Smartphones im Geschäftsalltag

Arbeitsauftrag einsehen, per Foto Fragen klären, Material nachordern, Arbeitszeiterfassung per App statt Stundenzettel: Viele Betriebe nutzen inzwischen die Vorteile von Smartphones oder Tablets für ihre Auftragsabwicklung.

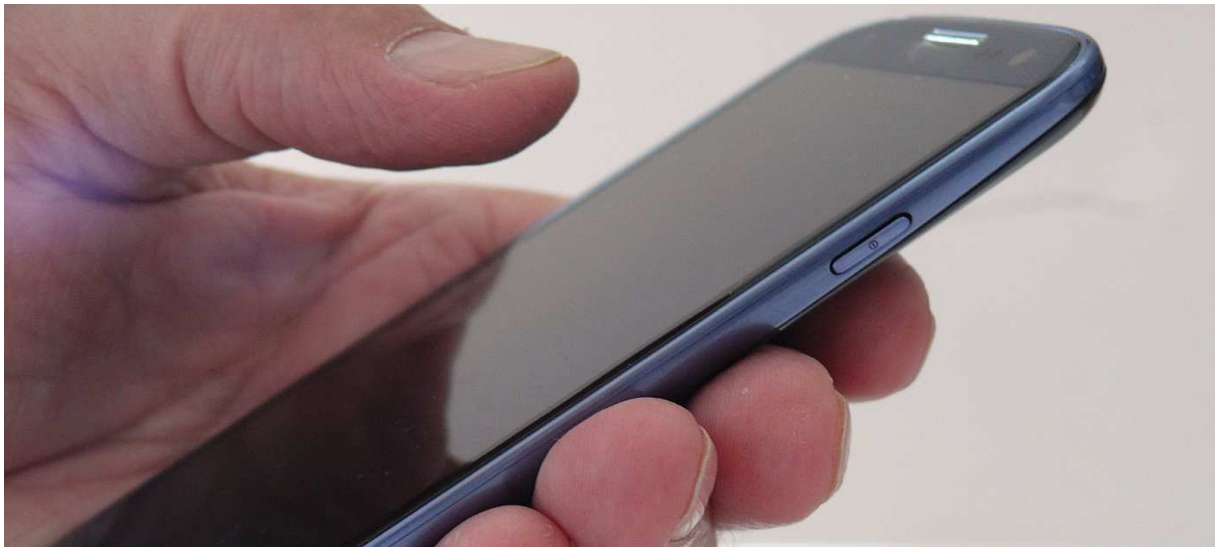

Foto: Lupo / pixelio.de

Diese einfache Kommunikation verführt aber auch dazu, die notwendige Sorgfalt zu vernachlässigen. Im betrieblichen Alltag geht es eben nicht um Privates und deshalb sollten Betriebe einige wichtige Aspekte berücksichtigen.

Je nach Ihrer eigenen Risikoanalyse gehören dazu der Schutz Ihrer betrieblichen Daten, die Wahl des „richtigen“ Messenger-Dienstes, der sensible Umgang mit Kundendaten, die Datenschutzrechte Ihrer Beschäftigten und die Smartphone-Nutzung Ihrer Auszubildenden.

Diese Information soll einige Hinweise geben, wie Sie Risiken bei der Nutzung von mobilen Endgeräten im Geschäftsalltag reduzieren können.

Messenger-Dienste

WhatsApp kennt jeder, aber im beruflichen Alltag ist dieser Messenger-Dienst für viele nicht mehr die erste Wahl. Das Auslesen und die unkontrollierbare Datenweitergabe an Facebook und der Server-Standort in den USA sind echte Negativpunkte.

Beim Einsatz betrieblicher Smartphones können Sie selber den Messenger-Dienst bestimmen und dafür sorgen, dass die gleiche Messenger-App auf allen mobilen Geräten installiert ist.

Es gibt inzwischen viele alterative Messenger-Dienste, wie z.B. *Signal, Threema* (kostenpflichtig), *Telegram, Wire-Messenger, Slack, Hip-Chat* und viele mehr.

Bei der Auswahl sollten Sie sich folgende Fragen stellen:

- Steht der Plattform-Server im EU-Raum oder den USA?
- Ist die gesamte Kommunikation Ende zu Ende verschlüsselt?
- Wird die App von Ihren betrieblichen Smartphones unterstützt?
- Können auch Tablets genutzt werden oder ist Mobilfunk notwendig?
- Sind andere Web-Dienste integrierbar?

IT-Sicherheit bei mobilen Geräten

Viele Handwerksbetriebe sind sich sicher, dass sie zu klein und uninteressant für Hackerangriffe sind. Das ist sicher richtig.

Die Gefahr für Ihre IT erwächst nicht aus individuellen Angriffen auf Ihr Unternehmen, sondern aus anonymen Massenangriffen mit Würmern oder Trojanern. Auch die Datensammlung durch Apps oder der Verlust der mobilen Endgeräte berührt Ihre IT-Sicherheit.

Folgende Grundsätze sollten Sie daher unbedingt beachten:

- Keine privaten Smartphones im Betrieb, weil Sie keinen Einfluss auf die Nutzung nehmen können.
- Achten Sie auf die Aktualität des Betriebssystems und der Apps.
- Richten Sie eine sichere Geräte- und Displaysperre ein.
- Verschlüsseln Sie das Gerät inklusiv Zusatzspeicherkarte.
- Installieren Sie möglichst wenige Apps, um Datensammlung zu reduzieren.
- Machen Sie regelmäßige Backups.
- Sorgen Sie für einen Notfallplan bei Verlust oder Diebstahl des Smartphones.

Datenschutz

Betriebe bedauern häufig, dass Sie keine Vorher-Nachher Fotos machen und auf ihre Internet-Seite stellen dürfen, weil Kunden das verweigern. Dies gilt für private wie gewerbliche Kunden gleichermaßen.

Bei der *Verletzung von Datenschutzvorgaben*, wie der informationellen Selbstbestimmung, können Abmahnkosten oder sogar Schmerzensgeldzahlungen auf Ihren Betrieb zukommen.

Gerade hat das Amtsgericht Bad Hersfeld über die Nutzung von WhatsApp geurteilt:

> *„Wer die andauernde Datenweitergabe zulässt, ohne zuvor von seinen Kontaktpersonen aus dem eigenen Telefon-Adressbuch hierfür jeweils eine Erlaubnis eingeholt zu haben, kann […] von den betroffenen Personen kostenpflichtig abgemahnt zu werden”*,

heißt es in dem Urteil.

Sie sollten also dringend dafür sorgen, dass alle Mitarbeiterinnen und Mitarbeiter eine *Datenschutzerklärung unterschreiben*, wie mit Kundendaten umzugehen ist. Dazu gibt es viele kostenfreie Muster im Internet, die Sie für Ihre Bedürfnisse anpassen können. Ihre Beschäftigten haben aber auch selber ein Anrecht auf informationelle Selbstbestimmung. Das sollte in der Datenschutzerklärung ebenfalls kommuniziert werden.

Smartphones in der Ausbildung

Auszubildende sind als „Digital Natives“ häufig besonders unbeeindruckt, was den Umgang mit ihren eigenen Daten angeht und wie die Schutzrechte Anderer gewahrt bleiben.

Kürzlich hat ein Azubi während einer Zwischenprüfung seine praktische Arbeit fotografiert und ins Netz gestellt. Dies könnte z.B. bei einer Gesellenprüfung dazu führen, dass alle Prüflinge wiederholen müssen.

Wenn eine Arbeit besonders gut gelungen ist, möchten die Auszubildenden diese vielleicht in ihrem Berichtsheft dokumentieren. Oder sie möchten ein Foto auf einem ihrer Accounts in den Social-Media veröffentlichen.

Das kann eine wunderbare Motivation für Ihre Auszubildenden sein. Sie sollten aber von betrieblicher Seite dafür sorgen, dass die schriftliche Zustimmung Ihrer Kunden eingeholt wird. In einer solchen Situation werden das nur wenige Kunden verweigern.

- Sensibilisieren Sie Ihre Auszubildenden für den Umgang mit Kundendaten.
- Wer kann durch die Art und Form der Information betroffen sein?
- Haben die Betroffenen der Veröffentlichung im Netz zugestimmt?

Ihre Ansprechpartnerin:

Anne Schütte
Beauftragte für Innovation und Technologie*
05121 162-129
anne.schuette@hwk-hildesheim.de

Wirtschaftsförderung
Handwerkskammer Hildesheim-Südniedersachsen
Braunschweiger Straße 53
31134 Hildesheim

Zentrale 05121 162-0
Telefax 05121 703432
Internet: http://www.hwk-hildesheim.de/

* Gefördert durch das Bundesministerium für Wirtschaft und Technologie aufgrund eines Beschlusses des Deutschen Bundestages

Stand: 04.07.2017