



So machen Sie Ihre Mitarbeiter zur Human
Firewall

Security Awareness

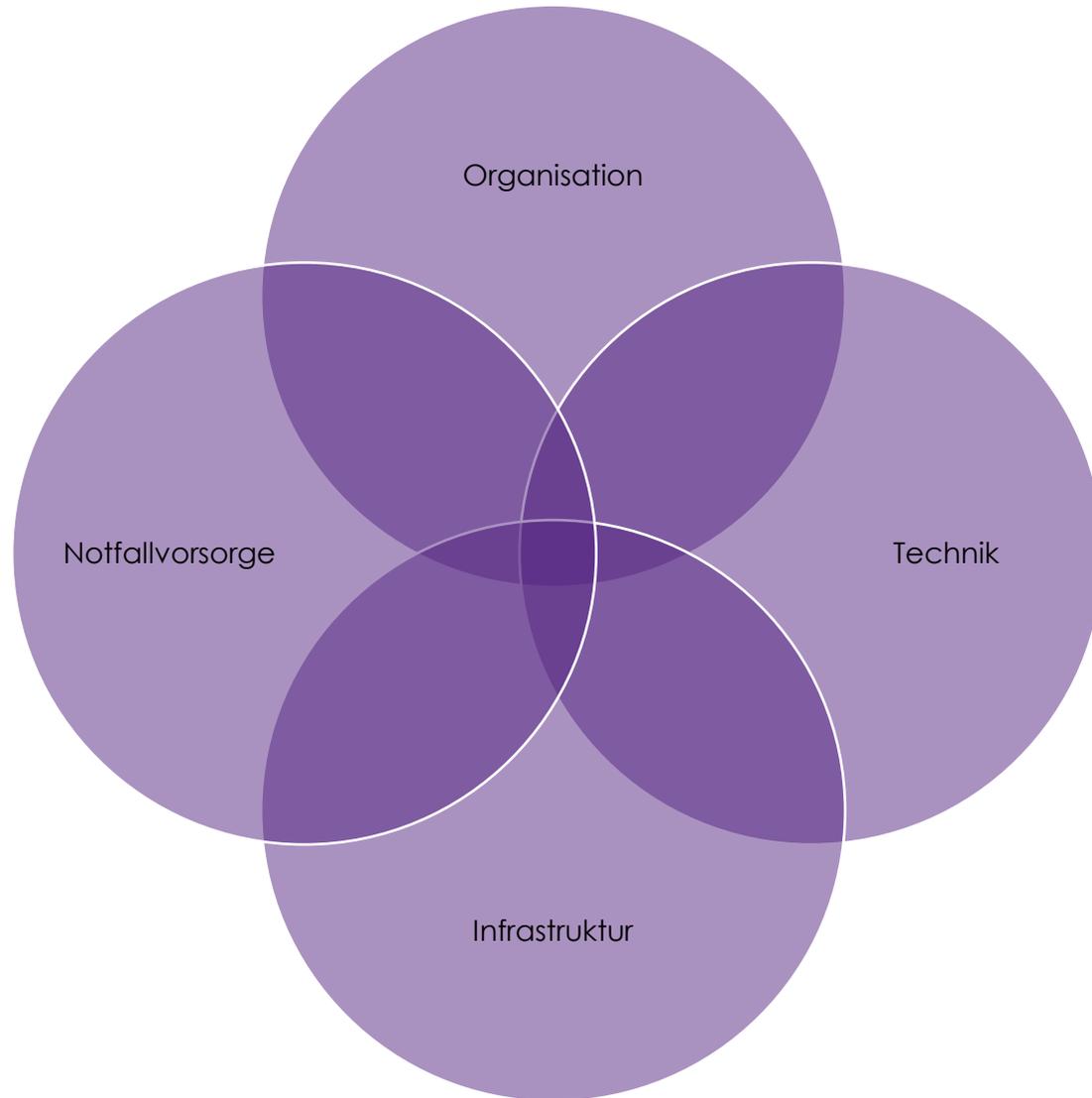
Agenda

- Themenkomplex
- Bindeglied
- Zahlen, Daten, Fakten
- Ansatz
- Gesamtbild

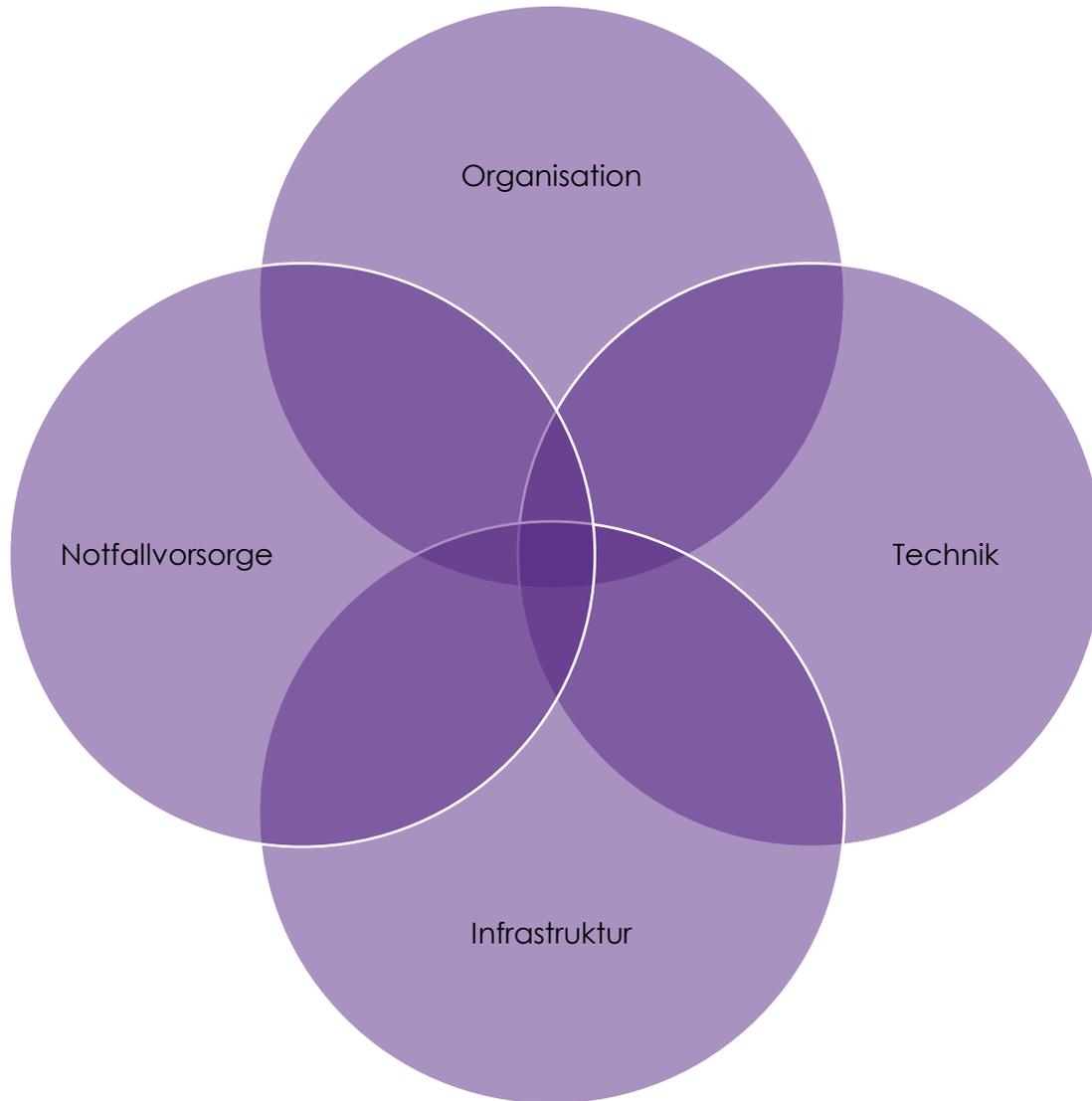
Themenkomplex



Themenkomplex – Einfache Darstellung



Themenkomplex - Schnittstelle



= Mensch

Schnittstelle - Mensch

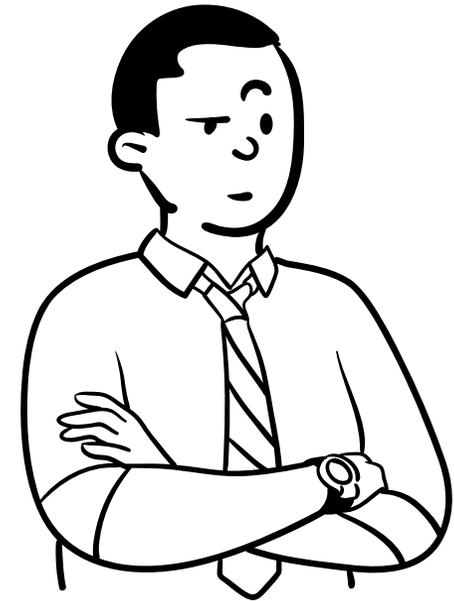
Kunden bauen mehrschichtige Sicherheitssysteme auf ...



Am Anfang steht dabei der Mensch.

Schnittstelle - Mensch

Eine Befragung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) hat ergeben, dass **der Mensch ein Schlüsselfaktor bei der Cybersicherheit** ist. Denn E-Mails oder manipulierte Webseiten stellen nach wie vor die **mit Abstand häufigsten Infektionswege** mit Schadsoftware dar.

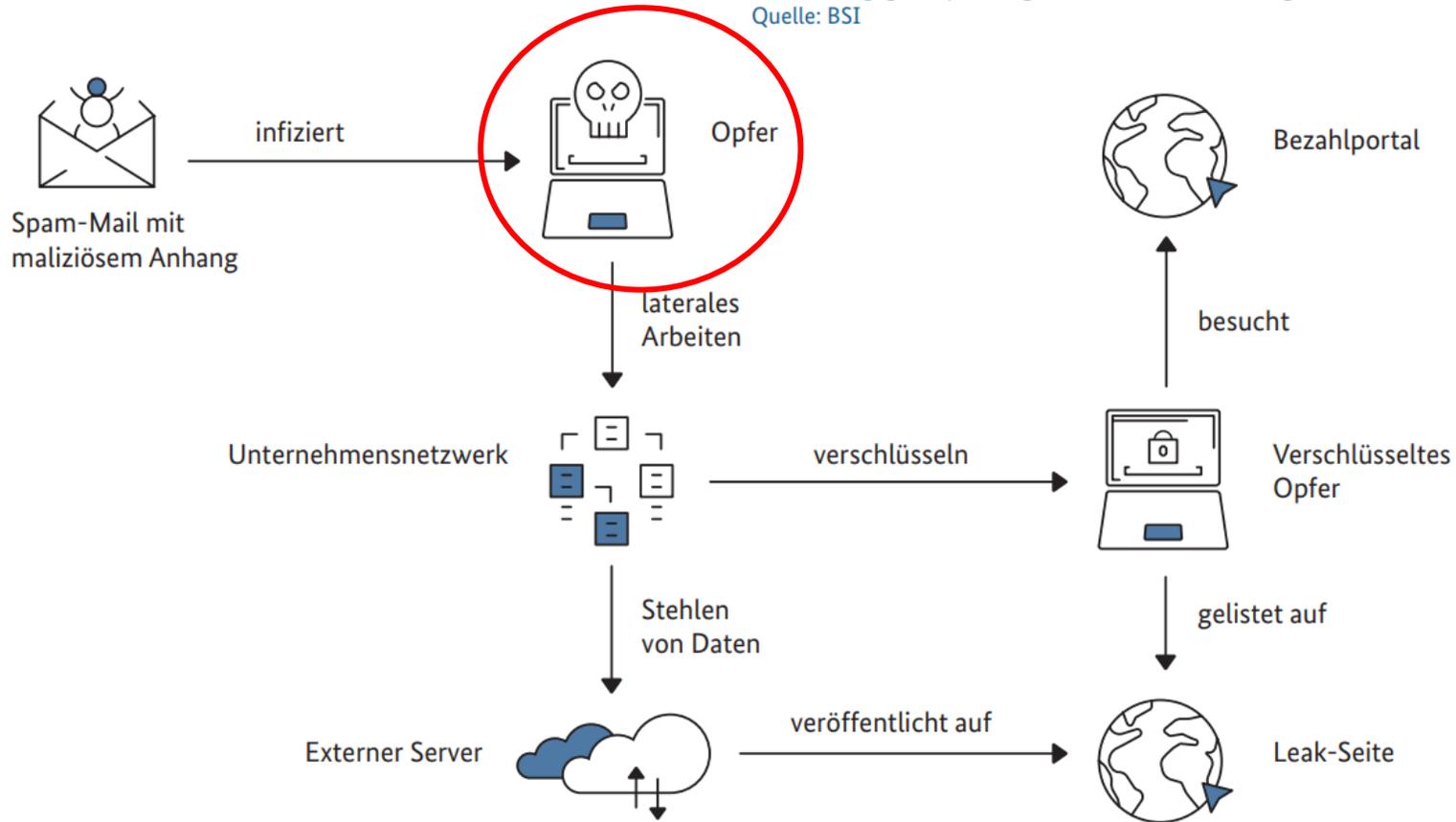


Quelle: <https://www.bdew.de/energie/digitalisierung/cybersicherheit-welche-rolle-spielt-der-faktor-mensch/#:~:text=Eine%20Befragung%20des%20Bundesamtes%20f%C3%BCr,h%C3%A4ufigsten%20Infektionswege%20mit%20Schadsoftware%20dar.>

Schnittstelle - Mensch

Beispielhafter Angriffsablauf

Abbildung 3:
Beispielhafter Ablauf eines Ransomware-Angriffs mit Lösegeld-
und Schweigegelderpressung (schematische Darstellung)
Quelle: BSI

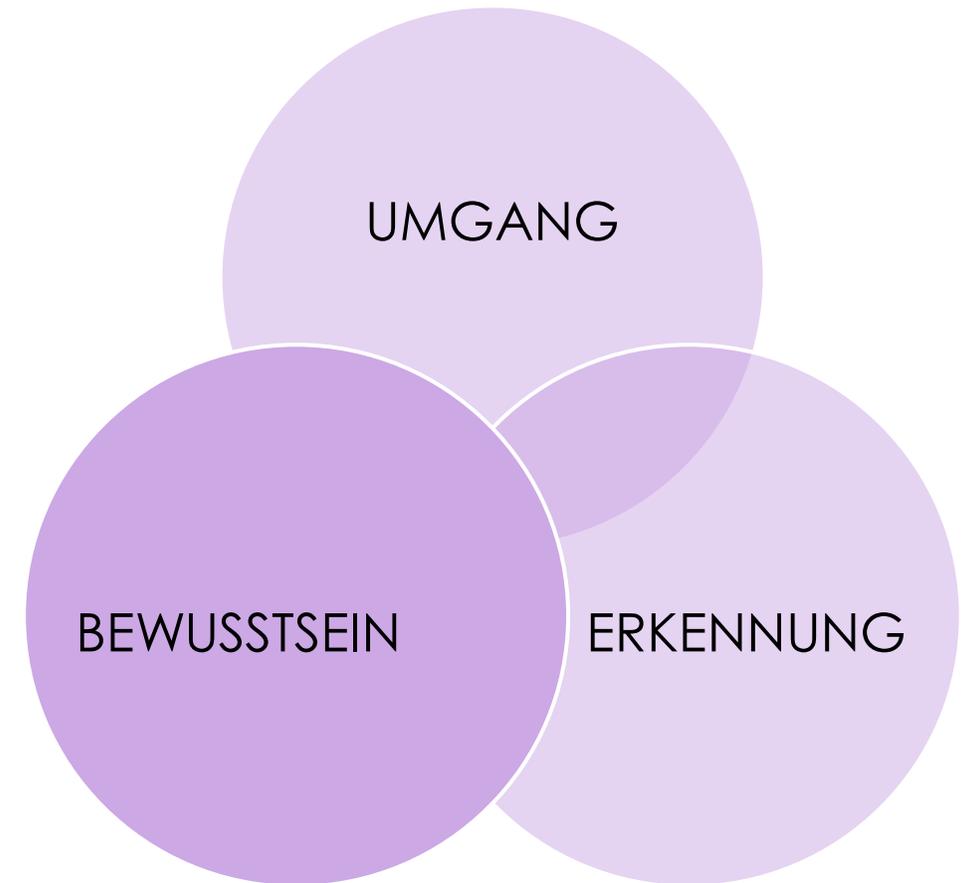


Schnittstelle - Mensch

BEWUSSTSEIN

- Warum ist Informationssicherheit wichtig
- Einhaltung von Gesetzen
- Einhaltung von Vorschriften
- Einhaltung von Richtlinien
- Nachfragen ist keine Schande!

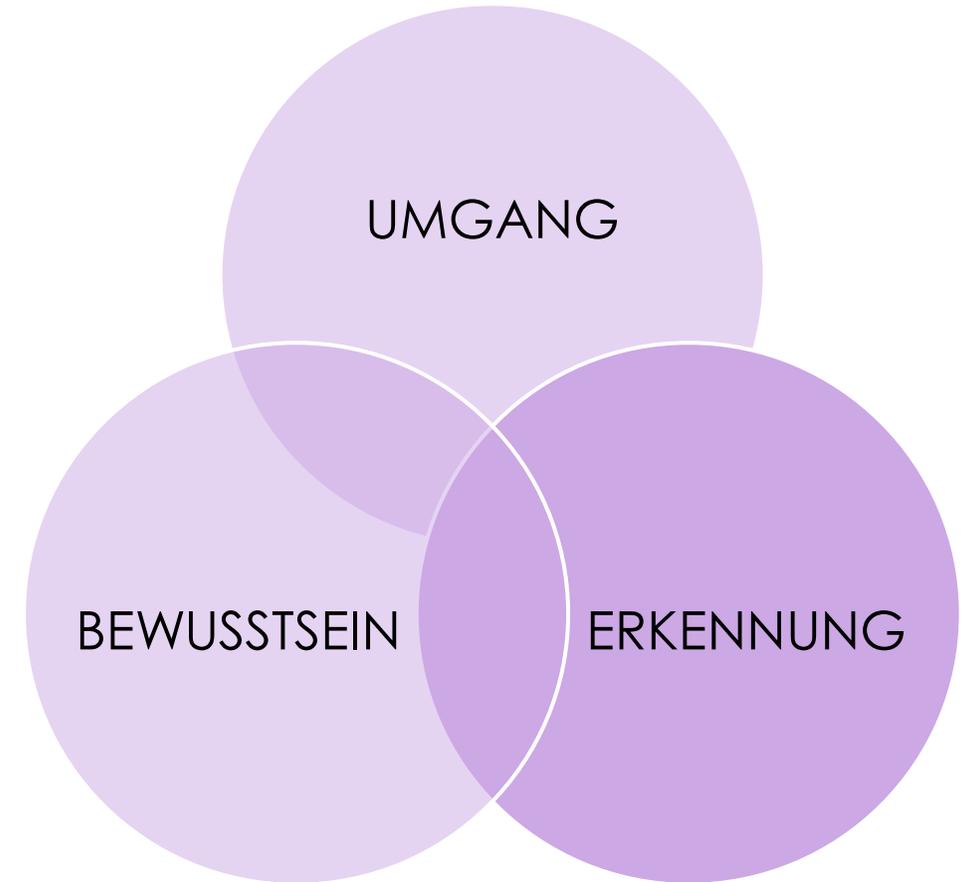
**Ohne das nötige Bewusstsein verpuffen
Schulungen und Sensibilisierungsmaßnahmen
ohne nennenswerten Effekt**



Schnittstelle - Mensch

ERKENNUNG

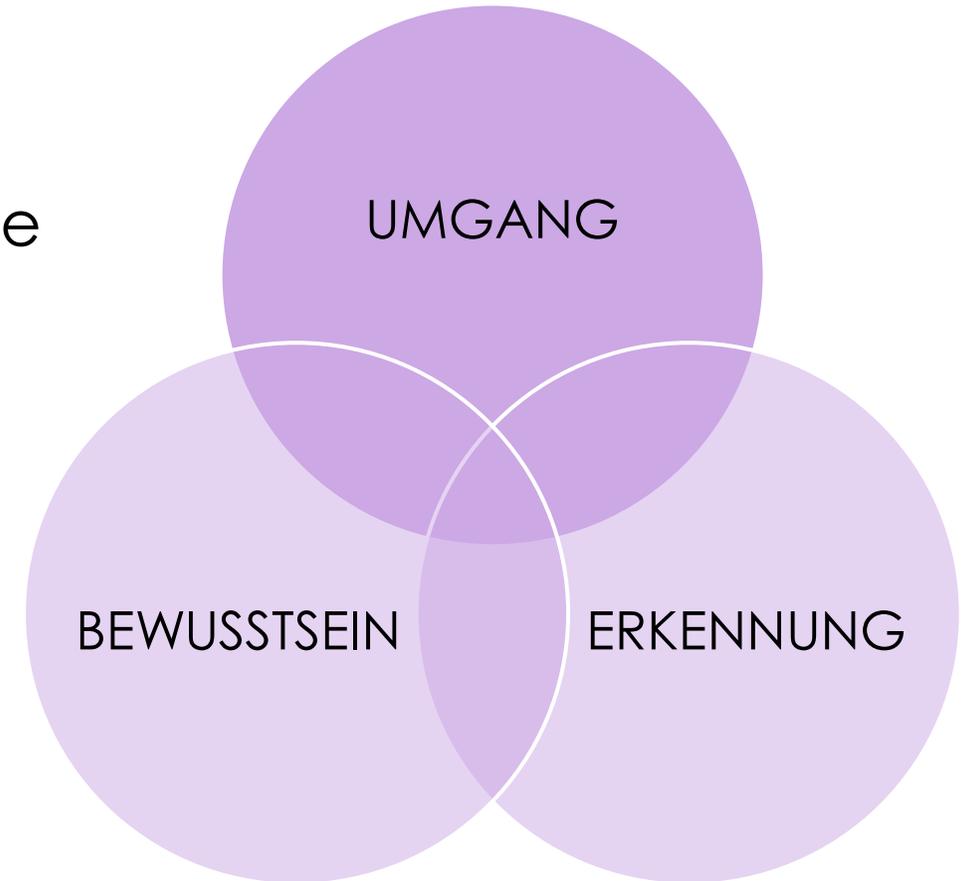
- Wie erkenne ich Sicherheitsvorfälle
- Wie erkenne ich Datenpannen
- Wie erkenne ich Phishing E-Mails
- Wie erkenne ich Telefon Phishing
- Wie erkenne Social Engineering



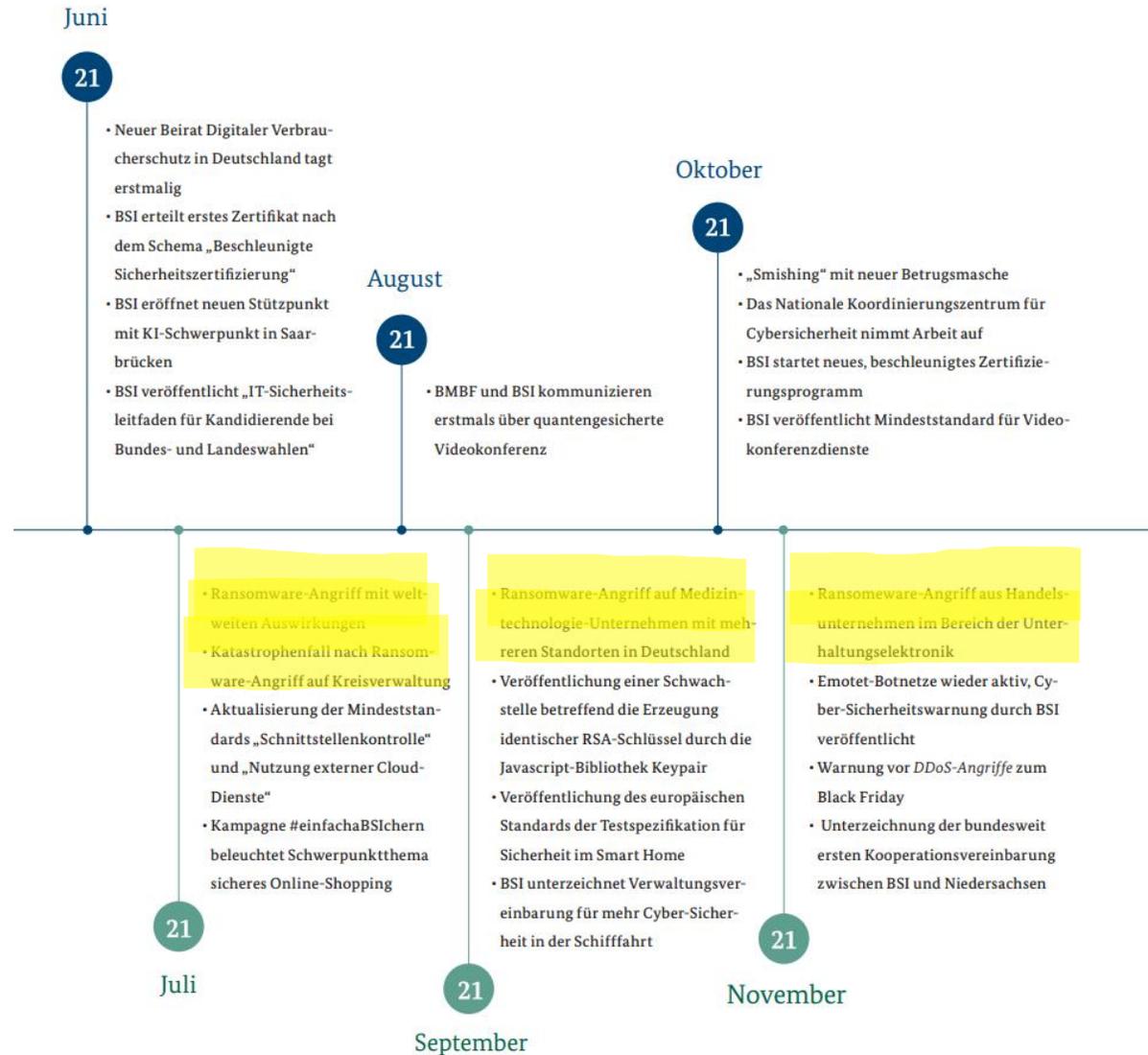
Schnittstelle - Mensch

UMGANG

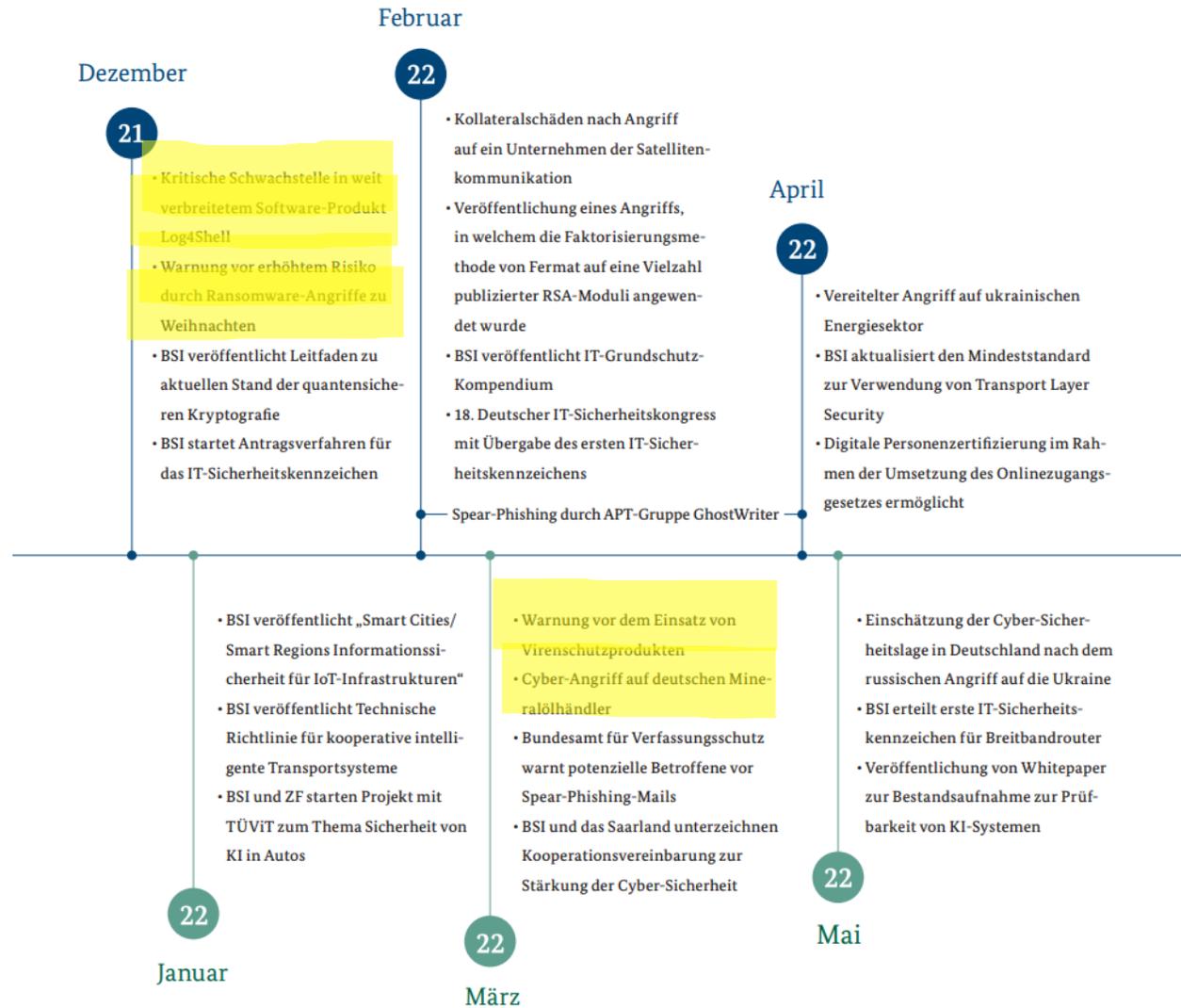
- Wie reagiere ich bei Sicherheitsvorfällen
- Wie reagiere ich bei Datenpannen
- Wohin melde ich vermutete Sicherheitsvorfälle
- Was sollte ich wann wie tun
- Wer sind meine Ansprechpartner



Zahlen, Daten, Fakten - BSI Lagebericht 2022



Zahlen, Daten, Fakten - BSI Lagebericht 2022



Zahlen, Daten, Fakten - BSI Lagebericht 2022

15 Millionen Meldungen zu Schadprogramm-Infektionen in Deutschland übermittelte das BSI im Berichtszeitraum an deutsche Netzbetreiber.



34.000 Mails mit Schadprogrammen wurden monatlich durchschnittlich in deutschen Regierungsnetzen abgefangen.



78.000 neue Webseiten wurden wegen enthaltener Schadprogramme für den Zugriff aus den Regierungsnetzen gesperrt.

69%

aller Spam-Mails im Berichtszeitraum waren Cyber-Angriffe wie z. B. Phishing-Mails und Mail-Erpressung.

90%

des Mail-Betrugs im Berichtszeitraum war Finance Phishing, d. h. die Mails erweckten betrügerisch den Eindruck, von Banken oder Sparkassen geschickt worden zu sein.

BSI ist weltweit der führende Dienstleister im Bereich Common-Criteria-Zertifikate.



5.100
2021

4.400
2020



Zehn Jahre Allianz für Cyber-Sicherheit: 2022 sind wir bereits

6.220

Teilnehmer.

Deutschland Digital•Sicher•BSI•

Die Lage der IT-Sicherheit in Deutschland 2022 im Überblick

Top 3-Bedrohungen je Zielgruppe:

Gesellschaft



Identitätsdiebstahl
Sextortion
Fake-Shops im Internet

Wirtschaft



Ransomware
Schwachstellen, offene oder falsch konfigurierte Online-Server
IT-Supply-Chain: Abhängigkeiten und Sicherheit

Staat und Verwaltung



Ransomware
APT
Schwachstellen, offene oder falsch konfigurierte Online-Server

Erster digitaler Katastrophenfall in Deutschland



207 Tage Katastrophenfall

Nach Ransomware-Angriff konnten Elterngeld, Arbeitslosen- und Sozialgeld, Kfz-Zulassungen und andere bürgernahe Dienstleistungen nicht erbracht werden.

Die Anzahl der Schadprogramme steigt stetig. Die Anzahl neuer Schadprogramm-Varianten hat im aktuellen Berichtszeitraum um rund

116,6 Millionen zugenommen.



Hackivismus im Kontext des russischen Krieges:

Mineralöl-Unternehmen in Deutschland muss kritische Dienstleistung einschränken



Kollateralschaden nach Angriff auf Satellitenkommunikation



20.174

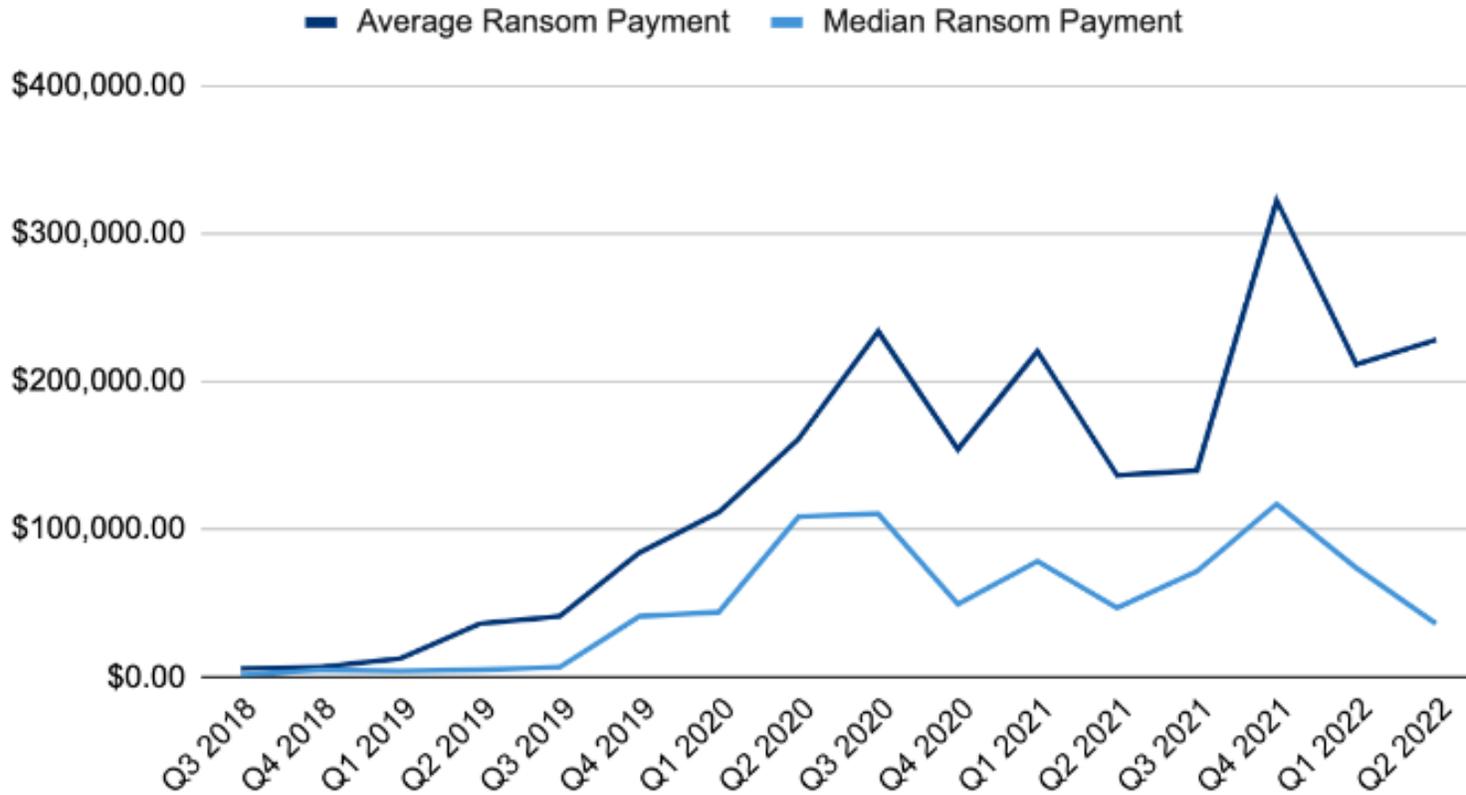
Schwachstellen in Software-Produkten (13 % davon kritisch) wurden im Jahr 2021 bekannt. Das entspricht einem **Zuwachs von 10 %** gegenüber dem Vorjahr.



Zahlen, Daten, Fakten - BSI Lagebericht 2022

Kurve: Lösegeldzahlungen pro Quartal

Ransom Payments By Quarter

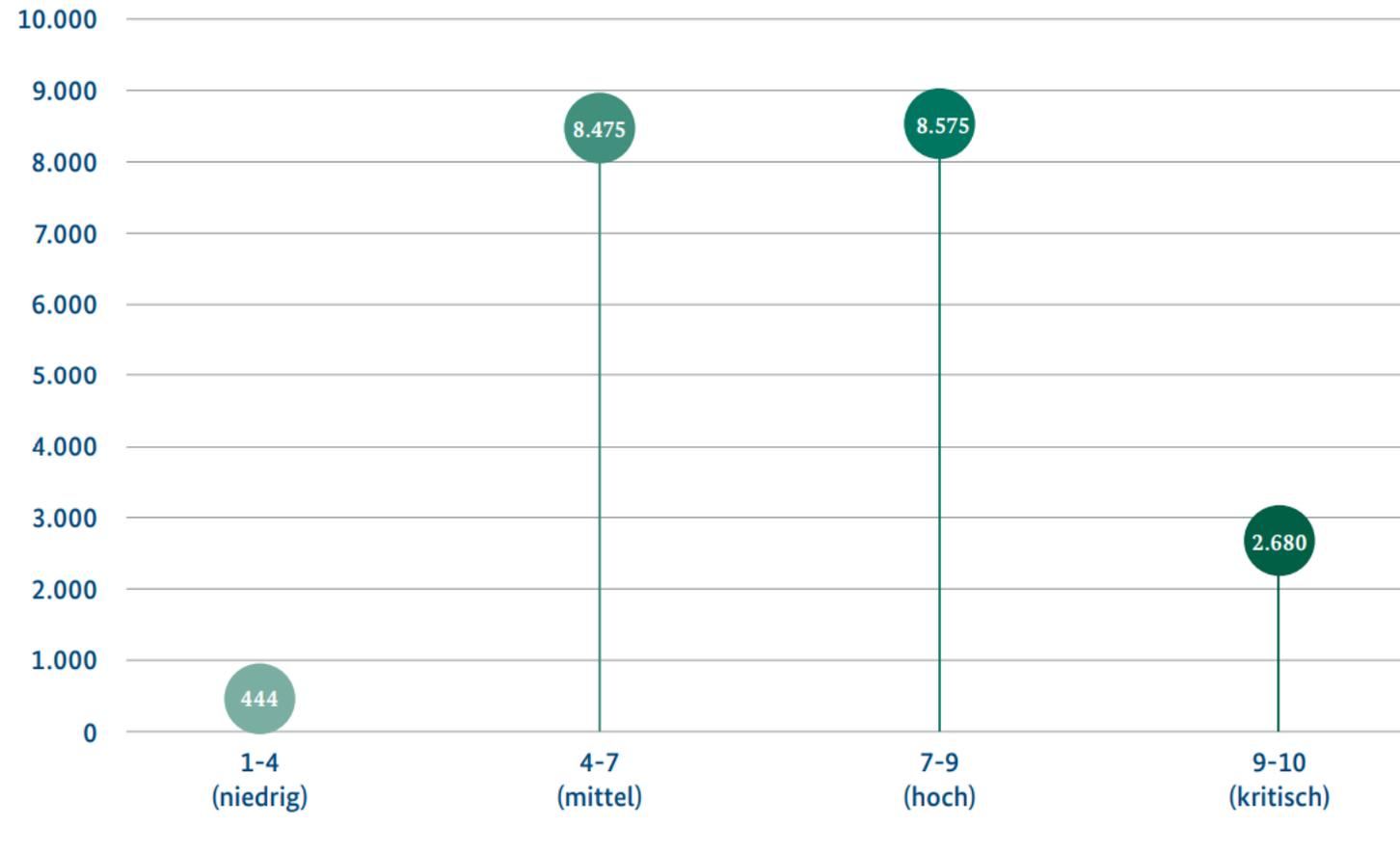


Zahlen, Daten, Fakten - BSI Lagebericht 2022

Bekannt gewordene Schwachstellen 2021 nach dem CVSS-Score¹ für Kritikalität Anzahl

Abbildung 15:
Bekannt gewordene Schwachstellen 2021
nach dem CVSS-Score für Kritikalität
Quelle: Schwachstellen-Statistik

¹ Risikobewertung nach CVSS-Version 3.1



Zahlen, Daten, Fakten - BSI Lagebericht 2022

Coordinated-Vulnerability-Disclosure-Fälle von 2017 bis 2021

Anzahl

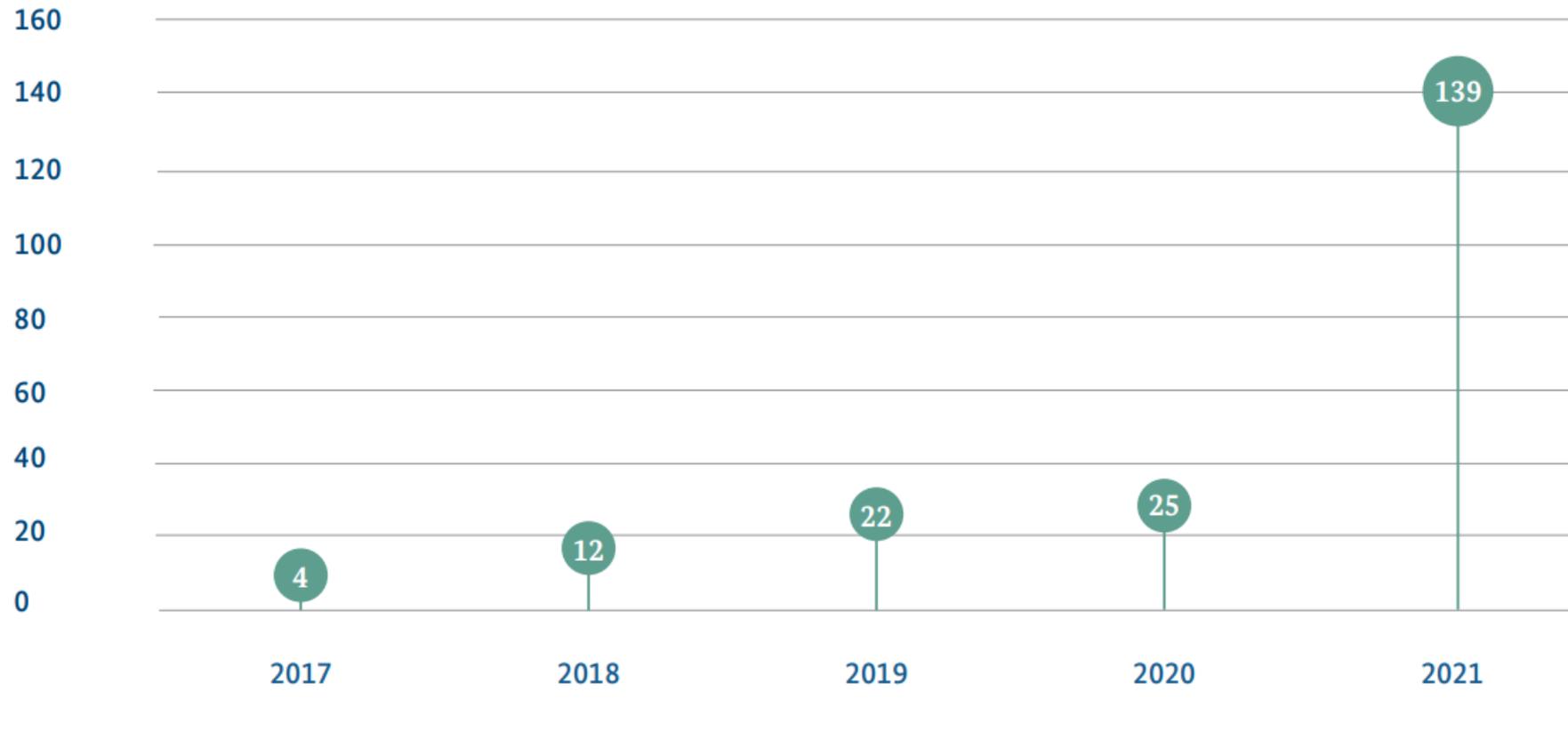


Abbildung 14: Coordinated-Vulnerability-Disclosure-Fälle von 2017-2021
Quelle: BSI

Zahlen, Daten, Fakten - BSI Lagebericht 2022

Sami Laiho, Microsoft MVP und Ethical Hacker, sagt dazu: „Das Entfernen von Administratorrechten bietet einen großen und proaktiven Schutz. Wir müssen die Einzelkomponenten schützen und so die Ausführung böswilliger Nutzlasten verhindern, insbesondere bei wichtigen Applikationen, die Internetzugriffe oder den Abruf von E-Mails erlauben. Die Daten im aktuellen Report belegen, dass das Entfernen von Administratorrechten einen wirksamen Schutz für Outlook, Office, IE und Edge bietet.“

Die Zahlen aus dem Jahr 2020 sagen indes mehr als Worte:

- **90 Prozent** der als kritisch eingestuften Browser-Sicherheitslücken im Internet Explorer hätten durch die Aufhebung von Administratorrechten entschärft werden können.
- **85 Prozent** der als kritisch eingestuften Sicherheitslücken im Microsoft-Browser Edge ließen sich durch den Entzug von Administratorrechten beheben.
- **100 Prozent** der kritischen Schwachstellen in Microsoft Outlook könnten durch die Aufhebung von Administratorrechten geschlossen werden.

Ansatz – Security Awareness Training

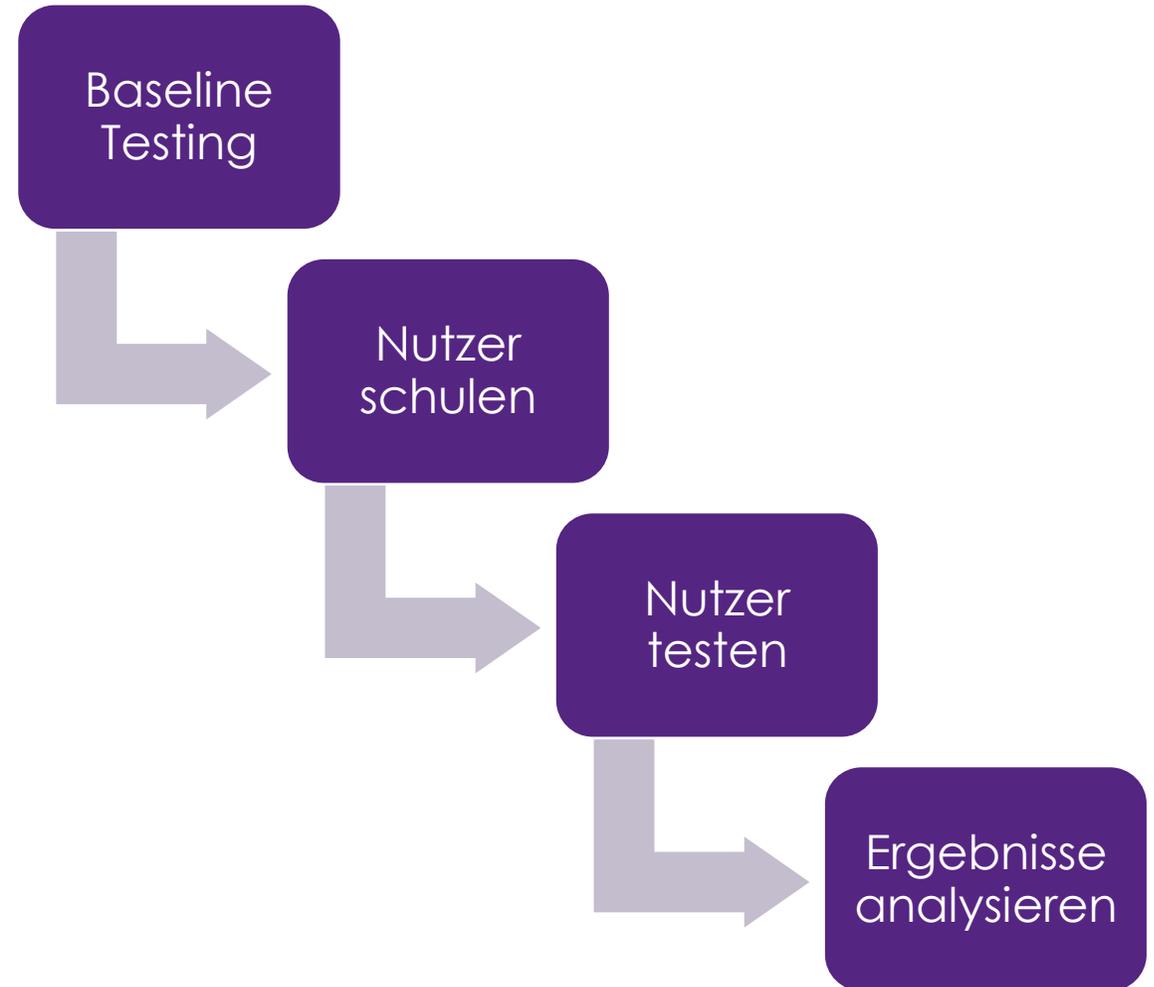
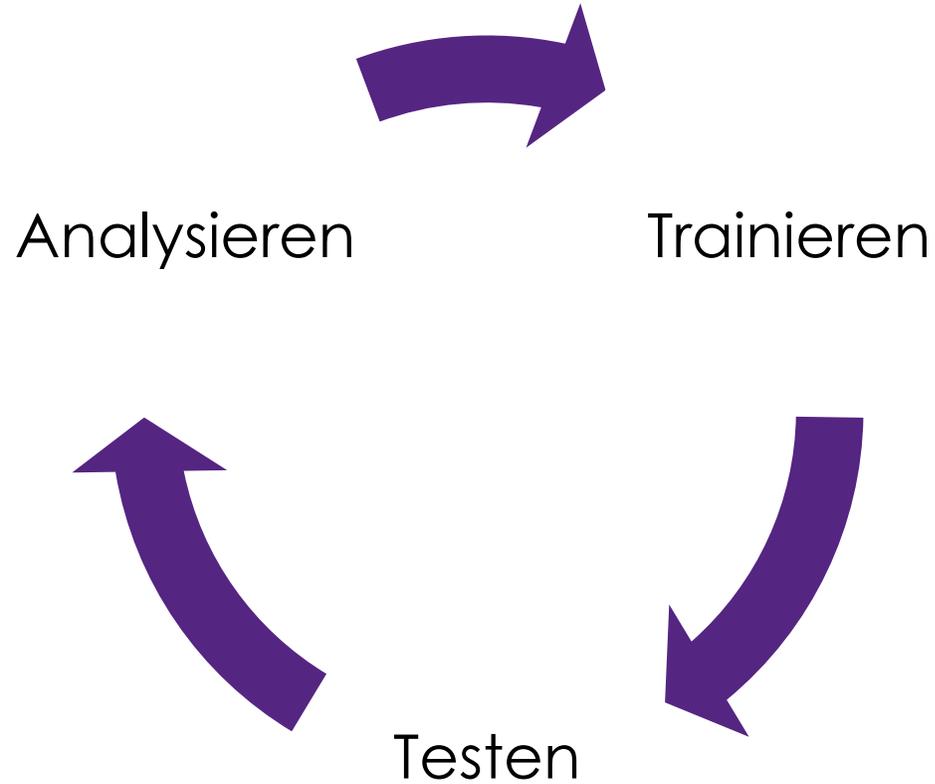
- Unterweisung der Mitarbeitern
- Regelmäßiges schulen der Mitarbeiter
- Regelmäßiges sensibilisieren der Mitarbeiter

Ja, verstanden

aber wie??

Ansatz – Security Awareness Training

In Kooperation mit **KnowBe4**
Human error. Conquered.



Ansatz – Security Awareness Training

ASAP Methode mit  KnowBe4
Human error. Conquered.

- **A**utomated **S**ecurity **A**wareness **P**rogram
 - Beantworten Sie 15 bis 25 Fragen
 - Erhalten Sie individuelle Vorschläge für das konkrete weitere Vorgehen
 - Verschaffen Sie sich einen umfassenden Überblick über die Inhalte Ihres Programms
 - Bleiben Sie stets über den Fortschritt Ihres Programms auf dem Laufenden

Ansatz – Security Awareness Training

SAPA Methode mit KnowBe4
Human error. Conquered.

- **S**ecurity **A**wareness **P**roficiency **A**ssessment
 - Kompetenzbasiertes Assessment
 - Zeigt Wissenslücken einzelner Benutzer auf
 - Empfehlung für Verbesserungspotenzial

Ansatz – Security Awareness Training

SCS Methode mit  KnowBe4
Human error. Conquered.

- **Security Culture Survey** (Umfrage zur Sicherheitskultur)
 - Erhalten Sie Daten zu der Einstellung Ihrer Mitarbeiter
 - Berücksichtigung psychologischer und sozialer Aspekte
 - Messung der Effektivität und der Verbesserung Ihrer Sicherheitskultur

Ansatz – Security Awareness Training

EEC Methode mit  KnowBe4
Human error. Conquered.

- **Email Exposure Check**
- Identifiziert die gefährdeten Benutzer in Ihrem Unternehmen, indem es Informationen aus sozialen Medien und Tausende von Datenbanken mit Sicherheitsverletzungen durchsucht.
 - Durchsucht das Internet nach öffentlich zugänglichen Organisationsdaten.
 - Findet alle Benutzer, deren Kontoinformationen bei einer der mehreren tausend Sicherheitsverletzungen preisgegeben wurden.

Ansatz – Security Awareness Training

Micro Learning mit  KnowBe4
Human error. Conquered.

- Schulungsinhalte werden in kleine „Häppchen“ verpackt
 - Für Mobilgeräte optimierte Module „Mobile Learning“
 - Gamification „Spielend lernen“
 - Videos „AwarenessTube“
 - Poster - Digital oder ausgedruckt bereitstellen
- Thematisch unterteilt (Lernpfad über das ganze Jahr verteilt)
- Trainingsempfehlungen die anhand von Performance-Metriken Ihrer Nutzer aus Phishing Security Test-Kampagnen abgeleitet werden

Ansatz – Security Awareness Training

PhishER mit KnowBe4
Human error. Conquered.

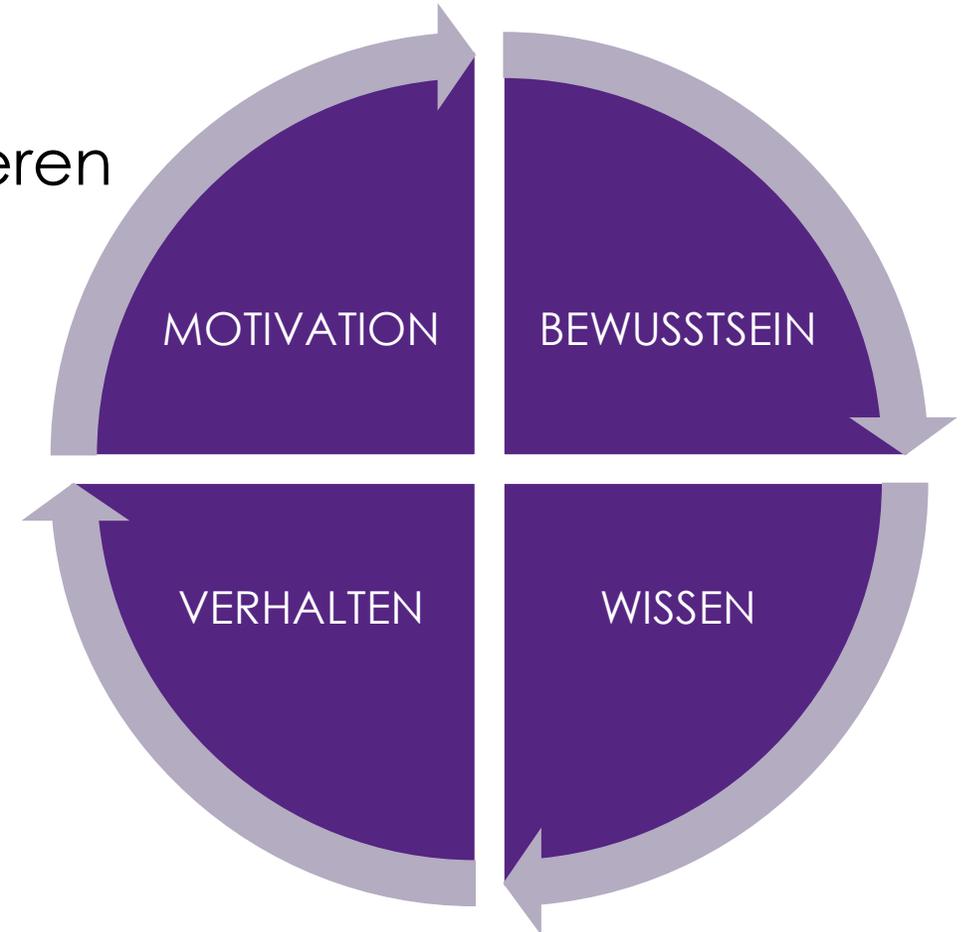
- Anzeige von Nachrichtenclustern oder -gruppen mit ähnlichem Muster
- PhishML: Sämtliche Nachrichten werden analysiert. Liefert Informationen, die den Priorisierungsprozess einfacher, schneller und genauer gestalten.
- PhishRIP: Quarantänefunktion. Hilft Ihnen dabei, E-Mail-Bedrohungen zu isolieren und sich vor aktuellen Phishing-Angriffen zu schützen.
- PhishFlip: Gemeldete tatsächliche Phishing-Angriffe werden im Rahmen sicherer Kampagnen mit simulierten Phishing-Angriffen eingesetzt.

Gesamtbild

Security Awareness ist mehr als ein notwendiges Übel

- Mitarbeiter sind die Stützpfeiler Ihrer Organisationen
- Bilden die erste Verteidigungslinie
- So sollten wir sie auch behandeln/sensibilisieren

- #Kronjuwelen



Vielen Dank



vaps group

