EVANGELISCHE KIRCHE
IN HESSEN UND NASSAU

IT-SICHERHEITS-NEWSLETTER für JULI 2023

UMGANG MIT DATEN IM MOBILEN UMFELD

GEFAHREN IM UMGANG MIT DATEN IM MOBILEN UMFELD

Werden Daten außerhalb der EKHN im mobilen Umfeld genutzt, existieren verschiedene Gefahren, denen die Daten bei der Nutzung ausgesetzt werden.

Datenverlust

USB Sticks, mobile Datenträger oder Akten können verloren gehen oder beschädigt werden, was zu einem Verlust von wichtigen Daten, einem einhergehendem finanzellen Schaden aber möglichweise auch zu einem schwerwiegenden Verlust der Vertraulichkeit von Informationen führen, kann.

Datenlecks

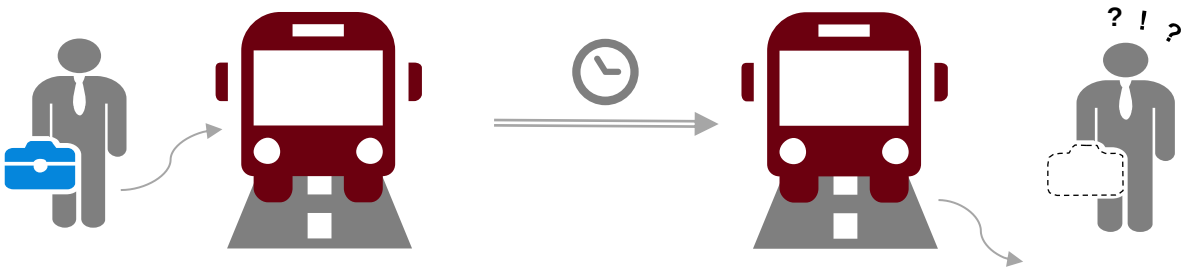
Werden Daten in ungesicherten Netzwerken, auf unverschlüsselten Datenträgern gespeichert oder offen liegen gelassen, besteht die Gefahr, dass diese von Unbefugten Dritten eingesehen, gestohlen oder manipuliert werden können.

Schadsoftware

USB Sticks und andere mobile Datenträger können mit Schadsoftware befallen sein, welche das IT-System durch herstellen einer Verbindung, infizieren und somit Schaden anrichten können. Auch manipulierte Geräte wie Tastaturen, Mäuse und Ladekabel können mit Schadsoftware versehen sein und sich als normales Gerät tarnen.

GEFAHREN AM BEISPIEL AKTENTRANSPORT

DATENVERLUST



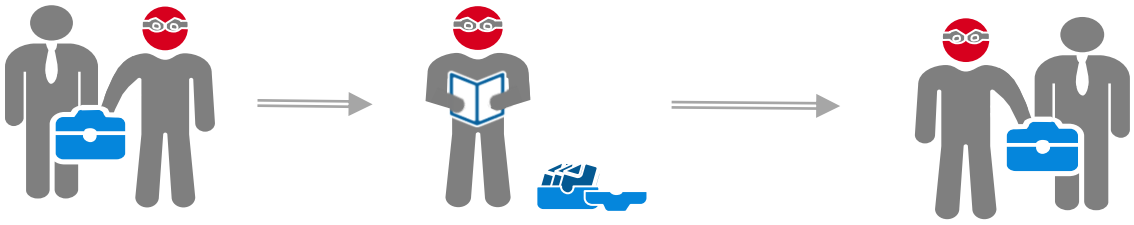
Werden Unikate transportiert und eine Datensicherung bzw. Kopie dieser Unikate fehlt, könnten Ziele und Aufgaben nicht wie geplant erreicht werden, wenn das Unikat verloren geht.

EVANGELISCHE KIRCHE
IN HESSEN UND NASSAU

IT-SICHERHEITS-NEWSLETTER für JULI 2023

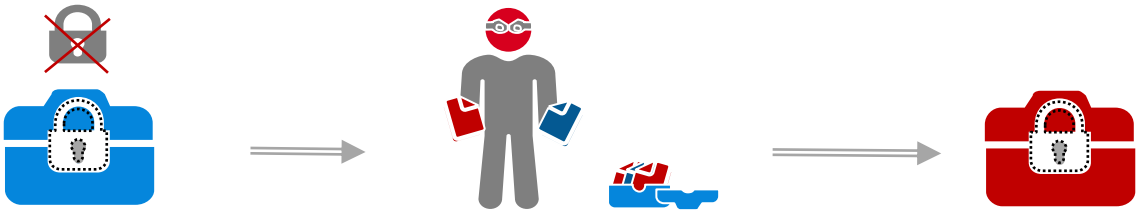
UMGANG MIT DATEN IM MOBILEN UMFELD

DATENLECKS



Geraten ungesicherte Dokumente in falsche Hände, kann dies unbemerkt zu einem schwerwiegenden Verlust der Vertraulichkeit von Informationen führen.

DATENMANIPULATION



Erfolgt für mobile Daten kein ausreichender Zugriffsschutz, könnten Akten oder Datenträger unbemerkt kopiert oder manipuliert werden.

QUICKTIPS

Regeln für den Umgang mit Daten im mobilen Umfeld

- Verwenden Sie wenn möglich verschlüsselte Datenträger und Netzwerke, um die Sicherheit von Daten zu gewährleisten.
- Nutzen Sie zur Weitergabe oder zum Speichern von Daten sichere Netzwerke und Services, so wie z.B. die Nextcloud des EKHN Portals.
- Legen Sie fest, welche Daten und Informationen außerhalb der EKHN bearbeitet oder transportiert werden dürfen.
- Lagern Sie mobile Geräte, Datenträger oder Dokumente nur in gesicherten Umgebungen und setzten Sie zur Absicherung der Umgebung auch einen weiteren Zugriffs-/Zutrittsschutz ein (z.B. Unterlagen und Geräte in einem Schrank verschließen).