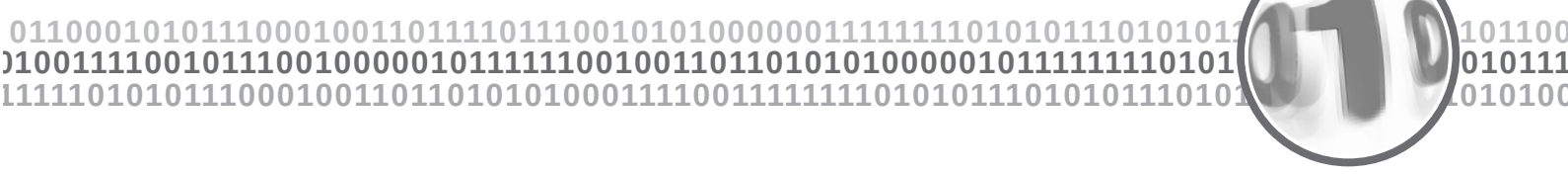
backUP

MAGAZIN FÜR IT-SICHERHEIT

IT-Sicherheitskonzepte

Planung • Erstellung • Umsetzung

Der Landesbeauftragte für den Datenschutz Schleswig-Holstein



HERAUSGEBER

Der Landesbeauftragte für den Datenschutz Schleswig-Holstein

Postfach 3607
24100 Kiel

Ansprechpartner: Heiko Behrendt

Telefon: 0431/988-1212
Telefax: 0431/988-1223
E-mail: LDSH@netzservice.de
Homepage: http://www.schleswig-holstein.datenschutz.de

VORWORT

IT-Sicherheitskonzepte
Planung, Erstellung und Umsetzung

Der Landesbeauftragte für den Datenschutz

Liebe Leserinnen, liebe Leser!
Die Erörterung datenschutzrechtlicher und sicherheitstechnischer Problemstellungen zwischen den datenverarbeitenden Stellen im Lande und dem Landesbeauftragten für den Datenschutz haben in der Vergangenheit auf drei Ebenen stattgefunden,

- anläßlich der Kontrollen,
- aufgrund von Beratungsersuchen und
- im Rahmen der Kurse, Seminare und Workshops der DATENSCHUTZAKADEMIE SCHLESWIG-HOLSTEIN.

Auf diese Weise konnten meine Mitarbeiter und ich Kontakte zu einer großen Zahl von datenverarbeitenden Stellen aufbauen. Häufig wurde dabei der Wunsch geäußert, die datenschutzrechtlichen und sicherheitstechnischen Informationen in praxisgerechte „Handlungsanweisungen“ umzusetzen. Diese Anregung haben wir gerne aufgegriffen.
Für die ausführende (IT-Betreuer) und die verantwortliche (Abteilungs, Amts- bzw. Büroleiter) Ebene geben wir zu aktuellen Themenbereichen ***backUP*-Magazine für die IT-Sicherheit** heraus, die dazu beitragen sollen, die Umsetzung der Gesetze, Verordnungen und Richtlinien zu vereinfachen.

***backUP*-Magazine** werden in unregelmäßigen Abständen erscheinen und unentgeltlich zur Verfügung gestellt. Sie sind Teil unserer Konzeption des *neuen* Datenschutzes, der neben der Kontrolltätigkeit vor allem auf Beratung und Service setzt. Die Dynamik der hard- und softwaretechnischen Veränderungen im Bereich der automatisierten Datenverarbeitung wird es mit sich bringen, daß die ***backUP*-Magazine** schon nach kurzer Zeit aktualisiert werden müssen. Für diesbezügliche Anregungen sowie für generelle Verbesserungsvorschläge sind wir dankbar.

Kiel, im August 1999
Dr. Helmut Bäumler

INHALT

1 GRUNDLAGEN

In diesem Kapitel erfahren Sie,

- wie ***backUP*** zu benutzen ist,
- welche Rechtsgrundlagen zu beachten sind,
- welche Bedeutung IT-Konzepte haben,
- welche Voraussetzungen für den IT-Bereich erforderlich sind.

1.1 Einleitung

Dieses ***backUP*-Magazin** zeigt praxisnah mit vielen Beispielen den Handlungs- und Regelungsbedarf auf, der entsteht, wenn IT-Systeme für die Verarbeitung personenbezogener Daten eingesetzt werden. Es soll die Leitungsebene (Abteilungsleiter, Dezernent, Referent, Fachbereichsleiter, Amtsleiter etc.) in die Lage versetzen, ein auf die organisatorischen Verhältnisse ihres Bereiches abgestimmtes **Sicherheitskonzept** zu erstellen. Das Magazin kann auch dazu benutzt werden, ein vorhandenes Sicherheitskonzept bezüglich des Aufbaus und der Regelungstiefe zu überprüfen.

1.2 Rechtsgrundlagen der Datenverarbeitung

Für die Verarbeitung personenbezogener Daten gelten die bereichsspezifischen landes- und bundesrechtlichen Vorschriften, die einschlägigen Vorschriften des Landesverwaltungsgesetzes und ggf. vertraglich vereinbarte Regelungen. Ergänzend sind die Bestimmungen des LDSG und der DSVO zu beachten. Die Verpflichtung zur Erstellung von Sicherheitskonzepten ergibt sich aus § 7 Abs. 1 LDSG i.V.m. § 8 der DSVO.

§ 8 Abs. 1 DSVO

*„Aufgrund der nach § 7 Abs. 1 und 2 LDSG zu treffenden technischen und organisatorischen Maßnahmen und der Sicherheitsanforderungen nach § 9 DSVO hat die datenverarbeitende Stelle für **alle automatisierten Verfahren**, die der Verarbeitung **personenbezogener Daten** dienen, darzustellen, welche Schutzmaßnahmen unter Berücksichtigung der tatsächlichen örtlichen und personellen Gegebenheiten getroffen wurden.“*

1.3 IT-Konzepte als Grundlage für Sicherheitskonzepte

Als Grundlage für die Festlegung von Schutz- bzw. Sicherheitsmaßnahmen dienen sogenannte Nutzungs- oder informationstechnische (IT-) Konzepte. In bezug auf die automatisierte Datenverarbeitung werden in ihnen u.a.

- die aufbau- und ablauforganisatorischen Gegebenheiten,
- interne Vorschriften (z.B. Allgemeine Dienstanweisungen),
- der Ist- und Soll-Bestand der Hardware- und Software,
- die Netzwerktopologie,
- die eingesetzten Fachverfahren sowie
- die Planungen bzw. die Anforderungen in bevorstehender Zeit

ausführlich beschrieben.

Mit der Erstellung von IT-Konzepten legt die Leitungsebene **Strukturen** für die Einführung und den Betrieb ihrer IT-Systeme fest. In diesem Stadium können bereits aufbau- und ablauforganisatorische Zusammenhänge sowie Risiken oder Angriffsmöglichkeiten lokalisiert werden.

Sofern kein IT-Konzept vorliegt, sind zusätzliche Arbeitsschritte für die Planung und Realisierung der erforderlichen und angemessenen Sicherheitsmaßnahmen unumgänglich. Diese werden im nächsten Kapitel ausführlich dargestellt.

1.4 Personelle Ausstattung des IT-Bereichs

Der IT-Bereich sollte für die Einführung und den Betrieb der IT-Systeme personell und fachlich ausreichend besetzt werden. Die Aufgaben der IT-Betreuer/Administratoren sollten in einer **detaillierten Beschreibung** dargestellt werden.

Musterbeispiel

Aufgabenzuordnung/-beschreibung Systemadministrator

- IT-Projektplanung
- Erstellung von IT-Konzepten
- Erarbeitung von Sicherheitsanforderungen
- Erstellung von IT-Dienstanweisungen
- Beratung der Fachabteilungen
- Beschaffung der Hard- und Software
- Installation und Konfiguration der Hard- und Software
- Überwachung des Systemverhaltens
- Durchführung der Datensicherung
- Benutzerverwaltung
- Fehlerbehandlung
- Protokollierung der durchgeführten administrativen Aufgaben
- Erstellung der Programm- und Verfahrensdokumentation
- Test und Freigabe der eingesetzten Verfahren
- Verwaltung der Software/Verfahren
- Schulung der Mitarbeiter
- .....

Mit der Erstellung einer Aufgabenbeschreibung wird besonders deutlich, wieviel **Know-how** für die Ausführung der administrativen Aufgaben erforderlich ist.
Die IT-Betreuer müssen in der Lage sein, die ihnen übertragenen Aufgaben **zuverlässig** zu bearbeiten. Ist dies nicht der Fall, befindet sich die Organisation in folgender Situation:

- Der Betrieb und der Einsatz der automatisierten Datenverarbeitung der Organisation kann nicht hinreichend sicher gestaltet werden.
- Die Schwachstellen bzw. Risiken lassen sich aufgrund fehlender technischer Kenntnisse nicht bestimmen.
- Das Sicherheitskonzept kann nicht selbst erstellt werden.

- Die Organisation benötigt Unterstützung von externen Dienstleistern.
- Die von externen Dienstleistern erarbeiteten Sicherheitsmaßnahmen können hinsichtlich ihrer Umsetzung und Wirksamkeit von der Organisation nur teilweise überprüft werden.

Selbst unter Zuhilfenahme externer Dienstleister wird die Organisation Gefahr laufen, die **Revisionsfähigkeit** der automatisierten Datenverarbeitung **selbständig** nicht gewährleisten zu können.

Es wird deshalb empfohlen, frühzeitig ein **Schulungsprogramm** für die IT-Betreuer zu entwickeln. Mit der Planung und Realisierung von Sicherheitsmaßnahmen und der Erstellung eines Sicherheitskonzeptes sollte erst dann begonnen werden, wenn die in der Organisation eingesetzten IT-Systeme weitestgehend in eigener Regie betreut werden können.

Merke

Die Planung und Realisierung von Sicherheitsmaßnahmen ist nur möglich, wenn die in der Organisation eingesetzten IT-Systeme auch von ihr beherrscht werden. Dies setzt voraus, daß die IT-Betreuer über ausreichendes Know-how verfügen.

Zusammenfassung

- Die Leitungsebene (Abteilungsleiter, Dezernent, Referent, Fachbereichsleiter, Amtsleiter etc.) soll in die Lage versetzt werden, ein auf die organisatorischen Verhältnisse ihres Bereiches abgestimmtes Sicherheitskonzept zu erstellen.
- Es sind dabei bereichsspezifische landes- und bundesrechtliche Vorschriften sowie die Bestimmungen des LDSG und der DSVO zu beachten.
- Als Grundlage für die Festlegung von Sicherheitsmaßnahmen dienen sogenannte Nutzungs- oder informationstechnische (IT-) Konzepte.
- Der IT-Bereich muß personell und fachlich ausreichend besetzt sein.

Notizen

2 PLANUNG DES SICHERHEITSKONZEPTES

In diesem Kapitel erfahren Sie,

- wie man methodisch richtig vorgeht,
- wer verantwortlich ist für die Definition von Sicherheitsmaßnahmen,
- welche Aktivitäten erforderlich sind, um die Schwachstellen zu analysieren,
- welche Gefährdungen grundsätzlich zu beachten sind,
- wie das Sicherheitsniveau festgelegt wird.

Voraussetzungen

- *Umfangreiche Kenntnisse über den Einsatz und den Betrieb der IT-Systeme*
- *Kenntnisse der aufbau- und ablauforganisatorischen Strukturen der Organisation*

2.1 Methodische Vorgehensweise

Eine zielgerichtete und durchdachte Vorgehensweise ist bei der Planung und Realisierung von Sicherheitsmaßnahmen von großer Wichtigkeit. Es sollte deshalb wie folgt vorgegangen werden:

Methodische Vorgehensweise

1. Klärung der Zuständigkeiten und Einrichtung einer Arbeitsgruppe vgl. Kapitel 2
2. Bestandsaufnahme der bereits eingesetzten und geplanten IT-Systeme
3. Feststellung der Angriffspunkte bzw. der Schwachstellen
4. Entwicklung einer IT-Sicherheitspolitik

5. Festlegung der Sicherheitsmaßnahmen in einem Sicherheitskonzept	vgl. Kapitel 3
6. Realisierung der IT-Sicherheitsmaßnahmen	vgl. Kapitel 4
7. Schulung und Sensibilisierung der Mitarbeiter	
8. Kontrolle der Einhaltung der IT-Sicherheitsmaßnahmen	vgl. Kapitel 5

2.2 Zuständigkeiten und Aufgabenzuordnung

Für die Durchführung der bevorstehenden Aufgaben sollte eine Arbeitsgruppe mit folgenden Personen gebildet werden:

- IT-Leiter
- IT-Betreuer, ggf. IT-Koordinatoren der Fachbereiche
- Datenschutzbeauftragter, sofern vorhanden
- Leiter der Organisationsabteilung bzw. Leiter des Hauptamtes

Die von der Arbeitsgruppe durchzuführenden Aufgaben sollten **gemeinsam** mit den Verantwortlichen für die Fachverfahren **(Leitungsebene)** abgestimmt werden. Sie tragen die Verantwortung für die in ihrem Zuständigkeitsbereich verarbeiteten Daten und wissen, welche **gesetzlichen Vorschriften (z.B. Berufs- oder Amtsgeheimnisse)** zu beachten sind.

In der Praxis stellt sich allerdings häufig das Problem, daß die Leitungsebene aufgrund unzureichender IT-Kenntnisse die **Risiken** der automatisierten Datenverarbeitung nicht abschätzen kann. Die Arbeitsgruppe (IT-Leiter, Datenschutzbeauftragter) hat dann die schwierige Aufgabe, die Leitungsebene über mögliche Risiken aufzuklären und über die Möglichkeiten ihrer Beseitigung zu beraten. Damit diesem wichtigen Aspekt ausreichende Beachtung zukommt, wird empfohlen, **Lagebesprechungen** in regelmäßigen Abständen durchzuführen.

Merke

Die Leitungsebene (Abteilungsleiter bzw. Fachbereichsleiter) trägt die Verantwortung für die in ihrem Bereich verarbeiteten Daten. Sie ist zuständig für die Festlegung des Sicherheitsniveaus.

Innerhalb der Arbeitsgruppe sollten zunächst die durchzuführenden Aufgaben definiert und anschließend den einzelnen Personen zugeordnet werden.

Musterbeispiel

• ***Funktion***	***Zuordnung***
IT-Leiter	A
IT-Betreuer	B
Datenschutzbeauftragter	C
Leiter der Organisationsabteilung bzw. Leiter des Hauptamtes	D
Leitungsebene bzw. Verfahrensverantwortliche für ihren Bereich	E

• ***Aufgabe***	***Zuordnung***
Leitungsebene regelmäßig informieren und beraten	A C D
Organisatorische Regelungen sammeln und auswerten	Alle
Netztopologie bzw. Konfigurationsplan erstellen	B C
Hard- und Softwarebestand aufnehmen	B C
Geräteverzeichnis erstellen	B C
Verfahren innerhalb der einzelnen Fachbereiche aufnehmen	B C
Verfahrensliste erstellen	B C
Zweck, Rechtmäßigkeit und Löschung der Verfahrensdaten prüfen	C D E
Benutzer- und Rechteverwaltung dokumentieren	B C E
Schwachstellen bzw. Risiken darstellen	Alle
Technische und organisatorische Sicherheitsmaßnahmen definieren	Alle
Sicherheitsniveau festlegen	C E
Sicherheitskonzept erstellen	A C
Technische Sicherheitsmaßnahmen umsetzen	A B
Organisatorische Sicherheitsmaßnahmen umsetzen	Alle
Verfahrensdokumentationen erstellen	B E
Mitarbeiter sensibilisieren und schulen	A C E
Sicherheitsmaßnahmen überprüfen/kontrollieren	A C E
.....	

Darüber hinaus wird empfohlen, die durchzuführenden Aufgaben unter Berücksichtigung der zeitlichen Komponente in einem **Projektplan** weiter zu spezifizieren. Es sollte dargelegt werden, **wann wer welche Aufgabe wie** umzusetzen hat. Zusätzlich sollten die erarbeiteten Ergebnisse festgehalten und in der Arbeitsgruppe besprochen werden, damit **rechtzeitig** auf neue, nicht vorhergesehene Gegebenheiten reagiert werden kann. Der Projektplan sollte in regelmäßigen Abständen auf den **tatsächlichen Stand** gebracht werden, so daß der Überblick nicht verloren geht.

Musterbeispiel

Projektplan

Termin	*Maßnahme/Arbeitsschritt*	*Person*	*Ergebnis*
22.05-30.05	Sammeln von Unterlagen und Informationen (Geräteverzeichnisse, Konfigurationsplan, Dienstanweisungen, besondere Vorschriften etc.) Welche Verfahren werden eingesetzt? Wie sind die IT-Systeme vernetzt? Gibt es externe Anbindungen?	*alle*	Unterlagen, soweit vorhanden gesammelt. Geräteverzeichnis nicht vorhanden. Konfigurationsplan nicht aktuell.
30.05-10.06	IT-Systeme begutachten, Rundgang durch die einzelnen Fachbereiche, Schwachstellen bzw. Risiken aufnehmen	*B C*	Schwachstellen wurden in gesonderter Liste aufgenommen.
11.06	Auswerten der Unterlagen und der Ergebnisse des Rundganges unter den Fragestellungen. Wo bestehen Risiken? Wo besteht ein erhöhtes Schutzbedürfnis?	*alle*	Ergebnisse wurden stichwortartig gesondert protokolliert.
20.06	Termine mit der Leitungsebene für die Lagebesprechung abstimmen.	*A*	
1.07-25.07	Durchführung der Besprechungen mit der Leitungsebene (beraten, sensibilisieren und Schutzbedürfnis feststellen).	*alle*	
26.07	Festlegung der Sicherheitsmaßnahmen mit Hilfe von Checklisten	*alle*	
27.07-30.08	Erstellung eines Sicherheitskonzeptentwurfs	*A C*	
30.08	Beratung und Anpassung (Optimierung) des Entwurfs	*alle*	
10.09	Übergabe des optimierten Sicherheitskonzeptentwurfs an die Leitungsebene zur Kenntnisnahme	*A C*	
25.09	Beschlußfassung	*E*	
01.10-31.12	Technische und organisatorische Umsetzung der im Sicherheitskonzept festgelegten Maßnahmen	*alle*	Hierfür ist ggf. ein neuer Projektplan erforderlich.

2.3 Erfassung der automatisierten Arbeitsabläufe

Um Sicherheitsmaßnahmen in einem Sicherheitskonzept festlegen zu können, sollten zunächst **detaillierte** Informationen über

- die aufbau- und ablauforganisatorischen Zusammenhänge,
- den Einsatz der Hard- und Software,
- die interne Netztopologie der Organisation sowie
- die verarbeiteten Daten

erfaßt werden.

Mit einer **Bestandsaufnahme** soll erreicht werden, daß **alle** für die Festlegung von Sicherheitsmaßnahmen erforderlichen **Sachverhalte aufgenommen** und keine Informationen übersehen werden. Sofern ein aktuelles IT-Konzept vorliegt, können daraus bereits wichtige Angaben über den IT-Einsatz der Organisation entnommen werden, so daß sich der Umfang der Bestandsaufnahme erheblich reduziert. Entspricht das IT-Konzept jedoch nicht mehr den tatsächlichen Verhältnissen, so sollte eine Bestandsaufnahme des IT-Einsatzes in allen Bereichen der Organisation durchgeführt werden.
Zur Unterstützung sollte bei der Durchführung der Bestandsaufnahme die in der Anlage aufgeführte **Checkliste** herangezogen werden.

Arbeitsschritte für die Durchführung der Bestandsaufnahme

- Personen für die Durchführung der Bestandsaufnahme bestimmen.
- Leitungsebene bzw. Abteilungsleiter über die geplanten Arbeitsschritte informieren, ggf. Termine für die Bestandsaufnahme vereinbaren.
- Akte für die Informationssammlung anlegen.
- Gesonderte Liste für die festgestellten Schwachstellen führen.
- Interne Regelungen (Geschäftsverteilungsplan, Dienstanweisungen) sammeln und auswerten.
- Zuständigkeiten innerhalb der Organisation prüfen.
- Organisationsbereiche auf Einhaltung besonderer Vorschriften (Amtsgeheimnisse, Geheimschutzordnung etc.) kontrollieren.
- Auswertung der Regelungen in bezug auf organisatorische und technische Schwachstellen.
- Sammeln, Sortieren und Auswerten von verfahrensbezogenen Unterlagen.

- Begutachtung der örtlichen Gegebenheiten in bezug auf
    - Arbeitsstationen,
    - Server,
    - Netzwerkkomponenten,
    - sonstige IT-Systeme.
- Aufnahme der bei der Begutachtung der IT-Systeme festgestellten Schwachstellen.
- Erstellung und Auswertung folgender Übersichten:
    - Geräteverzeichnis,
    - Hard- und Softwarebestandslisten,
    - Fachverfahrensliste,
    - Benutzer- und Rechteverwaltung,
    - Gebäude- und Verkabelungsplan,
    - Konfigurationsübersichten der eingesetzten IT-Systeme
- Prüfung der verfahrensbezogenen Datenverwaltung und Kommunikationswege.
- Überprüfung der von den IT-Betreuern durchgeführten Aufgaben.

Die Konfiguration der IT-Systeme sollte sorgfältig ermittelt werden. Ein **Konfigurationsplan** gibt in der Regel Auskunft über die Zusammensetzung der IT-Systeme. Wichtig ist, daß der Weg der Datenkommunikation zwischen den einzelnen IT-Systemen erkennbar ist. Somit läßt sich feststellen, auf welchen IT-Systemen Daten verarbeitet werden.

Darüber hinaus sollten Informationen über die technische Zusammensetzung der einzelnen IT-Systeme vorliegen. In einem **Geräteverzeichnis** sind meist folgende für die Festlegung von Sicherheitsmaßnahmen wichtige Angaben über die Komponenten dokumentiert:

Musterbeispiel

Geräteverzeichnis			
Abteilung	*Personal*	**Betriebssystem**	*MS-Windows 98*
Standort	*Raum 305*		
IT-System/Typ	*PC-Pentium 333 MHz*	**Standardsoftware**	*MS-Office-Paket*
Monitor	*Philips 17“*		
Drucker	*HP-Laserjet 5*		
Modem	-	**Fachverfahren**	*Lohnabrechnung*
Festplatte	*2 GB*		*Personalverwaltung*
CD-ROM	*24-fach*		
Diskettenlaufwerk	*3,5“*		
Sonstiges			

Insbesondere in größeren Organisationen ist der Einsatz von Hard- und Software sehr vielfältig. Um einen umfassenden Überblick zu bekommen, macht es Sinn, die in den Geräteverzeichnissen (sofern vorhanden) aufgeführten Komponenten zusammenzufassen. Die Erfassung der Daten kann natürlich auch in automatisierter Form erfolgen.

Die Ermittlung der eingesetzten **Fachverfahren** ist von entscheidender Bedeutung, weil mit ihnen die **zu schützenden Daten** verarbeitet werden. Es ist jedoch nicht immer einfach, die Kriterien für die Definition eines Verfahrens festzulegen.
Z.B. stellt die Software MS-Excel (Tabellenkalkulation) oder MS-Access (Datenbankverwaltung) allein noch kein Verfahren dar. Erst die mit dieser Software verarbeiteten (personenbezogenen) Daten lassen ein Verfahren daraus werden. **Jedes Verfahren** sollte namentlich und fachbereichsbezogen notiert werden, so daß eine **anschauliche Liste der eingesetzten Verfahren** entsteht. Dabei sollten die Verfahren, die nicht personenbezogene Daten beinhalten, gleichermaßen mit berücksichtigt werden, weil von ihnen ebenso Gefahren ausgehen könnten.

Musterbeispiel

Fachbereich	*Name Fachverfahren*	*Version*
Personal	Textbearbeitung MS-Winword Lohnabrechnung Personalmanagementsystem PERMIS	7.0 2.3 1.3
Organisation	Textbearbeitung MS-Winword	7.0
.....		

Die einzelnen Verfahren sollten unter Berücksichtigung folgender Kriterien begutachtet werden:

- Zugriffsmöglichkeiten (Benutzer der Fachbereiche und IT-Betreuer)
- Datenhaltung (lokal oder zentral)
- Verfahrensdokumentation
- Tests und die Freigabe

Merke

Werden Arbeitsabläufe mit personenbezogenen Daten automatisiert verarbeitet, liegt ein Verfahren im Sinne des LDSG i.V.m. der DSVO vor. Bezüglich der Festlegung des Sicherheitsniveaus ist jedoch die gesamte automatisierte Datenverarbeitung der Organisation von Bedeutung.

Die **physikalische Vernetzung** der IT-Systeme (Netztopologie) ist von großer Wichtigkeit für die Festlegung des Sicherheitsniveaus. In kleinen Organisationen ist die Netztopologie überschaubar und Angriffspunkte können in diesem Fall relativ einfach lokalisiert werden.
Ist das Sicherheitskonzept für eine mittlere oder große Organisation zu erstellen, ist der Arbeitsaufwand für die Ermittlung der Angriffspunkte auf die Netzkomponenten erheblich größer.
Deshalb sind **in Abhängigkeit von der Größe der Organisation** folgende Bereiche zu untersuchen:

- Kabelwege
- Anschlußdosen
- Verteilerräume
- Aktive Komponenten
- Knotenpunkte
- externe Anbindungen

Detailinformationen über die o.a. Systemkomponenten ergeben sich aus

- dem Gebäude- und Verkabelungsplan,
- der IP-Adreßverwaltung,
- dem Verteiler- bzw. Patchplan,
- der Konfigurationsübersicht der Router und Hubs sowie
- aus Vereinbarungen mit externen Dienstleistern in Bezug auf vorhandene Netzanschlüsse.

Wie bei der Bestandsaufnahme der Hard- und Software ist es auch hier ratsam, die einzelnen Komponenten **vor Ort aufzusuchen**, um deren Integration in die Organisation unter Sicherheitsaspekten besser beurteilen zu können. Wichtig ist, daß die Funktionsweise sowie die Konfiguration der einzelnen Komponenten analysiert wird.

Als **Datenkommunikation** einer Organisation kommen in der Regel folgende Bereiche in Betracht:

- Bereichsbezogene zentrale und/oder lokale Datenkommunikation
  Daten, die entweder auf den IT-Systemen der Fachabteilung oder auf einem zentralen IT-System abgelegt sind und ausschließlich in dem Zuständigkeitsbereich der Fachabteilung verbleiben, z.B. Daten des Fachverfahrens Personalverwaltung.

- Übergreifende Datenkommunikation
  Daten, die für mehrere Fachabteilungen im Zugriff stehen und den Zuständigkeitsbereich verlassen, z.B. Daten der Textbearbeitung oder interne E-Mails.

- Zugriff auf allgemeine interne Datenbestände
  Daten, die in der Regel nicht personenbezogen sind und allen Fachabteilungen zentral zur Verfügung gestellt werden, z.B. Rechtssammlungen, interne Informationen (Intranet).

- Anbindung von Außenstellen
  Daten, die zwischen der Organisation und einer zugehörigen Außenstelle ausgetauscht werden. Die Datenkommunikation erfolgt in der Regel über ein Gateway auf direktem Wege, so daß nur die eingestellten Verbindungen möglich sind.

- Internetnutzung
  Daten, die über die Dienste des Internets (E-Mail, WWW, Dateitransfer FTP) ausgetauscht werden. Diese Datenkommunikation kann über einen Einzelplatz-PC oder über das interne Netz der Organisation realisiert worden sein.

Die **Datenkommunikationswege** stehen in Abhängigkeit mit der Netztopologie der Organisation. Über das Fachverfahren sollten die Kommunikationswege und die Speicherungsorte der Anwendungen und der mit ihnen verarbeiteten Daten festgestellt werden. Von großer Bedeutung sind dabei die Übergänge in „fremde“ Netze (Internet, Außenstellen). Es sollte analysiert werden, wie diese Übergänge technisch konfiguriert wurden und inwieweit Angriffspunkte auf das interne Netz bestehen.

Sofern **externe Dienstleister** die IT-Systeme der Organisation administrieren, sollte die Art und Weise der Durchführung der ihnen zugewiesenen Aufgaben untersucht werden. Dabei ist zu differenzieren, ob die Aufgaben vor Ort oder über Fernadministration durchgeführt werden. Diesbezügliche Vereinbarungen zwischen der Organisation und dem Dienstleister sollten überprüft werden.

2.4 Schwachstellen bzw. Risiken

Die in der Bestandsaufnahme festgestellten Schwachstellen sollten mit Hilfe der **Checkliste** und des **Gefahrenkataloges** (siehe Anlage) aufgelistet werden. Bei der Festlegung des Sicherheitsniveaus kann dann mit der **„Mängelliste“** überprüft werden, inwieweit die Schwachstellen durch erforderliche und angemessene Sicherheitsmaßnahmen beseitigt werden können. Zu jeder Schwachstelle sollten von der Arbeitsgruppe technische und/oder organisatorische Vorschläge für ihre Beseitigung erarbeitet werden.

Musterbeispiel

Schwachstellen/Risiken	***Beseitigung/Sicherheitsmaßnahmen***
Keine Gefahrenanlage für Feuer und Wasser	Die Kosten für den Einbau stehen in keinem Verhältnis zum Nutzen.
Zu hohe Temperatur im Zentralrechnerraum	Einbau einer Klimaanlage
Fehlende Dienstanweisungen für Betrieb und Einsatz der IT-Systeme	Dienstanweisungen werden jeweils für die Benutzer- und Administrationsebene erstellt.
Keine Ersatzteile für zentrale IT-Systeme vorhanden	Ersatzteile werden für zentrale Komponenten beschafft.
Der Zutritt zu schutzbedürftigen Räumen ist möglich.	Der Zutritt wird über Schlüsselvergabe geregelt.
Unzureichende Dokumentation der Verkabelung	Die Dokumentation wird in der Dienstanweisung aufgenommen und nachgeholt.
Mangelhafte Kennzeichnung der Datenträger	Datenträger werden mit dem Organisations-kennzeichen versehen.
Fehlende Verfahrensdokumentation Unzureichendes Test- und Freigabeverfahren	Die Fachverfahren werden nach den Bestimmungen der DSVO dokumentiert und bei Veränderungen oder Neueinführung getestet und freigegeben.
Unzureichender Schutz der Bedieneroberfläche der Arbeitsstationen	Die Bedieneroberfläche wird auf das erforderliche Maß durch Einstellungen mit Hilfe der Systemrichtlinien eingeschränkt.
Fehlende oder unzureichende Schulung der Mitarbeiter und der IT-Betreuer	Es wird ein Schulungsprogramm für Mitarbeiter und IT-Betreuer erarbeitet.
Fehlerhafte Dokumentation der Benutzer und Rechteverwaltung	Die Benutzer sowie die ihnen zugewiesenen Rechte werden fachbereichsbezogen dokumentiert.
Unbeabsichtigtes Löschen von Programmen und/oder Daten	Die Rechte der Benutzer werden auf den IT-Systemen soweit eingeschränkt, daß ein Löschen von Programmen/Software nicht möglich ist.
Unstrukturierte Datenhaltung	Die Daten werden zentral gehalten und fachbereichsbezogen abgeschottet.
Keine Virenüberprüfung	Es wird ein Anti-Virenprogramm eingesetzt.
Offene Disketten- und CD-ROM-Laufwerke	Disketten- und CD-ROM-Laufwerke werden mit Sicherungsschlössern versehen.
.....	.....

2.5 Festlegung des IT-Sicherheitsniveaus

Nachdem über die Bestandsaufnahme alle erforderlichen Informationen ermittelt wurden, gilt es nun, das Sicherheitsniveau festzulegen. 100%ige Sicherheit ist praktisch nicht zu erreichen, 0% Sicherheit ist allerdings auch keine Alternative. Die in einer Organisation als ausreichend angesehene Sicherheit ergibt sich

- aus dem Wert der zu schützenden Daten,
- den Gefährdungen, denen diese Daten ausgesetzt sind sowie
- aus einer durch andere Faktoren bestimmten Risikobereitschaft.

Um das für die Organisation erforderliche und angemessene IT-Sicherheitsniveau festzustellen, sollten folgende Fragen beantwortet werden:

- Bestehen Regelungen, die den Schutz der Informationen **gesetzlich** vorschreiben?
- Werden mit den eingesetzten IT-Systemen Informationen verarbeitet, deren Vertraulichkeit **besonders** zu schützen ist?
- Welche Entscheidungen hängen von der **Richtigkeit, Aktualität und Verfügbarkeit** der Informationen ab?
- Gibt es Aufgaben der Organisation, die **nur** mit Unterstützung von IT-Systemen erledigt werden können?
- Gibt es **Massenaufgaben** in der Organisation, deren Erledigung nur mit IT-Einsatz möglich ist?

Nach Beantwortung dieser Fragen kann das Sicherheitsniveau in folgende Bereiche eingeordnet werden:

Hoch

- Der Schutz vertraulicher Informationen muß im besonderen Maße gewährleistet sein.
- Die Informationen müssen im höchsten Maß korrekt sein.
- Es können nur kurze Ausfallzeiten der automatisierten Datenverarbeitung toleriert werden.

Mittel

- Der Schutz von Informationen muß gewährleistet sein.
- Kleinere Fehler können toleriert werden.
- Fehler, die die Aufgabenerfüllung erheblich beeinträchtigen, müssen jedoch erkennbar oder vermeidbar sein.
- Längere Ausfallzeiten sind nicht zu tolerieren.

Niedrig

- Die Vertraulichkeit von Informationen ist nicht gefordert.
- Fehler können geduldet werden, solange sie die Erledigung der Aufgaben nicht völlig unmöglich machen.
- Längere Ausfallzeiten der IT-Systeme sind möglich.

Wichtig ist zu beachten, daß das gewählte IT-Sicherheitsniveau nur mit einem entsprechenden Aufwand zu erreichen ist. Das nachstehende Diagramm verdeutlicht, wieviel **Aufwand in Relation zu dem angestrebten IT-Sicherheitsniveau** zu betreiben ist. Der Aufwand bietet eine Orientierung für die personellen, zeitlichen und monetären Ressourcen, die zur Realisierung der IT-Sicherheitsziele notwendig sind.

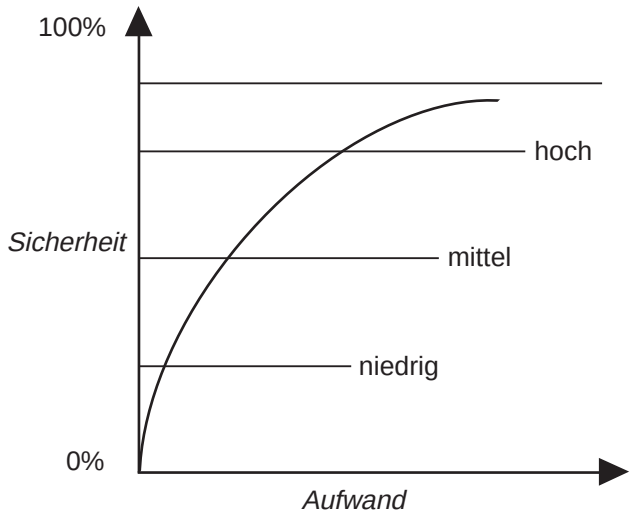


Diagramm IT-Sicherheit

Im Bereich der öffentlichen Verwaltung wird das Sicherheitsniveau aufgrund bereichsspezifischer gesetzlicher Vorschriften mindestens im **mittleren Bereich** der Skala angesiedelt werden müssen. Werden darüber hinaus Daten verarbeitet, die einem besonderen Amtsgeheimnis unterliegen, wie z.B. im Sozial- oder im Gesundheitsbereich, wird sich das erforderliche und angemessene Sicherheitsniveau im **oberen** Bereich befinden.
Ein hohes Sicherheitsniveau ist nur zu erreichen, wenn die IT-Betreuer über das entsprechende **Know-how** verfügen. Der Umkehrschluß, ein niedriges Sicherheitsniveau bedingt nur wenig Know-how, ist jedoch ein Trugschluß. Kann eine Organisation dauerhaft keine ausreichende Sicherheit gewährleisten, bewegt sie sich nicht mehr im rechtmäßigen Bereich.

Unter Umständen könnten gesetzliche Vorschriften eine Stillegung der automatisierten Datenverarbeitung erzwingen.

Es sollte vermieden werden, ein innerhalb der Organisation **stark abweichendes** Sicherheitsniveau zu realisieren. Dies führt im allgemeinen nicht zu weniger administrativen Aufwand.

Um das Sicherheitsniveau für die Beteiligten „greifbarer“ zu machen, wird empfohlen, mit Hilfe des in der Anlage dargestellten Maßnahmenkataloges **Mindestanforderungen** an die Sicherheit der automatisierten Datenverarbeitung unter Berücksichtigung der in der Bestandsaufnahme festgestellten Schwachstellen zu definieren.

Zusammenfassung

- Arbeitsgruppe für die Umsetzung der Aufgaben bilden.
- Die Verfahrensverantwortlichen über die Planung und Realisierung von Sicherheitsmaßnahmen informieren.
- Zuständigkeiten und Aufgaben innerhalb der Arbeitsgruppe festlegen.
- Projektplan aufstellen.
- Durchführung der Bestandsaufnahme planen.
- Checkliste für die zu überprüfenden Gegebenheiten verwenden.
- Aufbau- und ablauforganisatorische Regelungen sammeln und auswerten.
- Alle IT-Systeme innerhalb der Organisation begutachten und aufnehmen.
- Fachverfahren feststellen und fachbereichsbezogen zuordnen.
- Datenhaltung bzw. Datenspeicherungsorte ermitteln.
- Festgestellte Schwachstellen bzw. Risiken gesondert darstellen.
- Vorhandenes Sicherheitsniveau durch Auswertung der Informationen aus der Bestandsaufnahme einschätzen.
- Bereits getroffene Sicherheitsmaßnahmen über den Maßnahmenkatalog bestimmen.
- Schwachstellen der Reihenfolge nach bewerten, sortieren und gewichten.
- Anhand des Maßnahmenkataloges geeignete und angemessene Sicherheitsmaßnahmen auswählen. Dabei Änderungen in der Aufbau- und Ablauforganisation berücksichtigen.
- Schwachstellen, die nur mit verhältnismäßig hohem Aufwand zu beseitigen sind, zunächst zurückstellen.
- Sicherheitsniveau unter Berücksichtigung der zunächst hypothetisch ausgewählten Sicherheitsmaßnahmen erneut beurteilen.
- Ggf. Schritt für Schritt geeignete Sicherheitsmaßnahmen für zurückgestellte Schwachstellen bestimmen, um das Sicherheitsniveau weiter zu erhöhen.

- Offen gebliebene Schwachstellen bezüglich ihrer Risiken bewerten.
- Risikoübernahme durch die Leitungsebene abklären.

Notizen

3 ERSTELLUNG DES SICHERHEITSKONZEPTES

In diesem Kapitel erfahren Sie,

- wie ein Sicherheitskonzept erarbeitet wird,
- welche Struktur das Sicherheitskonzept enthält,
- wie die IT-Sicherheitsmaßnahmen zu Papier gebracht werden,
- wie verbleibende Sicherheitsrisiken durch eine Risikoanalyse in dem Sicherheitskonzept behandelt werden.

Voraussetzungen

- *Durchführung der Bestandsaufnahme*
- *Analyse der festgestellten Schwachstellen*
- *Festlegung des Sicherheitsniveaus*

3.1 Ausgangsbasis

In dem Sicherheitskonzept sollten alle zutreffenden Schutzmaßnahmen für **die in der Organisation eingesetzten Verfahren** unter Berücksichtigung der tatsächlichen örtlichen und personellen Gegebenheiten dargestellt werden. Damit definiert die Leitungsebene **verbindliche Regeln**, die von den IT-Betreuern umzusetzen sind.

In diesem Kapitel wird zunächst dargestellt, welche Form und Inhalte ein Sicherheitskonzept haben sollte. Da es keine Formvorschriften für die Erstellung eines Sicherheitskonzeptes gibt, sind natürlich auch alternative Darstellungsvarianten möglich.

3.2 Aufbau des Sicherheitskonzeptes

Nachfolgend werden nun **Hinweise und praktische Beispiele** für die Erstellung eines Sicherheitskonzeptes aufgeführt. Dabei ist zu beachten, daß weder die Hinweise noch die praktischen Beispiele **umfassend und abschließend** dargestellt werden können. Gleichwohl werden viele Anregungen vermittelt, die bei der Erstellung des Sicherheitskonzeptes behilflich sein können.

Das Sicherheitskonzept sollte in die Bereiche

- Zielrichtung,
- Allgemeiner Grundschutz,
- Arbeitsplatzebene,
- Zentralrechnerebene,
- Verfahren,
- Administration,
- Revision/Kontrolle,
- Notfallvorsorge,
- Schwachstellen/Risikoanalyse sowie
- Fortschreibung

gegliedert werden.

Größere Organisationen sollten für komplexe Verfahren, wie z.B. für die Anbindung des internen Netzes an das Internet, **separate** Sicherheitskonzepte erstellen. Dies hat u.a. den Vorteil, daß bei technischen Veränderungen die erforderlichen Anpassungen im Sicherheitskonzept besser erkannt werden. Obwohl die Sicherheitsproblematik bei kleinen Organisationen nicht weniger bedeutsam ist, kann ggf. von der o.a. Regelungstiefe abgewichen werden, weil aufgrund der überschaubaren Organisation Schwachstellen häufig **effizienter und pragmatischer** gelöst werden können.

3.3 Zielrichtung

Die Zielrichtung sollte Aufschluß darüber geben,

- welches Sicherheitsniveau angestrebt wurde,
- auf welcher Grundlage die Sicherheitsmaßnahmen festgelegt wurden,
- welche organisatorischen Bereiche einbezogen sind,
- welche technischen IT-Systeme aus welchen Gründen nicht einbezogen wurden und
- welche gesonderten Regelungen zu beachten sind.

Musterbeispiel

1. Zielrichtung

Bei der Organisation ..... wird für den Einsatz der IT-Systeme nach folgendem Sicherheitskonzept verfahren:

Gewährleistet werden soll

- die **Verfügbarkeit** der Systeme (z.B. Schutz vor Diebstahl, Zerstörung, Ausfallzeiten, Verlust von Datenträgern),
- die **Integrität** der Software und der Daten (z.B. Schutz vor vorsätzlicher oder fahrlässiger Verfälschung von Programmen, Manipulation von Dateien),
- die **Vertraulichkeit** von Daten (z.B. Schutz vor unbefugter Kenntnisnahme von Dateiinhalten).

In dem Sicherheitskonzept wird ein **hohes Sicherheitsniveau** zugrunde gelegt. Es bezieht sich auf alle in der Organisation technischen Systeme und Verfahrensabläufe, mit deren Hilfe **dienstliche Informationen** gespeichert und weiterverarbeitet werden können.

In dem Sicherheitskonzept werden ausschließlich **technische und organisatorische** Maßnahmen auf der Grundlage *der in der **Bestandsaufnahme** vom ..... ermittelten Informationen und des **IT -Konzeptes** vom .....* dargestellt.
Aus Gründen der Vereinfachung ist die Auswahl der Schutzmaßnahmen für die bei der Organisation ..... eingesetzten Verfahren **zusammenfassend** beschrieben worden. In den Verfahrensakten wird deshalb auf das Sicherheitskonzept verwiesen.
.....
.....

3.4 Allgemeiner Grundschutz

Beim Einsatz komplexer IT-Systeme sind i.d.R. Grundsatzentscheidungen zu treffen, die für die **gesamte** Organisation von Bedeutung sind. Hierunter fallen Regelungen über

- infrastrukturelle Vorkehrungen,
- den generellen Einsatz der IT-Systeme,
- die Betriebssicherheit der IT-Systeme,
- die Anbindung an externe Dienstleister,
- die Nutzung der Dienste im Internet,
- die Art und Weise der Datenhaltung,
- die Einrichtung von Benutzern und Zuweisung von Rechten sowie
- die Behandlung von externen Datenträgern und mobilen PC.

Sie sind **richtungsweisend** für die von der Organisation vertretende Sicherheitspolitik und geben Auskunft über den allgemeinen Grundschutz der Organisationsbereiche.

Musterbeispiel

2. Allgemeiner Grundschutz

2.1 Infrastruktur

- Für die zentralen IT-Systeme sind geeignete Räumlichkeiten bereitzustellen.
- Es ist im Zentralrechnerraum eine ausreichende Klimatisierung sicherzustellen.
- Es ist eine Gefahrenmeldeanlage zu installieren.
- Im Zentralrechnerraum sind die IT-Systeme an gesonderten Stromkreisen anzuschließen.
- Ein Handfeuerlöscher ist vorzusehen.
- Der Zutritt zu Netzwerkleitungen und -verteilern ist zu regeln.
- Fenster und Türen müssen abschließbar sein.
- .....

2.2 IT-Einsatz

- Alle IT-Systeme und externe Datenträger sind zu kennzeichnen.
- Die IT-Systeme sind zu inventarisieren.
- Es ist ein Geräteverzeichnis zu erstellen.
- Es ist ein Gebäude- und Verkabelungsplan herzustellen.
- .....

2.3 Betriebssicherheit

- Es sind die vom Hersteller geforderten Installations- und Betriebsvoraussetzungen, wie z.B. sicherer Stand und ausreichende Belüftung, zu schaffen.
- Es sind ausreichende Ersatzkomponenten vorzuhalten.
- Die Platten der Server sind zu spiegeln.
- Für die zentralen IT-Systeme ist eine Notstromversorgung vorzusehen.
- .....

2.4 Externe Dienstleister

- Die Übernahme administrativer Aufgaben durch externe Dienstleister ist vertraglich festzulegen.
- Die Durchführung der Aufgaben sind zu beschreiben.
- Ein Zugriff auf Verfahrensprogramme und Verfahrensdaten ist zu unterbinden.
- Die externen Dienstleister sind bei der Ausführung ihrer Tätigkeit zu überwachen. Über die Durchführung der administrativen Tätigkeiten sind vom Dienstleister Arbeitsprotokolle zu verlangen.
- Bei fernadministrativer Tätigkeit sind die durchzuführenden Aktivitäten vorher telefonisch zu besprechen.
- Die Modem-Verbindung ist nur für die Dauer der Administration zu aktivieren.
- .....

2.5 Internetnutzung

- Der Internetzugang darf nur von nicht am Netz angeschlossenen IT-Systemen (Einzelplatz-PC) realisiert werden.

- Die Nutzung der Internetdienste ist auf das WWW und E-Mail zu begrenzen.
- Die Einrichtung von Benutzerkennungen, E-Mail-Adressen und Postfächern ist einheitlich und gesondert zu regeln.
- Verfahrensbezogene Daten dürfen mit Ausnahme von E-Mails nicht auf Internet-IT-Systemen gespeichert werden.
- E-Mails sind grundsätzlich nur in verschlüsselter Form auszutauschen.
- Empfangene E-Mails sind nach Kenntnisnahme zu löschen.
- Eine Datenkommunikation über externe Datenträger auf vernetzte IT-Systeme ist nur mit Kenntnisnahme der Leitungsebene gestattet.
- .....

2.6 Datenhaltung

- Die Datenhaltung wird ausschließlich auf den Zentralrechnern vorgesehen.
- Die Speicherung verfahrensbezogener Daten auf den lokalen Festplatten der Arbeitsstationen ist zu unterbinden.
- Die eingesetzten Programme der Fachverfahren und die mit ihnen erzeugten Daten sind in separaten Verzeichnissen auf den Zentralrechnern zu verwalten.
- Für die Textbearbeitung ist eine der Organisation angepaßte Ablage zu erstellen.
- Sie ist vor Einrichtung oder Anpassung in Abstimmung mit der Leitungsebene zu dokumentieren.
- Das Prinzip der bereichsbezogenen Datenabschottung ist zu berücksichtigen.
- .....

2.7 Benutzer- und Rechteverwaltung

- Es ist eine bereichsbezogene Liste über PC-Benutzer und den ihnen zugewiesenen Rechten zu erstellen.
- Benutzer sind ausschließlich auf den Zentralrechnern einzurichten.
- Zur Vereinfachung der Rechtezuweisung sind Benutzergruppen zu bilden.
- Den Benutzern sind mit Zustimmung der Leitungsebene (Verfahrensverantwortliche) entsprechende Zugriffsrechte zu erteilen.
- Dateien und Verzeichnisse werden benutzerbezogen mit Lese-, Schreib- und Ausführungsrechten versehen.
- Die Benutzerrechte sind soweit einzuschränken, daß ausschließlich verfahrensbezogene Verzeichnisse genutzt werden können.
- .....

2.8 Externe Datenträger

- Die Datenträger der eingesetzten Betriebssysteme und der Anwendungssoftware sind unter Verschluß zu nehmen.
- Für die Datensicherung sind entsprechende Datenträger bereitzuhalten und in einem abschließbaren Behältnis zu verwahren.
- Informationsmedien, wie z.B. CDs, dürfen nur mit Absprache der Leitungsebene über die IT-Betreuer zur Verfügung gestellt werden.
- Externe Datenträger sind einer Virenprüfung zu unterziehen.
- Die Aussonderung von Datenträgern erfolgt über die IT-Betreuer.
- .....

2.9 Mobile PC

- Die Datenträger mobiler PC sind grundsätzlich zu verschlüsseln.
- Die Schlüsselverwaltung und die Zugangsberechtigungen sind mit Absprache der Leitungsebene zu vergeben und zu dokumentieren.
- Die Bereitstellung der auf den PC eingesetzten Verfahren ist von der Leitungsebene vor zugeben.
- Bei Rückgabe oder Aussonderung des PC sind die gespeicherten Datenbestände unter Anweisung der IT-Betreuer zu löschen.
- Der Datenaustausch zwischen den mobilen PC und dem vernetzten IT-Systemen erfolgt über die IT-Betreuer.
- Die Internetnutzung oder ein sonstiger externer Anschluß an öffentliche Netze ist nicht zulässig.
- .....

3.5 Arbeitsplatzebene

Unter der Arbeitsplatzebene ist die Arbeitsumgebung der Benutzer zu verstehen. Hier sollten alle Maßnahmen aufgeführt werden, die aus **Sichtweise des Mitarbeiters** von Bedeutung sind. Darunter fallen

- die Beachtung von allgemeinen und bereichsspezifischen Vorschriften,
- die Gestaltung der Arbeitsumgebung sowie
- die Nutzung der ihnen zur Verfügung gestellten IT-Systeme.

Musterbeispiel

3. Arbeitsplatzebene

3.1 Unterweisung

- Die Mitarbeiter sind aufgabenspezifisch zu schulen.
- Benutzerhandbücher sind auszugeben.
- Für die Benutzer ist eine Dienstanweisung zu erstellen, die u.a. die Zuständigkeiten, den Zugriff und die Befugnisse sowie den Umgang mit den IT-Systemen regelt.
- Die Benutzer sind auf die sicherheitsrelevanten Aspekte hinzuweisen.
- Es ist in regelmäßigen Abständen eine entsprechende Schulung durchzuführen.
- .....

3.2 Arbeitsumgebung

- Die IT-Systeme sind so zu plazieren, daß eine unbefugte Kenntnisnahme von dargestellten oder ausgedruckten Informationen durch Besucher ausgeschlossen wird.
- Bei Abwesenheit der Benutzer ist der Raum zu verschließen.
- IT-Systeme dürfen vom Benutzer nicht ohne Genehmigung der IT-Betreuer verändert oder transportiert werden.
- .....

3.3 Nutzung der IT-Systeme

- Die Anmeldung am System erfolgt über eine Benutzerkennung und das Paßwort.
- Es ist eine gesonderte Paßwortregelung zu erstellen.
- Die Bedieneroberfläche ist einheitlich zu gestalten.
- Eine Veränderung der Oberfläche durch Einspielung neuer Programme oder Aufruf nicht freigegebener Programme darf nicht möglich sein.
- Es dürfen nur die Anwendungen/Verfahren im Zugriff stehen, die für die eigentliche Aufgabenerfüllung erforderlich sind.
- Der Zugriff auf Daten anderer Bereiche ist über die eindeutige Zuweisung von Rechten abzusichern.
- Der Zugriff auf das Disketten- und CD-ROM-Laufwerk ist zu sperren.
- .....

3.6 Zentralrechnerebene

Zu der Zentralrechnerebene gehören die Zentralrechner, die Netzwerkkomponenten sowie die mit ihnen verbundenen Kommunikationssysteme. Hier sind für die Festlegung von Sicherheitsmaßnahmen folgende Bereiche zu berücksichtigen:

- Konfiguration der zentralen IT-Systeme
- Protokollierung von Systemaktivitäten
- Art und Weise der Durchführung der Datensicherung
- Management der einzelnen Netzwerkkomponenten

Musterbeispiel

4. Zentralrechnerebene

4.1 Konfiguration

- Die zentralen IT-Systeme sind soweit möglich einheitlich auszustatten.
- Die IT-Systeme sind gut zugänglich aufzubauen.
- Alle IT-Systeme sind unter Berücksichtigung ihrer Vernetzung in einem Konfigurationsplan graphisch darzustellen.
- Für die Konfiguration der Betriebssysteme sowie für die Vorgehensweise umfangreicher Systemaktivitäten sind Checklisten bzw. Arbeitsanweisungen zu erstellen.
- .....

4.2 Protokollierung

- Für jeden Zentralrechner ist eine Systemakte anzulegen.
- Auf den Zentralrechnern sind folgende Aktivitäten durch IT-Betreuer zu protokollieren:
    - Jede Veränderung von Dateien,
    - die Installation von Hard- und Software,
    - die Beseitigung von Fehlern und Störungen,
    - die Löschung von Daten,
    - die Durchführung der Datensicherung.

- Für die Aufzeichnung der Systemaktivitäten sind einheitliche Formblätter zu verwenden.
- Die vom Betriebssystem automatisiert erstellten Protokolle sind regelmäßig auszuwerten und in die Systemakte zu nehmen.
- .....

4.3 Datensicherung

- Die Datensicherung ist nach dem Fünftage-Generationen-Prinzip durchzuführen.
- Die gesamten Datenbestände der Zentralrechner sind täglich auf den entsprechenden Datenträgern zu sichern.
- Die Programme einschließlich der Betriebssysteme sind auf separaten Datenträgern nach jeder Veränderung zu sichern.
- Die Datensicherungsträger sind in einem abschließbaren Behältnis zu verwahren.
- Die Freitagssicherung ist im Schließfach der Hausbank auszulagern.
- Die Durchführung der Datensicherung ist in der Systemakte festzuhalten.
- .....

4.4 Netzwerkmanagement

- Die Netztopologie der Bereiche ist in einem Verkabelungsplan zu dokumentieren.
- Anschlußdosen sowie Patchfelder der Verteilerschränke sind sorgfältig zu beschriften.
- Verteilertechniken und Knotenpunkte sind graphisch darzustellen.
- Die Konfiguration aktiver Komponenten ist zu dokumentieren.
- Der Anschluß von IT-Systemen an das Netzwerk sowie Veränderungen an der Verkabelung sind ausschließlich von den IT-Betreuern durchzuführen.
- Das Abgreifen oder Ausspähen von Datenpaketen ist verboten.
- .....

3.7 Verfahren

Für die automatisierten Verfahren der Organisation sind Sicherheitsmaßnahmen festzulegen, die sich insbesondere auf die **Einführung und den Betrieb** der mit dem Verfahren eingesetzten **Software** beziehen. Es sind Maßnahmen zu ergreifen, die

- die Zuweisung von Benutzerrechten,
- die Verwaltung und Löschung der Daten,
- die Entwicklung von Anwendungen,
- die Zulässigkeit der Datenspeicherung,
- das Test- und Freigabeverfahren sowie
- die Dokumentation der Verfahren

regeln.

Musterbeispiel

5. Verfahren

- Die Funktionalität der in automatisierten Verfahren eingesetzten Software ist auf das erforderliche Maß zu beschränken.
- Die Speicherungsdauer sowie die Zuständigkeit für die Löschung der Daten ist zu regeln.
- Die Erstellung von Anwendungen z.B. über die Software MS-Excel oder MS-Access ist nur in Abstimmung mit der Leitungsebene zulässig.
- Die eingesetzten Verfahren sind von der entsprechenden Fachabteilung zu testen und von der Leitungsebene (Abteilungsleiter, Fachbereichsleiter, Amtsleiter etc.) freizugeben.
- Bei der Einspielung neuer Programmversionen ist von der Leitungsebene festzulegen, ob ein erneutes Test- und Freigabeverfahren durchzuführen ist.
- Jedes Verfahren ist nach folgenden Regeln zu dokumentieren:
    - Anlegen einer Verfahrensakte
    - Prüfung der Rechtsgrundlagen für die Speicherung der Daten
    - chronologische Sammlung aller verfahrensbezogenen Schriftstücke
    - Erstellung oder Anforderung einer Leistungsbeschreibung
    - Unterlagen über das Test- und Freigabeverfahren
    - Freigabeverfügung der Leitungsebene (Verfahrensverantwortlicher)

- Für die Durchführung der Tests sowie für die Erstellung der Dokumentation sind Checklisten bzw. Arbeitsanweisungen zu erstellen.
- Die Dokumentation wird von den IT-Betreuern geführt.
- .....

3.8 Administration

Die Administration der IT-Systeme ist unter sicherheitstechnischen Aspekten festzulegen. Es sind Maßnahmen zu ergreifen, die

- die Festlegung der Zuständigkeiten,
- die Zuweisung von Zugriffsberechtigungen sowie
- die Durchführung der administrativen Aufgaben

regeln.

Musterbeispiel

6. Administration

- Der Leiter der Organisation trägt die Verantwortung für den Einsatz und den Betrieb der IT-Systeme.
- Für die Aufgaben der Administration der IT-Systeme sind mindestens ein Mitarbeiter und eine Vertretungskraft einzurichten.
- Die Zuordnung der Aufgaben sowie die auszuführenden Systemarbeiten sind in einer Dienstanweisung für die IT-Betreuer festzuschreiben.
- Für die IT-Betreuer ist jährlich ein Schulungsprogramm aufzustellen.
- Die IT-Betreuer haben vollen Zugriff auf die Server und die Arbeitsstationen.
- Das Lesen, Kopieren oder Verändern von verfahrensbezogenen Dateien ist nur in Abstimmung mit der Leitungsebene zulässig.
- .....

3.9 Revision/Kontrolle

Um das festgelegte Sicherheitsniveau **dauerhaft** zu gewährleisten, muß sichergestellt sein, daß alle Maßnahmen so umgesetzt werden, wie es im Sicherheitskonzept beschrieben ist. Es sind deshalb in dem Sicherheitskonzept Regelungen mit aufzunehmen, die die Durchführung einer **Kontrolle** der vorgegebenen Sicherheitsmaßnahmen beschreiben.

Musterbeispiel

7. Revision/Kontrolle

- Die Zuständigkeit für die Überwachung der ordnungsgemäßen Benutzung der IT- Systeme liegt insgesamt bei dem Leiter der Organisation und für die Abteilungen/Bereiche bei der Leitungsebene (Verfahrensverantwortliche).
- Überwacht werden soll die Benutzer- und Administrationsebene auf die Einhaltung der in diesem Sicherheitskonzept festgelegten Sicherheitsmaßnahmen sowie der in den Dienstanweisungen festgeschriebenen Regelungen.
- Die Durchführung einer Überwachung wird vom Leiter der Organisation angewiesen. Die Personalvertretung ist entsprechend zu beteiligen.
- Das Ergebnis der Durchführung einer Überwachung ist schriftlich festzuhalten und der Leitungsebene zur Kenntnis zu geben.
- Bei der Feststellung von neuen Schwachstellen oder der Nichteinhaltung von Sicherheitsvorgaben ist eine Sitzung einzuberufen.
- .....

3.10 Notfallvorsorge

Bei einem Ausfall einzelner IT-Systeme sollten vorbeugend Sicherheitsmaßnahmen definiert werden, die vorwiegend Verhaltensregeln für die Benutzerebene und die Vorgehensweise der Beseitigung der Fehler oder Störungen beschreiben.

Musterbeispiel

8. Notfallvorsorge

- Für die Beseitigung von Fehlern oder Störungen der IT-Systeme sind die IT-Betreuer zuständig.
- Von den IT-Betreuern ist ein Notfallhandbuch bzw. ein Wiederanlaufplan über die häufigsten Störungen zu erstellen.
- Bei Ausfall zentraler IT-Systeme ist die Leitungsebene zu informieren.
- Für die Benutzerebene sind in der Dienstanweisung Verhaltensregeln aufzunehmen.
- Es sind im Bereich der Administration in regelmäßigen Abständen Notfallübungen durch zuführen.
- Es ist jährlich ein Ersatzbeschaffungsplan der eingesetzten IT-Systeme zu erstellen.
- .....

3.11 Schwachstellen/Risikoanalyse

Von besonderer Bedeutung sind die (bekannten) Schwachstellen bzw. Risiken, die **bewußt** nicht durch Sicherheitsmaßnahmen beseitigt wurden. Diese Schwachstellen sind in Form einer **Risikoanalyse** darzustellen. Die Risikoanalyse sollte jeweils

- die Schwachstelle anschaulich bezeichnen,
- den dadurch vorstellbaren Schaden aufzeigen,
- die nicht ergriffene Sicherheitsmaßnahme darstellen sowie
- Gründe für die Nichtergreifung der Sicherheitsmaßnahme enthalten.

Musterbeispiel

9. Schwachstellen/Risikoanalyse	
Schwachstelle:	Schäden durch höhere Gewalt (z.B. Feuer, Wasserschaden usw.) sind nicht vorhersehbar und i.d.R. erst zu spät erkennbar.
Schaden:	IT-Systeme können teilweise oder ganz zerstört werden, so daß die Nutzung der Datenverarbeitung eingeschränkt wird.
Fehlende Sicherheitsmaßnahme:	Feuer- und Wassermelder sind nicht vorhanden.
Begründung:	Die Kosten für die Installation von Feuer- und Wassermelder sind zu hoch. Die Maßnahme ist bauphysikalisch kaum durchführbar. Der Zuwachs an Sicherheit steht in keinem Verhältnis zu den Kosten.
Schwachstelle:	IT-Systeme werden gestohlen oder durch Vandalismus zerstört.
Schaden:	Die Nutzung der Datenverarbeitung ist eingeschränkt. Daten gelangen in „dritte“ Hände, so daß im Einzelfall Betroffene informiert werden müssen.
Fehlende Sicherheitsmaßnahme:	Installation einer Alarmanlage
Begründung:	Aufgrund fehlender finanzieller Mittel kann eine Alarmanlage vorerst nicht installiert werden.

Schwachstelle:	Die IT-Betreuer haben Vollzugriff auf alle IT-Systeme. Dies gilt insbesondere für die Verfahrenssoftware und die mit ihr gespeicherten Daten.
Schaden:	Die Kenntnisnahme und Manipulation verfahrensbezogener Daten ist möglich.
Fehlende Sicherheitsmaßnahme:	Vieraugenprinzip bzw. zweigeteiltes Paßwort und Verschlüsselung der Daten.
Begründung:	Aus praktischen Erwägungen wird eine technische Umsetzung der Sicherheitsmaßnahme nicht berücksichtigt. Die IT-Betreuer werden in der Dienstanweisung verpflichtet, auf Verfahrensdaten nicht zuzugreifen.
Schwachstelle:	Über die Textbearbeitung ist der Benutzer in der Lage, Dokumente lokal zu speichern. Unstrukturierte Datenhaltung. Es können Daten ohne Kenntnis der Leitungsebene gespeichert werden.
Schaden:	Rechtezuweisung auf der Festplatte der Arbeitsstation ist nur begrenzt möglich.
Fehlende Sicherheitsmaßnahme:	Der technische Aufwand für die Umsetzung der Schwachstelle steht in keinem Verhältnis zum Nutzen.
Begründung:	Die Festplatten der Arbeitsstationen werden jedoch regelmäßig in Bezug auf die Speicherung von Dokumentendateien und sonstigen temporären Dateien kontrolliert.
.....	

3.12 Fortschreibung

Das erstellte Sicherheitskonzept ist fortzuschreiben, wenn sich Änderungen in den örtlichen oder personellen Gegebenheiten ergeben haben. Spätestens nach 3 Jahren ist es zu überprüfen (§ 8 Abs. 4 DSVO). Es ist in diesem Zusammenhang auch zu prüfen, ob sich die ausgewählten Sicherheitsmaßnahmen in der Praxis bewährt haben. Sofern erneute Schwachstellen vorgefunden werden, oder ergriffene Sicherheitsmaßnahmen sich als **starke Behinderung im Arbeitsablau**f erwiesen haben, sollte versucht werden, „arbeitsablauffreundlichere“ Sicherheitsmaßnahmen zu finden.

Der Leiter der Organisation sollte das Sicherheitskonzept mit seiner Unterschrift in Kraft setzen. Das Sicherheitskonzept ist der Leitungsebene zur Kenntnis zugeben.

Musterbeispiel

10. Fortschreibung

Das Sicherheitskonzept ist bei jeder Änderung der aktuellen örtlichen und personellen Gegebenheiten und aus sonstigen Anlässen, die Auswirkungen auf das Sicherheitskonzept haben, fortzuschreiben und spätestens nach einem Jahr zu überprüfen.
.....

Das Sicherheitskonzept wird mit Wirkung vom ..... in Kraft gesetzt.

Ort, Datum und Unterschrift Leiter Organisation

Zusammenfassung

- Umfang und Zielrichtung des Sicherheitskonzeptes bestimmen.
- Gliederung festlegen.
- Für größere Fachverfahren gesonderte Sicherheitskonzepte erarbeiten.
- Mindestanforderungen definieren, die für die gesamte Organisation gelten.

- Sicherheitsmaßnahmen für
    - die Arbeitsplatzebene,
    - die Zentralrechnerebene,
    - die Verfahren sowie für
    - die IT-Betreuer

  festlegen.
- Maßnahmen für die Kontrolle der Sicherheitsmaßnahmen beschreiben.
- Notfallprogramm bzw. Verhaltensregeln bei Störungen festlegen.
- Schwachstellen bzw. Risikoanalyse erstellen.

Notizen

4 UMSETZUNG DES SICHERHEITSKONZEPTES

In diesem Kapitel erfahren Sie,

- welche Vorgehensweise bei der Umsetzung von Sicherheitsmaßnahmen zu berücksichtigen ist,
- welche Voraussetzungen für eine erfolgreiche Umsetzung erforderlich sind,
- was bei einer Schulung und Sensibilisierung der Mitarbeiter zu beachten ist.

Voraussetzungen

- *Vorlage des Sicherheitskonzeptes*
- *Tiefgreifende Kenntnisse über die eingesetzten IT-Systeme*
- *Kenntnisse über die Implementierung von technischen Sicherheitsmaßnahmen*

4.1 Realisierung der Sicherheitsmaßnahmen

Nachdem alle Sicherheitsmaßnahmen in einem Sicherheitskonzept niedergeschrieben wurden, sollte ein **Projektplan zur Realisierung dieser Maßnahmen** erstellt werden. Der Projektplan sollte alle erforderlichen Aktionen beinhalten, die zur Umsetzung der ausgewählten Sicherheitsmaßnahmen nötig sind.

Musterbeispiel

Projektplan

Termin	*Maßnahme/Arbeitsschritt*	*Person*	*Ergebnis*
01.10	MS-Windows-Systemrichtlinien für die Begrenzung der Bedieneroberfläche konfigurieren.	B	Funktionalitäten der Arbeitsplätze wurden auf das vorgegebene Maß eingeschränkt.
15.10	An allen Arbeitsstationen Disketten- und CD-ROM-Laufwerke deaktivieren	B	Für Disketten- und CD-ROM-Laufwerke wurden Verriegelungsschlösser beschafft und eingebaut
17.10	.....		
01.11	Anlegen von Systemakten	B	Für die zentralen IT-Systeme wurden Systemakten angelegt.
10.11	Erstellung von Dienstanweisungen	A B	.....
05.12	Aufbereitung der Verfahrensdokumentation	A B	.....

Der Projektplan sollte technische und organisatorische Sicherheitsmaßnahmen **getrennt** voneinander behandeln. Die Zuständigkeiten für die Umsetzung der einzelnen Aktionen sind entsprechend zuzuweisen. Anschließend werden über die Terminierung der Aktionen Prioritäten gesetzt.

Für die Umsetzung der im Sicherheitskonzept festgelegten Sicherheitsmaßnahmen sind weiterhin folgende **Voraussetzungen** zu schaffen:

- Die IT-Betreuer sind personell ausreichend zu besetzen.
- Sie müssen fachlich die Sicherheitsmaßnahmen umsetzen können.
- Ihre Aufgaben sind exakt zuzuweisen.
- Je nach Größe der Organisation sind IT-Koordinatoren in den Fachbereichen mit einzubeziehen.

Während der Umsetzung der Sicherheitsmaßnahmen ist **unbedingt zu beachten**, daß

- die Verantwortlichkeiten zugewiesen werden,
- Ressourcen bereitgestellt werden,
- die Kosten sich in dem vorher abgeschätzten Rahmen halten,
- die Maßnahmen korrekt umgesetzt werden,
- der Zeitplan eingehalten wird,
- der Datenschutzbeauftragte (sofern vorhanden) beteiligt wird.

Für die Umsetzung technischer Sicherheitsmaßnahmen wird empfohlen, für die IT-Betreuer dauerhaft ein **Test- und Schulungssystem**, bestehend aus einem Server und einer Arbeitsstation, bereitzustellen. Sicherheitsmaßnahmen sollten dann zunächst auf dem Testsystem implementiert und auf ihre **Wirksamkeit** hin analysiert werden. Erst danach sind die entsprechenden Einstellungen auf das „Echtsystem“ zu übertragen.

4.2 Schulung und Sensibilisierung der Mitarbeiter

Mit der Umsetzung des Sicherheitskonzeptes sind in der Organisation **aufbau- und ablauforganisatorische Veränderungen** notwendig, die von allen Mitarbeitern zu berücksichtigen sind. Um das Verständnis der sicherheitsrelevanten Regelungen zu erhöhen, sollte auf **allen Ebenen** der Organisation ein Schulungs- und Sensibilisierungsprogramm erarbeitet werden, das die **Sicherheitspolitik** der Organisation vermittelt. Mit dem Verständnis und der Motivation aller Mitarbeiter wird erreicht, daß die Richtlinien und die Vorschriften zur Sicherheit eingehalten werden.

Das Schulungs- und Sensibilisierungsprogramm sollte folgende Punkte behandeln:

- die Sicherheitsziele der Organisation sowie deren Erläuterung,
- die Gründe, warum Sicherheit für die Organisation wichtig ist,
- die Klarstellung der Verantwortlichkeit bezüglich der Sicherheit,
- die Aufgaben der IT-Betreuer besonders in ihrer Funktion als Dienstleister der Fachbereiche,
- die Pläne zur Implementierung der Sicherheitsmaßnahmen,
- die Vorgehensweise der Überprüfung der Einhaltung von Sicherheitsmaßnahmen sowie
- die Konsequenzen für Mitarbeiter bei Verstößen gegen Sicherheitsvorgaben.

Der wichtigste Schritt hierbei ist, der Leitungsebene ihre **Verantwortung** für die Sicherheit deutlich zu machen.

Die **Planung** der Schulungsveranstaltungen und der Beratungsgesprächen sollte vom Datenschutzbeauftragten, sofern vorhanden, oder von dem Organisationsleiter übernommen werden.
In Zusammenarbeit mit dem Datenschutzbeauftragten können dann die Veranstaltungen und die Beratungsgespräche von den IT-Betreuern durchgeführt werden.

Weiterhin ist zu empfehlen, die Schulungs- und Sensibilisierungsveranstaltungen in regelmäßigen Zeitabständen zu wiederholen, um insbesondere das vorhandene Wissen aufzufrischen und neue Mitarbeiter zu informieren.

Zusammenfassung

- Die in dem Sicherheitskonzept festgelegten Sicherheitsmaßnahmen auswerten.
- Sicherheitsmaßnahmen in technische und organisatorische Maßnahmen sortieren.
- Projektplan für die Umsetzung der Maßnahmen erstellen.
- Feststellen, ob Sicherheitsmaßnahmen personell und fachlich von den zuständigen Mitarbeitern umgesetzt werden können.
- Ggf. die IT-Betreuer auf entsprechende Schulungsseminare schicken.
- Sicherheitsmaßnahmen, wenn möglich, auf einem Test- und Schulungssystem erproben.
- Technische Sicherheitsmaßnahmen fachbereichsbezogen umsetzen.
- Schulungs- und Senibilisierungsprogramm erstellen.
- Die Leitungsebene in Beratungsgesprächen sensibilisieren und auf vorhandene Schwachstellen hinweisen.
- Mitarbeiter in Schulungsveranstaltungen auf die Veränderungen ausführlich hinweisen.

Notizen

5 IT-SICHERHEIT IM LAUFENDEN BETRIEB

In diesem Kapitel erfahren Sie,

- wie das Sicherheitsniveau dauerhaft aufrecht erhalten werden kann,
- wie die Wirksamkeit von Sicherheitsmaßnahmen kontrolliert werden,
- welche Reaktionen auf sicherheitsrelevante Ereignisse erforderlich sind.

Voraussetzungen

- *Sicherheitskonzept*
- *Kenntnisse der Aufbau- und Ablauforganisation der Organisation*

5.1 Aufrechterhaltung des erreichten Sicherheitsniveaus

Das in der Organisation eingeführte Sicherheitsniveau ist selbstverständlich nach Umsetzung der Sicherheitsmaßnahmen **dauerhaft** zu gewährleisten. Dies ist jedoch nur möglich, wenn folgende Handlungsanweisungen bestehen:

- Es sind in regelmäßigen Abständen die Sicherheitsmaßnahmen in bezug auf ihre Funktion zu überprüfen.
- Neu erkannte Schwachstellen sind durch geeignete Maßnahmen zu beseitigen.
- Personelle und organisatorische Änderungen sind unter Berücksichtigung der getroffenen

Sicherheitsmaßnahmen durchzuführen.
- Die Sicherheitsmaßnahmen sind bei Veränderungen im Hard- und Softwarebereich anzupassen.

Darüber hinaus sollte das Sicherheitskonzept **zeitnah** unter Berücksichtigung der o.a. Punkte fortgeschrieben werden.

5.2 Kontrolle der Sicherheitsmaßnahmen

Die im Sicherheitskonzept getroffenen Sicherheitsmaßnahmen sind **von Zeit zu Zeit** auf ihre Umsetzung hin zu kontrollieren. Es sollten u.a. folgende Fragestellungen während einer Kontrolle geklärt werden:

- Werden bzw. wurden die technischen Sicherheitsmaßnahmen richtig und vollständig umgesetzt?
- Finden die organisatorischen Sicherheitsmaßnahmen von den Mitarbeitern ausreichende Beachtung?
- Gibt es ggf. „neue“ Schwachstellen, die nicht im Sicherheitskonzept behandelt wurden?
- Sind die Sicherheitsmaßnahmen praxisgerecht ausgewählt worden, oder behindern sie unangemessen den Arbeitsablauf?

Die Ergebnisse einer Kontrolle sollten **dokumentiert** und der Leitungsebene zur Kenntnis gegeben werden. Für den Fall, daß erhebliche Änderungen an der Ausgestaltung der Sicherheitsmaßnahmen erforderlich sind, sollte die Leitungsebene unverzüglich mit der Fortschreibung des Sicherheitskonzeptes beginnen.

5.3 Reaktionen auf sicherheitsrelevante Ereignisse

Nachdem zahlreiche Sicherheitsmaßnahmen im Sicherheitskonzept definiert und diese in die Praxis umgesetzt wurden, ist das Auftreten von **Sicherheitsproblemen** keinesfalls ausgeschlossen. Mit sicherheitsrelevanten Ereignissen muß stets gerechnet werden. Sie lassen sich in folgende Bereiche gruppieren:

- Eine umgesetzte Sicherheitsmaßnahme hat keine ausreichende Wirkung, so daß ein sicherheitsrelevantes Ereignis eintritt.

- Es treten unvorhersehbare bzw. nicht erkannte Schwachstellen auf, die im Sicherheitskonzept keine Berücksichtigung fanden, so daß das Sicherheitsniveau nicht mehr gewährleistet ist.
- Für die in der Risikoanalyse aufgeführten Schwachstellen sind keine Sicherheitsmaßnahmen ergriffen worden, so daß in diesem Bereich stets Sicherheitsprobleme auftreten können.

Um auf ein eintretendes sicherheitsrelevantes Ereignis möglichst **schnell reagieren** zu können, sollten für die Mitarbeiter und IT-Betreuer **Verhaltensregeln** festgelegt werden, die insbesondere die Meldewege und die Maßnahmenergreifung beschreiben.

Zusammenfassung

- Die Aufrechterhaltung des Sicherheitsniveaus kann nur gewährleistet werden, wenn in regelmäßigen Abständen die Sicherheitsmaßnahmen überprüft und an technische und organisatorische Veränderungen angepaßt werden.
- Die Ergebnisse einer Kontrolle sollten dokumentiert und der Leitungsebene zur Kenntnis gegeben werden.
- Für auftretende Sicherheitsprobleme sollten Verhaltensregeln definiert werden.

Notizen

CHECKLISTE

Prüfansatz

- Sind die vom Hersteller geforderten Installations- und Betriebsvoraussetzungen (sicherer Stand, Stromversorgung, Temperatur, Luftfeuchtigkeit, Schutz vor Sonneneinstrahlung) geschaffen?
- Sind die Nutzer (einschließlich der Vertreter) von IT-Systemen aufgabenspezifisch geschult?
- Liegen aktuelle Benutzerhandbücher vor?
- Sind alle IT-Geräte und externen Datenträger (z. B. Disketten, Bänder, Streamer) gekennzeichnet?
- Sind Hard- und Software inventarisiert und im Geräteverzeichnis aufgenommen?
- Werden bei Abwesenheit der Benutzer die Räume verschlossen?
- Werden die Programme einschließlich der Betriebssysteme und der systemnahen Software sowie die Datenbestände regelmäßig gesichert?
- Sind externe Datenträger und Dokumentationen (inklusive Originalsoftware) gegen Feuer und andere schädigende Ereignisse geschützt entsprechend gelagert?
- Sind Ersatzgeräte bzw. Geräteteile für einen schnellen Austausch vorhanden?
- Wird bei dienstlichen Geräten, die für dienstliche Zwecke außerhalb der Diensträume eingesetzt werden, eine Dateiverschlüsselung eingesetzt?
- Wird Software vor deren Einsatz genehmigt bzw. freigegeben?
- Enthält das Freigabeverfahren Testmaßnahmen?
- Erfolgt die Freigabe von dem Verfahrensverantwortlichen?
- Besteht eine revisionsfähige Dokumentation der eingesetzten Fachverfahren?
- Kann die Benutzung des IT-Systems nur nach Eingabe einer individuellen Nutzerkennung und der Authentifizierung durch ein Paßwort erfolgen?
- Werden die Funktionen der Benutzer von IT-Systemen und der Administratoren getrennt?
- Können Benutzer nur auf getestete und freigegebene Anwendungssoftware zugreifen?
- Sind Zugriffe auf die Administrationsebene und dadurch Direktzugriffe auf Daten unterbunden?
- Sind die Zuständigkeiten der Administratoren abschließend festgelegt?
- Sind Vertreter in ausreichender Zahl vorhanden?
- Werden Systemaktivitäten revisionsfähig protokolliert?

- Ist die Zuständigkeit für die Überwachung der ordnungsgemäßen Benutzung der eingesetzten Hard- und Software festgelegt?
- Ist der Datenträgeraustausch mit externen Stellen nur aufgrund einer arbeitsplatzbezogenen Genehmigung zulässig?
- Sind die Disketten- und CD-ROM-Laufwerke deaktiviert?
- Wird ein permanenter Virenschutz eingesetzt?
- Werden benutzte externe Datenträger vor erneuter Ausgabe physikalisch gelöscht?
- Werden Datenträger nur unter Aufsicht oder in physikalisch gelöschter Form entsorgt?
- Sind die Zugriffsberechtigungen auf die Anwendungssoftware soweit wie möglich differenziert?
- Besteht eine Dokumentation der Benutzer- und Rechteverwaltung?
- Sind IT-Systeme so platziert, daß eine unbefugte Kenntnisnahme von dargestellten oder ausgedruckten Informationen (z. B. durch Besucher oder sonstige Nichtbeteiligte) ausgeschlossen wird?
- Kann vom Benutzer eine Bildschirmsperre aktiviert werden?
- Werden die Tätigkeiten von Dienstleistern (Installation, Wartung, Servicetechniker) beaufsichtigt und protokolliert?
- Sind die zentralen IT-Systeme in besonders gesicherten Räumen (Sicherheitsbereich) installiert?
- Sind die Zutrittsberechtigten geregelt?
- Werden Reinigungsarbeiten und technische Dienstleistungen unter Aufsicht der IT-Betreuer durchgeführt?
- Sind bei einer Fernwartung besondere Sicherheitsmaßnahmen vorgesehen?
- Wird die Fernwartung vor Beginn telefonisch mit den IT-Betreuern abgestimmt?
- Werden die Daten der Fachverfahren ausschließlich auf den zentralen IT-Systemen gespeichert?
- Wird eine Datensicherung durchgeführt?
- Wird eine Datensicherungsgeneration in regelmäßigen Abständen außerhalb der Organisation, z.B. in einem Bankschließfach, deponiert?
- Werden zentral erzeugte Ausdrucke (Massendrucke, Druckservice) den Veranlassern unverzüglich zur Verfügung gestellt?
- Ist die Art und Weise der Beseitigung des „Papierschrotts“ geregelt?

GEFAHRENKATALOG

Höhere Gewalt

- Personalausfall
- Ausfall des IT-Systems
- Blitz, Feuer, Wasser
- Kabelbrand
- Unzulässige Temperatur und Luftfeuchte
- Staub, Verschmutzung
- Datenverlust durch starke Magnetfelder
- Ausfall externer Netze

Organisatorische Mängel

- Fehlende oder unzureichende Anweisungen bzw. Regelungen
- Unzureichende Kenntnisse der bestehenden Regelungen
- Fehlende oder ungeeignete Betriebsmittel
- Unzureichende Kontrolle der IT-Systeme
- Fehlende oder unzureichende Wartung
- Unbefugter Zutritt zu schutzbedürftigen Räumen
- Mangelhafte Anpassung an den technischen Stand
- Unzureichende Dokumentation der Verkabelung
- Unzureichend geschützte Verteiler
- Beeinträchtigung der IT-Nutzung durch ungünstige Arbeitsbedingungen
- Vertraulichkeitsverlust schutzbedürftiger Daten
- Ungeordneter Benutzerwechsel auf Arbeitsstationen
- Mangelhafte Kennzeichnung der Datenträger
- Unzureichendes Schlüsselmanagement bei Verschlüsselung
- Fehlende Auswertung von Protokolldaten

- Fehlendes oder unzureichendes Test- und Freigabeverfahren
- Fehlende oder unzureichende Verfahrensdokumentation
- Softwaretest mit „Echtdaten“
- Unzureichender Schutz der Bedieneroberfläche der Arbeitsstationen
- Unzureichende Leitungskapazitäten
- Nicht gesicherter Aufstellungsort von Servern
- Fehlende oder unzureichende Aktivierung von Sicherheitsmechanismen
- Ungeeignete Einschränkung der Benutzerumgebung
- Unkontrollierter Aufbau von Kommunikationsverbindungen
- Konzeptionelle Schwächen des Netzes und der Serverstrukturen
- Ungesicherter Datenträgertransport
- Ungeeignete Entsorgung der Datenträger
- Fehlende oder unzureichende Schulung der Mitarbeiter und der IT-Betreuer
- Ungeordnete E-Mail-Nutzung

Technische Mängel

- Ausfall der Stromversorgung
- Ausfall interner Versorgungsnetze
- Ausfall vorhandener Sicherungseinrichtungen
- Spannungsschwankungen/Überspannung/Unterspannung
- Defekte Datenträger
- Bekanntwerden von Softwareschwachstellen
- Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
- Fehlende Authentisierungsmöglichkeit zwischen Server und Arbeitsstation
- Verlust gespeicherter Daten
- Absenden von Daten an einen falschen Empfänger durch Fehlverbindung
- Übertragungsfehler
- Informationsverlust bei unzureichender Speicherkapazität
- Datenverlust bei erschöpftem Speichermedium
- Schwachstellen oder Fehler in Standardsoftware

- Nicht getrennte Verbindungen
- Ausfall einer Datenbank
- Verlust von Daten einer Datenbank
- Verlust der Datenbankintegrität/-konsistenz
- Ausfall oder Störung von Netzkomponenten

Menschliche Fehlhandlungen

- Nichtbeachtung von IT-Sicherheitsmaßnahmen
- Unbeabsichtigte Leitungsbeschädigung
- Gefährdung durch Reinigungs- oder Fremdpersonal
- Fehlerhafte Nutzung des IT-Systems
- Fehlerhafte Administration des IT-Systems
- Übertragung falscher oder nicht gewünschter Daten
- Fehlerhafte Administration von Zugangs- und Zugriffsrechten
- Unbeabsichtigtes Löschen von Programmen und/oder Daten
- Unerlaubte private Nutzung des dienstlichen Systems
- Unstrukturierte Datenhaltung

Vorsätzliche Handlungen

- Manipulation/Zerstörung von IT-Geräten oder Zubehör
- Manipulation an Daten oder Software
- Unbefugtes Eindringen in ein Gebäude
- Diebstahl, Vandalismus, Anschlag
- Abhören von Leitungen
- Manipulation an Leitungen
- Unberechtigte IT-Nutzung
- Mißbrauch von Fernwartungszugängen
- Gefährdung bei Wartungsarbeiten durch internes Personal

- Gefährdung bei Wartungsarbeiten durch externes Personal
- Systematisches Ausprobieren von Paßwörtern
- Mißbrauch von Benutzerrechten
- Mißbrauch von Administratorrechten
- Trojanische Pferde
- Diebstahl bei mobiler Nutzung des IT-Systems
- Computer-Viren
- Unberechtigtes Kopieren der Datenträger
- Eindringen in Rechnersysteme über Modem oder externe Schnittstellen
- IP-Spoofing
- Mißbrauch der Datenübertragung
- Bewußte Fehlbedienung von Schutzschränken aus Bequemlichkeit
- Netzanalyse-Tools
- Unberechtigte Ausführung von Netzmanagementfunktionen
- Mißbrauch von Netzwerkkomponenten
- Unberechtigter Anschluß von IT-Systemen an ein Netz
- Unberechtigter Zugang zu den Netzkomponenten
- Mißbräuchliche E-Mail-Nutzung
- Vortäuschen eines falschen Absenders
- Mitlesen von E-Mails oder sonstigen Verfahrensdaten
- Ausspähen der internen gespeicherten Daten bei Internetnutzung

MAßNAHMENKATALOG

Infrastrukturelle Maßnahmen

- Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften
- Regelungen für Zutritt zu Verteilern
- Angepaßte Aufteilung der Stromkreise
- Blitzschutzeinrichtungen
- Einhaltung von Brandschutzvorschriften und Auflagen der örtlichen Feuerwehr
- Handfeuerlöscher
- Verwendung von Sicherheitstüren
- Geschlossene Fenster und Türen
- Geeignete Standortauswahl
- Pförtnerdienst
- Gefahrenmeldeanlage
- Einbruchsschutz
- Abgeschlossene Türen
- Überspannungsschutz
- Not-Aus-Schalter
- Klimatisierung
- Lokale unterbrechungsfreie Stromversorgung
- Geeignete Aufstellung eines IT-Systems
- Geeignete Aufstellung von Konsole, Geräten mit austauschbaren Datenträgern und Druckern
- Geeignete Aufbewahrung tragbarer PCs bei mobilem Einsatz
- Sichere Aufbewahrung der Datenträger vor und nach Versand
- Geeignete Aufstellung von Fax-Gerät und Modem
- Geeignete Aufstellung von Schutzschränken
- Schutz gegen elektromagnetische Einstrahlung
- Gesicherte Aufstellung von zentralen Servern

Personelle Maßnahmen

- Geregelte Einarbeitung/Einweisung neuer Mitarbeiter
- Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
- Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz
- Ernennung eines IT-Betreuers und eines Vertreters
- Vertretungsregelungen festlegen
- Schulung vor Verfahrensnutzung
- Schulung zu IT-Sicherheitsmaßnahmen
- Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern
- Anlaufstelle bei Anwendungsproblemen
- Ergonomischer Arbeitsplatz
- Schulung des Wartungs- und Administrationspersonals
- Einweisung des Personals in den geregelten Ablauf eines Datenträgeraustausches
- Informationen für alle Mitarbeiter über die Nutzung eines Fax-Gerätes
- Einweisung des Personals in die Modem-Benutzung
- Verpflichtung der PC-Benutzer zum Abmelden nach Aufgabenerfüllung

Organisatorische Maßnahmen

- Betriebsmittelverwaltung
- Datenträgerverwaltung
- Regelungen für Wartungs- und Reparaturarbeiten
- Aufgabenverteilung und Funktionstrennung
- Vergabe von Zugangsberechtigungen
- Vergabe von Zugriffsrechten
- Nutzungsverbot nicht freigegebener Software
- Überprüfung des Software-Bestandes
- Regelung des Paßwortgebrauchs
- Betreuung und Beratung von IT-Benutzern

- Schlüsselverwaltung
- Beaufsichtigung oder Begleitung von Fremdpersonen
- Zutrittsregelung und -kontrolle
- Dokumentation der Netzwerkkomponenten
- Hinterlegen des Paßwortes
- Herausgabe einer Benutzer und Administrationsdienstanweisung
- Einführung einer Systemakte
- Dokumentation der Systemkonfiguration (Geräteverzeichnis)
- Regelung für die Einrichtung von Benutzern bzw. Benutzergruppen
- Dokumentation der zugelassenen Benutzer und Rechteprofile
- Einrichtung einer eingeschränkten Benutzerumgebung
- Aufteilung der Administrationstätigkeiten
- Dokumentation der Veränderungen an einem bestehenden System
- Informationsbeschaffung über Sicherheitslücken des Systems
- Geregelte Übergabe und Rücknahme eines tragbaren PC
- „Der aufgeräumte Arbeitsplatz“, Clear-Desk-Anweisung
- Rechtzeitige Beteiligung des Personalrates
- Ausreichende Kennzeichnung der Datenträger beim Versand
- Sichere Verpackung der Datenträger
- Regelung des Datenträgeraustausches
- Software-Abnahme- und Freigabe-Verfahren
- Kontrolle der Protokolldateien
- Entwicklung eines Firewall-Konzeptes
- Festlegung einer Sicherheitspolitik für einen Firewall
- Anforderungen an einen Firewall
- Auswahl eines geeigneten Firewall-Typs
- Auswahl und Implementation geeigneter Filterregeln
- Sichere Anordnung weiterer Komponenten
- Sicherer Betrieb eines Firewall
- Installation und Konfiguration von Standardsoftware
- Rechtevergabe für den Fernzugriff
- Bereithalten von Handbüchern

- Festlegung einer Sicherheitspolitik für E-Mail-Nutzung
- Regelung für den Einsatz von E-Mail
- Einrichtung einer Poststelle
- Regelmäßiges Löschen von E-Mails
- Einheitliche E-Mail-Adressen
- Auswahl eines Mailproviders
- Geeignete Auswahl einer Datenbank-Software
- Installation und Konfiguration einer Datenbank
- Erstellung eines Datenbanksicherheitskonzeptes
- Gewährleistung der Datenbankintegrität
- Aufteilung von Administrationstätigkeiten bei Datenbanksystemen
- Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen
- Strukturierte Datenhaltung
- Entwicklung eines Netzkonzeptes
- Entwicklung eines Netz-Realisierungsplans
- Entwicklung eines Netzmanagementkonzeptes
- Anforderungen an ein Netzmanagement-Tool

Technische Maßnahmen

- Paßwortschutz für PC und Server
- Bildschirmsperre
- Regelmäßiger Einsatz eines Viren-Suchprogramms
- Verschluß der Diskettenlaufwerkschächte
- Verhinderung des unautorisierten Erlangens von Administratorrechten
- Verhinderung des Vertraulichkeitsverlusts schutzbedürftiger Daten durch IT-Betreuer
- Sicherer Aufruf ausführbarer Dateien
- Sicherstellung einer konsistenten Systemverwaltung
- Einsatz der Protokollierung auf Zentralrechner
- Regelmäßiger Sicherheitscheck der Zentralrechner
- Paßwort- und Verschlüsselungsschutz am mobilen PC

- Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen
- Einsatz eines Viren-Suchprogramms vor und nach einer Datenübertragung
- Einsatz von Verschlüsselung, Checksummen oder digitalen Signaturen
- Einsatz eines angemessenen PC-Sicherheitsproduktes
- Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung
- Prüfung eingehender Dateien auf Makro-Viren
- Protokollierung der Firewall-Aktivitäten
- Absicherung des Boot-Vorgangs auf Arbeitsstationen
- Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten
- Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse
- Test neuer Hard- und Software
- Sperren und Löschen nicht benötigter Accounts
- Sicherstellung einer konsistenten Datenbankverwaltung
- Regelmäßiger Sicherheitscheck der Datenbank
- Durchführung einer Datenbanküberwachung
- Datenbank-Verschlüsselung
- Sorgfältige Durchführung von Konfigurationsänderungen
- Sichere Zugriffsmechanismen bei Fernadministration
- Audit und Protokollierung der Aktivitäten im Netz
- Sichere Konfiguration der Netzkomponenten
- Auswahl einer geeigneten Netz-Topologie
- Dokumentation und Kennzeichnung der Verkabelung
- Monatlicher Sicherheitscheck des Netzes
- Absicherung von Remote-Zugängen
- Telefonische Ankündigung einer Fax-Sendung
- Telefonische Rückversicherung über korrekten Fax-Empfang
- Aktivierung einer vorhandenen Callback-Option
- Sicherer Einsatz von Kommunikationssoftware
- Absicherung der per Modem durchgeführten Fernwartung
- Einsatz von Einmalpaßwörtern
- Einseitiger Verbindungsaufbau
- Sicherheit von WWW-Browsern

- Einsatz von Standalone-Systemen zur Nutzung des Internets
- Schutz vor Mailüberlastung und Spam
- Sicherer Betrieb eines Mailservers
- Geeignete physikalische und logische Segmentierung des Netzwerkes

Maßnahmen für den Notfall

- Erstellung einer Übersicht über Verfügbarkeitsanforderungen
- Definition von Notfallsituationen
- Notfall-Verantwortlicher
- Erstellung eines Notfall-Handbuches
- Untersuchung interner und externer Ausweichmöglichkeiten
- Alarmierungsplan
- Erstellung eines Wiederanlaufplans
- Durchführung von Notfallübungen
- Erstellung eines Datensicherungsplans
- Ersatzbeschaffungsplan
- Brandschutzübungen
- Geeignete Aufbewahrung der Backup-Datenträger
- Sicherungskopie der eingesetzten Software
- Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
- Verhaltensregeln bei Auftreten eines Computer-Virus
- Erstellen einer PC-Notfalldiskette
- Regelmäßige Datensicherung der Server-Festplatte
- Regelmäßige Datensicherung
- Entwicklung eines Datensicherungskonzepts
- Dokumentation der Datensicherung
- Redundante Auslegung der Netzkomponenten

Quellen, Literaturhinweise

- Horst Abel, Praxishandbuch für den betrieblichen Datenschutzbeauftragten
  Interest Verlag

- Dworatschek, Büllesbach, Personal Computer und Datenschutz
  Datakontext-Verlag

- Hans-Dietrich Koch, Der betriebliche Datenschutzbeauftragte
  Datakontext-Verlag

- Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Grundschutzhandbuch
  Bundesanzeiger, Schriftenreihe zur IT-Sicherheit

- IT-Handbuch des Landes Schleswig-Holstein
  Innenministerium

- Landesdatenschutzgesetz – LDSG –
  Gesetz- und Verordnungsblatt für Schleswig-Holstein 1991 Seite 555

- Datenschutzverordnung - DSVO –
  Gesetz- und Verordnungsblatt für Schleswig-Holstein 1994 Seite 473

Der neue Datenschutz

- *kompetent*
- *bürgernah*
- *serviceorientiert*