Webinar
IHK Spezial

Datenschutz im Homeoffice am 6. Juli 2020
Referentin: Carolin Loy

IHK Schwaben

Arbeitsumgebung

Vertraulichkeit herstellen

- Einblicke von Familienmitgliedern oder Besuchern verhindern (auch an Fenster denken)
- Clean- Desk- Policy am Ende des Tages
- Papierunterlagen nicht offen aufbewahren
- Fenster beim Verlassen des Arbeitsplatzes schließen
- Laptop sperren, wenn der Arbeitsplatz verlassen wird
- Schutz vor Mithörern bei Telefongesprächen/ Videokonferenzen

Genutzte Hardware

Privatgeräte nur im Ausnahmefall

- Dienstliche Hardware nutzen (Notebooks, Smartphones etc.)
- Bei Privatgeräten Remoteverbindungen auf Terminalserver verwenden
- Dienstliche Geräte nicht für private Zwecke nutzen
- Regelungen zum Ausdruck

Umgang mit Papierdokumenten

Sicherheitsrisiken erkennen

- Papierunterlagen in geeigneten Mappen (mit Name des Unternehmens) mitnehmen
- Erhöhte Risikosituationen beim Transport vermeiden (zB. Offen auf dem Rücksitz beim Einkaufen)
- Papierunterlagen nur im Büro oder am heimischen Arbeitsplatz nutzen
- Entsorgung nicht über den Hausmüll, sondern im Büro oder zuhause durch einen Aktenvernichter mit mind. Sicherheitsstufe 5 nach DIN 66399
- Sensibilisierung über Schäden an wichtigen Papierdokumenten (Kopien bevorzugen)

Videokonferenzsysteme

Informieren, Prüfen und gezielt auswählen

- Vertrag zu Auftragsverarbeitung nach Art. 28 DS-GVO
- Bei Anbietern in Drittstaaten geeignete Garantien prüfen (z.B. Privacy- Shield- Zertifizierung)
- Verwendung einer Transportverschlüsselung (z.B. TLS)
- Zugangsschutz durch Passwörter und individuelle Einladungslinks
- Keine Aufzeichnung der Inhalte durch den Anbieter
- Konfigurationsmöglichkeiten bei Erhebung von Telemetriedaten (Empfehlung: Deaktivieren)
- Keine Aufzeichnung durch das Unternehmen
- Deaktivierung von biometrischen Features, wenn vorhanden
- Regelungen zum Screen Sharing (wann und durch wen)
- Regelungen zum Zweck und der Speicherdauer von Chat- Funktionen sind vorhanden
- Hintergrundeinstellungen möglich („Blurring“)
- Moderatorenfunktionen existieren (z.B. Teilnehmer entfernen)
- Beteiligung des Personal-/Betriebsrats
- Beteiligung des Datenschutzbeauftragten

Sicherheit

Sicherheitsrisiken erkennen

- Anbindung an das Firmennetz mit verschlüsselter VPN-Verbindung nach Stand der Technik
- Einsatz von Verfahren zur Zwei- Faktor- Authentifizierung neben Pin/Passwort
- Nutzung des heimischen Wi-Fi mit starken Passwörtern
- Nutzung öffentlicher Wi-Fi Hotspots nur bei durchgängiger Absicherung sämtlicher Kommunikation durch VPN- Anbindung
- Zugriff nur auf für das Homeoffice erforderliche Server, Dateiablagen und Anwendungen
- Speicherung von Daten auf über die VPN-Verbindung erreichbare Netzlaufwerke im Unternehmen
- Regelmäßiges Patch-Management/ automatische Sicherheitsupdates
- Tägliches Update Virensignaturen
- Regelungen zum Umgang mit USB-Ports
- Festplattenvollverschlüsselung bei Notebooks
- Vollverschlüsselung dienstlicher Smartphones
- Pin-Sperre bei dienstlichen Smartphones
- Regelungen für den Verlustfall
- Erreichbarkeit IT- Abteilung auch im Homeoffice

Nutzung von Cloud- Diensten

Dienste prüfen und gezielt auswählen

- Vertrag zur Auftragsverarbeitung nach Art. 28 DS-GVO
- Transportverschlüsselung (z.B. HTTPS) nach Stand der Technik
- Ruheverschlüsselung (auf Festplatten des Cloud-Anbieters)
- Wirksame Datenlöschung (z.B. bei Beendigung des Vertrags)
- Prüffähigkeit der technischen und organisatorischen Maßnahmen durch geeignete Dokumente, Zertifizierungen und zumindest der Möglichkeit, auch ein Vor-Ort-Audit durchzuführen
- Bei Anbieter in Drittstaaten sind geeignete Garantien ausgewählt worden
- Verwendung starker Passwörter für Nutzer
- Verwendung von Verfahren zur Zwei- Faktor- Authentifizierung bei administrativen Konten
- Sensibilisierung der Mitarbeiter für Risiken von Phishing- Attacken auf Cloud Konten

Nutzung von Messengern

Dienste prüfen und gezielt auswählen

- Kommunikation der Inhalte erfolgt Transport- und Ende- zu- Ende verschlüsselt
- Keine Verwendung oder Weitergabe der Verkehrsdaten an den Anbieter für Zwecke wie Profiling und Werbung
- Ende- zu Ende- Verschlüsselung auch von Anhängen wie Bildern oder Textnachrichten
- Einsatz von Mobile-Device- Management Lösung zur Steuerung von Kontakt- Uploads an Messenger- Anbieter

Allgemeine organisatorische Regelungen

Aufmerksam auf neue Sicherheitsprobleme achten

- Überblick über die Mitarbeiter im Homeoffice
- Überblick über die Geräte
- Schulungen und Informationen für Mitarbeiter
- Schriftliche Vereinbarungen/ Regelungen mit den Mitarbeitern
- Keine Weiterleitung von dienstlichen E-Mails an private E-Mail- Konten


Fragen?
Bayerisches Landesamt für Datenschutzaufsicht
Carolin Loy
carolin.loy@lda.bayern.de
Promenade 18, 91522 Ansbach
https://www.lda.bayern.de
Carolin Loy, 06. Juli 2020

Vielen Dank für Ihre Aufmerksamkeit!

Weitere Informationen unter
www.schwaben.ihk.de/ihkspezial

IHK Schwaben