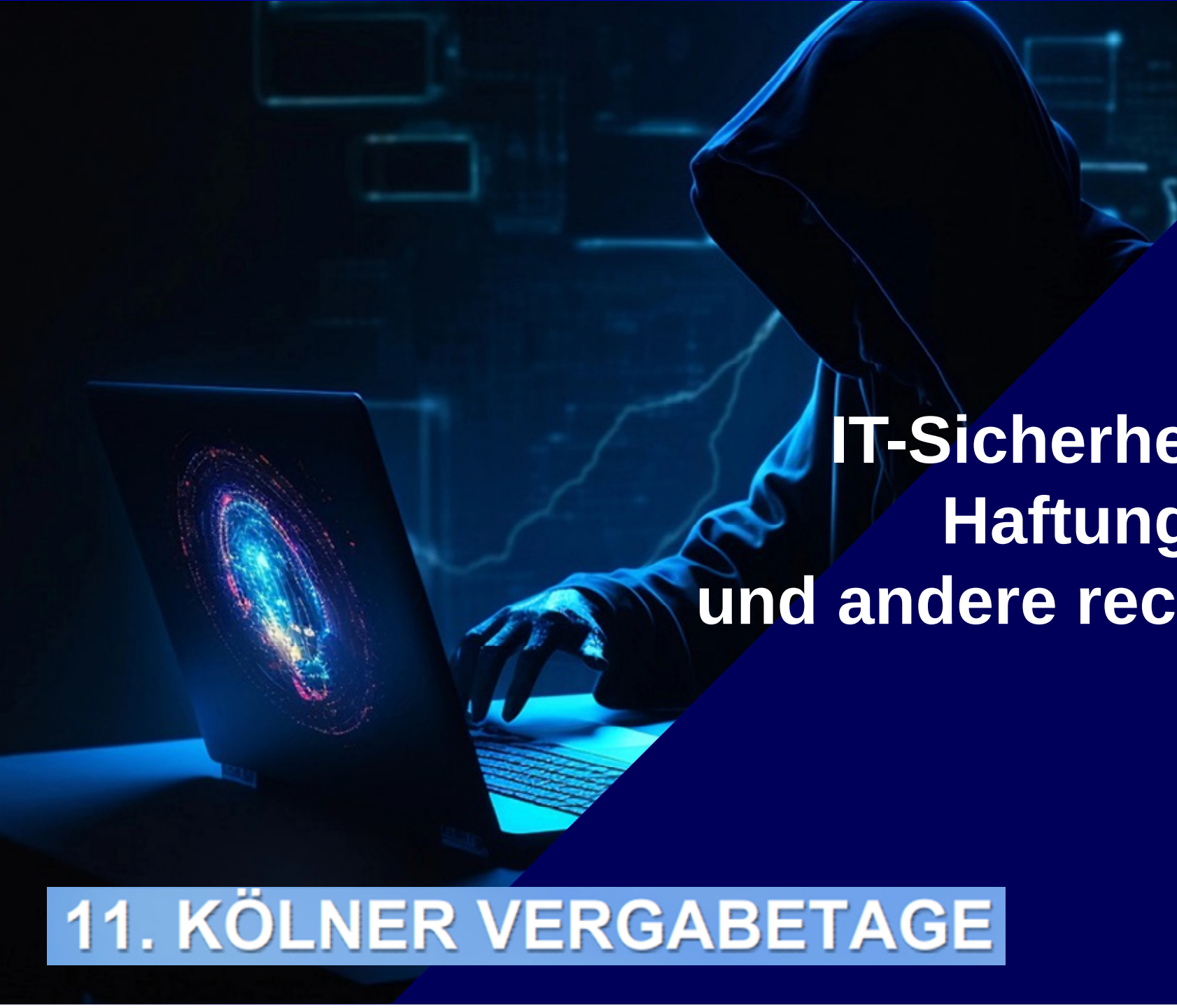


FPS

IT-Sicherheit ist Chefsache – Haftung, Schadensersatz und andere rechtliche Fallstricke

19. September 2023

Dr. Hauke Hansen
Fachanwalt für IT-Recht
Zert. Datenschutzbeauftragter (TÜV®)

11. KÖLNER VERGABETAGE

Oder: Warum Sie im Fall eines Cyberangriffs einen Anwalt brauchen


YOU
ARE
FUCKED

Geldbußen

1

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.

72

FPS

Meldung einer Verletzung des Schutzes personenbezogener Daten (Art. 33 DS-GVO)

Hinweise:

- Dieses Formular dient verantwortlichen Stellen zur Selbstanzeige gemäß Art. 33 DS-GVO. Für Beschwerden nutzen Sie bitte das hierfür bereitgestellte Formular:

  https://www.ldi.nrw.de/kontakt/ihre-beschwerde

- Weitere Informationen zu den Pflichten nach Art. 33, 34 DS-GVO finden sie hier:

  https://www.ldi.nrw.de/kontakt/meldeformular-fuer-datenpannen

1. Art der Meldung (Art. 33 Abs. 4)

- ○ Neumeldung
- ○ Ergänzende Meldung
- ☐ Es stehen derzeit nicht alle Informationen zur Verfügung, eine ergänzende Meldung erfolgt voraussichtlich bis zum:

2. Verantwortlicher (Art. 4 Nr. 7)

Name	
Straße	
PLZ	00000 ... Ort
Telefon	
E-Mail	
Art der Stelle	keine Angabe
Bereich	keine Angabe

3. Meldende Person

Beziehung zum Verantwortlichen	
Name	
Straße	
PLZ	00000 ... Ort
Telefon	
E-Mail	

4. Anlaufstelle für weitere Informationen (Art. 33 Abs. 3 lit. b)

- ○ Meldende Person
- ○ Datenschutzbeauftragter
- ○ Andere Person

5. Weitere an der Verletzung des Schutzes personenbezogener Daten Beteiligte

An der Verletzung des Schutzes personenbezogener Daten sind Dritte (z.B. Auftragsverarbeiter (Art. 4 Nr. 8), gemeinsam Verantwortlicher (Art. 26 Abs. 1)) beteiligt. ○ ja ○ nein

6. Bekanntwerden der Verletzung des Schutzes personenbezogener Daten

Zeitpunkt/-raum der Verletzung des Schutzes personenbezogener Daten:
○ am
○ von bis

Zeitpunkt des Bekanntwerdens der Verletzung des Schutzes personenbezogener Daten: TT.MM.JJJJ -- : --

Begründung der Verzögerung, falls Meldung nicht binnen 72 Stunden erfolgt (Art. 33 Abs. 1)

Wie wurde die Verletzung des Schutzes personenbezogener Daten bekannt?

1 Xpro Woche!
mit d. Datensch. [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
Bitte bei Antwort angeben [redacted]

zuständig
Durchwahl 14 08 - [redacted]

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, den 14. Juni 2022 und vom Mittwoch, den 15. Juni 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, den 14. Juni 2022 und vom Mittwoch, den 15. Juni 2022. 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 von count&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 vom 18.07.2022 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 Vorfall am 12. Juni 2022 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 Telefonnummer 0611-1408 122 oder Herr 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 Eintrittswahrscheinlichkeit 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

2


Frankfurter Allgemeine
VERGLEICHSANGEBOT AN KLÄGER
Mastercard will Kunden nach Datenleck bis zu 300 Euro zahlen


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.


Facebook Datenleck – LG Stuttgart spricht Schadenersatz zu
09.02.2023 • 2 Minuten Lesezeit • (5)

Schadensersatz und Anlässe vor dem EuGH-Urteil

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

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?

Kläger gesucht

RIESIGES FACEBOOK-DATENLECK

Sind Sie betroffen? Nutzen Sie Ihre Chance auf 1.000€ Schadensersatz – So hilft Ihnen WBS!

Christian Solmecke
14. April 2021

Dr. Stoll & Sauer
Rechtsanwaltsgesellschaft mbH

RECHTSGEBIETE ABGASSKANDAL FAC

Kanzlei für IT-Recht

DATENLECK BEI MASTER-CARD: KREDITKARTENUN-TERNEHMEN ZU VERGLEICH BEREIT

RightNow

VERKAUFE DEIN PROBLEM.

Schadensersatz bei Deezer-Datenpanne!

EuGD Europäische Gesellschaft für Datenschutz mbH

Urteile zum Scalable Capital Datenleck 2020: 1.200 - 2.500 EUR Schadenersatz!

Wir kämpfen für Ihre Rechte!
Schadenersatz geltend machen.

Strafantrag

3

Bundeskriminalamt

BKA

Unsere Aufgaben ▾ Ihre Sicherheit ▾ Aktuelle Informationen ▾ Kontakt aufnehmen ▾ Karriere ▾ Das BKA ▾

Startseite → Presse → Pressemitteilungen des BKA → 2023 → Gefährliches Schadsoftware-Netzwerk Qakbot zerschlagen

Gefährliches Schadsoftware-Netzwerk Qakbot zerschlagen

Eine Pressemitteilung des Bundeskriminalamtes und der Generalstaatsanwaltschaft Frankfurt am Main -ZIT-

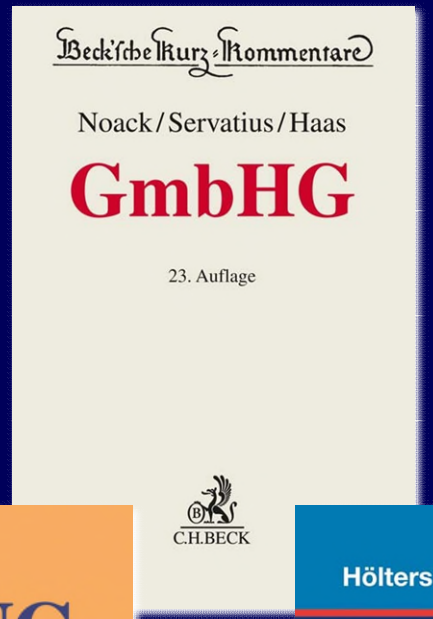
Datum: **30. August 2023** Ausgabejahr: **2023**

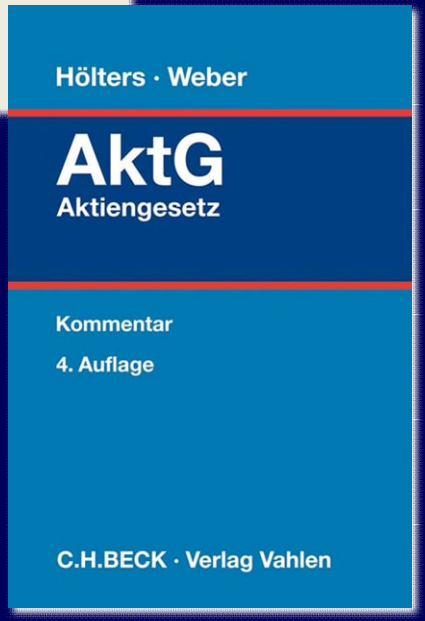
Das Bundeskriminalamt (BKA) und die Generalstaatsanwaltschaft Frankfurt am Main – Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) – haben am 26.08.2023 in einer international konzertierten Aktion unter Leitung der US-amerikanischen Behörden die in Deutschland befindliche Serverinfrastruktur der Schadsoftware Qakbot, auch als Qbot oder Pinkslipbot bekannt, übernommen und zerschlagen.

Persönliche Haftung

4

Initiativen des Gesetzgebers





Filmtipps

5


KEIN SYSTEM IST SICHER
WHOAMI


mdr
YOU ARE FUCKED
AB 6. JULI
IN DER ARD-AUDIOTHEK UND
ÜBERALL, WO ES PODCASTS GIBT


H
Crime

Bei Fragen einfach anrufen:

0173-6740473

FPS Frankfurt am Main
Eschersheimer Landstraße 25-27
60322 Frankfurt am Main

069-95957-0
www.fps-law.de
hansen@fps-law.de

Vielen Dank!

FPS im Überblick

4

Standorte

>300

Kolleginnen und Kollegen

>175

Jahre
Kanzleierfahrung

14

Kompetenzfelder

>130

Anwältinnen
und Anwälte

>50

Davon Partnerinnen
und Partner

Erfolg hat viele Gesichter. Unsere Auszeichnungen:

Renommierte Mandate, langjährige Erfahrung und ein exzellenter Ruf innerhalb der Branche: Was uns als Partner im Bereich TechLaw qualifiziert, wird auch regelmäßig von der nationalen und internationalen Fachpresse gewürdigt:

JUVE www.juve.de

Empfohlen im Bereich
Informationstechnologie

FPS PARTNERSCHAFT VON RECHTSANWÄLTEN MBB 2022
Best Lawyers RECOGNIZED BY
Handelsblatt

Empfohlen im Bereich
Datenschutzrecht & IT-Recht

FOCUS SPEZIAL

Empfohlen im Bereich
IT & Telekommunikation und Datenschutz

The LEGAL 500

Empfohlen im Bereich
IT & Digitalisierung

brand eins

Empfohlen im Bereich
IT & Kommunikation

Wirtschafts Woche

Ausgezeichnet als Top Kanzlei in den
Bereichen Datenschutz- und IT-Recht

Dr. Hauke Hansen

Rechtsanwalt | Partner

Fachanwalt für IT-Recht | Zert. Datenschutzbeauftragter (TÜV®)

Hauke Hansen ist Experte für Cybersicherheit, IT-Recht und Datenschutz. Er entwirft Cyber-Security-Strategien, um Unternehmer und Unternehmen zu schützen. Im Falle eines Angriffs koordiniert er die erforderlichen Sofortmaßnahmen, nutzt seine jahrelangen Kontakte zu IT-Security-Forensikern, Krisenkommunikations-agenturen, Ermittlungsbehörden und Versicherungen. Und er unterstützt seine Mandanten bei bei der Abwehr von Schadensersatzansprüchen und behördlichen Bußgeldern. Auf der Cybercrime Conference (C³) 2022 war Herr Hansen auf Einladung des Bundeskriminalamtes Gastredner.

Auszeichnungen

WirtschaftsWoche
In der WirtschaftsWoche 2020, 2021, 2022 und 2023 als TOP Anwalt im Rechtsgebiet Datenschutz ausgezeichnet.

Handelsblatt / Best Lawyers®
Seit 2021in The Best Lawyers™ im Bereich „Data Security and Privacy Law“ und „Information Technology“ gelistet.

Juve Handbuch 2023
Im Bereich IT und Datenschutz („sehr engagiert“, Wettbewerber) empfohlen.

Legal 500
Seit 2023 im Bereich Informationstechnologie und Digitalisierung empfohlen.

+49 69 95 957-237

hansen@fps-law.de

Auch bei in