COVID 19: CRISIS MANAGEMENT

IT Sicherheit & Datenschutz in Zeiten von Corona

DEKRA

Die aktuelle Krise rund um den Covid 19 führt zu einem rasanten Anstieg der Nutzung von Homeoffice in vielen Firmen. Dies hat natürlich eine Vielzahl von Vorteilen beispielsweise das Aufrechterhalten der administrativen Geschäftsprozesse, jedoch kommen dadurch ebenfalls neue Herausforderungen im Bereich der IT Sicherheit und des Datenschutzes auf die entsprechenden Organisationen und deren Mitarbeiter zu.
Im Folgenden einige Empfehlungen für Unternehmer und Mitarbeiter (Hinweis: In den nun folgenden Dokumenten wird aus Gründen der besseren Lesbarkeit ausschließlich die männliche Form verwendet. Sie bezieht sich auf Personen beider Geschlechter.)

2. IT SICHERHEIT IM HOMEOFFICE QUICK GUIDE FÜR MITTELSTÄNDLER UND DEREN MITARBEITER

Implementierte Informationssicherheitssysteme z. B. nach ISO 27001 bieten einen exzellenten Schutz

Die Grundlage betrieblicher Informationssicherheit liegt in der Implementierung, Etablierung und stetigen Verbesserung eines Informationssicherheit management system (ISMS). Dieses schreibt unter anderem Informationssicherheitsrichtlinie, regelmäßige Schulungen der Mitarbeiter zu den Themen Datenschutz und Informationssicherheit vor oder gibt Leitlinien beim Mobilen Arbeiten wie beispielsweise dem Homeoffice vor.

Letzteres ist insbesondere in der aktuellen Situation besonders notwendig. Daher im Folgenden ein Überblick.

Nutzung von VPN-Verbindungen

Um eine sichere Kommunikation im Homeoffice zu ermöglichen, sollten Arbeitnehmer sich lediglich über eine sichere VPN-Verbindung mit dem Netzwerklauf der Arbeitgeber verbinden. Das VPN ermöglicht eine verschlüsselte Kommunikation zwischen dem Sender und Empfänger und sorgt so für einen sicheren Kommunikationsablauf.

Evaluierung der Heimnetzwerke der Mitarbeiter

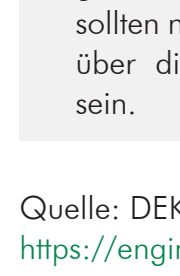
Arbeitnehmer sollten das eigene Heimnetzwerk und deren angeschlossene Geräte überprüfen.
Das schwächste Glied eines Netzwerks bestimmt deren Sicherheit. Einige Beispiele hierzu:

- Hat der PC der Kinder bereits das neueste Antivirus Update installiert?
- Ist der Router auf dem neuesten Releasestand?
- Sind Arbeits- und Privatnutzung strikt voneinander getrennt?
- Ist sichergestellt, dass für diesen Ausnahmezustand ein separates Gerät genutzt wird?

Durchführung eines Sicherheitscheck

Arbeitgeber sollten sicherstellen,
dass auch während sich eine Vielzahl der Arbeitnehmer im Homeoffice befindet:

- Softwareupdates und Patches regelmäßig eingespielt werden,
- Konfigurationen, Benutzer- und Administratorenrechte regelmäßig überprüft und gegebenenfalls angepasst werden,
- Prozessen als Reaktion auf Cyberattacken auch über Remotesteuerung greifen werden bzw. falls nicht, diese entsprechend angepasst werden.



Sensibilisierung der Mitarbeiter

Arbeitgeber sollten derzeit insbesondere die Arbeitnehmer im Homeoffice nochmals eindringlich auf die damit verbundenen Gefahren im Bereich Informationssicherheit sensibilisieren.
Hierzu gehören unter anderem:

- Zunahme von Phishing Emails durch Corona
  > Keine Öffnung von Nachrichten oder Anhängen unbekannter Absender
  > Wachsame Überprüfung von URLs und Absender-Adressen

- Zunahme von Social Engineering Attacken durch Corona
  > Besondere Vorsicht ist geboten bei:
  - Emotionalität und Dringlichkeit,
  - Angebliche Exklusivität und unbekanntem Absender,
  - Rechtschreib- und Grammatikfehlern

- Erziehung der Familie
  Der Arbeitsrechner ist lediglich zum Arbeiten da und darf nicht parallel von Kindern oder Partnern verwendet werden. Hier ist auf eine unbedingte Trennung zu achten!

- Prüfung der Arbeitsumgebung zum Schutz von Unternehmensinterna
  Arbeitnehmer sollten eine geschützte Umgebung vorfinden in dieser ungestört vertrauliche Gespräche und der Austausch sensiblen Informationen zur Erledigung der täglichen Aufgaben durchgeführt werden können. Somit wird gewährleistet, dass diese nicht nach außen dringen und unbefugten zugänglich gemacht werden.

- Soziale Netzwerke
  Arbeitnehmer sollten sich nicht über das Arbeitsgerät in soziale Netzwerke einloggen. Weiterhin sollten nur allgemein zugängliche Informationen über die Profile der Arbeitnehmer verfügbar sein.

- Schützen arbeitsrelevante Passwörter
  Arbeitnehmer sollten unbedingt darauf achten, Passwörter vor unbefugten Zugriff zu schützen und diese weder aufzuschreiben noch Familienmitgliedern mitzuteilen.

- Öffnung eines separaten Accounts bei geschäftlichen Nutzung eines privaten Gerätes
  Arbeitnehmer, welche über ein privates Gerät auf firmeninterne Software zugreifen, sollten zumindest einen separaten Account für diese Tätigkeiten erstellen.

- Meldung von Datenschutz- und IT-Sicherheitsvorfällen
  Datenschutz- und IT-Sicherheitsvorfälle sollten auch im Homeoffice direkt von den Arbeitnehmern an die entsprechenden Stellen umgehend gemeldet werden. Arbeitgeber haben Sorge zu tragen, dass die Ansprechpartner bekannt sind und ein funktionierender Prozess etabliert worden ist. Der Arbeitnehmer ist verpflichtet ausnahmslos und unverzüglich bei Verdachtsmomenten den Arbeitgeber zu informieren. Hier ist es sinnvoll eine Hotline beim Arbeitgeber einzurichten.

- Grundsätzliche Hygiene wahren
  Arbeitnehmer sollten grundsätzlich auf eine hohe Hygiene der verwendeten Arbeitsgeräte achten und diese regelmäßig reinigen.

Quelle: DEKRA internal
https://enginsight.com/de/blog/it-sicherheit-in-zeiten-von-covid-19/