

UNTERNEHMER ACADEMY

Part 20: IT-Sicherheit und
rechtliche Aspekte –
So schützt Du Dein
Unternehmen



Our Team - Herzlich Willkommen



Christina Schröder

Rechtsanwältin



Andreas Messerer

Prozesse / Technik



Hakan Tok

Social Media



Dr. Georg Schröder

Rechtsanwalt



Matthias Wolf

Rechtsanwalt, CIPP/E

Unternehmer-Academy



Jeden Freitag 16:00 Uhr

Frei und ohne Verpflichtung

30 Min. Vortrag / 15 Min. Fragen

Eure Fragen! Eure Vorschläge!

Keine §§ - nicht langweilig

service@recht24-7.de

Unternehmer-Academy - Part 20

IT-Sicherheit und rechtliche Aspekte – So schützt Du Dein Unternehmen



Inhaltsverzeichnis

IT-Sicherheit und Recht

Aktuelle IT-Sicherheitsvorfälle

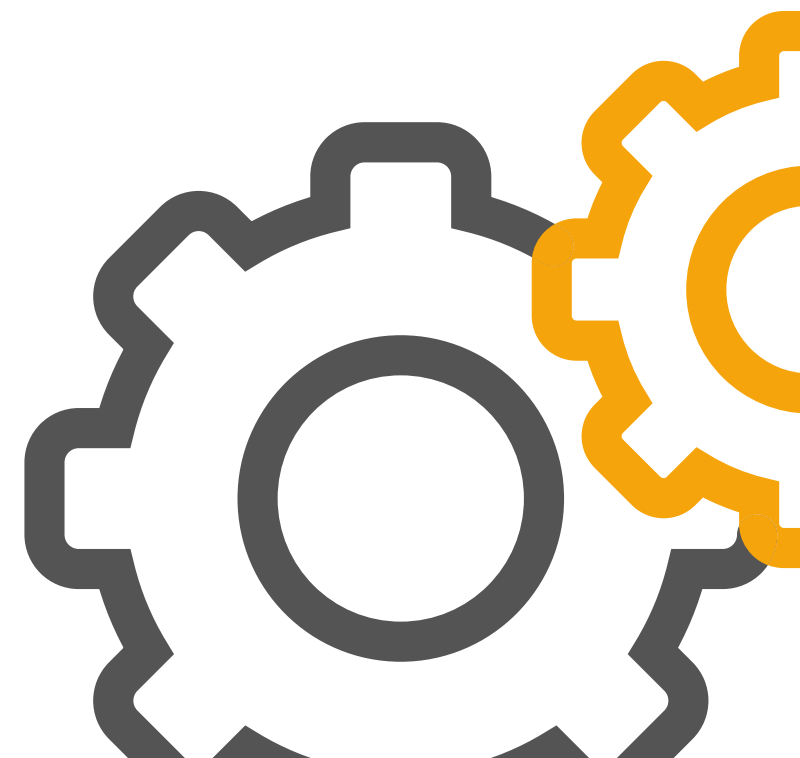
Zehn IT-Sicherheitsmaßnahmen

IT-Sicherheitsrecht

ISO 27001

Fallbeispiel: Ransomware-Angriff

Praxisfälle - TIPPS



1 Aktuelle Sicherheitsvorfälle

- ☠ Cyberangriffe auf die deutsche Wirtschaft (2024)
- ☠ 81 % der deutschen Unternehmen betroffen (Datendiebstahl, Spionage, Sabotage)
- ☠ 267 Mrd. Euro Schaden (+29 % im Vergleich zum Vorjahr) in Deutschland (!)
- ☠ Herkunft der Angriffe:
 - China: 45 %
 - Russland: 39 %

1

Aktuelle Sicherheitsvorfälle

Deepfake Betrug China/Hongkong
(Februar 2024):

Betrüger nutzten KI-Technologie, um in einer Videokonferenz den Finanzchef des Unternehmens zu imitieren. Durch diese Täuschung veranlassten sie den Angestellten, 24 Millionen Euro auf ihre Konten zu überweisen. Der Betrug wurde erst Tage nach der Überweisung entdeckt.



7

1 Aktuelle Sicherheitsvorfälle

BSI – aktueller Lagebericht:

"besorgniserregenden" Bedrohungslage
durch Cyberangriffe

Die digitale Angriffsfläche nimmt stetig
zu, Schwachstellen bieten allzu oft
gravierende Eingriffsmöglichkeiten und
Angreifer finden immer schneller und
geschickter Wege, diese auszunutzen.



2 IT-Sicherheitsrecht

Aktuelle Regelungen, u.a.:

- DSGVO
- NIS-2-Richtlinie
- IT-Sicherheitsgesetz 2.0
- KI-Verordnung
- DORA
- ...

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; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:

2 Rechtliche Folgen von IT-Sicherheitsvorfällen

Schadensersatzansprüche

- Von Kunden oder Beschäftigten
- Bei Kontrollverlust über die eigenen Daten
- Absenkung der Anforderungen durch den Bundesgerichtshof
- Niedriger Richtwert in Höhe von 100 Euro

☰ Menü

ZEIT  ONLINE

Abo testen



Urteil zu Massenverfahren

BGH zu Facebook-Fall: 100 Euro Schadenersatz nach Datenleck?

Aktualisiert am 18. November 2024, 17:01 Uhr ⓘ Quelle: dpa



ZEIT ONLINE hat diese Meldung redaktionell nicht bearbeitet. Sie wurde automatisch von der Deutschen Presse-Agentur (dpa) übernommen.

Quelle: <https://www.zeit.de/news/2024-11/18/nutzerfreundliches-bgh-urteil-nach-datenraub-bei-facebook>

2 Rechtliche Folgen von IT-Sicherheitsvorfällen

Bußgelder

- Bei Datenschutzvorfällen aufgrund mangelnder IT-Sicherheitsmaßnahmen
- Bei verspäteter Meldung von Datenschutzvorfällen
- Das Bußgeld gegen 1&1 wurde vom Landgericht Bonn auf 900.000 Euro reduziert



Quelle: www.spiegel.de/netzwelt/netzpolitik/datenschutz-grundverordnung-9-5-millionen-euro-bussgeld-gegen-1-1-a-1300415.html

3 Fallbeispiel Ransomware

- 1) Vorbereitung
- 2) Initiale Kompromittierung
- 3) Erkundung und Rechteerweiterung
- 4) Datendiebstahl
- 5) Verschlüsselung
- 6) Erpressung / Datenverkauf

4 Zehn IT-Sicherheitsmaßnahmen

- 1) IT-Sicherheit ist Sache der Geschäftsleitung
- 2) Management
- 3) Inventar der IT-Infrastruktur
- 4) Backups, Backups, Backups
- 5) Patchen, Patchen, Patchen

4

Zehn IT-Sicherheitsmaßnahmen

6) Schulungen und Sensibilisieren

7) Firewall und Virenschutz

8) Passwörter

9) Mehr-Faktor-Authentifizierung

10) Notfallplan

5 ISO 27001 Zertifizierung

Was ist ISO 27001?

- Weltweit anerkannte Norm für ein Informationssicherheits-
Managementsystem

Warum eine Zertifizierung nach ISO 27001?

- Schutz von Informationen, Daten, geistigem Eigentum
- Vertrauen von Kunden, Investoren, Banken
- Unterstützung bei der Einhaltung gesetzlicher Pflichten

5 ISO 27001 Zertifizierung

Schritte zur Zertifizierung nach ISO 27001

- Bestandsaufnahme / Gap-Analyse
- Benennung CISO
- Erklärung zur Anwendbarkeit
- Dokumentenerstellung
- Prozessentwicklung
- Implementierung technischer und organisatorischer Maßnahmen
- Durchführung Audit
- Kontinuierliche Überwachung und Verbesserung

6 Zusammenfassung

IT-Sicherheitsrecht

- NIS 2 kommt!

IT-Sicherheitsmaßnahmen

- Notfallplan

ISO 27001

- Zertifikat für das ISMS

Nächste Veranstaltung 14.02.2025

Die neue eGbR – Was steckt hinter der eingetragenen GbR und wie gelingt die Umwandlung in eine GmbH?

- Was ist die eGbR und warum ist sie die Weiterentwicklung der GbR?
- Welche Vorteile bietet die Eintragung im Gesellschaftsregister?
- Wie funktioniert die Umwandlung in eine GmbH Schritt für Schritt?
- Praktische Tipps und rechtliche Fallstricke, die Sie kennen sollten.

Für Gründer:innen, Selbstständige und Unternehmer:innen, die ihre Unternehmensstruktur zukunftssicher gestalten möchten.

Vielen Dank!



Video -> youtube Channel

Handout - www.recht24-7.de

Fragen - Anmerkungen:
service@recht24-7.de

Nächste Veranstaltung: 14.02.2025:
Die neue eGbR – Was steckt hinter der
eingetragenen GbR und wie gelingt die
Umwandlung in eine GmbH?

zur Anmeldung

<https://my.demio.com/ref/Qc5eLfmc3BASMETo>

<https://recht24-7.de/unternehmer-academy-by-recht-24-7/>