Anforderungen an mobil genutzte IT-Arbeitsgeräte

1. Erläuterung

Bei mobiler Arbeit gelten die gleichen Anforderungen an Datenschutz und Informationssicherheit wie bei der Tätigkeit in der Dienststelle. Da u. a. das Risiko für einen unberechtigten Zugriff auf zu schützende Daten durch Dritte außerhalb der Dienststelle als höher einzustufen ist, müssen Sicherheitsvorkehrungen getroffen werden. In Abhängigkeit von der Tätigkeit und dem Schutzbedarf der zu verarbeitenden Daten ergeben sich deshalb folgende Anforderungen an die verwendeten mobilen IT-Geräte.

Die Festlegungen zur Gestaltung der Mobilen Arbeit an der TU Bergakademie Freiberg orientieren sich am BSI-Grundschutzstandard 200-2 sowie am IT-Grundschutz-Kompendium des BSI (Bundesamt für Sicherheit in der Informationstechnik, http://www.bsi.bund.de).

Maßgeblich sind in den jeweils aktuellen Fassungen, insbesondere die Module

- CON 7 Informationssicherheit auf Auslandsreisen,
- INF1 Gebäude,
- INF 8 Häuslicher Arbeitsplatz,
- INF 9 Mobiler Arbeitsplatz,
- NET 3.3 VPN,
- OPS 1.2.4 Telearbeit,
- SYS 2.1 Allgemeiner Client,
- SYS 3.1 Laptops,
- SYS 3.2.1 Allgemeine Smartphones und Tablets,
- SYS 3.4 Mobile Datenträger

zzgl. aller dort verwiesenen Module.

2. Verarbeitung von Daten mit keinem oder geringem Schutz

2.1 Beispiele für Verarbeitungstätigkeiten

- Konzeptionelle Arbeiten
- Recherchearbeiten
- Fernwartung von Rechnern und Anlagen
- Nutzung von Remote-Diensten der TU Bergakademie Freiberg (z.B. Online Office, Webmail)
- Unzulässig ist in dieser Kategorie die Verarbeitung von personenbezogenen Daten in jeder Art und Weise bzw. anderen Daten mit (begründetem relevanten) Schutzbedarf.

2.2 Anforderungen

Es wird die Umsetzung der Basisanforderungen der BSI-Bausteine empfohlen. Die folgenden Punkte sind jedoch verpflichtend bzw. darüber hinausgehend zu beachten:

- Nutzung von privaten und dienstlichen mobilen IT-Geräten ist zulässig, z.B. Desktop, PCs, Laptops
- Installierte Software, insbesondere das Betriebssystem, muss regelmäßig auf Sicherheitsupdates überprüft werden. Verfügbare Updates sind umgehend zu installieren, nach Möglichkeit sollte dieser Prozess durch die vom Betriebssystem vorgesehenen automatisierten Algorithmen unterstützt werden.
- Um Datenverlust zu vermeiden, sind Arbeitsergebnisse regelmäßig in zentralen Speichersystemen des Universitätsrechenzentrums (URZ) zu sichern.

- Geräte müssen über ein Zugangsschutzverfahren gesichert sein (z.B. Passwort, PIN, Security-Token).
- Datenverbindungen zum Campusnetz und zu Diensten des URZ sind zu verschlüsseln (z.B. durch Nutzung von VPN, SSH, HTTPS).
- Für den Laien zumutbare Schutzmaßnahmen nach dem aktuellen Stand der Technik müssen umgesetzt werden, z.B.
  - sorgsamer Umgang mit Webbrowsern und E-Mail-Anhängen,
  - wo möglich Benutzung von verschlüsselten Datenübertragungsprotokollen (HTTPS, SSL/TLS),
  - keine Verwendung von Administratorberechtigungen für reguläre Tätigkeiten

3. Verarbeitung von Daten mit personenbezogenem Inhalt oder Daten mit Schutzstatus

Die Verarbeitung von Daten mit Schutzstatus, wie z.B. Probanden- und Personaldaten, ist in Mobiler Arbeit grundsätzlich unzulässig. Ausnahmeregelungen sind im Voraus mit dem Datenschutzbeauftragten, IT-Sicherheitsbeauftragten und dem URZ abzustimmen.

4. Zugang zum geschützten Netz / VPN

Der VPN-Zugang und andere kritische Dienste sind neben Nutzername/Passwort durch ein Verfahren der Zwei-Faktor-Authentifizierung geschützt. Voraussetzung zur Nutzung ist ein kompatibles Smartphone sowie die Installation der entsprechenden App. Bei Verlust des zweiten Faktors ist unverzüglich das URZ zu informieren.

Neben dem allgemeinen VPN stehen auch VPN-Profile zum Zugriff auf spezifische Ressourcen der Bereiche zur Verfügung. Dort gelten die Vorschriften zum Anschluss von Geräten ans Campusnetz analog, insbesondere muss die Endpoint- Protection Lösung "Sophos Intercept X with XDR" bei Windows/Mac installiert sein und die Nutzung von nicht mehr vom Hersteller unterstützten Betriebssystemversionen ist untersagt.

Fragen beantwortet das URZ.

Von diesem Merkblatt habe ich Kenntnis genommen und eine Ausfertigung erhalten.

Freiberg, den ……

……...

Beschäftigter