IT-LINUXMAKER

Checkliste: Sicheres mobiles Arbeiten

Beachtung betriebsinterner Sicherheitsrichtlinien bei der Nutzung mobiler Geräte

Generell sollten Sie sich über eventuelle Vorgaben des Betriebs zum sicheren Umgang informieren und Rücksprache bei Fragen nehmen. Dabei spielt es keine Rolle, ob es sich um ein betriebliches oder privates Gerät *("Bring your own Device")* handelt.

Sichere WLAN-Netze nutzen

Die Nutzung öffentlicher WLAN-Zugänge beinhaltet deutlich mehr Risiken als das Internet-Surfen per Mobilfunk-Netz.

Angreifer können via Smartphone und speziellen Sniffer-Apps den Datenverkehr über ungeschützte öffentliche Hot-Spots mitlesen. Passwörter für Accounts und Online-Banking werden so sehr leicht abgegriffen.

Sorgfältiges Prüfen von Apps

Apps können durchaus Schadsoftware enthalten, sensible Daten übertragen oder Zugriffe auf nicht benötigte Funktionen verlangen. Deshalb sollten Sie die Sicherheitseinstellungen der Apps vor der Installation und Updates überprüfen. Und installieren Sie nur Apps, die aus den App-Stores stammen und nicht aus unbekannten Quellen.

Mobile Geräte sind kein Datenspeicher

Daten ausschließlich auf dem mobilen Arbeitsgerät zu hinterlegen, ist keine gute Lösung. Denn bei einem Verlust des Gerätes, sind auch die Daten verloren. Außerdem können diese Daten nicht an den regelmässigen Backups teilnehmen, so dass auch hier ein Unsicherheitsfaktor besteht. Wichtige Daten gehören somit immer ins Firmennetzwerk respektiove in eine sichere Cloud.

Abschalten von WLAN, Bluetooth und NFC

Solange Sie die drahtlosen Schnittstellen wie WLAN, Bluetooth oder NFC *("Near Field Communication")* nicht im Augenblick nutzen, sollten diese deaktiviert sein. Denn so verringern Sie das Risiko, dass diese für Hackerangriffe genutzt werden können.

VPN-Nutzung in Öffentlichen Netzen

Ein VPN (Virtual Private Network) überträgt alle Daten vom Endgerät im Internet komplett verschlüsselt. Deshalb nutzen Sie nur diesen authentisierten und verschlüsselten Weg, wenn Sie auf das interne Firemennetzwerk und sensible Daten zugreifen wollen.

Absicherung vor Diebstahl und Verlust

Digitale Mobilgeräte können sehr leicht durch Diebstahl oder unbefugten Zugriff Dritter abhanden kommen. Schutz dagegen bietet die Bildschirmsperre, starke Passwörter, PINS sowie ein zweiter Faktor an Ihrem Gerät.

IT-LINUXMAKER
Inhaber: Andreas Günther
UST-ID Nr.: DE240267218
James-F.-Byrnes-Straße 9
70376 Stuttgart

e-Mail: info@it-linuxmaker.com
Website: https://www.it-linuxmaker.com
Telefon: +49 711 806 31 12