perseus.

Cybersicherheit auf den Punkt

Fit für Cybersicherheit in Zeiten von Corona und Homeoffice
und darüber hinaus.

Ihr Referent

Johannes Vakalis

Senior Sales Manager

johannes.vakalis@perseus.de

Agenda

(1) Warum Cybersicherheit so wichtig ist

(2) Warum Awarenesstraining so wichtig ist

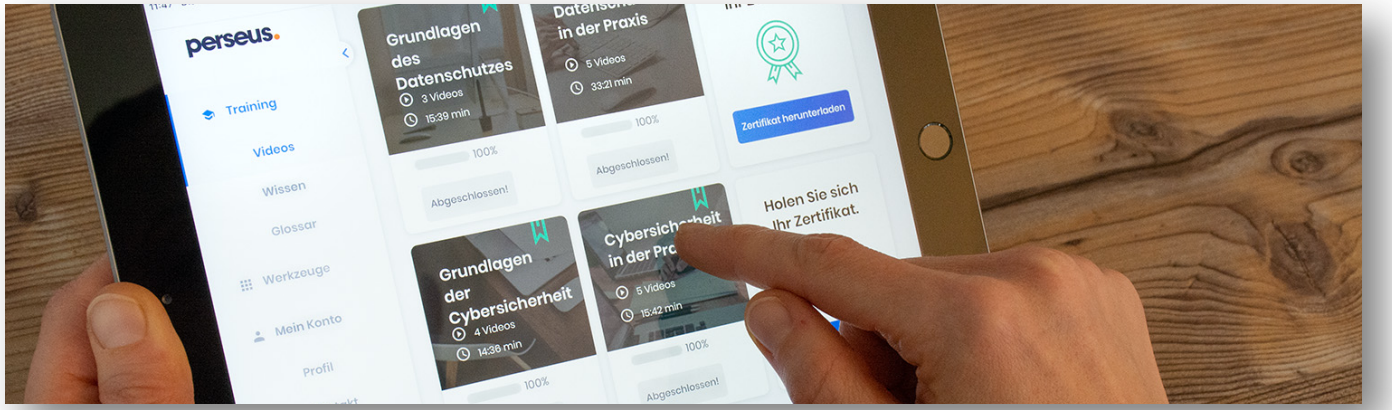
(3) Grundlagen der Cybersicherheit

(4) Cybersicherheit in der Praxis

(5) Lösungsvorschlag von Perseus

(6) Detaillierte Beschreibung der Sicherheitspakete

(7) Fragen & Antworten



Warum Cybersicherheit so wichtig ist

Ein globales Problem mit nationaler Dimension

100 Mrd.

Vernetzte Geräte bis 2030

600 Mrd. $

Kosten durch Cyberattacken

ca. 1,39%

vs. 0,6 - 0,8% global

Warum Cybersicherheit so wichtig ist

Cyberattacken und Datendiebstahl gehören zu den Top-Risiken der kommenden Jahre.

Global Risk Report **2015**		Global Risk Report **2020**
1. Zwischenstaatlicher Konflikt		1. Wetterextreme
2. Wetterextreme		2. Scheitern des Klimaschutzes
3. Versagen nationaler Regierungen		3. Naturkatastrophen
4. Staatszusammenbruch		4. Verlust der biologischen Vielfalt
5. Arbeitslosigkeit		5. Menschengemachte Umweltschäden
6. Naturkatastrophen		6. **Datendiebstahl**
7. Scheitern des Klimaschutzes		7. **Cyberattacken**
8. Wasserkrise		8. Wasserkrise
9. **Datendiebstahl**		9. Globales Regierungsversagen
10. **Cyberattacken**		10. Platzen der Vermögensblasen

vs.

Warum Cybersicherheit so wichtig ist

Nicht ob, sondern wann!

Ereignis	Wahrscheinlichkeit
Cyberangriff	1 zu 4
Wohnungseinbruch	1 zu 354
Golf: Hole-in-One	1 zu 3.000
Blitzschlag	1 zu 250.000
Bärenattacke im Yellowstone Nationalpark	1 zu 2.700.000
Haiangriff	1 zu 3.750.000
Tödlicher Flugzeugabsturz	1 zu 16.000.000
Lottogewinn	1 zu 140.000.000

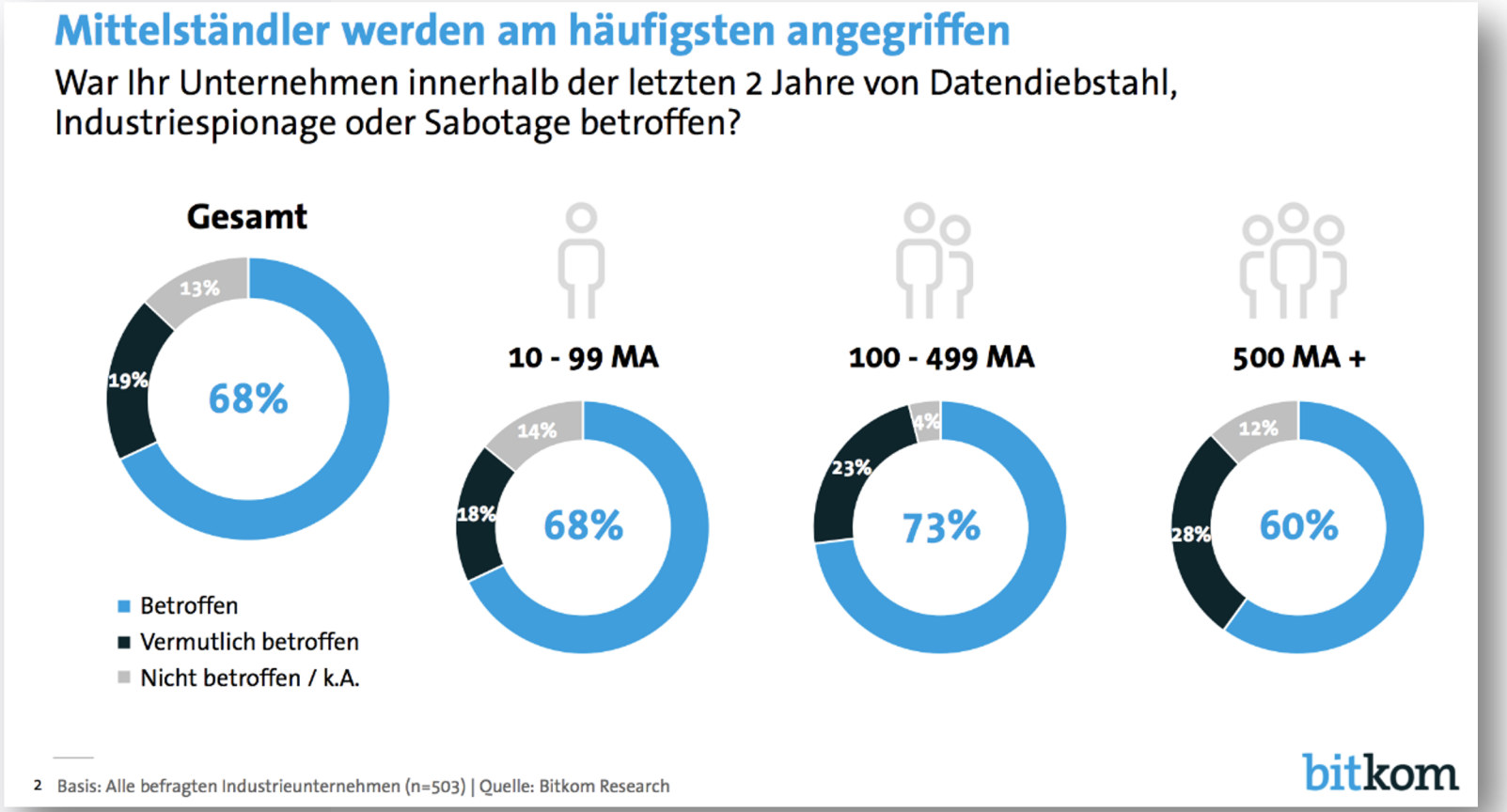
1 zu 4

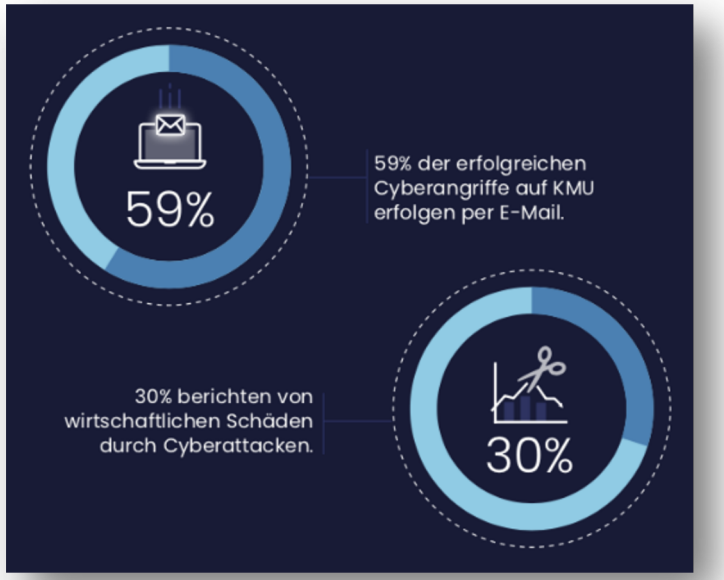
Wahrscheinlichkeit Opfer eines Datendiebstahls durch einen Cyberangriff zu werden

Quelle: Blog Wirtschaftswoche / Varonis |

Warum Awarenesstraining so wichtig ist

Zahlen – Daten – Fakten





41.000€

Durchschnittliche Höhe des finanziellen Schadens eines Cyberangriffs für ein mittelständisches Unternehmen

Warum Awarenesstraining so wichtig ist

Die häufigsten Arten von Cybersicherheitsvorfällen

Abfischen von Informationen (Phishing)

Schadprogramme (Malware)

Gezielte Manipulation (Social Engineering)

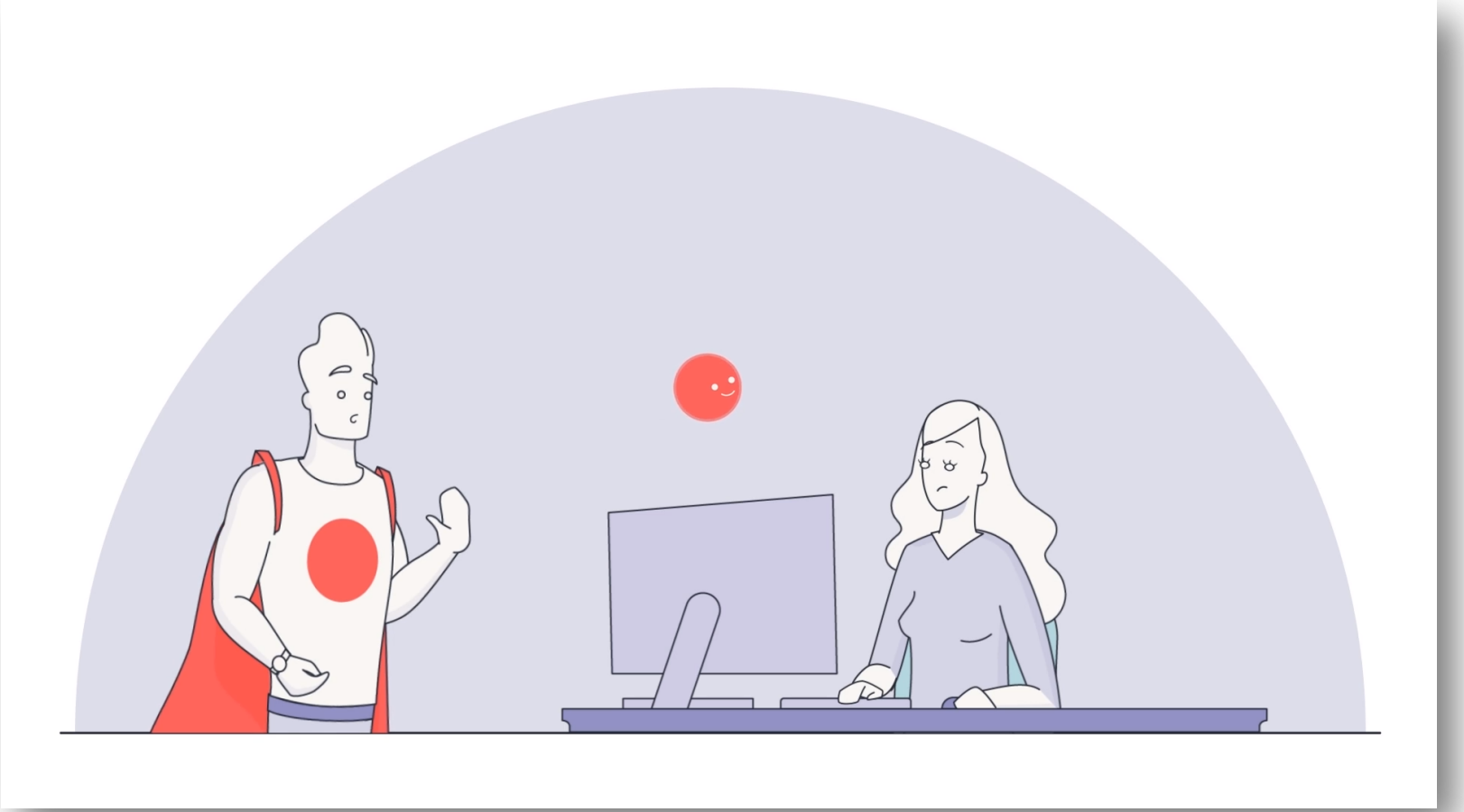
Kompromittierte Webanwedungen

46% der Cybervorfälle werden durch die eigenen, zumeist ungeschulten Mitarbeiter verursacht.

Grundlagen der Cybersicherheit

Was ist Cybersicherheit?

- Echtheit von E-Mails
- E-Mail-Adresse mit bösartigen Inhalten
- Sicherheitsrisiko USB-Stick
- VPN



Grundlagen der Cybersicherheit

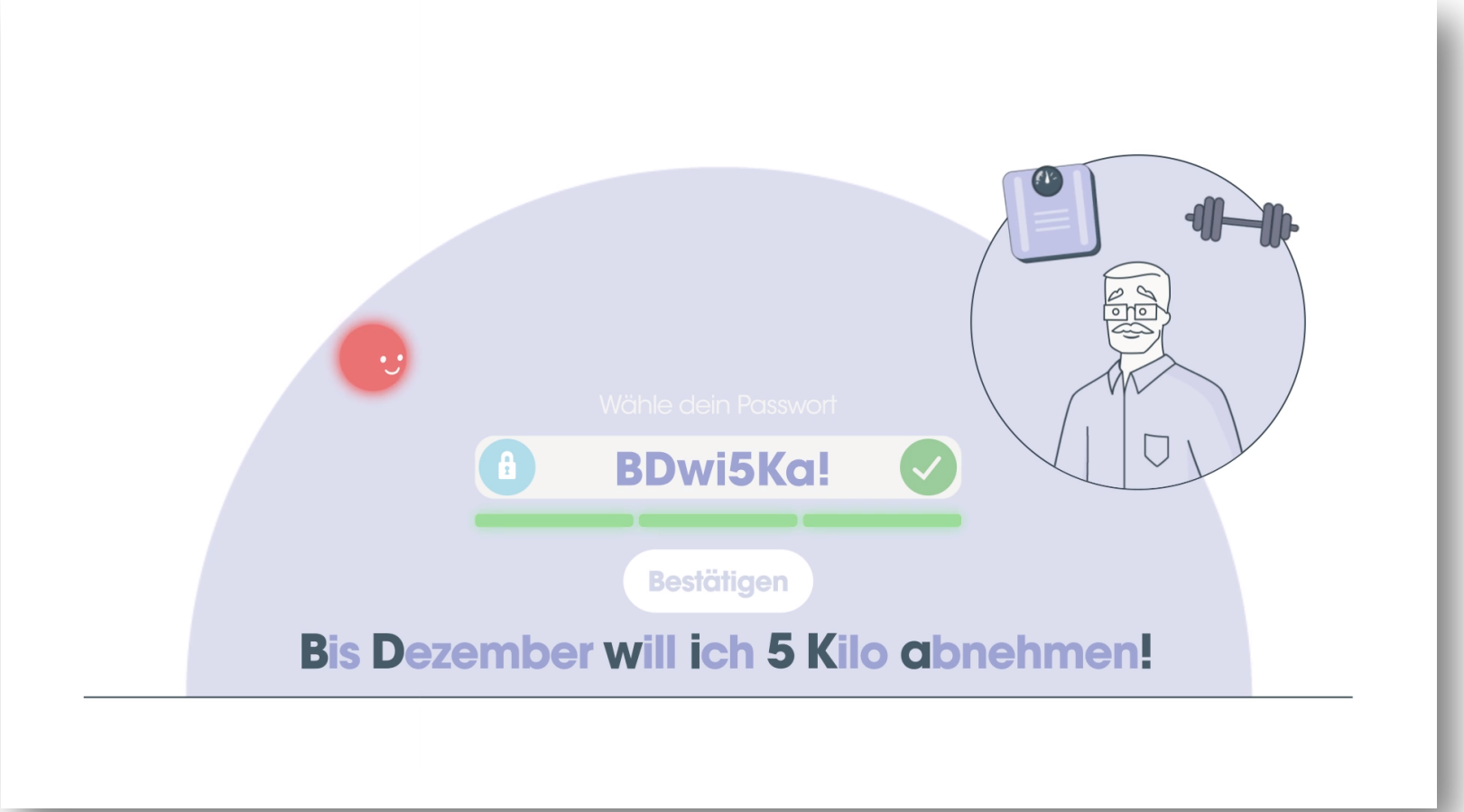
Sechs typische Cybersicherheitsfehler

- Automatische Updates
- PC ausschalten
- Sichere Passwörter wählen
- Regelmäßige Sicherheitskopien
- Firewall und Anti- Virus Software
- Administratorenrechte

Grundlagen der Cybersicherheit

Ist Ihr Passwort sicher?

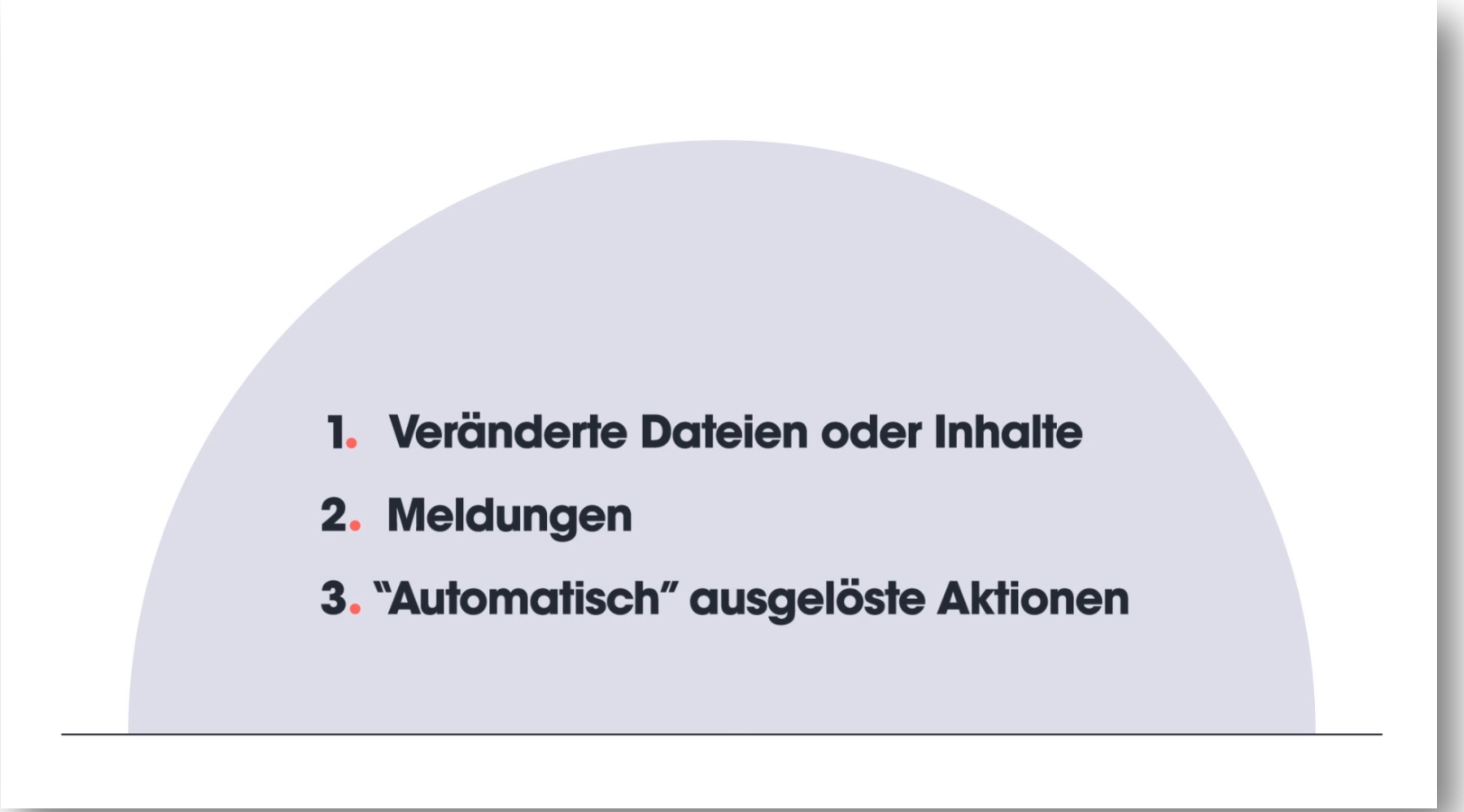
- Passwort-Management-Tool
- Zwei-Faktor-Authentifizierung
- Sichere Passwörter



Grundlagen der Cybersicherheit

Erkennen und Melden eines Cyberangriffs

- Erkennen von Cyberangriffen:
  - Veränderte Dateien oder Inhalte
  - ungewöhnliche Meldungen
  - scheinbar „automatische“ Aktionen
  - Windows-Fehlermeldungen (prüfen)
  - Lösegeldforderungen
  - Fakehacks
- Wie reagieren?
  - IT- Ansprechpartner kontaktieren (persönlich oder per Telefon) - Falls dieser nicht erreichbar ist- den Vorgesetzten Informieren!
  - Vom Netz trennen!
  - Dokumentation durch schriftl. Notizen oder Fotos über Fehlermeldungen oder Weiterleitungen

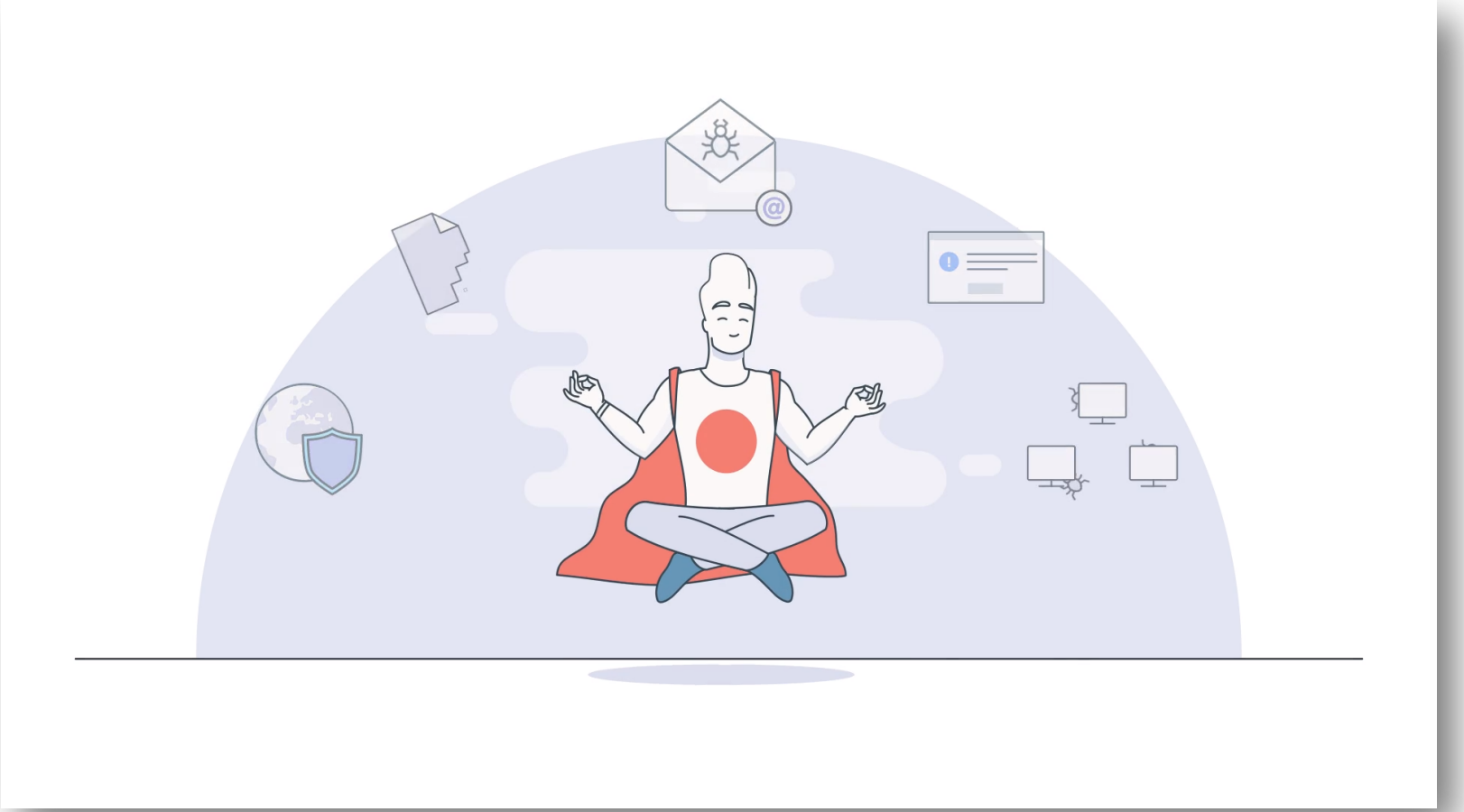


Cybersicherheit in der Praxis

Das Erste Hilfe-Set: Die richtigen Fragen

- Nach einer Cyberattacke hilft (Perseus gemeinsam mit dem) der IT-Beauftragte(n). Dazu sollten folgende Fragen beantwortet/vorbereitet werden:

- Ungewöhnliche Downloads/ Installationen aufgefallen?
- „Merkwürdige“ E-Mail geöffnet?
- Fremder USB- Stick (oder Gerät) genutzt?
- Wann ist der Vorfall passiert und wer hat ihn zuerst registriert? Was ist danach geschehen? PC weiter genutzt?
- Polizei oder Rechtsanwalt kontaktiert?
- ggf. gerichtliches Verfahren gewünscht, da ein interner MA verdächtigt wird?



Cybersicherheit in der Praxis

E-Mail-Echtheitscheck

- Kriterien zur Prüfung
  - Vergleich von Name des Absenders und E-Mail-Adresse. Kein Firmenname und/ oder das Kürzel nach dem @ ist nicht plausibel? Hinweise auf Betrug!
  - Passt die Anrede? Gibt es eine personalisierte Anrede?
  - Durch Druck/ Neugierde/ Angst soll eine Handlung vom MA erreicht werden?
- Überprüfung von Links
  - „Berühren“ des Links > wirkt die Einblendung der Linkadresse im unteren Rand plausibel?

Cybersicherheit in der Praxis

Was ist Spear Phishing und wie schützen Sie sich davor?

- Häufig imitierte Personenkreise: „schlüssige“ Kollegen, Vorgesetzte inkl. Kommunikationsstil und personalisierter Anrede
- Zielgruppe für Spear-Phishing-Angriffe: Führungskräfte, MA aus Finanz- und Personalabteilung und auch IT-Verantwortliche
- Schutz vor Spear Phishing
- Schutz persönlicher Daten im Internet

Cybersicherheit in der Praxis

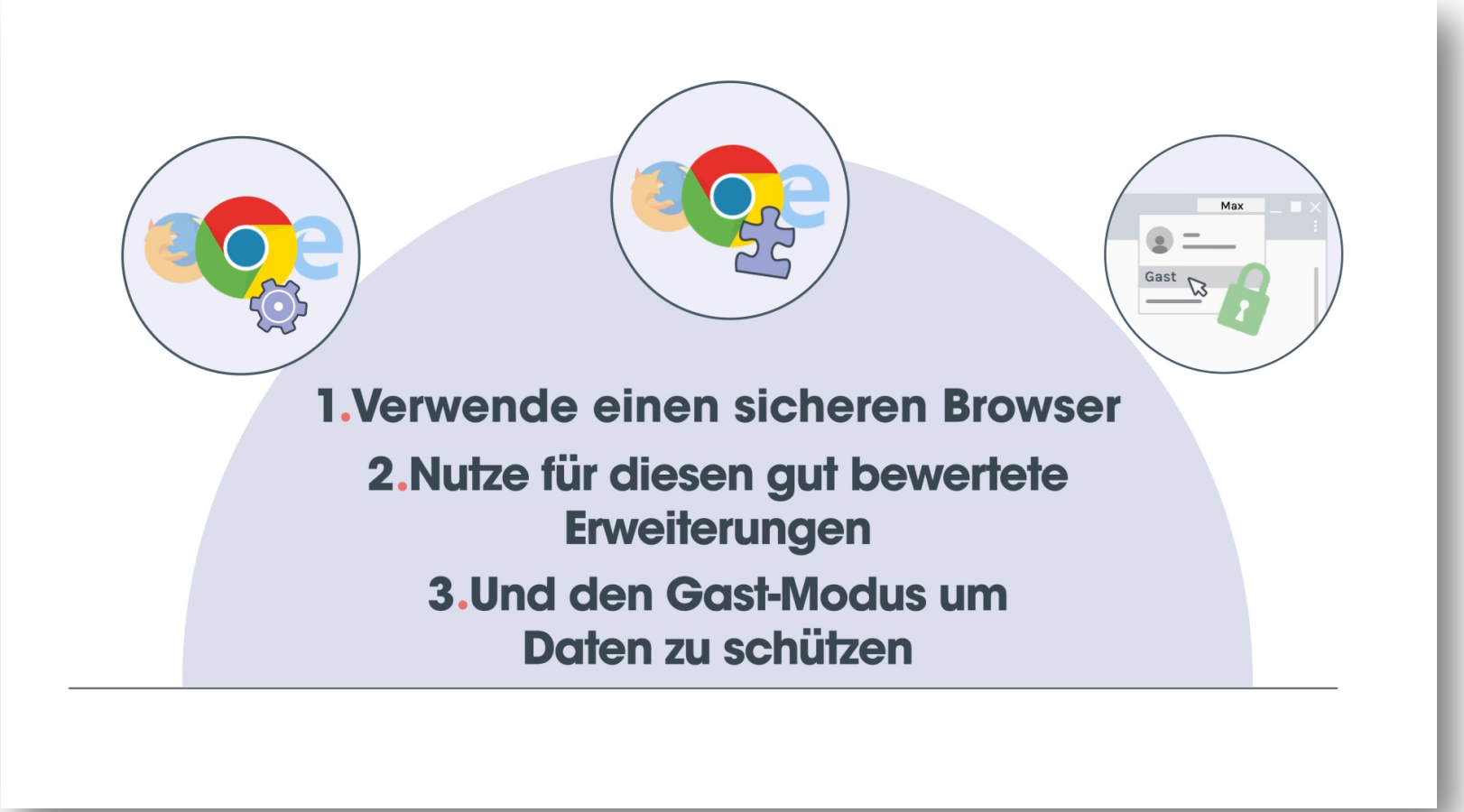
Sicheres Mobiles Arbeiten

- Sichere Internet-Verbindungen WLAN sicher? Entsprechende Symbole und Hinweise beachten!
- Browser sicher? Achten Sie auf das Symbol neben der Internetadresse!
- Sie sollten die Verschlüsselung der Festplatte einrichten!
- Speichern Sie wichtige Daten in einer sicheren Cloud!

Cybersicherheit in der Praxis

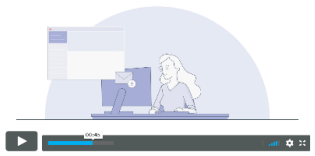
Sicheres Surfen im Netz

- Sicherer Browser
- Sicherheit ist Einstellungssache z.B.:
  Chrome: „Sicherheit und Datenschutz“ > aktivieren Sie: „Schutz vor schädlichen Websites“ und „Do not Track“ weitere Einstellungen:
  - Geheimhaltung des Standorts
  - Blockieren von Pop Ups
  - keine automatischen Aktionen/ immer Fragen
- Adblocker
- Browser-Updates
- Nutzen Sie den Gastmodus für Kollegen oder Kunden



Mitarbeiter-Awareness ist keine einmalige Angelegenheit

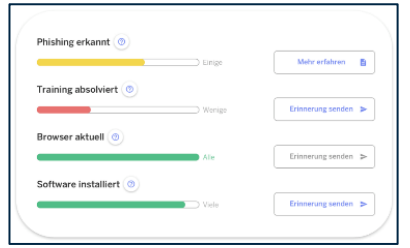
geringes Bewusstsein



Mitarbeiter Trainings

Phishing

Aktivierung



Monitoring

intitiale Situation → **Training** → **Verankerung** → **Verhaltens-änderung**

Bewusstsein erhöhen

alte Verhaltensformen durch neue ersetzen

messbar höhere Cybersicherheit

Lösungsvorschlag von Perseus

Cybersicherheit auf den Punkt - mehr als ein Slogan. Ihr Rundumsorglospaket.

Perseus 360° ist die erste ganzheitliche Cybersicherheits-Plattform für den deutschen Mittelstand.

Mehr als 3000 Unternehmen
… nutzen bereits Perseus zum Schutz vor Cyberangriffen.

Ca. 40% des deutschen Cyber-Versicherungsmarktes
… wird von Perseus' Partnern abgedeckt.

Detaillierte Beschreibung der Sicherheitspakete

Alle Lösungen in einem Paket

- **Fragen? & Antworten!**

Vielen Dank!

Sollten Sie noch Fragen haben – wir sind für Sie da!

Johannes Vakalis

Senior Sales Manager

johannes.vakalis@perseus.de