

Technischer Bericht

Fachhochschule Gießen

**Anforderungen an das Einsatzumfeld eines
elektronischen Personenstandsbuchs**

Autor: Ingo Graser

Version: alpha_0.4 (15.12.2004)

Zusammenfassung

Dieses Dokument stellt die Sicherheitsanforderungen dar, die für den Betrieb eines elektronischen Personenstandsbooks (e.P.b.) erfüllt sein müssen. Diese ergeben sich aus der Anwendung des BSI IT-Grundschutzhandbuchs auf das e.P.b.-System.

Dabei geht dieses Dokument lediglich auf die Gefährdungen des Umfelds ein. Dazu gehören die Räumlichkeiten für den e.P.b.-Archivserver, die Personalorganisation und die technische Infrastruktur.

Inhaltsverzeichnis

1	Das IT-Grundschutzhandbuch	2
2	Bausteine für e.P.b.	3
2.1	Rechenzentrum	3
2.2	Serverraum	6
2.3	Datenträgerarchiv	6
2.4	Servergestütztes Netz	7
2.5	Personal	9
3	Anwendung der Bausteine	11
	Literaturverzeichnis	12

1. Das IT-Grundschutzhandbuch

Das IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik [1] soll dabei helfen, in IT-Systemen ein Sicherheitslevel zu verwirklichen, welches für den normalen Sicherheitsbedarf ausreicht und eine solide Basis für weiterreichende Schutzmaßnahmen darstellt.

Das Handbuch definiert allgemeine Bausteine. Jedes IT-System soll sich durch eine Aneinanderreihung dieser Bausteine darstellen lassen. Beispiele für Bausteine sind: Serverraum, Personal, Kryptokonzept usw.

Der Aufbau des Handbuchs ist für jeden Baustein gleich. Nach der Definition des Bausteins folgen die möglichen Gefährdungen und die vorgeschlagenen Maßnahmen, mit denen auf die Gefährdungen geantwortet werden kann.

In allen bisherigen Papieren zum e.P.b. wurde ein ordnungsgemäßer Rechenzentrumsbetrieb vorausgesetzt. Im Folgenden soll dieser Begriff nun mit den im IT-Grundschutzhandbuch verfügbaren Bausteinen definiert werden. Dadurch soll ein Eindruck vermittelt werden, welche Anforderungen der Betrieb eines e.P.b. stellt.

Dabei wird ausschließlich auf den lokalen Betrieb eines e.P.b. eingegangen. Die Vernetzung verteilter e.P.b.-Archivserver stellt weitere Anforderungen an die Sicherheitseinrichtungen. Diese sind nicht Gegenstand dieser Untersuchung. Sicherheitsmechanismen, die eine e.P.b.-Software selbst mitbringen muss, hat Burkhardt Renz in [3] zusammengestellt. Nicht nur im Hinblick auf die kryptografische Sicherheit empfiehlt sich ebenso die Lektüre von [2].

2. Bausteine für e.P.b.

Dieses Kapitel stellt zunächst die benötigten Bausteine vor. Dies geschieht durch die Beschreibung des Bausteins. Darauf folgen die möglichen Gefährdungen und im Anschluss die vorgeschlagenen Maßnahmen. Das nächste Kapitel fügt diese Bausteine zusammen und gibt einen Überblick.

Dabei soll nur ein Eindruck der erforderlichen Sicherheitseinrichtungen vermittelt werden. Für die Realisierung eines IT-Grundschutzes muss unbedingt das IT-Grundschutzhandbuch herangezogen werden, um ein vollständiges Sicherheitskonzept zu erarbeiten.

2.1 Rechenzentrum

Siehe Kapitel 4.6 (S. 126) im IT-Grundschutzhandbuch.

Das Grundschutzhandbuch definiert verschiedene Bausteine für die Räume, in denen die Server des Systems aufgestellt werden. Das Rechenzentrum ist die höchste Sicherheitsstufe, die das Grundschutzhandbuch vorsieht. Es ist kein Hochsicherheitsrechenzentrum, bietet aber die Grundsicherheit, die der Betrieb eines e.P.b.-Archivservers erfordert.

Dieser Baustein sieht vor, dass mehrere Mandanten auf zentrale Server zugreifen können. Deshalb ist dieser Baustein auch anwendbar, wenn sich mehrere Standesämter dazu entschließen ihren e.P.b.-Archivserver in einem gemeinsamen Rechenzentrum zu betreiben. Zu diesem Zeitpunkt wird diese Lösung als die effektivste angesehen, da vielen Gemeinden die nötige Infrastruktur eines Rechenzentrums bereits zur Verfügung steht.

Bei den im Folgenden beschriebenen Gefährdungen geht es um solche, die durch den Rechenzentrumsbetrieb entstehen können. Die Absicherung der Server gegen Zugriffe von außerhalb ist Teil des Bausteins „Servergestütztes Netz“.

Durch die starke Vernetzung in einem Rechenzentrum genügt oft der Ausfall eines einzelnen IT-Systems, um den gesamten Betrieb lahm zu legen. Ein solcher Ausfall kann durch technisches Versagen, menschliches Fehlverhalten verursacht werden. Viele der nachfolgend vorgestellten Gefährdungen können Ursache eines Ausfalls sein.

Blitzschlag, Feuer, Wasser und Sturm können dabei die größten Schäden verursachen. Bei einem Blitzschlag sind es zumeist die erzeugten Überspannungen, die die empfindlichen IT-Systeme beschädigen. Auch Feuer kann durch einen Blitz verursacht werden. Die häufigsten Ursachen für Feuer sind jedoch der unsachgemäße Umgang mit offenem Feuer, falsche Verwendung von elektrischen Geräten oder auch technisches Versagen.

Neben den direkten Schäden durch die Flammen sind die Schädigungen durch Löschwasser dramatisch. Löschwasser kann auch Schäden außerhalb der Brandstelle anrichten. So können sich bei einem Brand eines PVC-Fußbodens in Verbindung mit dem Löschwasser Salzsäuredämpfe bilden. Über die Belüftungsanlagen können sich diese Dämpfe verbreiten und an anderen Stellen Schäden verursachen. Löschwasser ist jedoch nicht die alleinige Ursache von Wassereintrüben. So können z.B. auch defekte Klimaanlage mit Wasseranschluss Probleme verursachen.

2.1. Rechenzentrum

Ein Sturm schädigt dagegen meist nur die äußeren Einrichtungen des Rechenzentrums. Jedoch darf auch diese Gefährdung nicht unterschätzt werden.

Das Gebäudeklima muss den empfohlenen Bedingungen für den Betrieb der IT-Systeme und den Lagerbedingungen für Speichermedien entsprechen. Bei zu hoher Temperatur oder zu hoher Luftfeuchtigkeit kann die Langzeithaltbarkeit beeinträchtigt werden. Der Temperatur ist dabei besonderes Augenmerk zu widmen, da die IT-Systeme den Raum stark aufheizen können.

Bei der Planung des Gebäudes muss also auf die Gefährdung durch höhere Gewalt Rücksicht genommen werden. Darüber hinaus können sich Planungsfehler auch auf andere Weise später rächen. So ist meist absehbar, dass die benötigte Menge an Servern und Infrastruktur über die Jahre anwächst. Schon bei der Planung sollte also an die Zukunft gedacht werden. Ein übervoller Serverraum erhöht das Sicherheitsrisiko.

Aufgewirbelter Staub und Schmutz kann genauso zu Ausfällen führen. Davon sind besonders die mechanischen Komponenten betroffen. Festplatten, optische Laufwerke und Lüfter können schon durch kleinere Verunreinigungen betroffen sein.

Neben den Gefährdungen direkt im Rechenzentrum können auch technische Katastrophen oder Großveranstaltungen in der näheren Umgebung den Betrieb stören oder lahm legen. Dies kann z.B. durch eindringende Schadstoffe oder durch Gewalt gegen das Personal geschehen.

Gefahr für das IT-System droht auch bei mangelhafter Organisation. Existieren keine dokumentierten Regelungen und Schutzvorschriften oder hat das Personal keine Kenntnis davon, nützen auch die besten Konzepte nichts. Die Organisation des Personals muss entsprechend in das Schutzkonzept mit aufgenommen werden. Dazu gehört auch die regelmäßige Kontrolle aller Schutzmaßnahmen.

Nicht nur das Personal muss organisiert werden, auch die Zulieferung mit Verbrauchsmaterialien und Ersatzteilen muss zuverlässig funktionieren. Bei Engpässen könnte es sonst zu einem Ausfall des Betriebs kommen.

Auch im Gebäude installierte Sicherheitsmechanismen geben keinen hundertprozentigen Schutz. Im Sicherheitskonzept muss berücksichtigt werden, dass Strom- und Notstromversorgung ausfallen können. Auch Feuerlöscher, Brandmelder oder Türschlösser können durch schlechte Wartung ausfallen.

Zuletzt noch ein Blick auf die Gefahren, die nicht durch Versagen von Sicherheitseinrichtungen oder mangelhafte Organisation drohen. Gezielte Anschläge oder Sabotage aber auch einfach blinder Vandalismus können große Schäden verursachen.

Ziel eines gezielten Eindringens kann Diebstahl, aber auch Manipulation und Kopieren von Daten sein. Die Kosten, die durch Diebstahl und Beschädigung der Einrichtung verursacht werden, sind dabei noch abschätzbar. Die Vernichtung der gespeicherten Daten kann einen unüberschaubaren Schaden verursachen.

Es muss damit gerechnet werden, dass sowohl außen stehende Personen, als auch interne Mitarbeiter für Derartiges in Betracht kommen. Besonders bei Administrierungs- und Wartungsarbeiten könnten interne oder externe Mitarbeiter versuchen Berechtigungen entsprechend zu ändern, um Zugriff auf Daten oder Zugang zu Räumen zu erhalten.

2.1. Rechenzentrum

Die empfohlenen Maßnahmen greifen schon bei der Planung des Gebäudes an. Neben den Erfordernissen des eigentlichen Gebäudes muss bei der Bauplanung auch das Umfeld berücksichtigt werden. Faktoren sind Erschütterungen durch starken Verkehr, Beeinträchtigungen durch nah gelegene Sendeanlagen und Kraftwerke oder Fabriken, in denen Störfälle auftreten könnten. Daneben sind auch z.B. bekannte Demonstrationaufmarschgebiete als Standort u.U. ebenfalls ungeeignet.

Alle Zutrittmöglichkeiten zum Rechenzentrum müssen überwacht werden. Deshalb empfiehlt sich möglichst wenige Türen und Fenster zu planen, da diese das Sicherheitsrisiko erhöhen. Außerdem sollte der Zutritt über Kontrollmechanismen geregelt werden. Die Bauplanung sollte auch den Schutz vor äußeren Einflüssen, wie Wassereintrich oder EMV-Störquellen mit einschließen.

Ein wichtiges Hilfsmittel gegen den Ausfall einzelner Dienste ist die redundante Auslegung der Betriebseinrichtung.

Der nächste Punkt betrifft die Stromversorgung. Eine unterbrechungsfreie lokale Stromversorgung hält den Betrieb auch bei zeitweisem Netzstromausfall am Laufen. Zum Schutz vor äußeren Einwirkungen ist eine Blitz- und Überspannungsschutzeinrichtung vorzusehen. Der Zugang zu den versorgungskritischen Bereichen, wie Verteileranlagen muss wie der Zutritt zu den Datenverarbeitungseinrichtungen geregelt sein.

Nicht nur über das Stromnetz auch über Netzwerkanschlüsse können von außen schädliche Überspannungen eingebracht werden. Abhilfe schafft hier die komplette galvanische Trennung der Leitungen. Auch ein Trennen durch einen Schalter für Notfälle kann in Erwägung gezogen werden.

Der Brandschutz erfordert die Absprache mit der lokalen Feuerwehr, regelmäßiges Training des Personals und natürlich die richtige Brandschutz-, Brandmelde- und Brandbekämpfungsausrüstung. Eine automatische Brandlöschanlage erhöht den Schutz, ist aber für den Grundschutzbedarf nicht unbedingt nötig. Ein generelles Rauchverbot für die besonders schützenswerten Bereiche und eine regelmäßige Brandschutzbegehung gehören zur Brandprävention.

Im Bereich des Gebäudeschutzes können folgende Maßnahmen ergriffen werden. Für den Notfall müssen immer aktuelle Infrastruktur- und Versorgungsplankarten bereitgehalten werden, damit sich Helfer schnell orientieren können. Allerdings sollten besonders schützenswerte Räume, wie z.B. Serverraum etc. nicht explizit als solche gekennzeichnet werden, um die Planung von Sabotage und Diebstählen zu erschweren.

Vorschriften alle Türen und Fenster bei Abwesenheit geschlossen zu halten, erhöhen den Schutz gegen Eindringen. Allerdings sollten hier auch passive Schutzvorrichtungen wie besonders gesicherte Schlösser und Türen eingeplant werden. Eine Gefahrenmeldeanlage gegen Eindringen, aber auch gegen Feuer, Gas und Wasser ergänzt diese Vorkehrungen.

Die Klimatisierung der Serverräume ist meist unerlässlich, um die zulässigen Betriebstemperaturen nicht zu übersteigen. Diese Klimaanlage müssen an die Wasserversorgung angeschlossen sein. Dabei sind besondere Sicherheitsmaßnahmen wie Wasserauffangwannen etc. zu ergreifen.

Ein Pförtnerdienst, eine Videoüberwachung oder gar ein geschützter Perimeter um das Gebäude können den Schutz weiter erhöhen. Diese Maßnahmen sind jedoch nicht zwingend zur Erreichung des IT-Grundschutzniveaus erforderlich.

2.2. Serverraum

Für den sicheren Betrieb ist die Organisation von Schutzmaßnahmen unerlässlich. Organisiert werden muss der Ablauf von regelmäßigen Wartungs- und Reparaturarbeiten, die Gebäudereinigung, die Zutrittskontrolle und die Versorgung mit Verbrauchsmaterialien. Eine regelmäßige Überprüfung der Einhaltung von Sicherheitsmaßnahmen ist untrennbar mit deren Einführung verbunden.

Was die Zutrittskontrolle betrifft, so ist die Verteilung der Schlüssel und der Schließplan zu dokumentieren. Bei dem Eintreten von Fremdpersonen, seien es Besucher oder Handwerker ist der Grund zu überprüfen und deren Bewegung im Gebäude zu beaufsichtigen.

Das Sicherheitskonzept muss auch für eventuelle Notfälle Vorsorge treffen. Dazu gehören der Schutz der materiellen Einrichtung mittels ausreichender Versicherungen. Aber auch der Schutz der Datenarchive sollte gewährleistet werden. Dazu kann ein Notfallarchiv vorgesehen werden, mittels dem sich der gesamte Datenbestand nach einem Totalverlust wieder herstellen lassen kann. Dieses Notfallarchiv muss derart platziert sein, dass eine Katastrophe nicht den Bestand und dieses Archiv gleichzeitig zerstören kann. Allerdings sind diese beiden Maßnahmen nicht zwingend für den IT-Grundschutz notwendig.

2.2 Serverraum

Siehe Kapitel 4.3.2 (S. 115) im IT-Grundschutzhandbuch.

Der Serverraum ist ähnlich konzipiert wie das gerade vorgestellte Rechenzentrum. Der Unterschied liegt in der Anzahl der untergebrachten Server und der Mandanten, die auf die zur Verfügung gestellten Dienste zugreifen. Der Serverraum beherbergt hauptsächlich lokale Server und IT-Infrastruktur. Er ist nicht dafür konzipiert, Dienste für mehrere Mandanten zur Verfügung zu stellen.

Für das e.P.b. sollten die Vorschriften für einen Serverraum dann angewendet werden, wenn sich ein einzelnes Standesamt entschließt das elektronische Personenstandsbuch einzuführen und nicht auf die vorhandene Infrastruktur einer Gemeinde zurückgreifen kann.

Auf Grund der ähnlichen Konzeption gleichen die Maßnahmen denen eines Rechenzentrums. An einen Serverraum werden geringere Ansprüche an die Sicherheit gestellt. Viele Maßnahmen, die für ein Rechenzentrum obligatorisch sind, sind für einen Serverraum als optional angegeben. Ich werde die Maßnahmen daher nicht gesondert vorstellen.

2.3 Datenträgerarchiv

Siehe Kapitel 4.3.3 (S. 117) im IT-Grundschutzhandbuch.

Dieser Baustein definiert ein Datenträgerarchiv beliebiger Art. Für das e.P.b. kann der Raum zur Lagerung der Backupmedien mithilfe der Maßnahmen dieses Bausteins konzipiert werden.

Wiederum sind die Regelungen ähnlich, wie für ein Rechenzentrum oder einen Serverraum. Wichtige Punkte sind hier vor allem der Schutz vor Feuer und eine Klimatisierung, die die Haltbarkeit der Medien unterstützt.

2.4. Servergestütztes Netz

Um einen besseren Schutz vor Feuer zu erreichen, empfiehlt das Handbuch zusätzlich die Unterbringung der Medien in einem feuergeschützten Sicherheitsschrank. Vor allem der gleichzeitige Verlust von Livebestand und Sicherheitsmedien muss verhindert werden.

2.4 Servergestütztes Netz

Siehe Kapitel 6.1 (S. 159) im IT-Grundschutzhandbuch.

Dieser Baustein bildet alle Systeme ab, bei denen Dienste in einem Netzwerk angeboten werden. Dabei ist die Betrachtung unabhängig vom eingesetzten Betriebssystem. Je nach Betriebssystem existieren zusätzliche Bausteine.

Bei der Vorstellung dieses Bausteins werde ich nicht auf diejenigen Punkte eingehen, die beim Baustein Rechenzentrum schon angesprochen wurden. Dazu zählen alle Punkte, die die Infrastruktur und die Umgebung von Server und Netzwerk betreffen.

Wartungs- und Administrationspersonal ist für den reibungslosen Betrieb des Netzwerkes unbedingt notwendig. Fällt Personal an einer empfindlichen Stelle aus, kann das den Ausfall des Netzwerkes zur Folge haben. Wenn nur eine Person allein über wichtige Passwörter Bescheid weiß, führt deren Ausfall dazu, dass neues Personal die Aufgabe nicht ohne weiteres fortführen kann.

Organisatorische Regelungen müssen ständig an die sich ändernde IT-Struktur angepasst werden. Heute getroffene Regelungen können sich z.B. beim Einsatz einer neuen Software als hinderlich erweisen. Mangelnde Vorausschau auf die zukünftige Entwicklung des Netzwerkes kann dazu führen, dass es bei einem späteren Ausbau (z.B. mehr Benutzer) zu Leistungsgespässen kommt, die den gesamten Betrieb lahm legen.

Fehlbedienungen durch das Personal können enorme Folgeschäden verursachen. Die Fehlhandlungen könnten bewusst herbeigeführt werden, meist handelt es sich aber um mangelnde Kenntnis und unzureichende Schulung im Umgang mit den Systemen. Aber auch umfassende Regelungen in diesem Bereich garantieren nicht für eine korrekte Bedienung. Mitarbeiter können aus Unverständnis über existierende Sicherheitsregelungen diese einfach ignorieren.

Die korrekte Administration kann solchen Fehlbedienungen durch punktuelle Rechtevergabe vorbeugen. Auch gegen weitere Gefährdung des Systems hilft eine gute Administration. Werden hier Fehler gemacht, können sich durch die Unübersichtlichkeit der vielen aktiven Prozesse enorme Sicherheitsmängel einschleichen. Zur korrekten Administration gehört auch eine regelmäßige Überprüfung auf neu erschienene Sicherheitsupdates.

Eine weitere Gefährdung ist die unbeabsichtigte oder auch beabsichtigte Beschädigung von Leitungen und Hardware. Dies kann u.a. durch Unachtsamkeiten oder Unwissenheit von Mitarbeitern oder auch Reinigungspersonal geschehen. Diese Beschädigungen führen meist dazu, dass Dienste nicht mehr erreichbar sind. Es ist jedoch auch denkbar, dass Dienste, die bisher nicht erreichbar waren, da sie sich in einem anderen Netzbereich befanden, nun (z.B. durch das falsche Wiedereinführen eines Steckers) plötzlich erreichbar sind.

2.4. Servergestütztes Netz

Unzureichende Regelungen in Bereich der Datensicherung können zu Datenverlust und unübersichtlichen Datensammlungen führen. Wenn jeder Mitarbeiter seine eigene Datensicherung durchführt (z.B. auf Diskette oder CD) und kein zentrales Datensicherungssystem nutzt, sind diese Daten für die konsequente Sicherung verloren. Da hier keine Regelungen zur Lagerung etc. greifen können, sind diese Daten stark verlustgefährdet. Aber auch Datenträger, die zentral zur Datenspeicherung genutzt werden, sind vom Verfall und damit dem Verlust der Daten bedroht. Auch hier sind Maßnahmen erforderlich. Gerade bei digital signierten oder verschlüsselten Dokumenten bedeutet der Ausfall eines Bits eine vollständige Unlesbarkeit des Dokumentes, bzw. den Verlust der Signatur.

Neben den schon beim Rechenzentrum genannten Gefahren durch vorsätzlichen Missbrauch der IT-Systeme kommen durch diesen Baustein weitere hinzu. Das sind die bekannten Angriffsmethoden auf Server. Trojanische Pferde, Viren und Makroviren sind Malware, die Rechnern Schäden hinzufügen können oder sensible Informationen ausspähen. Das systematische Ausprobieren von Passwörtern, Wiedereinspielen von Nachrichten, Maskerade, Denial-of-Service und die Analyse des Nachrichtenflusses sind übliche Attacks von Hackern. Das System kann dadurch lahm gelegt oder übernommen werden.

Die Maßnahmen fangen schon bei der sicheren Aufstellung der IT-Systeme an. Dabei sollten möglichst wenige Kabel freiliegen, an denen man hängen bleiben kann. Es muss aber auch darauf geachtet werden, dass Konsolen, über die man sicherheitsrelevante Systeme erreichen kann nicht für jedermann zugänglich sind.

Alle eingesetzten Datenträger müssen in einem zentralen Bestandsverzeichnis erfasst werden, um sie später wieder auffinden zu können, aber auch um ihre (physikalische) Löschung und ein Backup organisieren zu können. Diese Maßnahmen gehören zu einer geregelten Datenträgerverwaltung.

Wollen Anwender neue Software oder Hardware auf den zur Verfügung gestellten Arbeitsplatzrechnern oder Notebooks installieren, müssen diese vorher kontrolliert und zugelassen werden. Damit diese Regelungen eingehalten werden, sind stichprobenartige Tests unumgänglich.

Die Überwachung und Konfiguration der IT-Systeme wird Administratoren zugeteilt. Dabei müssen die Aufgabengebiete der einzelnen Administratoren klar aufgeteilt sein, damit es zu keinen Zuständigkeitsproblemen kommt. Die Administratoren müssen eine Dokumentation der Systemkonfiguration anfertigen, die ständig auf dem neuesten Stand zu halten ist. Auch eventuell vergebene Passwörter müssen hinterlegt sein. Diese Maßnahmen ermöglichen es beim Ausscheiden oder beim Ausfall eines Administrators den Betrieb durch einen Vertreter am Laufen zu halten.

Die Administratoren sind ebenfalls für die Einrichtung von Benutzer und Benutzergruppen verantwortlich. Dazu muss es genaue Regelungen geben, wann bestimmte Rechte zu vergeben sind. Die vergebenen Rechte müssen dokumentiert werden. Je nach Benutzergruppe werden eingeschränkte Betriebsumgebungen eingerichtet, sodass Benutzer lediglich auf die von ihnen benötigten Dienste Zugriff erlangen.

Eine weitere Aufgabe der Administratoren ist die Informationsbeschaffung über neu aufgetretene Sicherheitslücken und die Erstellung eines Planes zum Schutz vor den erkannten Gefahren.

2.5. Personal

Zum Schutz des internen Netzes ist es dringend notwendig alle von außen eingehenden Verbindungen nur über gesicherte Zugänge (mindestens eine Firewall) ermöglicht werden. Die Nutzer müssen informiert werden, dass sämtliche von ihnen selbst ermöglichte Verbindungen (WLAN, Bluetooth, Modem) ein enormes Sicherheitsrisiko hervorrufen.

Wichtigste Grundlage eines sicheren Betriebes ist die ausreichende Schulung des Personals. Dabei müssen zum einen die generellen Sicherheitsmaßnahmen erläutert werden. Zum Anderen ist auch die Schulung der Mitarbeiter im Umgang mit neuer Anwendungssoftware erforderlich. Aber auch die Administratoren müssen über die Sicherheitsmaßnahmen informiert werden, damit alle am selben Strang ziehen.

Die angesprochenen Administratoren und deren Vertreter erhalten weitestgehende Befugnisse und Zugangsrechte, damit sie ihre Aufgaben erfüllen können. Damit sind sie ein Sicherheitsrisiko. Ihnen muss großes Vertrauen entgegengebracht werden können. Die Auswahl eines geeigneten Administrators muss deshalb mit größter Sorgfalt geschehen.

Hier nun die üblichen Maßnahmen zum Schutz der Hard- und Software: Einrichtung eines Passwortschutzes für den Zugang zu IT-Systemen und bei Verlassen des Arbeitsplatzes eine Sperre des Bildschirms. Voreingestellte Passwörter müssen sofort geändert werden. Der Login mit Übermittlung des Passwortes muss gesichert (verschlüsselt) erfolgen. Einsatz eines Antivirenprogramms für Dateien und Emails. Test neuer Hard und Software vor deren Einsatz. Sperren nicht mehr benötigter Accounts.

Die Einführung von Netzsegmenten erhöht die Sicherheit. Benutzer in einem Segment können damit gehindert werden, Dienste eines anderen Segmentes zu erreichen. Die Segmentierung geschieht mit Hilfe von Routern, Bridges oder Gateways.

Die Kommunikation innerhalb eines Netzes muss protokolliert werden, um Unregelmäßigkeiten zu erkennen und Missbrauchsversuche aufzudecken. Neben diesen Maßnahmen muss auch ein regelmäßiger Sicherheitscheck erfolgen, der überprüft, ob alle ergriffenen Maßnahmen wirksam sind.

Für den Notfall müssen aktuelle Sicherungen der installierten Softwareprodukte und der Daten existieren. Diese Backups müssen regelmäßig auf ihre Funktionalität überprüft werden und an einem geeigneten Ort gelagert werden.

Für den Notfall sind Verhaltensregeln festzusetzen, die dafür sorgen, weitere Schäden zu verhindern und den letzten Stand möglichst schnell wieder herstellen zu können.

2.5 Personal

Siehe Kapitel 3.2 (S. 87) im IT-Grundschutzhandbuch.

Dieser Baustein ist recht allgemein gehalten und gibt Maßnahmen vor, die generell beim Personalmanagement eingehalten werden sollten. Dass besondere Auswahlkriterien bei Systemadministratoren und Posten mit ähnlich weitgehenden Zugangsberechtigungen gelten müssen, wurde hier schon bei den vorigen Bausteinen angesprochen.

Personalausfall kann einen reibungslosen Betriebsablauf schnell behindern. Wenn Personal an wichtigen Schlüsselstellen ausfällt, für die keine Ersatzkraft mit dem nötigen Fachwissen vorhanden ist oder die ausscheidende Person allein bestimmte Passwörter kannte, kann der Betrieb über längere Zeit gestört sein oder komplett ausfallen.

2.5. Personal

Für einen sicheren Betrieb müssen Regelungen ausgegeben werden, wie Mitarbeiter, vor allem in Notfällen, zu verfahren haben. Jedoch müssen diese Regelungen auch bekannt gemacht werden. Mitarbeiter dürfen sich im Ernstfall nicht vor der Verantwortung drücken dürfen, indem sie behaupten, sie hätten keine Kenntnis dieser Regelungen.

Neben mangelnden Kenntnissen über Regelungen können Mitarbeiter auch wissentlich gegen Regelungen verstoßen. Dies muss keinen kriminellen Hintergrund haben. Oft mangelt es Mitarbeitern über das Verständnis der Sicherheitsbestimmungen. Durch falsche Verwendung der IT-Systeme können somit die Mitarbeiter unwissentlich sensible Informationen zugänglich machen oder Daten zerstören. Auch die IT-Hardware kann durch unsachgemäßen Umgang beschädigt werden. Gründe sind hier oft eindringende Feuchtigkeit oder Schmutz.

Nun zu den vorsätzlichen (kriminellen) Handlungen. Frustrierte Mitarbeiter könnten ihren Zorn an der IT-Hardware auslassen und somit direkte Schäden erzeugen. Dabei handelt es sich jedoch eher um Sachschäden. Problematischer ist das Ausspähen und die Weitergabe sensibler Informationen. Oft werden dazu Mitarbeiter mit weitreichenden Befugnissen verwendet, die z.B. durch die Vorspielung falscher Tatsachen zum Ausplaudern von Informationen gebracht werden. Kritisch ist auch eine Manipulation von Daten. Ein solcher Eingriff kann unter Umständen erst viel später oder gar nicht erkannt werden.

Die empfohlenen Maßnahmen zielen zunächst auf die Schulung der Mitarbeiter. Die Schulung soll dabei die korrekte Verwendung der Anwendungen aber auch die existierenden Sicherheitsmechanismen vermitteln.

Die Einweisung neuer Mitarbeiter sollte einheitlich und konsequent durchgezogen werden. Allen Mitarbeitern sollte klar sein, dass sie verpflichtet sind, die bestehenden Regelungen und Vorschriften einzuhalten.

Ähnlich zu der Einweisung neuer Mitarbeiter sollte auch eine Regelung für das Ausscheiden von Mitarbeitern eingeführt werden. Wichtig ist dabei u.a. eine Übergangszeit, in der der bisherige Mitarbeiter den neuen in die Arbeit einweisen kann. Außerdem müssen rechtzeitig alle Zugangsberechtigungen gelöscht werden. Mitarbeiter, die mit besonders sensiblen Informationen betraut waren müssen eine Verschwiegenheitserklärung abgeben.

Zuletzt noch optionale Maßnahmen: Zufriedene Mitarbeiter sind essenziell für einen sicheren und geordneten Betriebsablauf. So sollten Aktivitäten, die das Betriebsklima stören vermieden werden. Dazu zählen u.a. Umstrukturierungen, Verkauf und Fusionen. Einrichtungen zur Verbesserung des Betriebsklimas sind ebenfalls sinnvoll. Mitarbeitern mit persönlichen Problemen kann eine Anlaufstelle zur Verfügung gestellt werden.

3. Anwendung der Bausteine

Allgemein lässt sich festhalten, dass keine generelle Aussage über die benötigten Sicherheits-einrichtungen getroffen werden kann. Das Grundschutzhandbuch gibt die Richtlinien vor. Jedoch sollte für jede Installation des e.P.b. eine individuelle Sicherheitsanalyse durchgeführt werden.

Dabei muss zwischen den entstehenden Kosten und dem erreichten Nutzen (dem Sicherheitslevel) abgewogen werden. Dabei kann durchaus eine Mischung der im IT-Grundschutzhandbuch empfohlenen Maßnahmen der Bausteine angestrebt werden.

Die e.P.b.-Arbeitsgruppe empfiehlt die Anwendung der Maßnahmen für ein Rechenzentrum, wenn mehrere Standesämter einer Gemeinde eine gemeinsame IT-Infrastruktur nutzen möchten. Will ein Standesamt ein eigenständiges e.P.b. aufbauen, sollten die Maßnahmen für einen Serverraum angewandt werden.

Literaturverzeichnis

- [1] Bundesamt für Sicherheit in der Informationstechnik. *IT-Grundschutzhandbuch*. 2003.
- [2] Ingo Graser. *Sicherheitsmechanismen für ein elektronisches Archiv digital signierter Dokumente*. 2004.
- [3] Burkhardt Renz. *Das elektronische Personenstandsbuch - Ein Konzept*. 2004.