Home Office und IT-Sicherheit – Was gilt es zu beachten? Welche Sofortmaßnahmen gibt es?

Die Corona-Krise hat Deutschland fest im Griff. Viele Unternehmen haben, um die Gesundheit ihrer Angestellten zu schützen und einen Beitrag zur wirksamen Bekämpfung zu leisten, ihren Mitarbeitern die Möglichkeit eröffnet, im Home Office zu arbeiten oder werden diese Maßnahme in den nächsten Tagen umsetzen. Der zeitgleiche Zugriff der Mitarbeiter auf die unternehmensinternen Systeme kann diese schnell in die Knie zwingen. Aber auch die Gefahr externer Angriffe auf IT-Sicherheitsstruktur und unternehmensinterner Daten steigt, wenn ein Großteil der Beschäftigten von außerhalb des unternehmenseigenen Netzwerks arbeiten. Um Vertraulichkeit, Integrität und Verfügbarkeit sicherzustellen, ist es essenziell bereits im Vorfeld die richtigen Weichenstellungen sowie zielgerichtete Sofortmaßnahmen zu treffen.

IT-Sicherheit und ihre effektive Umsetzung

Klare einheitliche Vorgaben sowie die entsprechenden sicherheits-strukturellen Einrichtungen und Einstellungen sind in Bezug auf die IT-Sicherheit unerlässlich.

Folgende Aspekte sollten Unternehmen unbedingt beachten:

- Gesicherter Zugang auf unternehmensinterne Systeme (z.B. durch VPN-Zugang)
- Umsetzung einer effektiven und praktikablen Zugangsverifikation (stabiler Pass- bzw. Kennwortschutz und 2-Faktor-Authentifizierung)
- Nutzung von Verschlüsselungsmöglichkeiten für Festplatten oder USB-Sticks
- Verschlüsselung der elektronischen Datenübermittlung (z.B. E-Mails)
- Vorgabe technischer und organisatorischer Maßnahmen durch den Arbeitgeber, sofern der Arbeitnehmer eigene Hard- oder Software einsetzt

Maßnahmen im Vorfeld

- Entwicklung einer IT-Sicherheitsrichtlinie
- Belastbarkeitstest der VPN-Verbindung und der Systeme bei hohen Zugriffsraten von außen
- Ggf. kurzfristige Aufstockung von IT-Kapazitäten
- Prioritäre Zugänge für Führungskräfte und wichtige Geschäftsbereiche einrichten
- Notfallkonzepte und klar definierte Verantwortlichkeiten im Krisenfall

Hilfreiche Sofortmaßnahmen für Arbeitgeber

- Kommunikation von verständlichen und verbindlichen Regelungen zur IT-Sicherheit in einer Richtlinie / Handlungsempfehlung Home Office an die Mitarbeiter
- Sensibilisierung / Schulung der Mitarbeiter betreffend Phishing sowie weiteren Cyber Crime-Risiken
- Einrichtung von VPN-Zugängen für die Mitarbeiter für den Zugriff auf unternehmensinterne Ressourcen
- Sensibilisierung / Schulung der Mitarbeiter betreffend Sicherheitsmaßnahmen am häuslichen Arbeitsplatz: Verschließen von Türen, Vernichtung von Dokumenten, Clean-Desk-Policy etc.
- Umsetzung einer 2-Faktor-Authentifizierung beim Zugriff auf unternehmensinterne Ressourcen

Weitere Ausgestaltung

Die Maßnahmen zur Regelung der Arbeit im Home Office sind unternehmensindividuell anzupassen und entsprechend erweiterbar. Unabhängig von der weiteren Entwicklung der Corona-Krise sollten die aufgeführten Empfehlungen mittelfristig stetig weiterentwickelt werden.

Bei Ihren individuellen Herausforderungen und weiteren Frage zur IT-Sicherheit stehen Ihnen unsere erfahrenen Berater gerne mit Rat und Tat zur Verfügung.

Für Fragen zum Thema Datenschutz verweisen wir auf unseren Newsletter "Home Office während der Corona-Krise – was aus datenschutzrechtlicher Sicht jetzt zu beachten ist".

Ihre Ansprechpartner

Dirk Seeburg, M.A.E.S. (Basel), LL.M.
Rechtsanwalt

Technopark II | Werner-von-Siemens-Ring 12
85630 Grasbrunn | Germany

Tel. +49 (89) 90 420 49-62
Fax +49 (89) 46 14 90-78
Mobil +49 (170) 913 76 17

dirk.seeburg@bay-gmbh.com

Tobias Baader, M.Sc.

Luitpoldpark | Uferweg 11
88131 Lindau | Germany

Tel. +49 (8382) 27 30 79-21
Fax +49 (8382) 27 30 79-30
Mobil +49 (170) 888 60 84

tobias.baader@bay-gmbh.com