Foto: Voßbein

Autor
Jörn Voßbein
Geschäftsführer und Seniorberater,
UIMC Dr. Vossbein GmbH & Co KG

consultants@uimc.at

Foto: Hoffmann

Autor
Tim Hoffmann
Geschäftsstellenleiter und Berater,
UIMC.austria

thoffmann@uimc.at

Risiken reduzieren

So schützen Sie Ihre Personaldaten

Reisekosten abrechnen, Urlaubsanträge bearbeiten, Bewerbungen prüfen – viele Routinearbeiten können Personaler mithilfe von Smartphones oder Tablets unterwegs erledigen. Die Vorteile der mobilen Personalarbeit liegen auf der Hand: erhöhte Verfügbarkeit, schnellere Reaktionszeiten, größere Flexibilität und damit einhergehend eine größere Zufriedenheit der Mitarbeiter. Doch die mobile Personalarbeit birgt auch Gefahren für Datenschutz und Informationssicherheit.

Viele Risiken der mobilen Personalarbeit sind grundsätzlich nicht neu: Neben Diebstahl und Verlust des Geräts sind es vor allem Schadprogramme und die unsachgemäße Handhabung, die zu einem Vertraulichkeitsverlust sensibler Mitarbeiterdaten führen können und damit auch datenschutzrechtlich relevant sind. Aber auch die Vermischung von privaten und dienstlichen Daten ist in diesem Zusammenhang nicht unproblematisch. Während es für Desktop- und mobile PCs (Laptops/Notebooks) schon umfangreiche und etablierte Verfahren und Produkte gibt, um die Datensicherheit zu gewährleisten, stehen diese für Smartphones und Tablets noch aus. Denn die zurzeit verfügbaren Smartphones sind in der Regel für Konsumenten und deren Bedürfnisse entwickelt und sollen eher durch Features und Benutzerfreundlichkeit als durch Sicherheit begeistern. Auf viele sicherheitstechnische Anforderungen wie zum Beispiel die Verschlüsselung des Datenspeichers, den Einsatz von Firewall und Virenscanner sowie komplexe Beschränkungen von Zugangsrechten haben die Smartphone-Hersteller bislang noch nicht oder noch unvollständig reagiert (Blackberry bildet hierbei teilweise eine Ausnahme). Dabei verlangt das Datenschutzgesetz (§ 14 DSG 2000) entsprechende „Datensicherheitsmaßnahmen". Umso wichtiger ist es, dass Unternehmen, die mobile Personalarbeit einführen oder erlauben möchten, entsprechende Regelungen in Form von Dienstanweisungen oder Betriebsvereinbarungen sowie technische Vorkehrungen zur IT-Sicherheit treffen, die die Sicherheitsrisiken mindern, wenn sie sie auch nicht eliminieren können.

Konfiguration und Administration durch IT

Unternehmen sollten für die mobile Personalarbeit nur Smartphones einsetzen, die durch die IT-Abteilung (oder eine andere entsprechende Abteilung) zentral konfiguriert wurden, um sowohl ein einheitliches als auch entsprechend den Firmenanforderungen ausreichendes Sicherheitsniveau zu erreichen. So sollten sie die nachfolgenden Empfehlungen nicht nur in Form einer organisatorischen Anweisung, sondern auch technisch – soweit möglich – durch die IT so umsetzen, dass sie durch den Nutzer nicht verändert werden können. Die Nutzungsvereinbarung sollten den Mitarbeitern Jailbreaking (Entfernen von Nutzungsbeschränkungen), Modding (Modifikation, technische Veränderungen) oder Ähnliches untersagen, also Eingriffe in das Betriebssystem, um etwa Software zu installieren, die vom Hersteller nicht vorgesehen ist. Beide Maßnahmen sind auch – oder insbesondere – bei einer „Bring your own Device"-Strategie zu treffen (BYOD), bei der Mitarbeiter ihre privaten Endgeräte dienstlich nutzen dürfen.

Ferner sollte IT auf dem Smartphone Sicherheitseinstellungen wie Speicher- und

Übermittlungsverschlüsselung sowie eine Zugangsbeschränkung durch Passwort oder PIN vornehmen, die der Nutzer nicht mehr verändern darf. Der Einsatz von Virenscannern und von sogenannten Mobile-Device-Management-Systemen (MDM) zur zentralen Verwaltung von Smartphones ist genauso zu empfehlen wie die Einbindung in die allgemeine IT-Sicherheitsstrategie. Das Sicherheitsniveau beim Einsatz von Smartphones sollte sich somit möglichst wenig von dem unterscheiden, das Desktop- und mobile PCs bieten.

Apps kontrollieren

Es gibt eine Vielzahl von Apps, die Schadprogramme, zum Beispiel Viren, enthalten, die auf dem Smartphone befindliche Daten (zum Beispiel das interne Adressbuch oder die E-Mails) automatisch mit Internetservern synchronisieren oder das Smartphone anderweitig manipulieren. Nutzer sollten daher Apps nur aus „offiziellen" Quellen wie etwa Google Play Store oder Apple Appstore herunterladen.

Unternehmen können dem Nutzer eine Übersicht von zulässigen Apps an die Hand geben. Nicht auf der Liste befindliche Apps sind dann vor dem Herunterladen zunächst durch die IT-Abteilung zu kontrollieren. An dieser Stelle sei auch angemerkt, dass im Rahmen der mobilen Personalarbeit gegebenenfalls von der Standardanwendung von § 17 DSG 2000 abgewichen wird, wenn zusätzliche, von der innerbetrieblichen Software zur Personalverwaltung abweichende Apps genutzt werden, und somit eine Meldung im Datenverarbeitungsregister erforderlich wird.

Synchronisieren von Daten

Auf dem Smartphone befindliche E-Mails, Termine und Adressen dürfen Mitarbeiter nur mit unternehmenseigenen Systemen synchronisieren. Dabei muss gewährleistet sein, dass die Mitarbeiter nur die von der IT bereitgestellten Services und Programme nutzen. Frei verfügbare, aber nicht vom Unternehmen freigegebene Internet-Ablagedienste, wie zum Beispiel Dropbox, sollten die Beschäftigten nicht verwenden dürfen. Unternehmen sind daher gut beraten, dies in Nutzungsvereinbarungen festzulegen und eine technische Restriktion durch MDM-Systeme einzuführen. Ferner bieten viele Apps von sozialen Netzwerken die Möglichkeit, nach „Freunden" zu suchen, indem sie das Adressbuch auf dem Smartphone mit den Daten des sozialen Netzwerks abgleichen. Bei einem dienstlichen Smartphone befinden sich aber auch Geschäftspartner, Kollegen oder Bewerber im Adressbuch. Die Nutzung einer solchen Synchronisierung birgt massive datenschutzrechtliche Probleme und ist unter allen Umständen zu unterlassen.

Gespeicherte Daten schützen

Um unberechtigte Zugriffe auf die gespeicherten Daten zu verhindern, sollte das Smartphone durch ein Passwort geschützt sein, das mindestens eine vierstellige PIN umfasst. Höhere Komplexitätsanforderungen sind zwar durchaus sinnvoll, aber technisch oftmals nur mit deutlich schlechterer Handhabung realisierbar. Darüber hinaus sollte sich der Passwortschutz automatisch aktivieren, wenn das Gerät eine definierte Zeit lang inaktiv ist. Im Rahmen der Konfiguration durch IT ist es sinnvoll, verschlüsselte Tresore oder Container auf dem Gerät einzurichten, um Daten abzulegen.

Der beste Schutz ist jedoch, möglichst wenige vertrauliche Daten auf dem Mobiltelefon zu speichern. Denkbar ist daher auch, dass die Nutzer ihre E-Mails und andere Daten nur mittels geschützter Terminalsitzung, also ohne lokale Speicherung auf dem Gerät, einsehen können. Der Verlust eines Geräts würde somit nicht automatisch zu einem Verlust der Vertraulichkeit der darauf gespeicherten Daten führen.

Telefonieren in der Öffentlichkeit

Ein zwar nicht smartphonespezifisches, aber für die mobile Personalarbeit dennoch wichtiges datenschutzrechtliches Thema ist das Telefonieren in der Öffentlichkeit. Gerade im Rahmen der Personalarbeit werden häufig vertrauliche Themen diskutiert. Diese Gespräche sollten die HR-Mitarbeiter an öffentlichen Plätzen wie Flughäfen oder Bahnhöfen, Zügen oder oder Cafés so führen, dass keine Rückschlüsse auf die betroffene Person möglich sind. Darüber hinaus sollten sie auch

NUTZEN UND RISIKEN MOBILER PERSONALARBEIT

	Nutzen / Vorteile mobiler Personalarbeit	**Risiken** (mit regelmäßig einhergehenden Gesetzesverstößen)
1.	Hohe Flexibilität und leichte Verfügbarkeit von Informationen	Verlust von Geräten und vertraulichen Daten
2.	Bessere Organisation von Arbeits- und Privatleben	Vermischung von privaten und dienstlichen Daten sowie Nutzung durch betriebsfremde Personen
3.	Ortsunabhängiges Arbeiten	Fehlende Sozialkontrolle
4.	Schnelle Reaktionszeit	Vorschnelle, unüberlegte Reaktion auf E-Mails
5.	Einfache Bedienung und hohe Nutzerfreundlichkeit	Ungenügende oder fehlende Sicherheitsfunktionen (da diese die Nutzerfreundlichkeit reduzieren können)
6.	Viele (kostengünstige) Zusatzprogramme (Apps)	Hoher Anteil unsicherer und Schadcodes beinhaltender Apps sowie ungenügende Transparenz der Funktionsweisen
7.	Dezentrale Beschaffung der Geräte durch Mitarbeiter (BYOD)	Ungenügende Kontrolle durch fehlende zentrale Administrierbarkeit und mangelnde Beeinflussung von Sicherheitsanforderungen
8.	Zufriedenheit der Mitarbeiter durch individuelle Geräteauswahl (BYOD)	Heterogene Geräte- und Systemlandschaft mit erhöhtem Administrationsaufwand und gegebenenfalls sinkendem Sicherheitsniveau

keine vertraulichen Nachrichten auf Anrufbeantwortern hinterlassen.

Schnittstellen ausschalten

Um das Smartphone vor fremdem Zugriff zu schützen, muss auch die (kabellose) Datenübertragung geregelt sein. Die Bluetooth- oder Infrarot-Schnittstelle, aber auch die Ortungsfunktion sollten ausschließlich für die Dauer der Nutzung aktiviert werden. Sinnvoll sind sie nur zur Synchronisation von Dateien zwischen Handy und Notebook, während der Verbindung des Mobiltelefons mit der Freisprechanlage im Auto oder bei der mobilen Navigation.

Auch sollte die Nutzungsvereinbarung Regeln enthalten zum Umgang mit öffentlichen Netzwerken beziehungsweise Hotspots, also öffentlichen drahtlosen Internetzugängen. Am sichersten ist es, deren Nutzung zu verbieten, da diese unverschlüsselt oder manipuliert sein können.

Was tun bei Geräteverlust?

Die Nutzungsvereinbarung muss den Mitarbeiter verpflichten, das Smartphone nicht unbeaufsichtigt zu lassen und stets mit sich zu führen. Da jedoch auch bei gewissenhaftem Gebrauch ein Smartphone abhandenkommen kann, ist sicherzustellen, dass der Verlust möglichst schnell der IT-Abteilung gemeldet wird. Die IT-Mitarbeiter können das Gerät dann fernlöschen (Remote Wipe), die Synchronisierung von E-Mails stoppen oder den Fernzugang über das Virtual Private Network (VPN, persönlicher Zugang in ein Firmennetzwerk) sperren. Eine Verlustmeldung trifft jedoch oftmals verzögert in der IT-Abteilung ein, da der Nutzer hofft, „das Gerät schon irgendwo noch wiederzufinden". Es ist daher empfehlenswert, den Zeitpunkt der Verlustmeldung genau zu definieren und den Mitarbeitern eindringlich zu vermitteln, dass und warum eine rasche Meldung wichtig ist.

Private Nutzung regeln

Hat der Arbeitgeber die private Nutzung von dienstlichen Smartphones erlaubt (oder nicht explizit verboten), so ist der Zugriff durch die IT-Abteilung auf das Gerät beziehungsweise auf die Daten eng gesteckt. Eine zeitnahe Fernlöschung im Falle des Geräteverlusts etwa ist schwierig umsetzbar, wenn der Mitarbeiter seine persönlichen Daten nicht löschen lassen möchte. Unternehmen sollten zudem unbedingt die Nutzung durch Familienangehörige untersagen.

Besondere Regelungen sind im Rahmen einer BYOD-Strategie zu treffen, da bislang – auch hier bildet gegebenenfalls Blackberry eine Ausnahme – kaum sinnvolle Lösungen zur technischen Trennung von dienstlicher und privater Nutzung von Smartphones existieren. Empfehlenswert ist es, auf dem privaten Smartphone eine verschlüsselte Sandbox einzurichten, sodass geschäftliche von privaten Daten und Anwendungen getrennt werden, damit beispielsweise die private Facebook-App nicht auf das geschäftliche Adressbuch zugreifen kann.

Fazit

Die mobile Personalarbeit ist aufgrund der technisch wenig fortgeschrittenen Sicherheitslösungen bei den Smartphones sowie durch die Vermischung von privater und dienstlicher Nutzung der Geräte nicht unproblematisch. Daher ist es unumgänglich, dass Unternehmen, die mobile Personalarbeit ermöglichen wollen, nicht nur verbindliche Richtlinien schaffen, sondern die Mitarbeiter auch für die sicherheitstechnisch und datenschutzrechtlich relevanten Themen sensibilisieren. Denn viele notwendige Maßnahmen sind – mangels technischer Lösungen noch stärker als bei anderen Geräten – durch den Mitarbeiter selbst umzusetzen.

Auch ist der Nutzer grundsätzlich selbst ein Risikofaktor, der sich durch die fehlende Sozialkontrolle im Rahmen der mobilen Arbeit gegebenenfalls verschärft. Die Umsetzung ist ohnehin in vielen Fällen nur schwer durch strukturierte oder automatisierte Kontrollen zu prüfen, sodass letztendlich die Vorgesetzten gefragt sind, etwaigem Fehlverhalten durch Wachsamkeit entgegenzuwirken. Neben Präsenzschulungen durch die IT-Abteilung oder den Datenschutzbeauftragten sind E-Learning-Lösungen denkbar, mit denen eine kontinuierliche Sensibilisierung erreicht werden kann, da die Informationen laufend aktualisiert werden.