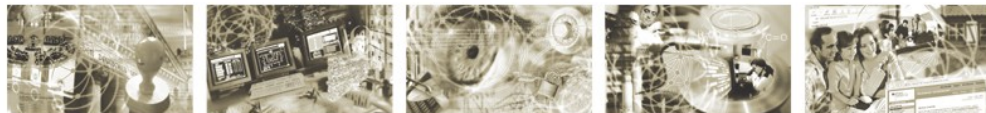




Bundesamt
für Sicherheit in der
Informationstechnik



Handreichung Informationssicherheit für deutsche Passbehörden

Auf der Basis der BSI-Standards und der IT-Grundschutz-Kataloge

Version 1.5

Bundesamt für Sicherheit in der Informationstechnik

Postfach 20 03 63

53133 Bonn

Tel.: +49 22899 9582-333

E-Mail: sicherheitsberatung@bsi.bund.de

Internet: <http://www.bsi.bund.de>

© Bundesamt für Sicherheit in der Informationstechnik 2008

Inhaltsverzeichnis

1	Einleitung.....	5
2	Geltungsbereich und Abgrenzung.....	6
3	IT-Grundschutz.....	8
3.1	Beispiel für organisatorische Aspekte.....	8
3.2	Beispiel für infrastrukturelle Aspekte.....	8
3.3	Beispiel für personelle Aspekte.....	9
3.4	Beispiel für technische Aspekte.....	10
4	Grundlegende Sicherheitsmaßnahmen.....	12
4.1	Allgemeine Aspekte.....	12
4.2	Gebäude und Verkabelung.....	13
4.3	Anwendungen.....	14
4.3.1	Datenbanksysteme.....	14
4.3.2	Datensicherungssysteme.....	14
4.4	IT-Systeme.....	15
4.4.1	Arbeitsplatzrechner.....	15
4.4.2	Datenbankserver, Infrastrukturserver.....	17
4.5	Netze.....	20
4.5.1	Lokales Netzwerk der Passbehörden.....	20
4.5.2	Transportwege innerhalb der Passbehörden.....	20
4.5.3	Transportwege von der Passbehörde zu anderen Stellen.....	20
4.6	Räume.....	21
4.6.1	Büroraum.....	21
4.6.2	Serverraum.....	21
5	Schlussbemerkungen.....	22

1 Einleitung

Durch die zunehmende Durchdringung unserer Gesellschaft mit Informationstechnik und die zunehmende Nutzung neuer Technologien in kritischen Geschäftsprozessen nimmt die Informationssicherheit eine immer zentralere Rolle ein. Mit der Einführung des ePasses Stufe 2 erwarten die Bürgerinnen und Bürger ein hohes Maß an Sorgfalt und Sicherheit im Umgang mit ihren personenbezogenen Daten. Dies zeigen auch die aktuellen Diskussionen über dieses Thema in den Medien.

Die Handreichung gibt einen Überblick über Standard-Sicherheitsmaßnahmen, die dazu geeignet sind, in den Passbehörden vor Ort das gesetzlich geforderte Schutzniveau einzuhalten. Darüber hinaus ist ein behördenpezifisches Sicherheitskonzept anzufertigen.

Als ganzheitliches Konzept für IT-Sicherheit hat sich das Vorgehen nach IT-Grundschatz zusammen mit den IT-Grundschatz-Katalogen des BSI als Standard etabliert. Diese vom BSI seit 1994 eingeführte und weiterentwickelte Methode bietet sowohl eine Vorgehensweise für den Aufbau einer Sicherheitsorganisation, als auch eine umfassende Basis für die Risikobewertung, die Überprüfung des vorhandenen IT-Sicherheitsniveaus und die Implementierung der angemessenen IT-Sicherheit.

Die von der Bundesregierung in der Drucksache 16/8477 des Bundestags angekündigte Bewertung aus datenschutzrechtlicher Sicht ist als wichtige Ergänzung in Hinblick auf den besonderen Schutzbedarf personenbezogener Daten zu diesem Dokument zu sehen. Grundsätzlich werden durch die IT-Grundschatzkonforme Verfahrensausgestaltungen datenschutzrelevante Anforderungen bereits abgedeckt. Beispielsweise handelt es sich bei den Schutzzielen Vertraulichkeit, Verfügbarkeit und Integrität von Information um gemeinsame Ziele des Datenschutzes und der Informationssicherheit.

Eine Zusammenfassung für datenschutzrelevante Maßnahmen bietet der optionale Baustein „1.5 Datenschutz“ (<http://www.bsi.bund.de/gshb/deutsch/baust/b01005.htm>) der IT-Grundschatz-Kataloge.

2 Geltungsbereich und Abgrenzung

Die vorliegende Handreichung ist als ergänzende Unterlage für die Nutzung der ePass-Anwendung und -Infrastruktur anzusehen und speziell für die grundlegende Sicherung der u.g. Schutzziele heranzuziehen. Der Geltungsbereich erstreckt sich dabei auf die deutschen Passbehörden der einzelnen Bundesländer.

Die genannten Maßnahmen sind nicht abschließend oder vollumfänglich, sondern dienen vielmehr dem Ziel, ein vergleichbares Standard-Niveau an Informationssicherheit bei den erfassenden und verarbeitenden Stellen zu erreichen. Neben diesen Maßnahmen sollte ein verfahrensbezogenes Informationssicherheitskonzept gemäß der einschlägigen Datenschutzgesetze erstellt werden. Empfehlenswert ist vor dem Hintergrund der hohen Vertraulichkeit weiterhin ein organisationsbezogenes Sicherheitskonzept auf der Basis von IT-Grundschutz je Passbehörde. Die Konzepte sollten den gesamten in der Zuständigkeit der Passbehörden liegenden Zuständigkeitsbereich berücksichtigen, in diesem Fall das gesamte Antragsverfahren. Gegenstand dieser Handreichung ist konkret die Ausstellung des ePasses im Antragsverfahren. Dabei ist die Vorgehensweise auf der Basis von IT-Grundschutz einzuhalten.

IT-Grundschutz bietet eine einfache Methode, dem Stand der Technik entsprechende Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Die IT-Grundschutz-Kataloge beinhalten Baustein-, Maßnahmen- und Gefährdungskataloge. Die Vorgehensweise nach IT-Grundschutz, Ausführungen zum Informationssicherheitsmanagement und zur Risikoanalyse sind in den BSI-Standards zu finden. Die IT-Grundschutz-Kataloge werden ständig bedarfsorientiert aktualisiert und ergänzt. Das BSI stellt weiterhin zahlreiche Werkzeuge zur Verfügung, um ein angemessenes Sicherheitsniveau zu erreichen, wie z. B. das GSTOOL und der Leitfaden IT-Sicherheit.

Wie andere Identitätsnachweise sind auch der ePass und seine Informationen vor Bedrohungen, wie z.B. Diebstahl, Manipulation (Fälschung), „Man in the Middle“- und Skimming-Angriffe, zu schützen. Dies schließt den Schutz der mit ihm verbundenen Verfahren, Systeme und Schnittstellen, wie zum Beispiel Reisepassanwendungen mit ein.

Gefahren für die Informationssicherheit können sich aus organisatorischen, personellen, infrastrukturellen und technischen Gründen ergeben. Hierzu gehört zum Beispiel die Zutrittskontrolle zu den genutzten zentralen IT-Systemen und Servern.

Auf folgende Schutzziele geht diese Handreichung im Detail ein:

- a. Vertraulichkeit der Antragsdaten – Die innerhalb des Beantragungsprozesses erhobenen, erfassten und an den Produzenten zu übermittelnden Informationen sind ihrem Charakter nach als schützenswerte, personenbezogene Daten (biometrische und passbezogene Daten), einzustufen. Deren Bekanntwerden oder missbräuchliche Verwendung kann die Betroffenen erheblich beeinträchtigen und für die Passbehörde einen andauernden Imageverlust darstellen. Diese Forderung gilt sowohl für die lokale Speicherung der Daten als auch für die Übertragung der Informationen an den Passhersteller. Zur Gewährleistung der Vertraulichkeit der Informationen bietet sich beispielsweise ein Rollenmodell an, das den Zugriff auf die entsprechenden Informationen regelt. Die Vertraulichkeit der Informationen sollte durch entsprechende Verfahren gewährleistet werden. Bei der Auswahl entsprechender Verfahren / Produkte sollten in diesem Fall die Maßnahmen:
 - M 2.164 Auswahl eines geeigneten kryptographischen Verfahrens (<http://www.bsi.bund.de/gshb/deutsch/m/m02164.htm>) und

- M 2.165 Auswahl eines geeigneten kryptographischen Produktes
(<http://www.bsi.bund.de/gshb/deutsch/m/m02165.htm>) berücksichtigt werden.
- b. Integrität der Antragsdaten – Die erfassten Daten sind vor einer absichtlichen oder unabsichtlichen Veränderung zu schützen. Die Bindung des Inhabers an das Passdokument und damit seine verbürgte Identität ist die zentrale Aufgabe des Identitätsdokumentes. Dies spiegelt sich in der Korrektheit der enthaltenen Daten wieder. D. h. dass diese Informationen bereits bei der Erhebung (im Antragsverfahren) verifiziert werden müssen und ausschließlich unverändert in den Produktionsprozess eingehen dürfen. Eine missbräuchliche Änderung der Daten kann zur Bestätigung einer falschen Identität und damit zu erheblichen Beeinträchtigungen der Betroffenen führen. Damit einher geht ein erheblicher Image- und Vertrauensverlust für die Behörde. Besonders sensitiv sind hierfür die Prozesse zum Nachweis der Identität, der Erfassung der biometrischen Daten (Scannen von Gesichtsbild, Fingerabdrücken und der Unterschrift), das Zwischenspeichern dieser Daten in der Behörde sowie die Übermittlung dieser Daten an den Produzenten. Die Integrität der Informationen sollte auf Grund des höheren Schutzbedarfs durch den Einsatz von geeigneten Verfahren (siehe 2.a) oder gleichwertigen Maßnahmen sichergestellt werden.
- c. Authentizität der Antragsdaten – Im Rahmen der Erfassung der ePass-Antragsdaten ist darauf zu achten, dass diese Daten nicht, auch nicht in Teilen, ausgetauscht oder vertauscht werden können. Entsprechend der Integrität der Antragsdaten ist besonders die Echtheit der vom Antragsteller vorgelegten Identitätsnachweise (z. B. Personalausweis, Pass, Führerschein oder Zeugenerklärungen) zu prüfen, um einer Erschleichung falscher Identitäten entgegenwirken zu können. Mangelnde Authentizität dieser Daten könnte dazu führen, dass eine eindeutige Identifikation des Inhabers nicht möglich ist bzw. eine nicht zutreffende Identität geschaffen wird.
- d. Verfügbarkeit bei der Beantragung: Fallen für den Beantragungsprozess erforderliche Geräte bzw. sonstige Ressourcen (z. B.: Erfassungssoftware, Lesegerät) aus, können in der Regel Ausweichverfahren (z. B.: vorläufige Dokumente) genutzt werden. Ausfallzeiten von bis zu 48 Stunden werden als unproblematisch angesehen. Sollte der Grundwert Verfügbarkeit später höherem Schutzbedarf folgen, so sind Maßnahmen aus der ergänzenden Sicherheitsanalyse bzw. ergänzenden Risikoanalyse entsprechend anzuwenden.

Eine zusätzliche rechtliche Randbedingung, die bei Beantragung des ePass Stufe 2 von den jeweiligen Passämtern zu beachten ist, ist die gesetzliche Vorgabe, dass die „bei der Passbehörde gespeicherten Fingerabdrücke [...] spätestens nach Aushändigung des Passes an den Passbewerber zu löschen“ sind (§ 16 Abs. 2 PassG).

3 IT-Grundschutz

Informationen sind ein wesentlicher Wert für Unternehmen und Behörden und müssen daher angemessen geschützt werden. Die meisten Informationen werden heutzutage zumindest teilweise mit Informationstechnik (IT) erstellt, gespeichert, transportiert oder weiterverarbeitet. Moderne Geschäftsprozesse sind heute in Wirtschaft und Verwaltung ohne IT-Unterstützung längst nicht mehr vorstellbar. Die Ansprüche an die Verfügbarkeit, Integrität und Vertraulichkeit von Verarbeitungsprozessen werden höher und komplexer, sodass die Sicherheit von Informationen immer mehr an Bedeutung gewinnt. Allerdings ist Informationssicherheit nicht nur eine Frage der Technik, sondern hängt in erheblichem Maße von den organisatorischen und personellen Rahmenbedingungen ab.

Bei der Betrachtung und Beurteilung von Sicherheit in einer Behörde oder einem Unternehmen sollten organisatorische, infrastrukturelle, personelle und technische Aspekte beachtet werden.

3.1 Beispiel für organisatorische Aspekte

Urlaubszeit-Reisezeit: Der Software-Verantwortliche für die Beantragung von Reisepässen macht für die Dauer von 6 Wochen Urlaub im brasilianischen Dschungel. Während seiner Abwesenheit ergibt sich ein kleineres Problem mit der Software im Bereich des Passwesens. Ein unzureichend geschulter und nur oberflächlich eingewiesener Vertreter bastelt am System mit der problembehafteten Software herum, um Fehler zu beheben und das System wieder in Gang zu setzen. Dabei verwendet er seinen privaten USB-Stick, unwissend, dass sich auf diesem ein Computer-Virus befindet, welcher sich in der Folge sehr schnell im Wirkbetrieb auf allen PCs ausbreitet. Durch die rasante Verbreitung wird ein Totalausfall von einer ganzen Woche verursacht, in der alle betroffenen PCs bereinigt und neu aufgesetzt werden müssen. In dieser Zeit können auch keine Pässe ausgestellt werden. Die Antragsteller sind verständlicherweise höchst unzufrieden.

Damit Fälle wie im vorgenannten Szenario gar nicht erst geschehen, sollte eine klare Rollenverteilung in der Institution erfolgen, in der die Frage: "Wer macht wann wo was?" geklärt und nach Möglichkeit schriftlich fixiert wird. Mit einbezogen werden sollte hier unbedingt auch eine Vertreterregelung bei Fällen von Urlaub, Krankheit oder Ausscheiden aus der Institution/Behörde.

In Hinblick auf die Vertraulichkeit der ePass-Daten ist das Mitbringen privater IT, dazu zählen neben USB-Sticks auch CDs, DVDs und andere Datenträger, gänzlich zu untersagen. In jedem Fall ist dafür Sorge zu tragen, dass private IT nicht im Wirksystem zum Einsatz gebracht wird. Diese Anforderungen sind nach Möglichkeit mit technischen Maßnahmen zu kontrollieren und umzusetzen (vgl. auch Virenschutz-Konzepte 4.1).

3.2 Beispiel für infrastrukturelle Aspekte

Während einer seltenen Hitzeperiode in den Sommermonaten wird in einem nicht klimatisierten Raum im Erdgeschoss zwecks Raumbelüftung das ebenerdige Fenster zum Hinterhof geöffnet und bleibt auch bei kurzer Abwesenheit des Mitarbeiters offen. Ein Angreifer nutzt die Gelegenheit, nachdem er sich zuvor durch ein nicht ausreichend gesichertes Tor auf das Gelände geschlichen hat,

und dringt durch das geöffnete Fenster in den Raum ein. Da zu dieser Zeit gerade Mittagspause ist, hat er genügend Zeit, sich unerlaubt an den PCs zu schaffen zu machen. Über eine Boot-CD ist der Passwortschutz relativ schnell umgangen und sensible Daten wechseln den Besitzer. Der Angreifer wird allerdings dabei überrascht und versucht zu fliehen. Dabei stolpert er über ein lose im Raum verlegtes Stromkabel eines wichtigen Rechners und unterbricht damit die Stromzufuhr. Die Folgen des Stromausfalls und die erforderliche Wiederherstellung nimmt einen kompletten Arbeitstag in Anspruch. Glück im Unglück war dabei noch, dass der Angreifer die Daten lediglich kopiert und nicht manipuliert hat. Die Zeit dazu wäre ausreichend gewesen. Die Überprüfung, ob der Datenbestand noch in unveränderter Weise vorhanden ist, nimmt mindestens einen weiteren halben Arbeitstag in Anspruch.

Zur Absicherung des Geländes gibt es viele technische Möglichkeiten, wie beispielsweise die Erhöhung des Zaunes und das Verschließen von nur vorübergehend genutzten Zugangstoren. Je nach Sicherheitsbedarf ist auch der Einsatz von Überwachungskameras oder Ähnlichem in die Überlegungen mit einzubeziehen.

Auf jeden Fall sollten die Mitarbeiter aber dahingehend sensibilisiert und geschult werden, die Fenster und Türen auch bei vorübergehender Abwesenheit zu verschließen sind. Da sich in vielen Büroräumen je nach Ausstattung hochwertige Geräte befinden, wäre schon allein aus Gründen der Raumüberhitzung bei hochsommerlichen Temperaturen die Anschaffung eines Klimagerätes oder einer Klimaanlage überlegenswert.

Server sollten nur in besonders gesicherten Räumen betrieben werden, zu denen nur wenige Berechtigte und deren Vertreter Zutritt haben. Damit kurzfristige Stromausfälle nicht zu einem längerfristigen Systemausfall führen, sollte eine unterbrechungsfreie Stromversorgung (USV) eingesetzt sein.

3.3 Beispiel für personelle Aspekte

Ein Mitarbeiter wählt als Passwort für die Bildschirmsperre an seinem Arbeitsplatz-Computer das Trivialpasswort "Schnuffi", den Namen seines Haustiers. Das letzte Passwort war der Name seiner Freundin. Aus Verbundenheit zu seiner Freundin und zu Schnuffi hat der Mitarbeiter selbstverständlich ein Foto von beiden auf dem Schreibtisch. Solche Passwörter können von Angreifern leicht erraten werden.

Die Mitarbeiter sollten für sichere Passwörter sensibilisiert werden. Damit ist gemeint, dass ein gutes Passwort aus einer Kombination aus Buchstaben, Ziffern und Sonderzeichen besteht, nicht in Wörterbüchern zu finden ist und schwer zu erraten ist.

Auch Bildschirmsperren sollten sich nur unter Verwendung von starken Passwörtern aufheben lassen.

Die Sensibilisierung aller Mitarbeiterinnen und Mitarbeiter für die Wahrung der Informationssicherheit in der Institution/Behörde ist als Basisarbeit unersetzbar.

Die konkrete Maßnahme M 2.11 Regelung des Passwortgebrauchs (<http://www.bsi.bund.de/gshb/deutsch/m/m02011.htm>) ist umzusetzen.

3.4 Beispiel für technische Aspekte

Da der Administrator eines Servers während der Urlaubszeit zahlreiche Kollegen vertreten musste, war es ihm nicht möglich, sicherheitsrelevante Betriebssystemaktualisierungen auf den Server zu installieren. Ein Angreifer nutzte die bekannten Schwachstellen aus und konnte auf alle Daten, die der Server empfangen und verarbeitet hat, zugreifen.

Besonders sicherheitsrelevante Aktualisierungen sollten so schnell wie möglich installiert werden. Hierfür muss ein Prozess für den Umgang mit Patches und Updates auch auf organisatorischer Ebene etabliert sein (z. B. im Rahmen des Änderungsmanagements).

Um die gesamte Software und insbesondere auch die Verschlüsselungsprogramme stets aktuell zu halten, sollte unbedingt ein Patch-Management eingeführt und Verantwortliche hierfür benannt werden. Um sicherstellen zu können, dass die neue Software auch zuverlässig funktioniert, sollte sie vor einem Einsatz im Wirkbetrieb getestet werden. So können viele Arten von Störungen und Sicherheitsvorfällen bereits im Vorfeld vermieden werden.

Die hier aufgeführten Beispiele zeigen, dass Informationssicherheit nicht durch punktuelle Einzelmaßnahmen, sondern nur durch ein umfassendes und ganzheitliches Konzept und einen systematischen Prozess erreicht werden kann. Zu den herausfordernden Aufgaben für Sicherheitsverantwortliche gehört es, den Überblick über die abzusichernden Geschäftsprozesse und die zugehörige IT zu bewahren und angemessene Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Mit dem IT-Grundschutz bietet das BSI hierfür eine bewährte Methode zur Realisierung an.

In dem BSI-Standard 100-2 ist die IT-Grundschutz-Vorgehensweise anwenderfreundlich beschrieben, also wie ein Informationssicherheitsmanagement in der Praxis aufgebaut und betrieben werden kann. Die Aufgaben des Informationssicherheitsmanagements und der Aufbau einer Informationssicherheitsorganisation sind dabei wichtige Themen. Die IT-Grundschutz-Vorgehensweise geht sehr ausführlich darauf ein, wie ein Sicherheitskonzept in der Praxis erstellt und wie angemessene Standard-Sicherheitsmaßnahmen ausgewählt werden können. Auch die Frage, wie Informationssicherheit im laufenden Betrieb aufrechterhalten und verbessert werden kann, wird beantwortet. IT-Grundschutz interpretiert damit die sehr allgemein gehaltenen Anforderungen der Standards ISO 27002 (ehemals ISO 17799) und ISO 27001 und hilft Anwendern in der Praxis bei der Umsetzung mit vielen Hinweisen, Hintergrund-Know-how und Beispielen.

Die IT-Grundschutz-Kataloge enthalten zu den verschiedensten Themenbereichen detaillierte Sammlungen von Gefährdungs- und Maßnahmenbeschreibungen, jeweils in Bausteinen zusammengefasst. Um möglichst nah am Stand der Technik zu bleiben, werden die IT-Grundschutz-Kataloge des BSI ständig fortgeschrieben und bedarfsorientiert weiterentwickelt. Derzeit enthalten die IT-Grundschutz-Kataloge über 70 Bausteine zu technischen und nicht-technischen Themen der Informationssicherheit.

Da die IT-Grundschutz-Kataloge mit der Zeit umfangreicher geworden sind, wird der Ruf nach Beispiel-Sicherheitskonzepten gemäß der IT-Grundschutz-Vorgehensweise immer größer. Hierzu hat das BSI mehrere Beispiel-Profile erarbeitet, die auf unterschiedliche Behördengrößen zugeschnitten sind. Darin wird anhand von Musterbeispielen der Prozess demonstriert, ein Sicherheitskonzept zu planen, umzusetzen und zu pflegen. Außerdem werden Tipps aus der Praxis

sowie spezielle, auf die jeweiligen Anwendergruppen abgestimmte Herangehensweisen an die Problematik vorgestellt.

Nachfolgend werden die grundsätzlichen heranzuziehenden Sicherheitsmaßnahmen für die Passbehörden angeführt. Neben diesen Maßnahmen ist eine Sicherheitskonzeption auf der Basis von IT-Grundschutz zu erstellen, die die notwendige Modellierung der individuellen Passbehörden vornimmt und die entsprechend anzuwendenden Sicherheitsmaßnahmen lokalisiert. Darüber hinaus muss eine ergänzende Sicherheitsanalyse im Sinne des hohen Schutzbedarfs und eventuell eine ergänzende Risikoanalyse abgestimmt werden.

4 Grundlegende Sicherheitsmaßnahmen

Für die folgenden Prozesse und Prozessschritte sind diese Standard-Sicherheitsmaßnahmen (basierend auf den IT-Grundschutz-Katalogen in der 9. Ergänzungslieferung oder der jeweils aktuellen Fassung) anzuwenden:

- IT-gestützte Erfassung der Antragsdaten für Passakte,
- IT-gestützte Erfassung der biometrischen Daten (Scannen von Gesichtsbild, Fingerabdrücken und Unterschrift),
- Zwischenspeichern der Antragsdaten in der Behörde,
- Übermitteln / Versand der Antragsdaten an Produzenten.

Folgende Anwendungen im Sinne des IT-Grundschutzes wurden grundsätzlich betrachtet:

- Passanwendung (Client) /Arbeitsplatzrechner,
- Passanwendung (Server) / Datenbankserver.

Die Datenübertragungsanwendung (Übermittlung der Produktionsdaten von den Antragsbehörden an den Produzenten) sowie der Infrastrukturserver oder die betreffende Netzinfrastruktur wird nicht betrachtet. Weiterhin ist die Betrachtung des Fingerabdruckverfahrens nicht Bestandteil der Maßnahmenauswahl. Beide Prozesse werden bereits hinreichend durch die Technische Richtlinie zur Produktionsdatenerfassung, -qualitätsprüfung und -übermittlung für Pässe (TR PDÜ) als Anlage zur Passdatenerfassungs- und Übermittlungsverordnung (PassDEÜV) geregelt.

Die angeführten IT-Grundschutzmaßnahmen können aufgrund der heterogenen Infrastrukturen der Passbehörden lediglich die Basis für Sicherheitsanforderungen des ePasses bilden. Einzelfallbezogen sind diese auf die jeweiligen örtlichen Gegebenheiten spezifisch anzupassen. Für die Administration ist die sicherere Installation und Inbetriebnahme der Sende- und Empfangs-Clients von Relevanz. Bezüglich der im Beantragungsprozess einzusetzenden Komponenten, des Datenübertragungsformats und weiterer Vorgaben zur Ausgestaltung und Umsetzung des Antrags- und Übermittlungsverfahrens sind die Regelungen der PassDEÜV zu beachten und einzuhalten. Insbesondere sei hier auf die Übergangsfrist Ende Oktober 2009 verwiesen, mit deren Ablauf die Daten ausschließlich unter Verwendung des Xpass-Datenaustauschformats und des OSCITransport-Protokolls übertragen werden müssen.

4.1 Allgemeine Aspekte

Die sichere Verarbeitung von Informationen ist heutzutage für nahezu alle Unternehmen und Behörden von existenzieller Bedeutung. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. Für den Schutz der Informationen reicht es nicht aus, nur technische Sicherheitslösungen einzusetzen. Ein angemessenes Sicherheitsniveau kann nur durch geplantes und organisiertes Vorgehen aller Beteiligten erreicht und aufrechterhalten werden. Voraussetzung für die sinnvolle Umsetzung und Erfolgskontrolle von Sicherheitsmaßnahmen ist eine systematische Vorgehensweise. Für einen Einstieg in dieses Thema ist der Baustein B 1.0

Sicherheitsmanagement (<http://www.bsi.bund.de/gshb/deutsch/baust/b01000.htm>) der IT-Grundschutz-Kataloge zu berücksichtigen.

Die Passbehörden sind zu jedem Zeitpunkt Eigentümer der Daten und verantwortlich für diese. Dies schließt vor allem die Einhaltung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit nachhaltig ein.

In dem Baustein B 1.1 Organisation (<http://www.bsi.bund.de/gshb/deutsch/baust/b01001.htm>) der IT-Grundschutz-Kataloge werden allgemeine und übergreifende Maßnahmen im Organisationsbereich aufgeführt, die als organisatorische Standardmaßnahmen zur Erreichung eines Mindestschutzniveaus erforderlich sind.

In dem Baustein B 1.2 Personal (<http://www.bsi.bund.de/gshb/deutsch/baust/b01002.htm>) werden die übergeordneten IT-Grundschutzmaßnahmen erläutert, die im Bereich Personalwesen durchgeführt werden sollten. Beginnend mit der Einstellung von Mitarbeitern bis hin zu deren Ausscheiden ist eine Vielzahl von Maßnahmen erforderlich. Hierzu gehören beispielsweise Empfehlungen zu:

- der geregelten Einarbeitung/Einweisung neuer Mitarbeiter,
- der Auswahl eines vertrauenswürdigen Administrators und Vertreters,
- Vertretungsregelungen,
- Schulung vor Programmnutzung und zu Sicherheitsmaßnahmen und
- der geregelten Verfahrensweise beim Ausscheiden von Mitarbeitern.

Ziel eines Computer-Viren-Schutzkonzeptes, das im Baustein B 1.6 Computer-Viren-Schutzkonzept (<http://www.bsi.bund.de/gshb/deutsch/baust/b01006.htm>) beschrieben wird, ist es, geeignete Maßnahmen zum Schutz vor Schadprogrammen zusammenzustellen. Es soll gewährleistet sein, dass das Auftreten von Computer-Viren verhindert oder so früh wie möglich erkannt wird. Zusätzlich sind Maßnahmen zu benennen, die Schäden minimieren helfen, wenn ein Schadprogramm nicht rechtzeitig entdeckt werden konnte. Wesentlich ist die konsequente Anwendung der Maßnahmen und die ständige Aktualisierung der eingesetzten technischen Methoden. Diese Forderung begründet sich durch die täglich neu auftretenden Computer-Viren bzw. der Variation schon bekannter Computer-Viren. Durch die Weiterentwicklung von Betriebssystemen, Programmiersprachen und Anwendungssoftware entstehen weitere mögliche Angriffspotentiale für Computer-Viren, so dass rechtzeitig geeignete Gegenmaßnahmen eingeleitet werden müssen.

Wenn Bestandteile des Informationsverbundes nicht selbst, sondern durch externe Dienstleister betrieben werden, ist der Baustein B 1.11 Outsourcing (<http://www.bsi.bund.de/gshb/deutsch/baust/b01011.htm>) anzuwenden und die daraus resultierenden Maßnahmen umzusetzen.

4.2 Gebäude und Verkabelung

Das Gebäude umgibt die aufgestellte Informationstechnik und gewährleistet somit einen äußeren Schutz. Die Infrastruktureinrichtungen des Gebäudes ermöglichen erst den Betrieb. Daher ist einerseits das Bauwerk, also Wände, Decken, Böden, Dach, Fenster und Türen zu betrachten und andererseits alle gebäudeweiten Versorgungseinrichtungen wie Strom, Wasser, Gas, Heizung,

Rohrpost etc. Für den Schutz der Gebäude müssen die Empfehlungen des Baustein B 2.1 Gebäude (<http://www.bsi.bund.de/gshb/deutsch/baust/b02001.htm>) der IT-Grundschutzkataloge umgesetzt werden.

Die elektrotechnische Verkabelung von IT-Systemen und anderen Geräten umfasst alle Kabel und Verteilungen im Gebäude vom Einspeisepunkt des Verteilungsnetzbetreibers bis zu den Elektro-Anschlüssen der Verbraucher. Die ordnungsgemäße und normgerechte Ausführung der elektrotechnischen Verkabelung ist Grundlage für den sicheren IT-Betrieb und ist im Baustein B 2.2 Elektrotechnische Verkabelung (<http://www.bsi.bund.de/gshb/deutsch/baust/b02002.htm>) zu finden. Die IT-Verkabelung umfasst alle Kommunikationskabel und passiven Komponenten (Rangier- bzw. Spleißverteiler, Patchfelder), die in eigener Hoheit der Institution betrieben werden. Sie ist also die physikalische Grundlage der internen Kommunikationsnetze einer Institution. Die IT-Verkabelung reicht von Übergabepunkten aus einem Fremdnetz (z. B. ISDN-Anschluss eines TK-Anbieters, DSL-Anbindung eines Internet-Providers) bis zu den Anschlusspunkten der Netzteilnehmer. Die Empfehlungen des Baustein B 2.12 IT-Verkabelung (<http://www.bsi.bund.de/gshb/deutsch/baust/b02012.htm>) müssen berücksichtigt werden.

4.3 Anwendungen

4.3.1 Datenbanksysteme

Datenbanksysteme sind ein weithin genutztes Hilfsmittel zur rechnergestützten Organisation, Erzeugung, Veränderung und Verwaltung großer Datensammlungen und stellen in vielen Unternehmen und Organisationen die zentrale Informationsbasis zu ihrer Aufgabenerfüllung bereit. Neben dem Schutz der Vertraulichkeit und der Integrität der Daten spielt die Verfügbarkeit des Datenbanksystems eine sehr wichtige Rolle. Daher müssen die Empfehlungen des Bausteins B 5.7 Datenbanken (<http://www.bsi.bund.de/gshb/deutsch/baust/b05007.htm>) der IT-Grundschutzkataloge erfüllt werden.

4.3.2 Datensicherungssysteme

Durch technisches Versagen, versehentliches Löschen oder durch Manipulation können gespeicherte Daten unbrauchbar werden bzw. verloren gehen. Eine Datensicherung soll gewährleisten, dass durch einen redundanten Datenbestand der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen. Hierfür ist es nicht ausreichend, nur statische Informationen wie Konfigurationsdateien zu sichern. Grundsätzlich sollten temporäre Informationen, die nach einem festgelegten Zeitraum wieder gelöscht werden, dauerhaft gesichert und archiviert werden. Für die temporären Informationen im Antragsverfahren - hier explizit die digitalen Fingerabdrücke - ist indes eine dauerhafte Speicherung unzulässig: Die Löschrufen müssen eingehalten werden und die Daten sind von der Datensicherung auszuschließen.

Für die Datensicherung muss der Baustein B 1.4 Datensicherungskonzept (<http://www.bsi.bund.de/gshb/deutsch/baust/b01004.htm>), für die Archivierung der B 1.12 Archivierung (<http://www.bsi.bund.de/gshb/deutsch/baust/b01012.htm>) der IT-Grundschutzkataloge angewendet werden. Besonderes Augenmerk muss in Hinblick auf die Vertraulichkeitsanforderungen des

ePasses gelegt werden: Der Vertraulichkeitsbedarf einer Datei überträgt sich bei einer Datensicherung auf die Sicherungskopie. Bei der Zusammenführung von Sicherungskopien mit gleichem Vertraulichkeitsbedarf auf einem Datenträger, kann sich durch die Kumulation ein höherer Vertraulichkeitsbedarf der gespeicherten Daten ergeben. Anzugeben ist also, wie hoch der Vertraulichkeitsbedarf der einzelnen zu sichernden Daten ist und zusätzlich, welche Kombinationen von Daten einen höheren Vertraulichkeitsbedarf haben als die Daten selbst. Diese Einschätzung wird neben der Erhebung der Löschrufen in der Maßnahme M 6.34 Erhebung der Einflussfaktoren der Datensicherung (<http://www.bsi.bund.de/gshb/deutsch/m/m06034.htm>) gefordert. Aus dieser Einschätzung ergeben sich aufgrund des hohen Schutzbedarfs beispielsweise Anforderungen an die geeignete Aufbewahrung der Backup-Datenträger (<http://www.bsi.bund.de/gshb/deutsch/m/m06020.htm>). Generell sollte die konkrete Vorgehensweise individuell in einem Datensicherungskonzept nach Maßgabe der Maßnahme M 6.33 Entwicklung eines Datensicherungskonzepts (<http://www.bsi.bund.de/gshb/deutsch/m/m06033.htm>) dokumentiert werden.

4.4 IT-Systeme

4.4.1 Arbeitsplatzrechner

In dem Baustein B 3.201 Allgemeiner Client (<http://www.bsi.bund.de/gshb/deutsch/baust/b03201.htm>) wird ein IT-System mit einem beliebigen Betriebssystem betrachtet, das die Trennung von Benutzern zulässt (es sollte mindestens eine Administrator- und eine Benutzer-Umgebung eingerichtet werden können). Typischerweise ist ein solches IT-System vernetzt und wird als Client in einem Client-Server-Netz betrieben.

Je nach dem eingesetzten Betriebssystem sind zusätzlich die weiterführenden Bausteine der IT-Grundschutz-Kataloge zu beachten. Hierzu gehören:

- B 3.204 Client unter Unix (<http://www.bsi.bund.de/gshb/deutsch/baust/b03204.htm>),
- B 3.207 Client unter Windows 2000 (<http://www.bsi.bund.de/gshb/deutsch/baust/b03207.htm>) und
- B 3.209 Client unter Windows XP (<http://www.bsi.bund.de/gshb/deutsch/baust/b03209.htm>).

Der Grundstein für die Sicherheit wird bereits bei der Vorbereitung der Installation gelegt. Vor der Installation sollte festgelegt werden, welche Komponenten des Betriebssystems und welche Anwendungsprogramme und Tools installiert werden sollen. Die getroffenen Entscheidungen müssen so dokumentiert werden, dass gegebenenfalls nachvollzogen werden kann, welche Konfiguration und Softwareausstattung für das System gewählt wurde (siehe M 4.237 Sichere Grundkonfiguration eines IT-Systems <http://www.bsi.bund.de/gshb/deutsch/m/m04237.htm>).

Für die Installation sollten nur Installationsmedien benutzt werden, die aus einer sicheren Quelle stammen (beispielsweise direkt vom Hersteller oder Distributor des Betriebssystems oder Programms). Die Installation des Betriebssystems sollte wenn möglich durchgeführt werden, ohne dass das System an das Netz angeschlossen ist (Offline-Installation). Falls bei der Installation Teile der Pakete über das Netz geladen werden sollen, sollte für die Installation ein eigenes Netz (Testnetz) genutzt werden, das vom übrigen Netz getrennt ist. Von einem Nachladen von Paketen

direkt über das Internet wird dringend abgeraten. Falls es in Ausnahmefällen erforderlich ist, ein System direkt im Produktionsnetz zu installieren, so muss durch geeignete zusätzliche Maßnahmen sichergestellt werden, dass auf das System während der Installation nicht von außen zugegriffen werden kann.

An die eigentliche Installation schließt sich die Grundkonfiguration eines Clients an. In dieser Phase wird die vorläufige Konfiguration, wie sie im Verlauf der Installation vom Installationsprogramm eingerichtet wurde, an die tatsächlichen Gegebenheiten und Anforderungen des IT-Verbunds angepasst, in dem der Client eingesetzt werden soll. Oft werden dabei weitere Programme installiert oder es werden Programme aus einer Standardkonfiguration entfernt, die Einstellungen für den Zugriff auf das Netz werden festgelegt und der Client wird für den Zugriff auf Verzeichnisdienste oder ähnliches konfiguriert. Außerdem werden nicht benötigte Benutzer-Kennungen gelöscht oder deaktiviert, und die Benutzer-Kennungen für die eigentlichen Benutzer werden angelegt.

In dieser Phase werden auch die benötigten Anwendungsprogramme installiert und konfiguriert. Für die Installation und Konfiguration der Anwendungsprogramme sind analoge Sicherheitsaspekte wie für die Installation des Betriebssystems selbst zu beachten.

Ein wichtiger Grundsatz bei der Konfiguration von Clients ist, dass normale Bedienungsfehler der Anwender zu keinen gravierenden Schäden am System und an Daten anderer Benutzer führen sollten. Auch dürfen Anwender nicht durch einfache Neugierde Zugriff auf Informationen erlangen, die nicht für sie bestimmt sind. Mehr dazu findet sich in M 4.237 Sichere Grundkonfiguration eines IT-Systems (<http://www.bsi.bund.de/gshb/deutsch/m/m04237.htm>).

Nachdem der Client fertig konfiguriert ist, kann der Rechner an die Anwender übergeben werden. Falls die Anwender keine ausreichenden Kenntnisse des eingesetzten Betriebssystems, einzelner Anwendungsprogramme oder Tools besitzen, so müssen sie vorab geschult werden.

Eine der wichtigsten Sicherheitsmaßnahmen beim Betrieb heutiger Client-Systeme ist es, die Systeme durch zeitnahes Einspielen von Sicherheitspatches stets auf einem aktuellen Stand zu halten (siehe M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates, <http://www.bsi.bund.de/gshb/deutsch/m/m02273.htm>) sowie die Installation und permanente Aktualisierung eines Virenschanners (siehe dazu auch B 1.6 Computer-Virenschutzkonzept, <http://www.bsi.bund.de/gshb/deutsch/baust/b01006.htm>). Allerdings wird von einem direkten Nachladen der Updates abgeraten (siehe oben). Empfohlen wird das Herunterladen der aktuellen Patches in einer gesicherten Umgebung, das Testen der sicherheitsrelevanten Patches und das zeitnahe Einspielen und Verteilen dieser auf den Client-Systemen. Daneben ist eine regelmäßige Datensicherung (siehe auch B 1.4 Datensicherungskonzept, <http://www.bsi.bund.de/gshb/deutsch/baust/b01004.htm>) eine grundlegende Voraussetzung dafür, dass Hardwaredefekte und Programm- oder Benutzerfehler nicht zu gravierenden Datenverlusten führen.

Ein Mittel zur Erkennung von Angriffen oder missbräuchlicher Nutzung ist die Überwachung des Systems. Dafür relevante Maßnahmen finden sich in M 4.93 Regelmäßige Integritätsprüfung (<http://www.bsi.bund.de/gshb/deutsch/m/m04093.htm>) und M 5.8 Regelmäßiger Sicherheitscheck des Netzes (<http://www.bsi.bund.de/gshb/deutsch/m/m05008.htm>) sowie im Baustein B 1.9 Hard- und Software-Management (<http://www.bsi.bund.de/gshb/deutsch/baust/b01009.htm>).

Es gelten die gesetzlichen Regelungen zur elektronischen Signatur (SigG und SigV) in Zusammenhang mit der Nutzung der Chipkartenlesegeräte und Behördensignaturkarten zur Signierung und Verschlüsselung während dem Versende-Vorgang. Insbesondere sind die Signaturkarten sicher aufzubewahren und die Kartenleser entsprechend zu sichern.

Auch bei Clients ist es wichtig, dass die Administration auf sicheren Wegen erfolgt und dass die Arbeit der Administratoren nachvollziehbar ist. Die entsprechenden Aspekte sind in M 4.234 Aussonderung von IT-Systemen (<http://www.bsi.bund.de/gshb/deutsch/m/m04234.htm>) beschrieben.

4.4.2 Datenbankserver, Infrastrukturserver

Server sind IT-Systeme, die Dienste (Services) für andere IT-Systeme (Clients) im Netz anbieten. Sie werden typischerweise in zentralen, besonders gesicherten Räumlichkeiten betrieben, beispielsweise in einem Serverraum oder einem Rechenzentrum, und nicht als Arbeitsplatzrechner genutzt. Für Server stehen unterschiedliche Betriebssysteme zur Verfügung, unter anderem Unix bzw. Linux, Microsoft Windows und Novell Netware. Der Baustein B 3.101 Allgemeiner Server (<http://www.bsi.bund.de/gshb/deutsch/baust/b03101.htm>) betrachtet Sicherheitsaspekte, die unabhängig vom eingesetzten Betriebssystem für Server relevant sind. Für betriebssystemspezifische Sicherheitsaspekte existieren in den IT-Grundschutz-Katalogen eigenständige Bausteine, die zusätzlich auf die jeweils betroffenen Server anzuwenden sind. Hierzu gehören beispielsweise:

- B 3.102 Server unter Unix (<http://www.bsi.bund.de/gshb/deutsch/baust/b03102.htm>),
- B 3.106 Server unter Windows 2000 (<http://www.bsi.bund.de/gshb/deutsch/baust/b03106.htm>) und
- B 3.108 Windows Server 2003 (<http://www.bsi.bund.de/gshb/deutsch/baust/b03108.htm>).

Für den erfolgreichen Aufbau eines selbst betriebenen Servers sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Konzeption über die Installation bis zum Betrieb. Ein besonderes Gewicht ist dabei auf die konzeptionellen Planungsmaßnahmen zu legen, wenn der Server im Rahmen des Aufbaus eines neuen servergestützten Netzes installiert wird. Sofern die Installation dagegen als Ausbau eines schon existierenden Netzes erfolgt, können sich die Planungsmaßnahmen häufig darauf beschränken, auf die Konformität des neuen Servers mit den schon vorhandenen Strukturen zu achten. Die Maßnahmen zur Beschaffung und zum Betrieb des Servers sind dagegen in jedem Fall umzusetzen. Die Schritte, die zum Schutz eines Servers zu durchlaufen sind, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Im Vorfeld der eigentlichen Planung ist die generelle Architektur des Netzes festzulegen bzw. zu analysieren, aus der sich im Allgemeinen auch Vorgaben für die einzusetzenden Betriebssysteme (Server und Client) ergeben. Insbesondere ist dabei festzulegen, welche Ziele mit dem aufzubauenden Server verfolgt werden. Dazu sind die voraussichtlichen Einsatzszenarien zu beschreiben und der Einsatzzweck zu definieren.

Falls ein neues Netz aufgebaut wird, muss als genaue technische Grundlage für die weiteren Arbeiten der detaillierte Aufbau des Netzes geplant werden. Anzahl und Zusammenspiel der vorgesehenen Server sind festzulegen. Die Aufgaben der Server und die Art ihrer Nutzung durch die Clients sind zu bestimmen. Anhand der Anforderungen an die Verfügbarkeit muss festgelegt werden, bis zu welchem Grad redundante Strukturen im Netz vorzusehen sind. Hier sind auch die notwendigen Vorgaben für die Infrastruktur (vor allem Klimatisierung und Stromversorgung, siehe dazu M 1.28 Lokale unterbrechungsfreie Stromversorgung, <http://www.bsi.bund.de/gshb/deutsch/m/m01028.htm>) festzulegen. Parallel dazu ist eine allgemeine Sicherheitsrichtlinie zu

erarbeiten (siehe M 2.316 Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server, <http://www.bsi.bund.de/gshb/deutsch/m/m02316.htm>), die anschließend durch systemspezifische Sicherheitsrichtlinien und detaillierte Richtlinien für den Einsatz der Hard- und Software im Netz zu ergänzen ist (siehe dazu die Bausteine zu den einzelnen Server-Betriebssystemen).

Im nächsten Schritt muss die Beschaffung der Software und eventuell zusätzlich benötigter Hardware erfolgen. Aufbauend auf Einsatzszenarien sind die Anforderungen an zu beschaffende Produkte zu formulieren und basierend darauf die Auswahl der geeigneten Produkte zu treffen. Mit der Beschaffung dieser Produkte ist dann die Grundlage für die Arbeiten des nächsten Schrittes gelegt.

Die Benutzer bzw. die Administratoren haben einen wesentlichen Einfluss auf die Sicherheit eines Servers. Vor der tatsächlichen Inbetriebnahme müssen die Benutzer und Administratoren daher für den Umgang bzw. die Nutzung des aufzubauenden Servers geschult werden. Insbesondere für Administratoren empfiehlt sich aufgrund der Komplexität in der Planung und in der Verwaltung eine intensive Schulung. Die Administratoren sollen dabei detaillierte Systemkenntnisse erwerben, so dass eine konsistente und korrekte Systemverwaltung gewährleistet ist. Benutzern sollte insbesondere die Nutzung der verfügbaren Sicherheitsmechanismen vermittelt werden.

Nachdem die organisatorischen und planerischen Vorarbeiten durchgeführt wurden, kann die Installation und Inbetriebnahme des Servers erfolgen. Dabei sind die folgenden Maßnahmen zu beachten:

Schon die Installation und Grundkonfiguration eines Servers muss mit besonderer Sorgfalt durchgeführt werden, um schwer reparierbare Fehler von vornherein zu vermeiden. Allgemeine Hinweise hierzu finden sich in M 2.318 Sichere Installation eines Servers (<http://www.bsi.bund.de/gshb/deutsch/m/m02318.htm>) und M 4.237 Sichere Grundkonfiguration eines IT-Systems (<http://www.bsi.bund.de/gshb/deutsch/m/m04237.htm>).

Nach der Installation und Grundkonfiguration der Server müssen gegebenenfalls übergeordnete Verwaltungsstrukturen konfiguriert werden. Dabei kommt unter anderem auch zum Tragen, für welchen Einsatzzweck die einzelnen Server geplant sind, beispielsweise als Dateiserver, Druckserver oder, im Falle von Thin Clients, als Terminalserver. Hier ist insbesondere die Maßnahme M 2.138 Strukturierte Datenhaltung (<http://www.bsi.bund.de/gshb/deutsch/m/m02138.htm>) wichtig, um einen kontrollierbaren Betrieb des Servers gewährleisten zu können.

Nachdem die Installation und Grundkonfiguration des Servers abgeschlossen ist, kann die eigentliche Serversoftware installiert und konfiguriert werden. Die dafür notwendigen Schritte unterscheiden sich je nach Art und Einsatzzweck der Software teilweise erheblich und werden teilweise in eigenen Bausteinen behandelt. Prinzipiell wird empfohlen, für die Installation und Konfiguration der Serversoftware analog wie für die Konfiguration des Betriebssystems selbst vorzugehen.

Nach der Ersteinstallation und einer Testbetriebsphase wird der Regelbetrieb aufgenommen. Unter Sicherheitsgesichtspunkten sind dabei folgende Aspekte zu beachten:

Client-Server-Netze ändern sich sehr häufig. Dabei muss bei jeder Änderung sichergestellt werden, dass die Sicherheit auch nach der Änderung nicht beeinträchtigt wird. Die dabei im Detail zu beachtenden Aspekte sind in den Bausteinen zu den jeweiligen Serverbetriebssystemen enthalten. Dabei ist zu berücksichtigen, dass auch der Entzug von Berechtigungen sowie das Löschen nicht mehr benötigter Datenbestände so geregelt wird, dass durch veraltete Strukturen keine

Sicherheitslücken entstehen. Eine wesentliche Hilfe ist dabei eine effiziente, umfassende Systemverwaltung, die sich jederzeit auf aktuelle Informationen über den Zustand des Systems und seiner Rechtestrukturen abstützen kann (siehe dazu M 4.24 Sicherstellung einer konsistenten Systemverwaltung, <http://www.bsi.bund.de/gshb/deutsch/m/m04024.htm>, und M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprofile, <http://www.bsi.bund.de/gshb/deutsch/m/m02031.htm>).

Ein Mittel im Rahmen der Aufrechterhaltung der Sicherheit eines Servers ist die Überwachung des Systems bzw. seiner Einzelkomponenten. Die hier relevanten Maßnahmen finden sich in M 4.93 Regelmäßige Integritätsprüfung (<http://www.bsi.bund.de/gshb/deutsch/m/m04093.htm>), M 5.8 Regelmäßiger Sicherheitscheck des Netzes (<http://www.bsi.bund.de/gshb/deutsch/m/m05008.htm>) und M 5.9 Protokollierung am Server (<http://www.bsi.bund.de/gshb/deutsch/m/m05009.htm>). Dabei spielen auch insbesondere Datenschutzaspekte eine Rolle. Die häufigen Sicherheitslücken der meisten Client-Server-Systeme und die Vielzahl von Angriffen, die sich gegen diese Schwächen richten, fordern von den Administratoren, dass diese sich permanent über den Sicherheitsstatus der Systeme und über neue Bedrohungen informieren (siehe M 2.35 Informationsbeschaffung über Sicherheitslücken des Systems, <http://www.bsi.bund.de/gshb/deutsch/m/m02035.htm>) und rechtzeitig Gegenmaßnahmen einleiten (siehe dazu M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates, <http://www.bsi.bund.de/gshb/deutsch/m/m02273.htm>).

Ein Server darf nicht einfach ohne Ankündigung abgeschaltet werden. Wenn ein Server außer Betrieb genommen werden soll, dann müssen die Anwender rechtzeitig informiert werden und es muss eine Reihe von Punkten beachtet werden, um Ausfallzeiten und Datenverluste zu verhindern. Diese Punkte sind in M 2.320 Geregeltete Außerbetriebnahme eines Servers (<http://www.bsi.bund.de/gshb/deutsch/m/m02320.htm>) beschrieben. Sollen die Dienste des Servers auf einen anderen Rechner migriert werden, so ist M 2.319 Migration eines Servers (<http://www.bsi.bund.de/gshb/deutsch/m/m02319.htm>) zu berücksichtigen.

Bei der Aussonderung eines Servers ist außerdem darauf zu achten, dass keine schützenswerten Informationen mehr auf den Festplatten vorhanden sind. Dazu genügt es nicht, die Platten einfach neu zu formatieren, sondern sie müssen mindestens zweimal, besser aber in drei Durchläufen, vollständig überschrieben werden. Beim zweiten Durchlauf sollte das zum ersten Durchlauf komplementäre Datenmuster (Bit-Folge) verwendet werden. Für den dritten Durchlauf werden Zufallsdaten empfohlen. Es ist zu beachten, dass ein reines logisches Löschen und auch das Neuformatieren der Platten mit den Mitteln des installierten Betriebssystems die Daten nicht von den Festplatten entfernt, so dass sie mit geeigneter Software, oft sogar ohne großen Aufwand, wieder rekonstruiert werden können. Entsprechende Hinweise finden sich in M 2.167 Sicheres Löschen von Datenträgern (<http://www.bsi.bund.de/gshb/deutsch/m/m02167.htm>) und M 2.13 Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln (<http://www.bsi.bund.de/gshb/deutsch/m/m02013.htm>). Letztere wird im Rahmen des übergeordneten Bausteins B 1.1 Organisation (<http://www.bsi.bund.de/gshb/deutsch/baust/b01001.htm>) behandelt. Ferner ist auch die Maßnahme M 4.234 Aussonderung von IT-Systemen (<http://www.bsi.bund.de/gshb/deutsch/m/m04234.htm>) ist in diesem Kontext zu berücksichtigen.

Werden die IT-Systeme generell bei einem ausgelagerten Dienstleister betrieben, sind entsprechende Sicherheitsanforderungen im zugrundeliegenden Dienstleistungs-Vertrag zu berücksichtigen (z. B.: Einhaltung der BSI-IT-Grundsatzvorgehensweise, Erstellung eines Sicherheitskonzeptes). Generell ist dann der Baustein B 1.11 Outsourcing (<http://www.bsi.bund.de/gshb/deutsch/baust/b01011.htm>) zu betrachten. Gerade hier ist zu berücksichtigen, dass die Passbehörden zu jedem Zeitpunkt Eigentümer der Daten und verantwortlich für diese sind. Die

Einhaltung und Sicherstellung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit sind entsprechend mit dem Dienstleister vertraglich festzuhalten und zu vereinbaren.

4.5 Netze

Es muss unterschieden werden, ob die Informationen über ein lokales Netz oder über eine öffentliche Wahl-Verbindung übertragen werden. Generell muss der Übergang zwischen Netzen mit unterschiedlichen Schutzbedarf mit einem Sicherheitsgateway getrennt werden

4.5.1 Lokales Netzwerk der Passbehörden

Ein lokales Netz setzt sich aus der Verkabelung (d. h. den passiven Netzkomponenten Kabel und den Verbindungselementen) sowie den aktiven Netzkomponenten zur Netzkopplung zusammen. Generell können dabei unterschiedliche Verkabelungstypen wie auch unterschiedliche aktive Netzkomponenten in ein LAN integriert werden. Als aktive Netzkomponenten werden alle Netzkomponenten bezeichnet, die eine eigene (Netz-) Stromversorgung benötigen. Dazu gehören unter anderem Repeater, Brücken, Switches, Router, Gateways. Für die Sicherheit der aktiven Netzkomponenten muss der Baustein B 3.302 Router und Switches (<http://www.bsi.bund.de/gshb/deutsch/baust/b03302.htm>) berücksichtigt werden. Als passive Netzkomponenten werden alle Netzkomponenten betrachtet, die keine eigene Netzstrom-Versorgung benötigen. Dazu gehören z. B. Kabel, Verteilerschränke, Patchfelder, Steckverbinder. Für weitere Empfehlungen für Netze muss der Baustein B 4.1 Heterogene Netze (<http://www.bsi.bund.de/gshb/deutsch/baust/b04001.htm>) berücksichtigt werden.

4.5.2 Transportwege innerhalb der Passbehörden

Sicherheitsgateways werden am zentralen Übergang zwischen zwei unterschiedlich vertrauenswürdigen Netzen eingesetzt. Unterschiedlich vertrauenswürdige Netze stellen dabei nicht unbedingt nur die Kombination Internet-Intranet dar. Vielmehr können auch zwei organisationsinterne Netze unterschiedlich hohen Schutzbedarf besitzen, z. B. bei der Trennung des Bürokommunikationsnetzes vom Netz der Personalabteilung, in dem besonders schutzwürdige, personenbezogene Daten übertragen werden. Um Sicherheitsgateways zu schützen, müssen die Empfehlungen des gleichnamigen IT-Grundschutz-Bausteins (B 3.301 Sicherheitsgateway (Firewall), <http://www.bsi.bund.de/gshb/deutsch/baust/b03301.htm>) umgesetzt werden.

4.5.3 Transportwege von der Passbehörde zu anderen Stellen

ISDN (Integrated Services Digital Network) ist ein digitales Telekommunikationsnetz, über das verschiedene Dienste, wie Telefon und Telefax, genutzt sowie Daten und Bilder übertragen werden können. In dem Baustein B 4.5 LAN-Anbindung eines IT-Systems über ISDN (<http://www.bsi.bund.de/gshb/deutsch/baust/b04005.htm>) wird die Anbindung eines abgesetzten IT-Systems an ein lokales Netz über ein öffentliches ISDN-Netz betrachtet. Hierbei erfolgt die Anbindung auf Seiten des abgesetzten IT-Systems mittels einer ISDN-Adapterkarte mit S0-

Schnittstelle. Die Anbindung des LAN wird über einen Router hergestellt, der über eine S2M-Schnittstelle mit einem öffentlichen ISDN-Netz verbunden ist.

4.6 Räume

4.6.1 Büroraum

Ein Büroraum ist ein Raum, in dem sich ein oder mehrere Mitarbeiter aufhalten, um dort der Erledigung ihrer Aufgaben eventuell auch IT-unterstützt nachzugehen. Diese Aufgaben können aus den verschiedensten Tätigkeiten bestehen: Erstellung von Schriftstücken, Bearbeitung von Karteien und Listen, Durchführung von Besprechungen und Telefonaten, Lesen von Akten und sonstigen Unterlagen. Die entsprechenden Empfehlungen finden sich in Baustein B 2.3 Büroraum (<http://www.bsi.bund.de/gshb/deutsch/baust/b02003.htm>).

4.6.2 Serverraum

Der Serverraum dient in erster Linie zur Unterbringung von Servern, z. B. eines LAN-Servers, eines Unix-Zentralrechners oder eines Servers für eine TK-Anlage. Darüber hinaus können dort serverspezifische Unterlagen, Datenträger in kleinem Umfang oder weitere Hardware (Sternkoppler, Protokolldrucker, Klimatechnik) vorhanden sein. Für den Schutz von Servern sind die Empfehlungen aus dem Baustein B 2.4 Serverraum (<http://www.bsi.bund.de/gshb/deutsch/baust/b02004.htm>) umzusetzen.

5 Schlussbemerkungen

Analog zur Entwicklung in der Informationstechnik sind auch die Anforderungen an die Informationssicherheit immer komplexer geworden. Besonders kleine und mittlere Institutionen mit beschränkten finanziellen und personellen Möglichkeiten wünschen sich deshalb einen leicht überschaubaren Einstieg in die Thematik. Der Leitfaden IT-Sicherheit greift diesen Wunsch auf: Er gibt einen kompakten und allgemeinverständlichen Überblick über die wichtigsten Sicherheitsmaßnahmen. Im Mittelpunkt stehen organisatorische Maßnahmen und die Veranschaulichung von Gefahren durch Praxisbeispiele. Auf technische Details wird bewusst verzichtet.

Um die Anwender des IT-Grundschutzes zu unterstützen, wurden zahlreiche weitere Hilfsmittel veröffentlicht, beispielsweise der Webkurs IT-Grundschutz. Ein etwa vierstündiges Selbststudium ermöglicht den Anwendern, eigene Sicherheitskonzepte gemäß IT-Grundschutz anzufertigen.

Vertiefende Informationen zum IT-Grundschutz und zu den Hilfsmitteln sind unter <http://www.bsi.bund.de/gshb> zu finden.