Der sichere Pfad durch den Datensecurity Jungle

Angela Espinosa
Lufthansa Systems AG
Kelsterbach

Schlüsselworte

Datensicherheit Regularien Datenschutz Audits ISO27001/27002 ISAE3402 PCI DSS Informationssicherheit

Einleitung

Dieser Vortrag reißt Themen an, die rund um die Datensicherheit kreisen. Welche Regularien muss ich kennen, damit ich meine Datenbank sicher betreiben und in Audits bestehen kann. Was kann ich darüber hinaus tun, um die Sicherheit zu erhöhen.

Zusätzlich soll es einen Ausblick auf die Zukunft geben. Die EU plant Maßnahmen um die IT-Sicherheit zu stärken.

Warum braucht man Standards in der Informationssicherheit?

Immer mehr Geschäftsprozesse werden digital abgebildet. Damit werden Unternehmensdaten und andere schützenswerte wie personenbezogene Daten in großer Zahl digital abgespeichert, verarbeitet und ggf. durch Provider gehostet. Der Angriffsvektor für Hacker von intern sowie extern wird vergrößert, damit steigen die Risiken für Unternehmen und öffentliche Einrichtungen, erheblichen Schaden zu erleiden.

Der Druck auf Unternehmen und öffentliche Einrichtungen wächst, Maßnahmen zur Informationssicherheit durchzuführen, Diese beziehen sich in der Regel auf die sog. Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit. .

Maßnahmen zur Informationssicherheit werden zunehmend vom Gesetzgeber und Kunden eingefordert. Es gibt gesetzliche Regelungen, die dies direkt oder indirekt vorschreiben. Außerdem haben sich (ausgehend vom Skandal um die Enron Bilanzfälschung im Jahr 2001) die gesetzlichen Anforderungen an Compliance und Transparenz von Finanz- und Rechnungswesen erhöht.

Informationssicherheit muss damit in jeder Firma groß geschrieben werden. Um einen sicheren Umgang mit Daten und informationsverarbeitenden Systemen zu gewährleisten, ist es erforderlich, entsprechend der jeweiligen Gefährdung, Sicherheitsstandards zu entwickeln und einzuhalten.

Welche Normen/Standards gibt es und welche sind für mein Unternehmen relevant?

Gesetzliche Vorgaben

Dreh- und Angelpunkt ist das KonTraG das Gesetz zur Kontrolle und Transparenz im Unternehmen. Es hat als Ziel, die Corporate Governance deutscher Unternehmen zu verbessern. In der Umsetzung bedeutet dies, daß verbindliche Regeln und ein unternehmensweites Risikomanagement eingeführt werden. Risiken müssen bewertet und darauf aufsetzend sinnvolle Maßnahmen formuliert werden. Wörtlich schreibt das Gesetz

dazu in § 91 Abs. 2 AktG eine neue Vorschrift vor, nach der der Vorstand verpflichtet wird „geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden".

Das Bundesdatenschutzgesetz (BDSG) wurde dafür erlassen, um den Schutz personenbezogener Daten sicherzustellen. Personenbezogene Daten sind zum Beispiel Name, Alter, Familienstadt, Geburtsdatum etc. Ein Datenschutzbeauftragter muss ab einer gewissen Unternehmensgröße bestellt werden. Zwischen Vertragspartnern muss eine Auftragsdatenverarbeitung-Vereinbarung (ADV-Vereinbarung) geschlossen werden, wenn im Auftrag der verantwortlichen Stelle personenbezogene Daten erhoben, verarbeitet oder genutzt werden. Im BDSG wird im Detail beschrieben, welche Rechte, Pflichten und Maßnahmen zu treffen sind.

Im Handelsgesetzbuch (HGB) wird gefordert, dass die Buchführung „ordnungsmäßig" und „in einer entsprechenden Zeit aufzustellen" sei – dies sind die Forderungen nach den Schutzzielen Integrität und Verfügbarkeit.Über Paragrafen zur Verletzung der Geheimnispflicht kann das Schutzziel „Vertraulichkeit" abgeleitet werden.

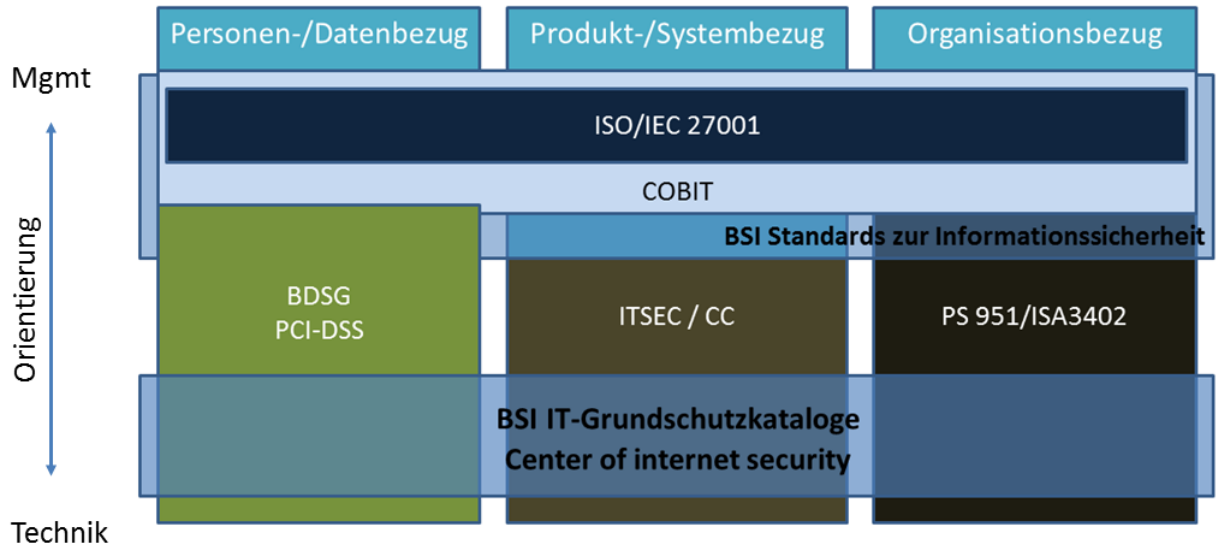
Das sind nur drei von vielen Vorgaben. Man muss verstehen, dass sich vieles überschneidet und dass es im Kern immer darum geht, Risiken zu erkennen, und durch entsprechende Maßnahmen zu vermeiden oder zu vermindern.

Normen bzw. Branchenregeln

Weltweit gibt es zahlreiche Gremien, die sich mit der Entwicklung von Sicherheitsstandards und Normen beschäftigen. Es gibt zahlreiche Standards, die man in dem Leitfaden der BITKOM wunderbar nachlesen kann. Als erstes bilden sie eine Orientierung und werden dann bindend, sofern ein Kunde diese vertraglich einfordert. Einige sind hier aufgeführt:

- ISO/IEC 27000,
- BSI-IT Grundschutz und BSI Standards zur Informationssicherheit,
- CObit (Control Objectives for Information and related Technology),
- 20 Critical Security Controls,
- PCI-DSS (Payment card industry-Data Security Standard),
- IDW PS951/ ISAE3402,
- ISO/IEC 20000,
- ITIL (IT Infrastructure Library)
- …

In der folgenden Grafik ist dargestellt, wie die Anwendungsbereiche der gängigsten Normen aussehen:



Quelle: Andreas J. Henke: Informationssicherheit für KMU (2014)

Die Grafik stellt dar, worauf die jeweilige Norm fokussiert (Personen/Datenbezug, Produkt/Systembezug bzw. Organisationsbezug). Des Weiteren ist dargestellt, ob die Norm eher Regelungen auf der Managementebene trifft (allg. Unternehmensleitlinien) oder mehr auf der technischen Ebene (z.B. Vorgaben für Systemkonfigurationen).

Je nach Anwendungsgebiet fallen Audit zu den jeweiligen Normen/Standards unterschiedlich aus. Ein Audit zu ISO 27000 ist demnach eher prozess- und managementorientiert, mit entsprechend kleinen Stichprobengrößen während beispielsweise eine Prüfung zu PCI DSS sich sehr stark auf technische Sachverhalte konzentriert und hierbei Stichprobenumfänge von 100% angewandt werden. Bei Prüfung eines internen Kontrollsystems (IKS) nach IDW PS 951 durch Wirtschaftsprüfer werden sowohl Prozesse als auch technische Sachverhalte betrachtet, wobei statistisch bestimmte Stichprobengrößen zur Anwendung kommen.

Jetzt stellt sich die Frage, welche Norm bzw. welchen Standard man für seine eigenen Belange wählen soll/muss. Die Entscheidung muss sich an der Art des eigenen Geschäftsmodells und an den Ansprüchen Dritter, die möglicherweise bestehen, orientieren:

- Fordern ggf. Kunden eine spezifische Zertifizierung oder gibt es in Ihrer Branche eine Norm also einen quasi Branchenstandard und/oder einen Wettbewerbsvorteil? Verarbeiten Sie Kreditkartendaten? Wenn Dritte (Geschäftspartner, Gesetzgeber ..) Anforderungen stellen, dann sollte das ökonomisch sinnvollste gewählt werden.

- Sind Sie frei in der Entscheidung, welche Norm/Standard Sie anwenden wollen, so sollten Sie sich die folgenden Fragen stellen: Wo unterliegen Sie einer gewissen

Exposition? Wo liegt das höchste Risiko für Ihren Geschäftszweck? Wie sichern Sie sich am effizientesten und effektivsten ab? (Quelle: Andreas J. Henke)

Drei branchenübliche Normen und Standards, die aufgrund ihres Anwendungsgebiets häufig implementiert und umgesetzt werden, sollen an dieser Stelle vorgestellt werden.

- Ein Zertifikat nach ISO/IEC 27000 ist eine häufige Vertragsanforderung an IT-Provider
- Das Testat nach IDW PS951 wird von Wirtschaftsprüfern erstellt und von den Wirtschaftsprüfern des jeweiligen Kunden bei seiner eigenen Abschlusstestierung benötigt.
- Die Prüfung nach PCI DSS ist für kreditkartenverarbeitende Unternehmen zwingend erforderlich.

Hier eine kleine Gegenüberstellung von Eigenschaften der 3 ausgewählten Standards:

	ISO/IEC 27000	IDW PS951/ISAE3402	PCI-DSS
Betrachtung	Momentaufnahme	Gesamtes Rechnungsjahr	Einmal jährlich (dafür monatliche Vulnerability Scans, einer in 3 Monaten grün)
Stichproben	Willkürlich	Nach statistischen Regeln festgelegt (Vertrauensintervall)	100%
Motivation	Kundenforderung, Gesetzesanforderung	Ausgelagerte oder eigene Rechnungslegung, Gesetzesanforderung	Verarbeitung von Kreditkartendaten, zwingender Branchenstandard
Schwerpunkt auf	Governance und Management	Management und Operations	Management und Operations
Prüfer	Auditoren	Wirtschaftsprüfer	PCI DSS Auditoren
Systeme zur Überprüfung	ISMS (Information security management system) • Aspekt der kontiuierlichen Verbesserung ist Kernpunkt • Strategiefestlegung • Maßnahmen und Rückschau	IKS (Internes Kontrollsystem) Einhaltung von Regelungen wird überprüft.	Mehr Kontrollsystem Weniger Verbesserungspotenzial, da kein Managementsystem dahinter.

	• Wirtschaftlichkeit spielt Rolle		

Fazit

Modelle unterscheiden sich bei ihren Gewichtungen bezüglich Hierarchie und Komponenten

Einzel-Maßnahmen können teils übereinander gelegt werden und sind auf technischer Ebene oft deckungsgleich.

Ein effektives ISMS muss alle Hierarchie-Ebenen abdecken - Governance, Management, Operations und alle Komponenten umfassen - Organisation, Technische Maßnahmen und physische Maßnahmen. (Quelle: Andreas J. Henke)

Was bedeutet das auf Datenbankebene für mich?

Erstmal heißt es Aufwand. Versteht man aber die Hintergründe, warum man all diese Prozesse befolgt oder Richtlinie aufbereiten/schreiben muss.

Eine Organisation muss vor Beginn jeglicher Aktivitäten ein klares Bild über den "Scope" haben, also in der Lage sein, zu definieren, was in die Prüfung einzubeziehen ist. In komplexen IT-Landschaften kann dies eine wahre Herausforderung sein.

Um Transparenz in die Datenbankebene herein zu bringen, ist es wichtig, eine Basis zu schaffen. Diese fängt damit an, dass ein Härtungs- und Administrationskonzept erarbeitet werden muss, inwiefern auf diesem Level verfahren wird. Gibt es bspw. differenzierte Härtungsstufen, wie arbeiten die Datenbankadministratoren nachvollziehbar auf den Datenbanken, etc. pp

Zu beachten ist auch, dass es damit nicht getan ist. Man muss sich auch überlegen wie man mit den Updates (Patchen) verfährt, welche Passwortregeln festgelegt werden müssen und wie mit Ausnahmen und Risikoübertagung umgegangen werden muss. Prozesse, wie Benutzer angelegt oder verwaltet werden, sollten beschrieben sein. Folgende Themen sollten beschrieben sein: Usermanagement (inklusive Passwortmanagement), Patchmanagement, Aufbau und Standards, Administrationskonzept, Härtungskonzept und regelmäßige Checks, Schutzbedarffestellung für eigene Systeme und der Umgang mit Ausnahmen von Härtungsregeln.

Dann beginnt die Umsetzung auf der technischen Ebene. Im Internet gibt es Hilfen, um Härtungsregeln zu erarbeiten. Die BSI IT Grundschutzkataloge oder Benchmarks beim Center of Internet Security geben Anhaltspunkte, wie man Härtungsregeln für seine Zwecke ableiten kann.

Sofern man Kreditkartendaten verarbeitet, gibt es klare Regeln im PCI-DSS Standard nachzulesen: PCI-DSS Version 2.0/3.0

Wichtige Themen spielen eine Rolle:

- Passwortregeln
  - Passwort Verify Funktion → sichere Passwörter
  - Profile einrichten (Reuse Max, Idle Time, Expire Time, Password Lock Time, Failed Login Attempts) und Benutzern zuweisen

- Nachvollziehbarkeit
  - Usermanagement
  - Persönliche Benutzer auf DB-Ebene verteilen
  - Auditing aktivieren
- Minimierung von Privilegien
  - Entfernen von unnötigen Rechten (PUBLIC, DBA …)
- Sicherheitsparameter einstellen
- Minimierung der Komponenten
- Standardeinstellungen ändern

Ausblick:

Deutschland: IT Sicherheitsgesetz Entwurf

Wesentliche Inhalte des Gesetzesentwurfes sind hier widergegeben. Jedoch sind noch einige Fragen offen.

- Die Einführung einer Meldepflicht für KRITIS-Betreiber:
  - Betreiber kritischer Infrastrukturen haben „schwerwiegende Beeinträchtigungen“ ihrer informationstechnischen
  - Systeme, Komponenten oder Prozesse „unverzüglich“ an das BSI zu melden.
- Die Ausweitung der Meldepflicht für Anbieter von Telekommunikationsdiensten und Netzbetreiber an die Bundesnetzagentur (BNetzA):

  - Zusätzlich zu der bestehenden und im Telekommunikationsgesetz81 festgelegten Meldepflicht
  - für Anbieter von Telekommunikationsdiensten und Betreiber von Telekommunikationsnetzen
  - haben diese „Beeinträchtigungen von Telekommunikationsnetzen und -diensten,
  - die zu einer Störung der Verfügbarkeit der über diese Netze erbrachten Dienste oder zu einem
  - unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssystemen der
  - Nutzer oder Teilnehmer führen können und von denen der Netzbetreiber oder der Telekommunikationsdiensteanbieter Kenntnis erlangt, der BNetzA unverzüglich mitzuteilen“.

- Die Ausweitung der Meldepflicht der TK-Diensteanbieter und Netzbetreiber an ihre Nutzer:
    - TK-Anbieter haben Störungen, die von Datenverarbeitungssystemen der Nutzer ausgehen,
    - an diese zu melden und die Nutzer auf angemessene technische Mittel zur Behebung der
    - Störung hinzuweisen.
- Die Einführung von IT-Sicherheitsstandards:
    - Betreiber kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische
    - Sicherheitsstandards erarbeiten, die auf Antrag durch das BSI anerkannt werden können.
- Die Einführung verpflichtender IT-Audits:
    - Betreiber kritischer Infrastrukturen werden verpflichtet, mindestens alle zwei Jahre einen
    - Sicherheitsaudit durchzuführen, um ihre organisatorischen und technischen Vorkehrungen
    - zur IT-Sicherheit überprüfen zu lassen. Die Auditergebnisse werden dem BSI übermittelt

Der Vorstoß, die Verbesserung der IT-Sicherheit der IT in Deutschland wurde wohlwollend aufgenommen, jedoch sind noch viele Dinge zu unklar formuliert und Fragen bleiben offen. Einige Maßnahmen stießen sogar auf heftige Kritik.

Fragen, die offen bleiben sind:

- Welche Unternehmen fallen unter die Regelungen?
- Und damit unter die vorgesehenen Meldepflichten?
- Was ist genau zu melden (Tatbestände)?
- Klärungsbedarf besteht besonders bei Fragestellungen zu möglichen Doppelregulierungen und etwaigen, nicht beabsichtigten Auswirkungen des Gesetzes. Diese sollten ausführlich beleuchtet und wenn möglich beseitigt oder ausgeglichen werden, um eine effiziente und effektive Umsetzung zu gewährleisten

Europa: Europäischen Kommission plant „Richtlinie des europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union“ (kurz Richtlinie zur Informationssicherheit)

(Quelle Studie zum IT Sicherheitsgesetz)

Quellen

Kompass der IT-Sicherheitsstandards

http://www.kompass-sicherheitsstandards.de/Default.aspx

Studie zum IT Sicherheitsgesetz

http://www.bitkom.org/files/documents/Studie_IT-Sicherheit_in_Deutschland_BDI.pdf

PCI DSS

http://de.wikipedia.org/wiki/PCI_DSS

https://www.pcisecuritystandards.org/documents/DSS_and_PA-DSS_Change_Highlights.pdf

https://www.pcisecuritystandards.org/documents/pci_dss_de-de_v2.pdf

Center of Internet Security

http://www.cisecurity.org/

http://benchmarks.cisecurity.org/downloads/show-single/?file=oracle11gr2.100

Präsentation zum Thema Informationssicherheit

http://ajhenke.com/fileadmin/Dokumente/Informationssicherheit_fuer_KMU.pdf

Kontaktadresse:

Angela Espinosa

Lufthansa Systems AG

Am Weiher 24

D-65451 Kelsterbach

Telefon: **+49 (0) 69-696 91904**

E-Mail **angela.espinosa@lhsystems.com**

Internet: **www.lufthansa-systems.com**