

Risiken bei der Nutzung privater Endgeräte

Im Zusammenhang mit dem Rundschreiben 1/2019, das auf die Gefahren hinweist, die bei der Nutzung von Privatgeräten für dienstliche Zwecke bestehen, ergeben sich immer wieder Rückfragen.

Die nachfolgende Erläuterung, die aus IT-technischer Sicht formuliert ist, kann hier vielleicht für größere Klarheit sorgen:

Der Dienstherr hat **keinen Zugriff auf private Endgeräte** und kann (bzw. darf) nicht prüfen, ob das private Endgerät überhaupt den Grundanforderungen an ein IT-Gerät genügt:

- sind gültige Lizenzen (z.B. Betriebssystem, Office-Produkt) vorhanden?
diese Frage betrifft nicht nur Betriebssystem und die Office-Produkte, sondern alle eingesetzten Softwarepakete. Von der Universität beschaffte Lizenzen dürfen nicht einfach auf privaten Endgeräten eingesetzt werden.
- ist ein Zugriffsschutz eingerichtet?
wenn z.B. ein *login* ohne Passwort eingerichtet ist, kann nach Verlust des Geräts der unehrliche Finder auf alle Daten oder auf die Uni-Systeme zugreifen. Ebenso darf sich nicht jedes Familienmitglied unter demselben privaten Account einloggen.
- ist ein aktueller Virenschutz installiert und wird sichergestellt, dass dieser jeden Tag Updates erhält? Und ist die Firewall aktiv?
- stellen Sie sicher, dass das Betriebssystem wie auch jegliche Software regelmäßige Updates erhalten?
- entspricht die Datenhaltung auf dem privaten Endgerät den (rechtlichen) Anforderungen?
Die Daten dürfen höchstens als Kopie temporär auf dem Endgerät liegen und müssen dort auch zuverlässig wieder gelöscht werden können; die Originaldaten müssen auf den Servern der Universität verbleiben. Regelmäßige Backups sind erforderlich.
- trennen Sie dienstliche Arbeiten am Rechner von privaten Tätigkeiten (wie auch Daten)?
- ist Ihr Heim-Netzwerk (Internetzugang) verschlüsselt? Bspw. *WPA2* Passwort bei *WLAN*?

Weitere Hinweise zur Sicherheit finden sich unter <https://wiki.uni-freiburg.de/rz/doku.php?id=tag:sicherheit>

Wenn Sie durch Nutzung vorhandener IT-Kompetenz (z.B. Ihre:s IT-Administrator:s) zu der Erkenntnis kommen, dass **im Einzelfall** das private Endgerät sich auf dem Niveau eines von Ihrer IT-Abteilung eingerichteten Dienstgeräts befindet, so ist das Betriebsrisiko mit dem vergleichbar, das auch vom Dienstgerät ausgeht. Dann dürfte das Risiko des Einsatzes dieses Privatgeräts in der aktuellen Lage akzeptabel sein.

Bitte bedenken Sie dabei: Den Herstellern von Computer-Viren ist es egal, aus welchen Gründen man den Einsatz von schlecht gesicherten privaten Endgeräten duldet. Jedes Einfallstor ist diesen Kriminellen willkommen. Als Folge des stark steigenden Einsatzes von IT in allen Bereichen dürfte die Computerkriminalität in den nächsten Wochen steigen.

Noch etwas: ein Dienstgerät ist nicht allein deshalb sicher, weil es aus einem Budget der Universität gekauft wurde. Die Einrichtung des Dienstgeräts sollte nicht Unerfahrenen überlassen werden und unterliegt denselben Regeln.