ESCHE
SCHÜMANN
COMMICHAU

Datenschutz

Cyberkriminalität

Cyberkriminalität

1. Warum ist jedes Unternehmen bedroht?

- Angriffsmittel sind aufgrund bestehender Internetverbindung stets verfügbar
- Angriffsziele sind omnipräsent, z. B. über Apps auf Smartphones und Tablets
- Mehrere Angriffsziele können gleichzeitig attackiert werden
- Hohe Gewinne bei geringem Entdeckungsrisiko für die Täter
- Mangelndes Bewusstsein für Bedrohung führt zu unzureichenden technischen und organisatorischen Schutzmaßnahmen
- Schwachstellen in der Software

2. Wer sind die Täter?

- Hacker
- Cyber-Aktivisten
- Konkurrenten
- Staatliche Nachrichtendienste

3. Was ist das Schadenspotenzial?

- Vermögensschäden
- Verlust von Geschäfts- und Betriebsgeheimnissen an die Konkurrenz
- Ausfall oder Beeinträchtigung von IT-Infrastrukturen
- Erpressung mit Veröffentlichung von Daten
- Identitätsdiebstahl
- Reputationsverlust

4. Wer ist zur Sicherung der IT-Systeme verpflichtet?

- Jeder Verantwortliche sowie jeder Auftragsverarbeiter (Art. 32 DSGVO)
- Vorstand einer AG (§ 91 Abs. 2 AktG)
- Geschäftsführer einer GmbH (§ 91 Abs. 1 AktG analog)
- Kredit- und Finanzdienstleistungsinstitute (§ 25a KWG)
- Telekommunikationsdiensteanbieter (§ 109 Abs. 1 TKG)
- Vertragsparteien aufgrund von Haupt- oder Nebenleistungspflichten

5. Welche Informationspflichten gibt es i.d.R. nach einem Cyberangriff?

- Unverzügliche Information der betroffenen Person
- Unverzügliche Information der Aufsichtsbehörde

6. Welche Risiken drohen bei Nichteinhaltung gesetzlicher und vertraglicher Pflichten?

- Bußgelder gegen Unternehmen und Verantwortliche bis zu EUR 10 Mio. oder – wenn dieser Betrag höher ist – 2 % des gesamten weltweit erzielten Konzern-Jahresumsatzes des vorangegangenen Geschäftsjahres
- Vertragliche oder deliktische Schadensersatzansprüche von betroffenen Personen in unbegrenzter Höhe

7. Unsere Leistung

Wir beraten Sie zu allen rechtlichen Fragen zum Thema Cyberkriminalität – vor und nach einem Cyberangriff:

Vor einem Cyberangriff

- Individuelle Risikoanalyse
- Vorbeugende Maßnahmen
- Umsetzung der gesetzlichen und vertraglichen Pflichten durch individuelle Lösungen

Nach einem Cyberangriff

- Prüfung der Informationspflichten
- Einrichtung eines Krisenmanagements unter Einbeziehung von IT-Sachverständigen
- Etwaige Einbindung von Strafverfolgungsbehörden / ggf. Strafantragstellung
- Erfüllung von Informationspflichten gegenüber betroffenen Personen und Aufsichtsbehörden
- Unterstützung des Unternehmens bei Prüfungen durch die Aufsichtsbehörde
- Öffentlichkeitsarbeit
- Prüfung und Durchsetzung von Schadensersatzansprüchen gegen Dritte
- Prüfung und Abwehr von Schadensersatzansprüchen Dritter

Das Datenschutz-Team

Für weitere Informationen kontaktieren Sie uns gern.

Dr. Frank Bongers
Rechtsanwalt, Fachanwalt für Arbeitsrecht
Datenschutzrecht, Arbeitsrecht
f.bongers@esche.de | Tel +49 (0)40 36805-317

Dr. Christoph Cordes, LL.M. (Georgetown)
Rechtsanwalt, Fachanwalt für Gewerblichen Rechtsschutz, Partner
IP-Recht, IT- & Datenschutzrecht
c.cordes@esche.de | Tel +49 (0)40 36805-331

Lara Bos
Rechtsanwältin
IT- & Datenschutzrecht
l.bos@esche.de | Tel +49 (0)40 36805-331

Allianz für Cyber-Sicherheit

Esche Schümann Commichau ist Teilnehmer der Allianz für Cybersicherheit des Bundesamtes für Sicherheit in der Informationstechnologie.

ESCHE SCHÜMANN COMMICHAU
Rechtsanwälte Wirtschaftsprüfer Steuerberater
Partnerschaftsgesellschaft mbB

Am Sandtorkai 44 | 20457 Hamburg
Tel +49 (0)40 36805-0
Fax +49 (0)40 36805-333
esche@esche.de | www.esche.de