Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise zum Baustein SYS.3.1 Laptops

1. Einleitung

Ein Laptop ist ein mobiler PC. Er hat eine kompakte Bauform, integriert Peripheriegeräte wie Tastatur und Bildschirm und kann über Akkus zeitweise unabhängig von externer Stromversorgung betrieben werden. Er verfügt über eine Festplatte und meist auch über weitere Speichergeräte, wie DVD- oder Blu-ray-Laufwerke, sowie über Schnittstellen zur Kommunikation über verschiedene Medien, beispielsweise LAN, USB, Firewire, WLAN. Laptops können mit allen üblichen Betriebssystemen wie Windows, Apple macOS oder Linux betrieben werden.

Da Laptops häufig mobil genutzt werden, sind sie oft nicht direkt am LAN der Institution angeschlossen, sondern wählen sich per Virtual Private Network (VPN) über das Internet oder andere Datennetze ein, um so auf die Ressourcen des LANs zuzugreifen. Auch die Infrastruktur einer klassischen Büroumgebung, wie kontrollierbare Umwelteinflüsse, eine stabile Stromversorgung oder zutrittsgeschütze Bereiche, kann für den mobilen Einsatz von Laptops nicht vorausgesetzt werden.

Für den Laptop wird vorausgesetzt, dass er innerhalb eines bestimmten Zeitraums nur von einem Benutzer gebraucht wird. Ein anschließender Benutzerwechsel wird berücksichtigt.

2. Maßnahmen

Im Folgenden sind spezifische Maßnahmen für die Anforderungen des Bausteins SYS.3.1 *Laptop* sowie für weitere Bausteinen aufgeführt, die hiermit im Zusammenhang stehen:

SYS.2.1 *Allgemeiner Client* und CON.3 *Datensicherungskonzept*

Diese zusätzlichen Maßnahmen sollten bei der Umsetzung der genannten Bausteine berücksichtigt werden. Alle Maßnahmen (gekennzeichnet mit M) sind aufsteigend nummeriert und korrespondieren mit den entsprechenden Anforderungen (gekennzeichnet mit A).

2.1 Maßnahmen zum Baustein SYS.3.1 Laptops

SYS.3.1.M1 Regelungen zur mobilen Nutzung von Laptops (B)

Laptops, die ausschließlich innerhalb einer hauseigenen Liegenschaft eingesetzt werden, sind oft bereits durch infrastrukturelle Sicherheitsmaßnahmen ausreichend vor Missbrauch und Diebstahl geschützt. Häufig sollen aber Laptops auch außerhalb der Institution eingesetzt werden, z. B. bei Dienstreisen oder Telearbeit. Um die Geräte auch in diesen Fällen ausreichend schützen zu können, muss die Mitnahme von Datenträgern und IT-Komponenten klar geregelt werden.

Dabei muss festgelegt werden,

- welche IT-Komponenten bzw. Datenträger außer Haus mitgenommen werden dürfen,
- wer IT-Komponenten bzw. Datenträger mitnehmen darf,
- welche grundlegenden Sicherheitsmaßnahmen dabei beachtet werden müssen (z. B. Virenschutz, Verschlüsselung schützenswerter Daten, Aufbewahrung).

Die Art und der Umfang der anzuwendenden Sicherheitsmaßnahmen für Laptops hängen einerseits vom Schutzbedarf der darauf gespeicherten IT-Anwendungen und Daten und andererseits von der Sicherheit der Einsatz- bzw. Aufbewahrungsorte ab.

Grundsätzlich sollte für alle Laptops, die extern eingesetzt werden sollen, eine entsprechende Genehmigung eingeholt werden.

Außerhalb der institutionseigenen Liegenschaften sind die Benutzer für den Schutz der ihnen anvertrauten Laptops verantwortlich. Darauf und auf die zu ergreifenden Vorsichtsmaßnahmen sind sie hinzuweisen.

SYS.3.1.M2 ENTFALLEN (B)

Die zugehörige Anforderung ist entfallen.

SYS.3.1.M3 Einsatz von Personal Firewalls (B)

Personal Firewalls kontrollieren und unterbinden Zugriffe auf Clients über angebundene IT-Netze bzw. von Clients auf diese Netze. Je nach Art des Netzdienstes und der Richtung des Verbindungsaufbaus kann von der Personal Firewall des Clients ein Kommunikationsaufbau gestattet oder abgewiesen werden. Eine Personal Firewall könnte beispielsweise so konfiguriert sein, dass alle Verbindungen, die von dem Client aufgebaut werden, erlaubt und alle von außen ankommenden Anfragen blockiert werden.

Personal Firewalls können nach unterschiedlichen Prinzipien arbeiten:

- Zustandslose (stateless) Personal Firewalls entscheiden anhand von Eigenschaften der übertragenen Datenpakete (z. B. Quell- und Ziel-Adressen oder Ports) darüber, ob die Verbindung erlaubt oder abgewiesen werden soll. Im Wesentlichen wird hierzu die Absender- bzw. Zieladresse und Port-Nummer des Dienstes herangezogen. Zustandslose Personal Firewalls können oft mit präparierten Paketen umgangen werden.
- Kontextsensitive (stateful) Personal Firewalls berücksichtigen bei der Entscheidung auch vorangegangene Pakete. So kann eine kontextsensitive Personal Firewall ein zu prüfendes Paket in den Kontext einer Verbindung bringen und nur dann erlauben, wenn die Verbindung selbst zulässig ist. Nicht in den Verbindungskontext passende Pakete werden verworfen.
- Anwendungsfirewalls (Application firewall) können Netzverkehr auf Basis der Anwendung, die eine Verbindung aufbauen will, prüfen. Dazu verfügt die Applikations-Firewall über eine Whitelist, in der die kommunikationsberechtigten Anwendungen eingetragen sind. Anwendungen, die nicht auf der Whitelist stehen, können keine Verbindungen über das Netz aufbauen oder entgegennehmen.

Viele Betriebssysteme beinhalten bereits eine Personal Firewall. Diese braucht oft nur aktiviert zu werden. Je nach Betriebssystem sind unterschiedlich umfangreiche Funktionen verfügbar. Zusätzlich werden von diversen Drittherstellern Sicherheitslösungen ("Security Suite") angeboten, die unter anderem eine Personal Firewall beinhalten. Oft sind die im Betriebssystem integrierten Personal Firewalls im Gegensatz zu den Sicherheitslösungen weniger umfangreich und weniger komfortabel. Dafür können diese bordeigenen Lösungen sofort aktiviert werden und es entstehen keine zusätzlichen Kosten für die Beschaffung. Es ist zu entscheiden, ob die bordeigene Personal Firewall oder eine Lösung von einem Dritthersteller eingesetzt werden soll, auf einen Mischbetrieb sollte verzichtet werden.

Einsatzumgebungen
Als alleinige Maßnahme um ein Behörden- oder Unternehmensnetz vor Angriffen aus dem Internet zu schützen genügen Personal Firewalls nicht. Der alleinige Einsatz von Personal Firewalls bringt folgende Nachteile mit sich:

- Alle direkt ans Internet angeschlossenen Clients müssen besonders gehärtet werden, d. h. die potenziellen Schwachstellen des Betriebssystems müssen behoben werden, da der Client nicht durch andere IT-Systeme, wie Sicherheitsgateways, geschützt wird.
- Wie bei jeder dezentral eingesetzten Software ist es aufwändig, die einzelnen Personal Firewalls zu managen und die jeweiligen Protokolle auszuwerten.

Es sollte geprüft werden, auf welchen Laptops und mit welchen Rahmenbedingungen eine Personal Firewall eingesetzt werden soll. Eventuell kann auf sie verzichtet werden, wenn die Laptops nur in einem LAN mit einem schützenden Sicherheitsgateway betrieben werden. Bei einem höheren Schutzbedarf sollte auch in diesem Fall der Einsatz von Personal Firewalls jedoch geprüft werden.

Wenn Laptops direkt an das Internet angeschlossen werden, sollten sie unbedingt durch eine restriktiv konfigurierte Personal Firewall gegen Angriffe aus dem Netz geschützt werden.

Aufgrund des vielfältigen Funktionsumfangs der verschiedenen Varianten von Personal Firewalls und deren Komplexität muss sichergestellt sein, dass sie nur durch geeignetes Personal administriert werden. Die Benutzer sollten sie weder selber konfigurieren müssen noch die Einstellungen ändern dürfen.

Personal Firewalls als Bestandteil einer Sicherheitslösung (Security Suite)
Personal Firewalls werden inzwischen von vielen Herstellern angeboten. Institutionen müssen dafür meistens eine Lizenz kaufen. Personal Firewalls werden häufig in Fachzeitschriften getestet. Die Ergebnisse dieser Tests können dabei helfen, ein geeignetes Produkt zu finden.

Prinzipiell ist es z. B. bei umfangreichen Sicherheitslösungen von Drittherstellern, die eine Personal Firewall beinhalten, möglich, mit ihnen die Clients auf Schadsoftware zu überprüfen, die über E-Mail, Java, ActiveX oder ähnliche Mechanismen übertragen werden kann. Hierfür können Mechanismen wie Sandboxing eingesetzt werden, mit denen der Zugriff von Applikationen, die vom Internet auf das lokale System übertragen werden (Java, ActiveX etc.), eingeschränkt werden kann. Mit diesen oft umfangreichen Sicherheitslösungen wird die Prüfung auf Schadsoftware dezentralisiert und damit das zentrale Firewall-System entlastet. Ein weiterer Vorteil liegt darin, dass die Problematik der Filterung von verschlüsselten Daten auf der zentralen Firewall umgangen werden kann.

Konfiguration
Bei Konfiguration und Betrieb einer Personal Firewall auf Laptops sollten folgende Aspekte berücksichtigt werden:

- Die Filterregeln sollten so restriktiv wie möglich eingestellt werden. Dabei gilt der Grundsatz: Alles was nicht ausdrücklich erlaubt ist, ist verboten. Es wird empfohlen, dass abgehende Verbindungen nur von dafür zugelassenen Anwendungen oder Diensten aufgebaut werden dürfen. Basierend auf der IP-Adresse des Zielsystems, der Port-Nummer des benötigten Dienstes und der zugreifenden Anwendung bzw. des zugreifenden Dienstes könnten folgende vom Client aufgebaute Zugriffe beschränkt bzw. erlaubt werden:Ankommende Verbindungen sollten auf die für Fernwartung, Software-Verteilung, Systemaktualisierung und Überwachung der erforderlichen Dienste und die hierfür verwendeten Server-Systeme beschränkt werden.

- zu Datei-Servern, zum Internet für den Browser über das Sicherheitsgateway,
- zum Internet für den Browser über das Sicherheitsgateway,
- zum E-Mail- und Kalender-Server für die E-Mail- und Kalenderanwendung,
- zu Update-Servern im lokalen Netz, um das Betriebssystem, Anwendungen und insbesondere das Virenschutzprogramm zu aktualisieren,
- Kommunikation zum eventuell vorhandenen zentralen Protokollierungsdienst für alle Dienste und Anwendungen, die Meldungen protokollieren.
- Ankommende Verbindungen sollten auf die für Fernwartung, Software-Verteilung, Systemaktualisierung und Überwachung der erforderlichen Dienste und die hierfür verwendeten Server-Systeme beschränkt werden.
- Die Filterregeln der Personal Firewall sollten nach der erstmaligen Konfiguration daraufhin getestet werden, ob die erlaubten Ereignisse zugelassen und unerlaubte Ereignisse unterbunden werden.
- Die korrekte Konfiguration der Filterregeln sollte in sporadischen Abständen überprüft werden, wenn die Installation des Clients nicht ohnehin regelmäßig gelöscht und anhand eines Festplatten-Abbildes (Images) erneut aufgespielt wird.
- Falls das verwendete Produkt diese Möglichkeit bietet, sollten die Regeln der Personal Firewall auch speziellen Programmen zugeordnet werden. Dadurch kann erkannt und verhindert werden, dass ein anderes als die vorgesehenen Client-Programme sich mit Rechnern im Internet verbindet.
- Da viele der Prüfmechanismen einer Personal Firewall auf aktuellen Erkenntnissen beruhen, müssen vom Hersteller veröffentlichte Patches bzw. Updates regelmäßig eingespielt werden. Dabei ist sicherzustellen, dass die dafür erforderlichen Dateien von einer vertrauenswürdigen Quelle bezogen werden, beispielsweise direkt vom Hersteller.
- Die Personal Firewall muss so konfiguriert werden, dass die Benutzer nicht durch viele Warnmeldungen belästigt werden, die sie nicht interpretieren können.
- Falls das verwendete Produkt diese Möglichkeit bietet, sollten sicherheitsrelevante Ereignisse protokolliert werden. Die Protokolldaten sollten regelmäßig durch fachkundiges Personal ausgewertet werden.

Einige Produkte verfügen über die Möglichkeit, mit einer sehr restriktiven Grundkonfiguration zu starten und danach die Einstellungen im laufenden Betrieb zu verfeinern. Dabei wird jedes Mal, wenn ein sicherheitsrelevantes Ereignis auftritt, für das bisher noch keine eindeutige Regel existiert, der Benutzer gefragt, ob dieses Ereignis zulässig ist. Ein Beispiel für ein solches sicherheitsrelevantes Ereignis ist der Zugriff eines bestimmten installierten Programms auf das Internet. Auf der Grundlage der Antworten des Benutzers ermittelt die Personal Firewall Schritt für Schritt die gewünschte Konfiguration, z. B. die Filterregeln.

Der Vorteil dieser inkrementellen Konfiguration ist, dass dadurch die Administration nicht mehr so komplex ist. Nachteilig ist jedoch, dass Benutzer oft nicht beurteilen können, ob ein bestimmtes Ereignis zulässig ist oder nicht. Die inkrementelle Konfiguration der Personal Firewall kann daher nur dann empfohlen werden, wenn den Benutzern entweder präzise Vorgaben gemacht werden, wie sie auf Rückfragen des Programms antworten sollen oder wenn dies unter Anleitung eines Administrators erfolgt, z. B. durch telefonische Rückfragen.

SYS.3.1.M4 ENTFALLEN (B)

Die zugehörige Anforderung ist entfallen.

SYS.3.1.M5 ENTFALLEN (B)

Die zugehörige Anforderung ist entfallen.

SYS.3.1.M6 Sicherheitsrichtlinien für Laptops (S)

Laptops, die außerhalb der eigenen Institution eingesetzt werden, sind mehr Risiken ausgesetzt, als solche, die sich innerhalb geschützter Räumlichkeiten befinden. Es gibt aber Möglichkeiten, sie auch unterwegs zu schützen. Es sollte eine Sicherheitsrichtlinie erstellt werden, in der alle umzusetzenden Sicherheitsmechanismen beschrieben sind. Zusätzlich sollte für die Benutzer ein kurzes und übersichtliches Merkblatt erstellt werden, das beschreibt, wie Laptops sicher genutzt werden.

Sensibilisierung der Benutzer
Je kleiner und leichter IT-Systeme werden, desto leichtfertiger wird erfahrungsgemäß damit umgegangen. Daher sollten Mitarbeiter für den Wert mobiler IT-Systeme und den Wert der darauf gespeicherten Informationen sensibilisiert werden. Sie sollten auch über die spezifischen Gefährdungen von Laptops aufgeklärt werden und die erforderlichen Maßnahmen kennen.

Die Mitarbeiter sollten auch darüber aufgeklärt werden, dass sie vertrauliche Informationen unterwegs nicht mit jedem austauschen und dies unterwegs auch nicht in Hör- und Sichtweite von Externen machen sollten. Insbesondere sollte die Identität des Kommunikationspartners hinterfragt werden, bevor detaillierte Auskünfte gegeben werden.

Regelungen zur Nutzung von Laptops
Für die sichere Benutzung von Laptops sind diverse Punkte zu regeln:

- Die Benutzer müssen darüber informiert sein, welche Informationen mit Laptops unterwegs verarbeitet werden dürfen. Die Daten sollten klassifiziert sein, um Einschränkungen für die Benutzer transparent zu machen. Dienstgeheimnisse dürfen nur dann auf Laptops verarbeitet werden, wenn hierfür geeignete und freigegebene Sicherheitsmechanismen eingesetzt werden.
- Daten, die ein hohes Maß an Sicherheit verlangen (z. B. Angebote, Konstruktionsdaten, Wirtschaftsdaten eines Unternehmens) sollten stets verschlüsselt auf dem Laptop abgelegt werden.
- Es ist zu klären, ob mobile Mitarbeiter von unterwegs Zugriff auf interne Daten ihrer Institution erhalten. Falls das vorgesehen ist, muss dieser Zugriff angemessen geschützt werden (siehe hierzu auch SYS.3.1.A9 Sichere Fernzugriff von unterwegs und SYS.3.1.A8 Sicherer Anschluss von Laptops an lokale Netze).
- Es muss geklärt werden, ob Laptops für private Zwecke benutzt werden dürfen.
- Die Benutzer sollten darauf hingewiesen werden, wie sie sorgfältig mit Laptops umgehen sollten, um einem Verlust oder Diebstahl vorzubeugen bzw. um eine lange Lebensdauer zu gewährleisten (z. B. Akkupflege, sichere Aufbewahrung außerhalb von Büro- oder Wohnräumen, Empfindlichkeit gegenüber zu hohen oder zu niedrigen Temperaturen).
- Es sollte geregelt sein, wie Laptops verwaltet, gewartet und weitergegeben werden.
- Bei jedem Benutzerwechsel müssen alle benötigten Passwörter gesichert weitergegeben werden.
- Laptops und deren Anwendungen können oft durch PINs oder Passwörter abgesichert werden. Diese Mechanismen sollten auch genutzt werden.
- Es sollte festgelegt werden, wie in öffentlichen Umgebungen gearbeitet werden darf (siehe INF.9 Mobiler Arbeitsplatz).
- Es sollte überlegt werden, zu protokollieren, wann und von wem welcher Laptop außer Haus eingesetzt wurden.

Werden Laptops in fremden Büroräumen benutzt, so sind die Sicherheitsregelungen der besuchten Institution zu beachten. In fremden Räumlichkeiten wie Hotelzimmern sollten sie nicht ungeschützt ausliegen. Alle Passwort-Schutzmechanismen sollten spätestens jetzt aktiviert werden. Wenn die Geräte in einem Schrank eingeschlossen werden, behindert das zumindest Gelegenheitsdiebe.

Entsorgung von Datenträgern
Es ist zu regeln, wie ausgediente Datenträger und Geräte entsorgt werden sollen. Ein unterwegs defekter werdender Laptop muss wieder mit zurück transportiert werden und darf nicht unterwegs entsorgt werden.

Das gilt auch, wenn die Datenträger defekt sind, da Experten auch hieraus wieder wertvolle Informationen zurückgewinnen können.

Nutzungsverbot
Es sollte überlegt werden, ob in allen oder bestimmten Bereichen einer Institution eingeschränkt oder verboten werden sollte, Laptops zu benutzen oder mitzubringen. Das kann z. B. für Besprechungsräume sinnvoll sein. Wenn die Sicherheitsrichtlinie der Institution es nicht zulässt, dass Laptops mitgebracht werden dürfen, muss an allen Eingängen deutlich darauf hingewiesen werden. Das sollte dann auch regelmäßig kontrolliert werden.

SYS.3.1.M7 Geregelte Übergabe und Rücknahme eines Laptops (S)

Laptops werden je nach Einsatzzweck nur von einem einzelnen Mitarbeiter eingesetzt, z. B. als Arbeitsplatzrechner, der auch mobil genutzt wird. Sie können aber auch abwechselnd von verschiedenen Mitarbeitern benutzt werden, z. B. für Präsentationen. Je nach Einsatzart ergeben sich verschiedene Sicherheitsanforderungen. Daher sollte Einsatzzweck und -art sorgfältig geplant werden.

Ist der Laptop ein Arbeitsplatzrechner, wird er typischerweise abwechselnd mobil und stationär benutzt. Dabei kann auf verschiedene Netze zugegriffen werden. Dafür müssen die Laptops so abgesichert sein, dass auf der einen Seite durch den mobilen Einsatz weder wichtige Daten des Laptops kompromittiert, manipuliert oder verloren werden können. Auf der anderen Seite dürfen über die Laptops keine Gefährdungen in die internen Netze eingeschleppt werden.

Wenn Laptops abwechselnd von verschiedenen Personen genutzt werden, ist eine geregelte Übergabe extrem wichtig. Damit dies gut funktioniert, sollte ein Laptop-Pool eingerichtet werden (siehe SYS.3.1.A17 *Sammelaufbewahrung tragbarer IT-Systeme*).

Wird ein Laptop übergeben oder zurückgenommen, sind folgende Punkte zu beachten:

Übergabe:

- Der neue Benutzer wird aufgefordert, direkt bei der Übergabe das alte Passwort des Laptops bzw. das Standardpasswort zu ändern.
- Dem neuen Benutzer sollte ein Merkblatt für den sicheren Umgang mit dem tragbaren IT-System übergeben werden.
- Damit jederzeit nachvollziehbar ist, wo sich die Geräte befinden, sollte jeder Benutzer mit Namen, Organisationseinheit, Telefonnummer, Einsatzzweck in ein Übergabe-/Rücknahmejournal eingetragen werden.

Rücknahme bzw. Weitergabe:

- Der Benutzer gibt sein zuletzt benutztes Passwort bekannt bzw. stellt ein Standardpasswort ein.
- Der Laptop muss mittels eines aktuellen Antivirenprogramms auf Malware überprüft werden.
- Der Benutzer muss sicherstellen, dass vor Übergabe des Gerätes sämtliche Daten, die der Benutzer noch benötigt, auf ihm zugängliche Datenträger übertragen werden. Darüber hinaus hat der Benutzer dafür zu sorgen, dass sämtliche von ihm erzeugten Dateien und Daten gelöscht werden. Hierfür müssen geeignete Tools vorhanden sein.
- Die Rückgabe des Laptops und das Ergebnis der Virensuche werden dokumentiert. Die Vollständigkeit des Gerätes, des Zubehörs und der Dokumentation ist sicherzustellen.
- Um sicherzustellen, dass die definierte sichere Grundkonfiguration vorhanden ist und sich keine schützenswerten Dateien mehr auf dem Laptop befinden, sollte er mithilfe einer Referenzinstallation neu installiert werden.

Die vorgesehenen Einsatzarten der Laptops sind zu dokumentieren.

SYS.3.1.M8 Sicherer Anschluss von Laptops an Datennetze (S)

Es ist wichtig festzulegen, welche Regelungen beim Anschluss von Laptops an eigene und fremde LANs und an das Internet zu beachten sind. Es sollte vermieden werden, dass dadurch der sichere Betrieb des eigenen LANs und anderer damit gekoppelter IT-Systeme beeinträchtigt wird, z. B. durch eingeschleppte Schadsoftware.

Wenn ein Laptop nach einem externen Einsatz wieder an das Unternehmens- bzw. Behördennetz angeschlossen werden soll, so ist zunächst durch eine gründliche Überprüfung mit aktuellen Virensignaturen sicherzustellen, dass dieser Laptop nicht infiziert ist.

Kopplung mit anderen IT-Systemen
Über Laptops werden auch häufig Daten mit anderen IT-Systemen ausgetauscht, etwa mit denen von Geschäftspartnern. Auch um auf das Internet zugreifen zu können, ist es häufig erforderlich, das eigene Gerät mit anderen IT-Systemen zu koppeln. Das kann auf verschiedene Arten erfolgen, je nachdem, welche Techniken die beteiligten Geräte unterstützen, beispielsweise über Bluetooth- oder WLAN-Schnittstellen. Hier müssen zum einen die Übertragungstechniken sicher eingesetzt werden, zum anderen muss der eigene Laptop sicher konfiguriert sein. Dazu gehören Sicherheitsmaßnahmen wie z. B. Zugriffsschutz, Benutzerauthentisierung, Virenschutz, Personal Firewall, restriktive Datei- und Ressourcenfreigabe auf Betriebssystemebene und eine lokale Verschlüsselung.

Soll ein Laptop an fremde Netze oder an das Internet angeschlossen werden, so sollte er grundsätzlich über eine Personal Firewall abgesichert werden (siehe SYS.3.1.M3 *Einsatz von Personal Firewalls für Clients*).

In allen Institutionen sollte klar geregelt sein, auf welche Daten von unterwegs zugegriffen werden darf und auf welche nicht. Vor allem muss allen Benutzern bekannt sein, unter welchen Randbedingungen sie Daten über externe Netze oder direkt mit fremden IT-Systemen austauschen dürfen.

Zertifikate/MAC-Adressen
Es sollte sichergestellt sein, dass nicht jeder beliebige Laptop sich an ein LAN anmelden kann. Bevor einem Laptop gestattet wird, auf ein LAN zuzugreifen, sollte er sich erfolgreich gegenüber einem Authentikationsserver authentisiert haben.

Um zu überprüfen, welche Geräte grundsätzlich zum Netzzugriff berechtigt sind, können beispielsweise Geräte-Zertifikate oder MAC-Adressen benutzt werden. Zu beachten ist hierbei allerdings, dass MAC-Adressen gefälscht werden können und deshalb nicht als alleiniges Authentisierungskriterium herangezogen werden sollten.

Zugriffsbeschränkungen
Es muss sichergestellt werden, dass ein VPN-Nutzer ausschließlich auf die zur Aufgabenerledigung notwendigen Dienste auf den Servern im LAN zugreifen kann. Das könnte beispielsweise durch eine benutzerbezogene Authentisierung auf Anwendungsebene und die Kontrolle des Verkehrs mithilfe von Paketfiltern (Paketfilter alleine sind aufgrund der Fälschbarkeit der IP-Adressen nicht ausreichend) sichergestellt werden.

DHCP
Über das Dynamic Host Configuration Protocol (DHCP) werden in IP-basierten Netzen den angeschlossenen Clients automatisch temporäre IP-Adressen sowie Routing- und DNS-Server-Informationen zugewiesen, sodass der Laptop zum Internet-Zugriff nicht mehr vom Benutzer konfiguriert werden muss.

Wenn DHCP aktiviert ist, wird einem IT-System automatisch eine gültige IP-Adresse für das lokale Netz zugewiesen, sodass es auf alle freigegebenen Ordner und Laufwerke zugreifen kann. Als Abhilfe sollte zum einen DHCP auf dem Laptop deaktiviert werden, wenn es nicht benötigt wird (dann müssen allerdings die IP-Adressen manuell verteilt werden). Zum anderen sollte bei der IP-Adressvergabe zusätzlich über die MAC-Adresse überprüft werden, ob der Client zum Netz zugelassen werden sollte.

Internet-Zugriffe

Es muss geregelt werden, ob Laptops direkt auf das Internet zugreifen dürfen. Der kritische Punkt hierbei ist, dass dabei die institutionseigenen Sicherheitsgateways und Sicherheitsmechanismen umgangen werden, dies also potenziell Sicherheitsprobleme nach sich ziehen kann.

Sofern Laptops bei mobiler Nutzung voraussehbar direkt an das Internet angeschlossen werden, ist es unabdingbar, sie durch eine restriktiv konfigurierte Personal Firewall gegen Angriffe aus dem Netz zu schützen. Der Virenschutz reicht alleine nicht aus, um alle zu erwartenden Angriffe abzuwehren. Ebenso ist es unbedingt erforderlich, die Software des Laptops auf aktuellem Stand zu halten und notwendige Sicherheitspatches zeitnah einzuspielen. Es ist sinnvoll, vor einem Zugriff auf das Produktivnetz zu überprüfen, ob Personal Firewall, andere Sicherheitsprogramme und Sicherheitspatches auf dem Laptop auf dem aktuellen Stand sind. Empfehlenswert ist es, über entsprechende Tools diese Prüfungen automatisiert durchzuführen, sodass bei Sicherheitsmängeln der Zugriff auf das interne Netz abgewiesen werden kann.

Die auf dem Laptop installierten Internet-Anwendungsprogramme, vor allem Browser und E-Mail-Clients, sollten mit sicheren Einstellungen betrieben werden. Es sollte administrativ unterbunden werden, dass der Benutzer voreingestellte Optionen verändern kann. Zusätzlich könnten Tools eingesetzt werden, die die Funktionalität des Browsers einschränken, sodass dieser in einer sandbox-ähnlichen Umgebung ausgeführt wird.

Für den Zugriff auf Internet-Anwendungen, bei denen schützenswerte Daten wie personenbezogene Daten, interne Informationen oder Kontendaten ausgetauscht werden, muss zumindest TLS zur Verschlüsselung genutzt werden.

Je nach Sicherheitsanforderungen und Einsatzumgebung kommen darüber hinaus verschiedene weitere Lösungsmöglichkeiten in Betracht:

- Verbot direkter Internet-Zugriffe: Diese Lösung hat natürlich den Vorteil, dass sie am einfachsten umzusetzen ist. Sie schränkt allerdings die Bewegungsfreiheit der Benutzer am meisten ein und wird daher nicht einfach durchzusetzen sein.
- Nutzung verschiedener Benutzerkennungen: Auf Betriebssystem-Ebene sollten in diesem Fall zwei verschiedene Benutzerkennungen genutzt werden, einmal für die allgemeine geschäftliche Nutzung und einmal für Internet-Zugriff. Hierbei sollte die Internet-Kennung nur über minimale Rechte verfügen.
- Nutzung verschiedener Partitionen/Betriebssysteminstallationen: Bei dieser Lösung werden verschiedene Partitionen angelegt, die möglichst stark getrennt sind, beispielsweise durch unterschiedliche Betriebs- und Dateisysteme. Je stärker die Trennung ist, desto höher sind die Hürden, mit denen verhindert wird, dass Schadsoftware aus dem Internet oder ähnliches die Produktiv-Umgebung beeinträchtigt.
- Virtuelle Maschinen: Hierbei kann das Internet ausschließlich über ein Betriebssystem benutzt werden, das in einer virtuellen Maschine betrieben wird (z. B. User Mode Linux, UML). Durch die virtuelle Maschine wird der benutzte Browser stärker vom eigentlichen Host-Betriebssystem getrennt, als das ohne virtuelle Maschine der Fall ist. Allerdings besteht bei dieser Variante das Restrisiko, dass Schadprogramme mittels Copy&Paste zwischen dem Host-Betriebssystem und dem virtuellen Betriebssystem hin und her kopiert werden können. Das Host-Betriebssystem könnte sich in diesem Fall bei der nächsten VPN-Einwahl in einem unsicheren Zustand befinden.
- Verwendung von Boot-CDs: Hierbei wird für die Internet-Nutzung von einem schreibgeschützten Medium wie einer CD-ROM eine internetfähige Betriebsumgebung hergestellt, wobei die Nutzbarkeit dadurch eingeschränkt wird, dass notwendige IP-Informationen eventuell von Hand eingetragen werden müssen. Hierzu kann beispielsweise Knoppix verwendet werden, eine komplett von einer CD lauffähige Zusammenstellung von GNU/Linux-Software (siehe [KNOP]).
- Internet-Zugriff nur über VPN (über Intranet über institutionseigenen Sicherheitsgateway ins Internet). Dies hat den Vorteil, dass gefährliche Inhalte aussortiert werden.

Nutzung von IrDA-Schnittstellen
Die Infrared Data Association (IrDA) hat Spezifikationen veröffentlicht, in der zunächst die unteren Schichten eines Protokolls für eine Infrarot-Schnittstelle definiert wurden. Dabei wird infrarotes Licht als Träger für den Datenaustausch über kurze Distanzen verwendet. Mittlerweile stellt IrDA auch höhere Protokolle für unterschiedliche Einsatzbereiche zur Verfügung. IrDA wird heute von allen gängigen Betriebssystemen unterstützt, allerdings verliert diese Schnittstelle im Vergleich zu Bluetooth, WLAN oder USB zunehmend an Bedeutung.

Im IrDA-Standard sind keine Sicherheitsmechanismen spezifiziert, die dagegen helfen, dass Angreifer den Datenverkehr mitschneiden können. Die Daten werden nur auf Protokollebene mittels Prüfsummenverfahren gegen Übertragungsfehler gesichert. Sicherheitsmechanismen wie Authentisierung, kryptografischer Integritätsschutz und Verschlüsselung sind nicht vorhanden. Daher sollte die IrDA-Schnittstelle nur bei konkretem Bedarf aktiviert werden.

Da die Kopplung nur in einem sehr eingeschränkten Bereich möglich ist, kann die Kommunikation meist nicht mitgehört werden. Das bestehende geringe Restrisiko aufgrund der Streustrahlung der IrDA-Komponenten kann durch zusätzliche Sicherheitsmechanismen (z. B. Authentisierung und Verschlüsselung auf Applikationsebene) oder den Ersatz von IrDA durch leitungsgebundene Übertragung weiter minimiert werden.

SYS.3.1.M9 Sicherer Fernzugriff mit Laptops (S)

Mit Laptops soll auch häufig unterwegs auf Daten aus dem internen Netz einer Institution zugegriffen werden. Dabei werden üblicherweise öffentliche Kommunikationsnetze benutzt. Da weder die Institution noch die mobilen Mitarbeiter großen Einfluss darauf nehmen können, ob die Vertraulichkeit, Integrität und Verfügbarkeit im öffentlichen Kommunikationsnetz gewahrt werden, sind zusätzliche Maßnahmen zum Schutz der Informationen erforderlich.

Generell muss die Datenübertragung zwischen einem Laptop und dem LAN einer Institution folgende Sicherheitsanforderungen erfüllen:

- Sicherstellung der Vertraulichkeit der übertragenen Daten: Die Datenübertragung muss ausreichend sicher verschlüsselt werden. Dazu gehört neben einem geeigneten Verschlüsselungsverfahren auch ein angepasstes Schlüsselmanagement mit periodischem Schlüsselwechsel.Sicherstellung der Integrität der übertragenen Daten: Mit den eingesetzten Übertragungsprotokollen muss es möglich sein, Veränderungen an den übertragenen Daten zu erkennen und eventuell sogar zu beheben. Solche Veränderungen können beispielsweise durch Übertragungsfehler (technische Probleme) oder durch absichtliche Manipulationen durch einen Angreifer entstehen. Zusätzlich kann der Einsatz digitaler Signaturen sinnvoll sein, um die Datenintegrität sicherzustellen.Sicherstellung der Authentizität der Daten: Bei der Übertragung der Daten muss vertrauenswürdig feststellbar sein, ob die Kommunikation zwischen den richtigen Teilnehmern stattfindet, sodass z. B. ein Man-in-the-Middle-Angriff ausgeschlossen werden kann. Zu diesem Zweck müssen sich die Kommunikationspartner gegenseitig authentisieren, beispielsweise über digitale Zertifikate.Sicherstellung der Nachvollziehbarkeit der Datenübertragung: Um eine Kommunikation nachvollziehbar zu machen, können Protokollierungsfunktionen eingesetzt werden, durch die sich nachträglich feststellen lässt, welche Daten wann und an wen übertragen wurden.
- Sicherstellung der Integrität der übertragenen Daten: Mit den eingesetzten Übertragungsprotokollen muss es möglich sein, Veränderungen an den übertragenen Daten zu erkennen und eventuell sogar zu beheben. Solche Veränderungen können beispielsweise durch Übertragungsfehler (technische Probleme) oder durch absichtliche Manipulationen durch einen Angreifer entstehen. Zusätzlich kann der Einsatz digitaler Signaturen sinnvoll sein, um die Datenintegrität sicherzustellen.Sicherstellung der Authentizität der Daten: Bei der Übertragung der Daten muss vertrauenswürdig feststellbar sein, ob die Kommunikation zwischen den richtigen Teilnehmern stattfindet, sodass z. B. ein Man-in-the-Middle-Angriff ausgeschlossen werden kann. Zu diesem Zweck müssen sich die Kommunikationspartner gegenseitig authentisieren, beispielsweise über digitale Zertifikate.Sicherstellung der Nachvollziehbarkeit der Datenübertragung: Um eine Kommunikation nachvollziehbar zu machen, können

Protokollierungsfunktionen eingesetzt werden, durch die sich nachträglich feststellen lässt, welche Daten wann und an wen übertragen wurden.

- Sicherstellung der Authentizität der Daten: Bei der Übertragung der Daten muss vertrauenswürdig feststellbar sein, ob die Kommunikation zwischen den richtigen Teilnehmern stattfindet, sodass z. B. ein Man-in-the-Middle-Angriff ausgeschlossen werden kann. Zu diesem Zweck müssen sich die Kommunikationspartner gegenseitig authentisieren, beispielsweise über digitale Zertifikate.Sicherstellung der Nachvollziehbarkeit der Datenübertragung: Um eine Kommunikation nachvollziehbar zu machen, können Protokollierungsfunktionen eingesetzt werden, durch die sich nachträglich feststellen lässt, welche Daten wann und an wen übertragen wurden.
- Sicherstellung der Nachvollziehbarkeit der Datenübertragung: Um eine Kommunikation nachvollziehbar zu machen, können Protokollierungsfunktionen eingesetzt werden, durch die sich nachträglich feststellen lässt, welche Daten wann und an wen übertragen wurden.

Die Stärke der dazu erforderlichen Mechanismen richtet sich nach dem Schutzbedarf der übertragenen Daten. Wie adäquate kryptografische Verfahren und Systeme ausgewählt und eingesetzt werden können, ist in Baustein CON.1 *Kryptokonzept* beschrieben.

VPN
Zugriffe von einem Laptop von außerhalb auf das interne Netz sollten ausschließlich über ein Virtual Private Network (VPN) erfolgen (siehe NET.3.3 Virtual Private Networks (VPN)). Entsprechende Produkte sind von diversen Herstellern und für praktisch alle gebräuchlichen Plattformen verfügbar. Auf Daten oder Systeme mit hohem Schutzbedarf darf nicht ohne entsprechende Sicherungsmaßnahmen zugegriffen werden. Betreibt die Institution in ihrem Netz einen Filter für Schadsoftware, so sollte die Netzverbindung des Laptops durch diesen Filter geleitet werden, um so das Endgerät besser vor Schadsoftware zu schützen.

Ermöglicht es die Institution dienstliche E-Mails über das Internet mittels einer Web-Mail-Lösung abzurufen, so ist sicherzustellen, dass die E-Mails ausschließlich verschlüsselt vom Server auf den Laptop übertragen werden, z. B. mittels TLS. Allerdings muss hierbei nicht nur der Transportkanal, sondern auch das Endsystem selbst besonders abgesichert werden. Ein Laptop kann kompromittiert werden, wenn neben der VPN-Nutzung gleichzeitig auch noch Standardprotokolle wie z. B. HTTP oder SMTP im Internet genutzt werden. Daher sollten Laptops möglichst so abgesichert werden, dass bei bestehender VPN-Verbindung in das interne Netz keine anderen Verbindungen möglich sind (Split-Tunneling). Dabei muss gewährleistet sein, dass alle abgehenden Datenpakete des Clients in den Tunnel gehen und ausschließlich Datenpakete aus dem Tunnel akzeptiert werden.

Es sollte in diesem Zusammenhang auch darauf geachtet werden, dass neben dem VPN-gesicherten Laptop-Zugriff nicht gleichzeitig andere Netzzugriffe auf das interne Netz möglich sind. Insbesondere darf während der VPN-Zugriffe kein WLAN oder Bluetooth auf dem Laptop aktiv sein.

Authentisierung der VPN-Nutzung
Ein Laptop kann leicht in falsche Hände geraten. Bevor ein VPN aufgebaut wird, sollte die Authentizität des Benutzers mit starken Authentisierungsverfahren sichergestellt werden. Starke Authentisierungsverfahren sind beispielsweise Einmal-Passwort- oder Challenge-Response-Verfahren.

Protokollierung
Die Zugriffe auf Server-Dienste sollten protokolliert werden. Dabei sollte auch erkennbar sein, ob der Laptop-Zugriff aus der Institution oder von extern erfolgte. Vertiefende Informationen zur Protokollierung sind in OPS.1.1.6 Protokollierung zu finden.

Temporäre Daten
Es sollte sichergestellt werden, dass alle zwischengespeicherten Authentisierungsinformationen, die den Aufbau eines VPNs ermöglichen, nach dem Ende der VPN-Nutzung automatisch gelöscht werden. Das gilt sowohl für absichtlich als auch unabsichtlich beendete VPN-Verbindungen. Zusätzlich sollte beispielsweise bei Browser-basierten SSL-VPNs darauf geachtet werden, dass sämtliche Zwischenspeicher deaktiviert werden, damit Authentisierungsinformationen erst gar nicht temporär gespeichert werden. Dies könnte sonst einem Angreifer ermöglichen, die VPN-Verbindung wiederherzustellen.

Weitere Empfehlungen des BSI zum sicheren Fernzugriff finden sich im Dokument "Sicherer Fernzugriff auf das interne Netz (ISi-S)" [SFIN].

SYS.3.1.M10 Abgleich der Datenbestände von Laptops (S)

Wenn ein Laptop unterwegs eingesetzt wird und nicht über ein VPN direkt auf den Dateiservern der Institution gearbeitet wird, ist es wichtig, dass alle erforderlichen Daten und Anwendungen aktuell sind. Ebenso sollten unterwegs bearbeitete Daten zügig auf IT-Systemen innerhalb des Informationsverbunds der Institution gespeichert werden, damit es nicht zu inkonsistenten Datenbeständen kommt. Der einfachste Weg hierfür ist, regelmäßig Datenbestände von Laptops abzugleichen, beispielsweise über Tools zur Synchronisation von Dateien und Verzeichnissen zwischen Laptops und Arbeitsplatzrechnern oder Servern.

Dafür sollte überlegt werden, welche Informationen an welchen Stellen gespeichert sind, also auf welchen Servern und in welchen Verzeichnissen. Bei der ersten Sichtung zeigt sich meist, an wie vielen verschiedenen Stellen in einem Informationsverbund sich die für einen Arbeitsplatz relevanten Informationen befinden.

Damit Synchronisationsvorgänge nicht zu lange dauern, sollten dafür Tools ausgewählt werden,

- über die Dateien und Verzeichnisse nach vorher festgelegten Kriterien automatisch abgeglichen und aktualisiert werden können,die über Filtermöglichkeiten komplette Verzeichnisse oder auch einzelne Dateien von einem Kopiervorgang ausschließen können,die Synchronisationskonflikte auflösen können. Synchronisationskonflikte können auftreten, wenn seit der letzten Synchronisation eine Datei in verschiedenen Verzeichnissen geändert wurde.
- die über Filtermöglichkeiten komplette Verzeichnisse oder auch einzelne Dateien von einem Kopiervorgang ausschließen können,die Synchronisationskonflikte auflösen können. Synchronisationskonflikte können auftreten, wenn seit der letzten Synchronisation eine Datei in verschiedenen Verzeichnissen geändert wurde.
- die Synchronisationskonflikte auflösen können. Synchronisationskonflikte können auftreten, wenn seit der letzten Synchronisation eine Datei in verschiedenen Verzeichnissen geändert wurde.

Synchronisationstools sollten außerdem möglichst benutzerfreundlich sein und trotzdem vor fehlerhafter Bedienung schützen. Synchronisationsvorgänge sollten zugriffsgeschützt sein, bei Laptops kann das über bereits vorhandene Zugriffsschutz-Verfahren erfolgen.

Damit Angreifer die Synchronisation nicht manipulieren können, sollten die Benutzer regelmäßig die relevanten Verzeichnisse daraufhin inspizieren, ob sich dort ihnen unbekannte Dateien befinden. Die Synchronisationssoftware sollte so konfiguriert werden, dass sie, bevor Programme installiert werden, den Benutzer fragt. Der Synchronisationsvorgang sollte nicht unbeobachtet ablaufen, auch die Informationen, welche Dateien jeweils transferiert werden, können entscheidende Hinweise enthalten. Die Synchronisation sollte protokolliert werden. Die Protokolle sollten dann regelmäßig zumindest überflogen werden, um festzustellen, ob unbefugte Synchronisationsvorgänge stattgefunden haben.

SYS.3.1.M11 Sicherstellung der Energieversorgung (S)

Um die Energieversorgung eines Laptops auch unterwegs aufrechterhalten zu können, werden üblicherweise Akkus eingesetzt. Diese können den Laptop je nach Kapazität und Bauweise für einen beschränkten Zeitraum, üblicherweise einige Stunden, mit Energie versorgen. Es ist schwierig, diesen Zeitraum genauer abzuschätzen, da er stark vom Alter des Akkumulators und von der Intensität der Nutzung abhängt. Damit keine Daten in flüchtigen Speichern verloren gehen, wenn der Akku leer ist, sollten einige Randbedingungen eingehalten werden:

- Die Warnanzeigen des Laptops, die den Spannungsabfall anzeigen, dürfen nicht ignoriert werden. Sie sollten so konfiguriert sein, dass nach der ersten Warnung noch genügend Zeit vorhanden ist, um z. B. wichtige Daten abzuspeichern oder offene Programme zu schließen.
- Falls ein längerfristiger mobiler Einsatz absehbar ist, sind die Akkus vorher vollständig aufzuladen und eventuell Ersatzakkus mitzuführen. Zusätzlich gibt es für viele Laptops sogenannte Akku-Packs, die über eine externe Schnittstelle angeschlossen werden können. Ein Ersatzakku sollte in einer Schutzhülle verwahrt werden, da Schäden durch Überhitzung oder Brand entstehen können, wenn die Kontakte des

Akkus mit leitenden Materialien in Berührung kommen. Dies kann durch viele Gegenstände des täglichen Gebrauchs verursacht werden, z. B. durch Schlüssel oder Ketten.

- Gerade bei älteren Akkus sind die Gebrauchszeiten verkürzt und sie entladen sich gegen Ende der Kapazität sehr schnell. Geöffnete Dateien müssen daher regelmäßig abgespeichert werden, um Datenverluste zu vermeiden. Da sich solche Akkus auch im Stand-by-Modus schnell entladen können, sollte der Ladezustand regelmäßig kontrolliert werden. Für den Notfall sollten Sicherungen der Konfigurationsdaten des Laptops mitgeführt werden. Es wird empfohlen, den Akku auszutauschen, sobald solche Alterungserscheinungen auftreten.
- Der Laptop sollte so aufgeladen werden, wie es im Handbuch empfohlen wird, damit die Lebensdauer des Akkus nicht beeinträchtigt wird.
- Vor einer Reise bzw. wenn ein Laptop übergeben wird, ist der ausreichende Ladezustand der Akkus oder Batterien sicherzustellen. Der Ladezustand sollte regelmäßig überprüft werden, da sich ein Akku auch entlädt, wenn er nicht verwendet wird.
- Das Ladegerät sollte immer mitgeführt werden. Nur im Ausnahmefall, beispielsweise bei voraussehbar kurzem mobilen Einsatz, ist es entbehrlich.

Es empfiehlt sich darüber hinaus, in kurzen Abständen die verarbeiteten Daten zusätzlich auf einem nichtflüchtigen Medium zu speichern. Dazu können auch automatische Datensicherungen in Standardprogrammen benutzt werden.

Bevor der Akku gewechselt wird, sollte der Laptop ausgeschaltet werden, damit der Speicher nicht beschädigt wird.

SYS.3.1.M12 Verlustmeldung (S)

Fällt ein dienstlich genutzter Laptop aus, ist er defekt, zerstört, geht verloren oder wird gestohlen, sollte dies umgehend gemeldet werden. Das gilt auch für private Geräte, die dienstlich genutzt werden. Hierfür sollte es in jeder Institution klare Meldewege und Ansprechpartner geben.

Insbesondere wenn ein Laptop verloren geht oder gestohlen wird, muss schnell gehandelt werden, da es hier nicht nur um die Wiederbeschaffung der Geräte geht, sondern auch darum, dass die betroffenen Informationen nicht missbraucht werden. Auf Laptops können sich vertrauliche Daten befinden, nach deren Verlust umgehend gehandelt werden muss, beispielsweise:

- Zugangsdaten wie Passwörter: Alle Zugangsdaten im eventuell betroffenen IT-System müssen umgehend geändert werden.Als vertraulich eingestufte Informationen: Alle betroffenen Bereiche (z. B. Fachabteilung, Kunden) müssen benachrichtigt werden, um entsprechende Maßnahmen ergreifen zu können.
- Als vertraulich eingestufte Informationen: Alle betroffenen Bereiche (z. B. Fachabteilung, Kunden) müssen benachrichtigt werden, um entsprechende Maßnahmen ergreifen zu können.

Falls möglich, sollten, nachdem ein Laptop verloren gegangen ist, auch Maßnahmen ergriffen werden, mit denen sich das Gerät sperren, löschen oder lokalisieren lässt. Die meisten Mobile-Device-Manage-ment-(MDM)-Lösungen (siehe SYS.3.2.2 Mobile Device Management) bieten diese Funktionen an. Dafür sind vorher klare Regeln zu definieren und entsprechende Maßnahmen in Absprache mit dem Benutzer, dessen Endgerät verloren ging, unverzüglich zu ergreifen.

Wenn verlorene Geräte wieder auftauchen, sollten sie auf eventuelle Manipulationen untersucht werden, z. B. ob Schrauben geöffnet, Siegel entfernt wurden oder sich das Gewicht gegenüber dem Aus-lieferungszustand geändert hat. Besteht ein Verdacht, sollte das Gerät entweder gleich entsorgt oder von einem Spezialisten weiter untersucht werden. Um sicherzustellen, dass sich keine manipulierten Programme auf den wiedererlangten Geräten befinden, müssen die Geräte zumindest neu installiert werden (SYS.3.1.M7 *Geregelte Übergabe und Rücknahme eines Laptops*).

SYS.3.1.M13 Verschlüsselung von Laptops (S)

Um zu verhindern, dass aus einem gestohlenen Laptop schutzbedürftige Daten ausgelesen werden können, sollte ein Verschlüsselungsprogramm eingesetzt werden. Mithilfe der marktgängigen Produkte ist es möglich, einzelne Dateien, bestimmte Bereiche oder die ganze Festplatte so zu verschlüsseln, dass nur derjenige, der über den geheimen Schlüssel verfügt, die Daten lesen und bearbeiten kann.

Die Sicherheit der Verschlüsselung hängt dabei von drei verschiedenen Punkten zentral ab:

- Der verwendete Verschlüsselungsalgorithmus muss so konstruiert sein, dass es ohne den verwendeten Schlüssel zu kennen, nicht möglich ist, den Klartext aus dem verschlüsselten Text zu rekonstruieren. Nicht möglich bedeutet dabei, dass der erforderliche Aufwand, mit dem der Algorithmus gebrochen bzw. entschlüsselt werden kann, in keinem Verhältnis steht zum dadurch erzielbaren Informationsgewinn.
- Der Schlüssel ist geeignet zu wählen. Er sollte zufällig erzeugt werden. Wenn es möglich ist, einen Schlüssel wie ein Passwort zu wählen, sollten die Regelungen der Institution zum Passwortgebrauch beachtet werden.
- Der Verschlüsselungsalgorithmus (das Programm), der verschlüsselte Text und die Schlüssel dürfen nicht zusammen auf einem Datenträger gespeichert werden. Es bietet sich an, den Schlüssel einzeln aufzubewahren. Das kann dadurch geschehen, dass er auf einer Pappkarte in Form einer Scheckkarte aufgeschrieben und anschließend wie eine Scheckkarte im Portemonnaie aufbewahrt wird. Die kryptografischen Schlüssel sollten auf einem auswechselbaren Datenträger wie z. B. auf einem USB-Stick gespeichert und getrennt vom Laptop aufbewahrt werden.

Eine Verschlüsselung kann online oder offline vorgenommen werden. Online bedeutet, dass sämtliche Daten der Festplatte (bzw. einer Partition) verschlüsselt werden, ohne dass der Benutzer dies aktiv veranlassen muss. Eine Offline-Verschlüsselung wird explizit vom Benutzer initiiert. Er muss dann auch entscheiden, welche Dateien verschlüsselt werden sollen. Zur Auswahl und Nutzung von kryptografischen Verfahren sollte auch Baustein CON.1 *Kryptokonzept* beachtet werden.

SYS.3.1.M14 Geeignete Aufbewahrung von Laptops (S)

Benutzer müssen darauf achten, dass sie ihre Laptops auch außerhalb der Institution sicher aufbewahren. Hierfür können nur einige Hinweise gegeben werden, die dabei zu beachten sind:

- Laptops sollten möglichst nicht unbeaufsichtigt bleiben.
- Wird ein Laptop in einem Kraftfahrzeug aufbewahrt, sollte das Gerät von außen nicht sichtbar sein. Zum Beispiel sollte es abgedeckt oder in den Kofferraum eingeschlossen werden. Ein Laptop kann einen hohen Wert darstellen, der potenzielle Diebe anlockt, zumal solche IT-Systeme leicht veräußert werden können.
- Wird der Laptop in fremden Büroräumen benutzt, so ist sollte der Mitarbeiter ihn auch mitnehmen, wenn er den Raum nur kurz verlässt oder er schließt das Gerät ein. Es sollte mindestens ein Zugriffsschutz aktiviert werden, um eine unerlaubte Nutzung zu verhindern. Wird der Raum für längere Zeit verlassen, sollte der Laptop zusätzlich ausgeschaltet sein.
- In Hotelräumen sollte der Laptop nicht unbeaufsichtigt herumliegen. Wird das Gerät in einen Schrank eingeschlossen, hält das zumindest Gelegenheitsdiebe ab.
- Ein Laptop kann zusätzlich durch ein Schloss gesichert werden. Ein Dieb braucht dann Werkzeug, um ihn zu stehlen.
- Ein Laptop sollte nie extremen Temperaturen ausgesetzt werden. Insbesondere der Akku und das Display können dadurch beschädigt werden. Auch sollten weder Laptops noch Akkus in geparkten Autos zurückgelassen werden, wenn die Außentemperatur extrem hoch oder niedrig ist.
- Ebenso sollten Laptops vor schädlichen Umwelteinflüssen geschützt werden, beispielsweise vor Feuchtigkeit durch Regen oder Spritzwasser.
- Laptops sind nicht unzerstörbar, daher sollten sie auch bei kürzeren Transportwegen möglichst stoßgeschützt befördert werden. So sollten sie beispielsweise immer zusammengeklappt werden, da

sowohl die Scharniere als auch der Bildschirm bei einem Sturz leicht beschädigt werden können. Grundsätzlich sollte für den Transport ein schützendes Behältnis verwenden werden, beispielsweise Taschen oder Rucksäcke mit eigenen Fächern und Polsterungen für Laptops.

Es ist empfehlenswert, für die Benutzer von Laptops ein Merkblatt zu erstellen, das die wichtigsten Hinweise und Vorsichtsmaßnahmen enthält, wie die Geräte geeignet aufzubewahren und zu transportieren sind.

Geeignete Aufbewahrung
Laptops sind durch ihre Bauform immer beliebte Ziele für Diebstähle. Daher müssen sie auch dann sicher aufbewahrt werden, wenn sie sich im vermeintlichen sicheren Büro befinden. Deshalb sind die in Baustein INF.7 *Büroarbeitsplatz* beschriebenen Anforderungen zu beachten. Da ein Laptop jedoch besonders leicht zu transportieren und zu verbergen ist, kann das Gerät außerhalb der Nutzungszeiten weggeschlossen werden, also beispielsweise in einem Schrank oder Schreibtisch verschlossen oder angekettet werden.

SYS.3.1.M15 Geeignete Auswahl von Laptops (S)

Laptops gibt es in verschiedensten Varianten und Geräteklassen. Diese unterscheiden sich nicht nur in ihren Abmessungen und Leistungsmerkmalen, sondern auch bei den Sicherheitsmechanismen und dem Bedienkomfort. Zudem stellen sie unterschiedliche Anforderungen an Hard- und Software-Komponenten im Einsatzumfeld.

Bei der Vielzahl verschiedener Laptop-Modelle mit den unterschiedlichsten Betriebssystemen sind Kompatibilitätsprobleme bei Hardware, Software auf Laptop und PC sowie Schnittstellen naheliegend.

Zunächst sollte eine Anforderungsanalyse durchgeführt werden. Ziel ist es hier einerseits, alle infrage kommenden Einsatzszenarien zu bestimmen und andererseits daraus Anforderungen an die benötigten Hard- und Softwarekomponenten abzuleiten.

Die folgende Liste gibt einen groben Überblick über mögliche allgemeine Bewertungskriterien. Sie erhebt jedoch keinen Anspruch auf Vollständigkeit und kann um weitere allgemeine Anforderungen erweitert werden.

Allgemeine Kriterien
- Wartbarkeit
- Ist das Produkt einfach wartbar?
- Wird das Gerät über den geplanten Nutzungszeitraum vom Hersteller unterstützt? Bietet der Hersteller regelmäßige Software-Updates an?
- Werden für das Produkt Wartungsverträge angeboten?
- Zuverlässigkeit/Ausfallsicherheit
- Wie zuverlässig und ausfallsicher ist das Produkt?
- Ist das Produkt im Dauerbetrieb einsetzbar?
- Gibt es einen im Produkt integrierte Backup-Mechanismus? Kann eine automatische Datensicherung durchgeführt werden?
- Benutzerfreundlichkeit
- Lässt sich das Produkt einfach installieren, konfigurieren und nutzen?
- Ist die Synchronisations-Software so konfigurierbar, dass die Benutzer möglichst wenig mit technischen Details belastet werden? Ist die Sicherheit dabei trotzdem immer gewährleistet?
- Sind Abmessungen und Gewicht bezogen auf den Einsatzzweck angemessen? Ist die Akku-Laufzeit ausreichend für die tägliche Arbeit? Kann der Akku gewechselt werden, wenn die Akku-Laufzeit nicht ausreichend ist und das Gerät zwischenzeitlich nicht geladen werden kann?
- Kosten
- Wie hoch sind die Anschaffungskosten der Hard- und Software?

- Wie hoch sind die voraussichtlichen laufenden Kosten der Hard- und Software (Wartung, Betrieb, Support)?
- Wie hoch sind die voraussichtlichen laufenden Kosten für das Personal (Administrator/Support)?
- Müssen zusätzliche Soft- oder Hardware-Komponenten angeschafft werden (z. B. Docking-Station, Konvertierungssoftware)?

Funktion
- Installation und Inbetriebnahme
- Kann das Gerät sowie die Synchronisations-Software so konfiguriert werden, dass die vorgegebenen Sicherheitsziele erreicht werden können?
- Können wichtige Konfigurationsparameter vor Veränderungen durch Benutzer geschützt werden?
- Arbeitet das Produkt mit gängiger Hard- und Software zusammen (Betriebssysteme, Treiber)?
- Administration
- Enthält die mitgelieferte Produktdokumentation eine genaue Darstellung aller technischen und administrativen Details?
- Können die Laptops über eine zentral gesteuerte Management-Software administriert werden? Ist die administrative Schnittstelle so gestaltet, dass auf fehlerhafte, unsichere oder inkonsistente Konfigurationen hingewiesen wird oder diese verhindert werden?
- Sicherheit: Kommunikation, Authentisierung, Zugriff und Protokollierung
- Unterstützt der Laptop alle benötigten Datenübertragungstechnologien (z. B. Bluetooth, WLAN, LAN)?
- Können mit dem Produkt die Daten zu anderen Endgeräten gesichert übertragen werden?
- Hat der Laptop geeignete Mechanismen zur Identifikation und Authentisierung der Benutzer?
- Können zusätzliche Sicherungsmechanismen (z. B. Verschlüsselungs- oder Antivirenprogramme) genutzt werden?
- Erlaubt die Produktarchitektur die nachträgliche Installation neuer Sicherheitsmechanismen?
- Wird dem mobilen Benutzer nur nach erfolgreicher Authentisierung der Zugang zu lokalen Endgeräten erlaubt?
- Ist die Systemarchitektur so aufgebaut, dass neue Authentisierungsmechanismen nachträglich integriert werden können?
- Lässt sich mit dem Laptop eine geeignete Protokollierung durchführen bzw. lässt er sich in bereits bestehende Protokollierungs-Prozesse integrieren?

Sind alle Anforderungen an das zu beschaffende Produkt dokumentiert, so müssen die am Markt erhältlichen Laptops dahin gehend untersucht werden, inwieweit sie diese Anforderungen erfüllen. Es ist zu erwarten, dass nicht jedes Produkt alle Anforderungen gleichzeitig oder gleich gut erfüllt. Daher sollten die einzelnen Anforderungen gewichtet werden. Aufgrund der durchgeführten Produktbewertung kann dann eine fundierte Kaufentscheidung getroffen werden.

Die Praxis zeigt, dass es aufgrund verschiedener Einsatzanforderungen durchaus sinnvoll sein kann, mehrere unterschiedliche Gerätetypen für die Beschaffung auszuwählen. Die Gerätevielfalt sollte aber eingeschränkt werden, damit der Support einfacher ist.

SYS.3.1.M16 Zentrale Administration und Verwaltung von Laptops (H)

Die Administration für mobile Endgeräte ist keine einfache Aufgabe, vor allem bei großen Institutionen und bei Benutzern, die sich häufig und in aller Welt bewegen. Es gibt Tools, die eine zentrale Administration und die Umsetzung von Sicherheitsrichtlinien erleichtern. Durch eine zentrale Administration können nicht nur

Software und Informationen verteilt, sondern auch die institutionseigenen Sicherheitsrichtlinien auf den Laptops durchgesetzt werden, z. B. für Authentisierung, Zugriff oder Datensicherung.

Wird eine Software zum zentralen Laptop-Management eingesetzt, synchronisieren sich die Laptops mit einem Server. Dabei lassen sich nicht nur Daten abgleichen, sondern auch Sicherheitsvorgaben technisch forcieren, indem sicherheitsrelevante Einstellungen auf ihre vorgegebenen Werte zurückgesetzt werden. Typische Funktionen solcher Tools zum zentralen Laptop-Management sind unter anderem:

- Datensicherungen können zentral durchgeführt werden, ohne dass die Benutzer sich darum kümmern müssen. Ebenso können Vorgaben gemacht werden, wann bzw. wie oft Daten zu sichern oder zu synchronisieren sind und welche Randbedingungen dabei eingehalten werden müssen.
- Es besteht die Möglichkeit, Rückmeldungen über den Status der Laptops zu erhalten und Diagnosen remote durchführen zu können.
- Es können Benutzerprofile angelegt werden, um die Benutzerverwaltung zu vereinfachen.
- Es lassen sich Passwortregeln und andere Sicherheitsregeln vorgeben.

Ein Tool zum zentralen Laptop-Management sollte möglichst alle in der Institution eingesetzten Betriebssysteme unterstützen, damit nicht mehrere solcher Tools parallel eingesetzt werden müssen. Dasselbe gilt ebenso natürlich für die eingesetzte Groupware und E-Mail-Plattform. Vertiefende Informationen sind auch in SYS.3.2.2 Mobile Device Management zu finden.

SYS.3.1.M17 Sammelaufbewahrung (H)

Sind in einer Institution viele Laptops im mobilen Einsatz und wechseln die Benutzer häufig, kann es angebracht sein, die zeitweise nicht genutzten Geräte in einer Sammelaufbewahrung (Pool) zu halten. Der dafür genutzte Raum sollte den Anforderungen aus INF.5 *Technikraum* entsprechen.

Darüber hinaus ist die Stromversorgung der Laptops sicherzustellen, damit die Batterien dieser Geräte den sofortigen Einsatz erlauben (siehe SYS.3.1.M11 *Sicherstellung der Energieversorgung*). Zusätzlich müssen die Rücknahme und die Ausgabe von tragbaren IT-Systemen dokumentiert werden (siehe SYS.3.1.M7 *Geregelte Übergabe und Rücknahme eines Laptops*).

SYS.3.1.M18 Einsatz von Diebstahl-Sicherungen (H)

Diebstahl-Sicherungen sind überall dort einzusetzen, wo große Werte zu schützen sind bzw. dort, wo andere Maßnahmen nicht umgesetzt werden können, wie etwa bei Laptops im mobilen Einsatz. Diebstahl-Sicherungen sind außerdem dort sinnvoll, wo Publikumsverkehr herrscht oder die Fluktuation von Benutzern sehr hoch ist. Dabei sollte immer bedacht werden, dass die zu schützenden Werte nur zu einem kleinen Teil aus den Wiederbeschaffungskosten für das Gerät bestehen, sondern bei Laptops der Wert der darauf gespeicherten Daten berücksichtigt werden muss.

Verhindern einer Cold-Boot-Attacke
In Bereichen, die nicht ausreichend gegen unbefugten Zutritt geschützt sind, könnte beispielsweise durch eine Cold-Boot-Attacke der Arbeitsspeicher ausgelesen werden. Gleiches gilt für Systeme, die durch "Suspend to RAM" in einen Energiesparmodus versetzt wurden.

Bei einer Cold-Boot-Attacke werden die Speicherbausteine stark gekühlt, bevor das System ausgeschaltet wird. Der Speicherinhalt bleibt dadurch mehrere Minuten erhalten und kann währenddessen mit geeignetem Gerät ausgelesen werden.

Cold-Boot-Attacken lassen sich nur verhindert, wenn Angreifer nicht ungestört auf den Arbeitsspeicher eines aktiven IT-Systems zugreifen können. Ein Zugriffsschutz, wie ein physisch verriegeltes Computer-Gehäuse, erschwert es, ein IT-System unbefugt zu öffnen, um den Arbeitsspeicher zu kühlen und auszubauen, kann es aber nicht dauerhaft unterbinden. Daher sollte ein unbenutzter Laptop stets ausgeschaltet werden, wenn er nicht in einem zutrittsgeschützten Bereich steht.

Arten von Diebstahl-Sicherungen
Auf dem Markt sind die unterschiedlichsten Diebstahl-Sicherungen erhältlich. Diese können zunächst in mechanische und elektronische Sicherungen unterteilt werden.

Zu den mechanischen Sicherungen gehören unter anderem Kabelsicherungen, Gehäusesicherungen (um das Gehäuse gegen Öffnung zu schützen), Sicherheitsplatten und Sicherheitsgehäuse. Es gibt hier zum einem Hardware-Sicherungen, die dem Diebstahl von IT-Geräten vorbeugen, z. B. indem der Laptop mit dem Schreibtisch verbunden wird. Es gibt zum anderen auch eine Reihe von Sicherungsmechanismen, die verhindern sollen, dass das Gehäuse geöffnet wird. Damit soll vorgebeugt werden, dass Angreifer Teile stehlen oder sicherheitsrelevante Einstellungen manipulieren, wie zum Beispiel Sicherheitskarten entfernen.

Bei der Beschaffung mechanischer Sicherungen ist die Wahl eines guten Schlosses wichtig, das über eine auf die jeweiligen Bedürfnisse abgestimmte Schließanlage verfügt. Je nach Produkt sind verschiedene Schließanlagen möglich:

- gleichschließend: Ein Schlüssel passt auf alle Gerätesicherungen einer Institution, Abteilung etc. Das hat den Vorteil, dass der Aufwand für die Schlüsselverwaltung geringer ist. Es bedeutet jedoch auch, dass sehr viele gleichartige Schlüssel im Umlauf sein können und dass im Schadensfall häufig keine Beweissicherung möglich ist.
- verschiedenschließend: Jede Gerätesicherung hat einen individuellen Schlüssel. Das hat den Nachteil, dass der Aufwand für die Schlüsselverwaltung höher ist. Es hat aber den Vorteil, dass es weniger Schlüsseldubletten gibt.
- Hauptschlüsselsystem: Jede Gerätesicherung hat einen individuellen Schlüssel, kann zusätzlich aber auch durch einen Hauptschlüssel geöffnet werden. Das hat den Vorteil, dass der Aufwand für die Schlüsselverwaltung geringer ist. Es hat aber den Nachteil, dass solche Systeme teurer in der Anschaffung sind.

Die meisten Laptops haben einen kleinen Schlitz, der mit einem Ketten- oder Schloss-Symbol gekennzeichnet ist. Diese kleine Öffnung befindet sich seitlich oder hinten am Gerät. Es gibt eine breite Palette von Kabelsicherungen und anderen Produkten, die diese Öffnung für die Sicherung von Geräten nutzt.

Bei Kabelsicherungen muss dann nur eine Kabelschlinge um ein solides Objekt in der Nähe des Gerätes gelegt, das zugehörige Schloss durch die entstandene Lasche gezogen und abgeschlossen werden.

Für Geräte, die diese Öffnung nicht haben, oder bei denen diese nicht stark genug ist, gibt es Sicherungsprodukte, bei denen eine stabile Platte auf das Gerät geklebt wird. An dieser wird dann das Sicherungskabel befestigt.

Daneben gibt es elektronische Sicherungen, die beispielsweise einen akustischen Abschreckungs-Alarm am Gerät selber auslösen, der potenzielle Diebe dazu bringen soll, den Laptop liegen zu lassen.

Bei Neuanschaffung von Laptops sollte darauf geachtet werden, dass sie Ösen am Gehäuse besitzen, um sie an anderen Gegenständen befestigen zu können.

2.2 Maßnahmen zum Baustein SYS.2.1 Allgemeiner Client

SYS.3.1.SYS.2.1.M1 Sichere Benutzerauthentisierung (B)

Jeder Laptop sollte mit einem Zugriffsschutz versehen werden, der verhindert, dass er unberechtigt benutzt werden kann. So ist es in nahezu allen Betriebssystemen möglich, Anmeldepasswörter einzurichten und diese mit geeigneten Restriktionen zu versehen (z. B. Mindestlänge, Lebensdauer). Da diese Bordmittel nur begrenzt sicher sind, empfiehlt es sich bei Laptops mit schützenswerten Daten, zusätzliche Sicherheitshard- oder -software einzusetzen. Dazu gehören beispielsweise Chipkarten oder Token, die die Authentisierung absichern.

Sind die Daten auf dem Laptop nicht verschlüsselt, sollte verboten werden, dass Mitarbeiter schutzbedürftige Informationen auf der Festplatte speichern (siehe SYS3.1.M13 *Verschlüsselung von Laptops*). Stattdessen sollten sie auf verschlüsselten mobilen Datenträgern gespeichert werden, z. B. USB-Sticks. Diese sind dann getrennt vom Laptop aufzubewahren.

Bei kurzen Arbeitsunterbrechungen muss unbedingt ein Zugriffsschutz aktiviert werden, z. B. ein kennwortgeschützter Bildschirmschoner. Ist es absehbar, dass die Unterbrechung länger dauert, ist der Laptop auszuschalten.

SYS.3.1.SYS.2.1.M6 Einsatz von Schutzprogrammen gegen Schadsoftware (B)

Um sich vor Schadprogrammen zu schützen, können unterschiedliche Wirkprinzipien genutzt werden (siehe OPS.1.1.4 *Schutz vor Schadprogrammen*). Antivirenprogramme, die IT-Systeme nach sämtlichen bekannten Schadprogrammen durchsuchen, sind ein wirksames Mittel in der Schadprogramm-Prävention. Daher müssen sie abhängig vom installierten Betriebssystem und anderer vorhandener Schutzmechanismen installiert und aktiviert sein.

Regelmäßige Untersuchung des gesamten Datenbestands
Auch wenn das Antivirenprogramm bei jedem Dateizugriff auf Schadprogramme prüft, müssen regelmäßig alle Dateien auf dem Laptop durchsucht werden. So können auch Schadprogramme gefunden werden, für die es noch keine Erkennungssignatur gab, als sie gespeichert wurden. In derartigen Fällen muss beispielsweise untersucht werden, ob das Schadprogramm bereits vertrauliche Daten gesammelt, Schutzfunktionen deaktiviert oder Code aus dem Internet nachgeladen hat.

Aus Performance-Gründen sollte der Datenbestand nur vollständig überprüft werden, wenn die IT-Ressourcen nicht stark beansprucht sind. Ideal ist es, wenn die Software überwacht, ob der Laptop ausgelastet ist und dessen "Arbeitspausen" automatisch nutzt, um ihn zu überprüfen. Das Antivirenprogramm könnte z. B. auch mit dem Start des Bildschirmschoners gekoppelt werden.

Datenaustausch und Datenübertragung
Daten, die versendet werden sollen, müssen unmittelbar vor dem Versand auf Schadprogramme geprüft werden. Analog müssen empfangene Daten unmittelbar nach dem Empfang auf Schadprogramme geprüft werden. Diese Überprüfungen sind sowohl erforderlich, wenn auf Datenträger zugegriffen wird als auch bei der Datenübertragung über Kommunikationsverbindungen. Sie sollten so weit wie möglich automatisiert werden.

Wechselwirkungen mit Verschlüsselungstechniken
Wenn Verschlüsselungstechniken eingesetzt werden, ist zu bedenken, wie sich das auf den Schutz vor Schadprogrammen auswirkt. Werden Daten verschlüsselt, so können Systemkomponenten bzw. Anwendungen auf diese Daten nicht zugreifen, solange sie nicht über die entsprechenden Schlüssel verfügen. Das impliziert, dass ein Antivirenprogramm entweder im Kontext des Benutzers laufen oder mit den entsprechenden kryptografischen Schlüsseln ausgestattet werden muss, um eine verschlüsselte Datei auf Schadprogramme überprüfen zu können. Wird jedoch die Benutzer-Kennung, unter der das Antivirenprogramm ausgeführt wird, mit den entsprechenden kryptografischen Schlüsseln ausgestattet, entstehen neue Sicherheitsrisiken, die es zu vermeiden gilt. Daher wird der Einsatz eines residenten Antivirenprogramms empfohlen, das die Prüfung auf Schadprogramme im Benutzer-Kontext bei jedem Zugriff auf eine Datei durchführt.

Schutz vor unerlaubter Deaktivierung oder Änderung
Die Antivirenprogramme auf den Laptops müssen so konfiguriert sein, dass die Benutzer keine sicherheitsrelevanten Einstellungen verändern können. Insbesondere muss sichergestellt sein, dass die Benutzer sie nicht deaktivieren können.

2.3 Maßnahmen zum Baustein CON.3 Datensicherungskonzept

Dieser Abschnitt enthält allgemeine Informationen zum Datensicherungskonzept für Laptops.

Laptops sind in aller Regel nicht permanent in ein Netz eingebunden. Der Datenaustausch mit anderen IT-Systemen erfolgt üblicherweise über temporäre Netzanbindungen. Letztere können beispielsweise durch ein Virtual Private Network (VPN) oder direkten Anschluss an ein LAN nach Rückkehr zum Arbeitsplatz realisiert sein. Anders als bei stationären Clients ist es daher bei Laptops meist unvermeidbar, dass Daten zumindest zeitweise lokal anstatt auf einem zentralen Server gespeichert werden. Deshalb ist mithilfe geeigneter Datensicherungsmaßnahmen vorzubeugen, dass Daten verloren gehen.

Generell bieten sich folgende Verfahren zur Datensicherung an:

- **Datensicherung auf externen Datenträgern**
  Der Vorteil dieses Verfahrens ist, dass die Datensicherung an nahezu jedem Ort und zu jeder Zeit erfolgen kann. Nachteilig ist, dass zusätzliche Datenträger, z. B. externe Festplatten, mitgeführt werden müssen und dass für den Benutzer mehr Aufwand für die ordnungsgemäße Handhabung der Datenträger entsteht. Die Datenträger sollten eine ausreichende Speicherkapazität besitzen, sodass der Benutzer nicht mehrere Datenträger pro Sicherungsvorgang verwenden muss. Bei unverschlüsselter Datenhaltung ergibt sich außerdem die Gefahr, dass Datenträger abhandenkommen und dadurch schützenswerte Daten kompromittiert werden können. Die Datenträger und der Laptop sollten möglichst getrennt voneinander aufbewahrt werden, damit bei Verlust oder Diebstahl des Laptops nicht beide abhandenkommen.
  Die Speicherung auf externen Datenträgern zur Datensicherung bietet sich insbesondere an, wenn auch der Datenaustausch mit anderen IT-Systemen über externe Datenträger erfolgt. Diese beiden Prozesse können auch kombiniert werden. Nach Rückkehr zum Arbeitsplatz müssen die Datensicherungen auf den Datenträgern in das Backup-System oder in das Produktivsystem bzw. die zentrale Datenhaltung der Institution eingepflegt werden.

- **Datensicherung über temporäre Netzverbindungen**
  Wenn es möglich ist, den Laptop regelmäßig an ein Netz anzuschließen, beispielsweise über VPNs, können die lokalen Daten auch über die Netzanbindung gesichert werden. Vorteilhaft ist hier, dass der Benutzer keine Datenträger verwalten und mitführen muss. Weiterhin lässt sich das Verfahren weitgehend automatisieren, beispielsweise kann die Datensicherung beim Einsatz von VPNs nach jedem Einwahlvorgang automatisch gestartet werden.
  Entscheidend bei der Datensicherung über eine temporäre Netzverbindung ist, dass deren Bandbreite für das Volumen der zu sichernden Daten ausreichen muss. Die Datenübertragung darf nicht zu lange dauern und nicht zu übermäßigen Verzögerungen führen, wenn der Benutzer gleichzeitig auf entfernte Ressourcen zugreifen muss. Einige Datensicherungsprogramme bieten daher die Möglichkeit an, lediglich Informationen über die Änderungen des Datenbestands seit der letzten Datensicherung über die Netzverbindung zu übertragen. In vielen Fällen kann hierdurch das zu transportierende Datenvolumen stark reduziert werden.
  Die Datensicherungssoftware muss unerwartete Verbindungsabbrüche erkennen und ordnungsgemäß behandeln. Die Konsistenz der gesicherten Daten darf durch Verbindungsabbrüche nicht beeinträchtigt werden.

Bei beiden Verfahren zur Datensicherung ist es wünschenswert, das Volumen der zu sichernden Daten zu minimieren. Neben verlustfreien Kompressionsverfahren, die in vielen Datensicherungsprogrammen integriert sind, können auch inkrementelle oder differenzielle Sicherungsverfahren eingesetzt werden. Hierdurch erhöht sich jedoch eventuell der Aufwand für die Wiederherstellung einer Datensicherung.

Die Datensicherung sollte möglichst weitgehend automatisiert werden, sodass die Benutzer nur wenige Aktionen selbst durchführen müssen. Wenn die Mitarbeit der Benutzer erforderlich ist, sollten sie dazu verpflichtet werden, Datensicherungen regelmäßig durchzuführen. Schließlich sollte sporadisch geprüft werden, ob angelegte Datensicherungen wiederhergestellt werden können.

3. Weiterführende Informationen

3.1 Wissenswertes

Das BSI hat im Rahmen der ISi-Reihe das folgende Dokument veröffentlicht:

Sicherer Fernzugriff auf das interne Netz (ISi-S): BSI-Studie zur Internet-Sicherheit (ISi-S), Bundesamt für Sicherheit in der Informationstechnik (BSI), September 2010

3.2 Quellenverweise

Für diese Umsetzungshinweise sind keine Quellenverweise vorhanden.