ESCHE
SCHÜMANN
COMMICHAU

Datenschutz

Cyberkriminalität

Cyberkriminalität

I. 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 Schadenspotential?

- 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?

- Jedes Unternehmen sowie jede andere öffentliche oder nicht öffentliche verantwortliche Stelle (§ 9 BDSG)
- 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
- Unverzügliche Information der Aufsichtsbehörde

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

- Bußgelder gegen Unternehmen und verantwortliche Personen bis zu € 300.000
- Vertragliche oder deliktische Schadensersatzansprüche von Betroffenen 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

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

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. Hermann H. Haas
Rechtsanwalt, Fachanwalt für Arbeitsrecht
Arbeitsrecht, Datenschutzrecht
h.haas@esche.de | Tel +49 (0)40 36805-285

Dr. Karsten Krupna
Rechtsanwalt
Datenschutzrecht, IT-Recht
k.krupna@esche.de | Tel +49 (0)40 36805-359

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