Artikel I. Hinweise zur Nutzung von mobilen Endgeräten

Im folgenden werden einige Sicherheitshinweise zum Umgang mit mobilen, dienstlichen Geräten im Allgemeinen und Laptops im Speziellen gegeben.

Es wird hiermit ausdrücklich darauf hingewiesen, dass Laptops, PDAs bzw. Mobiltelefone auf Dienstreisen oder auf der Fahrt zwischen Arbeitsplatz und Wohnort sicher zu transportieren und zu verschließen sind.

Im Einzelnen heißt das:

- Die von der Behörde / dem Unternehmen zur Verfügung gestellten Geräte sind pfleglich zu behandeln. Der Benutzer eines mobilen Gerätes ist für dessen ordnungsgemäßen Gebrauch verantwortlich. Vor Inbetriebnahme hat er sich daher mit den Funktionalitäten vertraut zu machen. Hierzu zählt auch das Studium der Betriebsanleitungen.
- Bei Diebstahl der Geräte ist dies unverzüglich der Polizei anzuzeigen und Abteilung Z darüber zu informieren (Hinweis: "Abteilung Z" steht hier als Platzhalter für diejenige interne Stelle, die zu benachrichtigen ist). Bei Beschädigung der Geräte ist Abteilung Z zu informieren. Die Geräte sind vor dem Zugriff unbefugter Dritter zu schützen. Hierfür werden im folgenden nur einige Hinweise gegeben werden, die zu beachten sind (siehe auch IT-Grundschutz-Kataloge M 1.33):
- Die Zeit, in denen das Gerät unbeaufsichtigt ist, ist zu minimieren.
- Wird ein Gerät bei einer Dienstreise in einem Kraftfahrzeug aufbewahrt, so sollte es von außen nicht sichtbar sein, z. B. indem es im Kofferraum eingeschlossen wird.
- In Hotelräumen sollten mobile Geräte nicht offen ausliegen. Das Verschließen des Gerätes in einem Schrank behindert Gelegenheitsdiebe. Gleiches gilt für Büroräume. Beim Verlassen sollte der Raum verschlossen und der Laptop ausgeschaltet werden.
- Soweit vorhanden, sind die Sicherheitsfunktionen der Geräte zu nutzen.

Im stationären Einsatz sind die tragbaren Geräte wie folgt zu schützen (siehe auch IT-Grundschutz-Kataloge M 1.15, M 1.23, M 1.46):

- Fenster und nach außen gehende Türen (Balkone, Terrassen) sind in Zeiten, in denen ein Raum nicht besetzt ist, zu schließen. Dadurch wird verhindert, dass auch zu Dienstzeiten Gelegenheitsdiebe eine Einstiegsmöglichkeit erhalten,
- Die Türen nicht besetzter Räume sollen abgeschlossen werden. Dadurch wird verhindert, dass Unbefugte Zugriff auf darin befindliche Unterlagen und IT-Einrichtungen erlangen. Auf das Verschließen der Türen kann verzichtet werden, wenn keine schutzbedürftigen Gegenstände wie Unterlagen oder Datenträger offen ausliegen und keine unbefugten Zugriffe mit den IT-Komponenten im Raum möglich sind.
- Bei laufendem Rechner kann auf das Abschließen der Türen verzichtet werden, wenn eine Sicherungsmaßnahme installiert ist, mit der der Rechner nur nach Eingabe eines Passwortes weitergenutzt werden kann (passwortunterstützte Bildschirmschoner) und wenn das Booten des Rechners die Eingabe eines Passwortes verlangt. Bei ausgeschaltetem Rechner kann auf das Verschließen des Büros verzichtet werden, wenn das Booten des Rechners die Eingabe eines Passwortes verlangt. Die gleiche Funktion erfüllen Zugangsmechanismen, die auf Token oder Chipkarten basieren.
- Fremde (Besucher, Handwerker, Wartungspersonal) sollten, außer in Räumen, die ausdrücklich dafür vorgesehen sind, nicht unbeaufsichtigt sein. Wird es erforderlich, einen Fremden allein im Büro zurückzulassen, sollte man einen Kollegen ins Zimmer oder den Besucher zu einem Kollegen bitten. Ist es nicht möglich, Fremdpersonen (z. B. Reinigungspersonal) ständig zu begleiten oder zu beaufsichtigen, sollte zumindest der persönliche Arbeitsbereich bei Verlassen des Büros abgeschlossen werden: Schreibtisch, Schrank und PC (Schloss für Diskettenlaufwerk, Tastaturschloss).

Die Umsetzung der beschriebenen Maßnahmen der IT-Grundschutz-Kataloge liegen im Verantwortungsbereich des Benutzers.

Die für den stationären Betrieb im Büro beschriebene Verhaltensweisen gelten in gleicher Weise auch für den häuslichen Arbeitsplatz z. B. eines Telearbeiters.

Bitte beachten Sie zukünftig diese Hinweise. Vielen Dank.