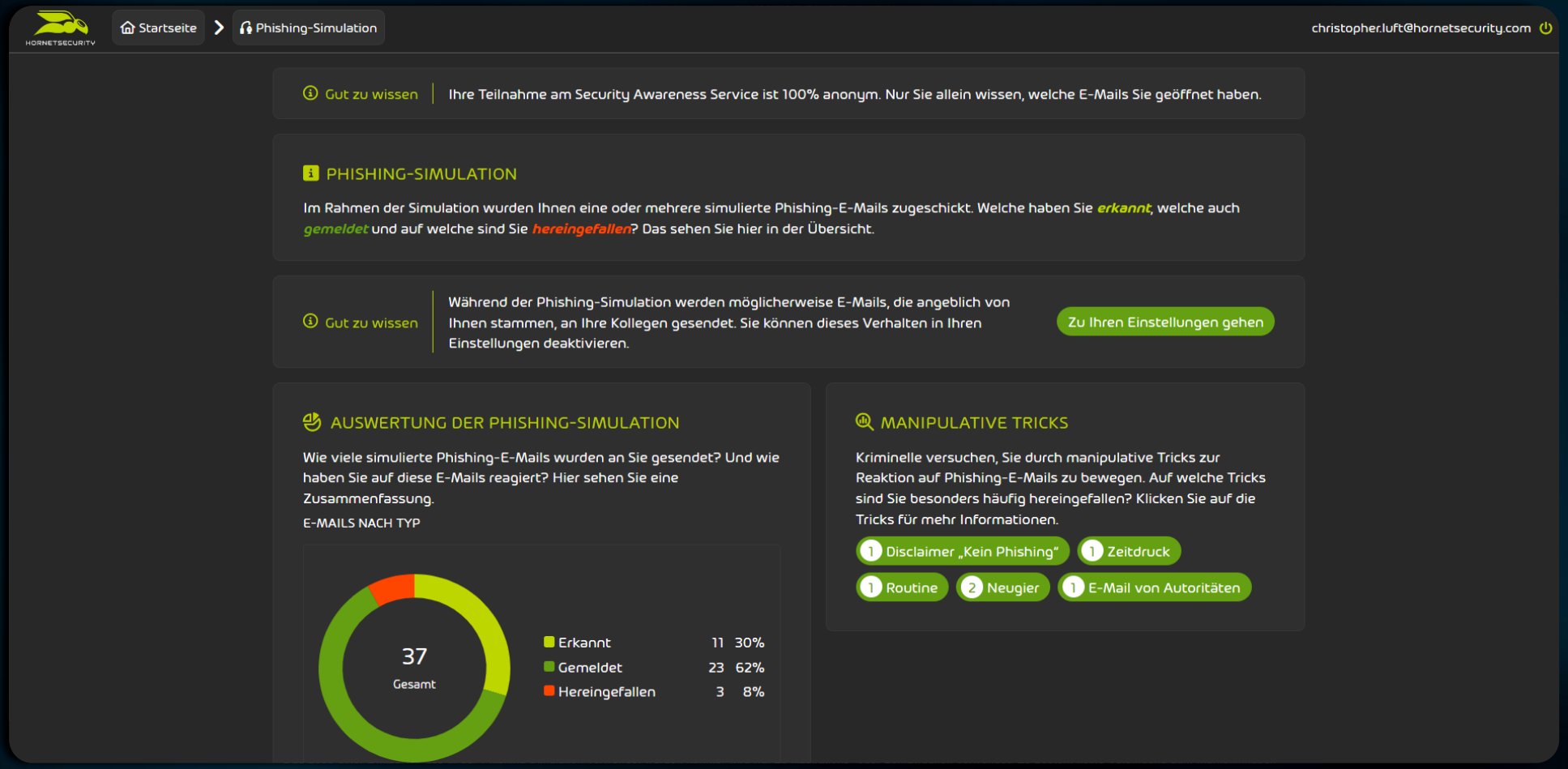
Legal notice | Data protection

PATENTIERTE SPEAR-PHISHING-ENGINE



SPEAR-PHISHING-ENGINE®

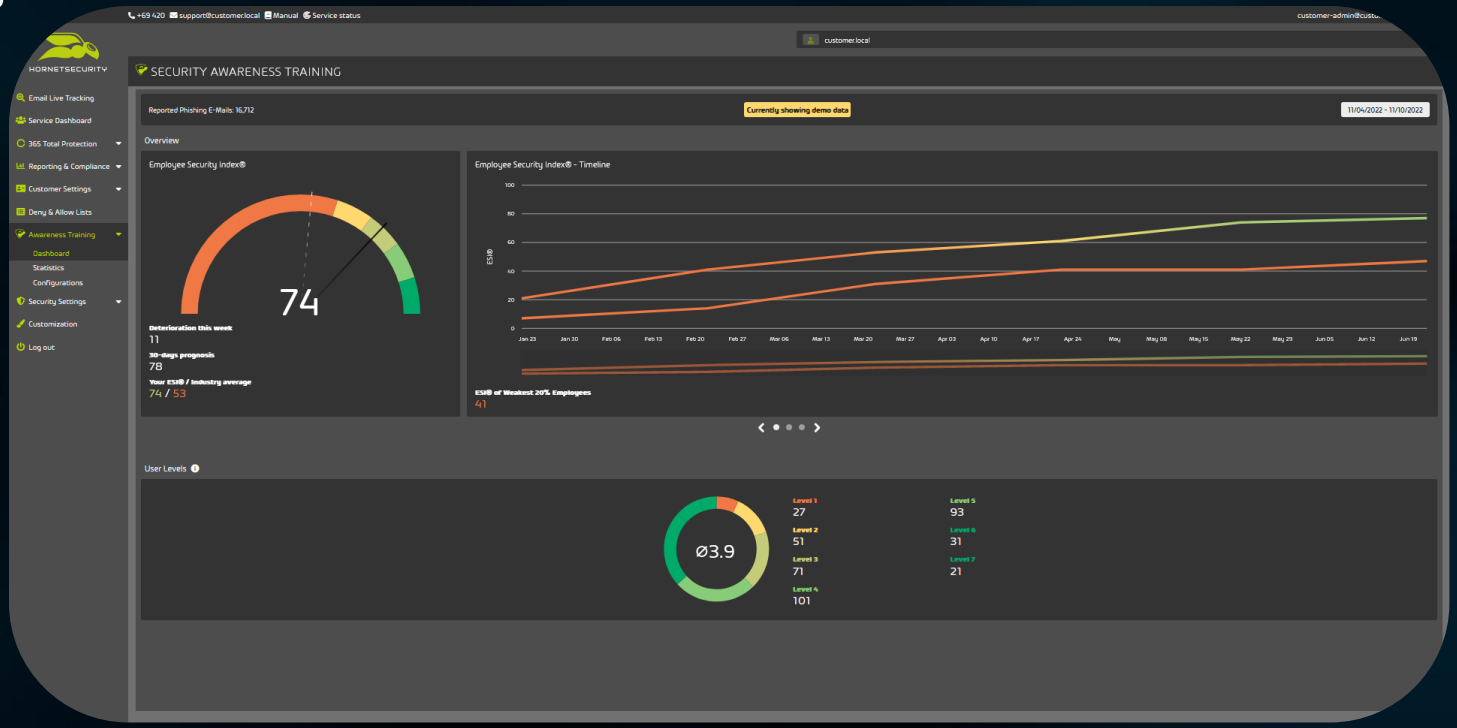
MOST TEACHABLE MOMENT



HORNETSECURITY

AWARENESS DASHBOARD IM CONTROL PANEL

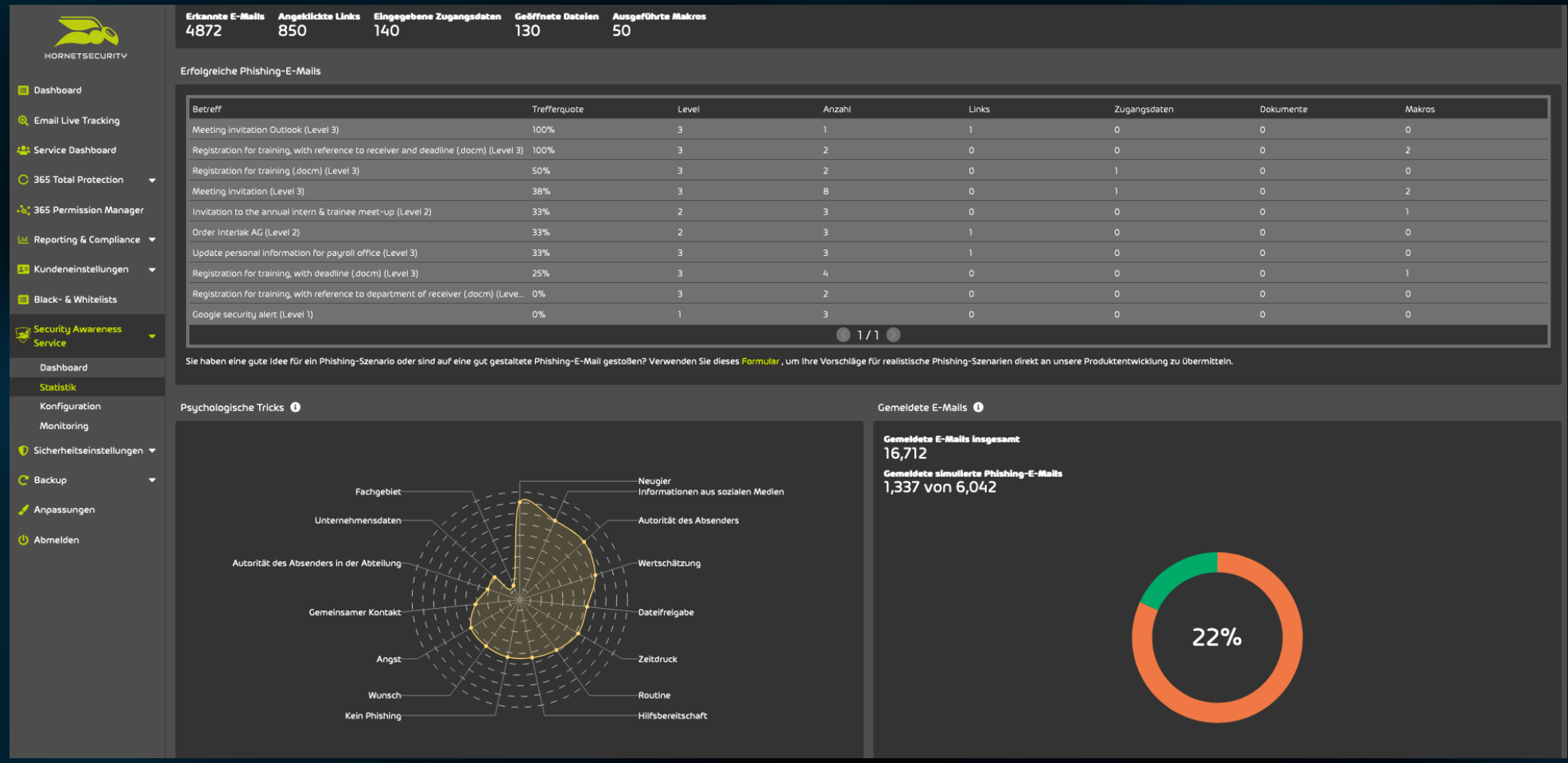
- Entwicklung des Security Awareness Trainings im Blick behalten
- ESI®-Reporting inkl. Historie und Forecast und Training KPIs
- Konfigurieren und passen Sie das Awareness Training an die Bedürfnisse Ihres Unternehmens an



HORNETSECURITY

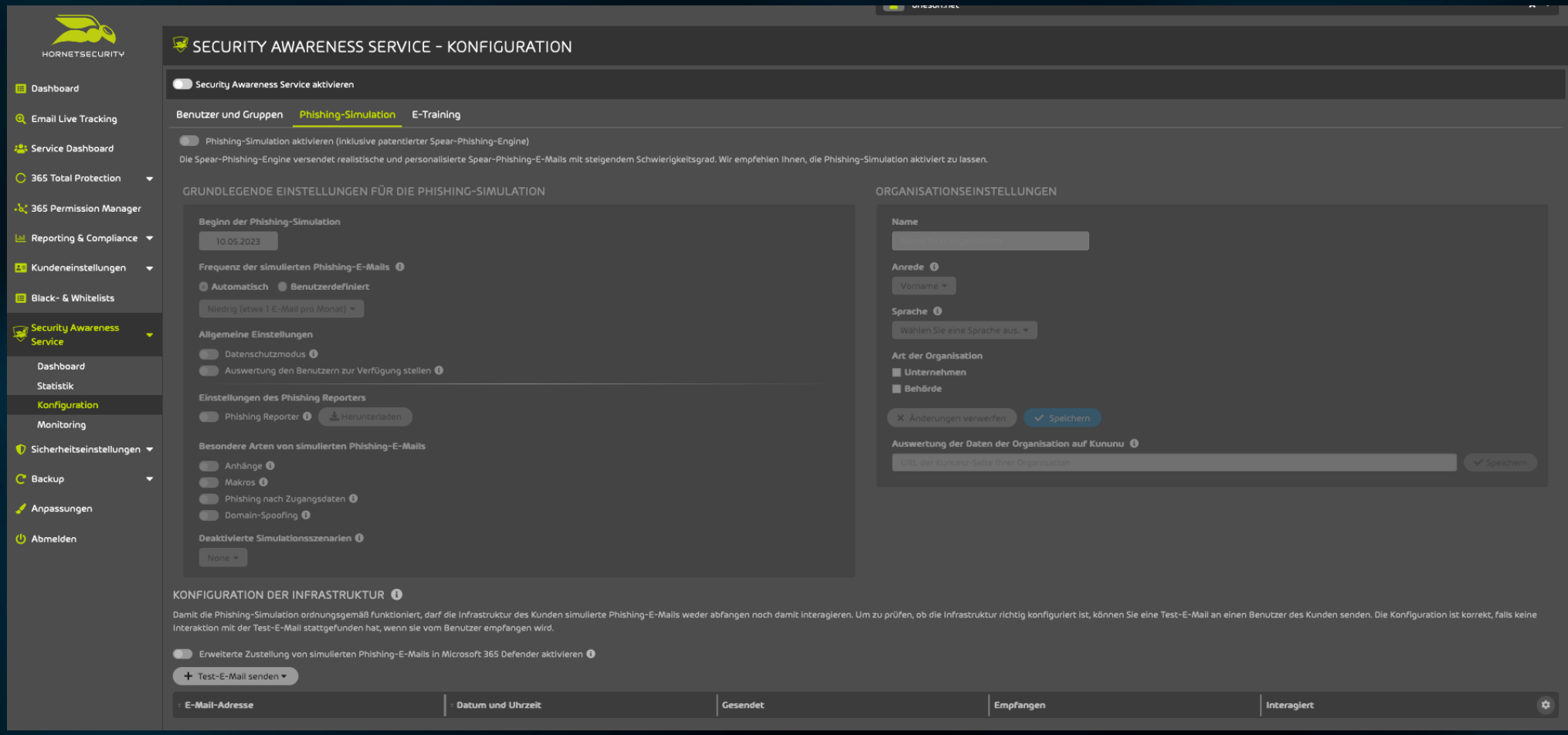
AWARENESS DASHBOARD IM CONTROL PANEL

HORNETSECURITY



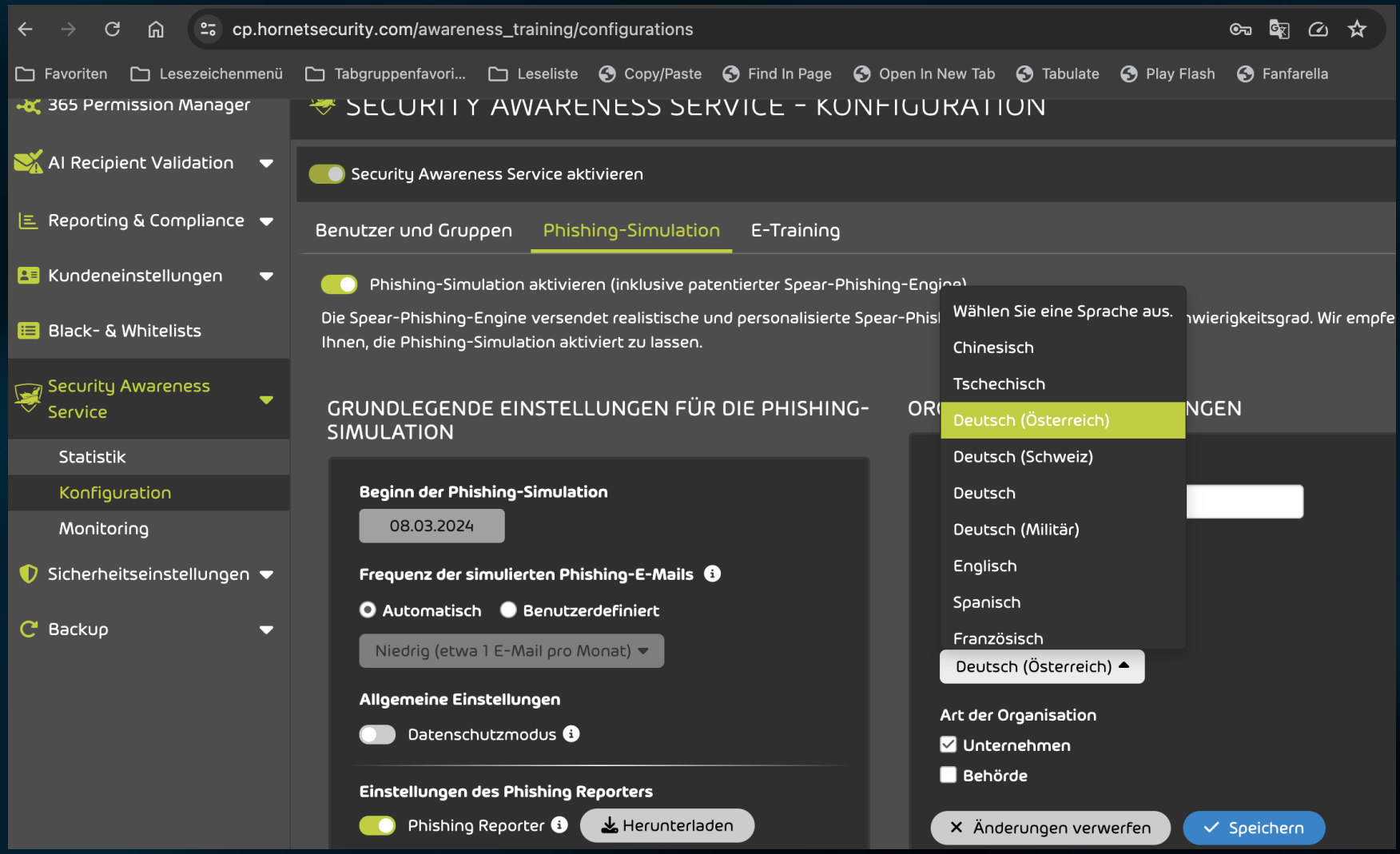
AWARENESS DASHBOARD IM CONTROL PANEL

HORNETSECURITY



AWARENESS DASHBOARD IM CONTROL PANEL

HORNETSECURITY



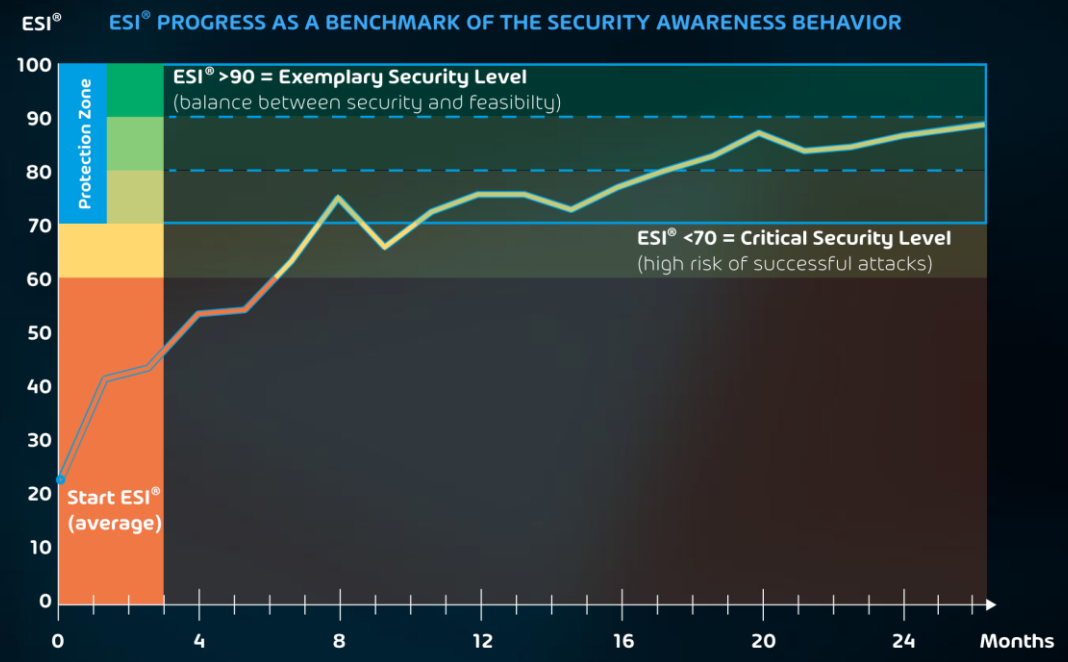
ENTSCHEIDENDE FAKTOREN FÜR EIN ERFOLGREICHES AWARENESS TRAINING

- 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 AWARENESS SERVICE

EMPLOYEE SECURITY INDEX®



ESI®Awareness-Benchmark ermöglicht eine standardisierte, transparente Messung und Steuerung des Sicherheitsverhaltens auf Unternehmens-, Gruppen- und User-Ebene.

HORNETSECURITY

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

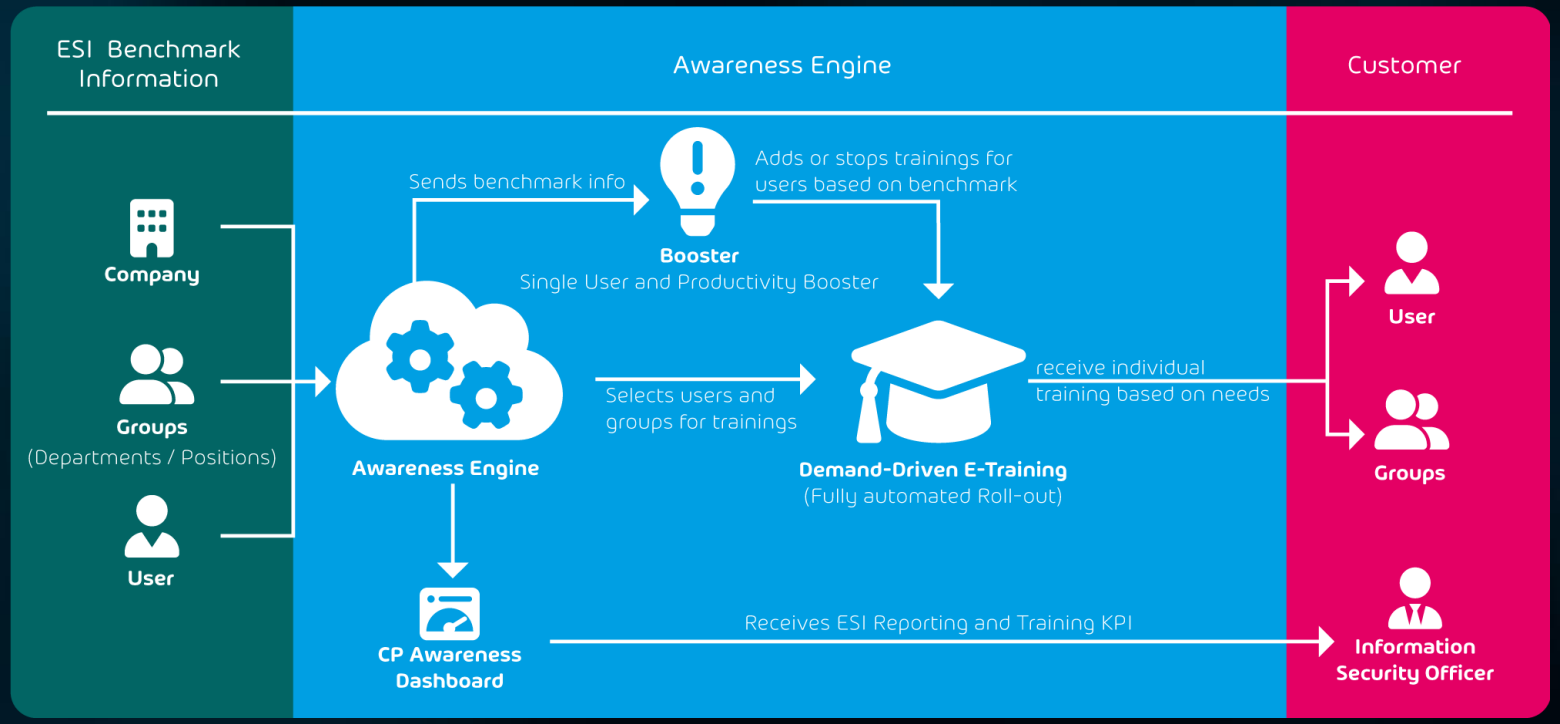
HORNETSECURITY

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



SECURITY AWARENESS SERVICE

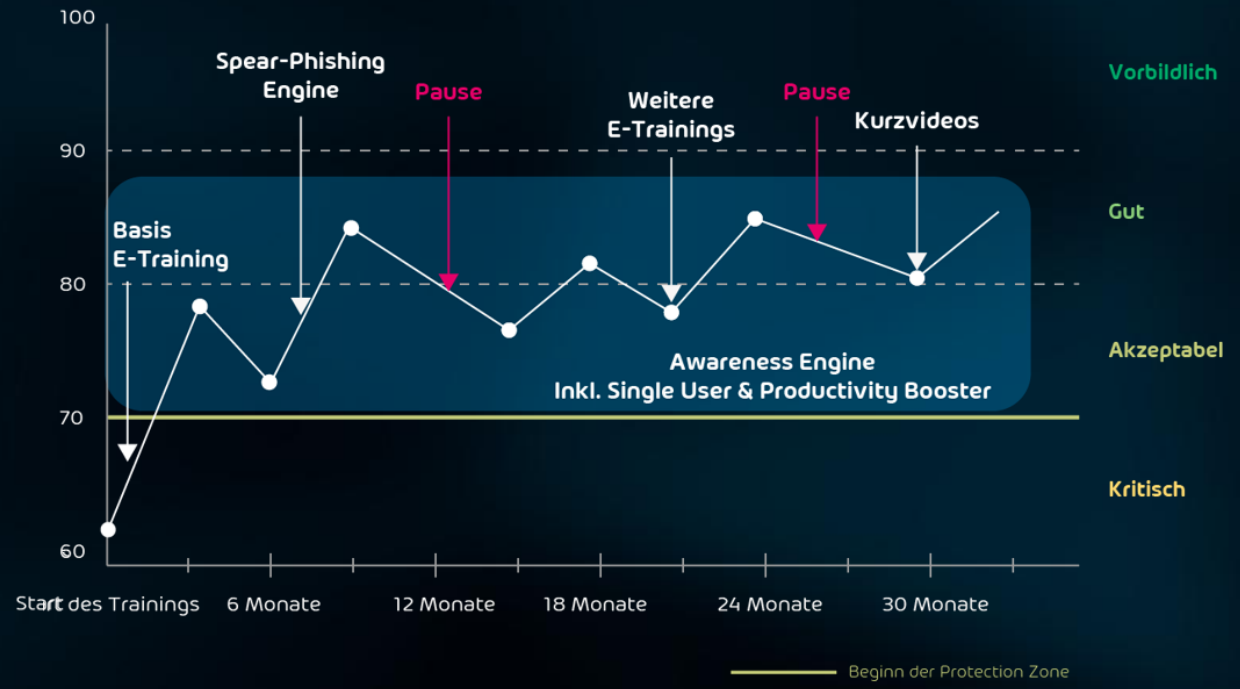
BEDARFSGERECHTES TRAINING

Einzigartig am Markt

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

Productivity Booster

Single User Booster



HORNETSECURITY

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

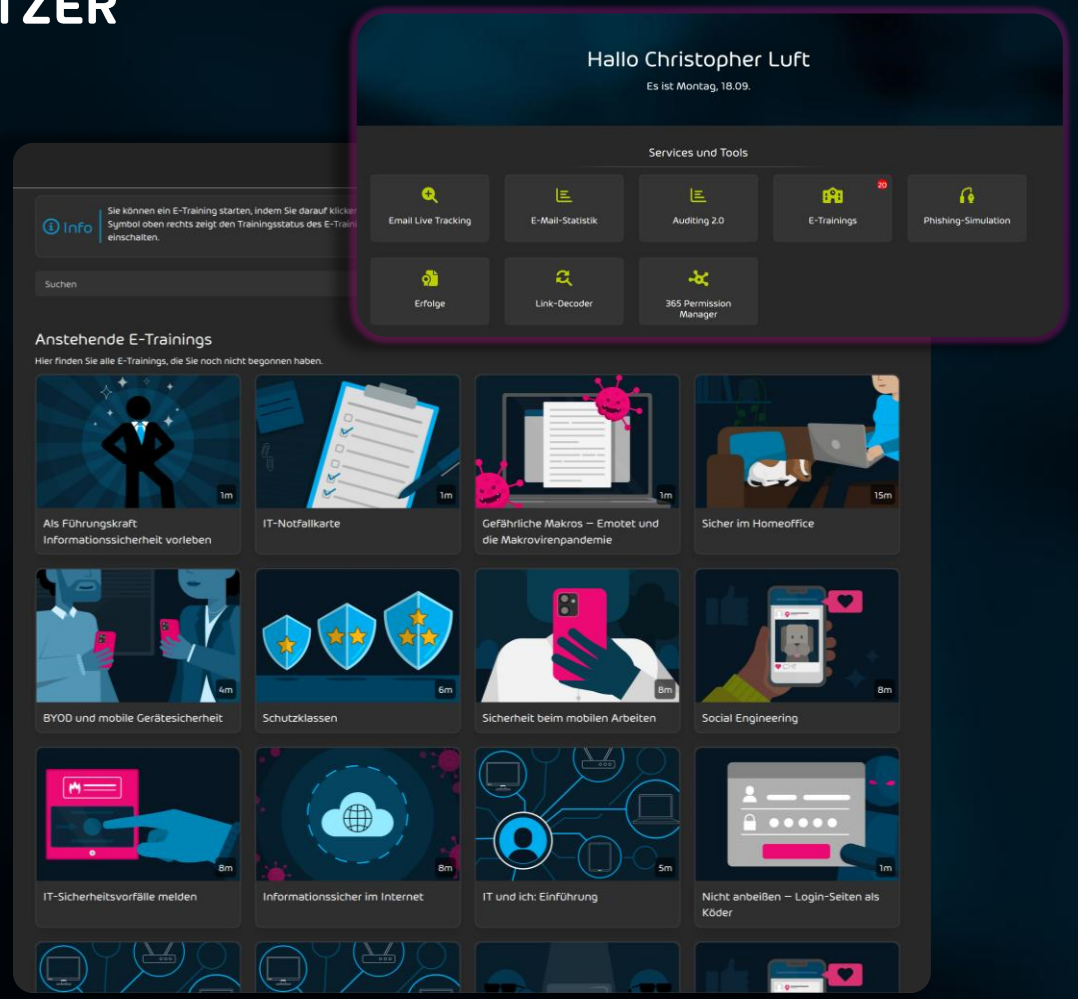
HORNETSECURITY

PLAN 4

USER PANEL

ZENTRALE LERNUMGEBUNG FÜR IHRE BENUTZER

- Zentraler Zugriff auf alle Lerninhalte über das **Hornetsecurity User Panel**
- Individuelle Auswertung der Phishing Simulation
- **Über 30 Lerninhalte** in mehreren Sprachen verfügbar
- **Interaktive** Inhalte, Kurzvideos, Quizze und PDF's
- **Dynamische Zertifikate** für die Mitarbeiter
- Regelmäßige Content Updates!



HORNETSECURITY

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

PLAN 4

SECURITY AWARENESS SERVICE

PHISHING-LEVEL 1-5 (7)

KI PHISHING	Level 7**	Inkl. Mitlesen des Postfachs
	Level 6**	Inkl. Antwort-Verlauf
SPEAR PHISHING	Level 5	Inkl. Spoofing Domains
	Level 4	Inkl. berufliche Position + Kollegen und Vorgesetzte
TARGETED PHISHING	Level 3	Nutzung spezifischer Unternehmensinformationen
	Level 2	Spear-Phishing von Geschäftsführung
DYNAMITE PHISHING	Level 1	Massen-Phishing oder Dynamite-Phishing

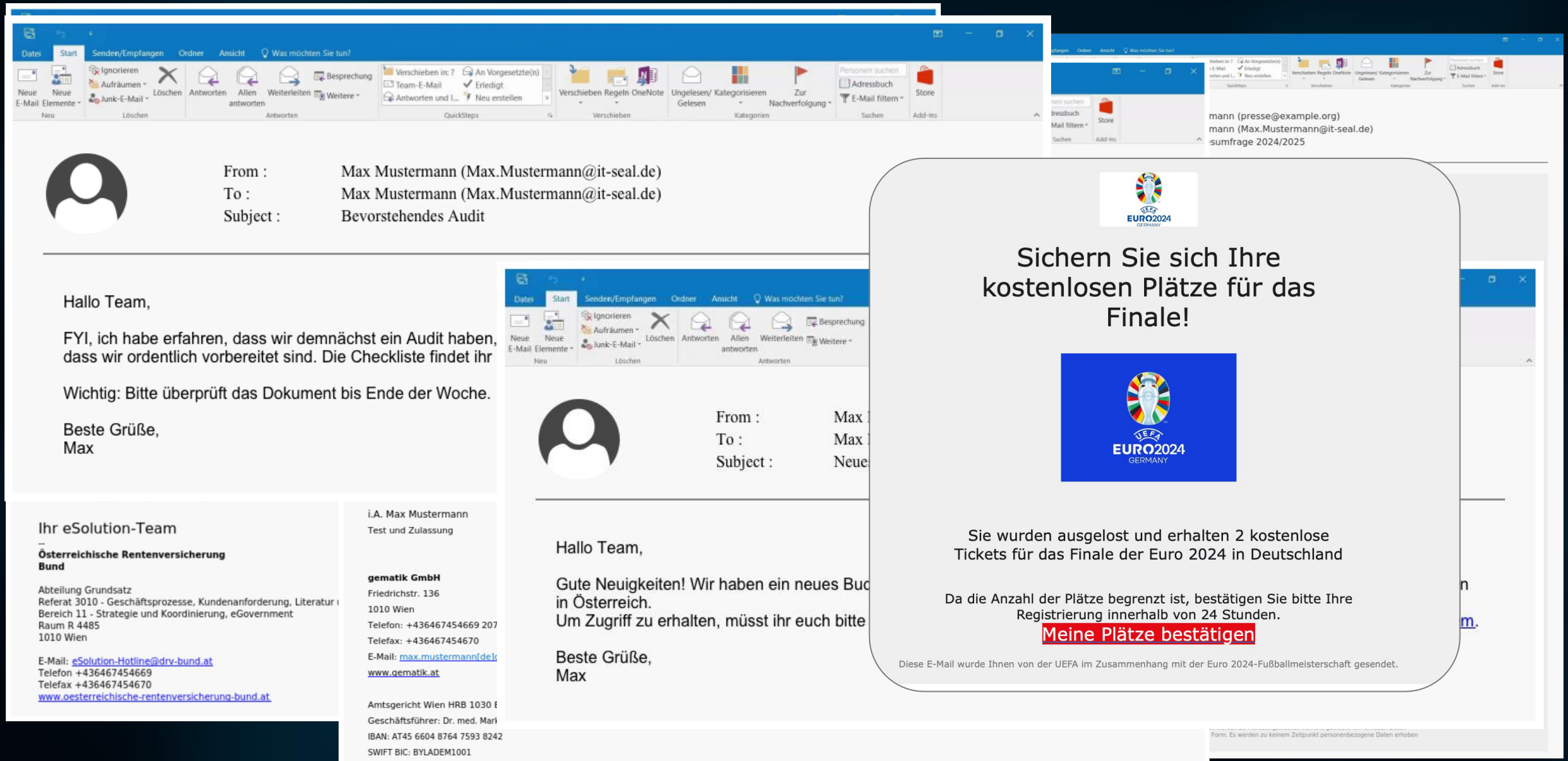
HORNETSECURITY

KI PHISHING

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

SPEAR-PHISHING-ENGINE® mit Österreich Bezug AT

VORGEHEN WIE EIN ECHTER ANGREIFER



From : Max Mustermann (Max.Mustermann@it-seal.de)
To : Max Mustermann (Max.Mustermann@it-seal.de)
Subject : Bevorstehendes Audit

Hallo Team,

FYI, ich habe erfahren, dass wir demnächst ein Audit haben, dass wir ordentlich vorbereitet sind. Die Checkliste findet ihr

Wichtig: Bitte überprüft das Dokument bis Ende der Woche.

Beste Grüße,
Max

Ihr eSolution-Team
--
Österreichische Rentenversicherung
Bund

Abteilung Grundsatz
Referat 3010 - Geschäftsprozesse, Kundenanforderung, Literatur
Bereich 11 - Strategie und Koordinierung, eGovernment
Raum R 4485
1010 Wien

E-Mail: eSolution-Hotline@drv-bund.at
Telefon +436467454669
Telefax +436467454670
www.oesterreichische-rentenversicherung-bund.at

i.A. Max Mustermann
Test und Zulassung

gematik GmbH
Friedrichstr. 136
1010 Wien
Telefon: +436467454669 207
Telefax: +436467454670
E-Mail: max.mustermann[de]
www.gematik.at

Amtsgericht Wien HRB 1030
Geschäftsführer: Dr. med. Mar
IBAN: AT45 6604 8764 7593 8242
SWIFT BIC: BYLADEM1001

From : Max
To : Max
Subject : Neue

Hallo Team,

Gute Neuigkeiten! Wir haben ein neues Buc
in Österreich.
Um Zugriff zu erhalten, müsst ihr euch bitte

Beste Grüße,
Max

Sichern Sie sich Ihre kostenlosen Plätze für das Finale!

EURO2024 GERMANY

Sie wurden ausgelost und erhalten 2 kostenlose Tickets für das Finale der Euro 2024 in Deutschland

Da die Anzahl der Plätze begrenzt ist, bestätigen Sie bitte Ihre Registrierung innerhalb von 24 Stunden.

Meine Plätze bestätigen

Diese E-Mail wurde Ihnen von der UEFA im Zusammenhang mit der Euro 2024-Fußballmeisterschaft gesendet.

mann (presse@example.org)
mann (Max.Mustermann@it-seal.de)
sumfrage 2024/2025

PATENTIERTE SPEAR-PHISHING-ENGINE

Ratschlag - Fußball

SP

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

An: Muhammed Gueleryuez

Donnerstag, 1. Oktober 2020 um 13:49

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

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

Dienstag, 5. Juli 2022 um 12:33

An: Muhammed Gueleryuez

Rahmenbedingunge...
117 KB

Rahmenbedingungen.docm

Alle herunterladen • Vorschau für alle

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 Jessika - 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

TOP 10 PHISHING ATTEMPTS

Scenario I	Description	Leve	Level (legacy)	Exploit Type	Click-rat
65	kunuunu: Arbeitgeber bewerten	1	1	link-doc	19%
546	Work Council Nomination	1	1	link-doc	18%
30	Charity appeal	1	1	link-doc	17%
996	Vacation Confirmation	2	2	link-doc	16%
401	Genehmigung des Zugriffs auf Sharepointseite	1	1	link-doc	16%
267	Scanned document (.docm)	2	1	attachment-docm	15%
265	Scanned document (.docm)	2	2	attachment-docm	14%
992	Project Tracker Notification: Mentioned in Report	2	2	link-doc	13%
985	Incomplete Cloud Storage Payment	2	2	link-doc	13%
247	Microsoft-AGB bestätigen	1	1	link-doc	13%
120	Google security alert	1	1	link-doc	13%

HORNETSECURITY

PLAN 4

SECURITY AWARENESS SERVICE

HIGHLIGHTS

PHISHING & ATTACK SIMULATION

SECURITY AWARENESS

ESI® REPORTING

450 Phishing-Szenarien

26 Sprachen

Voll automatisiert

ESI® Employee Security Index

Bedarfsgerechte Trainings

Ein Preis, alles inklusive!

HORNETSECURITY

KOSTENLOSE PHISHING-SIMULATION

HORNETSECURITY

SECURITY AWARENESS SERVICE

Kostenloser Phishing-Test

Testen Sie Ihr Sicherheitsbewusstsein und erleben Sie aus erster Hand, wie unsere patentierte Spear-Phishing-Simulation Ihren Mitarbeitern helfen kann, die notwendigen Fähigkeiten zum Schutz Ihres Unternehmens zu entwickeln.

Unsere Phishing-Simulation bietet:

- ✓ Realistische Simulationen von aktuellen Phishing-Angriffen
- ✓ Vielfalt an Arten und Raffinesse von Phishing-E-Mails
- ✓ Schritt-für-Schritt-Anleitungen zum Erkennen von Phishing-E-Mails

JETZT TESTEN

https://www.hornetsecurity.com/de/sas-phishing-simulation/

THANK YOU!

HORNETSECURITY

E-Day 2025 Aktion

- Exklusive Datacenter Führung in den DCs in Hallein oder Salzburg
- TopAwareness: Gratis bis 1. Juni (12 Monate Laufzeit)

-> Mail an g.rohrecker@conova.com

Günther Rohrecker
Chief Sales Officer
g.rohrecker@conova.com
+43 676 83050 343

Markus Todt
Country Manager Austria
todt@hornetsecurity.com
+49 511 515464240