



Einführung eines IT-Sicherheits- und Notfallkonzeptes

Einführung

Jedes Unternehmen im Bereich des Gesundheits- und Sozialwesens wie auch in anderen Wirtschafts- und öffentlichen Bereichen ist auf eine permanent verfügbare Informationstechnik angewiesen. In den Unternehmen werden unterschiedliche IT-Verfahren mit unterschiedlicher Zielsetzung der Datenverarbeitung eingesetzt. Die IT-Sicherheit in den Unternehmen kann sowohl durch interne Vorgänge als auch durch Einwirkungen von außerhalb des Unternehmens gefährdet werden. Zu diesem Zweck wird ein IT-Sicherheitskonzept erarbeitet, in dem die Datenverarbeitung unter Risikoaspekten in dem betroffenen Unternehmen durchleuchtet wird. Als Ergebnis kann dann für explizit definierte Notfälle ein Notfallkonzept, d. h. eine Handlungsanweisung für den Umgang mit Notfällen erarbeitet werden.

Während verschiedene Landesdatenschutzgesetze konkrete Vorgaben hinsichtlich der Erarbeitung von IT-Sicherheitskonzeptionen enthalten, sind im Bundesdatenschutzgesetz, sowie in den Datenschutzgesetzen der Evangelischen und Katholischen Kirche nur indirekte Vorgaben genannt (Vorabkontrolle, rechtzeitige Überprüfung neuer Verfahren durch den Datenschutzbeauftragten und Organisationskonzepte im Rahmen vorgegebener technisch-organisatorischer Maßnahmen).

1. IT-Sicherheitskonzept

Es empfiehlt sich auf der Basis der Veröffentlichung des Bundesamtes für Sicherheit in der Informationstechnik (BSI), insbesondere der BSI-Standards 100-1 bis 100-4), ein IT-Sicherheitskonzept zu erarbeiten (www.BSI.de/gshb/index.htm).

1.1. Bestandsaufnahme über die IT-Landschaft im Unternehmen

Zunächst ist zu ermitteln, auf welche Hardware im Unternehmen unter Berücksichtigung der Netzwerkstruktur welche Anwendungen und Verfahren zum Zwecke der Datenverarbeitung eingesetzt werden. Dabei ist eine Gewichtung dahingehend vorzunehmen, welche Folgen der Ausfall einer möglichen Datenverarbeitung im Unternehmen für das Unternehmen als solches oder Teile des Unternehmens nach sich zieht.

Es ist dann zu prüfen, welche Bedrohungen sich für die IT-Systeme in der Praxis einstellen können. Auch diese Bedrohungen müssen in verschiedene Kategorien, je nach Schwere der Beeinträchtigung, eingestuft werden.

Schließlich sind die Maßnahmen gegenüber den festgestellten Bedrohungen festzulegen, auch mit den wirtschaftlichen Folgen für das Unternehmen.

1.2. Durchführung einer Bedrohungs- und Risikoanalyse und Ermittlung des Schutzbedarfes

Alle im Unternehmen verarbeiteten Daten werden auf die **Verfügbarkeit** (wenn eine vorgegebene Funktionalität eines IT-Systems in der vorgesehenen Zeit erbracht werden kann und die Funktionalität des IT-Systems nicht vorübergehend bzw. dauernd beeinträchtigt ist), die **Integrität** (wenn Informationen und Daten nur von Befugten in vorgesehener Weise verarbeitet werden, d.h. während des Verarbeitungsprozesses unversehrt bleiben) und **Vertraulichkeit** (wenn Befugten die Informationen nur in der zulässigen Weise zugänglich sind und kein unbefugter Informationsgewinn stattfinden kann) ermittelt.

Anschließend sollte eine **Bewertung des Schadensbedrohungspotenzials** erfolgen, wobei insbesondere festzustellen ist, welche Auswirkungen ein Schadensereignis auf das ge-



samte Unternehmen hat (z. B. geringe, mittlere, große oder Existenz gefährdende Auswirkung).

Um detaillierte Bewertungen und Abstufungen der Bedrohungspotenziale vornehmen zu können, müssen auch die Verfügbarkeit, Integrität und Vertraulichkeit abgestuft bewertet werden (z. B. eine bei der Verfügbarkeit max. tolerierbare Ausfallzeit, bei Eingriffen mit großer Auswirkung auf das Unternehmen max. 1 Stunde, Stufe 2 z. B. max. 5 Stunden, Stufe 3 max. 20 Stunden und Stufe 4 z. B. max. 3 Tage).

Auch bei der Vertraulichkeit beispielsweise ist zu differenzieren zwischen geheimen betrieblichen Daten sowie hoch sensiblen Daten (beispielsweise Angabe über Krankheiten) auf der einen Seite und unbedenklichen Daten auf der anderen Seite mit den entsprechenden Abstufungen dazwischen.

Die **Notfälle** können beispielsweise in folgende Kategorien unterteilt werden. In den Notfall mit schwerwiegenden Folgen für wichtige Bereiche im Unternehmen, der Fall, der nur unterhalb des Notfalls angesiedelt wird, der bestimmte Vorgänge im Unternehmen abgegrenzt betrifft (z. B. Ausfall bei Zahlungsläufen, bei Monatsabschlüssen). Wiederum davon abzugrenzen ist der Ausfall beim normalen Betrieb im Unternehmen.

1.3. Klassifizierung des im Unternehmen bedrohten Objekts

Im Unternehmen können beispielsweise folgende Bereiche Bedrohungen und damit Risiken ausgesetzt sein:

- die Infrastruktur (allgemein und IT)
- die Hardware
- die Software
- die Papieraktenverwaltung und Datenträgerentsorgung
- die vorgehaltenen Daten
- die Kommunikationsstrukturen
- die handelnden Personen.

Beispiele für den Bereich Infrastruktur sind Räumlichkeiten der IT, wie z. B. Serverbetriebsräume, Netzknotenbetriebsräume, Stromversorgung, Telefonanlagen usw.; zur Hardware sind zu zählen die Netzwerktechnik, Fileserver, PCs, Drucker usw. als Endgeräte, Datenbankserver usw.; zu dem Bereich Papierverwaltung wären zu zählen alle Daten, die in Papier verwaltet werden einschließlich der Verträge im Unternehmen. Zur Software sind alle Arten von Software zu rechnen, wie z. B. Netzwerksoftware, Betriebssystemsoftware, Rechnungswesensoftware, Personalverwaltungssoftware, Klienten- und Patienteninformationssysteme usw.

Anwendungsdaten können vielfältiger Art sein, wie z. B. die Mitarbeiterdaten, Patientendaten, Klienten- und Bewohnerdaten, Buchhaltungsdaten, Rechnungswesendaten usw.

1.4. Definition der Schadensrealisierung

Einerseits können die Häufigkeiten von eingetretenen Schäden bezogen beispielsweise auf die zuvor genannten Bereiche ermittelt bzw. vorhergesagt werden auf der Basis der Häufigkeit, d. h. z. B. Schadenseintritte, die sehr selten, z. B. max. 1 x in 5 Jahren auftreten bis zu sehr häufig auftretenden Schäden, d. h. z. B. 1 x pro Tag. Auch die Auswirkung eines Schadens, die gering sein kann bis hin zu Existenz gefährdend in der schwerwiegendsten Schadenskategorie sollten in diesem Zusammenhang ermittelt werden. Beispielsweise kann ein sehr selten auftretender Schaden eine erhebliche Auswirkung haben (Computerviren legen

das gesamte Netzwerk lahm; Brand im Serverraum sorgt für Totalausfall bei der Datenverarbeitung usw.).

1.5. Maßnahmenkatalog auf Basis der Bestandsaufnahme und Risikobewertung

Jedes Unternehmen muss speziell definieren, auf welche Bedrohungen im Einzelfall oder Kategorie von Bedrohungen Abwehrmaßnahmen vorgesehen werden müssen. Insbesondere sollten in diesem Zusammenhang vorsorgliche Maßnahmen im IT-Sicherheitskonzept festgelegt werden, d. h. z. B. allgemeine Maßnahmen zur Verhinderung des Eintrittes allgemein bekannter Folgen (z. B. obligatorischer Bildschirmschoner mit Kennwort, Berechtigungskonzepte für Anwender und Administratoren, Verschlüsselungen bei Laptops) um zu verhindern, dass vertrauliche sensible Daten verloren gehen oder durch Unbefugte eingesehen werden. Schließlich sollte jede einzelne Maßnahme je nach Gewicht eines möglichen Schadens nicht nur definiert, sondern auch begründet werden und ein mögliches Restrisiko benannt sein.

2. Notfallkonzept/ Notfallhandbuch

2.1. Allgemeines

Jedes im Gesundheits- und Sozialwesen tätige Unternehmen sollte für Beeinträchtigungen der IT, ganz besonders für Notfälle ein Notfallkonzept für die Mitarbeiter im Unternehmen (Notfallhandbuch) erarbeiten mit Handlungsanweisungen und Abwehrmaßnahmen.

Ein **Notfall** ist ein Ereignis, das erhebliche Einflüsse auf die IT des Unternehmens hat und sich wesentlich auf das Unternehmen oder einen Geschäftsbereich des Unternehmens oder die Infrastruktur auswirkt.

2.2. Rechtsrahmen für ein Notfallkonzept

Das Erfordernis eines Notfallkonzeptes ergibt sich aus folgenden Rechtsbereichen

- **Die GoBs (Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme)** sind Hintergrund eines Schreibens des Bundesfinanzministeriums aus dem Jahre 1995, wo sich Vorschriften u. a. zur Datensicherheit, Dokumentation, Prüfbarkeit und Datenwiedergabe finden. Weitere Vorgaben ergeben sich aus § 147 AO (Abgabenordnung), § 257 HGB (Aufbewahrungsfristen), oder § 261 HGB (Wiederlesbarmachung).
- Weitere Anforderungen stellt das **KonTraG** in § 91 auf, wonach der Vorstand geeignete Maßnahmen treffen muss, insbesondere ein Überwachungssystem einzurichten hat, damit gefährdende Entwicklungen, welche den Fortbestand der Gesellschaft gefährden, früh erkannt werden.
- Der **IDW-Prüfungsstandard 330** ist von der Wirtschaftsprüferkammer vorgegeben. Danach sind bei Unternehmen mit hoher Abhängigkeit von IT-Systemen besondere Anforderungen an die Qualität der Risikovorsorge und den Detaillierungsgrad einer Notfallplanung zu stellen.
- **Basel II** fordert ebenfalls eine Notfallplanung ein, damit das Risiko von Verlusten, welche in inadäquaten oder fehlerhaften internen Prozessen ihre Ursache haben, ebenso wie durch Menschen und Systeme oder externe Ereignisse verursacht sind, ausgeschlossen werden.
- **Datenschutzgesetz** im oben genannten Sinne.

2.3. Vorgehensweise bei der Erarbeitung eines Notfallkonzeptes

Zunächst sind die **Ursachen** für Notfälle im Unternehmen bis hin zu Katastrophenfällen zu benennen. Notfälle können beispielsweise ihren Ursprung haben in einem Stromausfall, im Ausfall des Telefonnetzes, im Ausfall der Hardware sowie auch der Software, aber auch im Ausfall von Personal zu sehen sein.

Es ist zu klären, welche Beeinträchtigungen im Unternehmen tatsächlich als Notfall behandelt werden müssen, oder nur als geringfügige Störungen zu bewerten sind und im üblichen Tagesgeschäft beseitigt werden können. Schließlich ist dann zu definieren, in welchen Situationen welche Personen mit welchen Funktionen im Unternehmen Entscheidungen treffen und Maßnahmen in die Wege leiten müssen (Einrichtung eines **Krisengremiums**).

Dann sind die **Informationswege** zu definieren, wer wird intern benachrichtigt, auf welche Art und Weise (z. B. per Telefon, per E-Mail usw.). Schließlich ist zu klären, ob auch externe Beteiligte (Behörden, Kunden usw.) informiert werden müssen. Um Notfälle zu definieren, muss jedes im Gesundheits- und Sozialwesen arbeitende Unternehmen die entscheidenden Prozesse im Unternehmen festlegen, deren Bedrohung und Ausfall so wesentlich sind, dass das Vorhandensein eines Notfallkonzeptes erforderlich ist. Z. B. kann ein entscheidender Prozess im Bereich der Krankenhäuser die Leistungsabrechnung sein, aber auch der Zugriff auf ein Krankenhausinformationssystem.

3. Notfallhandbuch

Ein Notfallhandbuch ist somit eine „Betriebsanleitung zum praktischen Vorgehen der im Notfallkonzept definierten Notfälle“. Hier ist anhand eines Notfalles, d. h. anhand einer Störung des Gesamt- oder wesentlichen Teilprozesses das Notfallmanagement zu definieren und die erforderlichen Aktionen bestimmten Personen im Unternehmen zuzuweisen. Jedes Unternehmen muss im Notfallhandbuch zunächst die Notfälle als solche definieren, z. B. umfangreicher Stromausfall, Ausfall des SAP-Systems, Komplettausfall der Firewall usw.). Je nach Umfang der Realisierung eines Notfalls ist anhand der Eskalationsstufe jeweils zu definieren, welcher beteiligte Ansprechpartner in dem Unternehmen zunächst für die Störungsbeseitigung zuständig ist. Bei weiterer Eskalation ist dann auch festzulegen, wann ein Krisenstab einzuberufen ist und welche Personen daran zu beteiligen sind, welche Entscheidungskompetenz sie haben, welche Beteiligte im Unternehmen und extern (z. B. Systemhersteller) zu informieren sind.

Diese Auffassung ist die abgestimmte Meinung des GDD-Arbeitskreises „Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen“. Im Einzelfall sollte sie juristisch geprüft werden.

gez.: GDD-AK GSW (Bearbeiter Herr Christian Bake, Herr Dr. Peter Münch)
12.06.2007