Berliner Volksbank

perseus.

„Cyberattacken rechtzeitig erkennen und sicher abwehren“

Online-Seminar am 31. Mai 2022

Ihr Moderator

Klaus Martin-Steinmüller I Berliner Volksbank

- **Bankkaufmann/Dipl. Bankbetriebswirt (BA)**
- **über 38 Jahre bei der Berliner Volksbank eG**
- **als Leiter und Experte für Finanzierungsfragen prägen vielfältige Aufgaben seine Vita:**
  - Aufbau und Leitung der ImmobilienCenter
  - Aufbau und Leitung unserer Tochter Berliner Volksbank Immobilien GmbH
  - Aufbau und Leitung der BauFinanzierungsCenter
  - Leitung der Firmenkunden KomptenzCenter Ausland, Gründer, Ärzte, Institutionelle Kunden

Ihr Versicherungs-Experte

Lars Bielow I R+V Versicherung

- Leiter Bankenvertrieb Berlin, R+V Versicherung
- Lars Bielow ist Bezirksdirektor bei der R+V Versicherung und leitet den Firmenkundenbereich in Berlin in der Zusammenarbeit mit der Berliner Volksbank. Er ist seit 21 Jahren in der Versicherungsbranche tätig und hat in der Vergangenheit unterschiedliche Aufgaben im Firmenkundensegment wahrgenommen.
- Cyberattacken gehören seit geraumer Zeit auch für Versicherungskonzerne zum Alltag, mit überdurchschnittlich wachsenden Schadensfällen pro Jahr.

Ihr Referent der heutigen Veranstaltung

Johannes Vakalis - Head of Sales & Marketing

Johannes Vakalis

perseus.
Cybersicherheit auf den Punkt

Head of Sales & Marketing

Perseus Technologies GmbH

Berliner Unternehmen für Cyber Security, Incident Management & Risk Assessment

Agenda

1. Die aktuelle Cybersicherheitslage in Deutschland
2. Die Auswirkungen des Russland/Ukraine-Konflikts auf die Cybersicherheitslage
3. Mögliche Angriffsmuster (inkl. aktueller Cyberangriffe)
4. Abwehrmöglichkeiten durch Prävention
5. Handlungsempfehlungen und Absicherung für den Cybernotfall

Warum Prävention so wichtig ist

1. 9 von 10 Unternehmen (88%) 2020/2021 von Cyberangriffen betroffen
2. Schäden für die deutsche Wirtschaft belaufen sich auf 223 Milliarden EUR
3. Seit 2018/2019 haben sich die Schäden mehr als verdoppelt
4. 59 % der Unternehmen sagen, dass die vorgekommenen IT-Sicherheitsvorfälle auf Heimarbeit zurückzuführen sei
5. Faktor Mensch nach wie vor Einstiegstor Nummer 1

Quelle: Bitkom Research 2021

1 zu 4

Wahrscheinlich-keit Opfer eines Cyberangriffs oder Datendiebstahls zu werden!

Wohnungseinbruch
1 zu 354

Bärenattacke im Yellowstone Nationalpark
1 zu 2.700.000

Blitzschlag
1 zu 250.000

Tödlicher Flugzeuansturz
1 zu 16.000.000

Haiangriff
1 zu 3.750.000

perseus.

Source: Blog Wirtschaftswoche / Varonis

Die aktuelle Cybersicherheitslage

Einblick auf die Gefahrenlage in Deutschland allgemein

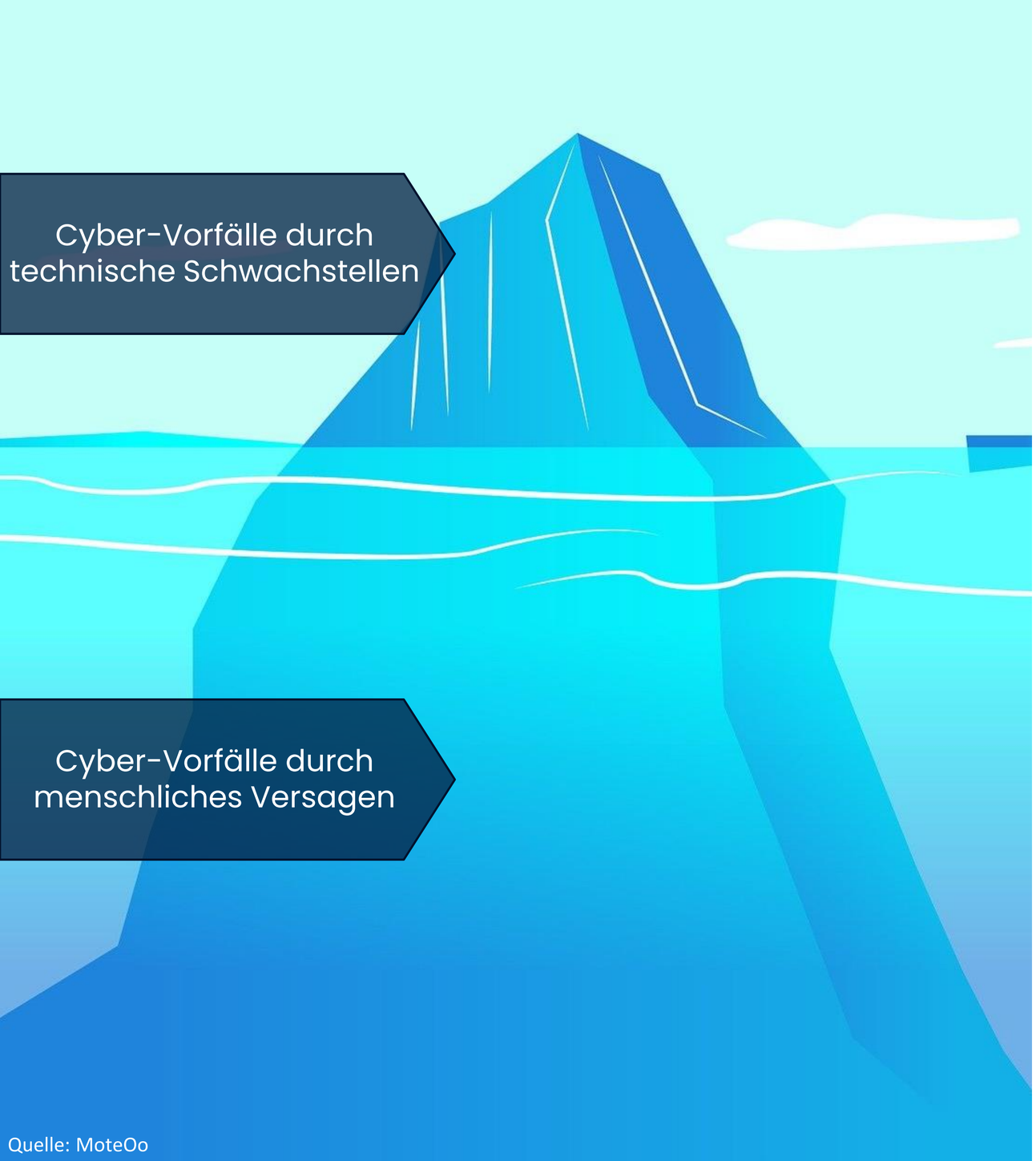
ø 73.000 €
finanzieller Schaden im Mittelstand pro Cybervorfall

47 % aller Mitarbeitenden erhalten wöchentlich mind. eine Spam E-Mail

21 % aller Mitarbeitenden erhalten mehr als 5 Spam E-Mails wöchentlich

Fast 60 % aller erfolgreichen Cyberangriffe setzen auf Phishing-E-Mails

Quelle: bitkom



Quelle: MoteOo

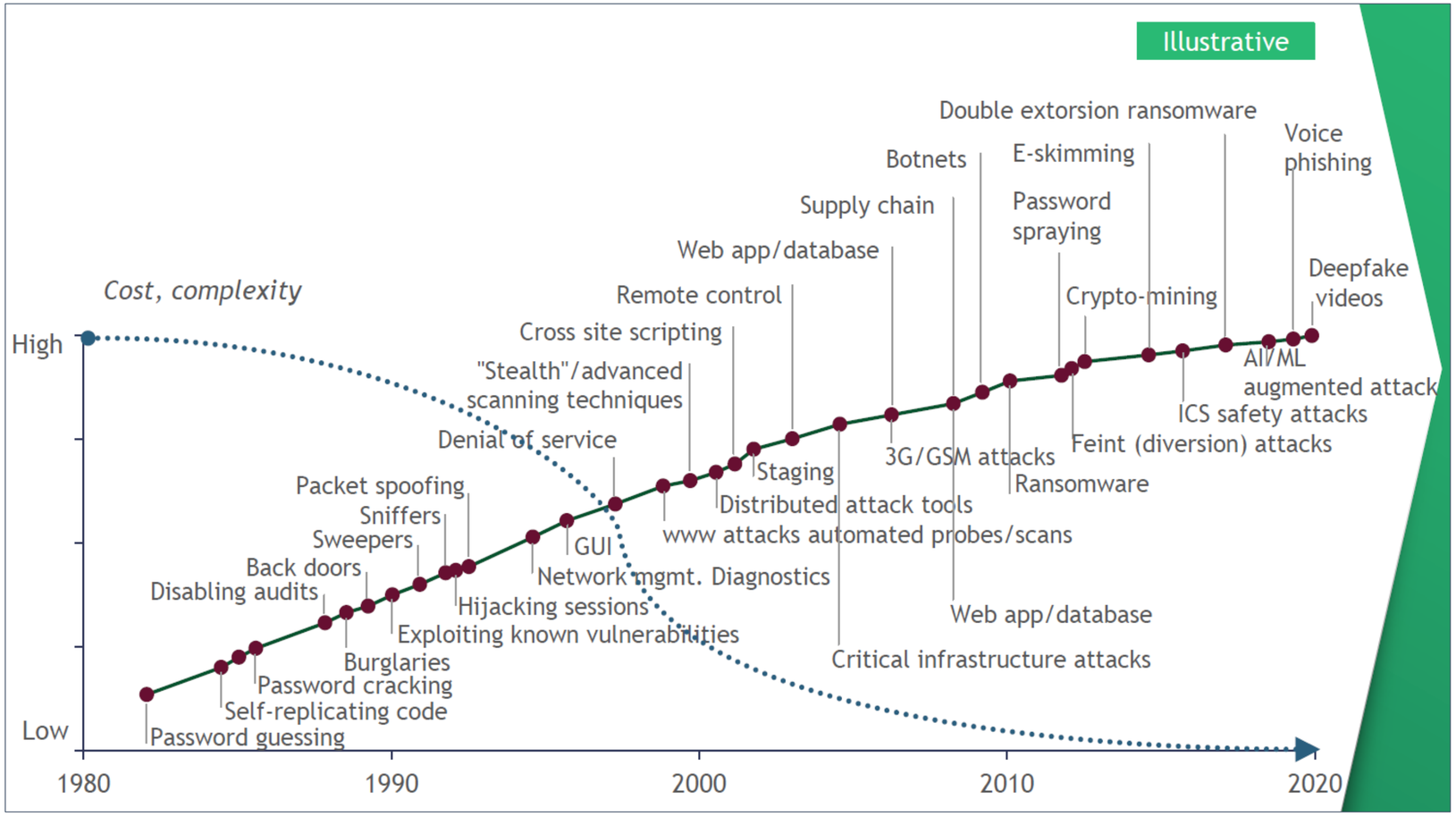
perseus.

Cybersicherheit auf den Punkt

Deswegen zielt unser Angebot auf die Hauptursache erfolgreicher Cyberangriffe

Die aktuelle Cybersicherheitslage

Einblick auf die Gefahrenlage in Deutschland allgemein



Deutliche **Kostendegression** bei gleichzeitiger **Komplexitätssteigerung** der Angriffe

perseus.

Quelle: Research Boston Consulting Group

Die aktuelle Cybersicherheitslage

Die Auswirkung des aktuellen Russland/Ukraine-Konflikts

Hessisches Ministerium
der Finanzen
Der Minister

HESSEN

Hessisches Ministerium der Finanzen · Postfach 3180 · 65021 Wiesbaden

Geschäftszeichen O1976 A-64-I6
Dokument-Nr.

Bearbeiter/in Herr Hohmann
Durchwahl (06 11) 3213 - 2275
Telefax:
Email: Kritis@hmdf.hessen.de
Ihr Zeichen
Ihre Nachricht

Datum 7. März 2022

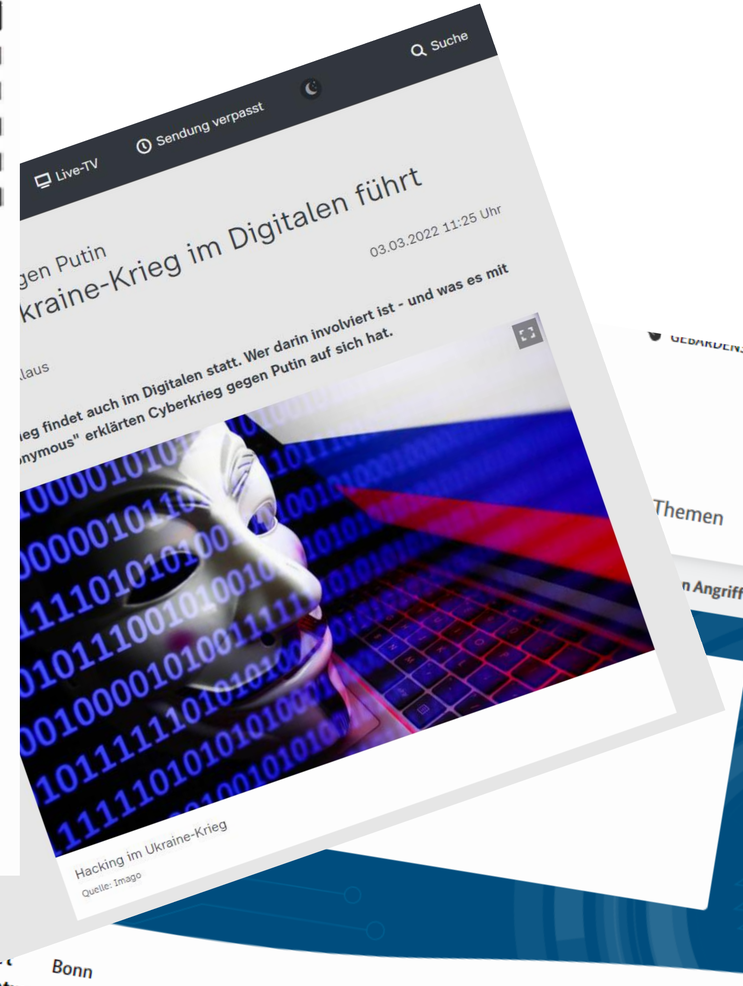
Elektronische Post

Empfänger laut Verteiler

Hinweise für die Betreiber Kritischer Infrastrukturen in Hessen

hier: Lagebild, Informationsaustausch und Meldewesen insbesondere vor dem Hintergrund des Russland-Ukraine-Konflikts

Anonymous gegen Putin: Wer den Krieg im Digitalen führt - ZDF
3 Mar 2022 — Der **Ukraine-Krieg** findet auch im Digitalen statt. ... Hacking im **Ukraine-Krieg** ... **Russlands** Zusammenarbeit mit **Cyber**-Kriminellen.



Bonn
Datum 04.03.2022

UPDATE vom 4. März 2022

perseus.

Die aktuelle Cybersicherheitslage

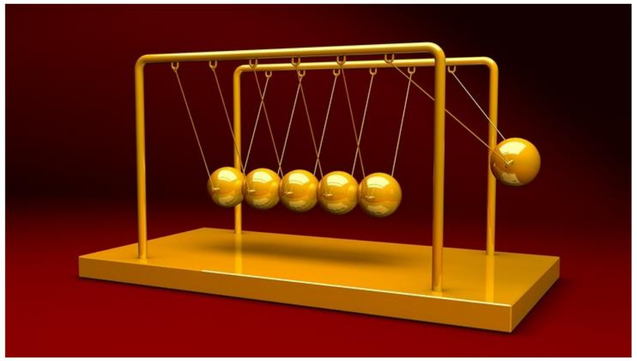
Die Auswirkung des aktuellen Russland/Ukraine-Konflikts

perseus. Preise Funktionen Angebote Unternehmen Wissen Par

Zurück zur Übersicht

Wenn die Einschläge näher kommen: der Einfluss des Konflikts in der Ukraine auf die Cybersicherheit von deutschen Unternehmen

17.03.2022



Pic source: QuinceCreative

perseus. Preise Funktionen Angebote Unternehmen Wissen Par

Aus aktuellem Anlass: Wie Sie sich jetzt am besten vor möglichen Cyberangriffen schützen

28.02.2022

Im Zusammenhang mit der aktuellen Situation in der Ukraine stehen deutsche Sicherheitsbehörden im ständigen Austausch mit Partnerorganisationen und warnen aktuell vor Cyberattacken bzw. rufen zu erhöhter Wachsamkeit auf. Auch wenn laut BSI keine akute Gefährdung der Informationssicherheit in Deutschland ersichtlich ist,

perseus. Preise Funktionen Angebote Unternehmen Wissen Pa

Wie der aktuelle Konflikt Unternehmen betreffen könnte: Eine Experteneinschätzung

09.03.2022

Bild von Tumisu auf Pixabay.com

Die aktuelle Cybersicherheitslage

Die Auswirkung des aktuellen Russland/Ukraine-Konflikts

Für eine allgemeine Einordnung ist wichtig zu wissen, dass der Krieg in der Ukraine sich von den Kriegen in der Vergangenheit in einem entscheidenden Punkt unterscheidet: **Erstmalig sind sowohl die unmittelbare Umgebung in der Ukraine als auch der gesamte Cyberspace Schauplatz von Gefechten.**

Bei Ausbruch des Krieges wurde angenommen, dass vor allem **Regierungen, Unternehmen und in Einzelfällen auch Privatpersonen, die sich der russischen Invasion in der Ukraine entgegenstellen und/oder die Ukraine unterstützen**, möglicherweise Opfer von böswilligen Aktivitäten russischer Cyberkrimineller oder verbündeter Hackergruppen werden könnten.

Die aktuelle Cybersicherheitslage

Die Auswirkung des aktuellen Russland/Ukraine-Konflikts

Beobachtet wurden in den vergangenen Wochen

- vermehrte Phishing-Attacken, die sich auf den aktuellen Konflikt beziehen,
- DDOS-Angriffe,
- Verbreitung ideologischer Botschaften auf gehackten Websites,
- und die Verbreitung von Falschinformationen über Social Media.

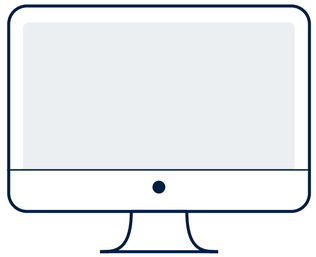
Gezielte Cyberangriffe auf deutsche Unternehmen, die einen Bezug zum Angriffskrieg Russlands auf die Ukraine haben, sind **bisher äußerst selten** vorgekommen oder nicht öffentlich bekannt. Allerdings kann jederzeit etwas passieren. Daher raten wir zu äußerster Vorsicht. **Jeder sollte gegenüber möglicher Gefahren aus dem Netz sensibilisiert sein.**

Mögliche Angriffsmuster

Wie werden IT -Systeme angegriffen? Welche Angriffsarten gibt es?

Phishing

Kriminelle versuchen mit Hilfe von **betrügerischen E-Mails, gefälschten Internetseiten** und anderen Methoden, an vertrauliche Unternehmensdaten wie **Zugangsdaten oder Zahlungsinformationen**, zu gelangen.

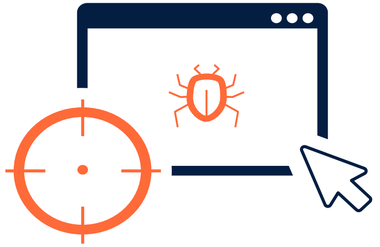


Malware

Schadprogramme werden in die Unternehmens-IT eingeschleust und beeinträchtigen den Betrieb negativ. So werden Daten und Systeme beispielsweise **verschlüsselt, ausspioniert oder beschädigt.**

Social Engineering

Mitarbeitende werden durch **Täuschung und Manipulation** ihrer Schwächen (Angst, Gewinnstreben, Neugier) dazu verleitet, **sensible Informationen preiszugeben oder schädlich zu handeln** (z. B. Malware herunterladen).



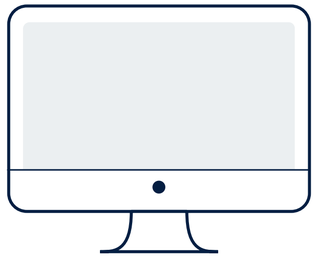
Kompromittierte Webanwendungen

Kriminelle nutzen die **Schwachstellen von Internetseiten** aus. Werden diese aufgerufen, haben sich die Täter die Anwendungen manipuliert. Dadurch können sie **Daten abschöpfen oder den Besucher heimlich weiterleiten.**

Mögliche Angriffsmuster

Wie werden IT -Systeme angegriffen? Welche Angriffsarten gibt es?

Phishing



Malware

Social Engineering

Kompromittierte Webanwendungen

67% der Cybervorfälle werden durch die eigenen, zumeist ungeschulten, Mitarbeitenden verursacht.

Quelle: Bitkom Research

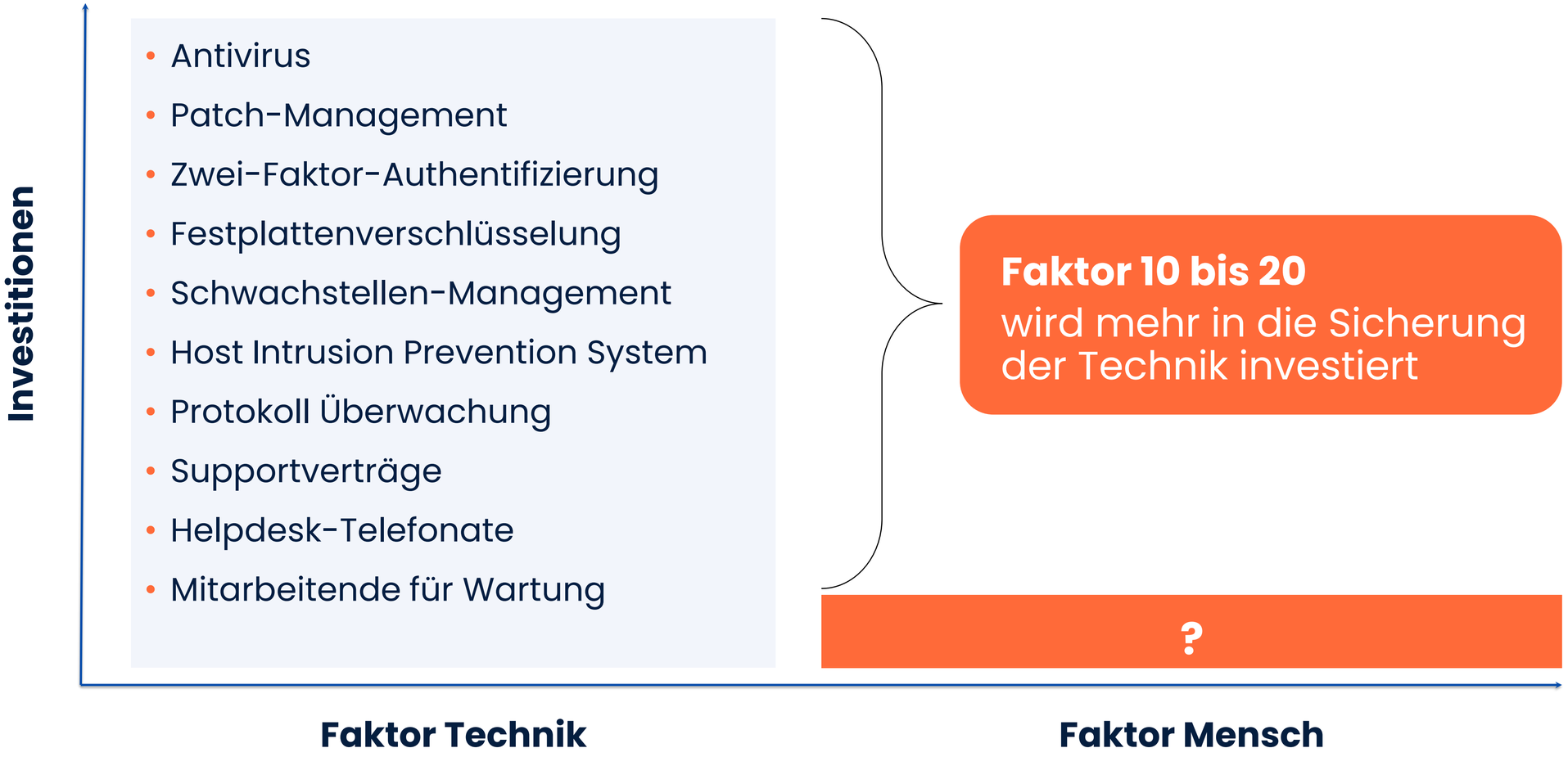
Schutz durch Prävention

Wie können meine Mitarbeitenden zu einem höheren Schutz beitragen?

Die 4 Dimensionen der Cybersicherheit

Schutz durch Prävention

Wie können meine Mitarbeitenden zu einem höheren Schutz beitragen?



Das Cyber-Risiko im Gesamtkontext

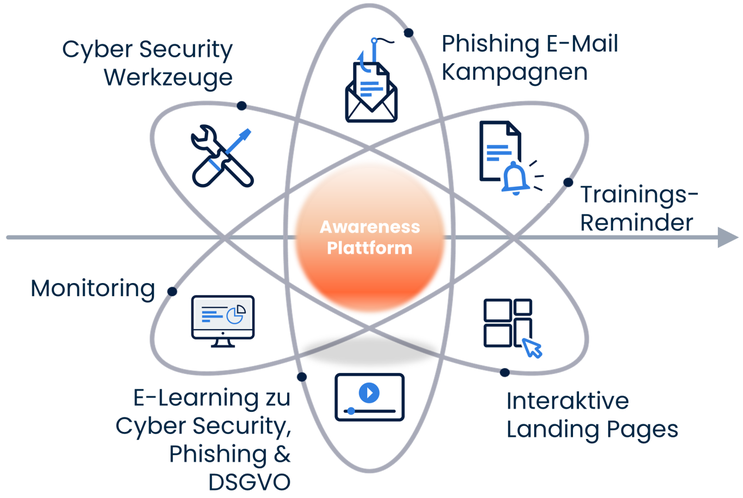
Das Cyber-Bewusstsein der Mitarbeiter ist keine einmalige Angelegenheit

Cybervorfälle durch technische Schwachstellen

Cybervorfälle durch menschliches Versagen

Perseus' Awareness Platfrom bietet permanente Sensibilisierung

Unsere Nutzer beginnen gewöhnlich mit **geringem Bewusstsein** über Cybersicherheit



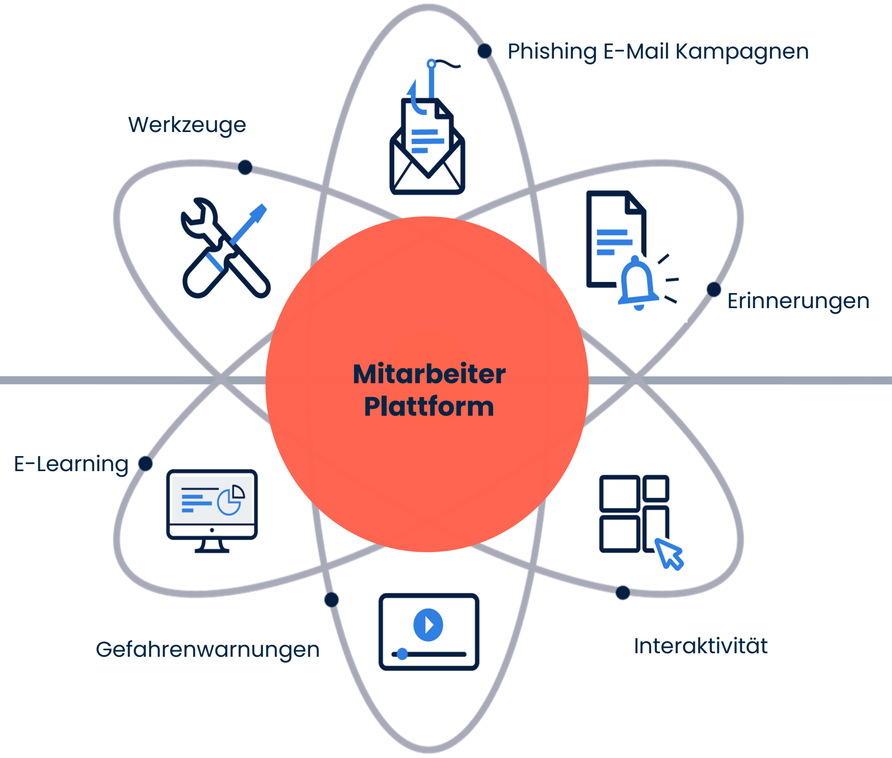
Unser selbst-entwickelter **Feedback-Loop** bewirkt eine **permanente Verhaltens-änderung**

Eigene Darstellung

Schutz durch Prävention

Wie können meine Mitarbeitenden zu einem höheren Schutz beitragen?

Mitarbeitende starten idR mit einem **geringen Bewusstsein** für Cyberrisiken.



Durch einen permanenten Feedback Loop wird eine **dauerhafte Verhaltens-änderung** erreicht.

Schutz durch Prävention

Wie können meine Mitarbeitenden zu einem höheren Schutz beitragen?

Checkliste der wichtigsten Grundschutzmaßnahmen:

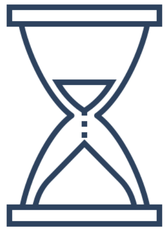
- Aufmerksamer Umgang mit E-Mails
- Unternehmensweite Phishing-Sensibilisierung
- Aufmerksamer Umgang mit Office-Dokumenten
- Sichere, einzigartige Passwörter
- 2- bzw. Multi-Faktor-Authentifizierung
- Backups
- Notfallplan
- Mobile Geräte sichern
- Vorsicht bei der WLAN-Nutzung

Handlungsempfehlungen für den Cybernotfall

Wie ist im Falle eines Angriffs zu handeln?

Umgehend reagieren

Mehr Schaden entsteht,
je länger nicht gehandelt wird.

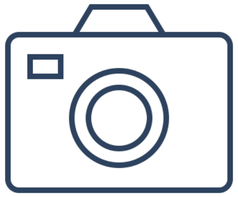


Ruhe bewahren

Besonnenes und informiertes Handeln kontern Panikmache der Angreifer.

Dokumentieren

Sammeln Sie Informationen zur Weitergabe an Ihre Vorgesetzten/IT-Abteilung.



Absicherung für den Cybernotfall

Absicherung für den Cybernotfall

Vielen Dank.
Ich freue mich auf Ihre Fragen!

Johannes Vakalis
Head of Sales and marketing

johannes.vakalis@perseus.de

perseus.

Perseus Technologies GmbH

CEO: Kevin Püster

Hardenbergstraße 32, 10623 Berlin

HRB 180356 B, Amtsgericht Charlottenburg

Für Sie vor Ort - in Berlin und Brandenburg.

Wir sind für Sie da in unseren
BeratungsCentern für Firmenkunden:
6 x in Berlin und 3 x in Brandenburg

Firmenkunden-Service der Berliner Volksbank:
(Montag – Freitag, 8 – 18 Uhr)
Telefon: 030 3063-3355
firmenkunden@berliner-volksbank.de

berliner-volksbank.de

Berliner Volksbank

Herzlichen Dank für Ihre Aufmerksamkeit …

… beim Online-Seminar:
„Cyberattacken rechtzeitig erkennen und sicher abwehren“

31. Mai 2022

perseus.
Cybersicherheit auf den Punkt

Berliner Volksbank