10 Tipps für mehr Sicherheit bei der Smartphone-Nutzung:

Sicher mobil arbeiten

Die Flexibilisierung von Arbeitsort und -zeit oder auch Freiheiten für die Mitarbeiter bei der Wahl ihrer Rechner und Smartphones bergen teilweise auch erhebliche Risiken – insbesondere wenn dabei unerwünschte Zugriffe von außen auf das hochsensible Firmennetzwerk ermöglicht werden. Worauf bei Smartphones zu achten ist, wird hier in zehn Punkten zusammengefasst.

Von Stefan Schaffner (li.) und Janis Kinast, Groß-Bieberau

Schon mit einigen einfachen Regeln für Policy und Aufklärung der Mitarbeiter kann man möglichen Gefahren bei der Smartphone-Nutzung proaktiv begegnen.

1. Niemals aus den Augen lassen: Smartphones sind klein, leicht und wertvoll. Damit sind die Geräte eine leichte Beute für Diebe. Es ist trotz GPS recht unwahrscheinlich, ein verlorenes Gerät zurück zu bekommen. Auch zum Schutz vor Manipulation sollte das Gerät nie (wirklich niemals) aus den Augen gelassen werden.

2. Nur die notwendigen Daten speichern: Viele Apps haben weitreichende Zugriffsberechtigungen, die selten vom Benutzer geprüft und schwer bis gar nicht überwacht werden können. Es sollten daher nur jene Daten auf dem Mobiltelefon gespeichert werden, die zwingend notwendig sind. Falls wichtige Daten auf dem Smartphone verbleiben müssen, sollten diese unbedingt mit geprüfter Software verschlüsselt werden.

3. E-Mail-Kommunikation verschlüsseln: Die E-Mail Kommunikation via Smartphone sollte nur mit SSL/TLS stattfinden und am besten PGP/GPG oder S/MIME verschlüsselt werden. Bei manchen Smartphones sind hierfür gesonderte Einstellungen nötig. Vor der Nutzung, sollten also in jedem Fall die entsprechenden Einstellungen geprüft werden.

4. Mitlesen verhindern: Zum Schutz vor dem Mitlesen von E-Mails, Nachrichten, Passwort oder Pin sollte das Smartphone mit einer Sichtschutzfolie ausgestattet werden.

5. Vorsicht bei WLAN: Das Smartphone sollte nicht unbedacht in ein WLAN eingebunden werden, da die Passwörter im Klartext auf den Geräten hinterlegt werden und sich mit Administratorrechten auslesen lassen (Android: /Data/misc/Wifi/WPA_supplicant.conf) und Daten von Apps und Geräteinformationen mitgelesen werden können.

6. Nur vertrauenswürdige Apps: Apps können Trojaner, Viren oder Malware enthalten und dann Passwörter oder Bankdaten abgreifen, sowie das Smartphone zu einer aktiven Gefahr für alle Netzwerke oder PC, die mit ihm in Verbindung stehen, werden lassen. Die Nutzung von Apps aus den Hersteller-Shops bietet zwar keine Garantie dafür, dass die App unschädlich ist, senkt aber das Risiko beträchtlich.

7. Schnittstellen im Blick behalten: Nicht genutzte Schnittstellen, wie Bluetooth, WLAN, GPRS und USB, sollten deaktiviert werden, wenn sie nicht benötigt werden. Somit bieten die Nutzer keine Angriffsfläche und erschweren das Erstellen von Bewegungsprofilen.

8. Backup und Remote-Löschung: Die Geräte sollten regelmäßig ein Backup erstellen und die Möglichkeit der Remote-Löschung bieten. So können bei Verlust des Gerätes sensible Daten von dem Smartphone entfernt werden und der Nutzer erleidet keinen Datenverlust.

Bild: Ute Mulder / pixelio.de

9. Zugriff erschweren: Um das Gerät vor dem Zugriff durch Unbefugte zu schützen, gilt es stets Displaysperre und Simlock zu verwenden. Dies erschwert auch das Auslesen der Daten oder die Weiterverwendung im Verlustfall.

10. Guter Virenschutz: Ein guter Schutz vor Viren und schädlichen Links ist unabdingbar, da sie Attacken frühzeitig erkennen helfen. Smartphones sind besonders gefährdet wegen der in der Regel schwer einsehbaren E-Mail Header oder den in Links häufig verwendeten gekürzten Web-Adressen.

Doch selbst wenn diese Regeln beachtet werden, ist dies nur eine Gefährdungsreduktion aber noch keine Garantie für einen sicher wirkenden Angriffsschutz. Zusätzlich helfen können hier grundlegende Sicherheitskonzepte, die die sichere Nutzung von Smartphones im beruflichen Alltag möglich machen. Dabei sollten sich Unternehmen und Behörden nicht scheuen, bei Bedarf externe Fachleute hinzuzuziehen.

Über unsere Autoren:

Stefan Schaffner ist Geschäftsführer, Janis Kinast, IT-Security-Consultant der ASS it-systemhaus GmbH, Groß-Bieberau.
Kontakt: info@ass-systemhaus.de