



Komfortable Alleskönner

# Smartphone-Sicherheit

## Komfortable Alleskönner

Smartphones werden in Unternehmen zunehmend als klassische Endgeräte eingesetzt: E-Mails einschließlich sensibler Anhänge werden hierüber verschickt oder empfangen, Termine verwaltet und Kontaktdaten gepflegt. Auch sorgen verschiedenste Apps für ausreichende Abwechslung im Alltag. Die Grenzen zwischen beruflicher und privater Nutzung verschwinden. Immer mehr Unternehmen gehen dazu über, auch private Geräte für berufliche Zwecke einzusetzen – Stichwort Bring Your Own Device.

---

## Sicherheitsrisiken

Smartphones können verloren gehen oder werden entwendet. Sofern das Gerät vorher nicht entsprechend abgesichert worden ist, hat der neue Besitzer anschließend Zugriff auf alle sensiblen Informationen und kann unter Umständen sogar auf das Firmennetzwerk zugreifen.

Ein anderes großes Problem stellen die zahlreichen Apps dar, die oftmals auch für private Zwecke auf das Gerät geladen werden, ohne dass der Entwickler der App bekannt ist oder deren vollständige Funktionsweise: Apps können nicht nur auf sämtliche hinterlegten Kontaktdaten zugreifen, sondern haben potentiell Zugriff auf Fotos, Videos, Standortdaten oder Informationen auf der Speicherkarte. Dies betrifft nicht nur die klassische Malware, sondern auch reguläre Apps, die im Rahmen ihrer Funktionalität Informationen abgreifen und über Clouddienste verteilen.

Wir helfen Ihnen, den Einsatz von Smartphones sicher zu gestalten!



**direkte Ansprechpartner**



**verständlich**



**ganzheitliches  
Projektmanagement**



**transparent**

---

## Sicherheitskonzept

Angesichts derartiger Risiken ist es erforderlich, für den Einsatz von Smartphones ein Sicherheitskonzept zu erstellen und dieses adäquat umzusetzen. In diesem Zusammenhang stellen sich zumeist folgende Fragen:

- ? Sollen im Unternehmen überhaupt private Geräte zum Einsatz kommen oder ist die private Nutzung von unternehmenseigenen Smartphones gestattet?
- ? Welche Risiken müssen bei einer heterogenen Betriebssystemplattform betrachtet werden?
- ? Muss die App-Installation reglementiert werden?
- ? Welche technischen Maßnahmen sind – neben der Verschlüsselung und der Gerätesperrung – noch erforderlich?
- ? Wie kann ein sicherer Zugriff auf das Unternehmensnetzwerk erfolgen?
- ? Welche Einstellungen im Mobile Device Management sind sinnvoll?
- ? Wie werden die Mitarbeiter sinnvoll in das Sicherheitskonzept eingebunden?
- ? Bieten App-Container- oder Terminalserver die notwendige Sicherheit?

---

## Unsere Dienstleistung

Als IT-Sicherheitsexperten und lizenzierte ISO-27001-Auditoren stehen wir Ihnen mit unserer Kompetenz und Erfahrung zur Seite und unterstützen Sie bei der Erstellung und Umsetzung eines Sicherheitskonzepts für Smartphones. Zunächst ermitteln wir im Rahmen einer Ist-Analyse die speziellen Bedürfnisse und Rahmenbedingungen in ihrem Unternehmen, anschließend formulieren wir konkrete Handlungsempfehlungen in einem lösungsorientierten Sollkonzept.

---

**datenschutz nord GmbH****Hauptsitz Bremen**

Konsul-Smidt-Straße 88  
28217 Bremen  
Tel.: +49 (0) 421 69 66 32-0

office@datenschutz-nord.de  
www.datenschutz-nord-gruppe.de

**datenschutz süd GmbH****Hauptsitz Würzburg**

Wörthstraße 15  
97082 Würzburg  
Tel.: +49 (0) 931 30 49 76-0

office@datenschutz-sued.de  
www.datenschutz-nord-gruppe.de

**Weitere Niederlassungen** der datenschutz nord Gruppe siehe [www.datenschutz-nord-gruppe.de/standorte](http://www.datenschutz-nord-gruppe.de/standorte)