

Checkliste: Smartphones

Sensible Unternehmensdaten sind auf mobilen Geräten wie Smartphones einem besonders hohen Risiko ausgesetzt. Immer wieder gehen die Geräte verloren, werden gestohlen oder sind über falsch konfigurierte und unsichere Verbindungen angreifbar. So können die Zugänge zu Bank- und E-Mail-Konten, zu anderen geschäftlichen Daten und sozialen Netzwerken schnell in falsche Hände gelangen. Vorsorgliche Schutzmaßnahmen für Smartphones sind daher unerlässlich für die geschäftliche Nutzung. Insbesondere wenn Sie private Smartphones geschäftlich nutzen, sollten Sie besonders achtsam sein. Die Checkliste kann Ihnen dabei helfen.

Der Umgang mit Apps

Erst durch die Nutzung von Apps werden Smartphones zu „Alleskönnern“. Allerdings können Apps auch Viren oder Trojaner enthalten, die Ihre Daten ausspähen oder schädigen können.

- Benötigen Sie die App auch wirklich?
- „Kennen“ Sie den Anbieter?
- Gibt es Zertifikate oder Testberichte?

Zugriffskontrolle

Ein funktionierender Zugriffsschutz verhindert einen unbefugten Zugriff auf Ihre Daten, E-Mails, Adressen oder Telefonnummern.

- Wurde eine individuelle PIN für das Smartphone gewählt?
- Wurde eine eigene PIN für die SIM-Card vergeben?
- Wurde ggf. eine PIN für das Synchronisieren vergeben?
- Wurde das Smartphone ggf. von einem Experten (Administrator) für die sichere Anwendung von VPN oder E-Mail konfiguriert?
- Wurden sichere Passworte gewählt?
- Ist gewährleistet, dass die Bluetooth-Funktion bei Nichtnutzung deaktiviert ist?
- Ist gewährleistet, dass die WLAN-Funktion bei Nichtnutzung deaktiviert ist?

Schutz vor Viren und Trojanern

Ähnlich wie PCs und Notebooks sind auch Smartphones immer häufiger von Viren und Trojanern bedroht.

- Haben Sie die von den Herstellern bereitgestellten aktuellen Software-Updates zeitnah installiert?
- Haben Sie Schutzsoftware (Antivirus, Antispyware, etc.) auf den Smartphones installiert und haben Sie sie regelmäßig aktualisiert?

Datenverschlüsselung

Wenn Sie Ihre persönlichen Daten verschlüsseln, wird es für Unbefugte wesentlich schwieriger, Ihre Daten auszukundschaften oder zu manipulieren. Ist die umfassende Verschlüsselung aller Nutzerdaten der benutzten Smartphones voreingestellt?

- Bietet Ihr Netzbetreiber Security-Services für E-Mail bzw. Netzzugriff an?
- Stellen Sie eine Lösung für die Datenverschlüsselung (ggf. Software) für private Smartphones, die auch geschäftlich genutzt werden, zur Verfügung?

Schutz bei Verlust eines Smartphones

Smartphones können verloren gehen oder gestohlen werden.

- Werden die Daten Ihrer Smartphones bei mehrmaliger falscher PIN-Eingabe gelöscht?
- Haben Sie eine Lösung, die verlorengegangene oder gestohlene Smartphones aufspürt und bei Bedarf außer Betrieb setzen kann?

Weitere Informationen zum Thema Smartphone-Sicherheit finden Sie in unserem Flyer:

„Smartphones sicher nutzen - 10 Praxistipps für kleine und mittlere Unternehmen und das Handwerk“

Das Netzwerk Elektronischer Geschäftsverkehr

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr, in 27 über das Bundesgebiet verteilten regionalen Kompetenzzentren und einem Branchenkompetenzzentrum für den Handel, Mittelstand und Handwerk bei der Einführung von E-Business Lösungen. In dieser Zeit hat sich das Netzwerk mit über 30.000 Veranstaltungen und Einzelberatungen mit über 300.000 Teilnehmern als unabhängiger und unparteilicher Lotse für das Themengebiet „E-Business in Mittelstand und Handwerk“ etabliert. Das Netzwerk stellt auch Informationen in Form von Handlungsanleitungen, Studien und Leitfäden zur Verfügung, die auf dem zentralen Auftritt www.ec-net.de heruntergeladen werden können. Die Arbeit des Netzwerks wird durch das Bundesministerium für Wirtschaft und Technologie gefördert.

Sichere E-Geschäftsprozesse in KMU und Handwerk

Die Checkliste IT-Sicherheit wurde im Rahmen des Verbundprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerks Elektronischer Geschäftsverkehr (NEG) erstellt. Das Verbundprojekt wird vom Bundesministerium für Wirtschaft und Technologie (BMWi) unterstützt und soll helfen, in kleinen und mittleren Unternehmen mit verträglichem Aufwand die Sicherheitskultur zu verbessern. Hier werden insbesondere kleine und mittelständische Unternehmen sowie das Handwerk zu wichtigen Aspekten der Informationssicherheit sensibilisiert und praxisnah informiert. Alle Details finden Sie unter: www.kmu-sicherheit.de

TeleTrust – Bundesverband IT-Sicherheit e.V.

TeleTrust wurde 1989 gegründet, um verlässliche Rahmenbedingungen für den vertrauenswürdigen Einsatz von Informations- und Kommunikationstechnik zu schaffen. TeleTrust entwickelte sich zu einem bekannten Kompetenznetzwerk und trägt seit 2011 die Bezeichnung „TeleTrust – Bundesverband IT-Sicherheit e.V.“. Heute umfasst TeleTrust mehr als 130 institutionelle Mitglieder. Die Mitgliedschaft setzt sich aus Industrie, insbesondere mittelständischen Unternehmen, Bundesbehörden, Forschungseinrichtungen und thematisch verwandten Organisationen aus Deutschland, Österreich, der Schweiz, Belgien, Frankreich und Großbritannien zusammen, was die allgemeine Bedeutung des Themengebietes IT-Sicherheit unterstreicht. TeleTrust hat Gemeinnützigkeitsstatus. In Arbeitsgruppen zu aktuellen Themen der IT-Sicherheit und des Sicherheitsmanagements findet interdisziplinärer Erfahrungsaustausch statt. TeleTrust äußert sich zu technischen, politischen und rechtlichen Fragen, organisiert Veranstaltungen und Veranstaltungsbeteiligungen und ist Trägerorganisation der „European Bridge CA“ (Bereitstellung von Public-Key-Zertifikaten für sichere E-Mailkommunikation) sowie des Zertifikates „TeleTrust Information Security Professional“ (T.I.S.P.). Hauptsitz des Verbandes ist Berlin. TeleTrust ist Mitglied des European Telecommunications Standards Institute (ETSI). Weitere Informationen finden Sie unter: www.teletrust.de