KOMPETENZZENTRUM
DIGITALES HANDWERK

DAS HANDWERK
DIE WIRTSCHAFTSMACHT. VON NEBENAN.

© Fotolia / paulfourk

Smartphones im Geschäftsalltag.

Kompetenzzentrum Digitales Handwerk - Schaufenster Nord

www.handwerkdigital.de

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

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. Diese vereinfachte Kommunikation birgt jedoch auch das Risiko, die notwendige Sorgfalt zu vernachlässigen, weshalb Betriebe einige wichtige Aspekte berücksichtigen sollten. Je nach Ergebnis der betrieblichen Risikoanalyse gehören dazu der Schutz der betrieblichen Daten, die Wahl des am besten geeigneten Messenger-Dienstes, der sensible Umgang mit Kundendaten, die Datenschutzrechte der Beschäftigten und die Smartphone-Nutzung der Auszubildenden.

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

Messenger-Dienste.

WhatsApp ist weit verbreitet. Die Nutzung im beruflichen Alltag ist jedoch als überaus kritisch anzusehen. Die unkontrollierbare Weitergabe insbesondere von Kontaktdaten wird aktuell intensiv diskutiert, da aus datenschutzrechtlichen Gründen WhatsApp-Nutzer alle ihre Kontakte um eine Einverständniserklärung bitten müssten. Ohne die Freigabe der Kontaktdaten funktioniert WhatsApp jedoch nicht bzw. kann ohne diese Option nicht installiert werden. Bei der Verletzung von Datenschutzvorgaben, wie der informationellen Selbstbestimmung, können Abmahnkosten auf Ihren Betrieb zukommen.

Vor Kurzem 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 werden",

Aktuell (Stand: Juli 2017) befindet sich ein „WhatsApp for Business" in der Entwicklung und wird bereits getestet. Ein verlässliches Datum steht noch nicht fest. Beim Einsatz betrieblicher Smartphones können Sie selbst den Messenger-Dienst bestimmen und dafür sorgen, dass die gleiche Messenger-App auf allen mobilen Geräten installiert ist. Es gibt inzwischen viele alternative 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:

- Gilt der europäische Datenschutz? (Steht der Plattform-Server in Europa oder in 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?

Die Auswahl einer Alternative zu WhatsApp entbindet jedoch nicht von der Verpflichtung, sich mit der Vereinbarkeit von Datenschutzbestimmungen und dem Verhalten des Messengers intensiv zu befassen.

IT-Sicherheit bei mobilen Geräten.

Viele Handwerksbetriebe sind sich sicher, dass sie uninteressant für Hackerangriffe sind. Die Gefahr für Ihre IT erwächst jedoch 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 berühren die Themenbreite der IT-Sicherheit.

Mittelstand-Digital

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Folgende Grundsätze sollten Sie daher unbedingt beachten:

- Keine privaten Smartphones im betrieblichen Einsatz, wenn 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.
- Nehmen Sie regelmäßige Backups vor.
- Sorgen Sie für einen Notfallplan bei Verlust oder Diebstahl des Smartphones.

Diese Tipps gelten generell für alle mobilen Endgeräte. Die Frage, ob Android oder z. B. IOS (Apple) sicherer ist, kann dahingehend beantwortet werden, dass bei IOS alle Daten grundsätzlich verschlüsselt sind, wogegen bei Android entsprechende Programme installiert werden müssen (Achtung: Bei der nachträglichen Installation können unverschlüsselte Daten verloren gehen!). Hinsichtlich Viren und anderer Schadprogramme sind für Android unterschiedliche Lösungen am Markt verfügbar. Für IOS hingegen gibt es keine Anwendung!

Empfehlung zum Datenschutz.

Es ist anzuraten, dass alle Mitarbeiterinnen und Mitarbeiter eine Datenschutzerklärung unterschreiben, in der geregelt ist, wie mit Kundendaten umzugehen ist. Diesbezüglich lassen sich zahlreiche kostenfreie Muster im Internet finden, die an die jeweiligen Bedürfnisse anpasst werden können. Auch die Beschäftigten selbst haben ein Anrecht auf informationelle Selbstbestimmung, wonach jeder selbst über die Weitergabe und Verwendung persönlicher Daten bestimmt. Das sollte in der Datenschutzerklärung ebenfalls kommuniziert werden.

Smartphones in der Ausbildung.

Insbesondere Auszubildende pflegen im Umgang mit mobilen Endgeräten eine gewisse Selbstverständlichkeit. Dennoch gelten auch hier die gleichen Regelungen. In der Ausbildung bestehen diesbezüglich zusätzliche Risiken durch diese „Digital Natives“:

In einem Fall fertigte ein Auszubildender während einer Zwischenprüfung ein Foto von seiner praktischen Arbeit an und stellte es ins Netz. Solche Situationen können beispielsweise bei einer Gesellenprüfung dazu führen, dass eine Prüfung mit einer neuen Aufgabe wiederholt werden muss. Eine digital erstellte Dokumentation zu einer handwerklichen Leistung, die bei einem Kunden vor Ort erbracht wurde, darf ebenfalls nicht ohne die ausdrückliche (am besten schriftliche) Genehmigung des Kunden in digitalen Medien zugänglich oder sogar sichtbar werden.

Daher gilt im Hinblick auf Auszubildende folgende Empfehlung:

- 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?

Autoren

Rainer Holtz
Kompetenzzentrum Digitales Handwerk – Schaufenster Nord
Bundestechnologiezentrum für
Elektro- und Informationstechnik e. V.
Donnerschweer Straße 184 | 26123 Oldenburg
Tel.: 0441 34092-280
E-Mail: r.holz@bfe.de

Werner Schmit
Kompetenzzentrum Digitales Handwerk – Schaufenster Nord
Bundestechnologiezentrum für
Elektro- und Informationstechnik e. V.
Donnerschweer Straße 184 | 26123 Oldenburg
Tel.: 0441 34092-280
E-Mail: w.schmit@bfe.de

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages