Datenschutz und Sicherheit

Theoretische Grundbegriffe der technischen und organisatorischen Datensicherheit.

Version 1.00 © Harry Zingel 2001, EMail: HZingel@aol.com, Internet: http://www.zingel.de

Inhaltsübersicht

1. Die drei Aspekte des Datenschutzes

Die mit dem deutschen Wort „Datenschutz“ korrespondierenden englischen Begriffe

- *Privacy*,
- *Safety* und
- *Security*

lassen den Inhalt des Datenschutzbegriffes *wesentlich anschaulicher* werden.

Wir können diese drei Begriffe in der folgenden Art und Weise *visualisieren*.

Dieses Skript befaßt sich *fast ausschließlich mit den Safety- und dem Security-Aspekt* des Datenschutzes.

Die umfassende Bedeutung des Datenschutzbegriffes anschaulich demonstriert:

Schutz vor Einsicht Dritter (z.B. Sichtschutz):
Privacy

Sicherheit gegen Unfälle oder Pannen (z.B. Airbag, ABS):
Safety

Schutz vor Einbruch, Diebstahl, Vandalismus oder Kriminalität (z.B. Panzerglas, Wegfahrsperre, Sicherheitsschlösser usw.):
Security

Privacy ist jede Form des Schutzes gegen unbefugte Einsicht Dritter, etwa Codierung oder Signatur von Daten.

Security ist der Schutz gegen Sabotage oder kriminelle Akte, etwa Computerviren, trojanische Pferde oder andere Arten der Spionage.

Safety ist der Schutz vor Datenverlust durch technische Ausfällen von Datenverarbeitungsanlagen etwa durch Datensicherung.

2. Benutzerberechtigungen

2.1. Relevante Grundfragen des Datenschutzes

Einige hierher passende Gebote des Datenschutzgesetzes sind:

- Zugangskontrolle: Festlegung befugter Personen, Berechtigungsausweise, Vieraugenprinzip, Regelung für Fremde, Besucherbuch;
- Anwendungskontrolle: Zuordnung zwischen Benutzergruppen und Anwendungen, Verantwortung von Projektleitern, Verfahrensdokumentation bei kritischen Anwendungen, Programmier-Regeln für kritische Anwendungen, Prüfregeln bei kritischen Anwendungen, Auftragskontrolle.

Hierzu müssen die folgenden Fragen durch die Geschäftsleitung beantworten werden:

- Wer darf mit dem System arbeiten?
- Was darf mit den Informationen und Daten gemacht werden oder nicht?
- Wer darf bestimmte Informationen lesen oder verändern?
- Warum muß eine bestimmte Operation ausgeführt werden?
- Wann darf eine bestimmte Operation ausgeführt werden?
- Wo darf eine bestimmte Operation ausgeführt werden?
- Wer darf einen Auftrag zu einer bestimmten Operation geben?

Organisatorisch festzulegen ist auch, wer sich hinter einer formalen Benutzerberechtigung verbirgt und wer gegebenenfalls für ihre Verwendung verantwortlich ist. Benutzer kann sein:

- eine eindeutige Person (z.B. „Max Mustermann“)
- ein Stellvertreter („der Oberarzt im Auftrag des Chefarztes“)
- ein Funktionsträger („der diensthabende Arzt“, „der Stationsarzt“)
- eine Rolle („Materialausgabe“, „Apotheke“,...)

Das Problem der Mehrfachbenutzung einer Identität kann zwar umgangen werden, indem jede natürliche Person nur unter einer eindeutigen Identifikation Zugang zum Datensystem bekommt. In der Praxis ist das aber oft zu kompliziert, etwa wenn die gleiche Funktion notwendig auf verschiedene Personen verteilt ist, denn sonst bräuchte man ständige An- und Abmeldevorgänge oder viele zusätzliche Terminals; problematisch ist auch stets die Regelung des Mehrfachzugriffs auf einen Datensatz. In solchen Fällen erhalten die Fragen des Wann und Wo besonderes Gewicht.

2.2. Identifikation und Authentifizierung

Mit der Identifikation beim Anmeldevorgang sagt der Benutzer, wer er zu sein vorgibt, mit der Authentisierung beweist er dem System, daß er das auch wirklich ist, in der Regel durch ein Paßwort. Dafür geeignet ist auch ein unveränderliches persönliches Merkmal wie der Fingerabdruck oder ein Geheimnis, welches nur der Benutzer und der Computer kennen. Die drei Prinzipien

- *wissen* (z.B. ein Paßwort),
- *haben* (einen Ausweis, eine Chipkarte oder einen Schlüssel),
- *sein* (nachgewiesen durch biometrische Merkmale

können einzeln oder kombiniert angewendet werden. Der Aufwand für einen Angriff ist entsprechend zu bewerten; er besteht aus:

- *Erlangen* des Wissens,
- *Entwenden* oder *Fälschen* des *Objekts*,
- *Fälschen* der *Merkmale*.

Strenggenommen ist die Indentifikation in der Authentifizierung enthalten, trotzdem ist eine Trennung der beiden Vorgänge von Bedeutung:

- Ein zufällig erratenes Paßwort nützt nur, wenn es auch der richtigen Identität zugeordnet werden kann.
- Benutzer sollten ihr Paßwort selbst wählen können. Wäre die Identifizierung kein getrennter Vorgang, so müßte verhindert werden, daß zwei Benutzer zufällig das gleiche Paßwort wählen. Aus der Ablehnung des Paßwortes könnte ein Benutzer schließen, daß dieses schon existiert.

Der Versuch, sich mit einer falschen Identifikation ins System einzuschleichen, wird als *Maskerade* bezeichnet. In vielen Fällen reicht hierzu ein enttarntes Paßwort. Die Authentisierung kann zusätzlich durch eine Chipkarte abgesichert werden. Eine Variante aus dem militärischen Bereich ist das Paßwort (besser nur einen Teil davon) auf der Karte abzuspeichern. Bei der Abmeldung wird ein vom Rechner zufällig erzeugtes neues Paßwort auf die Karte geschrieben.

Wichtig sind Maßnahmen bei Fehlversuchen zur Authentifizierung:

- *Alarm*,
- *Meldung* ungültiger Versuche beim nächsten korrekten Login unter der betroffenen Benutzeridentität
- *Stillegung* des Anschlusses.

Eine Alternative zum Paßwortschutz ist der Erkennungsdialog, in dem der Computer den Benutzer zufällig aus einer Liste gewählte Fragen stellt, etwa persönliche Fragen, besser aber einige Paßwörter. Das Verfahren hat sich in der Praxis nicht durchgesetzt, obwohl es bei sorgfältiger Implementierung durchaus Vorteile hat.

2.3. Paßwörter

Paßwörter sind der klassische Schutzmechanismus und das klassische Sicherheitsrisiko. Es ist sehr sorgfältig zu überlegen, wie die Paßwortpolitik des Systems aussehen soll. Die Handhabung von Paßwörtern ist per Vorschrift zu regeln; wichtigster Punkt:

Niemals ein Paßwort aufschreiben!

2.3.1. Angriffe auf Passwörter

Drei Stufen des systemischen Angriffs lassen sich unterscheiden:

1. Ziel: *Irgendein* Zugang zum System.

Häufige Methode: Der Angreifer kennt (oder errät) eine Benutzeridentifikation und probiert (per PC-Programm) Tausende von Paßwörtern (= „brute force attack“).

2. Ziel: *Privilegierter* Zugang zum System.

Einfachste Methode, falls man Zugang zu einem allgemein benutzten Terminal hat oder gar weitere Terminals für den Versuch requirieren darf: Ein zugelassener oder unbefugt ins System eingedrungener Benutzer stellt eine Paßwortfalle (= „spoofing attack“) auf.

3. Ziel: *Völlige Kontrolle* über das System.

Dazu braucht der Angreifer eine genügend privilegierte Benutzeridentifikation samt Paßwort.

Noch einmal zusammengefaßt: Paßwörter sind gefährdet durch

- Nachlässigkeit des Besitzers,
- ungenügende Schutzvorkehrungen des Systems,
- Abhören von Leitungen, Bildschirmen oder PCs
- Paßwortfallen
- systematisches Probieren und Fischzüge.

2.3.2. Planungshilfen für Passwortsicherheit

- Paßwörter dürfen bei der Eingabe nicht auf den Bildschirm erscheinen.
- Die Anzahl der zulässigen Falscheingaben muß beschränkt werden. Ein bewährtes Verfahren: Ein Fehl-

versuch ist frei, nach dem zweiten Versuch gibt es einen Alarm (hörbar oder als Meldung an eine Aufsichtsperson), nach dem dritten Versuch werden das Terminal und die Benutzeridentifikation gesperrt, und zwar so lange, bis der Systemverwalter die Sperre ausdrücklich aufhebt.

- Bei Fern- und Wählanschlüssen ist diese rigorose Sperre vielleicht nicht praktikabel, da es keine festen Terminaladressen gibt. In diesem Fall sollte man wenigstens Zeitsperren einbauen, deren Länge mit jedem Fehlversuch stark zunimmt. Auch die Rückrufmethode kann zusätzlichen Schutz bieten.
- Paßwörter müssen leicht änderbar sein, und zwar vom Benutzer selbst, in Notfällen aber auch vom Systemverwalter.
- Der Systemverwalter darf das Paßwortverzeichnis nicht lesen können; er muß jedes beliebige Paßwort ändern können, aber das darf nicht unbemerkt geschehen. Die gängige Methode, dieses zu erreichen, ist die Einweg-Verschlüsselung.
- Das Paßwortverzeichnis darf auch in verschlüsselter Form für unprivilegierte Benutzer nicht lesbar sein.
- Ein Paßwort darf niemals der einzige Schutz für kritische Daten sein.
- Paßwortverletzungen müssen protokolliert werden.
- Paßwortänderungen müssen leicht zu erzwingen sein, sowohl gezielt als auch automatisch per Verfallsdatum.
- Zu einfache Paßwörter müssen verhindert werden können, Standards müssen automatisch überwacht werden. Sinnvolle Kriterien:
  - Mindestens fünf Zeichen
  - Nicht gleich Benutzer-Identität
  - Nicht gleich Benutzer-Identität rückwärts gelesen
  - Nicht von der Form „xyzxyz“
  - Nicht von der Form „xyzzyx“
  - Nicht in der expliziten Negativliste enthalten
  - Nicht gleich einem vom selben Benutzer bereits verwendeten Paßwort
- Paßwörter sollten auf einzelne Personen beschränkt sein. Auch sollte sich jeder Benutzer möglichst nur ein Paßwort merken müssen.
- Nach Programmvorführungen sind Paßwörter sofort zu ändern.

Damit ein Paßwort nicht der einzige Schutz für ein sensitives System ist, kommen als Zusatzmaßnahmen in Frage:

- physische Zugangssperren,
- logische Terminalsperren,
- Zeitsperren,
- Hardwareschlüssel (sogenannte „Dongel“),
- Ausweiskarten mit einer Information, aus der zusammen mit Benutzernamen und Paßwort der eigentliche Zugangsschlüssel errechnet wird.

2.4. Benutzerprofil und Benutzer-Oberfläche

Die Autorisierung des Benutzers legt fest, welche Rechte der Benutzer nach einem erfolgreichen Systemzugang hat. Man spricht hier auch vom sogenannten Benutzerprofil. Die in diesem Profil in Form einer Datenbank gespeicherten Rechte sind über die Benutzeroberfläche zugänglich. Dazu gehören:

- spezielle Betriebssystem-Versionen,
- eine Startprozedur,
- die verfügbaren Betriebssystem-Funktionen, auch Tastenfunktionen (etwa „Break“, „Escape“...)
- Privilegien,
- die verfügbaren Anwendungsprogramme,
- Voreinstellungen für Parameter und Datei-Zugriffspfade,
- Berechtigungen zum Dateizugriff,
- Beziehungen zu anderen Benutzern (Kommunikation, Gruppenzugehörigkeit),
- Ein- und Ausgabemöglichkeiten,
- Verbrauchsrechte.

Anzustreben ist eine sichere Benutzer-Oberfläche mit jederzeit genau spezifiziertem Funktionsumfang. Eine solche Benutzer-Oberfläche ist die beste Absicherung gegen Bedienfehler, die zu unvorhergesehenen Zuständen führen, und stellt sicher, daß der Benutzer jederzeit nur im Rahmen seiner Rechte agiert. Da dieser Schutz auch in Fehlersituationen oder im Falle eines absichtlichen Abbruchs erhalten bleiben muß, muß er ins Betriebssystem integriert sein und kann nicht durch aufgepfropfte Maßnahmen erreicht werden.

Hergestellt wird die Arbeitsumgebung für den einzelnen Benutzer durch Parameter im Benutzerverzeichnis, vor allem aber durch die Startprozedur („autoexec“, „profile“). Diese ist zu Sicherheitszwecken nur geeignet, wenn sie vom Benutzer nicht selbst geändert, abgebrochen oder umgangen werden kann.

Wichtig ist die Gestaltung der Benutzer-Oberfläche nach ergonomischen Gesichtspunkten. Ein unübersichtlicher Bildschirm provoziert Fehler, ein langweiliger Programmablauf führt zu Schlamperei, etwa wenn wichtige Fehlermeldungen in einem Wulst von unwichtigen Informationen untergehen.

2.5. Überwachung und Beweissicherung

2.5.1. Teilaufgaben

Die beiden wesentlichen Teilaufgaben sind Überwachung gerade ablaufender Vorgänge und Aufzeichnung zur späteren Analyse. Alle sicherheitsrelevanten Vorgänge sind zu überwachen und zu protokollieren - manipulationsgeschützt! Die Beweissicherung muß untäuschbar und vollständig sein. Übeltäter werden dadurch gezwungen, Spuren zu hinterlassen.

Aufzeichnungen verhindern zwar Übergriffe nicht, lassen aber erkennen, wo die Sicherheit verletzt ist und in Zukunft bessere Maßnahmen zu treffen sind, und sie gestatten je nach den Umständen des Falles den Schaden wieder rückgängig zu machen. Darüber hinaus erhöhen sie das Vertrauen in das System, indem sie in Zweifelsfällen dokumentieren, daß im Moment die Daten sicher sind.

Protokolliert werden sollten alle An- und Abmeldevorgänge, vor allem falsche Paßworteingaben, Zugriffe auf Dateien, Benutzung von Programmen, Durchführung von Transaktionen, Zugriffen auf Systemtabellen, Änderungen von Systemparametern und der Ressourcenverbrauch.

2.5.2. Technische Verfahren

Die entsprechenden Schlagwörter sind:

- Logging: Aufzeichnung aller Aktionen und Meldungen der Systemkonsole oder eines bestimmten Benutzers, insbesondere von Start und Stop von Untersystemen und Prozessen, und alle Fehlermeldungen.
- Auditing: Aufzeichnung von An- und Abmeldevorgängen und Datenzugriffen, natürlich mit Zeitangaben; Aufzeichnung von Transaktionen und Änderungen von Systemparametern und Sicherheitsdefinitionen; Kontrolle, ob festgelegte Regeln eingehalten werden.
- Accounting: Aufzeichnung des Ressourcenverbrauchs zum Zwecke der Abrechnung; natürlich lassen sich mit einem solchen System auch mißbräuchliche Zugriffe auf Ressourcen aufdecken.
- Monitoring: laufende Überwachung des Ressourcenverbrauchs, um Engpässe zu erkennen und unbefugte Systemaktionen aufzudecken; schließlich läßt sich durch Blockade wichtiger Betriebsmittel (etwa CPU oder Ein- und Ausgabekanäle) das System ganz oder weitgehend lahmlegen. Ein Monitorsystem sollte sowohl gezielte Beobachtung einzelner Benutzer und Betriebsmittel erlauben als auch automatische Meldungen an die Systemkonsole oder an Verantwortliche geben, also ein Alarmsystem enthalten.

Alle Arten von Systemüberwachung konfrontieren den Verantwortlichen mit dem gesellschaftlichen Problem der Sammlung von personenbezogenen Daten und der Überwachung von Arbeitsabläufen. Aus Gründen des Datenschutzes sollten diese Daten nicht langfristig gesammelt, sondern baldmöglichst gelöscht werden. Sowohl die diesbezügliche Sensitivität als auch die entsprechende gesetzliche Regelungsdichte ist in Deutschland weitaus stärker ausgeprägt als etwa in den USA.

Hilfreich sind Prozeduren zur automatischen Auswertung solcher Daten, die ungewöhnliche Zustände und Ereignisse an die Verantwortlichen melden und ihnen (und den Überwachten) das lückenlose Durchlesen ersparen.

Zu den Überwachungsmaßnahmen gehören auch das Timeout für inaktive Terminals oder Kommunikationsverbindungen, ferner Tastatursperren, die nur mit einem Paßwort zu lösen sind, verbunden mit einer Abdunklung des Bildschirms.

Der Schwachpunkt bei jeder Überwachungsmaßnahme ist der Systemverwalter. Wichtige Daten können vor ihm nur durch Verschlüsselung verborgen werden; ansonsten sind organisatorische Maßnahmen wie das Vieraugenprinzip zur Überwachung unumgänglich. Vor allem muß er an der Manipulation von Überwachungsdateien gehindert werden.

3. Sicherheit von Datenbanken

Eine Datenbank ist ein spezielles Datenobjekt mit einem typischen Satz an Zugriffoperationen. Eine Datenbank hat als Datenobjekt einige besondere Merkmale:

- Sie enthält besonders viele Informationen, ist also ein lohnendes Angriffsobjekt.
- Die Daten sind oft sehr fein granuliert, d.h., Zugriffsrechte beziehen sich manchmal auf einzelne Felder in einzelnen Datensätzen.
- Der Benutzerkreis ist oft sehr groß.
- Durch die Verknüpfung von Informationen aus verschiedenen Datenbanken (dem sogenannten Abgleich) lassen sich oft Schlüsse ziehen, die den Datenschutz verletzen (unzulässige Inferenzen durch zulässige Datenzugriffe).

3.1. Klassischer Zugriffsschutz

Typisch für Daten, die in einer Datenbank organisiert sind, ist der „inhaltsgesteuerte Zugriff“ - die physische Struktur der Daten muß dem Anwender oder Anwendungsprogramm nicht bekannt sein, sie wird vom Datenverwaltungssystem („Data Base Management“) geregelt.

Die Daten müssen vor physischen Zugriffen und vor Zugriffen über das Betriebssystem geschützt sein. - das Datenbanksystem kann keinen besseren Schutz gewähren als das zugrundeliegende Betriebssystem. Ein Zugriff auf die Daten sollte nur über das Verwaltungssystem möglich sein.

In die Kategorie „klassischer Zugriffsschutz“ gehört auch der Vorschlag, die Datensätze oder zumindest ihren Identifikationsteil asymmetrisch durch Verfahren der Kryprographie zu verschlüsseln. Das erlaubt die Eingabe für einen größeren Personenkreis mit Hilfe des öffentliches Schlüssels; gegen Lesen sind die Daten - auch bei unsicheren Übertragungsweg - geschützt, außer vor autorisierten Personen, die den geheimen Schlüssel kennen.

3.2. Abgleich von Daten

Datenabgleich bedeutet, Informationen aus verschiedenen Quellen zusammenzuführen. Dies ist nicht immer erwünscht. Stellt man sich zum Beispiel Mitarbeiterdaten in einem Betrieb vor, so sind

- für den Geschäftsführer und ggfs. den Personalchef alle Daten zugänglich, keine Daten vertraulich,
- für einen Buchhalter nur lohn- und entgeltrelevante Daten zugänglich aber etwa gespeicherte weitere Informationen vertraulich,
- für den Pförtner nur Name und Zugangsberechtigung zum Werkstor zugänglich und alle weiteren Daten vertraulich.

Die Datenschutzgesetzgebung fordert die Löschung des Personenbezugs von Datensätzen (Anonymisierung), wo immer möglich. Es muß verhindert werden, daß vertrauliche Informationen aus zulässigen Zugriffen durch Interferenz hergeleitet und die Datensätze deanonymisiert werden können. Im allgemeinen enthält jedoch ein in einem betrieblichen Informationssystem gespeicherter Datensatz über einen Mitarbeiter noch genügend Merkmale eines Individuums, um dieses eindeutig zu identifizieren, selbst wenn er formal anonymisiert ist, also etwa Name, Anschrift und Geburtsdatum gelöscht sind.

3.3. Anonymisierung

3.3.1. Ziel der Anonymisierung von Daten

Für die betriebliche Forschung, die Marktforschung aber auch für administrative Planungszwecke bieten große Datensammlungen mit einer Vielzahl von personenbezogenen oder sachrelevanten Merkmalen zum Zwecke komplexer statischer Auswertungen erhebliche Möglichkeiten.

Der Datenschutz fordert, daß es unmöglich sein soll, die dazu benutzten Datensätze bestimmten Personen zuzuordnen. Datensätze sind um so besser geschützt, je geringer der Informationsgehalt der Überschneidungsmerkmale mit dem potentiellen Zusatzwissen eines Angreifers („Herr Mustermann ist Mitarbeiter der Einkaufsabteilung, ist verheiratet, hat zwei Kinder, von denen eines an Leukämie leidet, was größere Fehlzeiten bedingt“) ist.

3.3.2. Verfahren der Datenanonymisierung

Hier setzen die Verfahren zur Anonymisierung an: der Informationsgehalt des möglichen Überschneidungswissen wird absichtlich gemildert. Der Betrieb wird dadurch absichtlich „dumm“ gehalten. Dazu sind die folgenden Maßnahmen geeignet:

- Formale Anonymisierung: offensichtlich mehr oder weniger eindeutige Identifikationsmerkmale wie Name, Adresse, Telefonnummer werden weggelassen.
- Vergröberung der Merkmale etwa durch Rundung oder Klassenbildung; statt „Leipzig“ wird „Großstadt“ eingetragen, statt des Geburtsdatums „Alter 40-49“.
- Weglassen von einzelnen Datenfeldern mit extremen Merkmalsausprägungen wie „Größe 2.12 m“ oder „Beruf: Bilanzbuchhalter“.
- Störung der Daten durch absichtliche Fehler, etwa Addition einer zufälligen Größe oder zufällige Rundung.
- Stichprobenziehung: Statistische Prozeduren werden jeweils nur auf eine Stichprobe aus der Abfragemenge angewendet.
- Konstruktion synthetischer Datensätze, so daß die multivariable Verteilung möglichst wenig verändert wird:
- Austausch von Daten zwischen Datensätzen,
- Aggregation: Mittelbildung über jeweils 3 bis 5 Datensätze.

3.4. Die GRANT-Anweisung

Mit Hilfe der GRANT-Anweisung werden in SQL neue Benutzer in den Benutzerkatalog eingeführt. Gleichzeitig werden ihnen Befugnisse zugeteilt.

Die Anweisung zum Einführen neuer Benutzer lautet:

```
GRANT CONNECT
TO [Benutzer]...
IDENTIFIED BY [Kennwort]...
```

Beispiel: Zwei neue Benutzer sollen eingeführt werden, Hinz mit dem Paßwort „Ich_Darf“ und Kunz mit dem Paßwort „Ich_Auch“:

```
GRANT CONNECT
TO Hinz, Kunz
IDENTIFIED BY Ich_Darf, Ich_Auch
```

Die SQL-Synthax zur expliziten Zuweisung von Befugnissen lautet:

```
GRANT [ SELECT | INSERT | DELETE | UPDATE
{Spaltenname} | INDEX | ALTER | ALL ]
ON Tabellenspezifikation
TO [ [Benutzer]... | PUBLIC ]
{ WITH GRANT OPTION }
```

oder

```
GRANT [ DBA | RESOURCE ]
TO [Benutzer ]...
```

Beispiel: Gib Hinz die SELECT-Berechtigung für die Tabelle „Angestellte“:

```
GRANT SELECT
ON Angestellte
TO Hinz
```

4. Personenbezogener Datentransport

4.1. EMail

Elektronische Mitteilungssysteme (EMail) sind heute fester Bestandteil fast jeder Bürokommunikationssoftware. Die Nutzer dieser Systeme können im allgemeinen die Übertragungswege zu ihren Kommunikationspartnern nicht kontrollieren; daher ist die Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit der versandten Nachrichten ohne besondere Vorkehrungen nicht sichergestellt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat am 9./10. März 1995 eine Entschließung zum Datenschutz bei elektronischen Mitteilungssystemen verabschiedet. Hierin zeigen sie die Sicherheitsaspekte auf, die beim Einsatz dieser Systeme zu berücksichtigen sind. Insbesondere sollten elektronische Mitteilungssysteme zum Schutz der Vertraulichkeit der zu übertragenden Nachrichten und zur Feststellung der Authentizität der Absender sichere Verschlüsselungsverfahren beinhalten und die Möglichkeit der elektronischen Unterschrift.

Daneben sollten Sicherheitsmechanismen von Netzen wie z.B. geschlossene Benutzergruppen, Rufnummernidentifikation wie auch Möglichkeiten der Beweissicherung (Protokollierung von Sende-/Empfangsnachweisen) vorhanden sein.

In einer weiteren Entschließung vom 9. Mai 1996 haben die Datenschutzbeauftragten des Bundes und der Länder weitere Forderungen zur sicheren Übertragung elektronisch gespeicherter personenbezogener Daten aufgestellt. Hierbei und bei anderen Formen des Transportes von Daten fordern sie, Verschlüsselungsverfahren einzusetzen. Dies wird bei dem Transport von Daten auf Disketten, Magnetbändern und anderen Datenspeichern als auch bei der Nutzung von Netzen gefordert.

4.2. Die Chipkarte

Chipkartensysteme bestehen aus miniaturisierten IT-Komponenten (= Computern), die noch keine eigene Mensch-Maschine-Schnittstelle besitzen. Zur Interaktion bedarf es zwischengeschalteter technischer Geräte wie Kartenterminals. Die Risiken von Chipkarten entsprechen denen von tragbaren Rechnern.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder haben sich wiederholt mit Verfahrensentwicklungen befaßt, die den Einsatz einer Prozessorchipharte zugrundelegen. Im einzelnen fordern sie folgende Schutzmaßnahmen:

- Ausstattung des Kartenkörpers mit fälschungssicheren Authentifizierungsmerkmalen wie z.B. Unterschrift, Foto, Hologramm,
- Steuerung der Zugriffs- und Nutzungsberechtigungen durch die Chipkarte selbst und nicht durch andere am Interaktionsprozeß beteiligte Systeme,
- Realisierung aktiver und passiver Sicherheitsmechanismen gegen eine unbefugte Analyse der Chipinhalte sowie der chipintegrierten Sicherheitsfunktionen,
- Benutzung allgemein anerkannter veröffentlichter Algorithmen für Verschlüsselungs- und Signatur-Funktionen sowie zur Generierung von Zufallszahlen,
- Sicherung der Kommunikation zwischen der Chipkarte, dem Kartenterminal und dem gegebenenfalls im Hintergrund wirkenden System durch kryptographische Maßnahmen.
- Daneben sollten Chipkarteninhaber die Möglichkeit haben, auf neutralen, zertifizierten Systemumgebungen Dateiinhalte und Funktionalitäten ihrer Chipkarte einzusehen. Das gesamte System ist zu dokumentieren und sollte ein vorgeschriebenes Mindestschutzniveau besitzen.

5. Checklisten zum Datenschutz

5.1. Anforderungen und Bestandsaufnahme

Checkliste Anforderungsdefinition:

Leistungsanforderungen an die Datenverarbeitung

- Welche Anwendungen werden eingesetzt oder sollen eingesetzt werden?
- Was wird von der Arbeitsgeschwindigkeit gefordert oder erwartet?
- Welcher Komfort soll dem Benutzer geboten werden?
- Welche Einschränkungen müssen sie hinnehmen?
- Zu welchen Zwecken werden Daten verarbeitet? (Verwaltung, geschäftliche Transaktionen, Forschung, ...)

Gesetzliche Schutzanforderungen

- Welche Gesetze enthalten für den Betrieb relevanante Regelungen?
- Welche vertraglichen Regelungen haben Einfluß auf den Datenschutz? (Datenverarbeitung für andere Firmen, eingesetzte kommerzielle Software, ...)
- Welche Auskunftspflichten bestehen?
- Welche Aufbewahrungspflichten bestehen?

Betriebliche Schutzanforderungen

- Welche Datenschutzregelungen liegen im Interesse des Betriebs?
- Welche betrieblichen Sicherheitsnormen gibt es?
- Welche materiellen Schäden können bei Verstößen entstehen?
- Welche Folgen haben Datenverluste?
- Wo ist das Prinzip der Verhältnismäßigkeit zu beachten?
- Kosten-Nutzen-Abwägungen?

Checkliste Bestandsaufnahme:

Datenverarbeitungskonzept

- Gibt es ein Datenmodell des Betriebs?
- Wo und wie sind die Benutzer spezifiziert?
- Wo und wie ist das Datenverarbeitungssystem spezifiziert?
- Welches sind die Perspektiven für die Weiterentwicklung des Datenverarbeitungssystems?

Systemkonfiguration

- Gibt es Zentral- oder Abteilungssysteme?
- Mit welcher Peripherie sind sie ausgestattet?
- Wie sieht eine Skizze der Systemkonfigurationen aus?
- Wird mit Arbeitsplatzrechnern (PCs, Workstations) gearbeitet?
- Wie sind diese ausgestattet? (Liste!)
- Existieren lokale Netze?
- Wie sieht eine Skizze der Netzkonfiguration aus?
- Existieren Anschlüsse an öffentliche Netze? Welche? Wo?

Daten und Ressourcen

- Welche personenbezogenen Daten werden verarbeitet?
- Welche Anonymisierungsmaßnahmen sind möglich?
- Welche Betriebsgeheimnisse oder schutzbedürftigen betriebsinternen Daten werden verarbeitet? (Dokumente, Pläne, Rechnungen,...)
- Welche Systemdaten sind schutzbedürftig?
- Welche Systemprogramme sind sicherheitskritisch?

- Welche personenbezogenen Daten fallen bei der Systemüberwachung an?
- Mitbestimmung durch Betriebs- oder Personalrat vorhanden?
- Welche Gefahren drohen den Daten?
- Wo ist die Ausspähung schon kritisch?
- Wo nur die Änderung?
- Welche fremden Daten werden (im Auftrag) verarbeitet?
- Welche „privaten" Daten von Mitarbeitern werden im System gespeichert? (z.B. wissenschaftliche Korrespondenz, Gutachten, Entwürfe,...)
- Was darf mit den Daten gemacht werden und was nicht?

Kommunikation

- Welcher betriebsinterne Kommunikationsbedarf soll durch Vernetzung befriedigt werden?
- Welcher externe Kommunikationsbedarf soll durch Fernanschlüsse befriedigt werden?

Benutzer

- Wer darf mit dem System arbeiten?
- Welche Benutzergruppen lassen sich abgrenzen?

Schwachstellenanalyse, Angriffspunkte

- Welche Sicherheitsverstöße sind in der Vergangenheit vorgekommen? (Viren, Hacker, Wirtschaftsspione, eigene Mitarbeiter,...)
- Wie wird ihre Wiederholung verhindert?
- Liegt eine Risikoanalyse für die eingesetzten Verfahren vor?
- Welche potentiellen Angreifer gibt es?
- Welche Motive können sie haben?
- Welchen Nutzen können sie aus Sicherheitsverstößen ziehen?
- Welchen Aufwand nehmen sie mutmaßlich in Kauf?
- Welche System- und Schwachstellenkenntnisse muß man ihnen unterstellen?
- Welche Gefahren drohen durch gezielte Ausspähung?
- Lohnt sich der Einsatz eines Tiger-Teams? Oder kann ein Mitarbeiter des Betriebs kompetent Penetrationstests durchführen?

5.2. Organisation

Checkliste Planung von Maßnahmen:

- Wie ist die Datensicherheit in das allgemeine Datenverarbeitungskonzept eingebunden?
- Welches Sicherheitsniveau wird angestrebt?
- Welches Restrisiko wird in Kauf genommen?
- Wie sieht die Berechtigungsmatrix aus?
- Wer ist zuständig für Sicherheitsmaßnahmen auf Hardwareebene?
- Wer hat Sachverstand?
- Wer ist zuständig für Sicherheitsmaßnahmen auf Softwareebene?
- Wer hat die nötigen Systemkenntnisse?
- Wer plant und definiert organisatorische Maßnahmen?
- Wer ist für die Katastrophenvorsorge zuständig?
- Welche Risiken lassen sich durch Spezialversicherungen abdecken?

Checkliste Personal:

- Wie ist das Personal organisiert?
- Wer hat welche Funktion?
- Stellenbeschreibungen? Dienstverträge?
- Wie werden Zuverlässigkeit und Kompetenz geprüft?
- Wie sind die Benutzergruppen organisiert?
- Wer leitet sie?
- Wie groß ist die Gefahr der Abwerbung durch Konkurrenzunternehmen?
- Welche Vorkehrungen sind zu treffen?
- Wie wird das Betriebsklima gepflegt?
- Einstellungs- und Entlassungspolitik? Sind Racheakte zu befürchten?
- Welche Interessenkonflikte bestehen zwischen Management und Personal?
- Konflikte und mögliche Auseinandersetzungen zwischen verschiedenen Mitarbeitergruppen?
- Welche Akzeptanzprobleme oder inneren Widerstände bestehen?
- Wie wird das Personal motiviert? (Vorbildwirkung, Ernstnehmen von Vorschriften, Arbeitserleichterung, Unterstützung, Respekt vor Persönlichkeitsrechten, Schulung, Vertrauen, Kommunikationsverhalten des Managements)
- Wird die Ergonomie genügend berücksichtigt?
- Welche Dienstvorschriften und Arbeitsanweisungen gibt es?
- Welche sollte es noch geben?
- Wie sind und werden Zuständigkeiten geregelt?
- Wer bedient welche Geräte?
- Wer sorgt für Ordnung im Geräteraum, im Archiv, ...?
- Wie ist der Reinigungsdienst organisiert?
- Einsatz von Fremdfirmen?
- Wer hat welche Zugangsberechtigungen?
- Welche Schlüssel?
- wer ist für die Dokumentation der Datenschutzmaßnahmen zuständig?
- Wer verfaßt den Datenschutzbericht?
- Wer hält sich über aktuelle Sicherheitsprobleme auf dem laufenden?

Checkliste Überwachung:

- Welche Überwachungssysteme werden eingesetzt?
- Wer ist für die Revision zuständig?
- Wird diese Funktion genügend objektiv ausgeübt?
- Wo ist das Vier- (oder Mehr-) Augenprinzip einzuführen?
- Wie werden Mitarbeiter von Fremdfirmen überwacht?
- Wie weit greifen Überwachungsmaßnahmen in Persönlichkeitsrechte ein?

Checkliste Benutzerkontrolle:

- Wer darf mit dem System arbeiten?
- Wer darf bestimmte Informationen lesen oder verändern?
- Warum muß eine bestimmte Operation ausgeführt werden?

- Wann darf eine bestimmte Operation ausgeführt werden?
- Wo darf eine bestimmte Operation ausgeführt werden?
- Wer darf einen Auftrag zu einer bestimmten Operation geben?
- Wer oder was verbirgt sich hinter einer Benutzerberechtigung?
  - Eine eindeutige Person,
  - ein Stellvertreter,
  - ein Funktionsträger,
  - eine Rolle?

Checkliste Auftragskontrolle:

- Welche Datenverarbeitungsaufträge werden ausgeführt oder sollen ausgeführt werden?
- Für welche Firmen oder Institutionen?
- Welche vertraglichen Regelungen gelten für die Aufträge?
- Welche besonderen Datenschutzmaßnahmen sind für die Aufträge nötig?
- Wer darf Aufträge annehmen?
- Wie werden Aufträge ausgeführt?
- Wie gelangen die zugehörigen Fremddaten ins System?

5.3. Datensicherung und Katastrophenschutz

Checkliste Katastrophenvorsorge:

- Wie werden folgende Risikofaktoren berücksichtigt: Feuer, Sturm, Erdbeben, Wasser (Regenwasser, Hochwasser,...), Schmutz, Störungen der Infrastruktur (Stromausfall, Klimaanlage), Bedienungsfehler, menschliches Versagen, Hardware- und Softwarefehler, Sabotage, Zerstörung, Vandalismus, Kriminalität, Mißbrauch, Einbruch, Diebstahl?
- Welche Gefahren lauern in der Umgebung der Gebäude?
- Wie sieht die Ausstattung und Umfeld der Räume aus?
- Feuersichere Baumateralien,
- Brandschutztüren,
- feuerhemmende Datentresore,
- Schutz vor Wasserschäden, etwa Rohrbrüchen in höheren Stockwerken,
- Sicherheit vor Hochwasser und anderen Naturkatastrophen,
- Meldesysteme für Rauch, Feuer, Wasser,
- Sprinkler und andere Feuerlöscheinrichtungen,
- Notausschalter?
- Welche Brandschutzmaßnahmen sind eingeführt oder einzuführen? Sichere Lagerung brennbarer Stoffe (auch Druckpapier und Datenträger), Rauchverbote, Schutz vor Kabelbränden?
- Wie steht es mit der Ausfallsicherheit der Geräte und der Notstromversorgung?
- Welche Richtlinien für Notfälle existieren?
- Wer ist in Notfällen zuständig?
- Existiert ein Krisenstab?
- Wer ist in Notfällen für Notmaßnahmen kompetent?

Checkliste Datensicherung:

- Wie soll nach einem Totalausfall ein lauffähiges Betriebssystem wiederhergestellt werden?
- Wie sollen nach einem Totalausfall alle Daten restauriert werden?
- Wie lange sollen gesicherte Daten aufbewahrt werden?
- Wie oft sollen Die Daten gesichert werden?
- Wie schnell soll der Zugriff auf gesicherte Daten sein?
- Wann sind vollständige Sicherungen durchzuführen?
- Wann reichen inkrementelle Sicherungen?
- Welche Daten brauchen überhaupt nicht gesichert zu werden?
- Wo werden die gesicherten Daten aufbewahrt?
- Gibt es eine Möglichkeit, Zwillingskopien der gesicherten Daten in einem anderen Gebäude aufzubewahren? (Mit möglichst unterschiedlichem Gefährdungsprofil bei Katastrophen)
- Wer führt die Datensicherung durch?

5.4. Physischer Schutz

Checkliste Baupläne:

- Gibt es Baupläne des Gebäudes?
- Wo liegen die Zugänge?
- Gibt es ungesicherte Zugänge?
- Fenster? Schächte?
- Wo gibt es Doppelböden oder abgehängte Decken?
- Wie sieht es darüber bzw. darunter aus?
- Wo befinden sich Verteilerschränke und Anschlußpunkte (auch momentan unbenutzte)?
- Wo sind Kabelschächte?
- Welche Kabel verlaufen in ihnen?
- Wo besteht aktive Brandgefahr?
- Mögliche Brandursachen?
- Wo besteht passive Brandgefahr?
- Wo liegen elektrische Leitungen?
- Wo liegen Wasserleitungen? Gasleitungen? Sonstige Versorgungsleistungen?

Checkliste Zugangskontrolle:

- Wie sind Gelände und Gebäude geschützt?
- Welche Sicherungsbereiche gibt es?
- Maschinenraum?
- Stromversorgungs-, Hausanschlußraum?
- Klimaanlagen-Raum?
- Datenarchiv?
- Operatorraum?
- Räume der Systemabteilungen?
- Räume für Benutzer und Benutzergruppen?
- Wie ist der Zugang zu den Sicherheitsbereichen geregelt?
- Schließanlagen und Schleusen für Sicherheitsbereiche?
- Türsicherung mit Schlüsselregelung oder Zugangskontrollsystem?
- Personalschleusen mit Ausweis- und Gesichtskontrolle?
- Schalter mit Sicherheitsglas, Durchreiche und Gegensprechanlage zur Datenträgerausgabe?

- Nebeneingänge?
- Welche Maßnahmen zur Objektsicherung sind nötig?
- Videoüberwachung?
- Sicherung durch Alarmanlage, besonders außerhalb der Dienstzeit?
- Einbruchssicheres Glas in den Fenstern der Sicherheitsbereiche?
- Stahltüren zu den Maschinenräumen?
- Sicherung von Zugangsmöglichkeiten zu Kellerräumen und benachbarten Geschossen?
- Zugangssicherung zu Mitarbeiterräumen?
- Wer hat Zugang zu den Sicherheitsbereichen?
- Können Zugangssperren in Notfällen von autorisierten Personen abgeschaltet werden?
- Wie ist der Zugang für Betriebsfremde geregelt? (Besucher, Wartungspersonal, Handwerker, Fremdfirmen,...)
- Wird über den Zugang zu den Sicherheitsbereichen Buch geführt?
- Wo ist das Vieraugenprinzip nötig?
- Wie läßt sich nachträglich ermitteln, wer wann Zugang hatte?
- Wie kann man diese Aufzeichnungen umgehen oder fälschen?

Checkliste Datenträgerkontrolle:

- Welche Datenträger werden verwendet?
- Disketten? Festplatten? CDs? Datenbänder? Datenkassetten? Papier? Sonstige?
- Wo werden Datenträger aufbewahrt?
- Wie ist der Zugang zu Datenträgerarchiven geschützt? Sicherheitsbereiche?
- Wer kann die Datenträger lesen?
- Wer darf das?
- Welche Ausrüstung braucht man dazu?
- Wie können die Datenträger kopiert werden?
- Wer kann das?
- Wer darf das?
- Bleiben unerwünschte Datenreste auf Datenträgern stehen?
- Wie werden sie gelöscht oder geschützt?
- Wer ist für die Aufbewahrung und Ausgabe von Datenträgern verantwortlich?
- Klare Definition der Befugnis zur Datenträgerverwaltung?
- Wer ist für die Bestandskontrolle der Datenträger verantwortlich?
- Wie ist die Abgangskontrolle für Datenträger geregelt?
- Ausgabe von Datenträgern nur an befugte Personen?
- Kontrollierte Löschung oder Vernichtung von Datenträgern?
- Abgabemöglichkeiten für zu vernichtende Druckerlisten, Reißwolf?
- Wie wird der Transport von Datenträgern kontrolliert?
- Verpackungs- und Versandvorschriften, z.B. Verwendung verschlossener Transportkoffer?
- Transport nur durch befugte Personen?
- Nutzung eines gesicherten Eingangs und von Schaltern und Schleusen für An- und Ablieferung?
- Verschlüsselungsvorschriften?

5.5. Hardware und Betriebssystem

Checkliste Hardware:

- Welche Aussagen macht der Hersteller zu Sicherheitsfragen?
- Wie wird der Hauptspeicher geschützt?
- Grenzregister? Speicherschutzschlüssel? Virtuelle Adressierung?
- Welche Zustände kennt die CPU?
- Wie werden die Übergänge kontrolliert?
- Wie gelangt man in den privilegierten Zustand?
- Wie sind Ein- und Ausgabemedien geschützt?
- Schreibschutz auf Bändern und Disketten?
- Sperre von Diskettenlaufwerken?
- Schutz von Festplattenlaufwerken?
- Tastatursperre und Bildschirmverdunkelung bei inaktiven Sitzungen?
- Timeout oder absichtliche Aktivierung der Sperre?
- Welche spezielle Sicherheitshardware auf dem Markt paßt ins System?
- Zugangskontrollsysteme mit Ausweislesern?
- Separate Rechner oder Prozessoren?
- Verschlüsselungs-Chips?

Checkliste Betriebssystem:

- Welche Aussagen macht der Hersteller zu Sicherheitsfragen?
- In welcher Programmiersprache ist das Betriebssystem erstellt?
- Wie vollständig ist das Betriebssystem dokumentiert?
- Gibt es offizielle Zertifikate über die Sicherheit?
- Wie werden die Benutzerbereiche beim Mehrbenutzerbetrieb getrennt?
- Überwachung des Ressourcenverbrauchs?
- Überwachung der Stapelverarbeitung?
- Automatische Löschung von Plattenbereichen und Bändern vor einem Besitzerwechsel?
- Ein System zur Datensicherung, das Zuordnungsfehler beim Restaurieren verhindert?
- Automatische Löschung von temporären Dateien?
- Werden Angriffsversuche auf Daten sowohl dem Systemverwalter als auch dem Besitzer gemeldet?
- Wie funktioniert die Kommunikation zwischen verschiedenen Prozessen?
- Wie werden Serviceprozesse erzeugt und gestartet?
- Welche Befugnisse hat der Systemverwalter?
- Welche Möglichkeiten hat der Systemverwalter?
- Wie wird er überwacht?
- Welche Sicherheitslücken im Betriebssystem sind bekannt?
- Welche Möglichkeiten gibt es, Schutzmaßnahmen zu umgehen, etwa durch Laden einer anderen Version des Betriebssystems?
- Wie wird die Paßwortpolitik vom Betriebssystem unterstützt?
- Braucht man hierfür Zusatzsoftware? Eigene Modifikationen?

- Welche Sicherheitsvorkehrungen gibt es bei besonderen Betriebszuständen? (Wartung, Notfälle, Systemabstürze,...)
- Zugangs- und Zugriffssperren bis zum vollständigen Wiederanlauf?
- Selbstprüfungsmechanismen beim Wiederanlauf?
- Kontrolle von Dumps?
- Wartungspersonal unter Aufsicht?

Checkliste Identifikation und Paßwörter:

- Welcher Zugangsschutz ist vorgegeben?
- Paßwörter?
- Erkennungsdialog? Abhörsicher?
- Magnetkarten?
- Chipkarten?
- Prüfung persönlicher Merkmale (Fingerabdruck, Netzhaut, Gesichtsprofil, ...)
- Bindung von Personen an bestimmte Terminals oder Adressen?
- Mit zusätzlichem physischen Zugangsschutz?
- Bleiben Paßwörter bei Eingabe automatisch unsichtbar?
- Kann ein Benutzer sein Paßwort selbst wählen und jederzeit ändern?
- Kann der Systemverwalter jedes Paßwort in einem Notfall ändern?
- Wird eine solche Änderung manipulationssicher dokumentiert?
- Kann er jeden Benutzer zu einer Änderung zwingen?
- Ist das Paßwortverzeichnis lesegeschützt?
- Werden Lesezugriffe protokolliert?
- Welche Maßnahmen sind bei Eingabe eines falschen Paßworts vorgesehen?
- Alarm an zentraler Stelle?
- Aufzeichnung im Sicherheitsprofil?
- Zeitsperre?
- Meldung an den betroffenen Benutzer bei der nächsten korrekten Anmeldung?
- Stillegung des Anschlusses und der Benutzer-Identität nach einigen Versuchen?
- Welche Vorschriften zur Wahl von Paßwörtern gibt es?
- Länge des Paßworts?
- Negativliste von Paßwörtern, die zu einfach sind?
- Umkehrungen oder Wiederholungen naheliegender Wörter?
- Verfallsdatum?
- Werden diese vom Betriebssystem automatisch geprüft?
- Müssen sich die Benutzer viele komplizierte Paßwörter gleichzeitig merken?
- Besteht die Notwendigkeit, irgendwelche Paßwörter in einer Benutzergruppe gemeinsam zu verwenden?
- Welche Vorkehrungen gibt es gegen eine Paßwortfalle?
- Welche Möglichkeiten hat ein Benutzer nach Erraten eines privilegierten Paßworts?

Weicher zusätzlicher Schutz besteht?

Checkliste Sicherheitsprotokolle:

- Wie werden die Anzeigen des Systemkonsole aufgezeichnet?
- Werden außergewöhnliche Betriebszustände entdeckt, gemeldet und aufgezeichnet?
- Welche Möglichkeiten gibt es, einzelne Benutzer gezielt zu überwachen?
- Wie werden Sicherheitsverstöße und privilegierte (sicherheitskritische) Operationen protokolliert?
- An- und Abmeldevorgänge?
- Dateizugriffe?
- Änderungen von Systemparametern?
- Änderungen von Sicherheitsdefinitionen?
- Wie wird der Betriebsmittelverbrauch protokolliert?
- Welche Prozesse erledigen die Aufzeichnungen?
- Wer kann sie beeinflussen?
- Welche Systemprivilegien haben oder brauchen sie?
- Was passiert bei einem Systemabsturz mit noch offenen Protokolldateien?
- Wer hat Zugang zu den Protokollen?
- Vieraugenprinzip?
- Werden Protokolle manipulationssicher ausgewertet?
- Welche Persönlichkeitsrechte der Mitarbeiter werden durch die Aufzeichnungen berührt?
- Mitbestimmung des Betriebsrats oder Personalrats?
- Wie lange werden die Aufzeichnungen aufgehoben?
- Wie werden sie gelöscht?

Checkliste Viren und andere Schadprogramme:

- Welche Zugangsbeschränkungen verhindern das Einbringen unerwünschter Programme?
- Wird die eingeführte Software streng genug kontrolliert?
- Gibt es Quarantäne für Software unsicheren Ursprungs?
- Gibt es eine Möglichkeit, sie auf einem völlig isolierten System zu testen?
- Werden Originaldatenträger vor Installation mit Schreibschutz versehen, danach sicher verwahrt?
- Wird, wo immer möglich, mit Schreibschutz gearbeitet?
- Werden ungewöhnliche Ereignisse aufgezeichnet?
- Ungewöhnliche Aktivitäten im System sofort verfolgt?
- Sind geeignete Überwachungsprogramme vorhanden?
- Werden diese auch jeweils vor einer Datensicherung angewendet?
- Werden infizierte Programme sofort entfernt?
- Werden mehrere Generationen von gesicherten daten aufbewahrt und dabei auch Boot-Sektoren und Systemtabellen nicht vergessen?

5.6. Anwendungsprogramme

Checkliste Zugriffsrechte:

- Wie sieht die Berechtigungsmatrix aus? Welche Subjekte (Benutzer, Programme) dürfen auf welche Objekte (Programme, Daten) in welcher Weise zugreifen?
- Welche unterschiedlichen Zugriffsmöglichkeiten bietet das Betriebssystem?

- Gibt es einen „execute only“-Zugriff?
- Wie ist er abgesichert?
- Wie läßt sich die Zugriffsmatrix im System implementieren?
- Wo und wie sind die Zugriffsrechte abgelegt?
- Wer hat auf diese Daten Zugriff?
- Erlöschen Zugriffsrechte automatisch, wenn ein Subjekt oder Objekt ausgelöscht wird?
- Werden Daten und Zugriffsrechte von einem Server verwaltet?
- Welche Privilegien hat dieser, wenn er im Auftrag eines Benutzers arbeitet?
- Sind Sicherheitsstufen eingeführt oder ist ihre Einführung sinnvoll?
- Lassen sich Zugriffsrechte beim Restaurieren von Daten aus der Datensicherung umgehen?

Checkliste Selbsterstellte Software:

- Gibt es Programmierregeln für kritische Anwendungen?
- Welche Programmiersprachen und -werkzeuge werden verwendet?
- Welche besonderen Sicherheitslücken haben sie?
- Wie wird selbsterstellte Software getestet?
- Formale Verfahrensprüfung?
- Sachlogische Programmprüfung?
- Testdaten?
- Schnittstellenprüfung zwischen Programmteilen?
- Spezielle Prüfprogramme?
- Wer gibt selbsterstellte Software zur Anwendung frei?

Checkliste Fremdsoftware:

- Welche Fremdsoftware wird eingesetzt?
- Von welchen Herstellern oder Vertreibern?
- Wer entscheidet über Anschaffung und Eisatz von Fremdsoftware?
- Wer nimmt Anpassungen der Fremdprogramme vor? („Custmizing“)
- Welche Möglichkeiten zur Meldung von Fehlern und Problemen bietet der Hersteller oder Vertreiber? („Hotline“)
- Wie wird die Fremdsoftware gewartet?
- Wie schnell werden Fehler behoben?

Checkliste Anwendungskontrolle:

- Sind die Verfahrensabläufe für kritische Anwendungen ausreichend dokumentiert?
- Gibt es Prüfregeln für kritische Anwendungen?

Checkliste Datenbanken:

- Siehe auch Checkliste Zugriffsrechte.
- Welche Daten werden in einer Datenbank gehalten?
- Wo ist die Datenbank lokalisiert?
- Großrechner mit virtuellem Server? Server als Station im Netz?
- Welches Datenbanksystem wird eingesetzt?
- Welche eigenen Sicherheitsfunktionen bietet es?
- Welche Benutzer-Oberfläche bietet es?
- Wie sicher ist diese?
- Wie ausbruchssicher?
- Welche Anfragen sind erlaubt oder gesperrt?
- Welche Möglichkeiten zum Datenabgleich gibt es?
- Wie werden Tracker-Angriffe behindert?

Checkliste Benutzer-Oberfläche:

- Bieten Betriebssystem oder Anwendungsprogramm eine ausbruchssichere Benutzer-Oberfläche?
- Lassen sich Benutzerprofile manipulationssicher einrichten?
- Wie werden Privilegien, Verbrauchsrechte, Kommunikationsmöglichkeiten und Zugang zu Anwendungsprogrammen gesichert?
- Welcher Schutz besteht nach Programmabstürzen oder Programmabbrüchen?
- Welche Auskünfte kann ein Benutzer über das System erfragen?

5.7. Netze

- Checkliste Kabel
- gibt es eine Skizze der Kabelwege?
- Wo befinden sich Verteilerschränke und Anschlußpunkte (auch unbenutzte)?
- Wo sind die Kabelschächte?
- Welche Kabel verlaufen in Ihnen?
- Welche Kabeltypen werden verwendet?
- Wie sind die vorgesehenen Kabel abhörbar?
- Was müßte ein Angreifer unternehmen, um vorhandene Kabel anzuzapfen?
- Wie würde er dabei entdeckt?
- Welche baulichen Maßnahmen sind zum physischen Schutz der Kabel notwendig?
- Welche elektromagnetische Abschirmung ist zum Schutz der Kabel notwendig?

Checkliste Knotenpunkte:

- Wie kann ein Angreifer Knotenpunkte abhören?
- Welche Geräte braucht er dazu?
- Was leisten Schnittstellentester?
- Wie kann ein Angreifer den Netzverkehr aktiv verfälschen?
- Wie gut sind die Installationsschränke physisch geschützt?

Checkliste Netzmanagement:

- Welche Daten kann ein Netzverwalter sehen?
- Welche kann er manipulieren?
- Wie reagiert das Netz auf Unterbrechungen, etwa bei Anzapfversuchen?
- Wie reagiert das Netz auf das (eventuell unbefugte) Einfügen neuer Stationen?
- Welche Möglichkeiten bietet das Abhören von Netzmanagementdaten etwa beim ‘download’ von Konfigurationsdaten auf Bridges und ähnliche Komponenten?
- Durch welche Manipulationen in den unteren Protokollschichten sind Sicherheitsmaßnahmen der oberen Schichten zu unterlaufen?
- Treten beim Hochfahren des Netzes Sicherheitslücken, etwa in Form von undefinierten Zuständen, auf?

- Enthalten die Übertragungsprotokolle verdeckte Datenkanäle, die vom Netzmanagement nicht erkennbar sind?
- Was passiert mit einseitig hängenden Verbindungen (=Absturz eines Kommunikationspartners)?

Checkliste Daten im Netz:

- Welche Kommunikationsbeziehungen umfassen zu schützende Daten?
- Sind kryptographische Maßnahmen unumgänglich?
- Sind Verbindungsdaten schützenswert? (im lokalen Netz in der Regel wohl nicht)

Checkliste Fernzugriffe:

- Welche Gefahren entstehen durch die Anbindung an Fernverkehrsnetzen?
- Werden Zugriffsmöglichkeiten auf Daten innerhalb des Betriebs eröffnet?
- Wer darf elektronische Post von außerhalb empfangen?
- Nach außerhalb senden?
- Sind Fernwartungsmaßnahmen vorgesehen?

Checkliste Normen und Standards:

- Sind Exemplare folgender Schriften vorhanden?
- IT-Sicherheitskriterien?
- IT-Evaluationshandbuch?
- IEEE 802.10?
- ANSI-SP3_Protokoll („Secure Data Network System“)?
- ISO 7498/2?
- Wie weit sind die Standards erfüllt?

6. Das sogenannte Orange Book

Dieses Werk wnthält Sicherheitskriterien für PC-Rechner, die von „A“ (sehr hoch) bis „D“ (sehr niedrig) klassifiziert werden. Die verschiedene Sicherheitskriterien sind:

D Es werden keine besonderen Sicherheitsanforderungen gestellt. Beispiel: DOS-PC in einem frei zugänglichen Raum

C_1 System verlangt eine Anmeldung mit Name und Kennwort. Beispiel: normales UNIX-System.

C_2 System erfüllt die Anforderungen von C_1; zusätzlich müssen sicherheitsrelevante Ereignisse mitprotokolliert werden. Sicherheitsrelevante Ereignisse sind beispielsweise:

- Anmeldung bzw. Abmeldung von Anwendern
- Dateizugriffe
- IPC (=Inter-Process-Communication)-Aufrufe, z.B. in Unix:
  - shared memory
  - message queues
  - semaphores
- Start und Ende von Prozessen
- Benutzung ausgewählter Systemaufrufe, z.B. Datei öffnen / schließen

Die Festlegung der Zugriffsrechte erfolgt in der Sicherheitsstufe C durch den Anwender, in den Sicherheitsstufen B wird der Zugriffschutz durch einen Systemverantwortlichen festgelegt.

B_1 Das System erfüllt die Kriterien von C_2; zusätzlich legt das System genau fest, welcher Anwender auf welche Objekte zugreifen darf.

B_2 Das System erfüllt die Kriterien von B_1; Die Konfiguration des Systems wird gemäß sicherheitspolitischer Aspekte überprüft. Änderungen in der Konfiguration müssen lückenlos dokumentiert werden.

B_3 System erfüllt die Kriterien von B_2; Sicherheitsbeauftragte mit speziellen Rechten besitzen Kennungen. Das gesamte Sicherheitssystem ist modular aufgebaut.

A System erfüllt die Kriterien von B_1. Die Sicherheit des Systems muß formal, d.h. mit den Mitteln der theoretischen Informatik (im allgemeinen der Mathematik) bewiesen werden.

Die Stufen A und B finden hauptsächlich im militärischen Bereich Verwendung, normaler, geschäftlicher Bereich benutzt in der Regel UNIX. Lunux oder auf Windows NT basierende Systeme. UNIX und seine Derivate sowie Windows 2000 erfüllen C_1. C_2 kann durch zusätzliche Tools erreicht werden.