



# Home-Office

// IT-Sicherheit und Datenschutz



Vortrag von Maik Müller, CIPP/E  
Berater für Datenschutz und Informationssicherheit

Online-Event, 2021-02-25



**PSW GROUP**

**PSW CONSULTING**

**PSW TRAINING**

# Warum Home-Office?

// Kurzfristige und langfristige Ziele

- Geschäftskontinuität (Business Continuity)
- Digitalisierung
- New Work



# Warum Home-Office?

// Kurzfristige und langfristige Ziele

- Geschäftskontinuität (Business Continuity)
- Digitalisierung
- New Work
  - Flexibles Arbeiten unabhängig von Zeit und Ort
  - Neue Formen der Zusammenarbeit von Unternehmen
  - Teambasierend
  - Erweiterte Infrastruktur (Meeting-Räume)
  - Cloud-Computing



# Risiken im Home-Office

// Schutzziele C I A

1. Vertraulichkeit (Confidentiality)
2. Integrität (Integrity)
3. Verfügbarkeit (Availability)



# Risiken im Home-Office

// Gefahren für die Datensicherheit

- Arbeitgeber kann weniger die Sicherheit überwachen
- Fehlende IT-Infrastruktur
- Gefahr des Zugangs betriebsfremder Personen



# Risiken im Home-Office

// Vertraulichkeit (Confidentiality)

- Ausspähen von Informationen
- Offenlegung schützenswerter Informationen
- Unbefugtes Eindringen in IT-Systeme
- Unberechtigte Nutzung oder Administration von Geräten und Systemen
- Missbrauch von Berechtigungen
- Unbefugter Zugriff auf Personaldaten, Kundendaten
- Unbefugter Zugriff auf Geschäftsgeheimnisse

# Risiken im Home-Office

// Integrität (Integrity)

- Manipulation von Hard- oder Software
- Manipulation von Informationen
- Zerstörung von Geräten oder Datenträgern
- Fehlerhafte Nutzung oder Administration von Geräten und Systemen
- Integritätsverlust schützenswerter Informationen

# Risiken im Home-Office

// Verfügbarkeit (Availability)

- Ausfall von Geräten oder Systemen
- Unberechtigte Nutzung oder Administration von Geräten und Systemen
- Personalausfall
- Verhinderung von Diensten (Denial Of Service)
- Datenverlust



# IT-Sicherheit

// Sicherheit der Infrastruktur

## Home-Office

- Kommunikation
- Dokumentenzugriff
- Anwendungszugriff



# IT-Sicherheit

// Sicherheit der Infrastruktur

## 3 Möglichkeiten

- Remote Desktop
- VPN-Tunnel
- Cloudbasierte Lösung



# Sicherheit im Home-Office

// Anwendung sicherer technischer und organisatorischer Maßnahmen (TOM)

- Wer hat Installations- und Konfigurationsrechte? – Vorsicht Data Breach
- Zugangsregeln (Passwortmanagement, Clear-Screen)
- Berechtigungsmanagement (Datenweitergabe nach Vertraulichkeitsklassifikation)
- Datensicherung (Wer kümmert sich um Backups?)
- Externe Hardware innerhalb der IT-Infrastruktur – Vorsicht BYOD
- Datenschutz und Datensicherheit im öffentlichen Raume oder Home-Office
- Regelung der dienstlichen und privaten Nutzung – Vorsicht: Verbot privater Nutzung aber tatsächliche Duldung

# Sicherheit im Home-Office

// Beispiele für Regeln der IT-Sicherheitsrichtlinie des Arbeitgebers

- Privates Wi-Fi mit starken Passwörtern – Vorsicht: Angriff auf Heim-Router
- Festplattenverschlüsselung von Notebooks
- Updates von Anti-Virus- und anderer Software
- Schutz der IT-Infrastruktur durch gesicherte Verbindungen (VPN, Virtual Private Network)
- Vermeidung lokaler Datenspeicherung
- Zwei-Faktor-Authentifizierung (2FA) durch den Arbeitnehmer
- Keine Sprachassistenzsysteme (Apple Siri, Google Assistant, MS Cortana, Amazon Alexa)

# Datenschutz im Home-Office

1. Sicherheit der Verarbeitung personenbezogener Daten gewährleisten
2. Grundsatz der Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO)
3. Wichtig: Beschäftigte schulen



# Datenschutz im Home-Office

// Richtlinien des Arbeitgebers

- Mobiles Arbeiten / Home-Office
- IT-Sicherheit
- Bring-Your-Own-Device (BYOD) – Vorsicht: Betriebliche und private Daten trennen
- Prozess zur Meldung von Datenpannen (Datenschutzverletzungen)

# Datenschutz im Home-Office

// Vereinbarung zwischen Arbeitgeber und Beschäftigten

1. Fall  
Arbeitgeber stellt Endgeräte für die Arbeit im Home-Office
2. Fall  
Beschäftigte stellen Endgeräte zur Verfügung  
(Nutzungsvereinbarung)

# Datenschutz im Home-Office

// Risikobewertung

- Videokonferenzsystemen (Zoom, MS Team, TeamViewer)
  - Passwortschutz von Konferenzen
  - Keine Videoaufzeichnung
  - Regelungen zur Speicherdauer von Chats
- Kollaborationstools (MS Teams, Slack, Messenger)
- Grundsatz der Datenminimierung und Speicherbegrenzung
- Vertraulichkeit und Integrität der Kommunikation muss sichergestellt sein (Verschlüsselung)



# Datenschutz im Home-Office



// To-dos des Arbeitgebers

- Arbeitgeber muss das Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO) in Bezug auf die technischen und organisatorischen Maßnahmen (TOM) im Home-Office ergänzen
- Prüfung und Abschluss von Auftragsverarbeitungsverträgen (Art. 28 DSGVO)
- Hohe Hürden bei der Verarbeitung von besonders schützenswerten Daten nach Art. 9 Abs. 1 DSGVO

# Datenschutz im Home-Office



// To-dos des Arbeitgebers

- Arbeitgeber muss das Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO) in Bezug auf die technischen und organisatorischen Maßnahmen (TOM) im Home-Office ergänzen
- Prüfung und Abschluss von Auftragsverarbeitungsverträgen (Art. 28 DSGVO)
- Hohe Hürden bei der Verarbeitung von besonders schützenswerten Daten nach Art. 9 Abs. 1 DSGVO
  - „Informationen zur rassischen und ethnischen Herkunft, Gewerkschaftszugehörigkeit, zu politischen Meinungen, religiösen oder weltanschaulichen Überzeugungen sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.“

# Maik Müller, CIPP/E

Berater für Datenschutz und Informationssicherheit

Zertifizierter Datenschutzbeauftragter (TÜV)

ISO/IEC 27001 Officer (TÜV)

IT-Grundschutz-Praktiker gem. BSI (de-bit)

[www.psw-consulting.de](http://www.psw-consulting.de)



DANKE

// für Ihre Aufmerksamkeit



**PSW GROUP**

**PSW CONSULTING**

**PSW TRAINING**