IT-Handbuch

für die Verwaltung der
Freien und Hansestadt Hamburg

Grundschutzkonzept für die Informations- und Kommunikationstechnik in der hamburgischen Verwaltung (IuK-Grundschutzkonzept)

Stand: 18. November 1994

Grundlagen

In der hamburgischen Verwaltung werden Aufgaben in großem Umfang mit Hilfe der Informations- und Kommunikationstechnik (IuK) wahrgenommen. Da in dem Maße, in dem der Einsatz von IuK-Systemen zunimmt, auch die Abhängigkeit von dieser Technik steigt, kann eine Beeinträchtigung des IuK-Systems im Einzelfall zu beträchtlichen wirtschaftlichen Schäden oder erheblichem Vertrauens- und Ansehensverlust in der Öffentlichkeit führen.

Bei der konventionellen Aufgabenerfüllung ist der Schutz sowohl der Arbeitsmittel als auch der Dokumente vor unbefugten Eingriffen selbstverständlich. Bücher z.B. werden inventarisiert, in der Bücherei untergebracht und ihre Ausleihe besonders notiert. Dokumente werden in Akten aufgenommen und in Registraturen verwahrt, Schriftstücke mit einem hohen Schutzbedarf als geheim oder streng geheim eingestuft, unter Verschluß gehalten und nur an autorisierte Personen herausgegeben.

Bei Einsatz von IuK-Systemen richtet sich das Augenmerk demgegenüber häufig fast ausschließlich auf die Funktionsfähigkeit des Systems. Der systematische Einsatz adäquater Sicherheitsmaßnahmen ist jedoch auch hier unverzichtbar und zumindest ein mittleres Schutzniveau sollte selbstverständlich sein. Dies bedeutet, daß organisatorische, personelle und technische Maßnahmen ergriffen werden müssen, um eine ausreichende Verfügbarkeit, Integrität und Vertraulichkeit zu gewährleisten.

Die Verfügbarkeit ist gewährleistet, wenn das IuK-System zu den vorgesehenen Zeiten uneingeschränkt zur Verfügung steht, Integrität ist gegeben, wenn keine nicht beabsichtigten Veränderungen herbeigeführt werden können und Vertraulichkeit besteht, wenn kein unbefugter Informationsgewinn stattfinden kann.

Um hierfür eine übergreifende Unterstützung zu bieten, die unverhältnismäßigen Untersuchungsaufwand im Einzelfall vermeiden hilft, wurde das Grundschutzkonzept entwickelt. Es ist die Zusammenstellung der Regeln, die, umgesetzt in konkrete Maßnahmen (Sicherheitskonzept), einen geringen bis mittleren Schutzbedarf angemessen abdecken.

Umsetzung des Grundschutzkonzeptes

Für die Grundschutzmaßnahmen - ohne die als "empfehlenswert" gekennzeichneten Zusatzmaßnahmen - kann die Angemessenheit grundsätzlich als gegeben unterstellt werden. Wird nicht nach dem Grundschutzkonzept vorgegangen, ist in jedem Fall auch die Angemessenheit der geplanten Maßnahmen zu prüfen.

Das Grundschutzkonzept ist als Checkliste angelegt, um die Umsetzung zu erleichtern und steht als Diskette im Format Word für Windows 6.0 zur Verfügung (BN: 9.23.1625; PN: 040/3498-1625). Bei der Umsetzung soll jeder Punkt der Checkliste bearbeitet werden. Wenn zu einzelnen Punkten kein Handlungsbedarf besteht, soll dies mit Begründung in der Spalte "Bemerkungen, Erledigungsvermerke" dokumentiert werden.

Vorgehen bei bereits installierten IuK-Systemen

Bei installierten IuK-Systemen sollte zunächst das vorhandene Wissen im Hinblick auf Risiken und Gefahren und die ohnehin verfügbaren Gegenmaßnahmen zur Sicherung genutzt werden. So wird für die Zeit bis zum Einsatz der endgültig ausgewählten Sicherheitsmaßnahmen das Risiko unbefugter Handlungen gesenkt. Das weitere Vorgehen entspricht dann dem bei IuK-Systemen in Planung.

Vorgehen bei IuK-Systemen in Planung

Das geplante IuK-System ist vor Fertigstellung hinsichtlich seines Schutzbedarfs einzustufen (Risikoanalyse). Bei einem mittleren Schutzbedarf reichen die nach den Grundschutzregeln getroffenen Maßnahmen aus, bei einem hohen Schutzbedarf ist vor Einsatz des Systems eine individuelle Sicherheitsanalyse durchzuführen, so daß der Betrieb in jedem Fall mit den angemessenen Sicherheitsmaßnahmen aufgenommen wird.

Für die Einstufung des Schutzbedarfs wird als Anhalt in Anlage 1 eine Tabelle aus dem Grundschutzhandbuch des BSI beigefügt.

Werden Veränderungen an einem IuK-System vorgenommen, oder haben sich die Einsatzbedingungen verändert, muß überprüft werden, ob die vorhandenen Schutzmaßnahmen weiterhin ausreichend und angemessen sind. Es kann erforderlich sein, aufgrund der Veränderungen ergänzende Grundschutzmaßnahmen einzusetzen oder eine Sicherheitsanalyse durchzuführen und daraus resultierende zusätzliche oder wirksamere Schutzmaßnahmen einzuführen. Dies gilt auch für neue Möglichkeiten durch technischen Fortschritt.

Weiterführende Literatur

IuK-Sicherheitshandbuch - Herausgeber: Bundesamt für Sicherheit in der Informationstechnik; zu beziehen für 53,- DM bei der Bundesdruckerei, Südstr. 119, 53175 Bonn, Tel.: 0228/38202-0, Fax: 0228/38202-22.

IuK-Grundschutzhandbuch - Herausgeber: Bundesamt für Sicherheit in der Informationstechnik, Postfach 200363, 53133 Bonn. Das Grundschutzhandbuch wird voraussichtlich Anfang 1995 durch einen Verlag veröffentlicht.

Checkliste der Grundschutzregeln	Handlungsbedarf Nein	Ja	Bemerkungen, Erledigungsvermerke

1	Organisation			
1.1	Schriftliche Festlegung von Verantwortlichkeiten, so daß jeder IuK-Benutzer weiß, was er zu tun hat - Rollen definieren, z.B. Revision, Systemverwaltung, Anwendungsentwicklung, Anwendergruppe mit Rechten abc, Anwendergruppe mit Rechten xyz, Anwenderbetreuung, - klären, welche Rollen zueinander in Konflikt stehen, z.B. Systemverwaltung und Revision, - Rollen Personen zuordnen; miteinander in Konflikt stehende Rollen nicht einer Person zuweisen; möglichst weitgehende Trennung der Rollen einführen (s. auch IT-Handbuch 09.110 HKR-ADV-Best, 11.300 - 11.400 Freigabe-RL mit DB, 11.700 PC-RL), - auch bei kleinen IuK-Systemen die Systemverwaltung und Entwicklung von der Anwendung trennen, wenn mehr als eine Person das IuK-System nutzt.			
1.2	Festlegen, welche Rechte die einzelnen Rollen haben und - bei TK-Anlagen - welche Leistungsmerkmale benutzt werden dürfen Rechte (Zugangsrechte, Zugriffsrechte) nur in dem zur Aufgabenerfüllung notwendigen Umfang vergeben; bei TK-Anlagen nicht benötigte Leistungsmerkmale sperren.			
1.3	Schriftliche Regelungen in Bezug auf das IuK-System treffen, so daß jeder betroffene Benutzer weiß, wie er damit umzugehen hat (s. a. IT-Handbuch 11.100 DS-Richtlinie) Auf das IuK-System bezogene Konkretisierungen bestehender Vorschriften, z.B. Sicherheits-vorschriften, Zugangsregelungen, Regelungen zum Umgang mit Authentisierungsmitteln, (Magnetkarten, Chipkarten, Token u.ä.), Regelungen zur Verwaltung der Schlüssel für Rechnerräume, Regelungen über die Nutzung privater Hard- und Software (vgl. PC-RL).			
1.4	Beschaffungsverfahren für Hard- und Software regeln			
1.4.1	Hard- und Software nur aus vertrauenswürdigen Quellen beschaffen Bei Abruf aus Rahmenverträgen ist dieser Punkt erfüllt.			
1.4.2	Wartung und Pflege sicherstellen			
1.4.3	Kompatibilität zu vorhandener Hard- und Software sicherstellen			

Checkliste der Grundschutzregeln		Handlungsbedarf Nein	Ja	Bemerkungen, Erledigungsvermerke
1.5	Freigabe			
1.5.1	Hardware vor Einsatz auf Fehlerfreiheit prüfen			
1.5.2	Allgemeine Software (Betriebssystem, Dienstprogramme) vor Einsatz auf Fehlerfreiheit und Kompatibilität zur Anwendungssoftware prüfen			
1.5.3	Anwendungssoftware vor Einsatz auf Eignung und Fehlerfreiheit prüfen (s.a. IT-Handbuch 11.300 - 11.400 Freigabe-RL mit DB, 11.700 PC-RL)			
1.6	Bestandsverzeichnisse			
1.6.1	Geräte und Datenträger kennzeichnen			
1.6.2	Geräteverzeichnis über die gesamte Hardware anlegen Um einen Überblick über die eingesetzte Technik zu behalten, darf die Erfassung nicht auf Geräte beschränkt sein, mit denen personenbezogene Daten verarbeitet werden (s. IT-Handbuch 07.210 DB zu § 9 Abs. 3 und 4 HmbDSG). Von Strom- und Hafenbau kann eine technische Unterstützung (GERDA) bezogen werden.			
1.6.3	Datenträgerverzeichnis für wechselbare Datenträger (wie Band, Kassette, Wechselplatte, CD, Diskette) anlegen Das Verzeichnis sollte Quelle, Aufbewahrungsort, Aufbewahrungsdauer, berechtigte Empfänger enthalten.			
1.6.4	Softwareverzeichnis anlegen Das Verzeichnis sollte Vertragsdaten, Bezeichnung der Software und Installationsort enthalten. Bei kommerzieller Software sicherstellen, daß nur lizensierte Software eingesetzt wird (Urheberrecht). GERDA (s. Geräteverzeichnis) unterstützt auch die Führung des Softwareverzeichnisses.			

Checkliste der Grundschutzregeln		Handlungsbedarf Nein	Ja	Bemerkungen, Erledigungsvermerke
1.7	Software und ihre organisatorischen Zuammenhänge dokumentieren Soweit nicht ohnehin Vorschriften (s. auch IT-Handbuch 09.110 HKR-ADV-Best, 11.500 Dokumentations-RL, 11.300 - 11.400 Freigabe-RL mit DB, 11.700 PC-RL) die Dokumentation regeln, sollte aus Eigeninteresse immer sorgfältig dokumentiert werden, da sonst ein sicherer Betrieb nicht möglich ist. So wird nicht nur das Risiko von Fehlfunktionen und Ausfällen durch Bedienungsfehler oder Fehler bei der Programmierung gesenkt, sondern auch, da eine Überprüfung erleichtert wird, das Risiko unentdeckter Manipulationen.			
1.8	Datenträger			
1.8.1	Datenträger unter Verschluß verwahren und gesichert transportieren Dies gilt nicht nur für magnetische Datenträger, sondern auch für Papier. Sie sind vor Veränderung, Zerstörung und gegen unbefugte Kenntnisnahme zu schützen. Transport in verschlossenen Behältern. Drucker nicht allgemein zugänglich aufstellen. Wenn sichere Verwahrung oder sicherer Transport anders nicht gewährleistet werden können, magnetische Datenträger verschlüsseln. Dies ist auch hilfreich bei der Entsorgung (s. 1.8.3).			
1.8.2	Sicherungsdatenträger immer in verschlossenen Schränken, sensible Datenträger in Stahlschränken oder im Datentresor verwahren			
1.8.3	Nicht mehr benötigte Datenträger mit schützenswerten Daten sicher entsorgen (s. Entsorgungs-RL)			
1.9	Wartung und Pflege (Service) sicherstellen, bei Servicevereinbarungen neben Art und Umfang Auftragnehmer verpflichten: (s.a. IT-Handbuch 12.010 TK-DB)			
1.9.1	die zum Service berechtigten Personen zu benennen			
1.9.2	die Servicemaßnahme anzukündigen			
1.9.3	Datengeheimnis und Verschwiegenheit zu wahren			
1.9.4	erhaltene Daten nicht weiterzugeben			
1.9.5	Daten nur für vereinbarte Zwecke zu nutzen			
1.9.6	alle an ihn übertragenen Daten nach Abschluß der Arbeiten zu löschen			

Checkliste der Grundschutzregeln		Handlungsbedarf Nein	Ja	Bemerkungen, Erledigungsvermerke
1.10	Ablauf der Servicearbeiten organisieren (s. a. IT-Handbuch 12.010 TK-DB)			
1.10.1	Eigenen Ansprechpartner dem Serviceuntenehmen benennen			
1.10.2	Bei lokalem Service Zugang zu den zu wartenden Einrichtungen sicherstellen			
1.10.3	Bei Fernwartung innerhalb eines Anlagenverbundes (interner Fernwartung) sicherstellen, daß der Wartungsapparat nicht amtsberechtigt ist			
1.10.4	Bei externer Fernwartung sicherstellen, daß der Zugang mit Rückrufautomatik erfolgt			
1.10.5	Benutzerkontrolle organisieren Wartungskennung schützen (z.B. Paßwort, Magnetkarte) wie andere Benutzerkennungen auch (s. 1.12). Sicherstellen, daß die Wartungskennung bei Bedarf auf jeden Fall genutzt werden kann.			
1.10.6	Bedingungen festlegen, unter denen beim Service ausnahmsweise Systemverwalterstatus erlangt werden darf			
1.10.7	Umfang der Protokollierung festlegen Ziel ist die Nachvollziehbarkeit sicherheitsrelevanter Tätigkeiten.			
1.10.8	Ort der Protokollführung festlegen Die Protokolle müssen vor Ort geführt werden, bei technischer Unterstützung der Protokollierung auf dem gewarteten Rechner.			
1.10.9	Auswertungskriterien für die Protokolle festlegen			
1.10.10	Aufbewahrungsfristen für Protokolle und Protokollauswertungen festlegen			
1.10.11	Festlegen, auf welche Weise die Fernwartungstätigkeit überwacht wird			
1.10.12	Form der Datenübergabe an Serviceunternehmen festlegen Die Entscheidung über die Herausgabe von Daten muß beim Auftraggeber liegen. Kein eigenmächtiges Abrufen oder Mitnehmen von Daten zulassen. Buchführen, was an wen herausgegeben wurde.			
1.10.13	Organisieren, daß nach Abschluß der Servicemaßnahme alle bekanntgegebenen Paßwörter geändert werden (s. a. IT-Handbuch 11.650 Paßwort-RL)			

Checkliste der Grundschutzregeln		Handlungsbedarf Nein	Ja	Bemerkungen, Erledigungsvermerke
1.11	Zugangsregelungen für Räume mit zentraler Technik (z.B. Mehrplatzrechner, Server, Router) treffen			
1.12	Verwaltung von Benutzerkennungen regeln, dabei sicherstellen, daß			
1.12.1	Benutzerkennungen grundsätzlich personenbezogen vergeben werden			
1.12.2	Benutzerkennungen immer geschützt werden (Paßwort o.ä.)			
1.12.3	die Authentisierungsmittel mit der gebotenen Sorgfalt verwaltet werden (z.B. Paßwortverwaltung, Chipkartenverwaltung)			
1.12.4	Benutzerkennungen nur mit den notwendigen Rechten versehen werden			
1.12.5	bei Aufgabenveränderung, Versetzung oder Ausscheiden eines Bediensteten die Benutzerkennung aufgehoben bzw. in ihren Rechten angepaßt wird			
1.13	Protokollierung			
1.13.1	Ereignisse definieren, die im Normalfall und in Ausnahmefällen zu protokollieren sind Systemverwalteraktivitäten sollten immer protokolliert werden.			
1.13.2	Auswertung der Protokolle festlegen im Hinblick auf Sicherheitsverletzungen und Fehler (Hard-, Software, Bedienung). Die Protokolle über Systemverwalteraktivitäten durch eine Person auswerten lassen, die nicht der Systemverwaltung angehört.			
1.13.3	Vorgehen nach festgestellten Sicherheitsverstößen festlegen			
1.14	Unterlagen in erforderlichem Umfang zur Verfügung stellen Vorschriften, Regeln, Bedienungsanleitungen u.ä. müssen für die Bediensteten zugänglich sein. Häufig benötigte Unterlagen sollten am Arbeitsplatz verfügbar sein.			
1.15	Kontrollieren, ob die Vorschriften und Regeln eingehalten werden Hierzu gehören z.B. das HmbDSG, fachspezifische gesetzliche Regelungen, die im IT-Handbuch veröffentlichten Richtlinien der Finanzbehörde, behördeninterne Dienstanweisungen und Regelungen. Bei Verstößen Ursache herausfinden und beseitigen, z.B. Vorschriften verbessern oder Bedienstete über Inhalt und Sinn informieren.			

Checkliste der Grundschutzregeln		Handlungsbedarf Nein	Ja	Bemerkungen, Erledigungsvermerke
1.16	Sicherheitsmaßnahmen an geänderte Bedingungen und entsprechend dem technischen Fortschritt anpassen (s. auch IT-Handbuch 11.100 DS-Richtlinie)			

empfehlenswert:

1.17	Einsatz von Standardsoftware anstelle selbsterstellter Programme			
1.18	Einrichten eines Benutzerservices			

Checkliste der Grundschutzregeln	Handlungsbedarf Nein	Ja	Bemerkungen, Erledigungsvermerke
2	**Personal**		
2.1	Besonders sorgfältige Auswahl von Personal mit sicherheitsrelevanten Tätigkeiten (z.B. Systemverwaltung) Neben fachlicher Qualifikation besonderen Wert legen auf Zuverlässigkeit, Verantwortungsbewußtsein, Durchsetzungsfähigkeit, Ordnungssinn.		
2.2	Benutzer des IuK-Systems qualifizieren Eine Umfrage der Zeitschrift KES 1990 ergab, daß 44% der Beeinträchtigungen der IuK-Sicherheit durch Irrtum und Nachlässigkeit entstanden waren.		
2.2.1	Vorschriften und Regelungen bekanntgeben (s. auch IT-Handbuch 11.100 DS-Richtlinie)		
2.2.2	Bedienung der Hardware schulen		
2.2.3	Anwendung der Software schulen		
2.3	Vertreter einarbeiten Eine nur auf dem Papier stehende Vertretungsregelung ist sinnlos, der Vertreter muß auch die erforderlichen Kenntnisse haben.		

Checkliste der Grundschutzregeln	Handlungsbedarf Nein	Ja	Bemerkungen, Erledigungsvermerke

3	**Notfallvorsorge**			
3.1	Geeigneten Standort für zentrale und dezentrale Technik auswählen Zentrale technische Einrichtungen nicht in Räumen unterbringen, die besonders durch Feuer, Wasser, andere Umwelteinflüsse wie z.B. Abgase, Staub, chemische Dämpfe, elektromagnetische Felder oder durch Einbruch gefährdet sind, wenn nicht Vorkehrungen zur Abwehr dieser Bedrohungen getroffen sind. Für dezentrale Komponenten wie PC, Bildschirme, Drucker u.ä., die in aller Regel in Büroräumen aufgestellt sind, ist bei vorgesehenem Gebrauch in anderer Umgebung (z.B. auf einer Baustelle) die Eignung hierfür zu überprüfen. Unabhängig hiervon ist ein Standort nicht geeignet, an dem die Technik nicht gegen unbefugte Handlungen geschützt werden kann, wie z.B. der Flur eines jedermann offenstehenden Bürogebäudes.			
3.2	Endgeräte, an die besondere Rechte geknüpft sind (z.B. Systemverwaltung, Netzverwaltung) besonders sichern, z.B. in verschlossenen Räumen aufstellen.			
3.3	Handfeuerlöscher vor Räumen mit zentraler Technik anbringen.			
3.4	Vorgeschriebene Betriebsbedingungen beachten Ggf. Klimaanlage zum Schutz vor extremer Raumtemperatur und unzulässiger Luftfeuchtigkeit installieren.			
3.5	Technische Einrichtungen vor Spannungsunterbrechungen und -schwankungen im Stromnetz schützen Schutz vor Spannungsunterbrechung durch Hinweise in den Sicherungskästen, Stromabschaltung nur nach vorheriger Absprache mit den Anwendern bzw. Systemverwaltern, unterbrechungsfreie Stromversorgung (USV), Überspannungsfilter.			
3.6	Intervalle für die regelmäßige Datensicherung festlegen Datenbestandsname unter "Bemerkungen, Erledigungsvermerke" eintragen.			
3.6.1	Täglich			
3.6.2	Wöchentlich			
3.6.3	Monatlich			
3.6.4	Besonderes Intervall			

Checkliste der Grundschutzregeln		Handlungsbedarf Nein	Ja	Bemerkungen, Erledigungsvermerke
3.7	Meldewege für den Notfall festlegen			
3.8	Verantwortung für Notfallmaßnahmen regeln			
3.9	Verfügbarkeitsanforderungen der DV-Verfahren ermitteln			
3.10	Eingeschränkten IuK-Betrieb definieren Gemeint ist die Festlegung derjenigen Geräte und DV-Verfahren, die auch im Notfall verfügbar sein müssen. Hierfür muß eine Backup-Lösung zur Verfügung stehen.			
3.11	Interne und externe Ausweichmöglichkeiten festlegen			
3.12	Wiederanlaufplan erstellen Der Wiederanlaufplan muß Maßnahmen zur Sicherstellung etwa notwendiger Ersatzbeschaffungen enthalten. Es muß geklärt sein, daß die Ersatzbeschaffung innerhalb tragbarer Fristen möglich ist. Ggf. sind hierzu mit einzelnen Lieferanten Vereinbarungen zu schließen.			
3.13	Wiederanlaufmaßnahmen testen			

empfehlenswert:

3.14	Auslagerung wichtiger Sicherungsdatenträger in ein anderes Gebäude			
3.15	Redundanz bei wichtigen Komponenten (z.B. Leitungswege, Magnetplatten)			
3.16	Separater Stromkreis für die IuK-Technik			

Checkliste der Grundschutzregeln	Handlungsbedarf Nein	Ja	Bemerkungen, Erledigungsvermerke

4	**Rechnerbetrieb**			
4.1	Identifikation und Authentisierung der Benutzer durch individuelle Benutzerkennung und Paßwort (IT-Handbuch 11.100 DS-Richtlinie, 11.650 Paßwort-RL, 11.700 PC-RL) Dies erfordert u.U. die Installation von Sicherheitssoftware (z.B. bei MS-DOS). Bei PCs sollte immer das BIOS-Paßwort vergeben werden. Soweit keine individuelle Benutzerkennung möglich ist (z.B. bei Systemverwalterkennungen), durch andere Maßnahmen sicherstellen, daß nachvollzogen werden kann, wer jeweils tätig war.			
4.2	Technische Unterstützung der organisatorischen Vorgaben soweit wie möglich			
4.3	Verschlüsselte Speicherung von Paßwörtern (IT-Handbuch 11.650 Paßwort-RL-RL)			
4.4	Sperren der Betriebssystemebene für Anwender von DV-Verfahren			
4.5	Benutzung der externen Rechnerschnittstellen nur durch autorisierte Personen ermöglichen Schnittstellen ggf. ausbauen, verplomben oder per Sicherheitssoftware sperren. Bootschutz für Diskettenlaufwerk installieren (s. a. IT-Handbuch 11.700 PC-RL).			
4.6	Einspielen von Software nur durch autorisierte Personen nach Freigabe ermöglichen Schutz vor manipulierter Software, z.B. Viren (s. auch IT-Handbuch 11.300 - 11.400 Freigabe-RL mit DB, 11.700 PC-RL)			
4.7	Sicherstellen der Unversehrtheit eingespielter Software Mit Virenscanner prüfen, ggf. mit Prüfsumme versehen, Schreibzugriff nur an Befugte vergeben (s. auch IT-Handbuch 11.700 PC-RL).			
4.8	Sperren oder Löschen nicht (mehr) benötigter Zugangsmöglichkeiten wie Terminals oder Benutzerkennungen			

Checkliste der Grundschutzregeln	Handlungsbedarf Nein	Ja	Bemerkungen, Erledigungsvermerke
4.9 Arbeiten unter Benutzerkennungen mit Systemprivilegien (bei UNIX:root) auf ein Minimum reduzieren Soweit möglich, Systemverwaltertätigkeiten auf Benutzerkennungen verlagern, die nicht mit allen Systemprivilegien ausgestattet sind oder menügesteuert ohne Betriebssystemzugang ausführen. **Unter privilegierten Benutzerkennungen nur arbeiten, wenn unbedingt erforderlich.**			
4.10 Anwendungsprogrammen nicht ermöglichen, mit Systemprivilegien abzulaufen Anwendungsprogramme nicht aus privilegierten Kennungen (bei UNIX root) heraus starten, da sie in diesem Augenblick die Rechte der aufrufenden Kennung haben.			

Checkliste der Grundschutzregeln	Handlungsbedarf Nein	Handlungsbedarf Ja	Bemerkungen, Erledigungsvermerke
5 Netzbetrieb			
5.1 Technische Unterstützung der organisatorischen Vorgaben soweit realisierbar			
5.2 Strukturierte Verkabelung Darüber hinaus ist weitestgehende Verwendung von Glasfasertechnik anzustreben. Glasfasertechnik bietet einen hohen Schutz vor Abhören, da kaum kompromittierende Abstrahlung auftritt, und unbemerktem Aufschalten, da erheblicher Aufwand erforderlich ist, um das Kabel aufzutrennen und dies zudem zu Fehlermeldungen führen würde. Sie ist für hohe Übertragungsgeschwindigkeiten geeignet und unempfindlich gegen Störeinflüsse.			
5.3 Lokales Netz entsprechend den Anforderungen gestalten Stern, Baum, Bus, Ring haben jeweils spezifische Vor- und Nachteile.			
5.4 Netzbetriebssystem kompatibel zur eingesetzten Technik und lokalen Betriebssystemen mit mindestens folgenden Funktionen auswählen:			
5.4.1 Festlegen der Übertragungswege			
5.4.2 Berechtigungsprüfung bei Netzzugang			
5.4.3 Festlegen und prüfen von Übertragungs- und Zugriffsrechten			
5.4.4 Optional Protokollierung von Übertragungen			
5.4.5 Verschlüsselte Speicherung von Paßwörtern			
5.4.6 Verschlüsselte Übertragung von Paßwörtern			
5.5 Externe Netzanschlüsse unter eigener Kontrolle behalten Dies ist z.B. möglich durch Rückruf, (virtuelle) Standleitung, geschlossene Benutzergruppe.			
5.6 Kabel sicher verlegen An allgemein zugänglichen Orten, wie z.B. Fluren oder Warteräumen, Kabel nicht offen verlegen. In Dienstzimmern hingegen wäre dies kein Problem (eventuell sogar ein Vorteil, da Manipulationen bemerkt würden).			

Checkliste der Grundschutzregeln		Handlungsbedarf Nein	Ja	Bemerkungen, Erledigungsvermerke
5.7	Netz dokumentieren			
5.7.1	Verlegung der Kabel (Kabelpläne) aufzeichnen			
5.7.2	Leitungen an Verteilern kennzeichnen			
5.7.3	Netzkomponenten und ihre Verbindung dokumentieren			
5.7.4	Externe Anschlüsse dokumentieren			
5.8	Ankommende Wählverbindungen besonders absichern Geeignet ist hierfür z.B. die Installation eines Gateway-Rechners, der die Zulässigkeit des Verbindungswunsches prüft, die Einrichtung einer geschlossenen Benutzergruppe, die Einrichtung einer Rückrufautomatik, das Einrichten einer permanent virtuellen Verbindung. Immer sollte der Absender überprüft werden.			
5.9	An Netzübergängen mit Hilfe der Router die MAC-Adresse des Absenders prüfen Mit dieser Maßnahme kann eine Maskierung der IP-Adresse weitgehend ausgeschlossen werden.			
5.10	Den Self-Learning-Algorithmus der Router ausschalten, damit nicht unbekannte IP-Adressen im Netz zugelassen werden			
5.11	Eine Netzadministration einrichten Aufgabe der Netzadministration ist die Fehlerdiagnose und -behebung, das Festlegen der zugelassenen Verbindungen, die Autorisierung von Benutzern und die Rechteverwaltung im Netz. Diese Tätigkeit ist sicherheitsrelevant und sollte daher nur von wenigen Personen ausgeübt werden.			

Empfehlenswert:

5.12	Optionale Datenverschlüsselung im Netz Durch Verschlüsselung können Bedrohungen wie unbefugter Informationsgewinn oder Manipulation von Daten abgewehrt werden. Die Verschlüsselung von Daten im Netz erfordert jedoch im Verhältnis zu einem mittleren Schutzbedarf z.Zt. noch unangemessen hohen Aufwand und ist daher nicht als Grundschutzregel aufzustellen. Sie ist aber angemessen zur Abdeckung eines hohen Schutzbedarfs.			