Rechtliche Folgen eines Cyberangriffs

1. Forum Wirtschaftsschutz SH 2023

30. August 2023, IHK Kiel

Dr. Oliver Daum
RECHTSANWALT

Gliederung

1. Einführung
2. Pflichten
3. Ansprüche
4. Haftungsfragen
5. Fazit

zur Person

Rechtsanwalt

Ausbildung in Kiel, Paris & Trier

eigene Kanzlei in Kiel

Fachanwalt für IT-Recht

zertifizierter Datenschutzbeauftragter (IHK Kiel)

Einführung

1. Was ist ein Cyberangriff?
2. Daten und Fakten

Einführung

Daten und Fakten

tagesschau Sendung verpasst?

BKA-Lagebild für 2022

136.865 Fälle von Cybercrime

Stand: 16.08.2023 17:08 Uhr

Was die BKA-Statistik erfasst, ist nur "die Spitze des Eisbergs" - doch auch die ist schon beachtlich: 136.865 Fälle von Cyberkriminalität registrierte das BKA 2022. Gerade Erpressung mit Ransomware könne "existenzbedrohend" sein.

Finanzielle Schäden "häufig existenzbedrohend"

"Deshalb kann von einer Entwarnung im Bereich Cybercrime keine Rede sein", so BKA-Vizechefin Link. Die finanziellen Schäden seien "enorm" und "häufig existenzbedrohend". Der deutsche Digitalwirtschaftsverband Bitkom hat dazu eine Studie erstellt und beziffert die Schäden im vergangenen Jahr auf 203 Milliarden Euro - rund doppelt so viel wie 2019.

Einführung

1. Was ist ein Cyberangriff?
2. Daten und Fakten
3. **Realbeispiel:** Pilz GmbH & Co. KG

Pflichten

Unternehmen

- **Welche Unternehmen sind betroffen?**
  - "Kritis"
  - Anbieter digitaler Dienste, TK-Anbieter
  - DSGVO
- **Bereichsausnahmen**
  - Kleinstunternehmen (max. 10 MA, 2 Mio. €)
  - Kleine Unternehmen (max. 50 MA, 10. Mio €)

Pflichten

Meldepflichten

Mitwirkungspflichten

Informationspflichten

- **Cyberangriff/Hackerangriff**
  - Störung, Sicherheitsvorfall, Verletzung personenbezogener Daten
- **Meldung**
  - unverzüglich, binnen 72 Stunden
  - Angaben zu Ursache, Ausmaß, Folgen etc.
  - BSI, LDB, BNetzA
- **Mitwirkungspflichten**
- **DSGVO-Informationspflichten**

Ansprüche

des Unternehmens

- Angreifer
- Hersteller Software
- Mitarbeiter
- Geschäftsleitung

Ansprüche

gegen die Geschäftsleitung

- **Pflicht IT-Sicherheit**
  - Vorstände, Geschäftsführer
  - allgemeine Pflicht zur Vorsorge des Unternehmens (Risikovorsorge)
- **Pflichtenkatalog**
  - Errichtung einer IT-Sicherheit
  - Überwachung der IT-Sicherheit
  - Schulungen der Mitarbeiter
  - ggf. Benennung DSB oder IT-SiBe
- **Ressortzuweisung**

Ansprüche

gegen die Geschäftsleitung (2)

- **OLG Zweibrücken, Urteil v. 18.8.2022, Az: 4 U 198/21**
  - Zahlungen aufgrund von Phishing-Mails
  - kein Verstoß gegen organspezifische Pflicht des Geschäftsführers
  - konkludenter Gesellschafterbeschluss

Haftung

des Unternehmens

- **bei**
  - Verstoß gegen IT-Sicherheitspflichten
  - Verletzung der DSGVO
  - Verstoß gegen Meldepflicht bei Cyberangriff
- **durch**
  - Lieferanten, Kunden
  - Behörden
  - Mitbewerbern (UWG)

Maßnahmen

Abwehr

- **effektive IT-Sicherheit**
  - IT-Sicherheitspersonal und -komponenten
  - Überwachung und Aktualisierung des IT-Systems
  - Sensibilisierung der Mitarbeiter
- **"*best practises*" der präventiven Schadensminimierung**
  - Notfallteam
  - Notfallplan
  - schnelle Widerherstellung der Daten

Fazit

rechtliche Folgen
eines Cyberangriff

- Identifizierung des Angreifers
- Beweissicherung
- Meldepflichten gegenüber Behörden
- Kommunikation (PR)
- Mitwirkung gegenüber und Kooperation mit Behörden
- Strafanzeige
- Prüfung Ansprüche des Unternehmens
- Abwehr von Haftung

Kontakt

www.anwalt-daum.de

info@anwalt-daum.de

Twitter: @RA_Daum

LinkedIn: @Dr. Oliver Daum

Telefon: 0431 – 94 0 99

www.e-sportanwalt.de

Vielen Dank für die Aufmerksam keit !

Rechtliche Folgen eines Cyberangriffs