Datenschutzmanagement kompakt

Datenschutz im Unternehmen – professionell und rechtssicher umsetzen und organisieren

Bearbeitet von
Eugen Ehmann

1. Auflage Onlineprodukt.
ISBN 978 3 8111 1722 8

November 2015

6/9.17 Bring your own device

Unter dem Schlagwort „Bring your own device“ oder „Bring your own PC“ wird zurzeit in Datenschutz- und IT-Security-Kreisen diskutiert, inwieweit die Mitarbeiter ihren eigenen, privaten Computer als Arbeitsmittel mit ins Büro bringen können.

Worum geht's?

Die Idee kommt aus den USA. Dort geben immer mehr Unternehmen seit einigen Jahren ihren Mitarbeitern die Möglichkeit, anstelle des Firmencomputers ihren privaten PC als Arbeitsmittel zu benutzen. Dies gilt prinzipiell nicht nur für PCs, sondern auch für mobile Endgeräte wie Smartphones und Smartpads.

Für die Unternehmen würden dadurch die Anschaffungs- und meist teuren Wartungskosten entfallen. Auch für die Lizenzen und die Aktualisierung der Sicherheitssoftware wäre der Mitarbeiter selbst verantwortlich. Dafür bekommt er vom Unternehmen einen einmaligen Betrag, der z.B. in den USA schon mal um die 2.000 US$ betragen kann.

Als Vorteil für den Mitarbeiter wird gesehen, dass er die ihm aus dem privaten Bereich bereits vertraute Hardware einsetzen kann und zudem nicht zwei Endgeräte schultern muss, z.B. ein berufliches Smartphone und ein privates. Außerdem kann er das Betriebssystem seiner Wahl nutzen.

Probleme erkennen und Lösungen finden!

Was sich so zwanglos und flexibel anhört, birgt aber eine Vielzahl von Problemen, für die es nicht immer eine zufriedenstellende Lösung gibt. So ist es neben Urheberrecht, Fragen des Lizenzrechts und der Haftung, handels- und steuerrechtlichen Vorschriften sowie der IT-Sicherheit insbesondere der Datenschutz, der hier beleuchtet werden soll.

Risiken

Folgende Risiken sind zu bewerten:

- Die Übertragung personenbezogener Daten muss nicht mehr im unternehmenseigenen Netzwerk erfolgen. Auch potenziell unsichere Netzwerke wie öffentliche WLAN-Hotspots können genutzt werden.
- Personenbezogene Unternehmensdaten können lokal auf dem privaten Endgerät gespeichert werden. Dadurch entstehen diverse Folgeprobleme:
  - Auf den Geräten werden Daten gespeichert, die nicht im direkten Zugriff des Unternehmens stehen. Wie werden Herausgabeansprüche des Arbeitgebers umgesetzt an Daten, für die er die verantwortliche Stelle ist?

WEKA MEDIA GmbH & Co. KG

  - Personenbezogene Unternehmensdaten werden durch die lokale Speicherung mit privaten Daten vermischt. Dadurch wird das Trennungsverbot der Anlage zu § 9 BDSG tangiert.
  - Die Unternehmensdaten könnten auf dem privaten PC möglicherweise durch dort vorhandene Schadsoftware in ihrer Integrität geschädigt werden.
  - Der Mitarbeiter wäre außerdem für eine Datensicherung verantwortlich bzw. bei einer Sicherung durch das Unternehmen würden auch private Daten gesichert werden.
  - Wie kann die Anbindung externer Speichermedien (z.B. USB-Anschluss) unterbunden werden, um einen unberechtigten Abfluss von Unternehmensdaten zu erschweren?
- Grundsätzlich ist fraglich, ob die Zweckbestimmung der jeweiligen konkreten Datenverarbeitung es umfasst, dass die Daten auf einem privaten Endgerät verarbeitet werden und somit nicht mehr im unmittelbaren Einfluss der verantwortlichen Stelle sind.
- Wie ist zu verfahren, wenn das Endgerät defekt ist oder sogar abhandenkommt?
- Wie kann der Datenübertragungsweg vom Unternehmen zum Endgerät abgesichert werden?

Hauptprobleme

Eines der Hauptprobleme ist jedoch die Vermischung beruflicher und privater Daten, die datenschutzrechtlich gegen die Zweckbestimmung der rein beruflich zu verarbeiteten Daten verstößt. Außerdem ist bei privaten Geräten oftmals nicht der Mitarbeiter der alleinige Zugriffsberechtige, oft nutzen Familienangehörige das Gerät mit. Dabei ist der Verlust der Vertraulichkeit der beruflichen Daten leicht möglich, wenn nicht technisch der Zugriff auf den Mitarbeiter beschränkt wird.

Problemlösung: Verschiedene Ansätze

Helfen können hier bei der Problemlösung verschiedene Ansätze. Eine Möglichkeit ist, organisatorisch den Mitarbeitern mittels Dienstanweisung vorzugeben, dass sie auf ihrem privaten Endgerät neben dem aktuellen Virenschutz auch eine exakte Trennung der beruflichen Daten von den privaten vorzunehmen haben. Sich aber auf rein organisatorische Lösungen zu verlassen, wird in diesem Zusammenhang als eher unzureichend einzustufen sein. Vorzugswürdige technische Lösungen bieten dagegen an, eine Art „Sandbox“, also einen isolierten Bereich, auf dem privaten Endgerät zu erzeugen. Darin wäre eine berufliche Nutzung mit ausschließlich beruflichen Daten möglich, und es bestünden keine Verbindungen mit den außerhalb dieses Bereichs befindlichen privaten Daten. Hier gibt es am Markt bereits verschieden Lösungsversuche von unterschiedlichen Anbietern. Da das Thema erst wenige Jahre alt ist, liegen diese Lösungen noch nicht immer in einer vollends ausgereiften Form vor.

Fazit

Hier kann nur empfohlen werden, dass der Datenschutzbeauftragte sich eng mit den IT-Verantwortlichen des Unternehmens berät und auf die datenschutzrelevanten Punkte hinweist.

Grundsätzliche Empfehlungen

Hier noch einige grundsätzliche Empfehlungen:

- möglichst wenige Daten auf dem mobilen Endgerät speichern
- klare technische Trennung zwischen beruflichen und privaten Daten
- Verschlüsselung der beruflichen Daten auf dem privaten Gerät und im Übertragungsvorgang vom und zum Unternehmensnetzwerk
- eigener und sicherer Zugriffsschutz auf Gerät und berufliche Applikationen
- keine Synchronisation auf andere private Geräte zulassen
- Unternehmen sichert nur geschäftliche Daten
- Logging der geschäftlichen Datenverarbeitungen, soweit gesetzlich erlaubt
- Verbot bzw. Deaktivierung datenschutzkritischer Apps (Blacklist/Whitelist) und Gerätefunktionen (z.B. Geolokalisation)

Wenn auf alle hier aufgeworfenen Fragen eine akzeptable Antwort gefunden werden kann, die sich außerdem entsprechend dem Schutzbedarf der zu verarbeitenden Daten angemessen umsetzen lässt, kann auch das Modell des Bring your own device datenschutzkonform im Unternehmen umgesetzt werden.