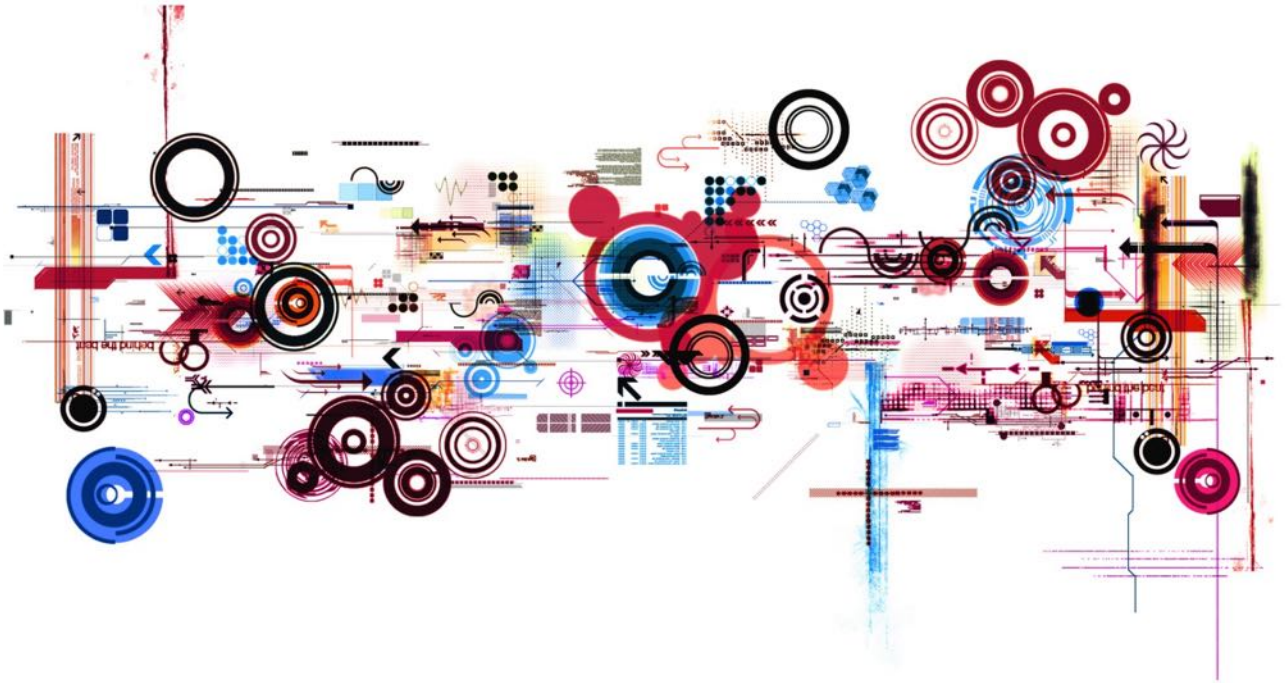
BSI-Grundschutzkatalog als Vertragsbestandteil

und Auswirkungen auf den Vertrag



Referent: Udo Steger
Rechtsanwalt, München

Inhalt

- IT Sicherheit
  - Qualitätsanforderungen
  - Verträge
  - Standards und Best Practices
- Geschichte des IT-Grundschutzkatalogs
- Verhältnis zu den BSI Standards
- Konzept des IT Grundschutzkatalogs
- IT-Sicherheit ≠ Datenschutz
- Aufbau des IT-Grundschutzkatalogs
- Rechtliche und behördliche Anforderungen
- Aufnahme in den Vertrag
- Fazit
- Literatur

IT-Sicherheit:
Das Problem mit den Qualitätsanforderungen

- Die Beurteilung der Qualität von IT-Leistungen ist eines >der< Kernprobleme des IT-Rechts, denn IT-Leistungen sind
  - meist komplex – viele Module, viele Abhängigkeiten von Drittsystemen
  - intransparent für den Anwender – Dokumentation meist nur für Profis verständlich (aber die haben keine Zeit/keine Lust)
  - meist hat man keinen Quellcode (den eh kaum einer versteht)
  - Anwender wollen einfach nur arbeiten, und sich nicht mit IT befassen
  - Messungen oft wenig aussagekräftig, Gefahr von Datenmüll
- Daher bemühen sich fast alle Ersteller von IT-Verträgen darum, irgendwie Regelungen zur Messbarkeit/Qualität zu finden.
- Muss denn etwas geregelt werden?
  - Leistung „mittlerer Art und Güte“, § 243 Abs 1 BGB
  - Rücksicht auf Rechtsgüter des Anderen, § 241 Abs. 2 BGB
  - Erforderliche Sorgfalt, § 276 BGB

- Beobachtung: Bei IT-Sicherheit besteht starkes Bedürfnis der Vertragsparteien nach **Sicherheit im Umgang mit IT-Sicherheit**.

IT-Sicherheit:
Das Problem mit den Verträgen

Häufig wird die geschuldete (Mindest-)Qualität durch Verweise auf „technische Standards“ und „Best Practices“ konkretisiert:

- „(Technischer) Standard“
  - Öffentlich zugängliches technisches Dokument, das auf Ergebnissen aus Wissenschaft und Technik beruht, unter Beteiligung der interessierten Parteien entwickelt wird und deren Zustimmung findet. (ugs. für Normung, vgl. https://de.wikipedia.org/wiki/Normung)
    - Unterscheide „de facto Standard“ (ugs. „Industriestandard“, basiert auf Marktmacht) und „de jure Standard“ (formales Normungsverfahren)
- „Best Practice“
  - Bewährte, optimale oder vorbildliche Methoden, Praktiken oder Vorgehensweisen im Unternehmen, bei denen Verfahren, technische Systeme und Geschäftsprozesse eingesetzt werden, die zumindest auf wesentlichen Arbeitsfeldern Musterbetrieben folgen. (https://de.wikipedia.org/wiki/Best_practice)
- Aber: welche rechtliche Bedeutung kommt dem zu?

IT-Sicherheit:
Das Problem mit den Standards und Best Practices

- „Standards“ und „Best practices“ einfach in den Vertrag als Maßstab für die geschuldete „IT-Sicherheit“ aufnehmen?
  - P: Abstraktheit
    - Standards und „best practices“ zu IT-Sicherheit sind meist abstrakt und immer im konkreten Einsatzszenario zu betrachten (Risikoprofil)
  - P: Fehlende oder schwierige Messbarkeit
    - anders als etwa Service Level oder Hardwareeigenschaften kann „IT-Sicherheit“ kaum gemessen werden
    - Evtl. Reaktionszeit auf Meldungen
  - P: Fehlende Vergleichbarkeit
    - Setzen zwei unterschiedliche Unternehmen die gleichen Standards und „best practices“ um, werden wahrscheinlich unterschiedliche Prozesse und damit Ergebnisse herauskommen

- Immerhin: Verweis auf „Standards“ und „Best practices“ kann Erwartung an Leistung „mittlerer Art und Güte“ konkretisieren.

IT-Grundschutzkatalog: Geschichte

Standards und „Best Practices“ des BSI:

- BSI entwickelte in den 90er Jahren das „IT-Grundschutzhandbuch“ (IT-GSHB)
  - für Behörden und Unternehmen, öffentlich zugänglich
  - soll praxisnahe und handlungsorientierte Hinweise zur Absicherung von IT-Komponenten geben
  - Bis 2004 58 Grundschutzbausteine mit > 700 Maßnahmen geschaffen
- Folge: es entstehen „Standards“ und „Best Practices“

  (Ähnlich ITIL, wurde ab 1989 von der (damaligen) britischen Central Computing and Telecommunications Agency (CCTA) entwickelt)
- 2005 nimmt BSI eine Aufteilung in <u>BSI-Standards</u> einerseits und <u>IT-Grundschutzkataloge</u> andererseits vor.
  - Ziel ist Angleichung an die „IT-Sicherheits“-ISO Norm 27001
  - Die Standardreihe soll entsprechend den internationalen (ISO) Standards den Aufbau eines ISMS (Information Security Management System) als kontinuierlichen Prozess beschreiben.

IT-Grundschutzkatalog: Verhältnis zu den BSI-Standards

- Der IT-Grundschutzkatalog ist eng mit den ebenfalls vom BSI veröffentlichten BSI-Standards 100-1 bis 100-4 verknüpft
  - **BSI-Standard 100-1**: Managementsysteme für Informationssicherheit (ISMS)
    - ohne ISMS sei lt. BSI, Aufbau und Aufrechterhaltung eines hinreichenden Sicherheitsniveaus praktisch nicht möglich
  - **BSI-Standard 100-2:** Grundschutz Vorgehensweise
    - beschreibt, wie ein ITSM in der Praxis aufgebaut und betrieben werden kann.
  - **BSI-Standard 100-3:** Risikoanalyse auf Basis von IT Grundschutz.
  - **BSI-Standard 100-4**: Notfallmanagement
    - Aufbau eines Notfallmanagementsystems

  - BSI-Standards werden (wie IT-Grundschutz) gerade überarbeitet.
    - Community-Drafts der (zukünftigen) BSI-Standards 200-1, 200-2 und 200-3 stehen zur Kommentierung durch die Anwender bereit

IT-Grundschutzkatalog: Das Konzept

„**IT-Grundschutz**“ soll durch Pauschalisierung und Simplifizierung schnell und günstig Basis-Sicherheit zu erreichen, denn;

- die meisten IT-Systeme haben ähnliche, typische Komponenten (z.B. Server und Clients, Betriebssysteme, Router), und
- auf viele Organisationen treffen pauschalisierte Annahmen zu Gefährdungen und Eintrittswahrscheinlichkeiten zu, daher
- kann ein Bündel von Standard-Sicherheitsmaßnahmen mit konkreten Umsetzungshinweisen die IT-Sicherheit deutlich verbessern („Good enough“ vs. „perfekt“)
- Vorteile:
  - ökonomisch, da Übernahme praxiserprobter Konzepte erfolgt
  - kompakte Dokumentation, gemeinsames Vokabular, durch Verweis auf Referenzquelle (ähnlich ITIL)
  - Erweiterbarkeit und Aktualisierbarkeit

Soweit die Theorie…

IT-Sicherheit ≠ Datenschutz

- IT-Sicherheit und Datenschutz bedingen einander und haben zumindest teilweise die gleiche Wirkrichtung.
  - Eine datenschutzrechtlich bedenkliche Weitergabe von Daten kann „IT-sicherheitlich“ einwandfrei sein
- IT-Sicherheit umfasst auch Maßnahmen, die keinen unmittelbaren Bezug zum Datenschutz haben
  - z.B. Brandschutz
- Datenschutz umfasst auch Maßnahmen, die keinen unmittelbaren Bezug zur IT-Sicherheit haben
  - z.B. Zweckgebundenheit, Auskunftsrechte
- Richtig ist, dass es eine große Schnittmenge von Maßnahmen, gibt, die sowohl für IT-Sicherheit als auch Datenschutz relevant sind.
  - TOMS nicht mit IT-Sicherheitskonzept verwechseln.

Aufbau des IT-Grundschutzkatalogs: Kataloge, Kataloge…

Die letzte 15. EL des IT-Grundschutzkatalogs beschreibt **2746 Maßnahmen auf 5082 Seiten**, unterteilt in

Bausteinkatalog:

- Je Baustein Beschreibung des in diesem Baustein betrachteten typischen Prozesses, IT-Systems oder der typischen Anwendung
- Überblick über die Gefährdungslagen und die Maßnahmenempfehlungen
- Für Gefährdungslagen und Maßnahmen werden hierbei Verweise in den Gefährdungskatalog und den Maßnahmenkatalog vorgenommen.

Gefährdungskatalog:

- Ausführliche Beschreibung der im Bausteinkatalog genannten Gefährdungslagen

Maßnahmenkatalog:

- Ausführliche Schilderung der in den anderen Bausteinen zitierten Sicherheitsmaßnahmen

Aufbau des IT-Grundschutzkatalogs: Inhalt der Kataloge

Bausteinkatalog (427 Einträge, B x.xxx)

- Übergreifende Aspekte (1.1 – 1.18)
- Infrastruktur (2.1 – 2.12)
- IT-Systeme (3.1 – 3.407)
- Netze (4.1 – 4.8)
- Anwendungen (5.1 – 5.27)

Gefährdungskatalog (710 Einträge, G x.xxx)

- Elementare Gefährdungen (0.1 – 0.46)
- Höhere Gewalt (1.1 – 1.19)
- Organisatorische Mängel (2.1 – 2.214)
- Menschliche Fehlhandlungen (3.1 – 3. 124)
- Technisches Versagen (4.1 – 4.101)
- Vorsätzliche Handlungen (5.1 – 5.206)

Maßnahmenkatalog (1609 Einträge, M x.xxx)

- 1. Infrastruktur (1.1 – 1.81)
- 2. Organisation (2.1 – 2.587)
- 3. Personal (3.1 – 3.98)
- 4. Hardware und Software (4.1 – 4.500)
- 5. Kommunikation (5.1 . 5.177)
- 6. Notfallvorsorge (6.1 – 6.166)

IT-Grundschutz-Kat
aloge 2016 EL15 DE

Aufbau des IT-Grundschutzkatalogs: Klassiker (Beispiel: GSHB Stand 07/1999)

Anrufbeantworter

8.3 Anrufbeantworter

Beschreibung

Betrachtet werden Anrufbeantworter, die zusätzlich zum Telefon an das lokale Haus-Telefonnetz angeschlossen werden können. Sie dienen üblicherweise der Aufzeichnung eingehender Gespräche oder Nachrichten in gesprochener Form, wenn der Angerufene nicht erreichbar ist. Technisch unterscheiden sich diese Geräte durch unterschiedliche Aufzeichnungsweisen: vollständig analog aufzeichnende Geräte, vollständig digital aufzeichnende Geräte und Kombinationsformen. Insbesondere das heute verbreitete Leistungsmerkmal der Fernabfrage legt es nahe, Anrufbeantworter als IT-System aufzufassen, ein erhebliches Gefährdungspotential darstellen kann.

Gefährdungslage

Für den IT-Grundschutz eines Anrufbeantworters werden folge angenommen:

Höhere Gewalt:
- G 1.8 Staub, Verschmutzung

Organisatorische Mängel
- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.5 Fehlende oder unzureichende Wartung
- G 2.6 Unbefugter Zutritt zu schutzbedürftigen Räumen

Menschliche Fehlhandlungen:
- G 3.15 Fehlbedienung eines Anrufbeantworters

Technisches Versagen:
- G 4.1 Ausfall der Stromversorgung
- G 4.18 Entladene oder überalterte Notstromversorgung im A
- G 4.19 Informationsverlust bei erschöpftem Speichermedium

Vorsätzliche Handlungen:
- G 5.36 Absichtliche Überlastung des Anrufbeantworters
- G 5.37 Ermitteln des Sicherungscodes
- G 5.38 Missbrauch der Fernabfrage

Maßnahmenempfehlungen

Zur Realisierung des IT-Grundschutzes wird empfohlen, die not ("Bausteine") wie in Kapitel 2.3 und 2.4 beschrieben auszuwählen.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Anrufbeantw

IT-Grundschutzhandbuch: Stand Juli 1999

Maßnahmenkatalog Organisation M 2.160 Bemerkungen

M 2.160 Regelungen zum Computer-Virenschutz

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT

Um einen effektiven Computer-Virenschutz zu erreichen, müssen über den Einsatz von Computer-Viren-Suchprogrammen hinaus einige zusätzliche Maßnahmen realisiert werden. In diesem Sinne sind unter anderem folgende Punkte zu regeln:

Einsatz von Computer-Viren-Suchprogrammen

Entsprechend der ausgewählten Strategie und des ausgewählten Produktes ist der Einsatz festzulegen und zu dokumentieren (vgl. M 2.156 *Auswahl einer geeigneten Computer-Virenschutz-Strategie*, M 2.157 *Auswahl eines geeigneten Computer-Viren-Suchprogramms*). Darüber hinaus ist zu regeln, wie, in welchen Abständen und durch wen die Computer-Viren-Suchprogramme aktualisiert werden (vgl. M 2.159 *Aktualisierung der eingesetzten Computer-Viren-Suchprogramme*).

Schulung der IT-Benutzer

Die betroffenen IT-Benutzer sind bezüglich der Gefahren durch Computer-Viren, Makro-Viren, Trojanische Pferde und Hoax (vgl. G 5.23 *Computer-Viren*, G 5.43 *Makro-Viren*, G 5.21 *Trojanische Pferde*, G 5.80 *Hoax*), der notwendigen IT-Sicherheitsmaßnahmen, der Verhaltensweise beim Auftreten von Computer-Viren und im Umgang mit dem Computer-Viren-Suchprogramm zu informieren bzw. zu schulen (vgl. M 3.5 *Schulung zu IT-Sicherheitsmaßnahmen*, M 3.4 *Schulung vor Programmnutzung*, M 6.23 *Verhaltensregeln bei Auftreten eines Computer-Virus*).

Verbot der Nutzung nicht freigegebener Software

Die Installation und Nutzung nicht freigegebener, insbesondere nicht virenkontrollierter Software ist zu verbieten (vgl. M 2.9 *Nutzungsverbot nicht freigegebener Software*). Darüber hinaus ist ggf. zu regeln, dass regelmäßig Prüfungen auf Einhaltung des Verbots durchgeführt werden (vgl. M 2.10 *Überprüfung des Software-Bestandes*).

Schutzmaßnahmen am IT-System

Die Boot-Reihenfolge beim Betriebssystemstart ist so umzustellen, dass generell zuerst von der Festplatte (oder vom Netz) und dann erst von einem externen Medium (Diskette, CD-ROM) gestartet wird (vgl. M 4.84 *Nutzung der BIOS-Sicherheitsmechanismen*). Zusätzlich ist für jeden vorhandenen Rechnertyp eine Notfalldiskette anzulegen, um im Falle einer Computer-Vireninfektion eine erfolgreiche Säuberung zu ermöglichen (vgl. M 6.24 *Erstellen einer PC-Notfalldiskette*). Für den Fall, dass ein neuer Computer-Virus dennoch Schäden verursacht, muss auf eine Datensicherung zurückgegriffen werden. Es sind daher regelmäßig Datensicherungen anzulegen (vgl. M 6.32 *Regelmäßige Datensicherung*). Beim Wiedereinspielen von Datensicherungen muss darauf geachtet werden, dass damit keine vom Computer-Virus befallenen Dateien wiederaufgespielt werden.

IT-Grundschutzhandbuch: Stand Juli 1999 1101

/Software M 4.78 Bemerkungen

ge Durchführung von Konfigurations-gen

ng: IT-Sicherheitsmanagement, Leiter IT

ng: Administrator

derungen an einem IT-System im Echtbetrieb ist tufen und entsprechend sorgfältig muss hierbei

System begonnen wird, muss als erstes die alte erden, so dass sie schnell verfügbar ist, wenn nfiguration auftreten.

en müssen die Benutzer rechtzeitig über die sarbeiten informiert werden, damit sie zum einen weise Systemabschaltung einrichten können, und nach Änderungen auftretende Probleme richtig

gen sollten immer nur schrittweise durchgeführt ollte immer wieder überprüft werden, ob die geführt wurden und das IT-System sowie die noch lauffähig sind.

ystemdateien ist anschließend ein Neustart prüfen, ob sich das IT-System korrekt starten lässt. für einen Notstart benötigten Datenträger vorrätig ten, Start-CD-ROM.

nsänderungen sollten möglichst nicht in den nmen werden, sondern in Kopien. Alle n sollten von einem Kollegen überprüft werden, übernommen werden.

hohen Verfügbarkeitsanforderungen ist auf ifen bzw. zumindest ein eingeschränkter IT-Betrieb rgehen kann sich dabei idealerweise nach dem

igurationsänderungen sollten Schritt für Schritt ei auftretenden Problemen das IT-System durch Änderungen wieder in einen lauffähigen Zustand e auch M 2.34 *Dokumentation der Veränderungen m*).

rungen schrittweise dokumentiert?

gen nachträglich rückgängig machen?

uli 1999 1668

Aufbau des IT-Grundschutzkatalogs: Modernes (Beispiel: GS-Kat Stand 15. EL 2016)

Maßnahmenkatalog Notfallvorsorge

M 6.160 Notfallvorsorgekonzept Umgebungen

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter
Verantwortlich für Umsetzung: IT-Sicherheitsbeauftragter

Fällt in einer serviceorientierten Architektur (SOA) zum B vice-Provider aus, kann sich das schwerwiegend auf die Ges einer Institution auswirken. Dann geht es darum, schnellstm nungsgemäßen Betrieb wieder aufzunehmen und geeignete S nahmen durchzuführen. Unter Berücksichtigung des übergre managements (siehe B 1.3 *Notfallmanagement* sowie M 6.8 *ge beim Outsourcing*) ist ein geeignetes Notfallvorsorgekonze gebungen zu erstellen. Dafür sollten zunächst alle möglicher siert, bewertet und zusammen mit den jeweiligen Sicherheitsm kumentiert werden.

Da in SOA-Umgebungen mitunter besondere Bedingungen vo diese auch im Konzept berücksichtigt werden. So ist beispiels die Verfügbarkeit sicherzustellen, sondern auch periodisch zu Dienste noch berechtigt registriert sind. Unberechtigte Diens zeichnis zu löschen.

Zudem sollte ein Betriebshandbuch erarbeitet werden, das a trieb in einem Business Continuity Plan regelt. Es berücksichtig heiten einer SOA-Umgebung, analysiert die Risiken für das E wiegender Schäden und enthält Empfehlungen zu Notfallmaß

Prüffragen:

- Gibt es ein Notfallvorsorgekonzept für SOA-Umgebungen?

IT-Grundschutz-Kataloge: 15. EL Stand 2016

Maßnahmenkatalog Organisation M 2.37

M 2.37 Der aufgeräumte Arbeitsplatz

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter Organisation
Verantwortlich für Umsetzung: Mitarbeiter

Jeder Mitarbeiter sollte dazu angehalten werden, seinen Arbeitsplatz "aufgeräumt" zu hinterlassen. IT-Benutzer müssen dafür sorgen, dass Unbefugte keinen Zugang zu IT-Anwendungen oder Zugriff auf Daten erhalten. Alle Mitarbeiter müssen mit der gleichen Sorgfalt ihre Arbeitsplätze überprüfen und sicherstellen, dass keine sensiblen Informationen frei zugänglich sind und die Verfügbarkeit, Vertraulichkeit oder Integrität von Daten nicht negativ beeinflusst werden kann. Es darf nicht möglich sein, dass Unbefugte auf Datenträger (wie Disketten, USB-Sticks oder Festplatten) oder Unterlagen (z. B. Ausdrucke) zugreifen können.

Für eine kurze Abwesenheit während der Arbeitszeit ist es ausreichend, den Raum, sofern möglich, zu verschließen und/oder den Bildschirm so zu sperren, dass Zugriffe nur nach erfolgreicher Authentisierung möglich sind. Bei geplanter Abwesenheit eines Mitarbeiters (z. B. längere Besprechungen, Dienstreisen, Urlaub, Fortbildungsveranstaltungen) ist der Arbeitsplatz so aufzuräumen, dass keine schutzbedürftigen Datenträger oder Unterlagen unverschlossen am Arbeitsplatz zurückgelassen werden. Dafür benötigen die Mitarbeiter ausreichend dimensionierte und verschließbare Staumöglichkeiten, wie z. B. stabile Schränke.

Auch Passwörter dürfen auf keinen Fall sichtbar (als Klebezettel am Monitor, an einem leicht zu erratenden Ort wie z. B. unter der Schreibtischauflage oder in der unverschlossenen Schreibtischschublade) aufbewahrt werden (siehe M 2.2 *Betriebsmittelverwaltung*). Ebenfalls sollten eindeutige Hinweise (z. B. Namen von Familienangehörigen oder sogenannte Trivialpasswörter wie aufeinanderfolgende Buchstaben und Zahlen) für das schnelle Erraten ausgeschlossen werden (siehe M 2.11 *Regelung des Passwortgebrauchs*).

Vorgesetzte und Mitarbeiter des Sicherheitsmanagements sollten sporadisch Arbeitsplätze überprüfen, ob dort schutzbedürftige Informationen offen zugreifbar sind und die Mitarbeiter auf korrektes Aufräumen hinweisen.

Prüffragen:

- Wurden alle Mitarbeiter darauf hingewiesen, dass an unbeaufsichtigten Arbeitsplätzen keine sensiblen Informationen frei zugreifbar sein dürfen?
- Werden Arbeitsplätze stichprobenartig kontrolliert, ob schutzbedürftige Informationen offen zugreifbar sind?

IT-Grundschutz-Kataloge: 13. EL Stand 2013 1559

Schicht Übergreifende Aspekte B 1.17

B 1.17 Cloud-Nutzung

Beschreibung

Mit Cloud Services nutzen Institutionen die Möglichkeit, IT-Infrastrukturen (zum Beispiel Rechenleistung, Speicherkapazitäten), IT-Plattformen (zum Beispiel Datenbanken, Applikations-Server) oder IT-Anwendungen (zum Beispiel Auftragssteuerung, Groupware) nach ihren spezifischen Bedürfnissen als Dienst über ein Netz zu beziehen. Dabei kann die Leistung sowohl in den Räumlichkeiten des Auftraggebers als auch bei einem externen Cloud-Diensteanbieter erbracht werden.

Die so ermöglichte bedarfsgerechte, skalierbare und flexible Nutzung von IT-Diensten wird unterstützt durch neuartige Geschäftsmodelle, bei denen die Abrechnung je nach Funktionsumfang, Nutzungsdauer und Anzahl der Benutzer erfolgen kann.

Nicht zuletzt aufgrund der genannten Eigenschaften erfreut sich Cloud Computing (zu Definitionen etc. siehe M 4.462 *Einführung in die Cloud-Nutzung*) bereits seit einigen Jahren wachsender Beliebtheit. Zahlreiche Studien belegen die steigende Nachfrage nach Cloud Services und prognostizieren diese auch für zukünftige Jahre.

In der Praxis zeigt sich jedoch häufig, dass die Vorteile, die sich Institutionen von der Cloud-Nutzung erwarten, oftmals nicht vollständig zum Tragen kommen, weil die diesbezüglich wichtigsten kritischen Erfolgsfaktoren nicht ausreichend betrachtet worden sind. Den nachfolgenden Aspekten kommt im Zusammenhang mit der Cloud-Nutzung durch Institutionen besondere Bedeutung zu:

- Strategische Planung des Einsatzes von Cloud-Diensten
- Sorgfältige Definition und Vereinbarung von (Sicherheits-)Anforderungen
- Sorgfältige Definition der Verantwortung und Schnittstellen, sowohl innerhalb einer Institution als auch nach außen
- Bewusstsein für ein erforderliches geändertes Rollenverständnis, sowohl aufseiten der IT als auch aufseiten der Anwender

Zusätzlich spielt im Zuge der Einführung von Cloud Services eine Reihe von Governance-Themen eine wichtige Rolle. Beispiele hierfür sind die Umsetzung von Mandantenfähigkeit, die Vertragsgestaltung, die Sicherstellung von Portabilität unterschiedlicher Services, die Abrechnung genutzter Service-Leistungen, das Monitoring der Service-Erbringung, das Sicherheitsvorfallmanagement und zahlreiche Datenschutz-Aspekte.

Thematische Abgrenzung

Im Sinne der IT-Grundschutz-Vorgehensweise umfasst Cloud-Nutzung alle Aspekte, die zur Nutzung einer Cloud-Umgebung erforderlich sind. Damit schließt Cloud-Nutzung insbesondere sowohl die Anwendung des Cloud Services durch Mitarbeiter der nutzenden Institution als auch die Administration des Cloud Services durch einen Cloud-Service-Administrator aufseiten der nutzenden Institution ein.

Ziel des vorliegenden Bausteins ist, Empfehlungen für die sichere Nutzung von Cloud-Diensten zu geben. Er richtet sich daher an alle Institutionen, die bereits Cloud Services in Anspruch nehmen oder deren zukünftigen Einsatz planen. Die Gefährdungen und Maßnahmen des Bausteins gelten dabei grundsätzlich unabhängig vom genutzten Service- und Bereitstellungsmodell.

Der Baustein ist so konzipiert, dass er immer auf einen konkreten Cloud Service anzuwenden ist. Nutzt eine Institution einen Verbund von Cloud Services, so ist jeder einzelne Service mithilfe des Bausteins zu modellieren (siehe M 2.545 *Modellierung der Cloud-Nutzung*). Die entstehende Schnittstelle zwischen den unterschiedlichen Services ist ebenfalls Gegenstand des Bausteins. Sie muss für alle Services betrachtet werden.

IT-Grundschutz-Kataloge: 14. EL Stand 2014 165

Aufbau des IT-Grundschutzkatalogs: Einige Beobachtungen

- Für „IT-Systeme“ und „Hard- und Software“ sind ca. 900 Maßnahmen vorgesehen
- Die weitaus meisten Maßnahmen befassen sich mit Organisation und organisatorischen Mängeln, und menschlichem Versagen
- Für typisierte Gefährdungslagen werden konkrete Einzelmaßnahmen angeboten
  - Anwender wird m.E. trotzdem fachkundige Unterstützung brauchen
- Im Grundschutzkatalog selbst keine Hilfestellung für
  - Aufbau eines ISMS
  - für Analyse des unternehmenseigenen Risikos und eines ggf. gesteigerten Sicherheitsbedarfs
  - Dazu sind **BSI-Standards** vorgesehen
- Umweltrisiken/höhere Gewalt/Notfälle scheinen weniger eine Rolle zu spielen
  - Notfallmanagement: BSI 100-4

Aufbau des IT-Grundschutzkatalogs: Einige Beobachtungen

- IT-Sicherheit ist v.a. ein organisatorisches Thema (ISMS).
  - IT-Systeme an sich sind scheinbar nicht (mehr) so wichtig.
- Eine organisatorische Maßnahme wie ein ISMS ist meist schwerer einzuführen, und fehleranfälliger, als der Kauf neuer IT-Systeme zu kaufen.
  - Auch wenn die Anbieter das glauben machen: nur kaufen reicht nicht
- ISMS verbessert IT-Sicherheit, führt aber (auch) zu Bürokratie
- IT-Sicherheit ist ein Prozess, den ein ISMS steuert
  - es gibt kein festes Ziel, welches erreicht werden kann
  - Aber: gibt das Unternehmen mittels einem BSI-basierten Regelwerk Maßnahmen zur IT-Sicherheit vor, fällt der Nachweis von Pflichtverletzungen eines Dienstleisters (etwas) leichter

IT-Grundschutzkatalog in der Rechtspraxis: Muss das alles sein?

Allgemeine rechtliche Anforderungen:

- §91 Abs. 2 AktG: Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.
  - Mangelnde IT-Sicherheit kann existenzgefährdend sein
- Grundsätze ordnungsgemäßer Buchhaltung: Vorsichtsprinzip, ungenau bezifferbare Bestände sollten pessimistisch eingeschätzt und Risiken berücksichtigt werden.
  - Mangelnde IT-Sicherheit ist ein Risiko
- Basel II: Banken prüfen vor einer Kreditvergabe das (IT) Risikomanagement

Aber es geht auch konkreter…

IT-Grundschutzkatalog in der Rechtspraxis: Rechtliche und behördliche Anforderungen im Überblick

- Min-dest-an-for-de-run-gen an das Ri-si-ko-ma-na-ge-ment von Banken (Ma-Risk)
- § 25a KWG, § 22 ZAG
- Mindestanforderungen an das Risikomanagement von Kapitalverwaltungsgesellschaften (KAMaRisk)
- Bestimmungen über die Mindestanforderungen für den Einsatz automatisierter Verfahren im Haushalts-, Kassen- und Rechnungswesen des Bundes (BestMaVB-HKR)
- § 20a Finanzverwaltungsgesetz (FVG)
- Ausschreibungen
- Informationssicherheitsleitlinie für die Hessische Landesverwaltung
- Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik (IuK-Mindestanforderungen 2016)

IT-Grundschutzkatalog in der Rechtspraxis: Bankenaufsicht

- **Min-dest-an-for-de-run-gen an das Ri-si-ko-ma-na-ge-ment von Banken (Ma-Risk)** - BaFin-RS 10/2012 (BA) vom 14.12.2012
  - Gilt für deutsche Kreditinstitute und Finanzdienstleistungsinstitute
    - In der bisherigen Praxis wendet die BaFin die Grundsätze der MaRisk, etwa zu IT oder zum Outsourcing, faktisch auch bei Zahlungsdienstleistern an
  - MaRisk ist prinzipienorientiert ausgerichtet:
    - Vorgabe eines Ergebnisses (IT-Sicherheit), und wie dieses Ziel erreicht wird, bleibt den Instituten selbst überlassen
    - Bei IT-Sicherheit: Prinzipien der Sicherstellung der Integrität, Verfügbarkeit, Authentizität und Vertraulichkeit der Daten (ähnlich Anlage zu § 9 BDSG).
  - AT 7.2, Nr. 2: „*…bei der Ausgestaltung der IT-Systeme und der zugehörigen IT-Prozesse* [ist] *grundsätzlich auf gängige Standards abzustellen.*“ „*Zu solchen Standards zählen z.B. der IT-Grundschutzkatalog des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der internationale Sicherheitsstandard ISO/IEC 2700x der International Standards Organization.*“ (Erläuterung der BaFin)
    Neue MaRisk wird (zusammen mit BAIT) seit Mitte 2017 erwartet

IT-Grundschutzkatalog in der Rechtspraxis: Banken, Zahlungsdienste

Aus **§ 25a KWG** ergibt sich mittelbar die Notwendigkeit für beaufsichtigte Institute, über ein ISMS zu verfügen:

- *„Eine ordnungsgemäße Geschäftsorganisation muss insbesondere ein angemessenes und wirksames Risikomanagement umfassen, auf dessen Basis ein Institut die Risikotragfähigkeit laufend sicherzustellen hat; das Risikomanagement umfasst insbesondere:*
  […]
  4. eine angemessene personelle und technisch organisatorische Ausstattung des Instituts;“

Ebenso aus **§ 22 Abs. 1 ZAG** für Zahlungsdienste:

- *Ein Institut muss über eine ordnungsgemäße Geschäftsorganisation verfügen. … [Diese] umfasst insbesondere*
  […]
  4. … ein angemessenes Risikomanagement und angemessene Kontrollmechanismen sowie Verfahren und Datenverarbeitungssysteme,…

IT-Grundschutzkatalog in der Rechtspraxis: Weitere Finanzbranche

- **Mindestanforderungen an das Risikomanagement von Kapitalverwaltungsgesellschaften (KAMaRisk)** - BaFin-RS 01/2017 vom 10.01.2017
  - gilt für Kapitalanlagegesellschafen i.S.d. § 1 KAG, löst ehem. „InvMaRisk“ ab (BaFin-RS 5/2010 vom 30.06.2010)
  - konkretisiert bestimmte Vorgaben der „Delegierten Verordnung zur AIFM-Richtlinie“ zur Organisation, zum Risikomanagement sowie zur Auslagerung bei Kapitalverwaltungsgesellschaften.
  - Ziff. 8.1 Nr. 3: „*…bei der Ausgestaltung der IT-Systeme und der zugehörigen IT-Prozesse* [ist] *grundsätzlich auf gängige Standards abzustellen.*“ „*Zu solchen Standards zählen z. B. der IT-Grundschutzkatalog des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der internationale Sicherheitsstandard ISO/IEC 27002 der International Standards Organization.*“ (Erläuterung der BaFin)
  - (fast wortgleich zur MaRisk)

IT-Grundschutzkatalog in der Rechtspraxis: Betrieb von IT-Systemen des Bundes

- Bestimmungen über die **Mindestanforderungen für den Einsatz automatisierter Verfahren** im Haushalts-, Kassen- und Rechnungswesen des Bundes (BestMaVB-HKR)

  - *„(1) Beim Einsatz eines automatisierten Verfahrens im Haushalts-, Kassen und Rechnungswesen des Bundes dürfen nur dokumentierte, hinreichend getestete und freigegebene Programme eingesetzt werden. Dabei müssen die Empfehlungen des IT-Grundschutz-Katalogs des Bundesamtes für Sicherheit in der Informationstechnik und notwendige Maßnahmen vor Einführung des Verfahrens bereits umgesetzt worden sein (z. B. IT-Sicherheitskonzept einschließlich Zugangs- und Zugriffskontrollen, Betriebshandbuch, ggf. Datenschutzkonzept, Freigabeprozess usw.).“*
    (Stand 01/2017)

IT-Grundschutzkatalog in der Rechtspraxis: Auslagerung von IT-Leistungen des Bundes

- **§ 20a Finanzverwaltungsgesetz (FVG)** - Druckdienstleistungen für Bundesfinanzbehörden
  - Neue Fassung zum 25.05.2018:*(1) Das Bundesministerium der Finanzen darf sich zum Drucken und Kuvertieren von schriftlichen Verwaltungsakten … nur dann einer nicht öffentlichen Stelle als Auftragsverarbeiter … im Rahmen eines Vertrages bedienen, wenn… […]*
    (5) der Auftragsverarbeiter im Rahmen der Artikel 25 und 32 der Verordnung (EU) 2016/679 [DS-GVO] ein vom Bundesministerium der Finanzen freizugebendes IT-Sicherheitskonzept nach dem Standard des aktuellen IT-Grundschutzkatalogs des Bundesamtes für Sicherheit in der Informationstechnik erstellt hat,…“

IT-Grundschutzkatalog in der Rechtspraxis: Bestandteil von Ausschreibungen

Lastenheft: Software für Museum-Kino-Verwaltung-Shop

deutsches filminstitut filmmuseum

2.3.4 Information Security/Datenschutz (NA-I)

⇒NA-I01: Die Basis aller Anforderungen an die Systemsicherheit bilden die IT-Grundschutzkataloge des BSI. Insbesondere die Anforderungen des Bausteins B5 MÜSSEN vom Anbieter mit der neuen Software erfüllt werden. Das Zielsystem DARF NICHT im Widerspruch zu einer Anforderung aus dem IT-Grundschutzkatalog stehen.⇐

Folgende weiteren Dokumente gelten als Bestandteile dieser Ausschreibung, falls es sich bei der Software um eine Webanwendung handelt:

- Bundesamt für Sicherheit in der Informationstechnik: „Sicherheit von Webanwendungen", (Maßnahmenkatalog und Best Practices)
- Bundesamt für Sicherheit in der Informationstechnik: „Leitfaden zur Entwicklung sicherer Webanwendungen", Empfehlungen und Anforderungen an die Auftragnehmer (2013)
- Bundesamt für Sicherheit in der Informationstechnik: „Sicheres Bereitstellen von Web-Angeboten (ISi-Web-Server)" (BSI-Studie zur Internet-Sicherheit (ISi-S))

(Ausschreibung „Software für Museum-Kino-Verwaltung-Shop" vom 1.3.2017)

Verhandlungsverfahren
„Lieferung von Hardware und Dienstleistungen", VV RE2/2150/12

Vergabeunterlagen

Teil B – Leistungsbeschreibung

1.2 Qualitätsmanagement und IT-Sicherheit

Dataport leistet prozessorientiertes IT-Servicemanagement für Betrieb und Support und richtet sich dabei nach dem De-facto-Standard für Gestaltung, Implementierung und Management von Serviceprozessen, der „IT Infrastructure Library" (ITIL).

Dataport ist verpflichtet, gemäß BSI Grundschutz zu arbeiten (Bundesamt für Sicherheit in der Informationstechnologie). Dies gilt auch für den zukünftigen Vertragspartner.

(Ausschreibung Dataport Rahmenvertrag 2012)

IT-Grundschutzkatalog in der Rechtspraxis: Standards der Verwaltung

Informationssicherheitsleitlinie für die Hessische Landesverwaltung

- *„Die Regelungen der Informationssicherheitsleitlinie orientieren sich sowohl an den GrundschutzStandards und der Grundschutzkataloge des BSI sowie der Informationssicherheitsleitlinie des Bundes und der Länder als auch an den internationalen Normen DIN ISO/IEC 27001ff.“*
  (Stand: 2016)

Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik (IuK-Mindestanforderungen 2016), Juni 2016

- *„Die IuK-Mindestanforderungen basieren auf den Prüfungserkenntnissen der Rechnungshöfe des Bundes und der Länder. Sie schaffen gemeinsame und transparente Prüfungsmaßstäbe.“*
- Enthalten mehrere Verweise auf IT-Grundschutzkatalog

IT-Grundschutzkatalog:
Das Problem mit den Aufnahme in den Vertrag

Verweis auf IT-Grundschutzkatalog im Vertrag kann weitreichende Folgen haben:

- Prozesse bei Auftraggeber/Auftragnehmer können unterschiedlich sein, u.U. aufwendige Anpassung nötig
- unterschiedliches Verständnis der Parteien bei Umsetzung der BSI-Standards und der IT-Grundschutzkatalog-Maßnahmen
- Abhängigkeit von externem Standard und dem Herausgeber BSI
  - Wie geht man mit Änderungen wie z.B. neue Version um?
  - Wer trägt Kosten für Änderungen von Leistungen/Prozessen, wenn sich BSI Standard/IT-Grundschutzkatalog ändert? Was soll gelten:
    - Risiko ist nicht vom Anbieter beeinflussbar, Kunde zahlt, oder
    - Shared risk – jeder betroffene Kunde trägt einen Anteil, oder
    - Anbieter trägt, da für Marktfähigkeit der Leistungen essentiell
- Was ist, wenn Aktualisierung durch BSI auf sich warten lässt?
  - Schnellebige IT-Branche, IT-Sicherheitsbranche

IT-Grundschutzkatalog: Das Problem mit den Aufnahme in den Vertrag

In der Praxis ist aber immer öfters zu beobachten:

- IT-Grundschutzkatalog Teil des Vertragsentwurfs oder in den Ausschreibungsunterlagen gefordert
  - In manchen Sektoren Pflicht (s.o., BaFin)
  - P: Durchreichen der Pflichten an Unterauftragnehmer
  - Nutzerhinweise EVB-IT System verweisen auf IT-Grundschutzkatalog
    - daher u.U. auch relevant, wenn gar nicht ausdrücklich in Ausschreibung erwähnt
- P: nationaler BSI Standard vs. internationale Anbieter, int. Normen, int. Zertifikate
  - „Mapping“ etwa von ISO 2700x Anforderungen auf IT-Grundschutzkatalog kann eine Herausforderung sein
- P: gesetzgeberischer und regulatorischer „run“ auf IT-Sicherheit
  - IT-Sicherheitsgesetz, NIS Richtlinie, EU DS-GVO, …
  - (nur Bankenaufsicht:) MaRisk 2017, BAIT, EBA RTS
  - zunehmende „prinzipienorientierte“ Regulierung lässt Betroffene ratlos

Fazit und Thesen

- IT-Grundschutzkatalog sind mittlerweile in vielen Sektoren Pflicht
  - Ähnlich wie bei ITIL entscheidet das „wie“ der organisatorischen Umsetzung, und die kann grundverschieden sein
- „Moderne“ Standards wie ISO 2700x sind stärker prinzipienorientiert, belassen Verantwortung für das „wie“ der Umsetzung beim Anwender
  - Überfordert aber KMUs, oft nur für Großunternehmen gut umsetzbar
  - IT-Grundschutzkatalog trotz seines Umfangs wertvoll für KMUs
  - Gefahr der Abhängigkeit von (IT-Sicherheits-)Beratern
- „Run auf IT-Security“ erhöht Gefahr von redundanten oder widersprüchlichen Anforderungen
- Auswirkungen auf Verträge individuell prüfen
  - Passen die Vorstellungen der Parteien zur IT-Sicherheit zusammen?

Literatur

- IT-Grundschutzkatalog: Download
- BSI Standards: Download
- **Timm, Haiko**, „IT-Sicherheit in Banken – Anspruch und Wirklichkeit“, in: Kreditwesen 2013, Ausgabe Technik Nr. 2, 9-11
- **Lensdorf, Mayer-Wegelin**, „Die Bedeutung von Standards und Best Practices beim Schutz personenbezogener Daten“, in: CR 2009, 545

Vielen Dank!

Udo Steger
Rechtsanwalt / Partner

Aderhold Rechtsanwaltsgesellschaft mbH
Wagmüllerstraße 23
80538 München
Tel.: +49 (89) 306683-270
E-Mail: u.steger@aderhold-legal.de

Follow me:

@LinkedIn: https://de.linkedin.com/in/usteger
@XING: https://www.xing.com/profile/Udo_Steger
@Twitter: @usteger
@Blog: www.paytechlaw.com