Mobiles Arbeiten

- datenschutzgerecht gestaltet -

Orientierungshilfe und Checkliste

Landesbeauftragter für den Datenschutz Niedersachsen

Vorbemerkungen

In Wirtschaft und Verwaltung werden zunehmend verschiedene Formen mobilen Arbeitens erprobt, um ortsunabhängig auf aktuelle Daten zugreifen und eMail-Dienste nutzen zu können. Unter mobilem Arbeiten wird im allgemeinen eine berufliche Ausübung verstanden, die von außerhalb unter Nutzung von Telekommunikation erfolgt. In der Praxis wird mobiles Arbeiten häufig als Ergänzung der herkömmlichen Büroarbeit eingesetzt. Auf Dienst- und Geschäftsreisen oder bei anderen temporären Tätigkeiten außerhalb der gewohnten Arbeitsumgebung bietet die mobile Kommunikation hier neue Möglichkeiten.

Im Gegensatz zur klassischen Telearbeit wird bei mobilem Arbeiten besonderes Gewicht auf große räumliche Beweglichkeit gelegt. Die Unterscheidung ist wichtig, da bei Telearbeit eine vollständige Büroarbeitsplatzumgebung abgebildet wird, für die besondere arbeitsrechtliche und ergonomische Bestimmungen einzuhalten sind. Mobile Arbeitsplätze hingegen dienen als zeitlich befristete Ergänzung zum Arbeitsplatz im Unternehmen oder der Behörde und ersetzen diesen Arbeitsplatz nicht. Ihre technischen und organisatorischen Ausprägungen können dabei höchst unterschiedlich sein. Bei mobilem Arbeiten wie auch bei Telearbeit wird zunehmend angestrebt, dass die Mitarbeiterinnen und Mitarbeiter in ihrer externen Arbeitsumgebung ähnliche oder gar gleiche Strukturen und Funktionalitäten vorfinden, wie sie von ihrem Büroarbeitsplatz her bekannt sind.

Die Orientierungshilfe weist auf Gefahren und Risiken bei Aufbau und Einsatz von mobilen Arbeitsplätzen hin und gibt konkrete Empfehlungen für technische und organisatorische Sicherungsmaßnahmen. Die Orientierungshilfe will

- Geschäfts- und Behördenleitung,
- Personalleitung und Personalvertretung sowie
- Organisations- und DV-Leitung

in die Lage versetzen, die erforderliche Vorabkontrolle vorzunehmen und ein Konzept für einen datenschutzgerechten Einsatz mobiler Arbeitsplätze zu finden.

Grundüberlegungen

Mobiles Arbeiten tritt derzeit in verschiedenen Ausprägungen auf, die sich im wesentlichen durch die Art der Telekommunikation unterscheiden. Möglich sind hier drahtgebundene oder drahtlose Telekommunikation; der Schwerpunkt dieser Orientierungshilfe liegt auf einer drahtgebundenen Kommunikation. Sollten zu einem späteren Zeitpunkt Erfahrungen zur drahtlosen Übertragung vorliegen, wird darauf in einer Ergänzung besonders hingewiesen.

Für die technische Realisierung des Zugriffs auf zentral vorgehaltene Informationen werden überwiegend Möglichkeiten genutzt, wie sie teilweise auch bei Telearbeitsplätzen zum Einsatz kommen:

- **Informationsaustausch via E-Mail über das Internet**

  Der Nutzer greift zum Datenaustausch über einen Access-Provider auf das Internet zu. Von einen Mail-Account aus werden Anfragen oder Inhalte als E-Mail und E-Mail-Anlagen über das Internet übertragen. Bei diesem Verfahren können Daten leicht auch an Externe gelangen oder im öffentlichen Internet mitgehört werden.

- **Remote-Access zu einer Workstation oder einem Server**

  Der Nutzer wählt sich über eine Modemverbindung auf seinen PC oder einen speziellen Server in der Organisation ein. Von diesen Geräten aus erhält er Zugriff auf das lokale Netzwerk und die sonstigen Ressourcen der Organisation. Dadurch hat er von zu Hause aus annähernd dieselben Zugriffsrechte (z.B. auch E-Mail), als wenn er selbst in der Firma an seinem Arbeitsplatz wäre. Die Administration erfolgt durch den Administrator der Organisation in enger Zusammenarbeit mit dem mobilen Arbeiter.

- **Remote-Access zu einem Terminal-Server**

  Der Mitarbeiter baut über öffentliche Kommunikationsnetze eine gesicherte Verbindung zu einem zentralen Rechner in seiner Arbeits- oder Dienststelle auf, der Terminal-Server-Dienste bereitstellt. Dieser Server ist einerseits in das Firmen- oder Dienststellen-Netzwerk integriert, ist auf einer getrennte Netzwerkschnittstelle jedoch auch von außen zu erreichen. Der Terminal Server übernimmt die komplette Verarbeitung aller Daten und stellt dem externen Mitarbeiter eine vollständige Arbeitsumgebung bereit, die mit der Installation im lokalen Netzwerk identisch sein kann. Die Datenhaltung erfolgt ausschließlich auf den zentralen Komponenten; die Administration des Gesamtsystems einschließlich der Anwendungen erfolgt ausschließlich zentral. Da lediglich Bild- bzw. Bedienungsinformationen über die öffentlichen Netze übertragen werden ist die Sicherheit bei diesem Verfahren deutlich höher; darüber hinaus bieten einige der am Markt verfügbaren Produkte ein zusätzliche Verschlüsselung der Daten an.

Die aufgeführten Kommunikationsverfahren sind nicht abschließend, weitere technische Ausgestaltungen sind möglich. Erst durch die Analyse der Gefahren und Risiken kann eine individuell geeignete Lösung erarbeitet werden.

Das Datenschutzrecht

Für mobiles Arbeiten im Rahmen eines Arbeits- oder Dienstverhältnisses trägt grundsätzlich der Arbeitgeber die datenschutzrechtliche Verantwortung. Dabei ist für Stellen der Wirtschaft (nicht-öffentliche Stellen) das Bundesdatenschutzgesetz (BDSG) und für öffentliche Stellen in Niedersachsen das Niedersächsische Datenschutzgesetz (NDSG) anzuwenden.

Nach § 9 BDSG bzw. § 7 NDSG haben Daten verarbeitende Stellen die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um eine datenschutzgerechte Verarbeitung personenbezogener Daten sicherzustellen. Der Aufwand für die Maßnahmen muss unter Berücksichtigung des Standes der Technik in einem angemessenen Verhältnis zu dem angestrebten Zweck stehen. Die Datensicherung kann dann als wirksam angesehen werden, wenn die getroffenen Maßnahmen in ihrer Gesamtheit einen hinreichenden Schutz der Daten vor Missbrauch leisten. Sicherungsziele sind:

- Gewährleistung der Vertraulichkeit der Daten,
- Sicherstellung der Integrität der Daten,
- Gewährleistung der Authentizität der Daten,
- Gewährleistung der Authentifikation von Benutzern,
- Gewährleistung der sicheren Zustellung,

- Sicherstellung der Verfügbarkeit,
- Sicherstellung der Revisionsfähigkeit.

Erfolgt eine Verarbeitung personenbezogener Daten durch Mitarbeiter auf der Basis von Werkverträgen in der Privatwohnung oder in Nachbarschafts- oder Satellitenbüros, unterliegt diese Tätigkeit in der Regel den Vorschriften der Datenverarbeitung im Auftrag (§ 11 BDSG bzw. § 6 NDSG). Ein solcher Mitarbeiter darf die Daten nur nach den Weisungen des Auftraggebers verarbeiten und nutzen. Auch hier bleibt der Auftraggeber für die Einhaltung datenschutzrechtlicher Vorschriften verantwortlich. Dies gilt nicht, sobald dem externen Mitarbeiter eine rechtliche Zuständigkeit für die Aufgabe zugewiesen worden ist (sog. Funktionsübertragung).

Für alle Formern mobilen Arbeitens sind Kontrollmöglichkeiten nicht nur durch den Arbeitgeber, sondern auch durch den internen Datenschutzbeauftragten (§§ 36, 37 BDSG bzw. § 8 NDSG), den Landesbeauftragten für den Datenschutz (§ 22 NDSG) bzw. die Aufsichtsbehörde für die Datenverarbeitung im nichtöffentlichen Bereich (§ 38 BDSG) zu gewährleisten. Hierfür muss ein Zugang zum häuslichen Arbeitsplatz gesichert sein. Dazu bedarf es wegen der Unverletzlichkeit der Wohnung jedoch der ausdrücklichen Einwilligung der betroffenen Beschäftigten. Dies muss zur Voraussetzung für die Ausübung mobiler Arbeit erklärt werden. Erfolgt der Widerruf einer solchen Einwilligung, ist die Möglichkeit zu mobilem Arbeiten sofort aufzuheben.

Gefahren- und Risikoanalyse

Mobiles Arbeiten in Wirtschaft und Verwaltung schafft neben vielen Vorteilen auch Gefahren und Risiken für die erklärten Sicherungsziele. Konkrete Gefahren sind z.B. der unkontrollierte Einsatz von Betriebsmitteln, die fehlerhafte Administration von Zugangs- und Zugriffsberechtigungen, Schadprogramme (Viren, Würmer, etc.), der Missbrauch von Fernwartungszugängen, die Nutzung der IuK-Technik durch unbefugte Personen und das Eindringen in Kommunikationsnetze. Die Auftraggeber sind verpflichtet, vor der Entscheidung über den Aufbau und die technische Ausgestaltung von mobilen Arbeitsplätzen zu prüfen, ob und in welchem Umfang mit der gewählten Form mobilen Arbeitens wegen der Art der zu verarbeitenden Daten oder der Verwendung neuer Technologien Gefahren für die Rechte der Betroffenen verbunden sind (Art. 20 EU-Datenschutzrichtlinie bzw. § 7 Abs. 3 NDSG). Arbeitsplätze für mobiles Arbeiten dürfen danach nur eingerichtet werden, soweit derartige Gefahren durch technische oder organisatorische Maßnahmen wirksam beherrscht werden können.[1]

Gerade der Informationsaustausch via E-Mail über das Internet und der Remote-Access zu einer Workstation oder einem Server im LAN eines Unternehmens oder einer Behörde haben eine Reihe organisatorischer und sicherheitstechnischer Schwachstellen, denen durch geeignete Maßnahmen begegnet werden muss. Beide Verfahren des Informationsaustauschs zwischen zentraler Organisation und den externen Mitarbeitern basieren auf dem Prinzip des Datenaustauschs; unabhängig vom hierfür verwendeten Medium. Die Transportphase erfordert umfangreiche Absicherungen, die eine unbefugte Kenntnisnahme der Informationen ebenso verhindern wie Manipulationen an den Informationsinhalten ausschließen.

[1] Orientierungshilfe „Vorabkontrolle“ des LfD Niedersachsen

Durch den Einsatz von Terminal-Server-Technik lassen sich die vorstehend genannten organisatorischen und sicherheitstechnischen Probleme erheblich einfacher lösen. Der wesentliche Unterschied zu den vorgenannten Punkten ist, dass die Daten nicht transportiert werden müssen, sondern den Zugang auf eine andere technische Weise realisiert wird. Über den Terminal-Server wird ein Fernzugang zu Daten und Ressourcen einer Organisation ermöglicht, ohne das die Daten den geschützten Bereich des lokalen Netzwerkes verlassen müssen.

Hierzu wird in der Organisation ein Server installiert, auf dem intern alle Programme ablaufen und der für den externen Nutzer als Arbeitsplatz-PC fungiert. Dazu werden die Steueranweisungen in Form von Tastatur- und Maus-Eingaben des externen Nutzers vom Terminal-Server empfangen und die Bildschirm-Darstellung der gewohnten Nutzeroberfläche an den externen Nutzer gesendet. Die Übertragung dieser Informationen wird, abhängig vom eingesetzten Produkt, bereits protokollseitig verschlüsselt, so dass fremde Kenntnisnahme oder Manipulation praktisch ausgeschlossen werden kann.

Für den Zugriff auf den Terminal-Server wird auf dem externen Endgerät (PC, Notebook, etc.) eine sogenannte Clientsoftware verwendet, die für die Kommunikation mit dem Terminal-Server sorgt. Wird anstelle eines vollwertigen PC oder Notebooks ein sogenannter Thin-Clients eingesetzt, bietet dies zusätzlichen Schutz. Der Thin Client bietet lediglich die Anschlussmöglichkeiten für Netzwerk, Monitor, Tastatur und Maus, besitzt hingegen aber keine Festplatte oder andere Laufwerke, auf denen Daten gespeichert oder von denen Daten aufgerufen werden können.

Der Bandbreitenbedarf der Übertragungsprotokolle variiert je nach dem eingesetzten Produkt, ist aber grundsätzlich recht bescheiden; eine 64 kBit/s ISDN-Leitung ist i.d.R. ausreichend. Damit ist eine nahezu universelle Einsetzbarkeit möglich, die für eine Übertragbarkeit der Musterlösung sehr wichtig scheint.

Trotz der gesicherten Übertragung der Bild- und Steuerungsinformationen ergibt sich beim mobilen Arbeiten auch beim Einsatz der Terminal-Server-Technik eine Reihe von Problemen; diese liegen in erster Linie in einer sicheren Authentifikation des mobilen Clients. Soweit möglich sollten Call-Back-Verfahren genutzt werden, um eine Authentifikation der Verbindung zu erreichen. Aber gerade bei wechselnden Rufnummern (z.B. aus verschiedenen Hotels) ist dies nur schwer oder überhaupt nicht administrierbar. Aus diesem Grund ist eine sichere, möglichst nutzerfreundliche Authentifikation des externen Mitarbeiters ein wesentlicher Punkt eines erfolgreichen Sicherheitskonzeptes. In Abhängigkeit von eingesetzten Übertragungsweg (direkte Telekommunikationsleitung / ISDN-Einwahl oder Nutzung des Internets) ist zudem zu prüfen, ob eine schlichte Protokollverschlüsselung ausreichend ist, oder ob eine weitere Absicherung erforderlich sein könnte.

Technische und organisatorische Maßnahmen

Eine ausreichend sichere Form mobiler Arbeit wird erreicht, wenn die getroffenen technischen und organisatorischen Maßnahmen in ihrer Gesamtheit einen ausreichenden Schutz bieten. Art und Umfang der notwendigen Sicherungsmaßnahmen richten sich nach der Sensibilität der verarbeiteten Daten und nach der jeweiligen technischen Anbindung des mobilen Arbeitsplatzes.

Neben dieser Checkliste können Sie zur datenschutzgerechten Ausgestaltung mobiler Arbeitsplätze weitere datenschutzrelevante Rechtsvorschriften, Empfeh-

lungen, Orientierungshilfen, Checklisten sowie sonstige Materialien unter der Internetadresse www.lfd.niedersachsen.de finden bzw. herunterladen. Darüber hinaus bietet auch das IT-Grundschutzhandbuch[2] wertvolle Hilfen zur Grundsicherung mobilen Arbeitens unter Nutzung zentraler IT-Strukturen. Eine Übersicht der Online Quellen finden Sie weiter unten in dieser Orientierungshilfe.

Handlungsempfehlungen

Aus datenschutzrechtlicher Sicht überwiegen die Vorteile der Terminal-Server-Lösung. Die anfallenden Daten verlassen nicht den geschützten Bereich des Unternehmens oder der Behörde. Bei Einsatz eines Thin Clients können zudem keine Daten beim Anwender gespeichert werden, was Fragen der lokalen Datenverschlüsselung und –sicherung entbehrlich macht. Auch muss der mobil Arbeitende keine abweichenden Benutzerrechte erhalten, um mit einem Terminal-Server arbeiten zu können.

Die Nachteile einer Terminal-Server-Lösung sind nicht datenschutzrechtlicher Natur, sollten aber grundsätzlich bei der Planung eines Telearbeitsplatzes berücksichtigt werden. Bei Ausfall der Terminalservers oder der Kommunikationsverbindung zwischen Terminalserver und Endgerät ist ein Arbeiten nicht mehr möglich. Dies gilt insbesondere bei Einsatz eines Thin Clients. Trotz guter Performanz ist eine Nutzung von Multimedia-Anwendungen ggfs. nur eingeschränkt möglich und sollte vorab getestet werden.

Insgesamt wird durch die Terminal-Server-Lösung ein hohes Maß an Sicherheit erreicht, die zudem von zentraler Stelle aus gut zu administrieren ist. Die Terminal-Server-Lösung ist auch im besonderen geeignet, um Telearbeitsplätze datenschutzgerecht zu gestalten. Wenn mobile Arbeitsplätze nicht ausreichend durch technische und organisatorische Maßnahmen gesichert werden können, muss auf ihren Einsatz bei der Verarbeitung personenbezogener Daten verzichtet werden.

Online Quellen:

Landesbeauftragter für den Datenschutz Niedersachsen	www.lfd.niedersachsen.de
Virtuelles Datenschutzbüro	www.datenschutz.de
Bundesamt für Sicherheit in der Informationstechnik (BSI)	www.bsi.bund.de

[2] Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Grundschutzhandbuch, 2002

Checkliste

Die folgende Checkliste soll eine Hilfestellung für die Erarbeitung datenschutzgerechter Lösungen bei der Einrichtung von mobilen Arbeitsplätzen leisten. Sie konzentriert sich auf die Gesichtspunkte des technisch-organisatorischen Datenschutzes. Die Checkliste unterteilt folgende Bereiche:

- **Sicherheit des mobilen Systems**

  Die Frage nach angemessenen Datensicherungsmaßnahmen stellt sich verstärkt bei mobilen Computern. Schon bei der Anschaffung der Geräte sollte auf eine Sicherheitsausstattung Wert gelegt werden. Mindestanforderungen an den mobilen Rechner sind zu definieren.

- **Sichere Kommunikation zwischen mobilem Arbeitsplatz und Arbeitsstelle**

  Da die Kommunikation über öffentliche Netze geführt wird, sind besondere Sicherheitsanforderungen für die Kommunikation zwischen mobilem Arbeitsplatz und Arbeitsstelle zu erfüllen.

- **Sicherheit des Kommunikationsrechners der Arbeitsstelle**

  Der Kommunikationsrechner stellt eine öffentlich zugängliche Schnittstelle dar, über die der mobile Arbeiter Daten der Arbeitsstelle nutzen kann. Hier ist ein Missbrauch durch Dritte zu verhindern.

Zur Beantwortung der Checklisten-Fragen wird es in der Regel ausreichen, jeweils anzukreuzen

- Erfüllt
- Nicht erfüllt
- Trifft nicht zu.

Diese Basisantworten können im Bedarfsfall durch kurze Erläuterungen in dem Feld Bemerkungstext ergänzt werden. Auf diese Weise liegt nach Durcharbeiten der Checkliste eine übersichtliche Aufstellung der noch zu treffenden Maßnahmen vor.

Eine beantwortete Checkliste deckt möglicherweise vorhandene Sicherheitslücken des Systems auf. Daher ist die ausgefüllte Checkliste bis zur vollständigen Beseitigung dieser Mängel entsprechend vertraulich zu behandeln!

1	Sicherheit des mobilen Arbeitsplatzes	Erfüllt	Nicht erfüllt	Trifft nicht zu	Bemerkung
1.1	Der Zugriff auf Daten oder Programme des mobilen Endgerätes ist gesichert durch: • Passwortschutz (fürs Booten, Bios, Netzwerk, Applikation), möglichst in Verbindung mit einer Chipkarten-Autorisierung • Pausenfunktion mit Tastatur- und Bildschirmsperre				
1.2	Die benutzten IT-Geräte werden von einer zentralen Stelle konfiguriert.				
1.3	Verändernde Zugriffe auf die Betriebssystemebene und auf Programme sind nur von der zentralen Systemadministration möglich.				
1.4	Lokale Datenbestände werden zwangsweise verschlüsselt. Die Verschlüsselungsmethode und die Schlüssel werden von der Zentrale vorgegeben.				
1.5	Nicht mehr erforderliche Daten werden frühestmöglich gelöscht.				
1.6	Auf dem Rechner werden nur dienstliche Daten verarbeitet und gespeichert.				
1.7	Der gespeicherte Datenbestand ist auf ein Minimum beschränkt				
1.8	Täglich läuft ein aktueller Virenscanner über den gespeicherten Datenbestand.				
1.9	Die Datensicherung erfolgt auf geeigneten Datenträgern in mehreren Generationen. Die Sicherungsdatenträger sind unter Verschluss.				
1.10	Eine Dokumentation über die Systemkonfiguration liegt vor.				
1.11	Ggf. Zusatzfrage:				

2	Sichere Kommunikation zwischen mobilem Arbeitsplatz und Arbeitsstelle	Erfüllt	Nicht erfüllt	Trifft nicht zu	Bemerkung
2.1					
2.2	Bei lokaler Wartung und bei Fernwartung/Administration sind die eingeräumten Zutritts-, Zugangs- und Zugriffsrechte auf das notwendige Minimum beschränkt.				
2.3	Mögliche Kommunikationspartner sind eindeutig festgelegt.				
2.4	Bei der Übertragung werden sämtliche Daten verschlüsselt.				
2.5	Dokumente werden bei der Übertragung mit einer digitalen Signatur versehen.				
2.6	Ein Schlüsselmanagement ist eingerichtet worden.				
2.7	Die Konfiguration der ISDN-Karten ist dokumentiert.				
2.8	Bei den ISDN-Netzkoppelelementen gibt es keine Fernwartung.				
2.9	Bei der Kommunikationssoftware sind die Passwortabsicherung und die Protokollierungsfunktionen aktiviert.				
2.10	Die Protokolldateien werden regelmäßig kontrolliert.				
2.11	Alle nicht benötigten Funktionalitäten auf dem Router und der ISDN-Karte sind deaktiviert.				
2.12	Ggf. Zusatzfrage:				

3	Sicherheit des Kommunikations-rechner der Arbeitsstelle	Er-füllt	Nicht erfüllt	Trifft nicht zu	Bemerkung
3.1	Das Firmen- oder Behördennetz ist durch eine Firewall geschützt.				
3.2	Es wird ein „Call-Back"-Verfahren genutzt.				
3.3	Ein Virenscanner wird täglich benutzt und regelmäßig aktualisiert.				
3.4	Autorisierungen erfolgen über ein Challenge-Response-Verfahren.				
3.5	Für jeden mobilen Arbeiter sind nur die Zugriffsrechte vergeben, die zur Aufgabenerfüllung erforderlich sind.				
3.6	Eine Dokumentation über die Systemkonfiguration liegt vor.				
3.7	Es wird eine Protokollierung über • erfolgreiche und nicht erfolgreiche Login-Versuche, • Kennwortänderungen, • Aktionen der Benutzerverwaltung (Löschung und Neueinrichtung von Benutzern) durchgeführt.				
3.8	Ggf. Zusatzfrage:				