IT-Sicherheitstipp Nr.5 – Juli 2019

Umgang mit mobilen Geräten

Was sind mobile Geräte?

Mobile Geräte gehören mehr und mehr zum alltäglichen Leben. Hierzu zählen Mobiltelefone, Laptops, Tablets, aber auch Chipkarten und USB-Sticks.

Mobile Geräte werden sowohl im Privatbereich als auch bei der täglichen Arbeit in Behörden eingesetzt. So ist es möglich, dass sich auf ein und demselben Gerät neben den privaten Daten und Anwendungen des Benutzers oder der Benutzerin auch sensible Behördendaten befinden.

Im Folgenden werden alle Geräte, die Daten speichern können, beweglich sind und damit leicht in das Verwaltungsgebäude gebracht oder aus diesem entfernt werden können, als mobile Geräte bezeichnet.

Gefahren und Risiken

Grundsätzlich unterliegen mobile Geräte und die auf ihnen gespeicherten Daten den gleichen Sicherheitsbestimmungen wie alle anderen IT-Systeme Ihrer Verwaltung. Mobile Geräte und Speichermedien unterliegen jedoch besonderen Gefahren, denn sie werden häufig auch außerhalb der Behörde verwendet und sie können leichter vergessen, verloren oder gestohlen werden; dadurch können vertrauliche Daten schnell in falsche Hände geraten. Diese Gefahren gilt es mit geeigneten Sicherheitsmaßnahmen zu verringern.

Gefahren bei Verlust mobiler Geräte:

- Vertrauliche Informationen können unkontrolliert preisgegeben werden
- Der Verlust ist ein finanzieller Schaden
- Der Dieb oder Finder hat viel Zeit, die Daten zu analysieren

Moderne Kommunikationstechnologien — „Jeder hört mit“

Mobile Geräte mit Benutzeroberflächen wie Smartphones bieten nicht nur Möglichkeiten zum Telefonieren, zur Adressverwaltung oder auch zum Betrachten und Bearbeiten von Dokumenten. Sie können auch zum Surfen im Internet oder zum Austausch von Kurznachrichten und Fotos verwendet werden.
Das alles geschieht kabellos mittels "Wireless"- (Drahtlos-) Technologien wie Bluetooth oder WLAN und natürlich den Telefon- und Datennetzen UMTS und LTE. Problematisch ist dabei, dass oft schwer festzustellen ist, wer bei einer drahtlosen Datenübertragung mithört und ob dieser Zugang gerade ausspioniert wird. Gerade unverschlüsselte WLANs erlauben leicht Angriffe auf die über sie übermittelten Daten.

Viele Anwendungen auf Smartphones (Apps) verlangen bei der Installation weitgehende Rechte, die nicht immer benötigt werden. Bitte achten Sie darauf, den Apps nicht notwendige Rechte zu entziehen.

Drahtlose Übertragungstechniken:

- NFC = Near Field Communication; Übertragungsstandard zum kontaktlosen Datenaustausch; Reichweite: bis 10 cm
- Bluetooth = Dient der drahtlosen Verbindung von Endgeräten; Reichweite: 10–100 Meter
- WLAN = Wireless Local Area Network; Verbindung mehrerer Endgeräte über einen lokalen Sender (Access Point); Reichweite: 50+ Meter
- UMTS = Universal Mobile Telecommunications System; Nachfolger des GSM-Netzes mit bis zu 21 MBit/s
- LTE = Long Term Evolution; Weiterentwicklung von UMTS mit bis zu 300 MBit/s
- 5G = Fifth Generation; Weiterentwicklung von LTE mit bis zu 10.000 MBit/s

LANDKREIS MARBURG BIEDENKOPF

Projekt der interkommunalen Zusammenarbeit

Cybersicherheit

Landkreis Gießen
HESSENS MITTE • WISSEN WIRTSCHAFT & KULTUR

WLAN — Wireless Local Area Network

Bei Wireless LAN (WLAN) handelt es sich um eine Funknetzwerktechnik, die – wenn einmal aufgebaut – wie ein normaler, aber kabelloser Netzwerkzugang funktioniert. Oftmals werden WLAN-Techniken in Besprechungsräumen und in Außenbüros eingesetzt. WLANs stehen aber auch in Cafés, Hotels oder anderen öffentlichen Bereichen bereit. Die Nutzung eines unverschlüsselten WLANs erleichtert den unerkannten Angriff und das Mitlesen von gesendeten Daten.

So verhalten Sie sich richtig:

- Wenn eine eigene drahtgebundene Netzwerkverbindung möglich ist, ist diese der WLAN-Technik vorzuziehen
- Wenn WLAN eingesetzt wird, muss grundsätzlich der höchstmögliche Sicherheitsstandard zur Verschlüsselung des Zugangs gewählt werden (derzeit WPA2)
- Jeder ungewöhnliche Vorgang auf Ihrem Endgerät in Verbindung mit Funknetzen könnte ein Angriff sein; im Zweifel deaktivieren Sie die WLAN-Verbindung und informieren Sie Ihre IT-Ansprechpersonen
- Sollten Sie keine Kenntnis über die Funktion und das Einstellen dieser Mechanismen haben, informieren Sie sich bitte bei Ihren IT-Ansprechpersonen
- Besuchen Sie wenn möglich nur Internetseiten, die per „https://“ aufrufbar sind

Mobiltelefone

Heute haben viele Handys umfangreiche, computerähnliche Funktionen. Entsprechend ist auch hier Vorsicht geboten, vor allem beim Speichern von Informationen auf dem Mobiltelefon:

- Es sollte eine PIN-Abfrage (über Passwort, Fingerabdruck oder Gesichtserkennung) und eine damit einhergehende Geräteverschlüsselung eingerichtet sein
- Alle drahtlosen, nicht für die aktuelle Nutzung benötigten Kommunikationsmöglichkeiten sollten aus Sicherheitsgründen deaktiviert sein
- Es sollten keine vertraulichen Daten gespeichert werden (z.B. Aktenauszüge)
- Ist die Speicherung vertraulicher Daten notwendig und von Ihrer Verwaltung erlaubt, so sind diese zu verschlüsseln
- Der Verlust eines Geräts mit vertraulichen Daten ist den Vorgesetzten und der Ansprechperson zu melden

Notebooks

Viele Organisationen stellen ihren Beschäftigten Smartphones, Laptops oder Tablets zur Verfügung, die oft bereits besondere Sicherheitseinstellungen enthalten.

Richtig

- Mindestens einmal pro Woche mit dem Behördennetz verbinden, um Software-Updates und Konfigurationsänderungen zu ermöglichen
- Dem Virenschutzprogramm bei Nutzung täglich die Aktualisierung ermöglichen
- Bei Fehlermeldungen des Virenscanners oder der Verschlüsselungssoftware sofort Ihre IT-Ansprechperson benachrichtigen
- Den Verlust des Endgeräts unverzüglich der IT-Ansprechperson und den Vorgesetzten melden
- Regelmäßig alle Daten sichern und gemäß ihrer Vertraulichkeitsklasse aufbewahren
- Wenn möglich die Daten im Endgerät verschlüsseln

Falsch

- Geräte- und Login-Informationen an Dritte weitergeben
- Die Konfiguration des Notebooks selbstständig verändern
- Eigenmächtig Programme installieren
- Unberechtigte Personen wie Familienangehörige das Gerät bedienen lassen

Bei Fragen wenden Sie sich bitte an Ihre Informationssicherheitsbeauftragten oder die Projektleitung Cybersicherheit.

Eine gemeinsame Sensibilisierungskampagne zur Informationssicherheit der Landkreise Marburg-Biedenkopf und Gießen im Rahmen des IKZ-Projekts Cybersicherheit.

Geht mich nichts an?
Mit Sicherheit!

Cybersicherheit

Apps und „Bring your own device“

Stellt Ihnen Ihre Behörde ein Smartphone zur Verfügung, das Sie auch privat nutzen dürfen? Oder erlaubt sie die dienstliche Nutzung Ihres privaten Handys ("Bring your own device — BYOD")?
Dann müssen Sie sich an die Sicherheitsvorgaben Ihrer Verwaltung halten!
Insbesondere müssen Sie darauf achten, dass dienstliche und private Daten nicht vermischt werden. Außerdem können viele Apps Ihr Nutzungsverhalten ausspähen. Viele Apps wollen mehr Rechte haben, als es für ihre Nutzung erforderlich ist. Verweigern Sie den Apps diese Rechte oder verzichten Sie ganz auf sie.

Folgende Punkte sollten Sie stets beachten:

- Installieren Sie zeitnah alle verfügbaren Updates
- Installieren und nutzen Sie nur Apps, die sie benötigen
- Schränken Sie die Zugriffsberechtigungen für Ihre Kontakte, Standortangaben etc. möglichst ein
- Verarbeiten Sie keine dienstlichen Daten in privaten Apps
- Auch sogenannte Messenger wie z.B. WhatsApp, die Sie privat verwenden, dürfen nicht für dienstliche Zwecke genutzt werden
- Löschen Sie nicht benötigte WLAN-Netzwerke
- Der Verlust eines Geräts ist unverzüglich den Vorgesetzten und Ihren IT-Ansprechpersonen zu melden

Mobile Datenträger

Trotz Vernetzung, E-Mail und Internet kann es notwendig sein, Daten zwischen zwei nicht verbundenen Rechnern auszutauschen. Zu diesem Zweck werden üblicherweise mobile Datenträger wie CDs/DVDs oder USB-Sticks verwendet (aber auch MP3-Player, Smartcards und Chipkarten).

Dabei ist doppelte Vorsicht geboten:

- Es können auf diese Weise interne und vertrauliche Informationen an Unbefugte geraten
- Zum anderen können durch die Verwendung mobiler Datenträger leicht Viren und andere schädliche Programme in das Verwaltungsnetz gelangen

Schutz mobiler Datenträger

- Auf mobilen Datenträgern sollten, wenn möglich, keine geheimen oder vertraulichen Daten gespeichert werden
- Ist die Speicherung vertraulicher Daten notwendig, so sind diese zu verschlüsseln
- Darüber hinaus sollten alle mobilen Datenträger vor der Verwendung mit einem aktuellen Virenscanner auf Viren untersucht werden
- Mobile Datenträger müssen an einem sicheren Ort aufbewahrt werden
- Der Verlust eines Datenträgers mit vertraulichen Daten ist unverzüglich den Vorgesetzten und der IT-Ansprechperson zu melden