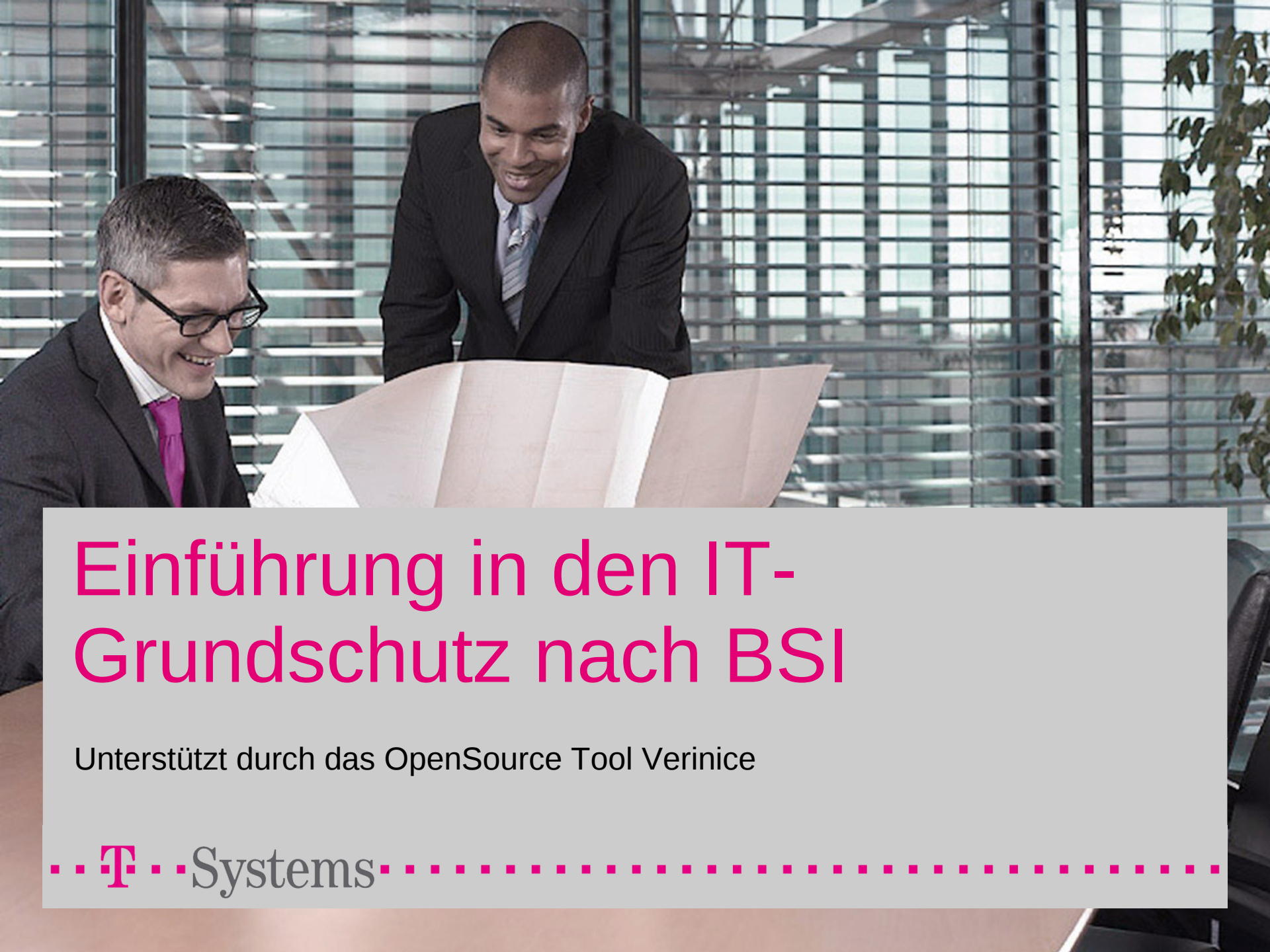


Einführung in den IT-Grundschutz nach BSI

Unterstützt durch das OpenSource Tool Verinice

T Systems

Robert M. Albrecht

T-Systems Enterprise Services GmbH
- Senior Experte für technische Infrastruktur

- www.FedoraProject.org
  - Ambassador: Messen, Veranstaltungen, Marketing, ...
  - Packager & QA: Nagios & PlugIns, usb_modeswitch, …

- 30 Bücher, internationale Übersetzungen, Zeitschriften-Artikel
- Mein erster Linux-Kernel lief unter Minix

Unsere IT-Sicherheit ist spitze.
Wir haben viel Geld für unsere Firewall ausgegeben !

Das mag ja sein, aber was machen Sie, wenn trotzdem jemand einbricht ?

Achselzucken.

Nicht alle Probleme lassen sich durch Technik lösen.
Einige lassen sich nur durch Nachdenken lösen.

Agenda

- Was ist das BSI ?
- ISO 27.000 ? ISO 20.000 ? ITIL ? IT-Grundschutz ? Hä ?
- Einführung in den BSI IT-Grundschutz
  - Aber wirklich nur eine Einführung, das Ding hat fast 4000 Seiten.
- Das OpenSource ISMS: Verinice

Was ist das BSI ?

- Bundesamt für Sicherheit in der Informationstechnik heute angesiedelt im Bundesministerium des Innern früher im Bundesnachrichtendienst
- Nachfolger der Zentralstelle für das Chiffrierwesen und der Zentralstelle für Sicherheit in der Informationstechnik
- 400 Leute,1991 Gegründet

- http://www.bsi.bund.de
- http://www.bsi-fuer-buerger.de
- http://www.buerger-cert.de

NNN: Normen, Nummern und Namen

- ISO 27.000 = ISO Norm zum Management von IT Sicherheit
- ISO 20.000 = ISO Norm passend zu ITIL
- ISO 9.000 = Qualitätsmanagementsystem
- ISO 14.000 = Umwelt (sind Windows-CDs Sondermüll ?)
- ITIL = IT Infrastructure Library, beschreibt wie man eine IT-Abteilung in einem Betrieb organisiert. Beschreibt Prozesse für Störungsbearbeitung, Change-Management, Capacity-Planing, Business Continuity Management (Nofallplanung)
- BSI IT-Grundschutz: ursprünglich eine Eigenentwicklung des BSI um Bundesbehörden zu unterstützten, keine Norm im Hintergrund
- Inzwischen passt das BSI das GSHB an ISO 27.000 und ITIL an.

Zum Begriff des IT-Sicherheitskonzeptes

- Sicherheit ist integraler Bestandteil des gesamten Lebenszyklus: Entwurf / Architektur, Entwicklung, Betrieb und Stilllegung
- Keine Trennung zwischen Betriebs- und Sicherheitskonzept !
- Merke: Es gibt nur einen sicheren Betrieb !
- Wenn man die beiden trennt, zieht man eine künstliche Mauer und schafft zusätzliche Probleme:
  - „Eine Firewall kostet Geld und macht wegen zusätzlicher Komplexität den Betrieb unzuverlässiger und aufwändiger.“ (reine Betriebssicht)

IT-Sicherheit = Datenschutz ?

- Nein.
- Datenschutz und IT-Sicherheit sind nicht das gleiche, manchmal stimmen deren Ziele und Methoden überein, manchmal aber auch nicht. Das BSI arbeitet an der Integration des Datenschutzes.
- Das ein Subunternehmen (Callcenter) die Kundendaten trotz anderslautender Verträge kopiert und weiterverkauft, wird durch keine Firewall verhindert.
- Datenschutzkonzepte sind häufig eher organisatorisch als technisch: Müssen wir die Daten überhaupt erfassen ? Wie lange müssen wir sie aufheben ? Können wir sie anonymisieren ?
- Die IT-Sicherheit ist häufig eine Voraussetzung für den Datenschutz: Zugriffskontrolle, ...

All show no go ?

- Niemand wird bestreiten, dass Betriebs- & Sicherheitskonzepte wichtig sind.
- Trotzdem gibt es so wenige dieser Konzepte.

Warum ?

All show no go ?

- Konzepte sind kompliziert (und die Erde ist eine Scheibe)
- Risikoanalysen sind noch komplizierter
  - Was kann passieren ? (Murphy lässt grüßen)
  - Wie wahrscheinlich ist das ?
  - Wie hoch wäre der Schaden ?
- IT-Leute hassen das Schreiben von Dokumentationen
- Kein System. Keine Vorlage. Kaum Beispiele.
- Falsche Zielvorstellungen: Schreiben Sie mal ein Sicherheitskonzept für die Firewall (Einzelbetrachtungen ergeben nur selten Sinn)

Welche Lehre ziehen wir daraus ?

- Wird es einfacher, wird es mehr gemacht. Damit steigt das Sicherheitsniveau.
- Lieber alle Systeme mit einem tatsächlich umgesetzten Grundschutz, als wenige Systeme mit anspruchsvollen, aber nicht umgesetzten Zielen.
- Wir brauchen ein System / Vorlagen / Beispiele.
- Wir brauchen ein hippes multiplattform datenbankgestütztes in Eclipse geschriebenes OpenSource-Tool, damit es dem Admin Spaß macht, damit zu arbeiten.
- Außerdem hat er dann endlich einen Grund das 40 Zoll Breitbild-Display zu bestellen.

Welche Lehren ziehen wir daraus ?

- Basis eines IT-Grundschutzkonzepts ist der Verzicht auf eine detaillierte Risikoanalyse. Es wird von pauschalen Gefährdungen ausgegangen und dabei auf die differenzierte Einteilung nach Schadenshöhe und Eintrittswahrscheinlichkeit verzichtet.
- Das IT-Grundschutzhandbuch bietet ein Kochrezept für ein normales Schutzniveau (Grundschutz). Durch die Verwendung des Grundschutzhandbuches entfällt eine aufwändige Sicherheitsanalyse, die Expertenwissen erfordert. Auch als Laie ist es möglich die zu ergreifenden Maßnahmen zu identifizieren und in Zusammenarbeit mit Fachleuten umzusetzen.

Welche Lehren ziehen wir daraus ?

- Durch Standard-Maßnahmen in den Bereichen Organisation, Personal, Technik und Übergreifendes wird Gefährdungen begegnet und dadurch ein Standard-Sicherheitsniveau (IT-Grundschutz) erreicht.
- In diesem allgemeinen Bereich finden in den meisten Fällen die größten Fortschritte statt. Die Technik (Firewall, ...) ist üblicherweise ok. Gerade Organisation ist wichtig: Wer löscht denn tatsächlich Firewall-Regeln und entzieht Benutzern auch mal Zugriffsrechte ?
- Für sensiblere Bereiche wird eine stabile Basis gelegt. Das notwendige Vorgehen wird durch eine ergänzende Sicherheitsanalyse ermittelt (BSI-Standard 100-3).

Muss das alles sein ?

- §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. (Gilt durch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich auch für viele GmbHs)
- Grundsätze ordnungsgemäßer Buchhaltung: Zusätzlich gilt das Vorsichtsprinzip, ungenau bezifferbare Bestände sollten eher pessimistisch eingeschätzt und mögliche Risiken gegebenenfalls berücksichtigt werden.
- Basel II: Banken prüfen vor einer Kreditvergabe das (IT) Risikomanagement

Was habe ich davon ?

- Sie schlafen besser.
- ISO 27.000 und ISO 20.000 (ITIL) werden so wichtig wie ISO 9.000 werden. Kunden werden es einfach verlangen.
- Investitionen werden an die richtigen Stellen gelenkt werden, nämlich da, wo ein Schaden wirklich teuer wird. Unnötige Investitionen und Bauchentscheidungen werden vermieden.
- Dokumentation ist immer gut: Wissen Sie nach einem Jahr noch was beim Kunden wie eingerichtet ist ?
- Nach der Einführung von ITIL und BSI bewerten die meisten IT-ler die Arbeitsorganisation als verbessert. Was nicht verhindert, dass sie während der Einführung schimpfen (früher war alles besser).

Wie funktioniert das Grundschutzhandbuch ?

Aufbau des IT-Grundschutzhandbuches

Das Grundschutzhandbuch besteht aus mehreren Einzelwerken

- 100-1: Managementsysteme für Informationssicherheit
  - Anforderungen an das System (ISO 27.000)
- 100-2: Vorgehensweise nach IT-Grundschutz
  - Wie setzt man 100-1 praktisch um ? (ISO 27.000)
- 100-3: Risikoanalyse auf der Basis von IT-Grundschutz
  - Risikoanalysen für Besonderheiten erstellen (BSI)
- 100-4: Notfallmanagement
  - Business Continuity Management (ISO 20.000, ITIL)
- IT-Grundschutzkataloge
  - Beschreibung der Gefährungen und Maßnahmen

BSI 100-1: Aufgaben für das Management

BSI 100-1 ist eine redaktionelle Überarbeitung der ISO 27.000: sprachlich verständlicher, Unklarheiten beseitigt, Erklärungen eingefügt.

Themen:

- Management-Prinzipien (u.a. Übernahme der Verantwortung durch GL)
- Ressourcen bereitstellen
- Mitarbeiter einbeziehen (Verpflichtungen, Schulungen, ...)
- Sicherheitsprozess etablieren
  - Leitlinie zur Informationssicherheit, in der die Ziele und Strategien zu ihrer Umsetzung dokumentiert sind
  - Informationssicherheit steuern und funktionsfähig halten
- 37 Seiten

BSI 100-1

Ziele
Rahmenbedingungen
Sicherheitsstrategie
Hilfsmittel zur Umsetzung
Sicherheitskonzept
IS-Organisation
Dokumentation, Bekenntnis
Leitlinie zur Informationssicherheit
(englisch: security policy)

BSI 100-2: Aufgaben des IT-Sicherheitsverantwortlichen

Beschreibt, wie BSI 100-1 in die Praxis umgesetzt werden kann:

- Aufgaben des IT-Sicherheitsmanagements
- Etablierung einer IT-Sicherheitsorganisation
- Erstellung eines IT-Sicherheitskonzepts
- Auswahl angemessener IT-Sicherheitsmaßnahmen
- IT-Sicherheit aufrecht erhalten und verbessern
- Hinweise zur Umsetzung mit Hintergrundwissen und Beispielen
- Verweise auf IT-Grundschutz-Kataloge zur detaillierten (auch technischen) Umsetzung
- 95 Seiten

BSI 100-3 und 100-4

100-3 beschreibt, wie man eine Risikoanalyse für Systeme mit erhöhten Anforderungen erstellt.

100-4 beschreibt, welche Prozesse und Dokumentationen für ein Nofallmanagement (ITIL Business Continuity Management) notwendig sind.

Machen wir heute nicht.

IT-Grundschutzkataloge

Hier sind die konkreten Gefährdungen und Maßnahmen für Standard-Objekte beschrieben:

- 3700 Seiten
- Das ist im Prinzip das alte IT-Grundschutzhandbuch

Kapitel

- Bausteine: Objekte, denen Gefährdungen zugeordnet sind
- Gefährdungen: Höhere Gewalt, Fehladministration, Sabotage
- Maßnahmen: Wie lösen wir das Problem ?

IT-Grundschutzkataloge

Beispiel für einen Baustein: Client Windows XP

- http://www.bsi.de/gshb/deutsch/baust/b03209.htm

Beispiel für eine Gefährdung:

- http://www.bsi.de/gshb/deutsch/g/g04023.htm

Beispiel für eine Maßnahme:

- http://www.bsi.de/gshb/deutsch/m/m04057.htm

Die praktische Anwendung des Grundschutzhandbuches

Was heißt das jetzt alles für die Praxis ?

Wir müssen einmal 100-1 durcharbeiten:

- Das Management muss Verantwortung übernehmen
- Das Management muss Ziele definieren
- Das Management muss Aufgaben delegieren
- Das Management muss Geld und Leute rausrücken
- Das Management IT-Sicherheit in andere Prozesse einbauen (HR)

Dann machen wir 100-2:

- Hier wird die tatsächlich vorhandene IT-Umgebung erfasst und modelliert.

BSI 100-2 praktisch umsetzen

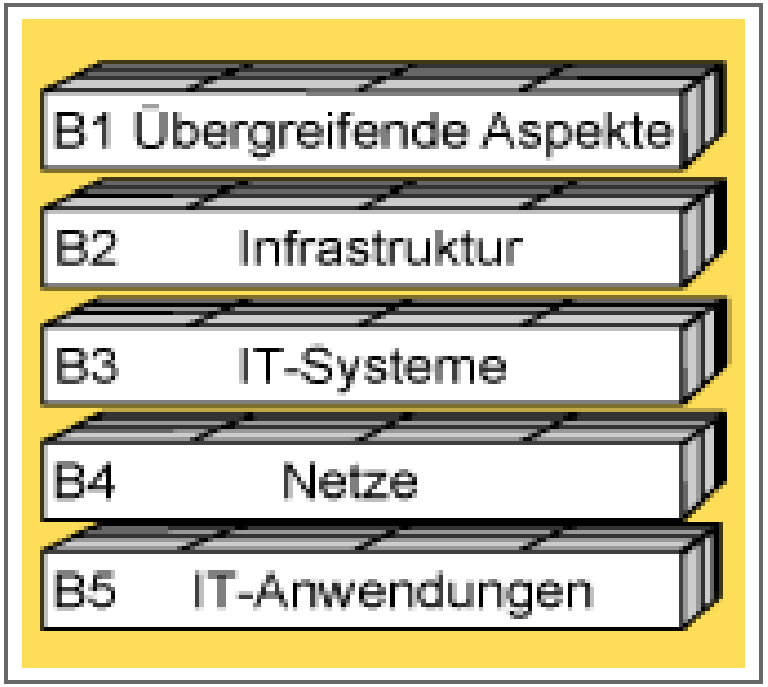
Strukturanalyse machen

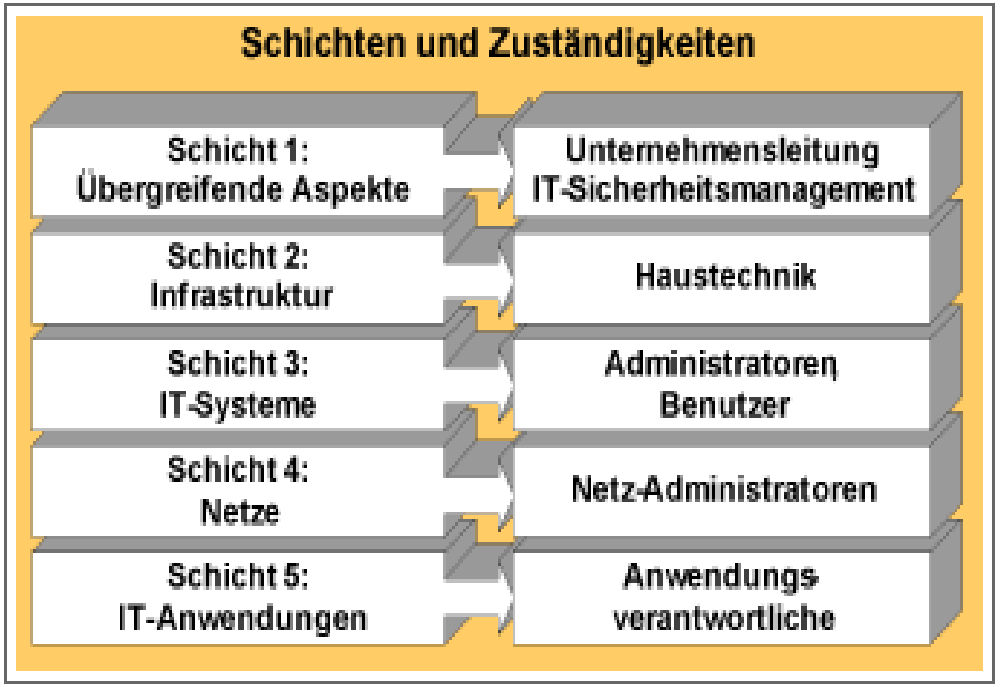
- Netzplan beschaffen
- Raumpläne beschaffen
- Anwendungen, Mitarbeiter, Rollen erfassen

Schichtenmodell aufbauen

- Tool-gestützt: Verinice oder GS Tool
- Masochisten: Papier oder Excel-Tabellen

Schichtenmodell & Modellierung





Schichtenmodell & Modellierung

- Übergreifende Aspekte: grundsätzliche organisatorische Aspekte für den gesamten IT-Verbund. B 1.0 IT-Sicherheitsmanagement, B 1.1 Organisation, B 1.4 Datensicherungskonzept.
- Infrastruktur: baulich-technische Fragen B 2.1 Gebäude, B 2.4 Serverraum, physischer Schutz etwa vor Feuer, Wasser oder Diebstahl
- IT-Systeme: IT-Sicherheitsaspekte B 3.101 Allgemeiner Server, B 3.201 Allgemeiner Client
- Netze: LAN / WAN, B 4.1 Heterogene Netze, B 4.2 Netz- und Systemmanagement
- IT-Anwendungen: Sicherheit der Anwendungen B 5.3 E-Mail, B 5.7 Datenbanken, B 5.8 Telearbeit

Was heißt das jetzt alles für die Praxis ?

- Objekte anlegen
- Gefährdungen zuweisen: Ist es ein Unix-Server, ein Windows-Server, eine Datenbank, ein Mail-System ...
- Objekt klassifizieren
  - Vertraulichkeit normal / hoch /sehr hoch
    - normal: Die Schadensauswirkungen sind begrenzt und überschaubar.
    - hoch: Die Schadensauswirkungen können beträchtlich sein
    - sehr hoch: Existentiell bedrohlich, katastrophales Ausmaß
  - Integrität normal / hoch /sehr hoch
  - Verfügbarkeit normal / hoch /sehr hoch
- Aus den Gefährdungen folgen Maßnahmen. Diese müssen wir bewerten und eventuell umsetzen.

Schutzbedarf ist relativ (Beispiele)

Normaler Schutzbedarf:

- Der finanzielle Schaden ist kleiner als 50.000 Euro. Die Abläufe werden unerheblich beeinträchtigt. Ausfallzeiten von mehr als 24 Stunden können hingenommen werden.“

Hoher Schutzbedarf:

- Der mögliche finanzielle Schaden liegt zwischen 50.000 und 500.000 Euro. Die Abläufe werden erheblich beeinträchtigt. Ausfallzeiten dürfen maximal 24 Stunden betragen.

Sehr hoher Schutzbedarf:

- Der mögliche finanzielle Schaden beträgt mehr als 500.000 Euro. Die Abläufe werden so stark beeinträchtigt, dass Ausfallzeiten, die über 2 Stunden hinausgehen, nicht toleriert werden können.

Schutzbedarf vererbt sich weiter

Der Schutzbedarf vererbt sich weiter.

Beispiel: die Anwendung Online-Shop ist bei Verfügbarkeit als Hoch eingestuft, dann gilt das automatisch auch für

- den Server
- das Netzwerk
- den Raum
- den IT-Verbund

- Für den Schutzbedarf Hoch und Sehr hoch ist IT-Grundschutz normalerweise nicht mehr ausreichend !

Schutzbedarf klebt und krümelt

Beispiel: Alle zehn Anwendungen sind als Verfügbarkeit normal eingestuft.

Da aber alle zehn Anwendungen auf dem gleichen Server (Virtualisierung) laufen, sollte der Server insgesamt höher eingestuft werden.

Ein einzelner Ausfall einer Normal-Anwendung ist vielleicht akzeptabel, aber nicht wenn alle gleichzeitig ausfallen.

Das BSI nennt das **Kumulationseffekt**.

Andersherum ist das der **Verteilungseffekt**. Ein Server kann bei Verfügbarkeit normal sein, auch wenn die Anwendung eine Verfügbarkeit voln Hoch hat. Zum Beispiel, wenn es sich bei dem Server um einen einzelnen Node eines Clusters handelt.

Siegelstufen

Die Maßnahmen sind in A B C und Z eingeteilt.

- A: Unabdingbare Standardsicherheitsmaßnahmen; die Umsetzung ist für alle drei Stufen der IT-Grundschutz-Qualifizierung erforderlich.
- B: Wichtigste Standardsicherheitsmaßnahmen; die Umsetzung ist für die Aufbaustufe und für das Zertifikat erforderlich.
- C: Für ein Zertifikat darüber hinaus erforderliche Maßnahmen.
- Z: Die Umsetzung dieser zusätzlichen IT-Sicherheitsmaßnahmen sollte zur Steigerung der IT-Sicherheit erfolgen, ist jedoch zur Qualifizierung nach IT-Grundschutz nicht erforderlich.

Maßnahmenstatus

Möglicher Status einer Maßnahme:

- Ja: Die Maßnahme wurde erfolgreich umgesetzt.
- Nein: Die Maßnahme wurd nicht umgesetzt.
- Teilweise: Teilweise umgesetzt.
- Entbehrlich: Brauchen wir nicht.

Maßnahmenstatus

Sie müssen den Status dokumentieren und begründen.

- Ja: umgesetzt von wem wan wie ?
- Entbehrlich: Wir brauchen keine USV an diesem Server, weil das gesamte Rechenzentrum USV-versorgt ist.
- Nein: Begründung: Zu teuer. Das ist eine gültige Entscheidung. Aber das Konzept hat sie gezwungen, darüber nachzudenken. Jetzt kennen Sie zumindest ihr Risiko.
- Teilweise: Grad der Umsetzung, wann ist die Fertigstellung geplant.

Das OpenSource Tool Verinice

Die ISMS-Anwendung Verinice

- http://www.verinice.org
- Platformunabhängig durch Java (Linux, Windows, MacOS)
- Entwickelt von Sernet (die Samba-Leute)
- GPL V3
- Erweiterbares Schema: Kundennummer, Seriennummern, Telefonnummer, Standort, Configuration Item Database für ITIL)
- Datenbank: Derby (Standard), PostgreSQL, MySQL
- GS-Tool Import
- offizieller Datenschutz-Baustein des Bundesbeauftragten für Datenschutz und Informationssicherheit (BfDI)
- Wizard für Risikoanalyse nach BSI 100-3

Vorführung Verinice

Start

- BSI Bücher importieren
- Datenbank verbinden
- IT-Verbund anlegen: Wayne Enterprises
- Standorte: Wayne Manor, Gotham City
- Räume: Batcave, ServerRaum

Funktionen

- Konsolidator
- Bulk Edit

Vielen Dank für Ihre Aufmerksamkeit!

Robert M. Albrecht
robert-manfred.albrecht@t-systems.com
http://www.romal.de
GNU FDL 1.3+
CC-BY-SA 3.0

Photos © T-Systems Enterprise Services GmbH
Alle rechte vorbehalten.

T Systems