



Foto: © Cortado

### Von Julian Rother & Marian Lettow – ED Computer & Design GmbH & Co. KG

Empörung macht sich breit, wenn wir hören, dass schon wieder ein großer Datenschutzskandal aufgedeckt wurde. Das Thema Datensicherheit wird in Deutschland wahrscheinlich derzeit weltweit am sensibelsten behandelt. Unternehmen versuchen die vielen Datenschutzverordnungen und Gesetze in ihre Organisationsstruktur zu integrieren und lassen an dieser Stelle einen wichtigen Punkt völlig außer Acht: Bring Your Own Device – kurz BOYD – ist in den meisten kleinen und mittelständischen Unternehmen, aber auch großen Organisationen, heutzutage Gang und Gebe.

Das neue Smartphone, der Tablet-PC oder auch das eigene Notebook, private Hardwaregeräte werden

immer mehr in unseren Arbeitsalltag eingebaut. In unserer heutigen Gesellschaft wollen wir ständig mit Informationen versorgt werden. Ein Makler möchte beispielsweise ständig über die neuesten Anfragen per Email auf seinem Handy informiert werden, um eventuell noch unterwegs einen Besichtigungstermin mit einem Interessenten zu vereinbaren. Für den erfolgreichen Mitarbeiter ist ein normaler Arbeitstag mit acht Stunden schon lange kein Thema mehr. Denn wer im Job erfolgreich sein möchte, muss sich mit seinem Unternehmen identifizieren und auch außerhalb der normalen Arbeitszeit hinaus engagieren. Ein weiterer Vorteil neben der Erreichbarkeit und der verkürzte Bearbeitungszeit von

Anfragen potenziellen Immobilieninteressenten ist, dass Hardwaregeräte, die sich im Eigenbesitz der Mitarbeiter befinden dem Unternehmen zum einen kein Geld kosten und diese Geräte in den meisten Fällen auch viel besser gepflegt werden als das Unternehmens-Smartphone, das dem Mitarbeiter gestellt wird.

Das Engagement Ihrer Mitarbeiter in allen Ehren – die Verwendung von privaten mobilen Endgeräten ist mit dem deutschen Datenschutzgesetz jedoch nicht vereinbar. Als Geschäftsführer, und somit die verantwortliche Stelle, haben Sie keinerlei Kontrolle über die Verwendung der Daten außerhalb Ihrer Organisationseinheit, und Ihre Kunden geben Ihnen

ihre Daten mit dem Vertrauen, dass diese auch ausschließlich von Ihnen eingesehen werden können. Es stellt sich daher die dringende Frage, ob Ihr Unternehmen ein Sicherheitskonzept zum Thema „Bring Your Own Device“ erstellt und auch im Einsatz hat?

Haben Sie für Ihr Unternehmen die Entscheidung getroffen, dass beispielsweise Tablet-PCs oder Smartphones Ihrer Mitarbeiter auf Firmendaten zugreifen dürfen, darf BOYD nicht mehr nur als Synonym für die Verwendung eigener Endgeräte im Arbeitsalltag verstanden werden, sondern dient ab diesem Zeitpunkt als Organisationsrichtlinie für die Sicherheit Ihrer Unternehmensdaten. Über diese Richtlinien müssen die offenen Fragen geklärt werden- die sich unweigerlich in diesen Zusammenhang stellen.

Die wichtigsten Fragen dabei sind:

1. Wer hat Zugang zu den Geräten meiner Mitarbeiter?
2. Wer hat hierdurch direkten oder indirekten Zugriff auf Daten?
3. Wie kann ich mich vor Missbrauch schützen?

Als Lösungsansatz sollte daher durch die BOYD-Richtlinie ein geeignetes Sicherheitskonzept passend zur Ihrem Unternehmen erstellt werden. Softwarehersteller wie Kaspersky Labs bieten hier bereits komplette Lösungen zur Integration mobiler Endgeräte in eine bestehende Organisationseinheit. Diese beinhalten praktikable Lösungen zur Realisierung von:

- Zugang-/Zugriffssperren auch über die Ferne
- Verschlüsselungen
- Schutz der Privatsphäre

- Over the Air Management
- Virtuell Privat Network (VPN)
- SSL Zertifikate beim Empfang und Versand von Emails

Wichtig bei diesen Maßnahmen ist jedoch, dass im Unternehmen zum Schutz Ihrer Mitarbeiter ebenfalls eigene Richtlinien verfasst werden. Denn als Unternehmen haben Sie selbstverständlich rechtlich keine Erlaubnis die privaten Daten Ihrer Mitarbeiter einzu-



sehen oder Einfluss auf die Geräte außerhalb Ihrer Eigentumsverhältnisse zu nehmen.

Ein weiterer Lösungsansatz wäre die Sicherung von Unternehmensdaten in Cloudumgebung. Dabei werden Daten idealerweise gar nicht mehr lokal auf mobilen Endgeräten oder Notebooks abgelegt, sondern zentral verschlüsselt auf einem Server in einer sicheren Umgebung. Bei Diebstahl oder Verlust des Gerätes sind so keine großen Datenverluste zu befürchten.

Wichtig zu beachten sind hierbei wieder die deutschen Datenschutzgesetze – personenbezogene oder personenbeziehbare Daten müssen diesem Gesetz nach entsprechend besonders behan-

delt werden und dürfen nur auf Servern in Ländern mit entsprechendem Datenschutzniveau gespeichert werden. Schauen Sie daher deshalb immer an welchem Standort sich die Server befinden, hierzu sind Sie allein schon von gesetzlich verpflichtet (§11 BDSG).

Der Einführung von BYOD sollten Sie als Unternehmer durchaus kritisch gegenüberstehen, denn dieses Thema lässt sich nur sehr schwer mit dem hohen Standard an Datensicherheit in Deutschland vereinbaren. Der durchaus große Mehrwert für Ihr Unternehmen, der durch die Bereitstellung unternehmensinterner Daten auch außerhalb des Arbeitsumfeldes entsteht, kann schnell zu einem enormen Sicherheitsrisiko werden.

Um eine Entscheidung zu diesem Thema zu treffen, sollten Sie sich für Ihr Unternehmen und Ihre Mitarbeiter im Vorfeld eine Pro- und Contra Liste erstellen und über eine Checkliste die Sicherheitsanforderungen und Maßnahmen feststellen.

#### KONTAKT



Die Adresse von ED Computer & Design GmbH & Co. KG als QR Code, welcher mit einem Smartphone per QR Code Reader eingelesen werden kann.