perseus.
technologies

Leistungsbeschreibung

Unsere Lösungen für Ihre Cybersicherheit

Lösungen im Überblick

Perseus' Lösung für Cybersicherheit besteht aus der Kombination aus individueller Risikobewertung, Prävention und Sensibilisierung sowie professionellem Cybernotfall-Management.

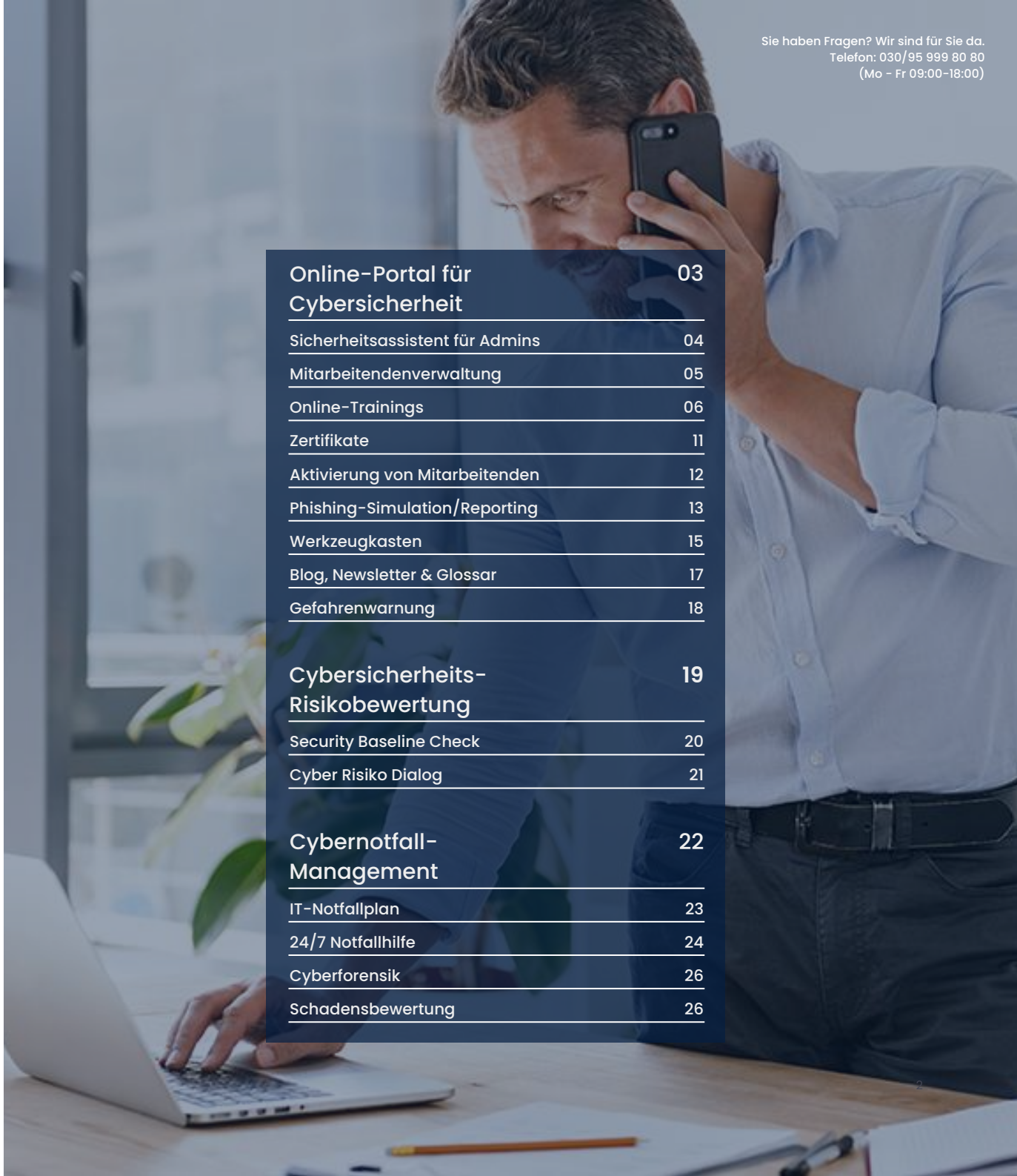
Unser Komplett-Paket für Cybersicherheit lässt sich einfach und schnell in Unternehmen jeder Größe integrieren und mit wenig Aufwand von zentraler Stelle (z. B. vom CISO, von der IT etc.) steuern.

In dieser Leistungsbeschreibung stellen wir Ihnen alle Leistungen* von Perseus im Detail vor.

Online-Portal für Cybersicherheit

Jetzt Demo anfragen

*Sollten Sie Kunde von einem unserer Kooperationspartner sein, dann können Ihre Leistungen evtl. abweichen. Bei Fragen wenden Sie sich bitte an unseren Kundenservice: 030/95 999 80 80. Wir freuen uns auf Sie!



Sie haben Fragen? Wir sind für Sie da.
Telefon: 030/95 999 80 80
(Mo - Fr 09:00-18:00)

Online-Portal für Cybersicherheit

Cybersicherheit für Unternehmen leicht gemacht. Das Online-Portal für Cybersicherheit von Perseus ist schnell installiert, einfach zu bedienen und jederzeit erreichbar.

Bestandteile des Online-Portals:

- **Sicherheitsassistent für Admins:** Sicherheitsübersicht über Ihr ganzes Unternehmen
- **Mitarbeitendenverwaltung:** Fortschritt der Mitarbeitenden bei den Trainings einsehen und Erinnerungen versenden
- **Online-Trainings:** Die Trainings vermitteln wichtiges Wissen zu Cybersicherheit, Datenschutz und Phishing
- **Zertifikate:** Unsere Zertifikate gelten als Schulungsnachweis der Mitarbeitenden im Sinne der DSGVO
- **Aktivierung von Mitarbeitenden:** Wir erinnern regelmäßig per E-Mail daran Trainings abzuschließen
- **Phishing-Simulation:** Perseus versendet vollautomatisierte, simulierte Phishing-E-Mails an Mitarbeitende, um sie auf Gefahren zu sensibilisieren
- **Werkzeugkasten:** Tools, die den Arbeitsalltag sicherer machen
- **Gefahrenwarnungen:** WIr warnen Mitarbeitende vor neuen Online-Bedrohungen

Zwecke und Zielsetzung des Online-Portals

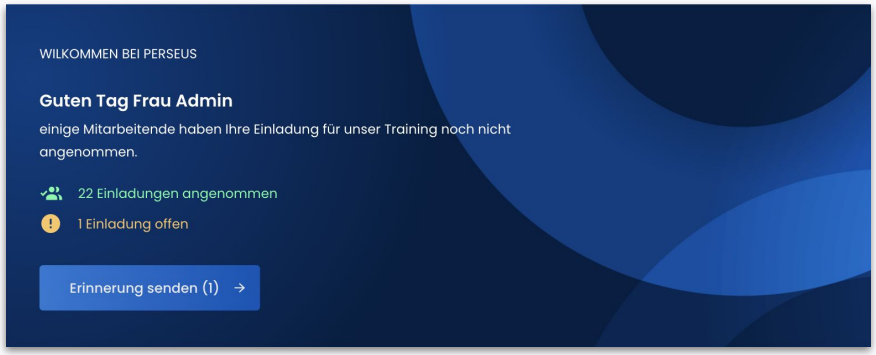
- Herstellung, Wahrung und Verbesserung der Cybersecurity- und Datenschutz-Compliance
- Datenschutz und Informationssicherheit zur Wahrung von Vertraulichkeit, Verfügbarkeit und Integrität von Informationen und personenbezogener Daten
- Reporting von IT-Sicherheitsprozessen für Verantwortliche
- Durchführung und Nachhalten von Online-Trainings zu den Themen Cybersicherheit und Datenschutz
- Erteilung von persönlichen Zertifikaten als Nachweis für erworbenes Wissen zu Cybersicherheit und Datenschutz

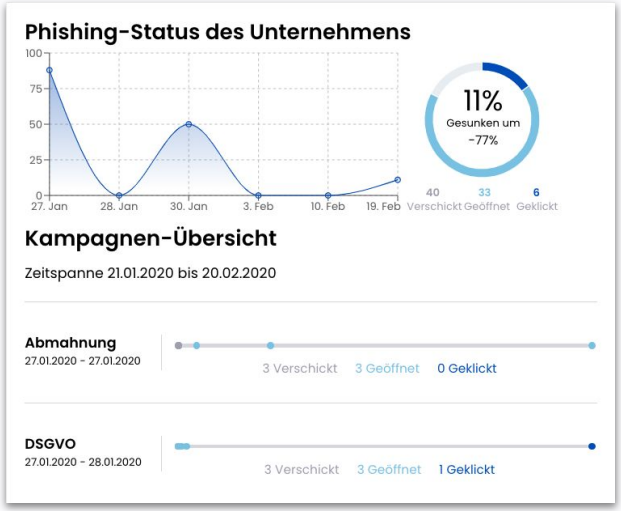
Sicherheitsassistent für Admins

Der Sicherheits-Assistent für Admins gibt einen Sicherheitsüberblick über Ihr ganzes Unternehmen. Neben dem aktuellen Sicherheitsstatus erhalten Sie hier Statistiken zu absolvierten Schulungen oder Phishing-Tests, bzw. Hinweise darüber, wie Sie Ihr Unternehmen noch sicherer machen können.

Überblick auf Knopfdruck:

- **Phishing erkannt:** Wie erfolgreich waren Ihre Mitarbeitenden beim letzten Phishing-Test?
- **Training absolviert:** Erfahren Sie jederzeit den Trainingsstand des gesamten Unternehmens.
- **Browser aktuell:** Veraltete Software ist ein großes Sicherheitsrisiko. Haben alle Ihre Mitarbeitenden die neueste Browser-Version installiert?
- **Phishing-Status des Unternehmens:** Statistiken zu aktuellen Phishing-Kampagnen (kann als XLS-Datei heruntergeladen werden).





Mitarbeitenden-verwaltung

Rechte & Trainingsstatus

Alles im Blick:

- **Mitarbeitende einladen:** Neue Mitarbeitende fügen Sie einfach und schnell über die Eingabe von E-Mail-Adressen hinzu.
- **Rollen-/Rechteverteilung:** Sie möchten mehreren Nutzern Admin-Rechte geben? Kein Problem. Auch die Rollenverteilung lässt sich mit einem Klick über die Mitarbeitendenverwaltung regeln.
- **Trainingsstatus:** Erfahren Sie als Admin jederzeit, wie weit Ihre Mitarbeitenden in den Online-Trainings fortgeschritten sind.
- **Erinnerungen senden:** Einzelne Mitarbeitenden haben das Training noch nicht begonnen oder noch nicht abgeschlossen? Erinnern Sie sie mit einem Klick per vorgefertigter E-Mail.
- **Erneut einladen:** Die Anmeldung einiger Mitarbeitenden steht noch aus? Versenden Sie von hier aus einfach eine erneute Einladung zur Registrierung bei Perseus.

Cybersicherheit und Controlling

Über die Mitarbeitendenverwaltung können Sie neue Mitarbeitenden zu Perseus einladen und ihnen Admin- oder eingeschränkte Mitarbeitendenrechte erteilen. Hier versenden Sie auch automatische Erinnerungsmails bei Trainingsrückstand.

Sie haben Fragen? Wir sind für Sie da.
Telefon: 030/95 999 80 80
(Mo - Fr 09:00-18:00)

Online-Training für Cybersicherheit

Grundlagen der Cybersicherheit:

1. Sicherheitsupdates
2. Antivirensoftware
3. Firewall
4. Öffentliche WLAN-Netze
5. Sicherheitskopien

Cybersicherheit in der Praxis:

1. Sichere Passwörter
2. 2-Faktor-Authentifizierung
3. Sicher E-Mails versenden
4. Sicher online zusammenarbeiten

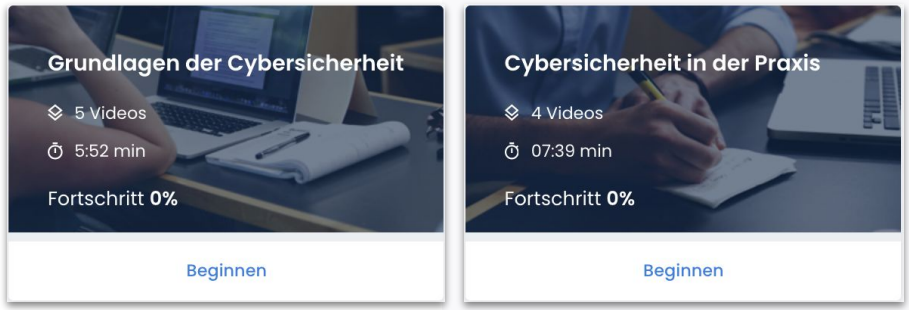
Zielsetzung und Zweck

Durchführung und Nachhalten von Online-Trainings zu den Themen Cybersicherheit und Datenschutz zur Herstellung, Wahrung und Verbesserung der Cybersecurity- und Datenschutz-Compliance bei Kunden und Bezugsberechtigten

Modernes E-Learning-Format

Die Kombination aus lehrendem Dozent und hilfreichen Animationen zum besseren Verständnis führen zu einem nachhaltigen Lernerfolg.

Online-Videos: Hintergründe zu Cybergefahren und Sicherheitsrisiken mit konkreten Handlungsempfehlungen.



ZERTIFIKAT

Herunterladen

Mehrsprachigkeit: Die Leistungen des Online-Portals sind aktuell in den Sprachen Deutsch, Englisch und Spanisch verfügbar.

Sie haben Fragen? Wir sind für Sie da.
Telefon: 030/95 999 80 80
(Mo - Fr 09:00-18:00)

Online-Training für Datenschutz

DSGVO – Die Grundlagen:

1. DSGVO – Die Grundlagen (Intro)
2. Ziele & Bedeutung für Unternehmen
3. Personenbezogene Daten
4. Verarbeitung personenbezogener Daten
5. DSGVO im Privatleben & Zusammenfassung

Personenbezogene Daten – Der richtige Umgang (Teil 1):

1. Grundsatz der Rechtmäßigkeit
2. Grundsatz der Zweckbindung
3. Grundsatz der Datenminimierung
4. Grundsatz der Speicherbegrenzung

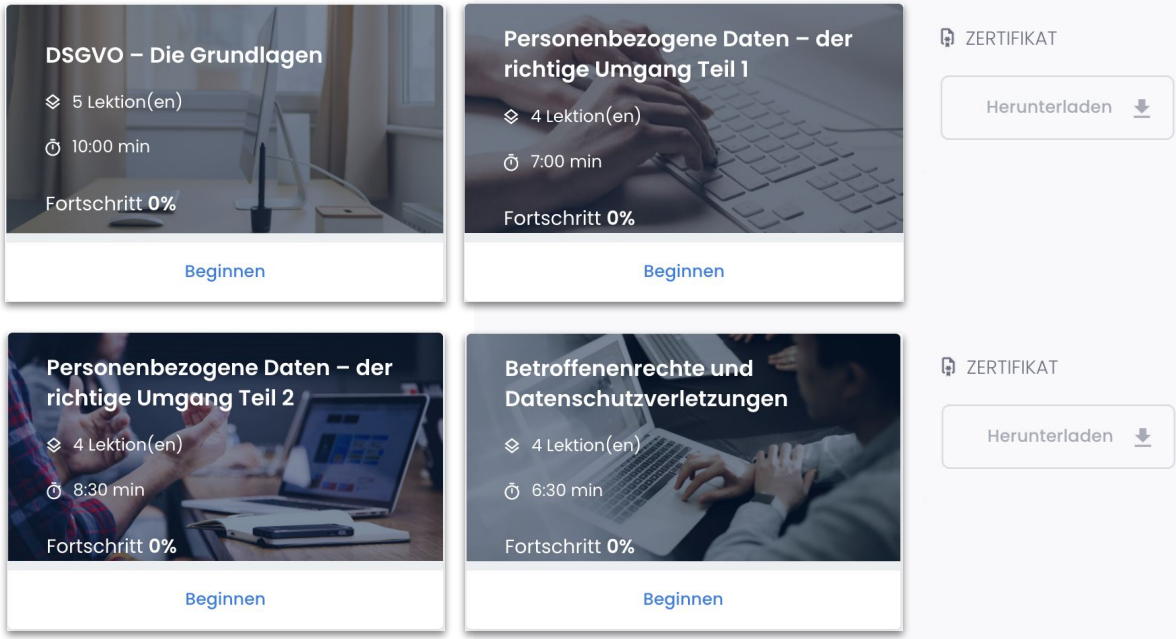
Personenbezogene Daten – Der richtige Umgang (Teil 2):

1. Grundsätze der Richtigkeit und der Transparenz
2. Grundsatz der Integrität und Vertraulichkeit
3. Grundsatz der Rechenschaftspflicht
4. Wissenswertes zur Weitergabe personenbezogener Daten

Betroffenenrechte und Datenschutzverletzungen:

1. Allgemeines und das Recht auf Auskunft
2. Das Recht auf Löschung
3. Verletzung des Schutzes personenbezogener Daten
4. Meldung, Benachrichtigung und Dokumentation

Online-Videos: Einfach, verständlich und kompakt – Informationen zu Datenschutz und seinen gesetzlichen Anforderungen.



Sie haben Fragen? Wir sind für Sie da.
Telefon: 030/95 999 80 80
(Mo - Fr 09:00-18:00)

Online-Training gegen Phishing

Die neue E-Learning-Serie zum Thema Phishing ist die perfekte Ergänzung zu unserem Phishing-Training. So werden Lernen und Sensibilisierung zum ganzheitliches Awareness-Konzept.

Phishing – die Methoden:

1. Interessante Links
2. Vertraute Links
3. Handeln aus Angst
4. Ist Ihr Passwort sicher?
5. Gehackte Freunde
6. Gefährliche Anhänge
7. Wie können Sie sich schützen?

Phishing – die Auswirkungen:

1. Spyware
2. Ransomware
3. Computerviren und Würmer
4. Merkmale von Phishing-Nachrichten

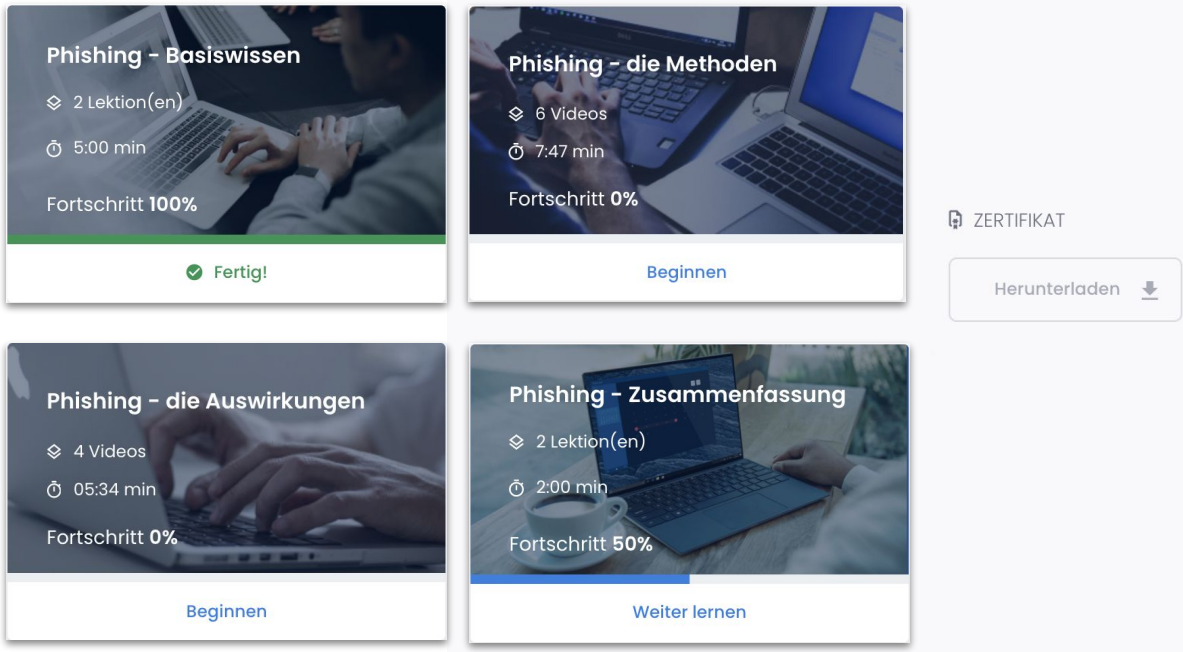
Phishing – Basiswissen:

1. Phishing – Definition
2. Wie können Sie sich schützen

Phishing – Zusammenfassung:

1. Zusammenfassung
2. Gut zu wissen

Phishing-Videos: Phishing-Attacken sind die größte Cyberberbedrohung für kleine und mittelständische Unternehmen. Aus diesem Grund legen wir bei unseren Online-Trainings einen besonderen Fokus auf dieses Thema. Ihre Mitarbeitenden lernen Phishing-Attacken zu erkennen und abzuwehren.



Quizzes & Zertifikate: Nach allen Lernvideos folgt ein kurzes Quiz als Lernkontrolle. Lernnachweise (Zertifikate) können nach erfolgreich absolviertenn Kursen heruntergeladen werden.

Sie haben Fragen? Wir sind für Sie da.
Telefon: 030/95 999 80 80
(Mo - Fr 09:00-18:00)

Online-Training

Vertiefende Lektionen zu Cybersicherheit & Datenschutz

Social Media:

1. Online-Quiz
2. Berufliche Netzwerke
3. Beruflich und privat
4. Wie können Sie sich schützen

Mobiles Arbeiten:

1. Öffentliches WLAN
2. Gefahren der Schatten-IT
3. Online Meetings & Kollaboratives Arbeiten
4. Spear Phishing und CEO-Fraud
5. Sicheres Homeoffice & DSGVO

Umgang mit Informationen:

1. Lebenszyklus von Informationen
2. Vertrauliche vs. öffentliche Informationen
3. IT-, und Informationssicherheit
4. Clean Desk Policy

Menschliche Firewall:

1. Menschliche Firewall
2. Gefahren im Netz

Cyber-Notfall:

1. Warnsignale
2. Handeln im Notfall
3. Sicherheitskopien
4. Ausschalten oder nicht?

Sie haben Fragen? Wir sind für Sie da.
Telefon: 030/95 999 80 80
(Mo - Fr 09:00-18:00)

Online-Training

Vertiefende Lektionen zu Angriffsmitteln & Methoden

Schadsoftware:

1. Viren & Würmer
2. Trojaner & Keylogger
3. Ransomware
4. Wie können Sie sich schützen?

Verschlüsselungssoftware:

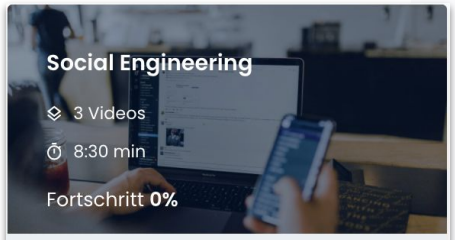
1. Schadsoftware - die Sichtbaren
2. Trojaner - das Transportmittel
3. Scareware - der Angstmacher
4. Wie können Sie sich schützen?

Social Engineering:

1. Die menschliche Psyche
2. Arten von Social Engineering
3. Wie können Sie sich schützen?

Beginnen

Beginnen



Beginnen

Sie haben Fragen? Wir sind für Sie da.
Telefon: 030/95 999 80 80
(Mo - Fr 09:00-18:00)

Zertifikate für Cybersicherheit & Datenschutz

(DSGVO-/Versicherungs-Nachweise)

Die Perseus-Zertifikate für Cybersicherheit und Datenschutz unterstützen Sie bei der Einhaltung der EU-Datenschutz-Grundverordnung und sind ein wichtiger Nachweis bei eventuellen Prüfungen durch die Behörden.

Immer auf neuestem Wissensstand

Auch nach dem Abschluss der Online-Trainings und dem Erhalt der Trainingszertifikate werden Ihre Mitarbeitenden weiterhin mit wichtigen Lerninhalten zu den Themen Cybersicherheit und Datenschutz informiert.

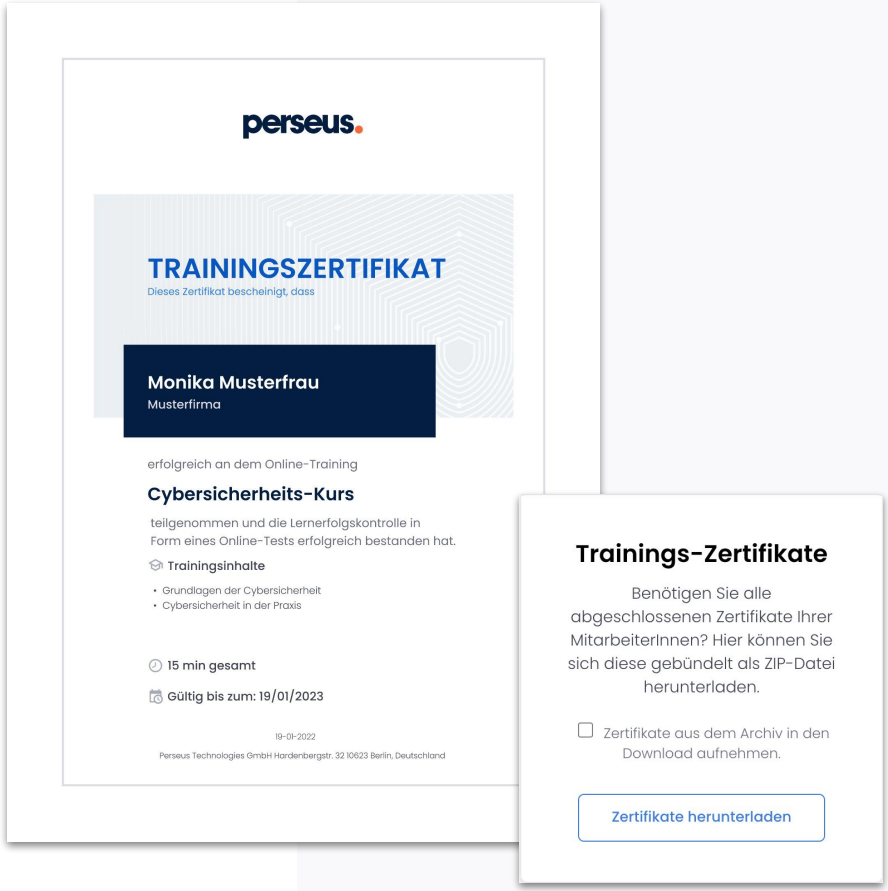
Einfacher Download

Alle Ihre Mitarbeitenden können die von ihnen erworbenen Zertifikate leicht und schnell online herunterladen – zu Zwecken der Dokumentation oder zum Ausdrucken. Als Admin haben Sie sogar die Möglichkeit, alle Mitarbeitenden-Zertifikate gesammelt in einem einzigen Ordner herunterzuladen.

Informationen auf dem Zertifikat:

- Trainingsinhalte
- Dauer des Kurses
- Art der Lernerfolgskontrolle
- Ende der Gültigkeit (Laufzeit)

Das Abschlusszertifikat: Das Zertifikat gilt als Nachweis einer Schulung im Sinne der DSGVO.



Alle Zertifikate gesammelt laden: Admins laden alle Mitarbeitenden-Zertifikate mit nur einem Klick herunter.

Aktivierung von Mitarbeitenden

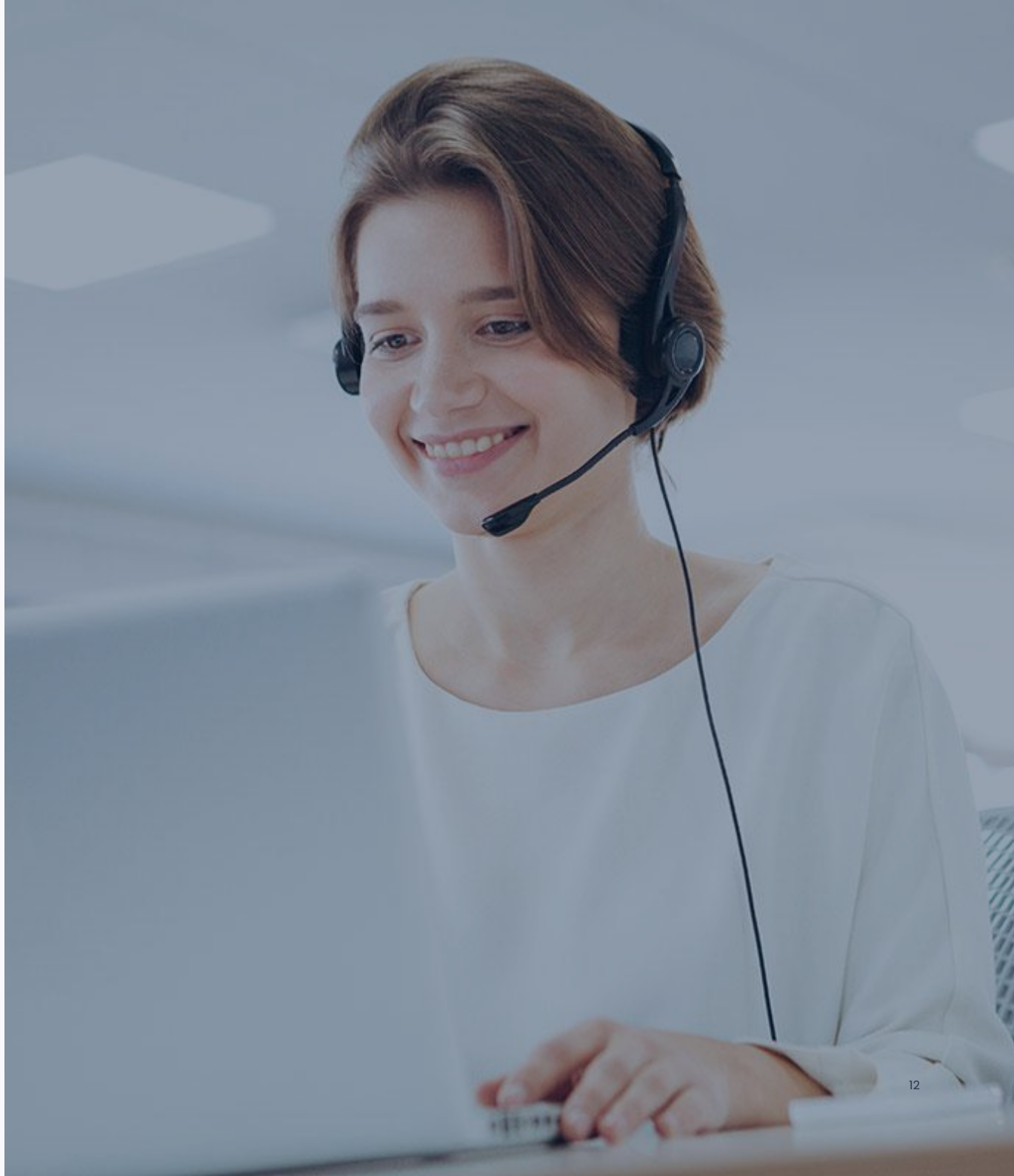
Auch wenn Sie und Ihre Mitarbeitenden Cybersicherheit in Ihrem Unternehmen ernst nehmen, geht der Fokus darauf in der täglichen Arbeit schnell verloren. Aus diesem Grund erinnert Perseus Sie und Ihre Mitarbeitenden regelmäßig daran, Online-Schulungen abzuschließen oder andere wichtige Maßnahmen durchzuführen.

Zu Ihrer Entlastung erinnern wir Ihre Mitarbeitenden bspw. in automatischen E-Mails daran,...

... die Perseus-Anmeldung durchzuführen/abzuschließen,
... die Online-Trainings zu beginnen,
... die angefangenen Trainings zu beenden.

Aktivierung von Verantwortlichen

Auch Admins werden wir durch gezielte und zweckgebundene E-Mails an wichtige Maßnahmen erinnern – zum Beispiel daran, Perseus-Einladungen an weitere Mitarbeitende zu versenden.



Sie haben Fragen? Wir sind für Sie da.
Telefon: 030/95 999 80 80
(Mo - Fr 09:00-18:00)

Phishing-Simulation

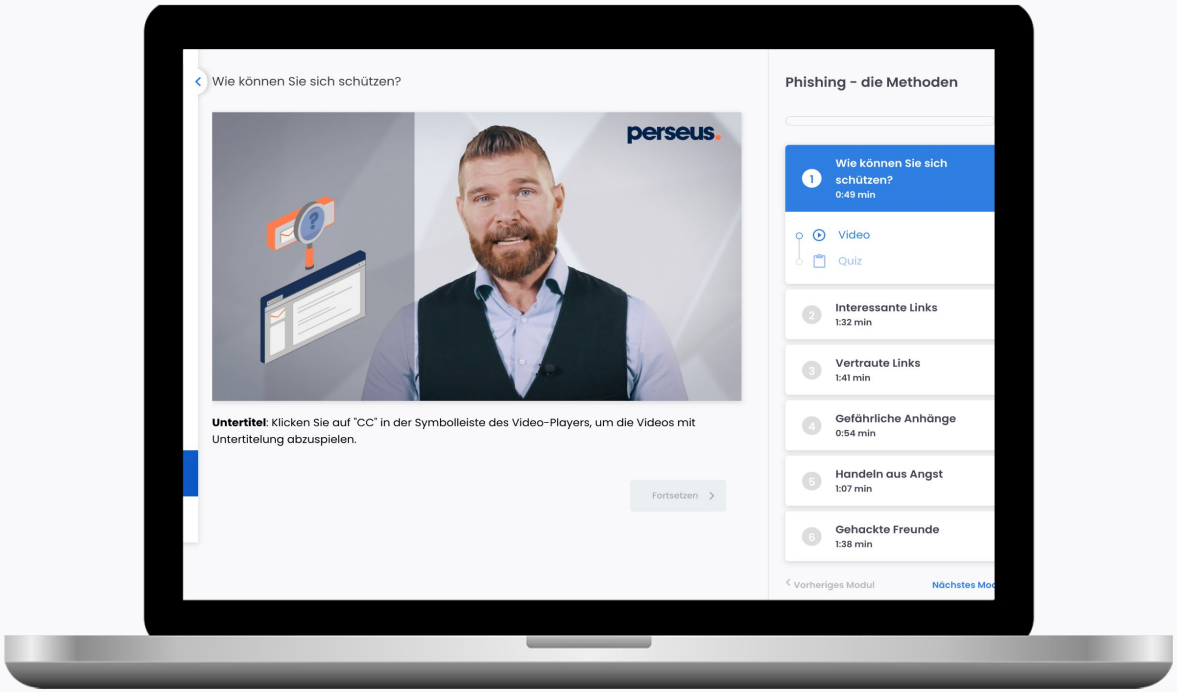
Mit simulierten Betrugs-E-Mails wird das Gefahrenbewusstsein Ihrer Mitarbeitenden kontinuierlich überprüft. Perseus führt in unregelmäßigen Abständen Phishing-Tests mit verschiedenen Vorlagen durch, die echten Phishing-Attacken nachempfunden sind.

Theorie & Praxis effizient kombiniert

Phishing-Angriffe gehören zu den größten Cyberrisiken für Unternehmen. Unsere Phishing-Lernstrecke schult Ihre Mitarbeitenden mit leicht verständlichen Online-Videos, wie sie Gefahren erkennen und abwehren können. Im Anschluss wird dieses Wissen über Phishing-Simulationen im Arbeitsalltag beständig weiter trainiert.

Lernen durch Sensibilisierung

Klicken Ihre Mitarbeitenden in einer unserer simulierten Phishing-Mails auf Anhänge oder Links, werden sie auf eine Trainingsseite weitergeleitet. Auf dieser Website werden Mitarbeitenden wiederholt über die Erkennungsmerkmale und Gefahren von Phishing-E-Mails aufgeklärt. Genau dieses wiederholte Training von Theorie und Praxis macht die Phishing-Lernstrecke von Perseus so effektiv und nachhaltig.



Aktivierung

Mitarbeitende werden wiederholt an die Absolvierung der Phishing-Lernstrecke erinnert

Online-Video-Training

Einfach verständliche Lernvideos klären Mitarbeitende über Phishing-Gefahren auf

Phishing-Simulation

Simulierte Phishing-Mails testen Mitarbeitende auf Cyberwissen und bereiten sie auf den Ernstfall vor

Sie haben Fragen? Wir sind für Sie da.
Telefon: 030/95 999 80 80
(Mo - Fr 09:00-18:00)

Phishing-Reporting

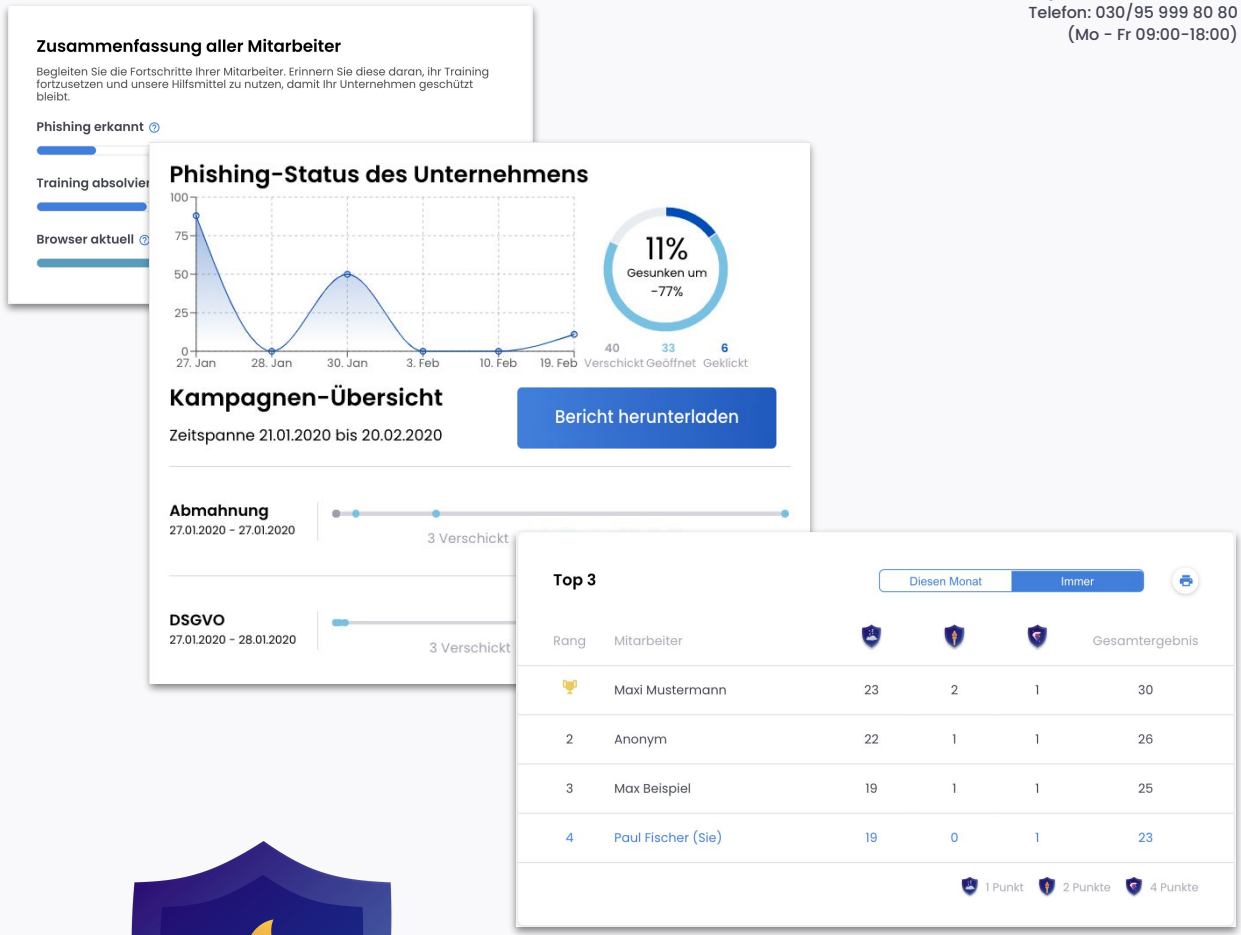
Admins können den Phishing-Status jederzeit einesehen und erhalten dadurch wichtige Informationen über die Cybersicherheit des Unternehmens.

Kampagnen-Übersicht

Auf einen Blick erhalten Sie einen Überblick darüber, welche simulierten Phishing-Mails kürzlich an Ihre Mitarbeitenden verschickt wurden und wie erfolgreich Ihre Kolleginnen und Kollegen diese abwehren konnten. Falls Sie eine Dokumentation für ein internes Reporting benötigen, können Sie jederzeit per Klick eine ausführliche Statistik als XLS-Datei herunterladen.

Sensibilisierung mit Abwechslung

Cyber-Awareness ist zwar ein ernstes Thema, doch Sensibilisierung kann auch Spaß machen. Bei richtigem Verhalten werden Mitarbeitende mit verschiedenen Phishing-Trophäen belohnt und können sich auf einer Rangliste mit ihren Kolleginnen und Kollegen messen. Das ermutigt, die eigenen Leistungen noch zu verbessern. Natürlich haben Mitarbeitende dabei die Möglichkeit, ihre Ergebnisse zu anonymisieren.



Phishing-Trophäen

Mehr Lern-Anreiz durch Gamification-Elemente

Bestenliste

Spielerischer Wettbewerb kann Phishing-Ergebnisse und die Sicherheit des Unternehmens verbessern

Sie haben Fragen? Wir sind für Sie da.
Telefon: 030/95 999 80 80
(Mo - Fr 09:00-18:00)

Werkzeugkasten für Cybersicherheit

Im Mitgliederbereich von Perseus finden Sie und Ihre Mitarbeitenden praktische und einfach zu bedienende Tools, um den Arbeitsalltag noch sicherer zu gestalten. Sobald Sie und Ihre Kolleginnen und Kollegen unsere Online-Trainings für Cybersicherheit und Datenschutz absolviert haben, werden Sie Hintergrund und Wichtigkeit unserer Werkzeuge verstehen und diese mühelos in die tägliche Arbeit integrieren.

Einen ersten Überblick über ihre Funktionalität und warum unsere Fachleute für Cybersicherheit Ihnen die Benutzung der Tools so dringend empfehlen, finden Sie auf dieser Seite. Die digitale Welt verändert sich und damit auch ihre Bedrohungen. Aus diesem Grund wird Perseus den Werkzeugkasten für Cybersicherheit für Ihr Unternehmen fortlaufend optimieren und neue Werkzeuge hinzufügen.

Darknet-Scan

Wurde Ihre E-Mail-Adresse im Zusammenhang mit einem Daten- und Sicherheitsvorfall gemeldet, finden Sie das mit nur einem Klick heraus und können Maßnahmen ergreifen (bspw. Passwörter ändern).

Browser-Check

Veraltete Browser-Versionen sind ein enormes Sicherheitsrisiko und Einfallstor für kriminelle Hacker. Browser-Anbieter optimieren die Sicherheit ihrer Software regelmäßig. Sind die Browser in Ihrer Firma auf dem neuesten Stand? Mit unserem Werkzeugkasten finden Sie es im Nu heraus.

Passwort-Erinnerung

Wahlweise können Ihre Mitarbeitenden die automatische Passwort-Erinnerung aktivieren. So werden sie alle 8 Wochen daran erinnert, ein neues und sicheres Passwort für Ihre betrieblichen Accounts zu erstellen.

E-Mail-Scanner

Zur Verwendung für alle Ihre Mitarbeitenden ist im Werkzeugkasten die E-Mail-Adresse unseres Malware-Scanners hinterlegt. Einfach verdächtige E-Mail weiterleiten und in wenigen Minuten erfahren, ob Dateianhänge gefährlich oder unbedenklich sind. Denken Sie daran: 70 % der erfolgreichen Cyberangriffe erfolgen durch E-Mails.

Sie haben Fragen? Wir sind für Sie da.
Telefon: 030/95 999 80 80
(Mo - Fr 09:00-18:00)

Darknet-Scan

Sind Ihre Daten im Darknet? Jeden Tag werden über eine Millionen Zugangsdaten gestohlen. Finden Sie heraus, ob Ihre Mitarbeitenden bereits betroffen sind.

Perseus durchsucht das Internet nach gestohlenen Daten, die von Hackern veröffentlicht wurden und lässt Sie wissen, ob eine der E-Mail-Adressen Ihres Unternehmens bei einer Sicherheitslücke entdeckt wurde. Anschließend helfen wir Ihnen, sich vor Datendiebstahl zu schützen.

Überprüfen Sie noch heute, ob Ihre Daten in Zusammenhang mit Sicherheitsvorfällen genannt werden.

Darknet-Scan für Ihre Unternehmensdomain:

Wir überprüfen anhand Ihrer Unternehmens-Domain (z. B. @perseus.de), ob es Sicherheitsvorfälle im Zusammenhang mit Ihren Firmen-E-Mail-Adressen gab.

Ihre überprüfte Domain:
perseus.de

Für die Domain perseus.de ist kein Sicherheitsvorfall bekannt.

Darknet & Erpressung

Hacker verkaufen Daten für Profit online oder erpressen betroffene Unternehmen

Rache & Willkür

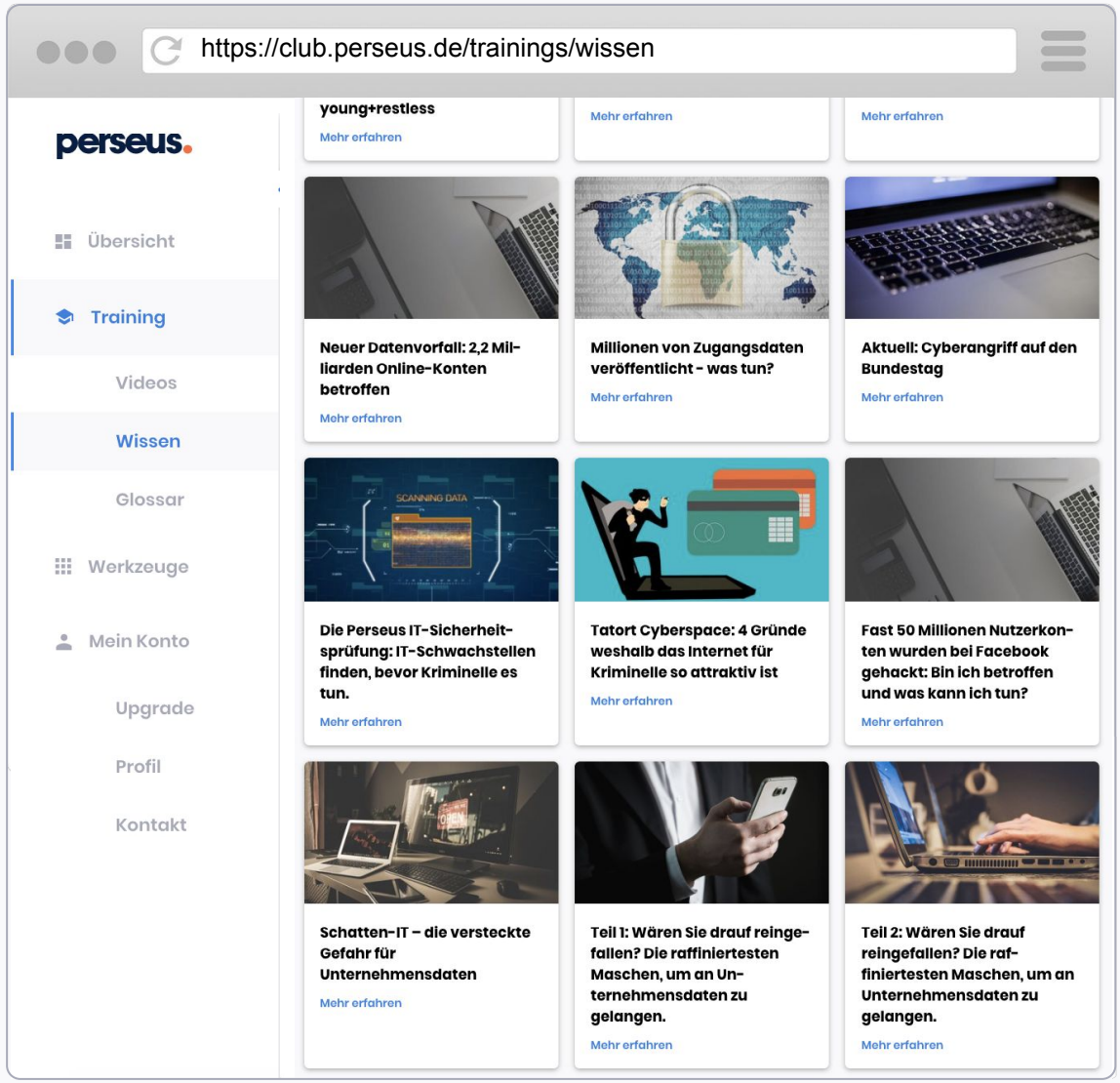
Kriminelle handeln auch aus politischen oder privaten Gründen oder wollen sich profilieren

Blog, Newsletter & Glossar

Als Mitglied von Perseus werden Sie und Ihre Mitarbeitenden über aktuelle gesellschaftliche, rechtliche und technische Entwicklungen im Bereich Cybersicherheit informiert.

Wir wissen, was unser Geschäftsklientek bewegt und stellen regelmäßig neue Artikel mit Hintergrundinformationen und konkreten Handlungsempfehlungen in den Wissensbereich. Ausgewählte Themen stellen wir ebenfalls im Newsletter vor.

Sie haben keine Ahnung, was ein Botnet ist? Oder was bspw. Doxing oder Spoofing bedeutet? Kein Problem. In unserem fortlaufend aktualisierten Cyber-Glossar finden Sie und Ihre Mitarbeitenden die gängigen Begriffe aus der Welt der Cybersicherheit anschaulich und mit nützlichem Kontext erklärt.



Gefahrenwarnung

Regelmäßig sorgen Hacker-Attacken, Datendiebstähle, Sicherheitslücken oder andere Cybervorfälle für Risiken in der digitalen Welt. Damit unsere Mitglieder rechtzeitig über mögliche neue Gefahren Bescheid wissen, gibt es die Perseus-Gefahrenwarnung.

Unsere Cybersicherheits-Fachleute erfahren frühzeitig von neuen Gefahren für Ihr Unternehmen und informieren Sie sofort per E-Mail.

Handlungsempfehlung bei Gefahren

Neben Hintergründen und einer Einschätzung der Gefahren geben wir Ihnen und Ihren Mitarbeitenden natürlich auch direkte Empfehlungen dafür, wie Sie der neuen Gefahr vorbeugen können oder handeln sollten, falls Sie betroffen sind.

Auf Anfrage

Cybersicherheits-Risikobewertung

Cyberrisiken für Unternehmen steigen weiter an. Die Risikobewertung der Cybersicherheit ist das Fundament jeder wertigen Sicherheitsstrategie. Aus diesem Grund entwickelt Perseus Services zur Risikobewertung, die den Ansprüchen unserer Unternehmenskunden entsprechen.

Der **Security Baseline Check** prüft ob grundlegende Cybersicherheits-Standards etabliert sind und unterstützt bei Korrekturen und Optimierungen. Der **Cyber Risiko Dialog** geht in die Tiefenanalyse Ihrer IT-Sicherheit, mit dem Ziel, die individuellen Ansprüche von Unternehmen und Branche zu erfüllen.

Warum ist Risikobewertung von Cybersicherheit so wichtig?

- Die Anzahl schädlicher Cyberangriffe auf Unternehmen steigt jährlich weiterhin rapide
- Kleine und mittlere Unternehmen geraten vermehrt ins Visier von Kriminellen
- Betriebsunterbrechungen, Datendiebstahl oder Aufwände zur Bereinigung der Cyberschäden können für KMU existenzgefährdend sein
- Nur Unternehmen, die die Schwachstellen in der eigenen IT-Sicherheit kennen, können eine effektive Cybersicherheit aufbauen und sich nachhaltig vor Bedrohungen schützen
- Die Risikobewertung der eigenen Cybersicherheit ist das Fundament für jede wirksame Cybersicherheitsstrategie

Auf Anfrage

Security Baseline Check

Wir prüfen Ihre Sicherheitsstandards

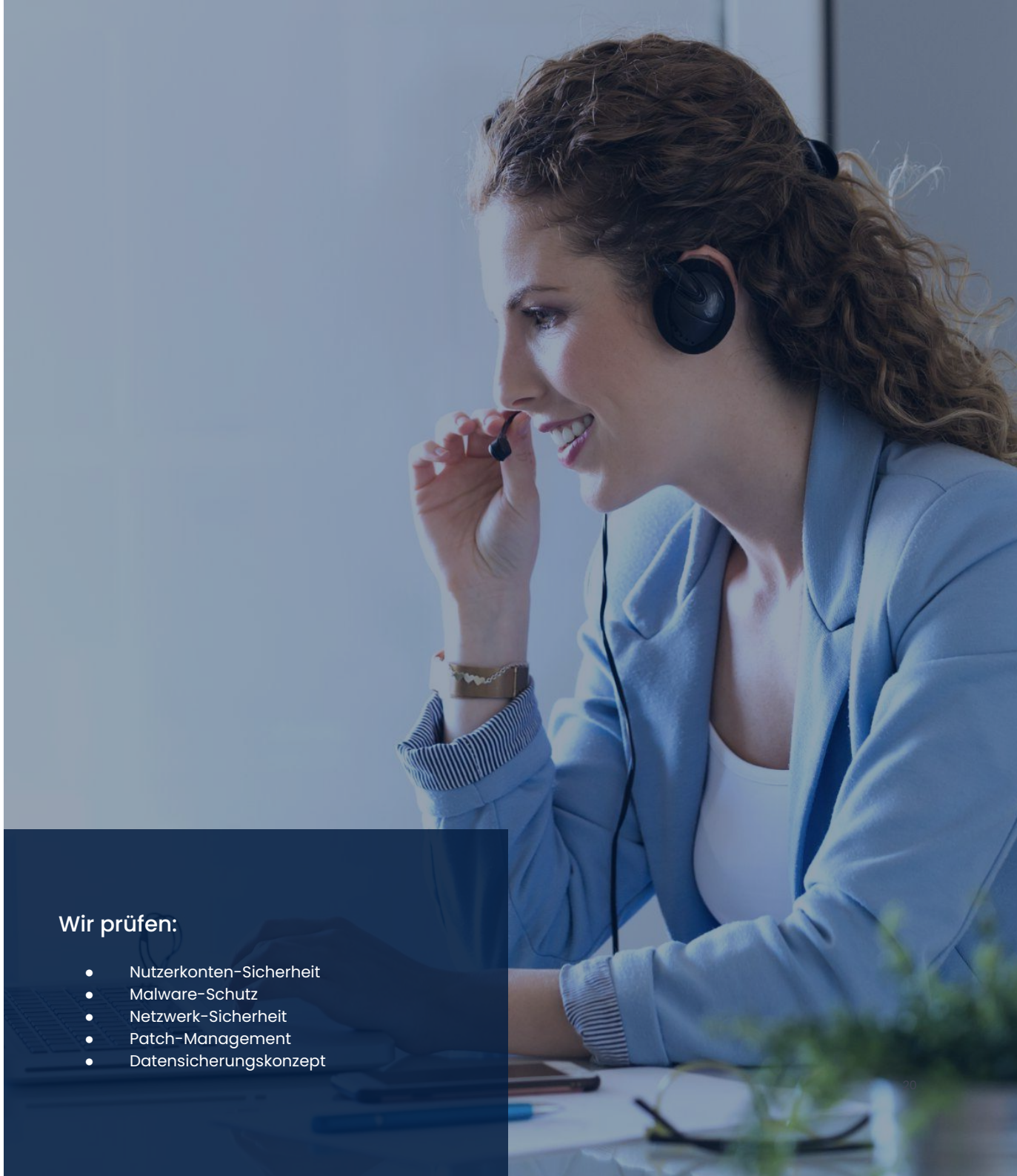
Jeden Tag kümmern sich die Expertinnen und Experten von Perseus um die Cybervorfälle unserer zahlreichen Unternehmenskunden. Aufgrund dieser Expertise wissen wir ganz genau, worauf es bei guter Cybersicherheit ankommt. Im Rahmen des Security Baseline Checks prüfen wir, ob grundlegende Sicherheitsstandards und -protokolle in Ihrem Unternehmen etabliert sind und helfen Ihnen, wenn nötig, bei Korrekturen und Optimierungen.

Ideale Ergänzung zur Cyber-Versicherung

Dank unserer langjährigen Erfahrung wissen wir, welche präventiven Maßnahmen kleine und mittelständische Unternehmen optimal vor Cyberangriffen schützen. Sollte es dennoch einmal zum Schadensfall kommen, dient ein bestandener Security Baseline Check als wichtiger Nachweis für Versicherungsleistungen.*

Jetzt Angebot anfragen

*Abhängig von Ihrem Versicherer. Ist im Vorhinen zu klären.



Wir prüfen:

- Nutzerkonten-Sicherheit
- Malware-Schutz
- Netzwerk-Sicherheit
- Patch-Management
- Datensicherungskonzept

Unsere Lö[illegible] für Ihre Cybersicherheit

Auf Anfrage

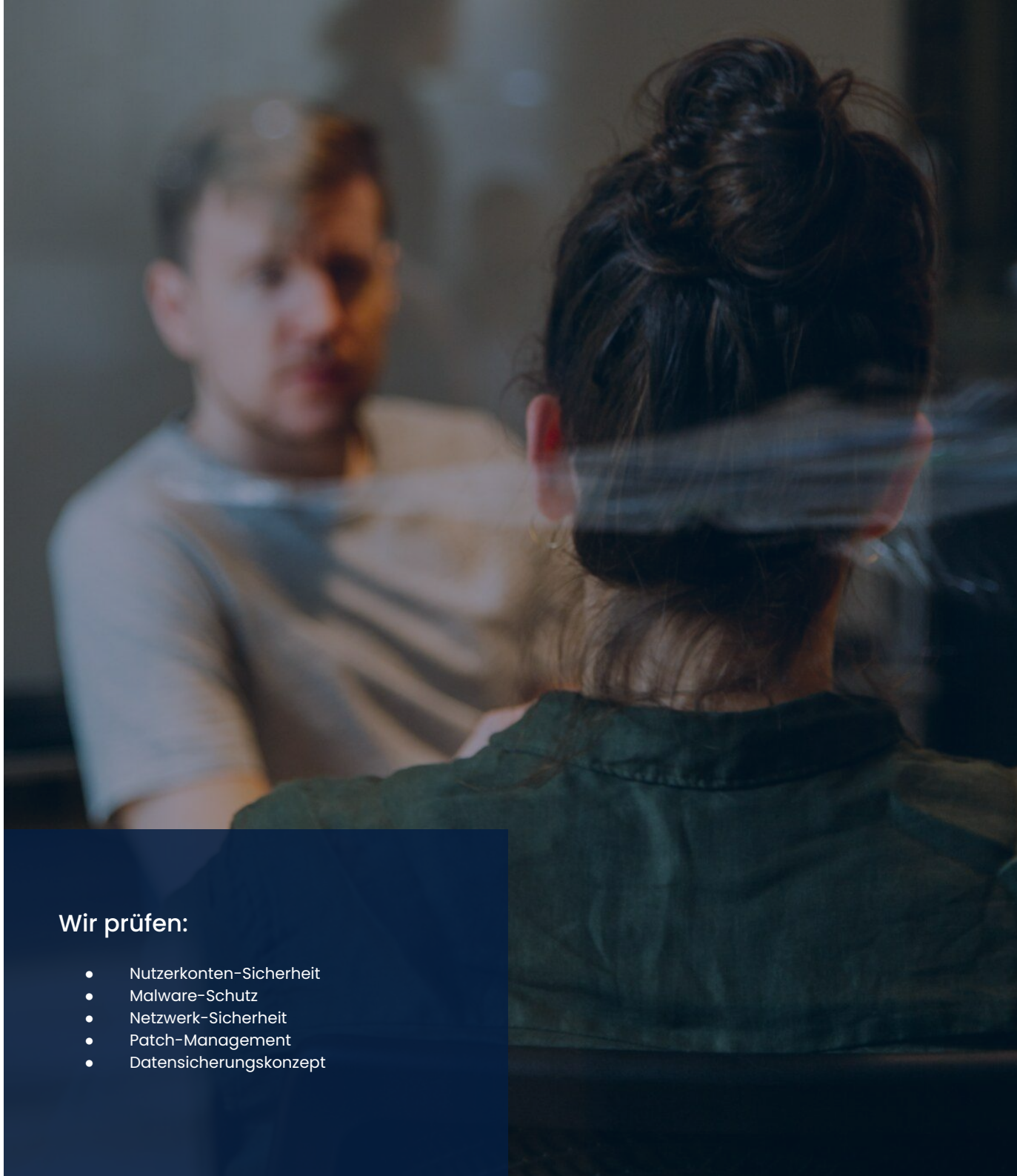
Cyber Risiko Dialog

Alle Cyberrisiken im Blick: Individuelle Tiefenanalyse Ihrer IT-Sicherheit mit konkreten Handlungsempfehlungen Gemeinsam mit Cybersicherheitsexperten beleuchten Sie die Stärken und Schwächen der IT-Sicherheit Ihres Unternehmens – weit über eine klassische Auditierung hinaus. Außerdem erhalten Sie konkrete und individuelle Handlungsempfehlungen unter Berücksichtigung aktueller Branchen-Benchmarks.

Das bietet Ihnen der Cyber Risiko Dialog:

- Ganzheitlichen Einblick in das Sicherheitsniveau Ihres Unternehmens
- Validierung des Cybersicherheitsstatus in einem gemeinsamen Austausch: Dialog statt Prüfsituation
- Standardübergreifende Bewertung – basierend auf einer breiten Branchen- und Markterfahrung
- Aussagekräftige Informationen über die Widerstandsfähigkeit Ihrer IT
- Identifikation konkreter Schwachstellen in Ihrer IT-Sicherheitsorganisation
- Nachhaltige Verbesserungsmaßnahmen, die auf Ihr Unternehmen und Ihre Bedürfnisse abgestimmt sind

Jetzt Angebot anfragen



Wir prüfen:

- Nutzerkonten-Sicherheit
- Malware-Schutz
- Netzwerk-Sicherheit
- Patch-Management
- Datensicherungskonzept

Auf Anfrage

Cybernotfall-Management

Gute Prävention ist unerlässlich. Doch gerade im Ernstfall zeigt sich, wie gut die Cybersicherheit eines Unternehmens wirklich aufgestellt ist. Perseus unterstützt Unternehmen bei der Vorbereitung für Cybernotfälle.

Dazu gehören bspw. das Stellen eines **Notfallplans** oder von spezifischen IT-Richtlinien-Sets. Unsere **24/7 Notfallhilfe** verbindet Sie im Ernstfall zu jeder Zeit mit unseren Fachleuten für Cybersicherheit. Und im Anschluss auf einen Cybernotfall hilft die **Cyberforensik** bei **Schadensbewertung** und angepasster Systemverbesserung.

Unsere Services für Ihr Cybernotfall-Management

- Mit unseren Notfallplänen vermeiden Sie Fehlverhalten und Panik der Angestellten im Ernstfall
- Unsere Leistungen fördern eine offene Kommunikation für Risiken und Gefahren im Unternehmen. Nur aufgeklärte und vorbereitete Mitarbeitende handeln im Notfall selbstbewusst und richtig
- Sie und Ihre Mitarbeitenden erreichen unsere Krisenmanager für Cybernotfälle rund um die Uhr, sieben Tage die Woche
- Die Fachleute unserer Cyberforensik übernehmen die Schadensbewertung und unterstützen Sie bei der Optimierung der Systeme

Auf Anfrage

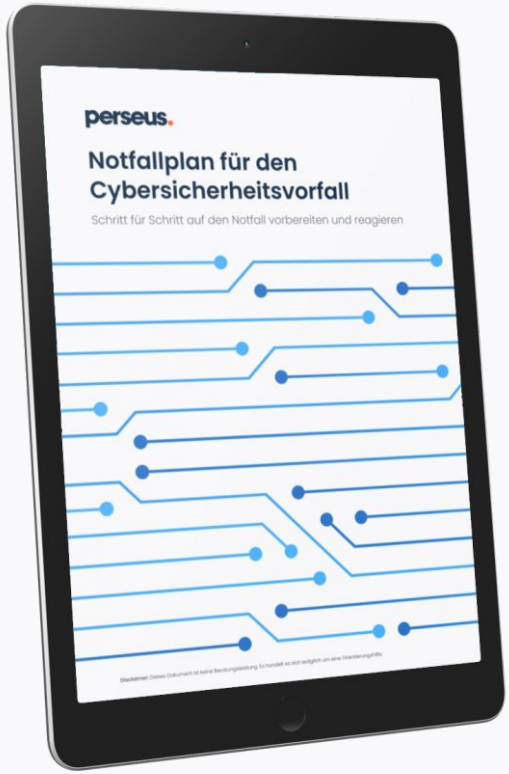
IT-Notfallplan

Bereiten Sie Ihr Unternehmen und Team auf einen IT-Ausfall oder IT-Störfall vor. Unser Notfallplan soll Ihre Mitarbeitenden optimal dafür rüsten, im Notfall richtig zu reagieren. Nur so können teure Schäden verhindert oder minimiert werden.

Unser Notfallplan ist mehr als nur eine Notfallkarte mit den wichtigsten Handlungsanweisungen im Störfall. Betrachten Sie den Plan als detaillierten Leitfaden, um sich der individuellen Sicherheitslage Ihres Unternehmens bewusst zu werden und diese im Notfall zu verteidigen.

Jedes Unternehmen ist anders, daher kann es keinen allgemein gültigen Plan für alle Unternehmen geben. Mit Hilfe unseres Notfallplans arbeiten Sie und Ihre Mitarbeitenden sich durch alle wichtigen Aspekte, die in Vorbereitung auf einen eventuellen Notfall wichtig sind.

Jetzt Angebot anfragen



45 Seiten als digitales Dokument (**PDF**) mit leicht verständlichen Handlungsanweisungen und Informationen sowie Platz zum strukturierten Festhalten Ihrer unternehmensspezifischen Daten. Damit alles an einem Ort versammelt ist.

Vorteile des IT-Notfallplans von Perseus im Überblick

- Cyberrisiken beherrschbar machen
- Gewappnet sein für Cyberattacken
- Konkrete Maßnahmen für den Cybernotfall erstellen
- Alle wichtigen Informationen an einem Ort
- Individualisierbar für jedes Unternehmen
- Mitarbeitenden Sicherheit und Handlungsfähigkeit im Notfall geben

Auf Anfrage

24/7 Notfallhilfe

Vom Verdachtsfall über Abwehr bis zur Dokumentation

Unsere Expertinnen und Experten unterstützen Sie rund um die Uhr – auch beim kleinsten Verdacht auf einen Cyberangriff. Per Telefon, E-Mail und (falls notwendig) via Fernwartung. Selbstverständlich behandeln wir Ihr Anliegen vertraulich.

Cybervorfälle sind ein Wettlauf gegen die Zeit. Nur wer jetzt schnell handelt, kann finanzielle Schäden und Image-Schäden vermeiden. Unsere IT-Sicherheitsfachleute stehen Ihnen Tag und Nacht zur Seite. Ganz gleich ob Ernstfall oder Verdacht.*

Jetzt Angebot anfragen

*Die Kosten für die Leistungen der Notfallhilfe sind abhängig vom Umfang der vollbrachten Aufwände. Stundensätze werden abhängig von Ihrem spezifischen Vertrag berechnet.

24h-Notfall-Hotline

Sie erreichen unseren Kundendienst und unsere Cyber-Fachleute rund um die Uhr, sieben Tage die Woche. Sie vermuten einen Cybervorfall? Verlieren Sie keine Zeit. Die Mitarbeitenden für Incident Management nehmen sich Ihrem Notfall an.

Erstberatung

Unsere Kundenberaterinnen und Berater besprechen mit Ihnen den gemeldeten Cybervorfall. Es folgt die Aufnahme aller relevanten Daten und Informationen zum Vorfall sowie eine erste Beurteilung. Sollte sich Ihr Verdacht bestätigen, werden ggf. Sofortmaßnahmen empfohlen.

Beweisaufnahme

Nach dem bestätigen Cybervofall bauen wir ggf. einen sicheren Fernzugriff auf, um uns ein genaues Bild der betroffenen Systeme zu machen. Gesammelte Beweise dienen als Orientierung für alle weiteren Maßnahmen.

Analyse

Wir führen eine umfassende Beurteilung des Vorfalls durch und entscheiden, welche Maßnahmen Schäden vermindern oder eindämmen können. Hierzu gehören die Identifizierung der Angriffsquelle, die Rekonstruktion der Ereignisse sowie die Evaluierung des Kompromittierungsniveaus (Impact Analyse).

Abwehr- & Bereinigungsstrategie

Erfahrungsgemäß können wir in 98 % der Anfragen bereits über Telefon und Fernwartung die potenziellen Cybervorfälle unserer Mitglieder klären bzw. beheben. Zu diesen effizienten Maßnahmen gehört die punktuelle Erarbeitung einer Abwehr- & Bereinigungsstrategie, die den Angreifer aussperrt (Lock-out), die Systeme bereinigt und somit vor weiteren Schäden bewahrt. Ggf. erfolgt ein zeitlich begrenztes Monitoring der Aktivitäten.

Weitere Leistungen auf der nächsten Seite

Auf Anfrage

24/7 Notfallhilfe

Über Telefon, E-Mail oder Kontaktformular

Notfälle können Sie uns per Telefon oder Kontakformular über den Mitgliederbereich melden. Einfach auf “Notfallhilfe” klicken und die wichtigsten Informationen telefonisch oder per Formular an uns weiterleiten. Wir melden uns dann schnellstmöglich bei Ihnen. Selbstverständlich werden alle Ihre Anliegen streng vertraulich behandelt.
Erfahrungsgemäß lässt sich ein Großteil der Fälle schon im Rahmen der ersten Kontaktaufnahme klären.

Jetzt Angebot anfragen

Datenrettung

Je nach Art des Cybervorfalls oder Angriffs können Daten kompromittiert bzw. unzugänglich sein. Wir sorgen dafür, dass Sie wieder vollständigen Zugriff auf Ihre geschäftlichen Daten bekommen.

Wiederherstellung

Kommt es im Rahmen eines Vorfalls zur Beschädigung oder Entfernung von Daten, initiieren unsere Fachleute eine Wiederherstellung der verlorengegangen Daten.

Beweissicherung

Während unsere Fachleute die akute Gefahr abwehren, sammeln sie Beweismittel für die anschließende Strafverfolgung der Cyberkriminellen. Sollte es zu einem Erpressungsversuch kommen, führen wir eine aktive Krisenberatung durch.

Handlungsempfehlung

Schädliche Cybervorfälle sind meist das Resultat von bestehenden Schwachstellen in der IT-Sicherheit. Zusätzlich zu den Maßnahmen, die wir zum Schließen der akuten Sicherheitslücken durchgeführt haben, entwickeln wir präventive Handlungsempfehlungen für Sie, um zukünftigen Vorfällen vorzubeugen.

Fortführende Maßnahmen

Sollte der Cybervorfall größere Ausmaße angenommen haben, kann dieser eventuell nicht abschließend via Fernwartung behandelt werden. Wir koordinieren die weiteren Maßnahmen mit Ihrer internen IT sowie externen IT-Expertinnen und Experten vor Ort.

Dokumentation

In unserem Abschlussbericht fassen wir Ihnen die wichtigsten Erkenntnisse des Cybervorfalls zusammen. Dies ist ein mehrseitiger Bericht, der unter anderem eine Chronik der Ereignisse, mögliche Ursachen und Handlungs-empfehlungen umfasst. Diese durch Fachleute erstellte Dokumentation ist Voraussetzung, um Meldepflichten und Versicherungsanforderungen nachzukommen.

Auf Anfrage

Cyberforensik

Die Cyberforensik von Perseus bietet eine detaillierte Übersicht bzw. die intensive Analyse eines Cybervorfalls und wird in Form eines Berichts im Nachgang zur Verfügung gestellt. Unser Team erstellt nach Abschluss des Cybervorfalls einen umfangreichen forensischen Bericht, der entweder dem Kunden, der Versicherung oder beiden zur Verfügung gestellt wird. Ein Forensikbericht kann im Zuge eines Cybervorfalls als Entscheidungsgrundlage dienen, ob der entstandene Schaden gedeckt wird oder nicht.

Schadensbewertung

Die Schadensbewertung hilft bei der Optimierung der IT-Sicherheitsinfrastruktur. Im Nachgang eines Cybervorfalls wird mit Hilfe des forensischen Berichts und der Analyse der vorhandenen Informationen sowie der Infrastruktur des Kunden eine Sammlung konkreter Verbesserungsvorschläge und Handlungsempfehlungen erstellt. Die konkreten Handlungsempfehlungen sowie eine Begründung, warum diese implementiert werden sollten, tragen dazu bei, dass zukünftige Cybervorfälle vermieden werden können.

In Zukunft sicher mit Perseus

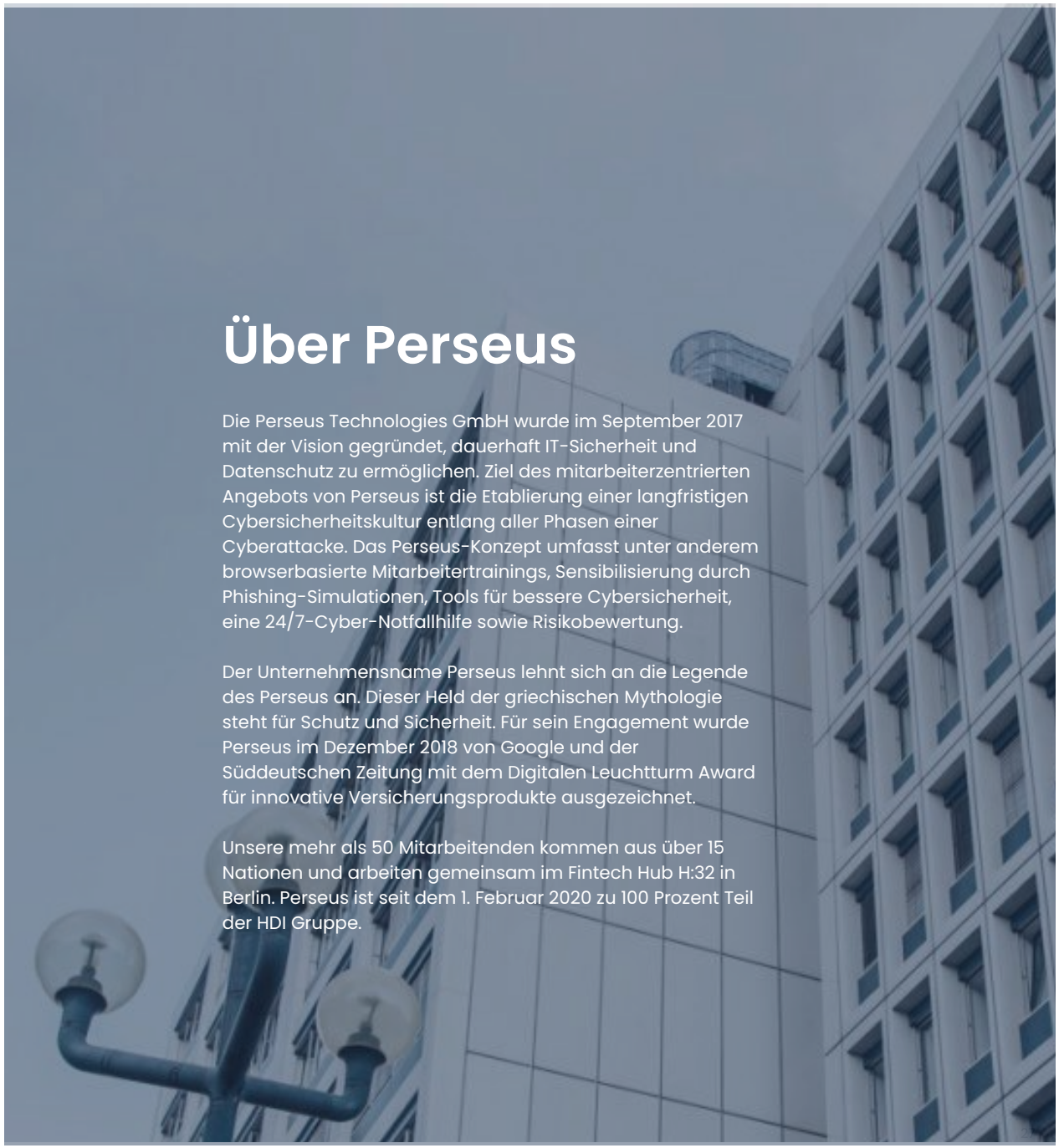
Online-Portal für Cybersicherheit

Jetzt Demo anfragen

Sie haben Fragen? Wir sind für Sie da.

Hagelberger Str. 53-54
10965 Berlin

030/95 999 80 80
support@perseus.de



Über Perseus

Die Perseus Technologies GmbH wurde im September 2017 mit der Vision gegründet, dauerhaft IT-Sicherheit und Datenschutz zu ermöglichen. Ziel des mitarbeiterzentrierten Angebots von Perseus ist die Etablierung einer langfristigen Cybersicherheitskultur entlang aller Phasen einer Cyberattacke. Das Perseus-Konzept umfasst unter anderem browserbasierte Mitarbeitertrainings, Sensibilisierung durch Phishing-Simulationen, Tools für bessere Cybersicherheit, eine 24/7-Cyber-Notfallhilfe sowie Risikobewertung.

Der Unternehmensname Perseus lehnt sich an die Legende des Perseus an. Dieser Held der griechischen Mythologie steht für Schutz und Sicherheit. Für sein Engagement wurde Perseus im Dezember 2018 von Google und der Süddeutschen Zeitung mit dem Digitalen Leuchtturm Award für innovative Versicherungsprodukte ausgezeichnet.

Unsere mehr als 50 Mitarbeitenden kommen aus über 15 Nationen und arbeiten gemeinsam im Fintech Hub H:32 in Berlin. Perseus ist seit dem 1. Februar 2020 zu 100 Prozent Teil der HDI Gruppe.

VW_012023