# Herzlich willkommen! Ihre Online-Session startet gleich.

Schön, dass Sie dabei sind. Hören Sie uns einfach per Kopfhörer oder Lautsprecher zu.

Wir schalten die Mikrofone der Teilnehmer:innen stumm. Dann hören Sie alles besser. Auch alle Webcams sind automatisch deaktiviert.

Ihre Fragen können Sie über das Fragen-Fenster stellen. Der/die Moderator:in bringt Ihre Fragen entsprechend ein.

## Session wird aufgezeichnet

Educational Month |

# Cyber Security

Online-Session

## IT-Sicherheit ist Chefsache:

Unternehmenswerte schützen,
(persönliche) Haftung minimieren

19.09.2024

vodafone business

# Herzlich willkommen!

Schön, dass Sie dabei sind. Hören Sie uns einfach per Kopfhörer oder Lautsprecher zu.

Wir schalten die Mikrofone der Teilnehmer:innen stumm. Dann hören Sie alles besser. Auch alle Webcams sind automatisch deaktiviert.

Ihre Fragen können Sie über das Fragen-Fenster stellen. Der/die Moderator:in bringt Ihre Fragen entsprechend ein.

## Session wird aufgezeichnet

# Heute für Sie dabei:

**Dr. Hauke Hansen**

Rechtsanwalt

# Agenda

01 Intro

02 Geldbußen

03 Schadensersatz

04 (Persönliche) Haftung

05 Lösegeld

06 Filmtipps

# Intro

01


YOU
ARE
FUCKED

# Auswirkungen von Cyberangriffen

- Abfluss von Daten
- Negative Presse
- Ausfall oder Übernahme der IT oder OT
- Kritische Kundenfragen
- Verschlüsselung von Daten
- Zusammenbruch der Geschäftstätigkeit

Startseite › Rhein-Main › Landespolitik

## Millionenschaden nach IT-Angriff auf Frankfurter Uniklinik – Hacker-Attacken nehmen zu

14.01.2024, 18:43 Uhr

HACKERANGRIFF

## Datenleck trifft auch Kunden der Direktbanken ING und Comdirect

## IT-Sicherheitsvorfall: Varta stoppt Produktion

Der Batteriehersteller Varta AG hat nach einem Cybervorfall die IT-Systeme sowie seine Produktion heruntergefahren.

RECHERCHE VON „CORRECTIV“

## Tausende Daten des BSW nach Hackerangriff im Netz verfügbar

NACH CYBERANGRIFF

## Continental informiert von Datenraub betroffene Mitarbeiter

Erstmals beziffert Continental das Ausmaß des Cyberangriffs. Jetzt plädiert der Konzern in Berlin für ein Verbot, Lösegeld zu zahlen.

NORDRHEIN-WESTFALEN BEHÖRDEN EINGESCHRÄNKT

## Seit einem Hackerangriff ist in Südwestfalen nichts mehr, wie es einmal war

Suche nach Ursache

## War es ein Hacker-Angriff? Chaos bei VW - IT-Störung legt Produktion lahm

# Geldbußen

02

Datenschutzverstoß

# Hotelkette Marriott drohen mehr als 100 Millionen Euro Bußgeld

Ein Datenleck von Marriott betraf 383 Millionen Hotelgäste. Der Vorfall ist nicht nur für Kunden ärgerlich, sondern auch ein Verstoß gegen die Datenschutz-Grundverordnung, sagen britische Datenschützer.

Teures Datenleck

# British Airways soll 200 Millionen Euro wegen Datenklau zahlen

## Passwörter im Klartext: 20.000 Euro Bußgeld nach DSGVO gegen Knuddels.de

Anfang September waren Hunderttausende Passwörter von Knuddels-Nutzern im Netz aufgetaucht. Für die unverschlüsselte Speicherung muss das Forum nun zahlen.

0

DER HESSISCHE BEAUFTRAGTE
FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT

# Meldung von Verletzungen des Schutzes personenbezogener Daten (Art. 33 DS-GVO/§ 65 BDSG i.V.m. § 500 StPO/§ 60 HDSIG)

| **1. Verantwortlicher (Art. 33 Abs. 1, Abs. 3 Buchst. b DS-GVO i. V. m. Art. 4 Nr. 7 DS-GVO/ § 65 Abs. 1, Abs. 3 Nr. 2 BDSG i.V.m. § 46 Nr. 7 BDSG/ § 60 Abs. 1, Abs. 3 Nr. 2 HDSIG i. V. m. § 41 Nr. 8 HDSIG)** |
|---|
| Kontaktdaten |
| Bezeichnung bzw. Name der verantwortlichen Stelle:<br>*Klicken oder tippen Sie hier, um Text einzugeben.* |
| Straße & Hausnummer:<br>*Klicken oder tippen Sie hier, um Text einzugeben.* |
| Postleitzahl und Ort:<br>*Klicken oder tippen Sie hier, um Text einzugeben.* |
| Allgemeine E-Mail-Adresse der verantwortlichen Stelle:<br>*Klicken oder tippen Sie hier, um Text einzugeben.* |
| Meldende Person (Ihr Name):<br>*Klicken oder tippen Sie hier, um Text einzugeben.* |
| Ihre Funktion:<br>*Klicken oder tippen Sie hier, um Text einzugeben.* |
| Ihre E-Mail-Adresse (für Rückfragen):<br>*Klicken oder tippen Sie hier, um Text einzugeben.* |
| Ihre Telefonnummer (für Rückfragen):<br>*Klicken oder tippen Sie hier, um Text einzugeben.* → |
| Behördliche/r bzw. betriebliche/r Datenschutzbeauftragte/r:<br>*Klicken oder tippen Sie hier, um Text einzugeben.* |

| **2. Zeitlicher Ablauf/Zeitpunkt des Vorfalls (Art. 33 Abs. 1 DS-GVO/ § 65 Abs. 1 BDSG/ § 60 Abs. 1 HDSIG)** |
|---|
| Wann hat der Vorfall stattgefunden/begonnen?<br>*Klicken oder tippen Sie, um ein Datum einzugeben.*<br>Oder:<br>☐ Zeitpunkt nicht bekannt |
| Wann war der Vorfall abgeschlossen?<br>*Klicken oder tippen Sie, um ein Datum einzugeben.* |
| Dauert der Vorfall noch an?<br>☐ ja ☐ nein |
| Ist eine Wiederholung des Vorfalls zu befürchten?<br>☐ ja ☐ nein |
| Wann haben Sie Kenntnis vom Vorfall erhalten?<br>*Klicken oder tippen Sie, um ein Datum einzugeben.* |
| Erfolgt Ihre Meldung später als 72 Stunden nach Bekanntwerden des Vorfalls, begründen Sie hier bitte die Verzögerung:<br>*Klicken oder tippen Sie hier, um Text einzugeben.* |
| **3. Beschreibung der Datenschutzverletzung (Art. 33 Abs. 3 Buchst. a DS-GVO/§ 65 Abs. 3 Nr. 1 BDSG/§ 60 Abs. 3 Nr. 1 HDSIG)** |
| Art der Verletzung des Schutzes personenbezogener Daten:<br>☐ Gerät verloren/gestohlen<br>☐ Unterlagen verloren, gestohlen oder an einem unsicheren Platz gelagert<br>☐ Unverschlüsselter E-Mail-Versand<br>☐ Postsendung ging verloren oder wurde versehentlich geöffnet<br>☐ Hackerangriff, Schadsoftware, Phishing<br>☐ Nicht datenschutzgerechte Entsorgung von Materialien (z. B. Akten, Bild- oder Tonträger)<br>☐ Nicht datenschutzgerechte Geräteentsorgung (z.B. Festplatten)<br>☐ Missbrauch von Zugriffsrechten (Nichtberechtigter Abruf durch eigene Mitarbeiter)<br>☐ Unbeabsichtigte Veröffentlichung<br>☐ Webportal zeigte falsche/-fremde Daten an |

1 Xpro Woche !
mit d. Datensch. F [redacted]
1
Hansen!

**DER HESSISCHE BEAUFTRAGTE**
**FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT**

DER HESSISCHE BEAUFTRAGTE
FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT
Postfach 31 63 · 65021 Wiesbaden

[redacted]
Datenschutzbeauftragter
[redacted]

vorab Via E-Mail an [redacted]

Aktenzeichen [redacted]
*Bitte bei Antwort angeben*
zuständig [redacted]
Durchwahl 14 08 -
Ihr Zeichen
Ihre Nachricht vom [redacted]
Datum [redacted]2022

**Datenschutz im nichtöffentlichen Bereich nach der Datenschutz-Grundverordnung (DS-GVO), dem Bundesdatenschutzgesetz (BDSG) und dem Hessischen Datenschutz- und Informationsfreiheitsgesetz (HDSIG)**

**Ihre Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DS-GVO vom Dienstag, d[redacted] und vom Mittwoch, d[redacted] 2022**

Sehr geehrter Herr [redacted]
sehr geehrter Herr [redacted]
sehr geehrter Herr [redacted]

ich nehme Bezug auf Ihre Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DS-GVO vom Dienstag, d[redacted]2 und vom Mittwoch, de[redacted]2. Für die bisherige Darstellung des Sachverhaltes danke ich Ihnen.

Zur Prüfung benötige ich jedoch weitere Informationen. Ich bitte Sie daher folgende Fragen detailliert zu beantworten und mir die ggf. erforderlichen Unterlagen einzureichen:

## I. Beschreibung des Vorfalls

1. Wie wurden Sie auf die Angreifer aufmerksam?
2. Welche IT-Systeme und -Dienste waren von dem Vorfall betroffen? Bitte übermitteln Sie eine vollständige und aussagekräftige Aufstellung der Systeme inkl. Angaben zu
   - deren Einsatzzwecken,
   - den Software-Versionen der darauf laufenden Betriebssysteme und
   - den Software-Versionen der darauf laufenden relevanten Dienste.





3. Wie war der vollständige inhaltliche und zeitliche Ablauf des Vorfalls? Beschreiben Sie bitte den vollständigen Hergang des Vorfalls. Bitte fügen Sie hierzu Übersichten bei, wie z. B. die am [redacted] 2022 erbetene Aufstellung der von Ihnen genutzten und von dem Angriff betroffenen Dienstleistungen und Produkte [redacted]care.

## II. Beschreibung der Analysen und Maßnahmen

4. Welche Arten von Analysen führten Sie oder von Ihnen beauftragte Dienstleister in welcher Form, in welchem Umfang und mit welchen konkreten Analyseaufträgen in Folge des Angriffs durch?
5. Stellen Sie als Teil Ihrer Antwort alle zugehörigen, aussagekräftigen Abschlussberichte (oder derzeitige Zwischenberichte) sowie weitere für das Verständnis erforderliche Unterlagen zur Verfügung.
6. Mit Telefonat [redacted]022 teilten sie mit, dass 95% ihrer Backups lauffähig sind.
   - Welche Strategie der Wideraufnahme des Betriebes verfolgten sie?
   - Wie wurde sichergestellt, dass die widerhergestellten Backups nicht kompromittiert sind oder waren?
   - Wie wurde sichergestellt, dass eine Analyse der Systeme hinsichtlich Quelle/Ursprung und Verlauf des Angriffs nach dem wiedereinspielen des Backups möglich waren?
7. Welche Datenflüsse existieren zwischen weiteren IT-Systemen und -Diensten die mit den betroffenen IT-Systeme und –Dienste verbunden sind?
8. Wie konnten Sie ausschließen, dass keine Ausweitung des Angriffs von den IT-Systemen und –Diensten auf dahinterliegende IT-Systemen und –Diensten erfolgte?
9. Wie haben Sie sichergestellt, dass die von Ihnen berücksichtigten Informationen ein vollständiges Bild über den Hergang und das Ausmaß der Verletzungen des Schutzes personenbezogener Daten liefern?
10. Sie haben angegeben, dass der Vorfa[redacted]022 begonnen hat. Wie konnten Sie einen früheren Zugriff auf Ihre IT-Systeme sicher ausschließen?

11. Gemäß Ihren Angaben kam es zu Datenabflüssen, daher bitte ich folgende Fragen dazu zu beantworten:

    - Welche Arten von Daten sind abgeflossen?
      Führen sie die Kategorien und die spezifischen Daten innerhalb der jeweiligen Kategorien auf. Bitte liefern Sie eine vollständige Zuordnung der Datenarten zu den jeweiligen Tochterunternehmen oder Mehrheitsbeteiligung.
    - Konnten eine oder mehrere Schnittstellen identifiziert werden, über die Daten abgeflossen sind?
    - Wie sieht die jeweilige Schnittstelle aus?
    - Lassen sich die Daten, die hierüber abgeflossen sind kategorisieren?
    - Wie lautet der ihnen bekannt gewordene Darknet-Link?
    - Wie und in welchem Umfang wurden die veröffentlichten Daten analysiert? Fügen sie bitte einen aussagekräftigen Bericht oder Zwischenbericht je Stand bei.

12. Gab es in der Vergangenheit Auffälligkeiten beim Betrieb der vom Vorfall betroffenen IT-Systeme und -Dienste? Falls ja, erläutern Sie bitte, wann es zu welchen Auffälligkeiten gekommen ist und wie Sie darauf reagiert haben.

13. Konnten Informationen bzgl. der Angreifer gewonnen werden?

    - Welche Art und Umfang der Kommunikation fand statt? Bitte fügen sie hierzu entsprechende Korrespondenz bei.
    - Welche Maßnahmen im Hinblick auf die Angreifer wurden mit anderen Behörden eingeleitet?
    - Sofern eine Kommunikation zu Hessen3C stattfand, darf eine Kontaktaufnahme bezüglich der Untersuchungsergebnisse durch uns stattfinden?

14. Welche Maßnahmen zur Vermeidung eines erneuten Vorfalls

    - haben sie bereits umgesetzt?
    - werden sie noch bis wann umsetzen?
    - wurden von ihnen aus welchen Gründen verworfen?

15. Welches Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen



Maßnahmen wurde bzw. werden künftig von Ihnen gemäß Art. 32 Abs. 1 lit. d) der DS-GVO umgesetzt?

**III. Betroffene Personen**

16. Welche konkreten Folgen ergaben sich für die Betroffenen?
17. Wie viele Betroffene gibt es und wie lassen sich diese kategorisieren?
18. Konnten Sie bereits vor der Veröffentlichung der Daten im Darknet feststellen, welche Daten abgeflossen sind?
19. Zu welchem Zeitpunkt und aufgrund welchem Analyseergebnis haben Sie festgestellt, dass aus den abgeflossen/ eingesehen personenbezogenen Daten ein hohes Risiko für die Betroffenen bestand?
20. In welcher Form wurden die betroffenen Personen wann informiert? Bitte übersenden Sie eine Kopie dieser Information. Sollten Sie betroffene Personen im Geltungsbereich der DS-GVO zu unterschiedlichen Zeitpunkten oder ggf. mehrfach informiert haben, geben Sie bitte den jeweiligen Zeitpunkt, den Inhalt und den Adressatenkreis an.
21. Welche möglichen Risiken für die Rechte und Freiheiten der betroffenen Personen wurden kommuniziert?
22. Welche Maßnahmen wurden den betroffenen Personen empfohlen?

Wenn Sie mir im Zusammenhang mit unserer Kommunikation sensible Informationen zukommen lassen wollen, können Sie dies gerne auf einem sicheren Übermittlungsweg durchführen. Auf meiner Homepage können Sie für diesen Zweck unter „Service > Verschlüsselte Kommunikation HBDI" einen PGP-Key herunterladen. Darüber hinaus besteht auch die Möglichkeit der Übermittlung auf dem Postweg.

Für den Eingang Ihrer schriftlichen Stellungnahme habe ich mir

**Dienstag, den [redacted]2022**

vorgemerkt.

Für juristische Rückfragen stehen Ihnen gerne Frau [redacted] unter der Telefonnummer [redacted] oder Frau [redacted] unter der Telefonnummer [redacted] zur Verfügung. Für technische Rückfragen steht Ihnen gerne [redacted] unter der Tele[redacted]-140[redacted]r Zimmer unter der Telefonnummer [redacted] zur Verfügung.

Nach Art. 31 DS-GVO sind Sie verpflichtet, mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammenzuarbeiten. Ein Verstoß gegen Art. 31 DS-GVO kann gem. Art. 83 Abs. 4 lit. a) DS-GVO mit einer Geldbuße von bis zu 10.000.000,00 € oder im



Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem welcher Betrag höher ist, geahndet werden.

Nach § 40 Abs. 4 S. 1 BDSG sind Sie verpflichtet, die erforderlichen Auskünfte zu erteilen. Bitte beachten Sie, dass Sie nach Art. 58 Abs. 1 lit. a) DS-GVO auch zur Bereitstellung der erforderlichen Informationen angewiesen werden können.

Ich weise gemäß § 40 Abs. 4 S. 2 BDSG darauf hin, dass Sie die Auskunft auf solche Fragen verweigern können, deren Beantwortung Sie selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozessordnung (ZPO) bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten (OWiG) aussetzen würde. Sollten Sie von dem Auskunftsverweigerungsrecht Gebrauch machen wollen, sind Sie verpflichtet, mir dies mitzuteilen.

Mit freundlichen Grüßen
Im Auftrag

gez. [redacted]

# Dürfen die das?

# Vorschriften

Art. 83 DSGVO

**Allgemeine Bedingungen für die Verhängung von Geldbußen**

1. Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 4, 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist. […]

Art. 32 DSGVO

**Sicherheit der Verarbeitung**

1. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrschein-lichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; […]

# Vorschriften

Art. 83 DSGVO

**Allgemeine Bedingungen für die Verhängung von Geldbußen**

1. Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 4, 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und **abschreckend** ist. […]

Art. 32 DSGVO

**Sicherheit der Verarbeitung**

1. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrschein-lichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; […]

# Vorschriften

Art. 83 DSGVO

**Allgemeine Bedingungen für die Verhängung von Geldbußen**

1. Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 4, 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und **abschreckend** ist. […]

Art. 32 DSGVO

**Sicherheit der Verarbeitung**

1. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrschein-lichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter **geeignete technische und organisatorische Maßnahmen**, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; […]

# Vorschriften

Art. 83 DSGVO

**Allgemeine Bedingungen für die Verhängung von Geldbußen**

1. Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 4, 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und **abschreckend** ist. […]

Art. 32 DSGVO

**Sicherheit der Verarbeitung**

1. Unter Berücksichtigung des **Stands der Technik**, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrschein-lichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; […]

# Vorschriften

Art. 83 DSGVO

**Allgemeine Bedingungen für die Verhängung von Geldbußen**

1. Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 4, 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und **abschreckend** ist. […]

Art. 32 DSGVO

**Sicherheit der Verarbeitung**

1. Unter Berücksichtigung des **Stands der Technik**, der **Implementierungskosten** und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrschein-lichkeit und **Schwere des Risikos** für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; […]

# Schadensersatz

03

# Facebook Datenleck – LG Stuttgart spricht Schadenersatz zu

09.02.2023 • 2 Minuten Lesezeit • ★★☆☆☆ (5)

Handelsblatt

URTEIL

## Nach Datenleck: Scalable Capital soll Schadensersatz zahlen

Im Oktober 2020 waren mehr als 33.000 Personen von einem Datendiebstahl bei dem digitalen Vermögensverwalter betroffen. Nun ist ein erstes Urteil gefallen.

Frankfurter Allgemeine

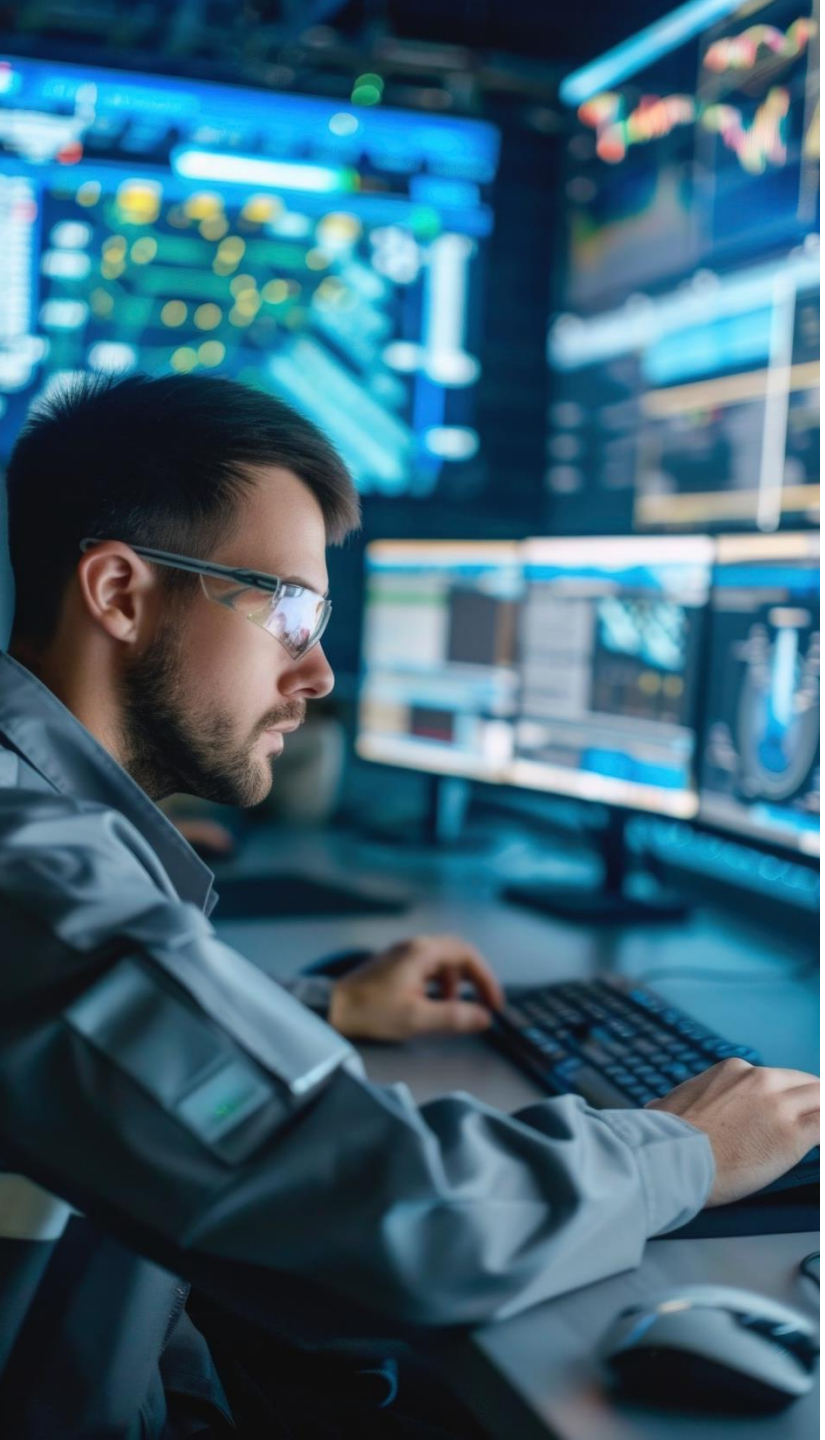
VERGLEICHSANGEBOT AN KLÄGER

## Mastercard will Kunden nach Datenleck bis zu 300 Euro zahlen

# Kernaussagen des EuGH

- Bloßer Verstoß gegen die DSGVO reicht nicht aus
- Schaden muss nachgewiesen werden
- Keine Bagatellgrenze
- Kein Strafschadensersatz

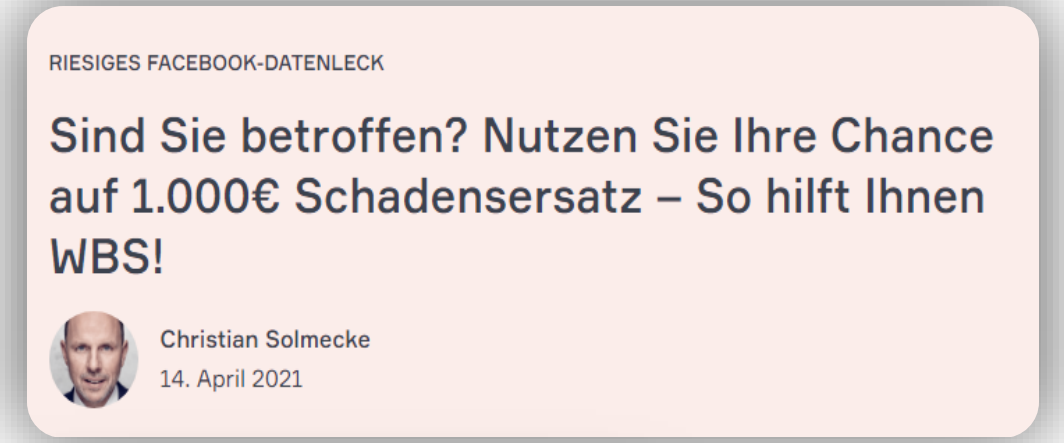
**Aber:**
Wie wird ein immaterieller Schaden berechnet?



# Schadensersatz und Anlässe vor dem EuGH-Urteil

| | Schadensersatz pro Person |
|---|---|
| **LG Lübeck, LG Paderborn**<br>Facebook, Kein Schutz gegen Scraping | **500 €** |
| **LG München**<br>Google Fonts, Übermittlung IP-Adresse in die USA | **100 €** |
| **LG Köln, LG München**<br>Scalable Capital, Hackerangriff bei Dienstleister | **1.200 € bis 2.500 €** |
| **Außergerichtlicher Vergleich**<br>Mastercard, Datendiebstahl | **300 €** |
| **ArbG Oldenburg**<br>Verspätete Auskunft | **10.000 €** |

# Kläger gesucht



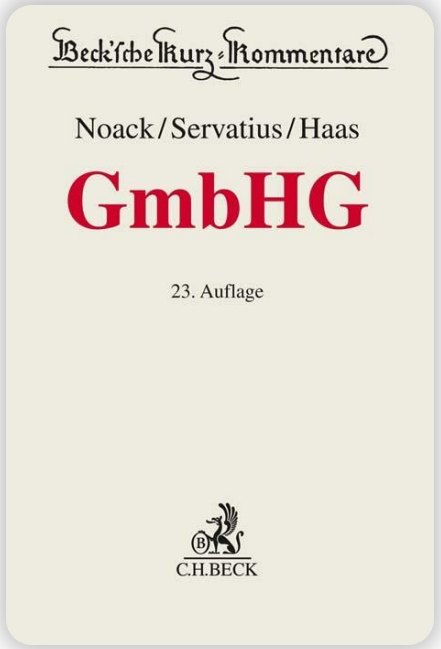



# (Persönliche) Haftung

04

# Initiativen des Gesetzgebers








# NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG-E

§ 38

**Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleiter besonders wichtiger Einrichtungen und wichtiger Einrichtungen**

1. Geschäftsleiter [ … ] sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden Risikomanagementmaßnahmen im Bereich der Cybersicherheit umzusetzen und ihre Umsetzung zu überwachen.

2. Geschäftsleitungen, die ihre Pflichten nach Absatz 1 verletzen, haften ihrer Einrichtung für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts. [ … ]

3. Die Geschäftsleiter [ … ] müssen und deren Mitarbeiter müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagement-praktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.

# NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG-E

§ 38

**Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleiter besonders wichtiger Einrichtungen und wichtiger Einrichtungen**

1. **Geschäftsleiter [ … ] sind verpflichtet**, die von diesen Einrichtungen nach § 30 zu ergreifenden Risikomanagementmaßnahmen im Bereich der Cybersicherheit umzusetzen und ihre Umsetzung zu überwachen.

2. Geschäftsleitungen, die ihre Pflichten nach Absatz 1 verletzen, haften ihrer Einrichtung für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts. [ … ]

3. Die Geschäftsleiter [ … ] müssen und deren Mitarbeiter müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagement-praktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.

# NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG-E

§ 38

**Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleiter besonders wichtiger Einrichtungen und wichtiger Einrichtungen**

1. Geschäftsleiter [ … ] sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden Risikomanagementmaßnahmen im Bereich der Cybersicherheit umzusetzen und ihre Umsetzung zu überwachen.

2. **Geschäftsleitungen**, die ihre Pflichten nach Absatz 1 verletzen, **haften ihrer Einrichtung** für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts. [ … ]

3. Die Geschäftsleiter [ … ] müssen und deren Mitarbeiter müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagement-praktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.

# NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG-E

§ 38

**Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleiter besonders wichtiger Einrichtungen und wichtiger Einrichtungen**

1. Geschäftsleiter [ … ] sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden Risikomanagementmaßnahmen im Bereich der Cybersicherheit umzusetzen und ihre Umsetzung zu überwachen.
2. Geschäftsleitungen, die ihre Pflichten nach Absatz 1 verletzen, haften ihrer Einrichtung für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts. [ … ]
3. Die **Geschäftsleiter** [ … ] müssen und deren Mitarbeiter **müssen regelmäßig an Schulungen teilnehmen**, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagement-praktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.

# Lösegeld

05

# 90 Prozent der Unternehmen zahlen bei Cyberangriffen Lösegeld

14.02.2024 · Quelle: Pressemitteilung · 3 min Lesedauer ·

90 Prozent der Unternehmen haben in den letzten zwei Jahren Lösegeld gezahlt, um nach Cyberangriffen ihre Daten schnell wieder zu erhalten, Leaks zu schließen und den operativen Betrieb aufrecht zu erhalten. Das zeigt eine Studie von Censuswide im Auftrag von Cohesity.

# Ransomware: 1,1 Mrd. Euro Lösegeld an Hacker weltweit

5. April 2024 08:19

# Sind Lösegeldzahlungen legal?

# Strafvorschriften

§ 129 i.V.m. § 129b StGB
**Bildung krimineller Vereinigungen**

1. Mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe wird bestraft, wer eine Vereinigung gründet oder sich an einer Vereinigung als Mitglied beteiligt, deren Zweck oder Tätigkeit auf die Begehung von Straftaten gerichtet ist, die im Höchstmaß mit Freiheitsstrafe von mindestens zwei Jahren bedroht sind. Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer eine solche Vereinigung unterstützt oder für sie um Mitglieder oder Unterstützer wirbt.

§ 18 AWG i.V.m. EU-Embargolisten
**Zuwiderhandlung gegen Bereitstellungsverbote**

§ 89c StGB
**Terrorismusfinanzierung**

§ 261 StGB
**Geldwäsche**

§ 266 StGB
**Untreue**

# Strafvorschriften

§ 129 i.V.m. § 129b StGB
**Bildung krimineller Vereinigungen**

1. Mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe wird bestraft, wer eine Vereinigung gründet oder sich an einer Vereinigung als Mitglied beteiligt, deren Zweck oder Tätigkeit auf die Begehung von Straftaten gerichtet ist, die im Höchstmaß mit Freiheitsstrafe von mindestens zwei Jahren bedroht sind. **Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer eine solche Vereinigung unterstützt** oder für sie um Mitglieder oder Unterstützer wirbt.

§ 18 AWG i.V.m. EU-Embargolisten
**Zuwiderhandlung gegen Bereitstellungsverbote**

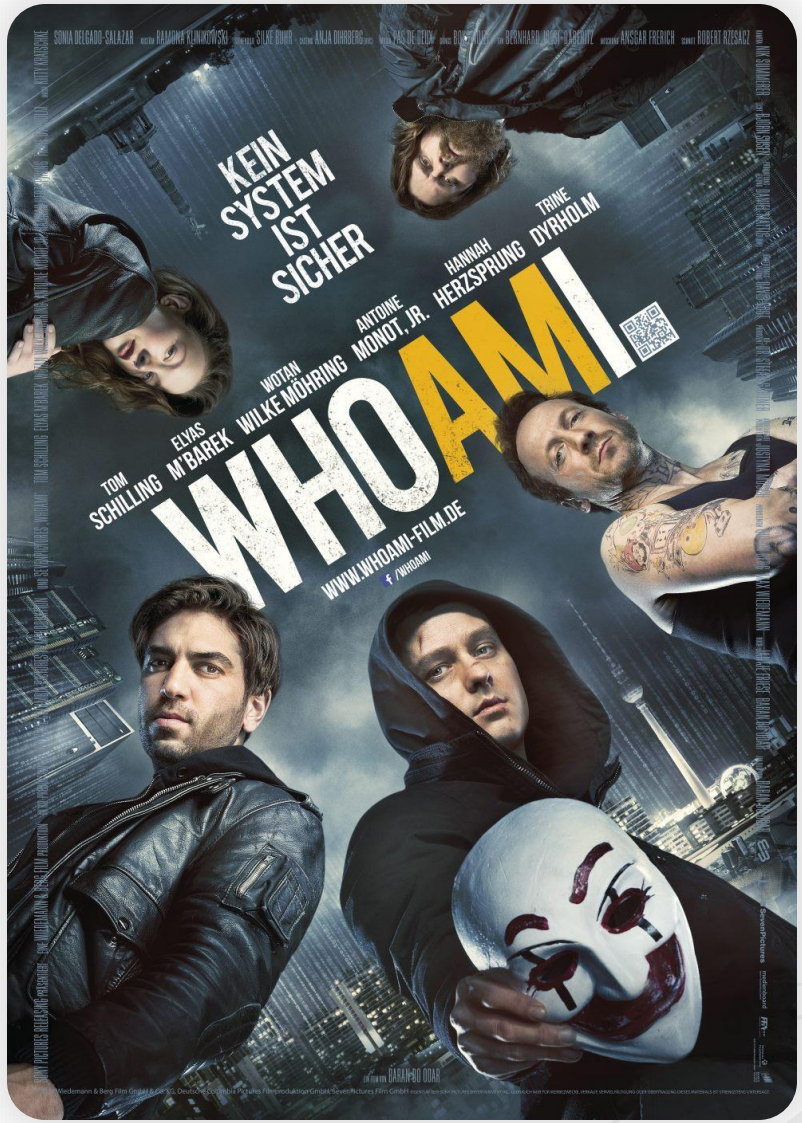
§ 89c StGB
**Terrorismusfinanzierung**

§ 261 StGB
**Geldwäsche**

§ 266 StGB
**Untreue**

# Filmtipps

06




Deutschlandfunk

## Zero Day in Südwestfalen (1/5) - Hackeralarm bei Nacht

Hintergrund · 17.06.2024 · 19 Min.

Abspielen + Merken


# Bei Fragen – oder einem Notfall – einfach anrufen:

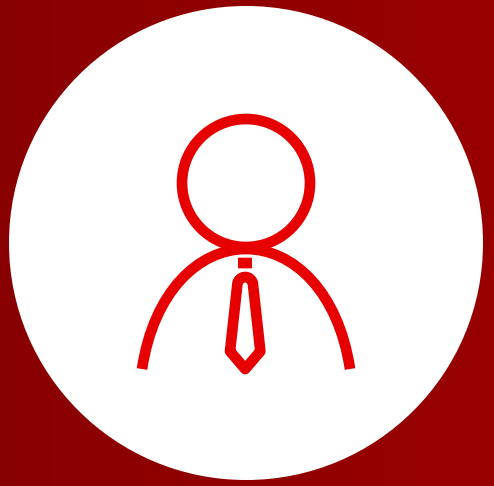

+49 (173) 674 04 73

**hansen@fps-law.de**

www.fps-law.de

# IHRE FRAGEN.

# Vielen Dank für Ihre Teilnahme!



Bei Fragen
melden Sie sich gern
bei Ihrem:r Vodafone-
Ansprechpartner:in.

Sie sind neu bei uns?
Schreiben Sie uns an
online.sessions@vodafone.com
eine E-Mail.

Die Aufzeichnungen und
Unterlagen aller Sessions
finden Sie hier.

# TIMETABLE 2024

## Educational Month Cyber Security

VODAFONE BUSINESS EDUCATION

**KW 38**

**19.09.** | 10:00 IT-Sicherheit ist Chefsache: Schützen Sie Ihre Unternehmenswerte und minimieren Sie die (persönliche) Haftung
Dr. Hauke Hansen (FPS Law)

**20.09.** | 10:00 KI-gesteuerte Security: Ende-zu-Ende-Sicherheit mit Microsoft
Andreas Wach (Microsoft)
Thomas Schmidt (PCG)

**KW 39**

**24.09.** | 10:00 Human Firewall – aus Sicht eines White-Hat-Hackers
Immanuel Bär (Prosec Networks)

**25.09.** | 10:00 Live Hacking: Die Methoden der Hacker und wie Sie sich gegen Ransomware Attacken schützen können
Lukas Garlik (Accenture)
Emil Stahr (Accenture)

**26.09.** | 10:00 Cyber Security im Zeitalter der KI: Strategien und Best Practices
Fabian Flanhardt (PCG)
Thomas Schmidt (PCG)

**KW 40**

**30.09.** | 10:00 Kampf der Ransomware! Wie Sie sich mit Zero Trust richtig schützen
Thanh Trieu (Zscaler)

Together we can

vodafone business