Regelung zur Verschlüsselung von mobilen Endgeräten und Datenträgern

Ziel: Schutz sensibler bzw. personenbezogener Daten der WWU, Erfüllung der Forderung der LDI NRW

Laptops, Mobilgeräte und mobile Datenträger unterliegen einem höheren Risiko von Datenverlusten als bei stationären Systemen. Ursache können Diebstahl oder Geräteverlust sein, aber auch technische Probleme oder schlichter Strommangel.

Umsetzung

Auf allen Geräten, auf denen dienstliche Daten verarbeitet werden, muss ein angemessener Zugriffsschutz vorhanden sein. Dieser verhindert, dass das Gerät unberechtigt benutzt werden kann bzw. unberechtigt auf Daten zugegriffen werden kann. Festplatten bzw. Datenträger müssen verschlüsselt werden. Für die Verschlüsselung muss ein sicherer Verschlüsselungsalgorithmus eingesetzt werden. Die Schlüssel müssen zufällig erzeugt werden und geeignet aufbewahrt werden.

Mobile Geräte sollten nur zur vorübergehenden Speicherung von Daten verwendet werden. Diese Daten müssen regelmäßig gesichert werden.

Begleitende Maßnahmen

1) Über Microsoft Exchange werden sofern möglich Einstellungen für Zugriffsschutz und Verschlüsselung von ZIV und IVVen auf mobilen Endgeräten erzwungen. Dies betrifft auch private Geräte, mit denen auf dienstliche Daten zugegriffen wird.
2) Beim Einkauf von mobilen Endgeräten sollte darauf geachtet werden, dass sie bereits von Beginn an verschlüsselt sind oder sich die Verschlüsselung zumindest aktivieren lässt.

Hinweise

- Zur Verschlüsselung sollten vorrangig die im Betriebssystem integrierten Verfahren genutzt werden (z.B. BitLocker unter Microsoft Windows).
- Zur Synchronisation der Daten zwischen Mobilgerät und Arbeitsplatz sollte sciebo (https://sciebo.de/) genutzt werden.
- Siehe auch https://www.uni-muenster.de/IT-Sicherheit/anwender/verschluesselung.html
- Siehe auch https://www.uni-muenster.de/imperia/md/content/ziv/pdf/sicherheit/mobil_empfehlungen.pdf