DSSV Verband für die Fitness-Wirtschaft

Cyberkriminalität im Unternehmen

Gero Kretschmer | 07.12.2022

Was haben wir heute vor?

1 Aktuelle Cyberrisikolage

2 Ein Blick hinter die Kulissen

3 Rechte, Pflichten und Haftung im Alltag

4 Präventiver Schutz für Ihr Unternehmen

Aktuelle Cyberrisikolage

SPIEGEL ONLINE

NETZWELT

Sabotage durch Hacker

BSI registriert deutlichen Anstieg bei Cyber-Angriffen auf Infrastruktur

Wasser- und Stromnetze sind zuletzt deutlich häufiger Ziel von Hackerangriffen geworden. Das zeigen einem Medienbericht zufolge bisher unveröffentlichte Zahlen des Bundesamts für Sicherheit in der Informationstechnik.

Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bonn

DIENSTAG, 30. APRIL 2019

Daten von Großkunden gestohlen

Hacker erpressen deutsche Online-Firma

Deutscher Mittelstand im Visier

Cyber-Angriffe verursachen 43 Milliarden Euro Schaden

ntv

WIRTSCHAFT

Spur führt nach China

Hacker nehmen Dax-Konzerne ins Visier

Hacker knacken weltweit Mobilfunkanbieter

Alu-Konzern im Handbetrieb

Hacker greifen Norsk Hydro an

50 Millionen Profile betroffen

Facebook meldet Hackerattacke

ntv

DER BÖRSEN-TAG

DONNERSTAG, 04. APRIL 2019

Der Börsen-Tag

Bayer erstattet Anzeige wegen Cyberkriminalität - Spur nach China

Der Chemie-Riese Bayer ist Opfer eines Cyber-Angriffs geworden. Wie der Konzern der dpa bestätigte, habe es bereits seit Anfang 2018 Anzeichen dafür gegeben, dass das Firmennetzwerk mit Schadsoftware der Winnti genannten Hackergruppe angegriffen wurde.

Quellen: Spiegel online, NTV

AKTUELLES

Warnungen des BSI: Wie der Konflikt in der Ukraine deutsche Unternehmen gefährdet

1 März 2022

Der russische Angriff auf die Ukraine schickt nicht nur schreckliche Bilder, Angst und Furcht um die Welt, er birgt auch ganz konkrete Gefahren für Netzwerke und Systeme in Europa und Deutschland. Das BSI warnt bereits vor einer erhöhten Gefahr von Cyberangriffen.

Einschätzung der aktuellen Cyber-Sicherheitslage in Deutschland nach dem russischen Angriff auf die Ukraine

Ort Bonn
Datum 04.03.2022

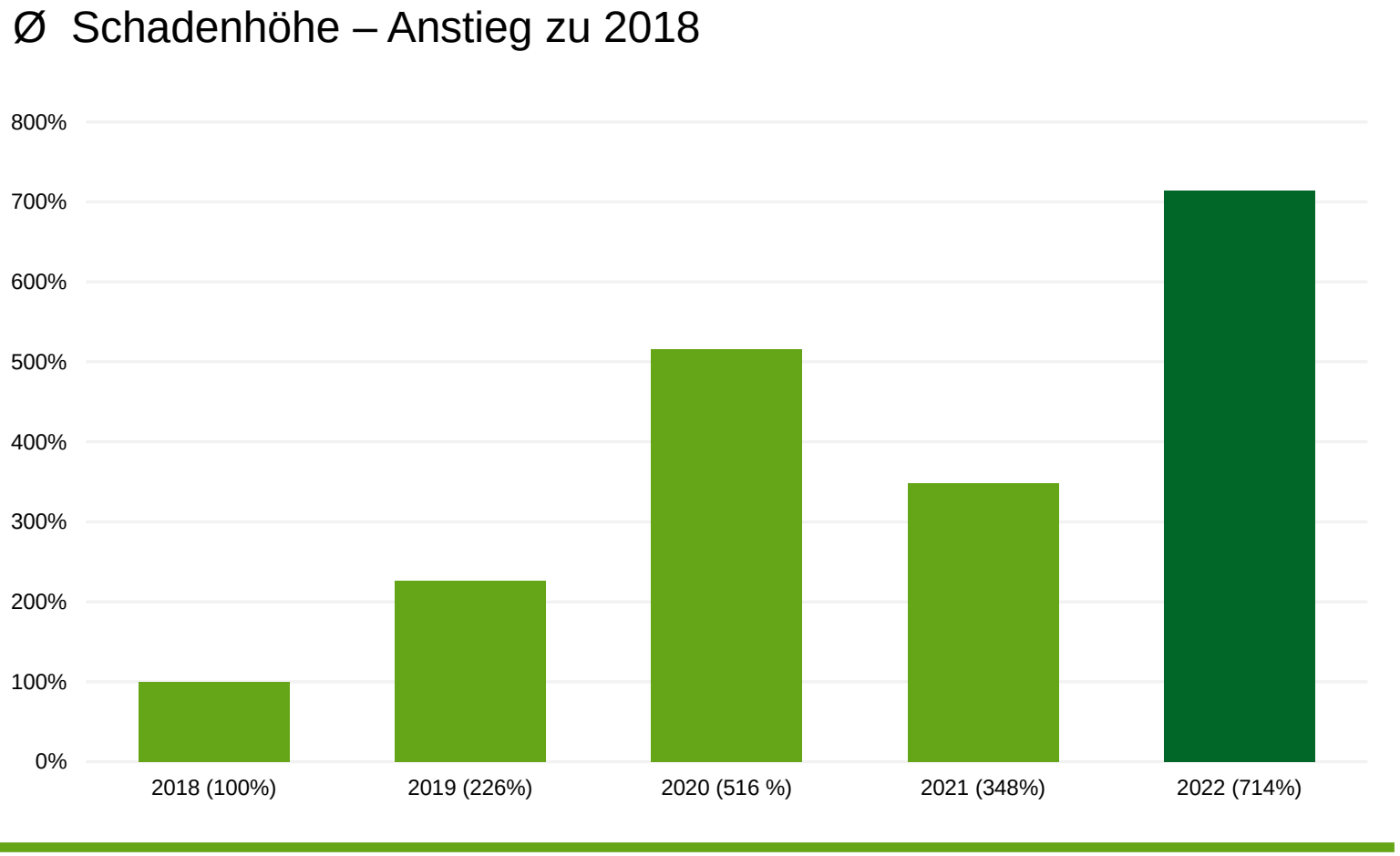
UPDATE vom 4. März 2022

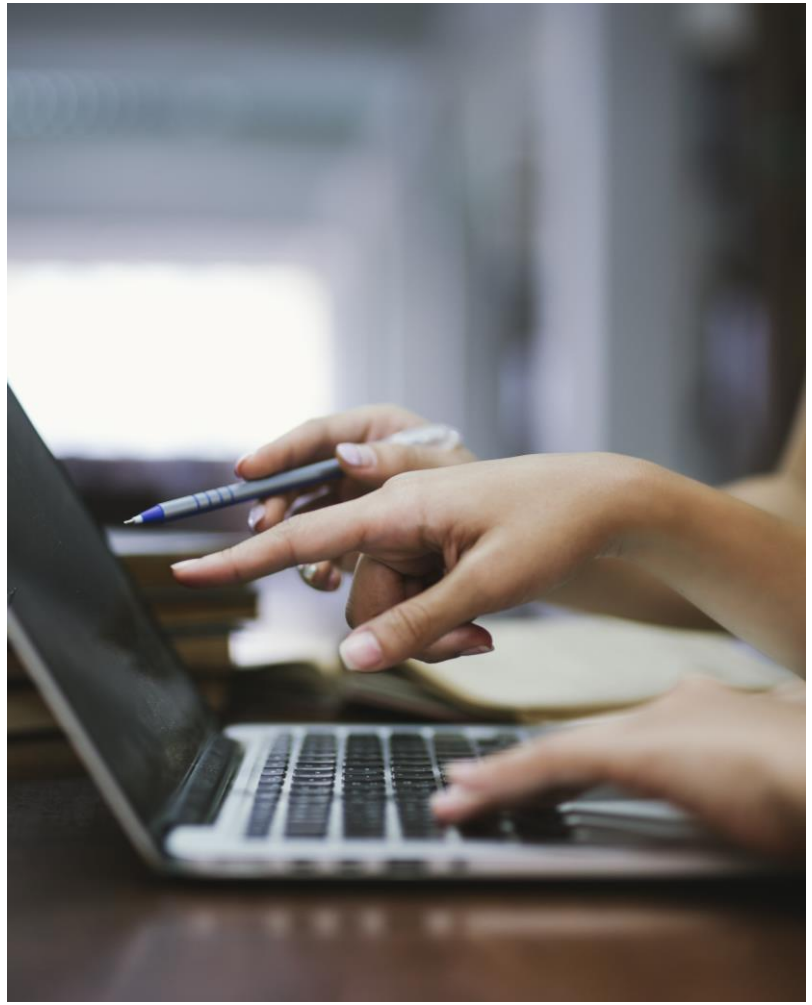
In Anbetracht der Situation in der Ukraine bewertet das Bundesamt für Sicherheit in der Informationstechnik (BSI) fortwährend die Lage mit Bezug zur Informationssicherheit.

Weiterhin erkennt das BSI eine abstrakt erhöhte Bedrohungslage für Deutschland. Für das BSI ist aber aktuell keine akute unmittelbare Gefährdung der Informationssicherheit in Deutschland im Zusammenhang mit der Situation in der Ukraine ersichtlich. Diese Bewertung kann sich nach Einschätzung des BSI jederzeit ändern.

Das BSI ruft daher weiterhin Unternehmen, Organisationen und Behörden dazu auf, ihre IT-Sicherheitsmaßnahmen zu erhöhen. Weitere Informationen stellt das BSI auf seinen Webseiten und im Rahmen Allianz für Cyber-Sicherheit bereit.

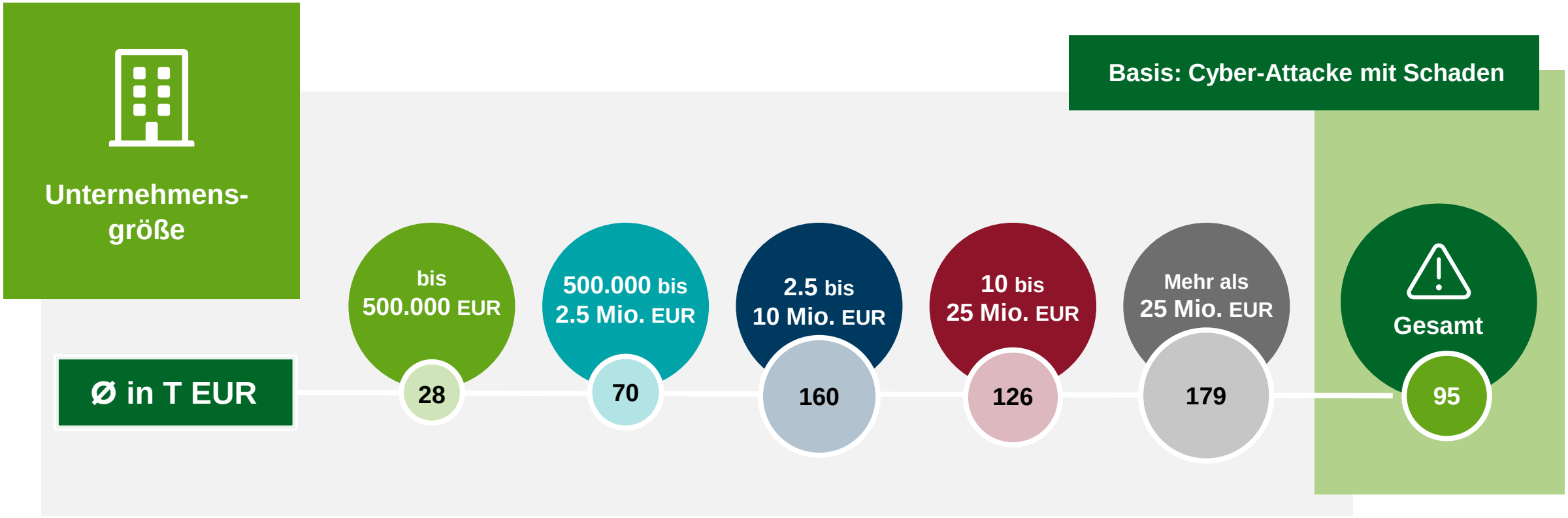
Änderungsrisiko auf einen Blick





Quelle: Eigene Zahlen, HDI Versicherung AG

Erfahrung Cyber-Attacke. Wie hoch ist der finanzielle Schaden, der Ihrem Unternehmen durch die Attacke entstanden ist?



Quelle: Repräsentative KMU-Stichprobe von 518 Unternehmen durch Sirius Campus im Auftrag von HDI im November und Dezember 2021.

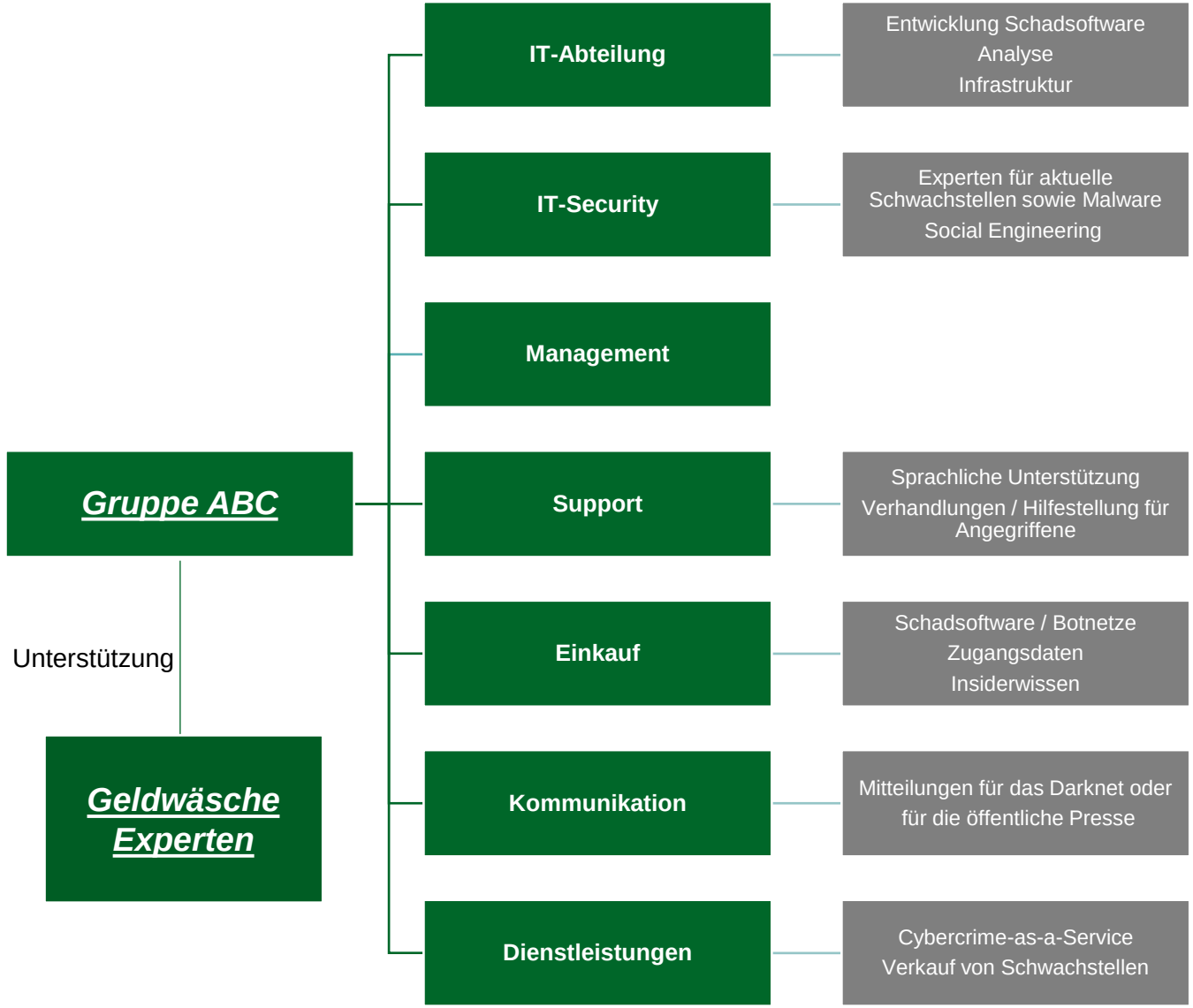
2

Ein Blick hinter die Kulissen

2. Ein Blick hinter die Kulissen

Warum steigt die Gefahr durch Cyberkriminelle?

- **Angreifergruppen werden immer professioneller**
  - Aufbau der Gruppen gleicht einem Unternehmen
  - Bildung eigener Abteilung mit spezialisierten Zielen
  - Erweiterung der Einnahmequellen durch Verkauf
  - Schreiben spezifischen Handbücher, mit Schritt für Schritt Anleitungen
- **Cyberkriminelle werden immer kreativer**
  - üben Druck über die Presse aus (eigene PR-Abteilung)
  - KI wird immer besser und wird genutzt



2. Ein Blick hinter die Kulissen

30.01.2019 Bewerbung via Arbeitsamt - Tim Krieger von Tim Krieger <tim.krieger@mailpulser.com>

Sehr geehrte Damen und Herren,

über die Internetseite des Arbeitsamts bin ich auf Ihre geschaltete Stellenanzeige aufmerksam geworden.
Durch meine mehrjährige Berufserfahrung und die kontinuierliche, selbständige Weiterbildung bin ich davon überzeugt, die mit der herausfordernden Stelle verbundenen Anforderungen zu Ihrer Zufriedenheit erfüllen zu können.

Meine Bewerbungsunterlagen finden Sie im Anhang dieser E-Mail.

Mein Ziel ist es, die angeeigneten Fähigkeiten gewinnbringend in Ihrem Unternehmen einzusetzen und mich dabei selbst kontinuierlich weiterzuentwickeln, um stets ein leistungsfähiger Mitarbeiter in Ihrem Unternehmen zu sein.

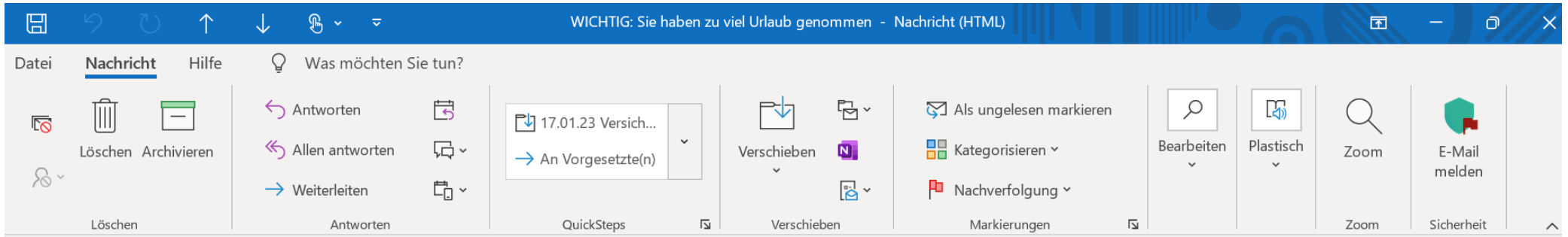
Für weitere Fragen stehe ich gerne zur Verfügung. Auf eine persönliche Vorstellung, in der ich Sie von meinen fachlichen Kenntnissen und Motivation überzeugen kann, freue ich mich.

Mit freundlichen Grüßen,

Tim Krieger

Anhang: Tim_Krieger_Bewerbungsunterlagen.doc (77,3 kB) (Vorsicht Virus)

2. Ein Blick hinter die Kulissen



WICHTIG: Sie haben zu viel Urlaub genommen

HR

Human Resources <human.resources@hdi.de>
An Kretschmer, Gero

Antworten | Allen antworten | Weiterleiten | ...

Fr 02.12.2022 13:47

Urlaub_Kretschmer.xls
186 KB

Sehr geehrter Herr Kretschmer,

bei der Überprüfung Ihres Restanspruchs auf Urlaub ist uns aufgefallen, dass Sie für dieses Jahr zu viele Urlaubstage beantragt haben. Um zu vermeiden, dass es zu Problemen im System kommt, bitten wir Sie, uns bis zum **04.12.2022** in der angehängten Excel-Datei Rückmeldung zu geben.

Dort befindet sich auch eine Übersicht Ihrer Urlaubstage.

Vielen Dank für Ihre Mithilfe!

Hier finden Sie das Dokument in Sharepoint: https://hdi.sharepoint.com/:x:/s/g-finance/EQI8iYAHW79Pv31oa6B_GwYB4I0EtKHrGmqv2RYnReud8w?e=6umtRR.

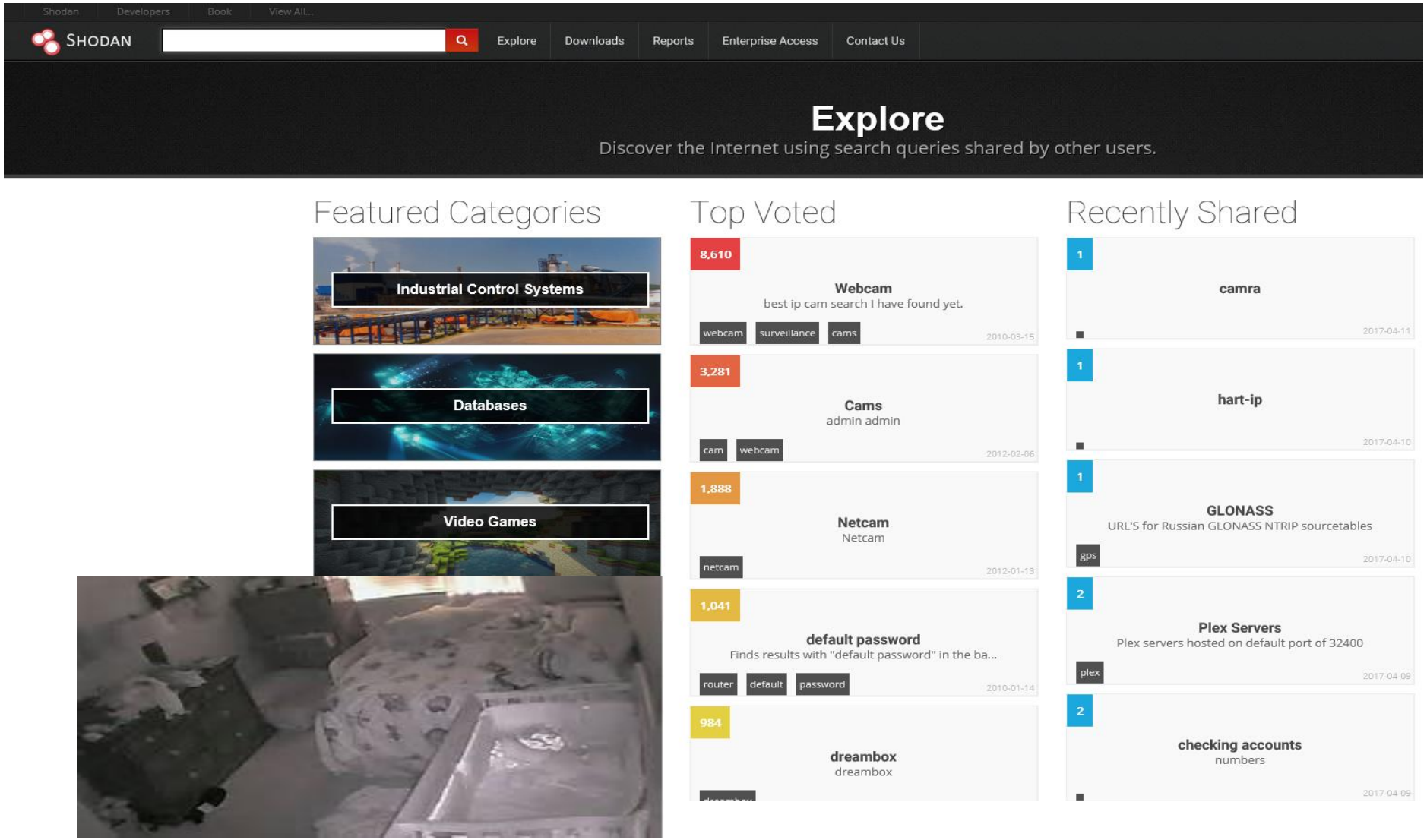
Ihre Personalabteilung

Support-Team | Gehaltsabrechnung
Human Resources

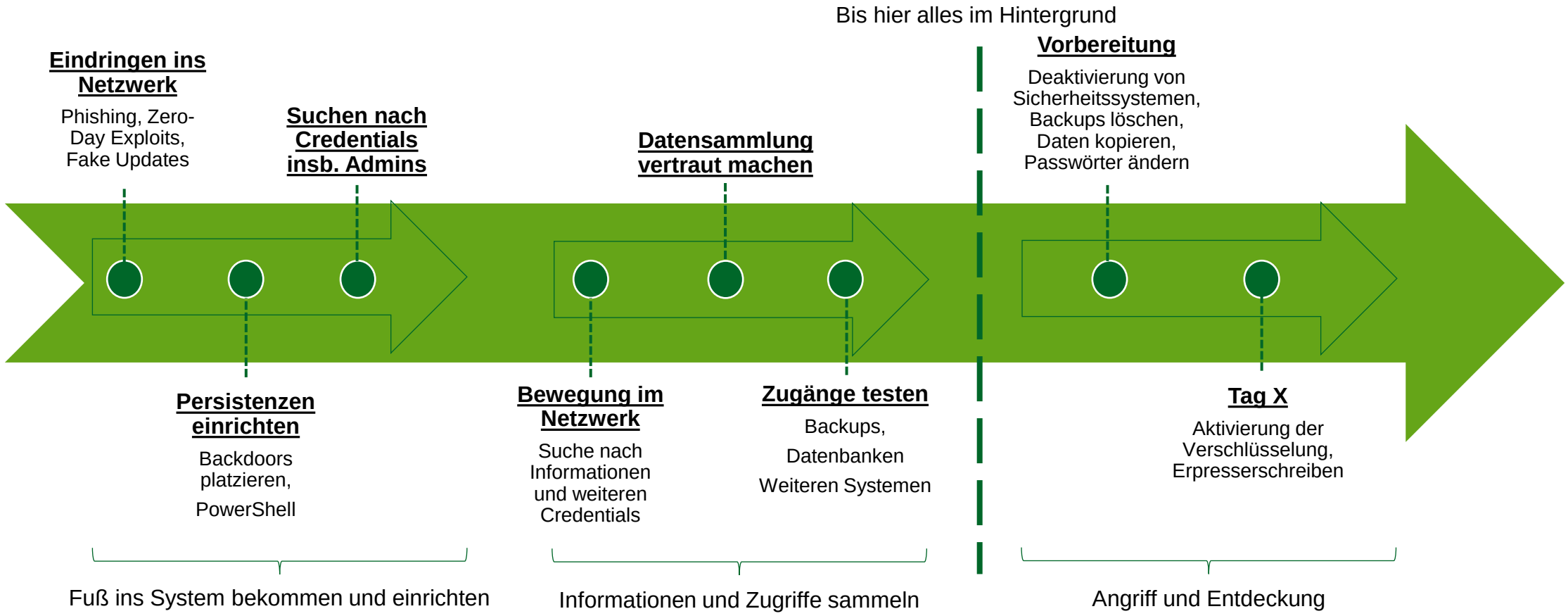
HDI AG

2. Ein Blick hinter die Kulissen

2. Ein Blick hinter die Kulissen



2. Ein Blick hinter die Kulissen



2. Ein Blick hinter die Kulissen

Schadenfall im Fitnessstudio

https://www.youtube.com/watch?v=sG8lNuoQiEg&feature=youtu.be

3

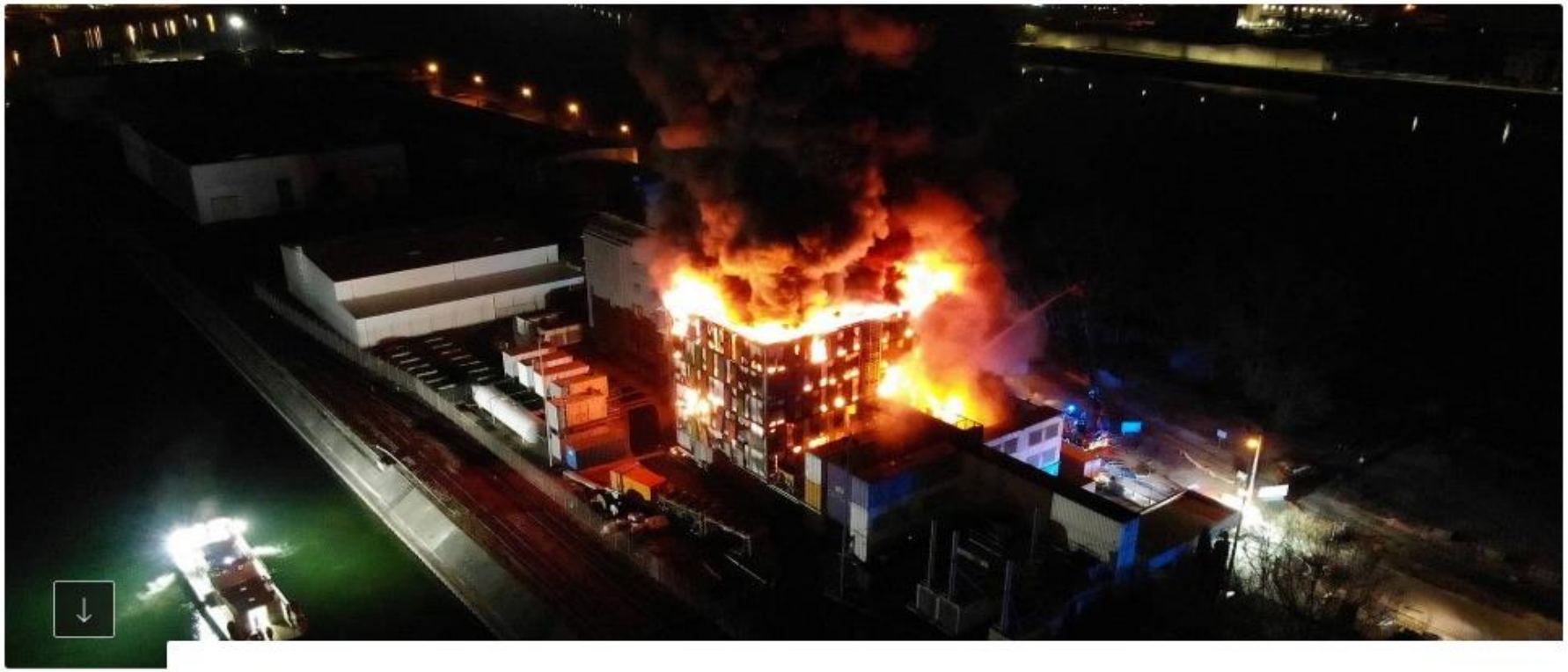
Rechte, Pflichten und Haftung im Alltag

Cloud - Eine gute Datensicherung?

RECHENZENTRUM IN FLAMMEN

Am Rhein brennt Europas Datenschatz

VON NIKLAS MAAK - AKTUALISIERT AM 13.03.2021 - 14:20



Ein ikonisches Bild: Europas größtes Rechenzentrum geht in Flammen auf, viele Daten sind für immer verloren. Was bedeutet das für uns Internetnutzer?

Cloud - Eine gute Datensicherung?

Welche Daten müssen geschützt werden?

- Gem. Art 4 Abs 1 DSGVO
  - Namen und Adressen
  - Fotos
  - E-Mailadressen und Internet-Adressen
  - Titel, Geschlecht, Größe, Haarfarbe usw.
  - Telefonnummern
  - Personalausweisnummern
  - Sozialversicherungsnummern

- Gem. Art 9 DSGVO
  - Politische Meinungen
  - Religionszugehörigkeit
  - Gewerkschaftszugehörigkeit
  - Gesundheitszustand
  - Sexualität

- **Verantwortlich** gem. DSGVO für die Einhaltung des Datenschutzes sind **u.a. Vorstände, Geschäftsführer oder Manager**. Also alle, die alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden

- **Alle Verantwortlichen haben Kontrollpflichten**. Wegen Nichteinhaltung der neuen Regeln können sie zudem persönlich zur Haftung (Art. 82 I DSGVO i.V.m. § 43 II GmbHG, §§ 93 II, 91 II AktG), wie bisher auch nach §§ 7 (1), 8 I BDSG, herangezogen werden und sowohl **Schadenersatzansprüchen und Geldbußen ausgesetzt sein**.

- Gem. Art. 82 I DSGVO hat jede Person, der ein **materieller oder immaterieller Schaden** entstanden ist, einen **Direktanspruch gegen den Verantwortlichen, einschließlich den Geschäftsführer, den Vorstand oder den Auftragsverarbeiter**.

- **Die Beweislast trägt hier gem. Art. 82 III DSGVO der Verantwortliche**.

Cloud - Eine gute Datensicherung?

Unternehmen die über die Cloud arbeiten wiegen sich oft in (falscher) Sicherheit

- Einfallstor ist meistens das eigenen IT-System und nicht der Cloud-Anbieter
- Bei Datenabfluss haftet der Cloud-Anbieter nur für die Datenwiederherstellung, nicht aber für:
  - Betriebsunterbrechungsschaden
  - Datenschutzverletzung
  - PR-Maßnahmen etc.
- Stichwort: Innentäter

Datenschutz

Datum	Behörde	Unternehmen	Verstoß	Bußgeldhöhe (ca. EUR)
02.09.21	Irland	WhatsApp Ireland Ltd.	Informationspflichten / Datenübermittlung an Facebook	225 Mio.
30.07.21	Luxemburg	Amazon Europe Core S.à r.l	Werbung / Datenweitergabe an Dritte	746 Mio.
08.01.21	**Niedersachsen**	Notebooksbilliger.de	Unzureichende Rechtfertigung	10 Mio.
30.10.19	**Berlin**	Deutsche Wohnen SE	Unzulässige Datenarchivierung	15 Mio. → durch LG Berlin aufgehoben (nicht rkr.)
11.11.20	**Bundesbeauftragter**	1&1 GmbH	Mängel bei Datensicherheit	9,5 Mio. **→ von LG Bonn herabgesetzt auf 900k (rkr.)**
01.10.20	Frankreich	Google LLC + Google Ireland Ltd.	Cookies / Einwilligung	60 Mio. + 40 Mio.
01.10.20	**Hamburg**	H&M	Ausspähung von Mitarbeitern	35 Mio.

Datenschutz

Zurückhaltende Auslegung	Weite Auslegung
OLG Stuttgart (Urt. V. 31.03.2021 – 9 U34/21): Mastercard- „Priceless Specials“ Hack – **Kein Sachdenersatz**, da Kläger Verstoß gegen Art. 32 DSGVO nicht nachgewiesen hat.	**LAG Köln** (Urt. v. 14.09.2020 – 2 Sa 358/20): Veröffentlichung einer PDF-Datei mit einem beruflichen Tätigkeitsprofil auf der Webseite der Beklagten nach Ende des Arbeitsverhältnisses – **300 EUR Schadensersatz**.
LG Frankfurt a.M. (Urt. v. 18.01.2021 – 2-30 O 147/20): Mastercard – „Priceless Specials“ Hack – **Kein Schadensersetz**, da Datenleck weder Pflichtverletzung durch Beklagte oder Erfüllungsgehilfen indiziert; Kausalität zwischen Datenleck und Spam-Anrufen nicht sicher festzustellen.	**LG Darmstadt** (Urt. v. 26.05.2020 – 13 O 244/19): Unbefugte Offenlegung von Bewerberdaten und Verstoß gegen Mitteilungspflicht aus Art. 34 DSGVO – **EUR 1.000 Schadensersatz**.
LG Köln (Urt. v. 07.10.2020 – 28 O 71/20): Unbefugte Zusendung eines Kontoauszugs an einen Dritten – **Kein Schadenersatz**, da SE in Bagatellfällen nicht dem Sinn und Zweck des Art. 82 DSGVO entspricht.	**LG Lüneburg** (Urt. v. 14.07.2020 – 9 O 145/19): Unzulässige Meldung einer Person bei einer Wirtschaftsauskunft – **EUR 1.000 Schadensersatz**.
LG Frankfurt a.M. (Urt. v. 18.09.2020 – 2/27 O 100/20): Mastercard „Priceless Specials“-Hack – **Kein Schadensersatz**, da keine Kausalität zwischen DSGVO-Verstoß und Schaden.	**ArbG Dresden** (Urt. v. 26.08.2020 – 13 Ca1046/20): Unbefugte Veröffentlichung von Gesundheitsdaten – **EUR 1.500 Schadensersatz**.
AG Frankfurt a.M. (Urt. v. 10.07.2020 – 385 C 155/19 (70): Marriott/Starwood-Hack – **Kein Schadensersatz**, da „Gefühl des Unbehagens“ nicht für immateriellen Schaden ausreiche; es bedürfte zumindest „öffentlicher Bloßstellung“.	**ArbG Münster** (Urt. v. 25.03.2021 – 3 Ca 391/20): Unbefugte Veröffentlichung eines Mitarbeiterfotos, welches besondere Kategorien personenbezogener Daten (Hautfarbe) enthielt – **EUR 5.000 Schadensersatz.**
AG Hannover (Urt. v. 09.03.2020 – 531 C 10952/19): Offenlegung von Daten gegenüber Reisebüro – **Kein Schadensersatz**, da lediglich Bagatellverstoß ohne ernsthafte Beeinträchtigung.	**AG Hildesheim** (Urt. v. 05.10.2020 – 43 C 145/19): Unbefugte Offenlegung von auf einem Computer gespeicherten Dateien durch Weiterverkauf nicht gelöschten PCs – **EUR 800 Schadensersatz**.
	AG Pforzheim (Urt. v. 25.03.2020 – 13 C 160/19): Unbefugte Offenlegung von Gesundheitsdaten – **EUR 4.000 Schadensersatz**.

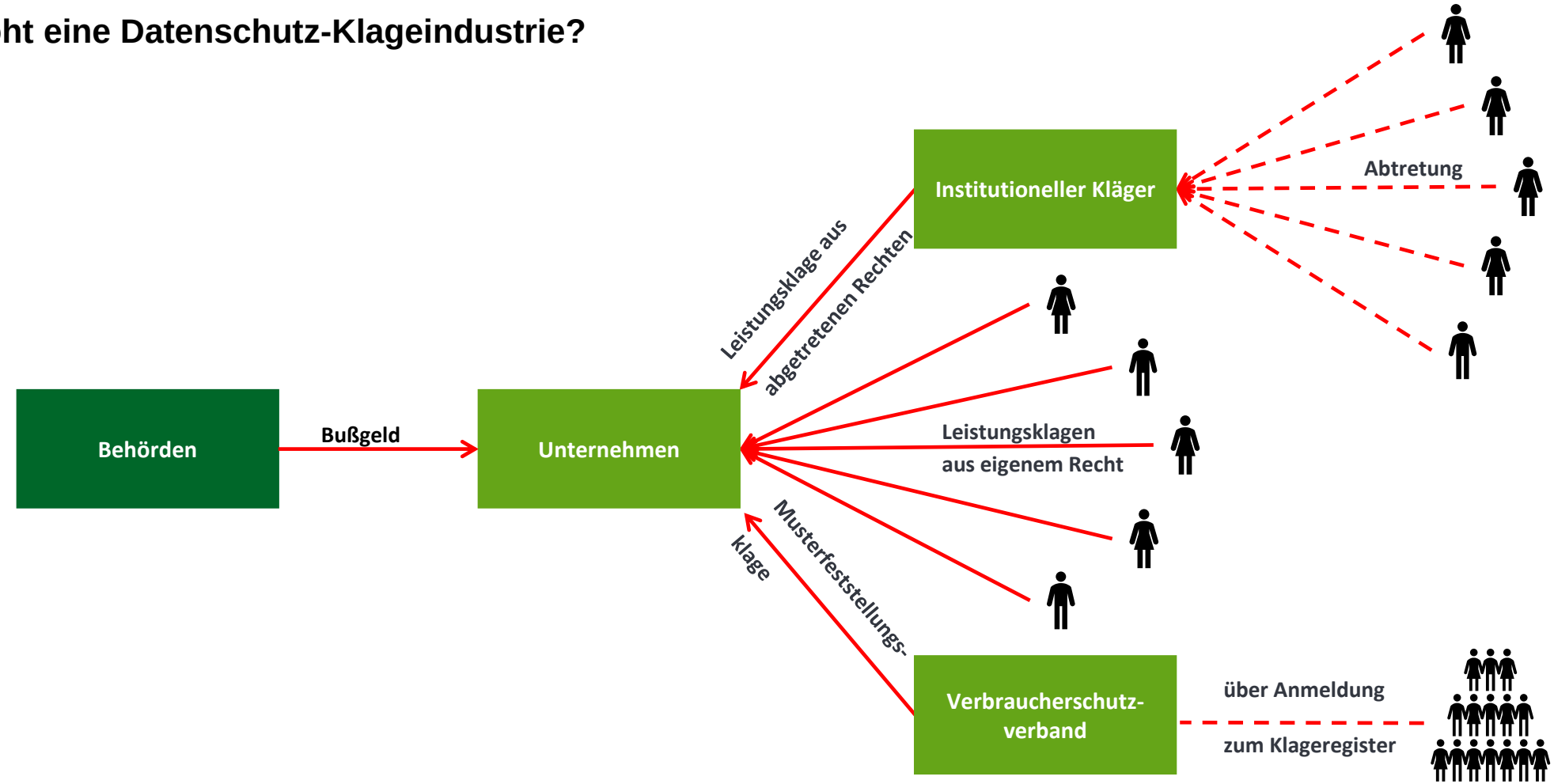
Datenschutz

LG München I, Urt. v. 9.12.2021, Az. 31 O 16606/20:

2.500,00 EUR immaterieller Schadensersatz nach Data Breach für Gefahr des Identitätsdiebstahls

Datenschutz

Droht eine Datenschutz-Klageindustrie?



4

Präventiver Schutz für Ihr Unternehmen

Schutzmaßnahmen der IT-Sicherheit

Technische Maßnahmen

- Passwortschutz
- Firewall
- Rollen & Berechtigungen
- Verschlüsselung

Organisatorische Maßnahmen

- IT-Richtlinien
- Sicherheitsaudits
- Datenklassifizierung

Personelle Maßnahmen

- Geheimhaltungs-vereinbarung
- Schulungen
- Background-Check

Risikotransfer / Versicherung

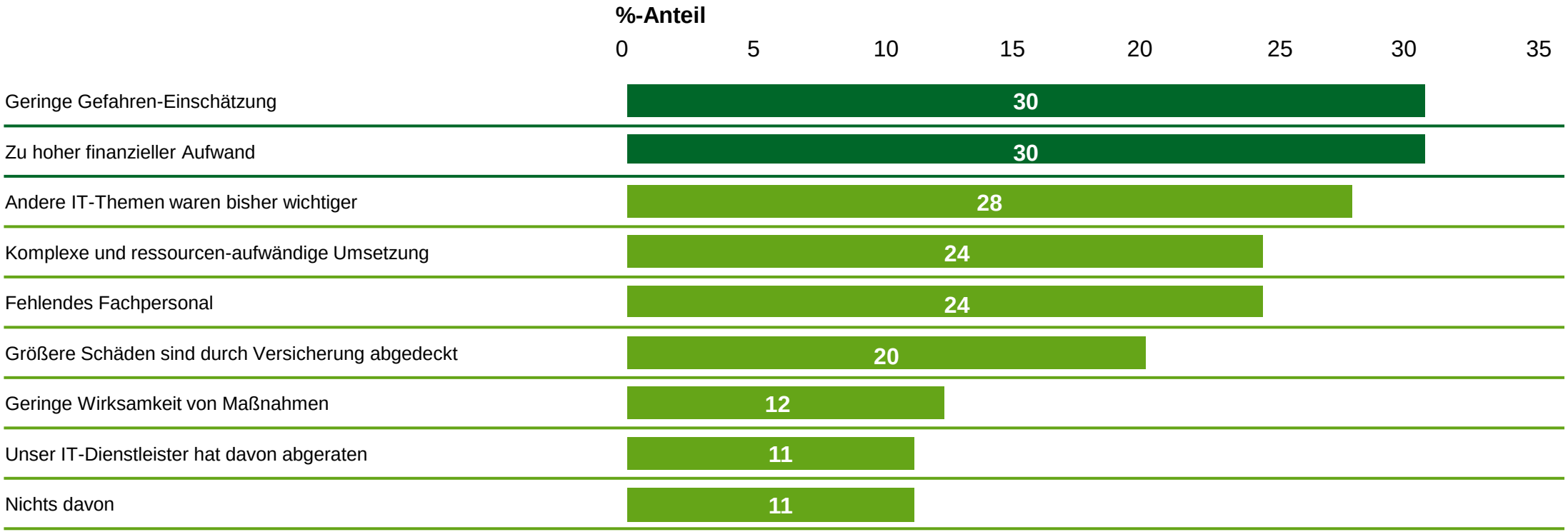
- Risikoakzeptanz
- Risikoabwälzung

Geringe Einschätzung und finanzieller Aufwand sind die häufigsten Gründe, die gegen weitere Präventionsmaßnahmen sprechen.

Prävention

Aus welchen Gründen werden in Ihrem Unternehmen Präventionsmaßnahmen im Bereich Cybersicherheit nicht umgesetzt?

Basis: alle Befragten

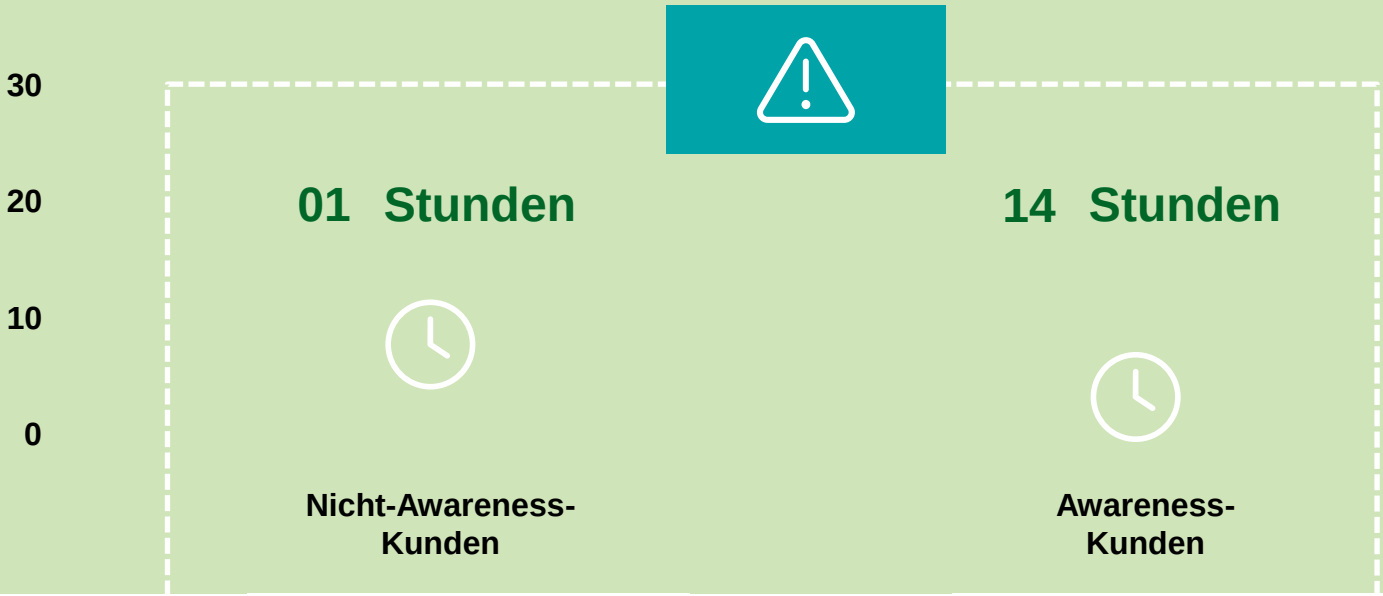


Basis: alle Angaben in %, Mehrfachantwort möglich.

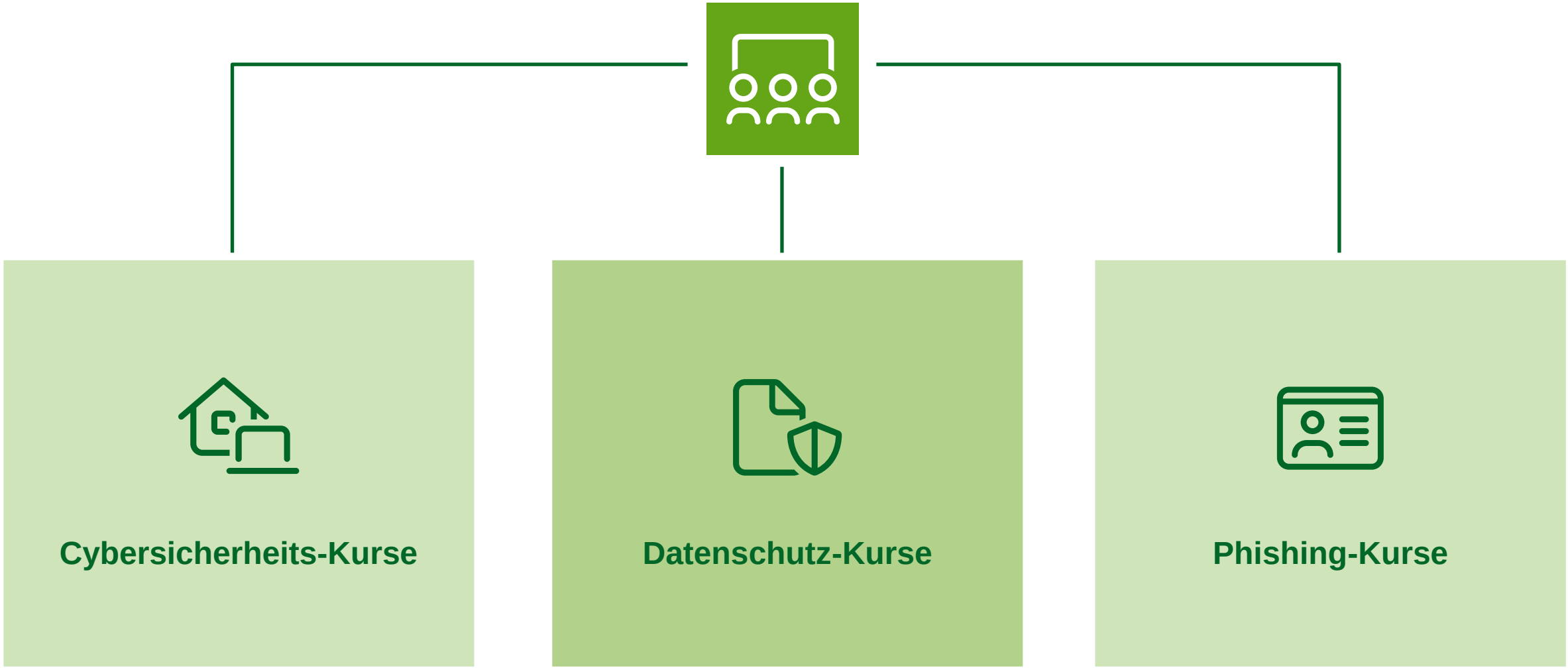
Quelle: Repräsentative KMU-Stichprobe von 518 Unternehmen durch Sirius Campus im Auftrag von HDI im November und Dezember 2021.

Geringe Einschätzung und finanzieller Aufwand sind die häufigsten Gründe, die gegen weitere Präventionsmaßnahmen sprechen.

Bei Nicht-Awareness-Kunden durchschnittliche Bearbeitungszeit im Incident Response von 14 Stunden und bei Awareness-Kunden von 7 Stunden



Security-Konzept – Schulungen



Security-Konzept – Phishingsmails

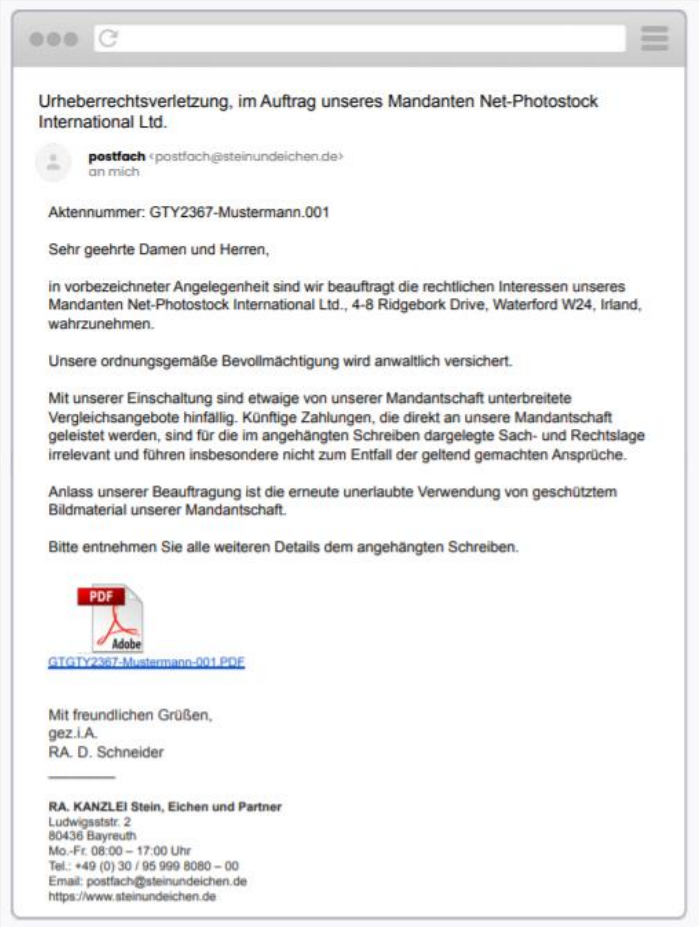
Mit simulierten Betrugs-E-Mails wird das Gefahrenbewusstsein kontinuierlich überprüft. Perseus führt in unregelmäßigen Abständen Phishing-Simulationen mit verschiedenen Phishing-Vorlagen durch. Mit Hilfe von Tracking-Links kann das Verhalten Ihrer Mitarbeitenden nachverfolgt und statistisch ausgewertet werden

Lernen durch Sensibilisierung

Klicken Ihre Kollegen und Kolleginnen während einer Phishing-Simulation fälschlicherweise auf Anhänge oder Links in der simulierten Betrugs-E-Mail, werden sie auf eine Phishing-Test-Webseite geleitet. Hier werden sie noch einmal über die Erkennungsmerkmale und Gefahren von Phishing-E-Mails aufgeklärt.

Auswertung Phishing-Simulationen

Die Ergebnisse der Phishing-Tests sind für Admins auf der Perseus-Plattform einsehbar. Dort können Sie die Lernerfolge Ihrer Mitarbeitenden nachverfolgen.



Urheberrechtsverletzung, im Auftrag unseres Mandanten Net-Photostock International Ltd.

postfach <postfach@steinundeichen.de>
an mich

Aktennummer: GTY2367-Mustermann.001

Sehr geehrte Damen und Herren,

in vorbezeichneter Angelegenheit sind wir beauftragt die rechtlichen Interessen unseres Mandanten Net-Photostock International Ltd., 4-8 Ridgebork Drive, Waterford W24, Irland, wahrzunehmen.

Unsere ordnungsgemäße Bevollmächtigung wird anwaltlich versichert.

Mit unserer Einschaltung sind etwaige von unserer Mandantschaft unterbreitete Vergleichsangebote hinfällig. Künftige Zahlungen, die direkt an unsere Mandantschaft geleistet werden, sind für die im angehängten Schreiben dargelegte Sach- und Rechtslage irrelevant und führen insbesondere nicht zum Entfall der geltend gemachten Ansprüche.

Anlass unserer Beauftragung ist die erneute unerlaubte Verwendung von geschütztem Bildmaterial unserer Mandantschaft.

Bitte entnehmen Sie alle weiteren Details dem angehängten Schreiben.

PDF
GTGTY2367-Mustermann-001.PDF

Mit freundlichen Grüßen,
gez.i.A.
RA. D. Schneider

RA. KANZLEI Stein, Eichen und Partner
Ludwigsststr. 2
80436 Bayreuth
Mo.-Fr. 08:00 – 17:00 Uhr
Tel.: +49 (0) 30 / 95 999 8080 – 00
Email: postfach@steinundeichen.de
https://www.steinundeichen.de

Security-Konzept – Notfallplan

Allgemeine Inhalte:

- Vorbereitung auf den Notfall
- Verhaltensregeln für Verantwortliche und Mitarbeiter
- Vordefinierte Szenarien
- Wiederherstellungsplan / Wiederanlaufkonzept
- Umfangreicher Notfallplan für Notfallbeauftragte
- Individualisierbar für jedes Unternehmen
- Hinterlegung aller wichtigen Ansprechpartner

Cyber-Versicherung als Präventiver Partner

Nachhaltige Prävention durch proaktives Mitarbeiter-Training

Bereit für digitale Verantwortung

perseus.

- **Einfache** Sensibilisierung aller Mitarbeiter
- **Praxisnah** – Fingierte Hackerangriffe/Phishingversuche
- Schulungen **bequem** per Knopfdruck verwalten

Direkte Hilfe im Notfall mit umfassendem Service und Krisenmanagement

Wenn es darauf ankommt

- Schadenhotline rund um die Uhr verfügbar
- Soforthilfe und Expertennetzwerk
- Krisenmanagement

Service

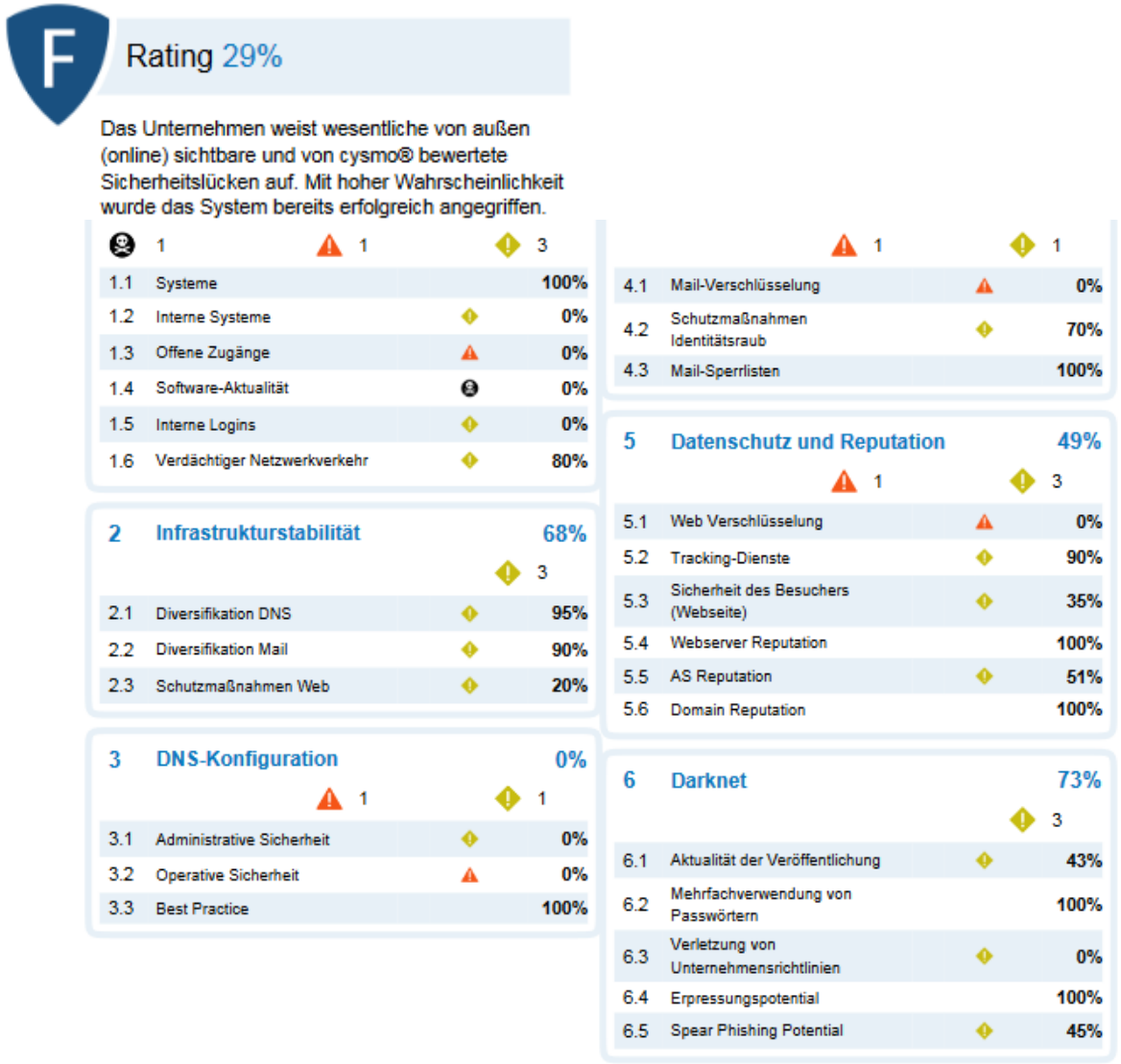
So existenziell wie eine Feuerversicherung für Ihr Unternehmen

- **Technische Unterstützung bei Schwachstellenanalyse** – z.B. Log4J
- **Audits und Schwachstellenscan**
- **Schulungen und Fortbildungen**

HDI


LIVE-RATING …
Kostenloser Scan
by ppi

Cysmo Report



cysmo® -Reports bieten einen Mehrwert für alle Segmente:

- Risikoinformationen über das Unternehmen
- Einfache Erklärungen für Kunden
- Technische Details für IT-Verantwortliche
- Unterstützung der Verbesserung der eigenen IT

Ihr Ansprechpartner

DSSV
Arbeitgeberverband deutscher
Fitness- und Gesundheits-Anlagen

Herr
Mario Böhnlein

+49 (0) 175 9353626

mb@pisa-experts.de

www.pisa-experts.de


VIELEN DANK
für die Aufmerksamkeit.