TaylorWessing

Gaps in Cyber Security? Unternehmensrisiko mit hohem Bußgeldrahmen

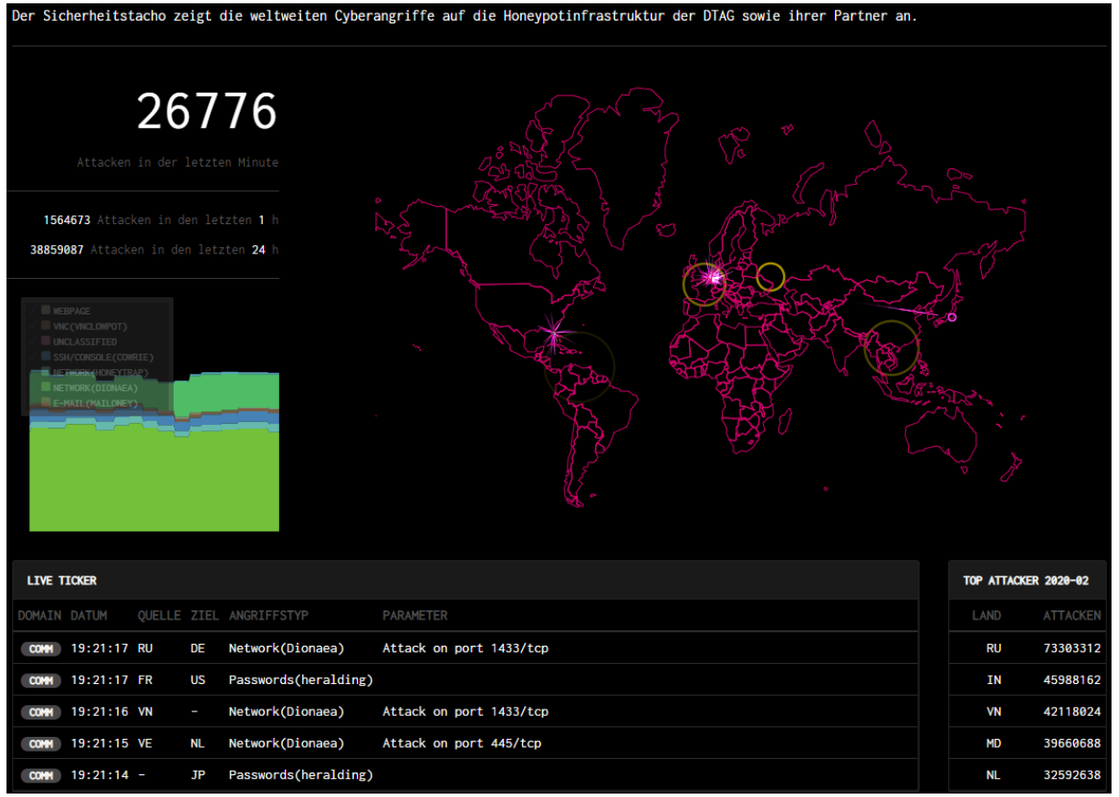
17. Internationaler Insurance Day

5.11.2020 | Detlef Klett, Rechtsanwalt und Fachanwalt für IT-Recht
Mareike Gehrmann, Rechtsanwältin und Fachanwältin für IT-Recht

Ist Ihr Unternehmen bereits mit einem Hacker-Angriff konfrontiert gewesen?

Aktuelle Gefährdungslage für Unternehmen

- Beispiel: Sicherheitstacho der DTAG
- Zeigt die weltweiten Cyberangriffe auf die „Honeypot“-Infrastruktur der DTAG an.
- Ca. 25.000 (+) Angriffe pro Minute allein auf „Honeypot“-Infrastruktur der DTAG.



Quelle: https://sicherheitstacho.eu/start/main

Gefährdungslage für Unternehmen

Unternehmen sind ständiges Ziel von Hackerangriffen.

- 30 Prozent aller Unternehmen geben an, Opfer eines Cyberangriffs geworden zu sein.*

BSI warnt vor erhöhter Gefährdungslage durch die Corona-Pandemie

- Viele Unternehmen hatten keine Strategie für Homeoffice
- Häufig unzureichende technische Sicherheitsmaßnahmen
- Zeitdruck

Ein Hackerangriff kann ein Unternehmen nicht nur erheblich schädigen, sondern auch Schadensersatzanforderungen und Bußgelder nach sich ziehen.

Was bedeutet das für Versicherungen?

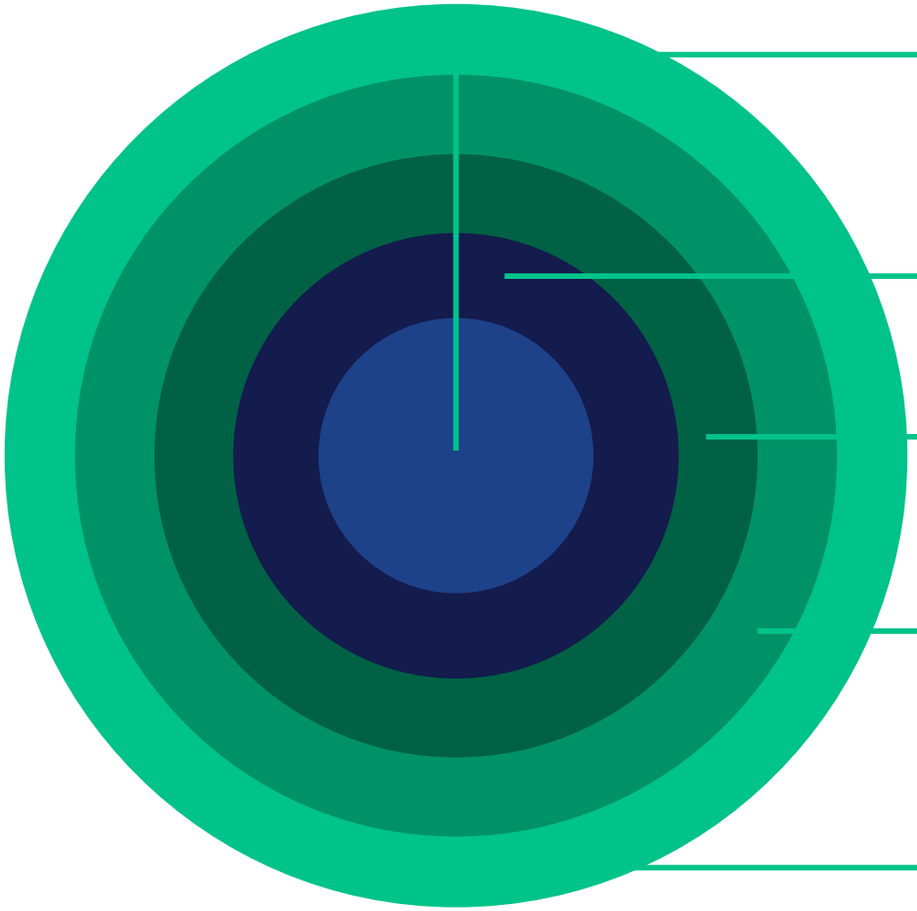
- Schutz des eigenen Unternehmens
- Auswirkungen Cyber Security-Versicherungen

*Quelle: https://www.tagesschau.de/wirtschaft/hackerangriffe-wirtschaft-unternehmen-corona-101.html

Rechtslage

IT-Sicherheitsstandards (ISO 27001, BSI Grundschutz etc.)

Für Unternehmen ergibt sich aus einer Vielzahl von Rechtsnormen - neben den allgemeinen zivilrechtlichen Vorgaben – die Pflicht, hinreichende Schutzmaßnahmen zu implementieren und Cyber-Vorfälle zu melden.



Rechtslage

Normen, die Unternehmen verpflichten, angemessene IT-Sicherheitsmaßnahmen zu ergreifen, u.a.:

Art. 25, 32 DSGVO

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.

§ 8a BSIG

Es sind angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind.

§ 13 Abs. 4, 7 TMG

Telemedien-Diensteanbieter haben bestimmte technische und organisatorische Vorkehrungen zu treffen.

§ 109 Ab. 2 TKG

Betreiber eines öffentlichen Telekommunikationsnetzes oder Anbieter öffentlich zugänglicher Telekommunikationsdienste haben bestimmte angemessene technische Vorkehrungen und sonstige Maßnahmen zu treffen.

§ 11 Abs. 1a) und 1b) EnwG

Auch Betreiber von Energieversorgungsnetzen und Betreiber von Energieversorgungsnetzen, die als KRITIS eingestuft und an ein Energieversorgungsnetz angeschlossen sind, haben angemessene Schutzmaßnahmen zu implementieren.

§ 7c Abs. 2 AtG

Auch Genehmigungsinhaber nach dem Atomgesetz haben Schutzmaßnahmen zu ergreifen.

Rechtslage

Im Falle eines Cyber-Vorfalls kann das Unternehmen verschiedene Meldepflichten haben, u.a.:

Art. 33 DSGVO

Meldepflicht bei der zuständigen Datenschutzbehörde

Art. 34 DSGVO

Benachrichtigung des Betroffenen

§ 8b BSIG

Meldepflicht gegenüber dem BSI
(ähnlich: § 109 TKG – Meldung ggü. BNetzA)

Art. 28 DSGVO

Meldepflicht gegenüber dem Auftraggeber

Bußgelder

Seit Wirksamwerden der DSGVO wurden gerade wegen IT-Sicherheitsvorfällen Bußgelder verhangen:

Fall 1: Marriott Inc.

Im Fall der Marriott Inc. hatten Hacker von 2016 bis 2018 Zugriff auf die personenbezogenen Daten von mehr als 339 Mio. Kunden. Dazu gehörten auch Zahlungsinformationen. Das Bußgeld belief sich auf über 110 Mio. EUR. Marriott hat den Angriff über Jahre nicht bemerkt und hatte keine hinreichenden Schutzmaßnahmen zur Verhinderung ergriffen.

Fall 2: British Airways

Hacker leiteten 2018 den Besucherverkehr der Webseite von British Airways auf eine betrügerische Webseite um. Die personenbezogenen Daten von 550 Mio. Kunden konnten abgeschöpft werden. Zunächst wurde ein Bußgeld in Höhe von 180 Mio. EUR verhangen, welches im Nachhinein auf 20 Mio. EUR herabgesenkt wurde. British Airways hatte keine hinreichenden technischen Schutzmaßnahmen ergriffen, um Hackerangriffen vorzubeugen.

Bußgelder

Fall 3: Morele.net

Die polnische Datenschutzbehörde verhing im September 2019 ein Bußgeld gegen Morele.net in Höhe von 645.000 EUR, da die personenbezogenen Daten von 2,2 Mio. Personen durch einen Hackerangriff abgeschöpft wurden. Das Unternehmen hatte keine hinreichenden Schutzmaßnahmen implementiert.

Fall 4: DSK Bank Bulgarien

Durch eine Hackerattacke konnten die Kundendaten von 33.000 Kunden, die die DSK Bank gespeichert hatte, abgeschöpft werden. Zu diesen Daten gehörten auch Ausweis- und Kreditkartennummern, Ausweiskopien und biometrische Daten. Die bulgarische Datenschutzbehörde verhing ein Bußgeld in Höhe von 511.000 EUR.

→ Solche Bußgelder sind auch in Deutschland zu erwarten, wenn unzureichende IT-Schutzmaßnehmen zu Datenschutzverletzungen führen sollten. Es gibt bereits erste Verfahren im Hinblick auf unzureichende technische und organisatorische Maßnahmen.

IT-Sicherheitsgesetz 2.0

- IT-Sicherheitsgesetz 1.0 seit 2015 in Kraft
- IT-Sicherheitsgesetz 2.0 sollte 2019 verabschiedet werden
- Stand: Referentenentwurf (Mai 2020)
- Wesentlichste Änderung:
  - Sprunghafte Erhöhung des Bußgeldkatalogs, bislang: 100.000 EUR
  - Nun: Bis zu 20 Mio. EUR oder 4 Prozent des gesamten, weltweiten Vorjahresumsatzes der Unternehmensgruppe
  - Zugleich: Erweiterung des Bußgeldkatalogs
- Zudem: Erweiterung des Adressatenkreises des BSIG
  - Neuer Sektor „Entsorgungswirtschaft“
  - „Unternehmen im besonderen öffentlichen Interesse“:

    Rüstungshersteller, Hersteller von IT-Produkten für die Verarbeitung staatlicher Verschlusssachen und Unternehmen, die einer Regulierung durch die Verordnung zum Schutz vor Gefahrstoffen unterliegen

Detlef Klett
Partner, Düsseldorf

+49 211 8387-170
d.klett@taylorwessing.com

Beratungsschwerpunkte

- IT-Recht
- Datenschutz und Cybersecurity

Mareike Gehrmann
Salary Partnerin, Düsseldorf

+49 211 8387-162
m.gehrmann@taylorwessing.com

Beratungsschwerpunkte

- Datenschutz und Cybersecurity
- IT-Recht

Europe > Middle East > Asia

taylorwessing.com