Datenschutzgerechter Einsatz von Notebooks und mobilen Endgeräten

Orientierungshilfe

Landesbeauftragter für den Datenschutz Niedersachsen

1. Erforderlichkeit und Risiken

In Wirtschaft und Verwaltung lässt sich ein deutlicher Trend hin zu mobilen Rechnern (z.B. Notebooks, PDA´s) erkennen. Dabei sind zunächst die gleichen Gefährdungen wie beim Einsatz von PCs abzusichern. Zusätzliche Gefahren entstehen beim mobilen Einsatz durch Diebstahl und unbeabsichtigten Verlust. Während in herkömmlicher Büroumgebung der Zugang zu den Geräten abgesichert werden kann, verlassen beim mobilen Einsatz sowohl die Daten als auch das Gerät den Kontrollbereich der Behörde oder des Unternehmens. Das Notebook kann im Auto vergessen oder in einem Sitzungssaal unbeaufsichtigt liegen gelassen werden. Bereits ein kurzer Zugriff bietet vielfältige Gelegenheiten zur unbefugten Kenntnisnahme schutzwürdiger Daten. Missbrauchsgefahren entstehen aber nicht nur durch unbefugtes Lesen (Verlust der Vertraulichkeit), sondern auch durch unbefugte Modifikation von Daten (Verlust der Integrität) und durch Beeinträchtigung der Funktionalität (Verlust der Verfügbarkeit).

2. Datenschutzgerechter Einsatz von Notebooks

In DV-Verfahren der Verwaltung und bei geschäftsmäßiger Datenverarbeitung in der Wirtschaft werden gegenwärtig überwiegend Notebooks mit den Standard-Betriebssystemen Windows NT und Windows 2000/XP sowie verschiedenen LINUX - Derivaten eingesetzt. Die folgenden Empfehlungen für organisatorische und technische Sicherungsmaßnahmen beschränken sich daher auf diese Geräteklassen. Die technischen Maßnahmen sind in Abhängigkeit der Sensibilität der personenbezogenen Daten zu wählen.

2.1 Organisatorische Maßnahmen

Die organisatorisch möglichen Sicherheitsmaßnahmen liegen sowohl beim Administrator der Notebooks als auch beim Endanwender. Durch den Einsatz außerhalb der Büroumgebung und das damit verbundene höhere Sicherheitsrisiko ist der Benutzer eines mobilen Endgerätes allerdings in besonderem Maße gehalten, die Sicherheitsbestimmungen einzuhalten.

- Auswahl und Beschaffung der Hard- und Software sollten zentral oder zumindest abgestimmt erfolgen, damit die Kompatibilität gewährleistet ist und ein einheitliches Sicherheitskonzept als Mindeststandard umgesetzt werden kann. Bei der Anschaffung der Geräte sollte von vornherein auf eine Sicherheitsausstattung Wert gelegt werden (z.B. Geräteschloss oder fester Transportbehälter mit Zahlenschlosskombination, Verschluss der Schnittstellen für periphere Geräte, BIOS-Absicherungen).
- Die Geräte sollten sowohl an der Arbeitsstätte als auch im Heimbereich oder auf Reisen sicher verschlossen aufbewahrt werden.
- Beim Einsatz des Gerätes in fremden Räumen ist das Notebook auch bei kurzfristigem Verlassen zu sperren und ggfs. zu verschließen.
- Ausgabe und Kontrolle der Geräte sowie Einrichtung und Wartung sollten zentral in der Dienststelle erfolgen. Die Verantwortung sollte dem Systemverwalter übertragen werden.
- In der öffentlichen Verwaltung sollte der Notebook-Einsatz einem formalen Freigabeverfahren unterzogen werden. Mit der Freigabe bestätigt die verantwortliche Stelle, dass die Geräte den dienstlichen Erfordernissen entsprechen und legt fest, wie die Notebooks in die bestehende DV-Organisation einzubinden sind.
- Art und Umfang des Notebook-Einsatzes sind verbindlich und für jeden nachvollziehbar in einer Dienstanweisung zu regeln.
- Mitarbeiter sind für Probleme des Datenschutzes und der Datensicherung zu sensibilisieren (Schulung / Unterweisung).

2.2 Technische Maßnahmen

- Das Disketten- und das CD-ROM-Laufwerk des Laptop sollte grundsätzlich für den Bootvorgang gesperrt werden, um das Laden eines anderen Betriebssystems unter Umgehung der Sicherungseinstellungen zu verhindern.
- Die Datensicherung auf bewegliche Datenträger sollte dem Systemverwalter vorbehalten sein, um sicherzustellen, dass nicht unerlaubt fremde Betriebssysteme, Anwendungsprogramme oder Daten verwendet werden.
- Auf dem Notebook ist ein Virenscanner einzusetzen. Die regelmäßige Aktualisierung ist durch den Systemverwalter organisatorisch/technisch sicherzustellen.
- Für die berechtigten Benutzer sind individuelle Kennungen mit individuellen und von ihnen änderbaren Passworten einzurichten (*siehe „Gestaltung und Verwendung von Passworten").* Die Kennungen erlauben einen Zugriff als Standardbenutzer. Administrative Rechte werden für die Benutzer nicht eingerichtet.
- Werden sensitive Daten (Schutzstufe C und D oder solche, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen) auf dem Notebook gespeichert, sollten diese Daten mittels einer geeigneten Softwarelösung verschlüsselt gespeichert werden (z.B. PGP-Disk). Damit soll erreicht werden, dass im Falle eines Diebstahls oder Verlustes des Gerätes die Daten für Dritte nicht verwertbar sind.
- Insbesondere Daten der Schutzstufe E sollten auch nicht auf mobilen Endgeräten verarbeitet werden.

3. Datenschutzgerechter Einsatz von PDA´s

Die Zahl der sogenannten Personal Digital Assistents (PDA) nimmt in Wirtschaft und Verwaltung stetig zu. Diese Geräte werden zur Verwaltung von Terminen, Aufgaben, Kontakten und auch E-Mails genutzt. Aber gerade der Vorzug, dass auf Knopfdruck die gespeicherten Daten ohne Bootvorgang zur Verfügung stehen, ist ein zusätzliches datenschutzrechtliches Problem, wenn das Gerät in falsche Hände fällt.
Zudem wächst der Leistungsumfang dieser Geräte. Über Infrarot-Schnittstellen, Funk- und GSM-Erweiterungen sind Daten aus dem lokalen Netzwerk und über das Internet abrufbar. Auch für diese Geräte müssen geeignete Sicherungsmaßnahmen geplant werden. Vielfach werden die Geräte von den Mitarbeitern der Verwaltungen und Firmen selbst beschafft und dienstlich genutzt. Daraus ergeben sich neue Notwendigkeiten für Organisatoren und Systemverwalter.
Ergänzend zu den für Notebooks genannten Schutzmaßnahmen sollte folgendes beachtet werden:

3.1 Organisatorische Maßnahmen

- Durch Organisatorische Regelungen sollten Art und Umfang der auf dem PDA eingesetzten Software sowie die Art der gespeicherten Informationen festgelegt werden.

3.2 Technische Maßnahmen

- Auf dem PDA sollte zumindest die im Betriebssystem enthaltene Kennwort-Abfrage aktiviert werden. Darüber hinaus sollte eine geeignete Zusatzsoftware zur Sicherung der Datenbestände installiert werden.
- Werden sensitive Daten auf dem PDA gespeichert, sind diese durch eine geeignete Verschlüsselungssoftware zu schützen.
- Werden Dokumente und Mails auf dem PDA verarbeitet, sollte ein Virenscanner eingesetzt werden. Die regelmäßige Aktualisierung muss dabei gewährleistet werden.
- Die auf dem PDA eingesetzte Software sollte vom Systemverwalter vor ihrem Einsatz geprüft und freigegeben werden. So wird evtl. entstehenden Sicherheitslücken vorgebeugt.