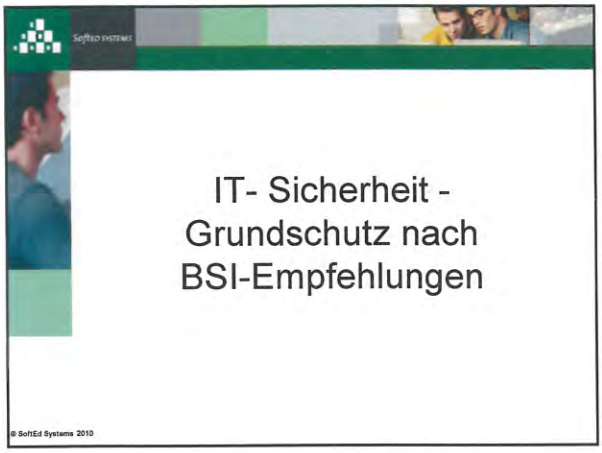
IT Sicherheit Grundschutz nach BSI-Empfehlungen

SoftED SYSTEMS

SOFTWARE · SUPPORT · SEMINARE

SoftEd Systems GmbH
Gerichtsweg 28 | 04103 Leipzig
www.softed.de



IT- Sicherheit - Grundschutz nach BSI-Empfehlungen

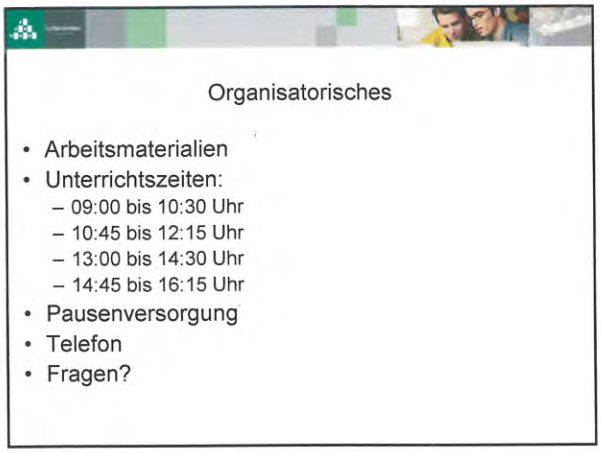
Vorstellung

- Name
- Firma / Behörde
- Aufgabengebiet
- Erfahrungen auf dem Gebiet der IT-Sicherheit
- Erwartungen an diesen Kurs

Agenda

- Motivation für IT-Sicherheit, gesetzliche Rahmenbedingungen
- Managementsysteme für IT-Sicherheit nach ISO 27001 (BSI-Standard 100-1)
- IT-Grundschutz-Vorgehensweise (BSI-Standard 100-2, Grundschutz-Kataloge)
- Risikoanalyse (BSI-Standard 100-3)
- Notfallmanagement, Business Continuity Management (BSI-Standard 100-4)
- Werkzeuge für die Dokumentation (GSTOOL, Alternativen)
- Modellierung eines Informationsverbundes mit den Grundschutzkatalogen als praktisches Beispiel

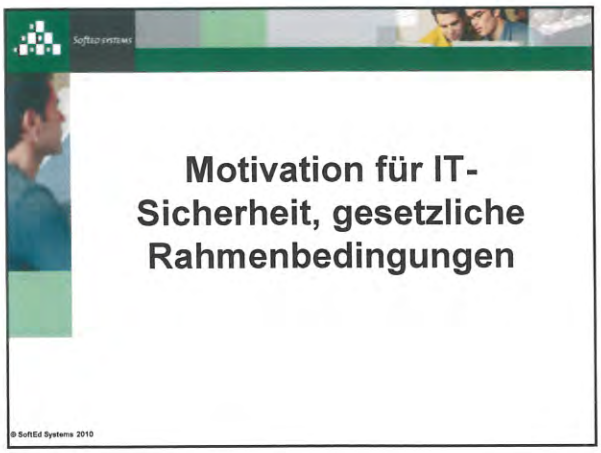
auf der BSI-Seite als Download



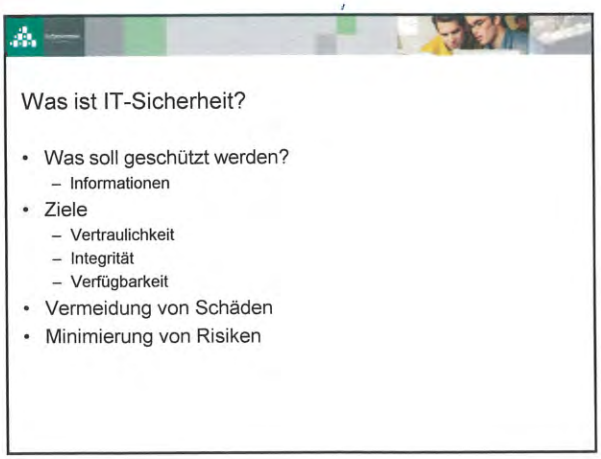
Organisatorisches

- Arbeitsmaterialien
- Unterrichtszeiten:
  - 09:00 bis 10:30 Uhr
  - 10:45 bis 12:15 Uhr
  - 13:00 bis 14:30 Uhr
  - 14:45 bis 16:15 Uhr
- Pausenversorgung
- Telefon
- Fragen?

bei Fragen:
- support@softed.de
0351 / 867700



Motivation für IT-Sicherheit, gesetzliche Rahmenbedingungen



Was ist IT-Sicherheit?

- Was soll geschützt werden?
  - Informationen
- Ziele
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
- Vermeidung von Schäden
- Minimierung von Risiken

Bedrohungslage

Angreifer

- Script-Kiddies
- Kriminelle
- Spione
- Hacktivisten

Integrität

- Website-Defacement
- Beispiel: www.kernenergie.de, 09.Nov.2010

Kernenergie.
So sicher wie diese Webseite.

Integrität

- Am 19.07.2011 hackt die Hackergruppe LulzSec „The Sun"

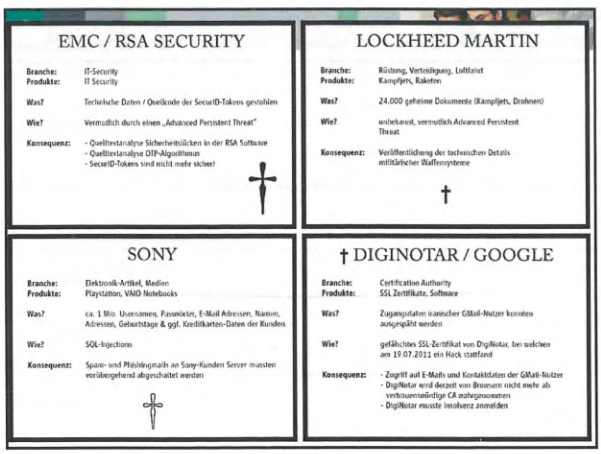
Preisliste für gehackte Server

Site	Details	Level of Control	Traffic	Price
http://gs.mil.al/	ARMY Forces of republic of albania	Full SiteAdmin Control + High value informations	unknown	$499
http://www.scguard.army.mil/	Souce Carolina National Guard	MySQL root access + High value informations	unknown	$499
http://cecom.army.mil/	The United States Army | CECOM	Full SiteAdmin Control/SSH Root access	unknown	$499
http://pec.ha.osd.mil/	The Department of defense pharmacoeconomic Center	Full SiteAdmin Control/Root access, High value informations!	unknown	$399
http://www.woodlands.edu.uy/	Wooldlands School Uruguay.	Full SiteAdmin Control.	5200	$33
http://s-u.edu.in/	Singhania University	Full SiteAdmin Control.	unknown	$55
http://www.nccu.edu.tw/	National Chengchi University.	Students/Exams user/pass and full admin access!	56093	$99
http://www.terc.tp.edu.tw/	Taipei City East Special Education Resource Center	Full SiteAdmin Control.	74188	$88
http://itcpantaleo.gov.it/	Italian Official Government Website.	Full SiteAdmin Control.	292942	$99
http://donmilaninapoli.gov.it/	Istituto Statale Don Lorenzo Milani	Full SiteAdmin Control.	292942	$99
http://itcgcesaro.gov.it/	Official Italian gov website.	Full SiteAdmin Control.	292942	$99

Verfügbarkeit

Feuerwehr muss eigene Wache löschen

DUISBURG. Einen kurzen Weg zum Einsatz hatte die Duisburger Feuerwehr in der Nacht zum Freitag: Ihre eigene Hauptwache brannte. Die Löscharbeiten dauerten mehrere Stunden, der Schaden dürfte rund eine Million Euro betragen. Kollegen der Freiwilligen Feuerwehr halfen beim Löschen und sahen auch das Gute: „Immerhin kannten wir uns dort aus", sagte der Einsatzleiter. (AP)



Angriffe von außen

- Website-Defacement durch Script-Kiddies
- Phishing, Money-Mules
- Bot-Netze
- Zero-Day-Exploits, Drive-By-Downloads, XSS, SQL Injection, Buffer Overflow, ...
- Keylogger, Spyware, Rootkits, Deny-Of-Service, ...

„Angriffe“ von innen

- Faktor „Mensch“
  - Bewusstes oder unbewusstes Fehlverhalten
  - „Praktikanten“
  - „Innere Kündigung“
- Social Engineering
  - Ausnutzen der Hilfsbereitschaft der Mitarbeiter

Steuererklärung an Privatdetektiv

- Herr Müller von der Abteilung III der Oberfinanzdirektion Chemnitz rief im Finanzamt Löbau an.
- Er ließ sich allerlei Daten geben. Steuerzahlen, Einkommen, mögliche Steuerschulden, Bankdaten, Angaben über die Kinder und das Auto-Kennzeichen
- Zwar hatte der Anrufer die falsche Adresse und die falsche Steuernummer genannt. Dennoch gab die Sachbearbeiterin dem Kollegen hilfsbereit Auskunft. Schließlich hat die Löbauer Behörde in Rankings stets vordere Plätze als eines der freundlichsten Finanzämter belegt.
- Dumm nur, dass es weder eine Abteilung III noch einen Herrn Müller bei der Oberfinanzdirektion gibt.

Social Engineering - Ursachen

- Reziprozität
  - Wie du mir, so ich Dir
- Commitment
  - Wer A sagt, muss auch B sagen
- Sympathie
- Autorität

Weitere Risiken

- Höhere Gewalt
- Organisatorische Mängel
- Technisches Versagen
- Bauliche Mängel

Typische Probleme in der Praxis

- Resignation, Fatalismus und Verdrängung
- Kommunikationsprobleme
- Sicherheit wird als technisches Problem mit technischen Lösungen gesehen
- unsystematisches Vorgehen bzw. falsche Methodik
- Management: fehlendes Interesse, schlechtes Vorbild
- Sicherheitskonzepte richten sich an Experten, der IT-Benutzer wird vergessen.

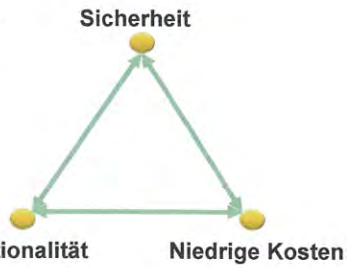
- Bei uns ist noch nie etwas passiert!
  - Wurden frühere Sicherheitsvorfälle überhaupt bemerkt bzw. gemeldet?
  - Wurden Sicherheitsvorfälle als solche erkannt?
- Was soll bei uns schon zu holen sein?
  - Es werden nahezu überall Daten verarbeitet, die missbräuchlich verwendet werden könnten.
- Unser Netz ist sicher!
  - Die Fähigkeiten potentieller Angreifer werden oft unterschätzt.
  - Auch ein erfahrener Administrator macht gelegentlich Fehler.
- Unsere Mitarbeiter sind vertrauenswürdig!
  - Die Mehrzahl der Sicherheitsverstöße wird durch „Innentäter" begangen.
  - Schäden entstehen nicht nur durch Vorsatz:
    - Versehen
    - Neugierde
    - Unwissenheit

Konsequenzen fehlender Regelungen
...oder: Jeder tut, was er für richtig hält

- Konfusion im Notfall
  - Was ist zu tun? Wer hilft?
- lückenhafte Datensicherung
  - Notebooks, Heimarbeitsplätze, lokale Datenhaltung
- fehlende Klassifizierung von Informationen
  - Verschlüsselung, Weitergabe und Austausch von Informationen
- Disziplinlosigkeit
  - Was alle machen kann doch nicht unsicher sein...?
  - Ignoranz und Arroganz statt geregelter Prozesse
  - Konsequenzen bleiben aus, sind zu hart, sind willkürlich

Sicherheit und Komfort

Sicherheit ist ein Kompromiss



Die IT rückt mehr in den Blickpunkt des Managements

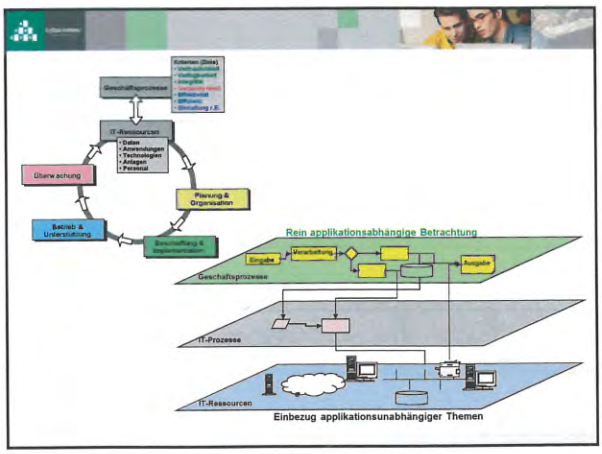
- IT betrifft wesentliche Geschäftsprozesse und Aufgaben
- Management hat Verantwortung für Geschäftsprozesse, Einhaltung von Verträgen und Gesetzen
- Management hat Verantwortung für den wirtschaftlichen Einsatz von Ressourcen
- IT-Governance
  - Geschäftsziele erreichen
  - Ressourcen verantwortungsvoll einsetzen
  - Risiken überwachen

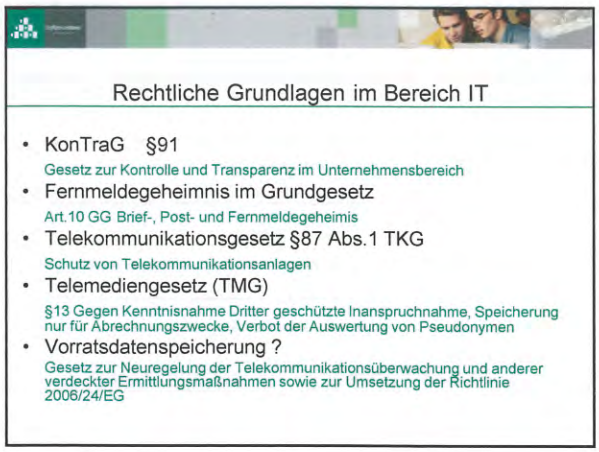
Standardisierung des IT-Managements

- Security
  - IT-Grundschutz
  - ISO/IEC 27001
- USA: Sarbanes Oxley Act
  - COBIT
  - SAS 70
- Deutschland: Steuerrecht
  - GoBS, GdPdU
  - IDW PS
- Service Management
  - ITIL
  - ISO/IEC 20000

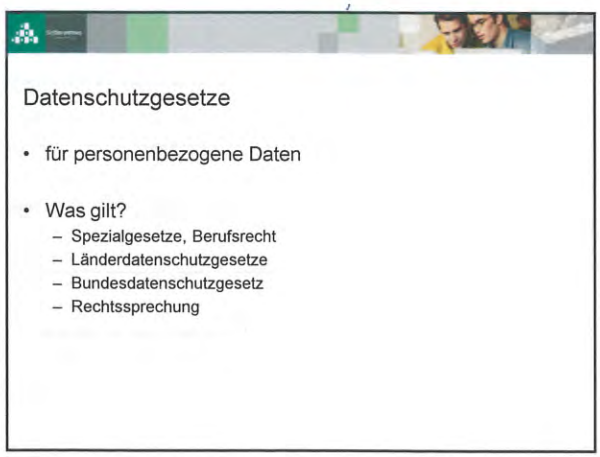
COBIT - Control Objectives

- Effektivität
  - für einen Prozess relevante Informationen stehen zum erforderlichen Zeitpunkt und inhaltlich korrekt in der benötigten Weise (Format) zur Verfügung
- Effizienz
  - datenliefernde Ressourcen werden optimal genutzt
- Verlässlichkeit
  - IT-Systeme liefern die Informationen zeitlich und inhaltlich korrekt
- Compliance
  - die Informationen entsprechen rechtlichen und vertraglichen Anforderungen und an die der Geschäftsprozess gebunden ist
- Vertraulichkeit
- Verfügbarkeit
- Integrität





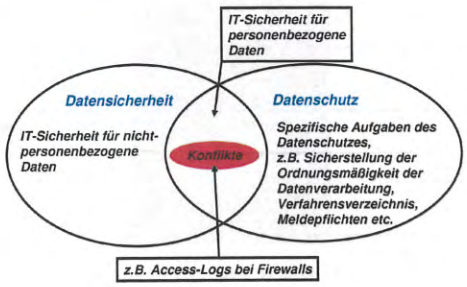
- SPAM-Filter verwenden nur
nach Zustimmung des Benutzers
- es darf nur Internetüberwachung
keine Klartextüberwachung erfolgen



Prinzipien des Datenschutzes

- Zulässigkeit
  - Rechtsgrundlage für die Verarbeitung, öffentlich oder Einwilligung
- Zweckbindung
  - Daten dürfen nur für den Zweck verarbeitet werden, für den sie auch erhoben wurden
- Transparenz
  - Betroffenenrechte, Verfahrensverzeichnis, Benachrichtigungspflicht
- Direkterhebungsvorrang
- Verhältnismäßigkeit
  - Datensicherheit: Angemessenheit, Stand der Technik
- Datensparsamkeit
  - Anonymisierung, Pseudonymisierung, Löschung

Datenschutz und Informationssicherheit



Weitere Rahmenbedingungen

- HGB §238 (Handelsgesetzbuch)
  - GoBS
    Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme
  - GDPdU
    Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)
- KWG §44 (Kreditwesengesetz)
- Basel II
- Sarbanes-Oxley Act (SOX)
  - Unternehmensberichterstattung für an US-Börsen gehandelte Unternehmen und deren Töchter

Signaturgesetz, Signaturverordnung

- Wofür?
  - Vertraulichkeit -> Verschlüsselung
  - Integrität -> Signatur
  - Authentizität -> Signatur
  - Nichtabstreitbarkeit -> Signatur
- Stufen
  - einfache Signatur
  - fortgeschrittene Signatur
  - qualifizierte Signatur mit Anzeige des Zertifizierungsdiensteanbieters
  - qualifizierte Signatur mit Akkreditierung des Zertifizierungsdiensteanbieters

Elektronische Signatur in anderen Gesetzen

- BGB §§ 125 ff., Formanpassungsgesetz
  - die qualifizierte Signatur entspricht der Unterschrift
  - Kopie/Fax -> einfache oder fortgeschrittene Signatur
- Verwaltungsverfahrensgesetz §3a
  - Der Empfänger muss die Anwendung der elektronischen Kommunikation billigen
  - Er muss einen Zugang für die elektronische Kommunikation eingerichtet haben
  - Angabe einer E-Mail-Adresse -> Zugang eröffnet ?
  - Fehler -> Benachrichtigung des Absenders erforderlich
- §14(3) Umsatzsteuergesetz
  - Qualifizierte Signatur für elektronische Rechnungen
  - Seit 2012 Alternative: sorgfältige kaufmännische Prüfung der Rechnung

Hacker-Paragraph

- **§ 202a Ausspähen von Daten**
  Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, ...
- **§ 202b Abfangen von Daten**
  ... unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten aus einer nichtöffentlichen Datenübermittlung ...
- **§ 202c Vorbereiten des Ausspähens und Abfangens von Daten**
  Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er
  - Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten ermöglichen, oder
  - Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

  herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, ...

Wege zur IT-Sicherheit

Methodik für IT-Sicherheit?

Viele Wege führen zur IT-Sicherheit...

Welcher Weg ist der effektivste?

Sicherheit ist...

- kein Produkt
  - Sicherheit kann man nicht kaufen, Sicherheit muss man schaffen (dabei kann man auf Produkte zurückgreifen).
- kein Projekt
  - Es genügt nicht, Sicherheit einmal zu schaffen.
  - Sicherheit muss aufrechterhalten werden.
- Sicherheit ist ein Prozess
- Sicherheit ist Chefsache

Risikoanalyse

Definition:

(engl. Risk Assessment/Analysis): Untersuchung, wie wahrscheinlich das Eintreten eines bestimmten Schadens ist und welche negativen Folgen der Schaden hätte.

Probleme:

- ungenaue Eingangsgrößen
- hoher Zeitaufwand
- teuer
- individuelle Betrachtung nötig

ISO 27001 Native

Schritt 1:
Festlegung des Anwendungsbereichs

Schritt 2:
Inventarisieren der Werte (Assets)

Schritt 3:
Analysieren und Behandeln von Risiken

Schritt 4:
Maßnahmen festlegen umsetzen

Schritt 5:
Aufbau des Statement of Applicability (SOA)

ISO 27002

A.9.2.1	Equipment siting and protection	*Control* Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
A.9.2.2	Supporting utilities	*Control* Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
A.9.2.3	Cabling security	*Control* Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

IT-Grundschutz Prinzipien

- Gesamtsystem enthält **typische** Komponenten (Server, Clients, Serverraum, E-Mail...)
- **Pauschalisierte** Gefährdungen und Eintrittswahrscheinlichkeiten, keine klassische Risikoanalyse
- Empfehlung von **Standard**-Sicherheits-maßnahmen
- **konkrete** Maßnahmenbeschreibung
- **kostenlose** Verteilung

www.bsi.bund.de/gshb

Ziel des IT-Grundschutzes

Durch infrastrukturelle, organisatorische, personelle und technische

Standard-Sicherheitsmaßnahmen

ein

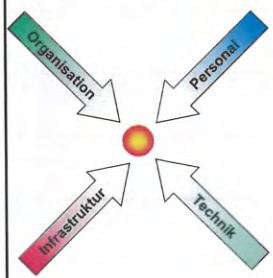
Standard-Sicherheitsniveau

für IT-Systeme aufbauen, das auch für sensiblere Bereiche

ausbaufähig

ist.

Verschiedene Facetten von IT-Grundschutz



- Vorgehensweise zur Erstellung von IT-Sicherheitskonzepten (Methode für ein „Information Security Management System")
- Sammlung von Standard-Sicherheitsmaßnahmen für typische IT-Systeme
- ganzheitlicher Ansatz
- Nachschlagewerk
- Referenz und Standard für Informations-Sicherheit

IT-Grundschutz - Vorteile

- arbeitsökonomische Anwendungsweise durch **Soll-Ist-Vergleich**
- kompakte IT-Sicherheitskonzepte durch Verweis auf **Referenzquelle**
- praxiserprobte, meist kostengünstige Maßnahmen mit hoher **Wirksamkeit**
- **Erweiterbarkeit** und **Aktualisierbarkeit**

Erreichbares Sicherheitsniveau

Schutzwirkung von Standard-Sicherheitsmaßnahmen nach IT-Grundschutz sind

- für die Schutzbedarfskategorie „normal"
  - im Allgemeinen ausreichend und angemessen,
- für die Schutzbedarfskategorie "hoch"
  - Basisschutz,
  - unter Umständen nicht ausreichend; ergänzende Sicherheitsanalyse bestimmt, ob zusätzliche Sicherheitsmaßnahmen durch Risikoanalyse ermittelt werden müssen,
- für die Schutzbedarfskategorie "sehr hoch"
  - Basisschutz,
  - im Allgemeinen nicht ausreichend, so dass eine Risikoanalyse notwendig ist.

Empfehlungen für IT-Grundschutz

- Der Bundesbeauftragte für den Datenschutz
- Bundesregierung (zur Sicherheit im elektronischen Rechts- und Geschäftsverkehr mit der Bundesverwaltung)
- Die Rechnungshöfe des Bundes und der Länder
- Landesverwaltungen verschiedener Bundesländer für Behörden, Gerichte und sonstige Stellen der Landesverwaltung
- Wirtschaftsprüfungsgesellschaften

BSI-Standards + Loseblattsammlung

Publikationen zum IT-Sicherheitsmanagement

- BSI-Standards zur IT-Sicherheit (IT-Sicherheitsmanagement)
  - 100-1 Managementsysteme für Informationssicherheit (ISMS)
  - 100-2 Grundschutz-Vorgehensweise
  - 100-3 Risikoanalyse auf der Basis von IT-Grundschutz
  - 100-4 Notfallvorsoge, Business Continuity Management
- IT-Grundschutz-Kataloge
  - Bausteine
  - Gefährdungen
  - Maßnahmen

BSI-Standard 100-1

Managementsysteme für
Informationssicherheit
(ISMS nach ISO 27001)

Komponenten eines ISMS

- Strategie
- Ressourcen
- Mitarbeiter
- Management-Prinzipien

Management-Prinzipen

- Übernahme der Gesamtverantwortung
- Integration der IT-Sicherheit
- Steuerung und Aufrechterhaltung der IT-Sicherheit
- Setzung erreichbarer Ziele
- Abwägung IT-Sicherheitskosten gegen Nutzen
- Vorbildfunktion

Kommunikation und Wissen

- Berichte an die Leitungsebene
- Informationsfluss
- Dokumentation
  - technische Dokumentation (für sicherheitsrelevante Daten)
  - Anleitungen für IT-Anwender
  - Management-Reports
  - Management-Entscheidungen
- Nutzung verfügbarer Informationsquellen und Erfahrungen

Sicherheit ist ein Prozess

- Planung und Konzeption (plan)
- Umsetzung der Planung (do)
- Erfolgskontrolle (check)
- Optimierung (act)

- => PDCA-Modell

Deming-Zyklus

IT-Sicherheitsprozess

- Dokumentation, Bekenntnis
  - Leitlinie zur Informationssicherheit (Security Policy)
- Hilfsmittel zur Umsetzung
  - Sicherheitskonzept
    - Beschreibung der IT-Struktur
    - Risikobewertung
    - Maßnahmen
  - Sicherheitsorganisation
    - Regeln, Anweisungen
    - Prozesse, Abläufe
    - Strukturen

Aufgaben des Managements

- Planung des IT-Sicherheitsprozesses
  - Festlegung des Geltungsbereichs für das ISMS
  - Ermittlung von Rahmenbedingungen
  - Formulierung von Sicherheitszielen und einer Leitlinie zur Informationssicherheit
  - Aufbau einer Sicherheitsorganisation
- Unterstützung bei der Umsetzung
  - Bereitstellung von Ressourcen
  - Benennung von Prioritäten
- Erfolgskontrolle im Sicherheitsprozess

IT-Sicherheitskonzept

- Erstellung
  - Auswahl einer Methode zur Risikobewertung
  - Klassifikation von Risiken bzw. Schäden
  - Risikobewertung
  - Entwicklung einer Strategie zur Behandlung von Risiken
  - Auswahl von IT-Sicherheitsmaßnahmen
- Umsetzung
  - Realisierungsplan
  - Steuerung und Kontrolle der Umsetzung

BSI-Standard 100-2

IT-Grundschutz-Vorgehensweise

IT-Grundschutz-Vorgehensweise

- Konkretisiert den allgemeinen Standard 100-1
- Bietet „Best Practice“ für ein ISMS
- weiterentwickelt seit 1994
- Umsetzung zertifizierbar nach ISO 27001
- Alternative zu ISO 27002

Informationsverbund (IT-Verbund) Definition

Unter einem **Informationsverbund (IT-Verbund)** ist die Gesamtheit von

- infrastrukturellen,
- organisatorischen,
- personellen und
- technischen Komponenten

zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen.

Ein IT-Verbund kann dabei als Ausprägung die gesamte IT einer Institution oder einzelne Bereiche, die durch organisatorische Strukturen (z. B. Abteilungsnetz) oder gemeinsame IT-Anwendungen (z. B. Personalinformationssystem) gegliedert sind, umfassen.

IT-Grundschutz Zertifizierung Anwendungsbereiche

Was kann zertifiziert werden?

- Ein oder mehrere Geschäftsprozesse
- Eine oder mehrere Fachaufgaben
- Eine oder mehrere Organisationseinheiten

- Es braucht nicht gleich das gesamte Unternehmen zu sein!

Bedingung:

- IT-Verbund muss eine sinnvolle Mindestgröße haben!

Zertifizierung (TÜV oder BSI) → ISO27001 → deutlich umständlicher

- Auditor-Testat „Einstiegsstufe“
  - alle Maßnahmen Siegelstufe A
- Auditor-Testat „Aufbaustufe“
  - alle Maßnahmen Siegelstufe A, B
- IT-Grundschutz-Zertifikat
  - alle Maßnahmen Siegelstufe A, B, C

IT-Grundschutz-Zertifizierung
Ablauf (vereinfacht)

- Prüfung erfolgt durch einen vom BSI lizensierten IT-Grundschutz-Auditor
- Auditor prüft die Umsetzung von IT-Grundschutz und erstellt den Auditreport
  - Prüfung der vorhandenen Dokumente
  - Prüfung von Stichproben vor Ort
- Unternehmen stellt Zertifizierungsantrag beim BSI
  - BSI prüft den Auditreport
  - Falls Prüfung positiv: Zertifikat wird erteilt
- Zertifikat wird veröffentlicht

IT-Grundschutz-Zertifizierung

- Umsetzung Grundschutz: 6 - 48 Monate, 100...1000 PT
- Aufwand des Auditors: 10...30 PT

Erfolgsfaktoren:

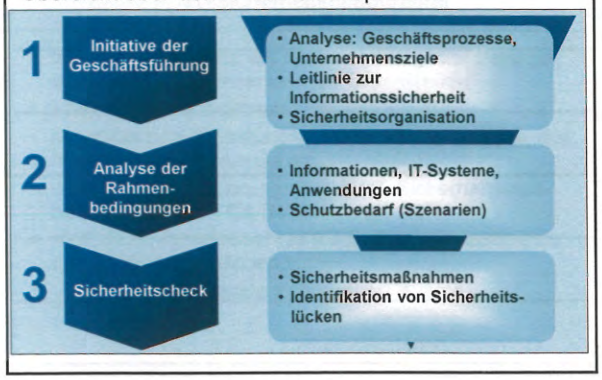
- Unterstützung durch die Geschäftsleitung
- Verständnis, Kooperationsbereitschaft und aktive Unterstützung durch die IT- und TK-Verantwortlichen
- konsequente Gruppenbildung
- Tool-Unterstützung

Hindernisse:

- Personalwechsel
- Umbau der Systemlandschaft

Der Sicherheitsprozess nach IT-Grundschutz-Vorgehensweise

Übersicht über den IT-Sicherheitsprozess



Übersicht über den IT-Sicherheitsprozess

Sicherheitsprozess

Struktur eines Sicherheitskonzeptes

IT-Sicherheitsstrategie

Rahmenbedingungen
(Gesetze, Verträge, Kundenanforderungen, Unternehmensziele, Aufgaben der Behörde, Technik, Bedeutung der IT für Geschäftsprozesse, ...)

IT-Sicherheitsstrategie

- Sicherheitsziele
- Umsetzung der Strategie durch Sicherheitsorganisation und IT-Sicherheitskonzept
- Dokumentation in der **Leitlinie zur Informationssicherheit**

Verantwortung der Leitung

Es wird schriftlich festgehalten, dass die Unternehmens/Behördenleitung die **Gesamtverantwortung** für die IT- Sicherheitsleitlinie, die Sicherheitsziele, das Sicherheitskonzept und seine Umsetzung trägt.

Ihr strategischer Einfluss auf das Erreichen von IT-Sicherheitszielen im Unternehmen und die Umsetzung von Sicherheitsmaßnahmen soll deutlich werden, auch wenn Sicherheitsaufgaben von ihr an Mitarbeiter delegiert werden.

IT-Sicherheitsbeauftragter

- ist verantwortlich für die Wahrnehmung aller Belange der IT-Sicherheit innerhalb der Organisation
- leitet das Sicherheitsmanagement-Team
- koordiniert die Erstellung des Sicherheitskonzepts, des Notfallvorsorgekonzepts etc.
- erstellt den Realisierungsplan für IT-Sicherheitsmaßnahmen und prüft die Realisierung
- stellt den Informationsfluss zur Leitungsebene und zu den IT-Verantwortlichen sicher
- untersucht auftretende sicherheitsrelevante Zwischenfälle

IT-Sicherheits-Management-Team

Aufgaben
- Mitwirkung an der Erstellung der Leitlinie
- Konsens-Bildung bei strittigen Fragen der IT-Sicherheit
- Mitwirkung bei der Erstellung von Teilkonzepten

Mitglieder
- IT-Sicherheitsbeauftragter der Organisation
- IT-Sicherheitsbeauftragte von Teilorganisationen
- Verfahrensverantwortliche oder Anwender aus den Fachabteilungen
- Mitarbeiter aus dem IT-Betrieb
- Datenschutzbeauftragter
- Personalrat/Betriebsrat
- Mitarbeiter aus der Rechtsabteilung

Leitlinie zur Informationssicherheit

(IT-Sicherheitsleitlinie, Security Policy)

Sicherheitsziele bestimmen

Strategische und operative Bedeutung der IT für das Unternehmen einschätzen

Ziel ist herauszufinden, welches
IT- Sicherheitsniveau für die Organisation angemessen ist und angestrebt werden sollte.

Inhalte dokumentieren

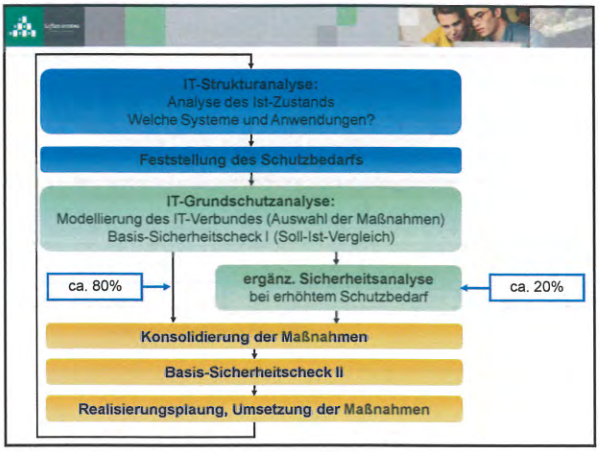
Die Inhalte der **Leitlinie zur Informationssicherheit** sind zu dokumentieren.
Mindestens folgende Informationen werden erwartet:

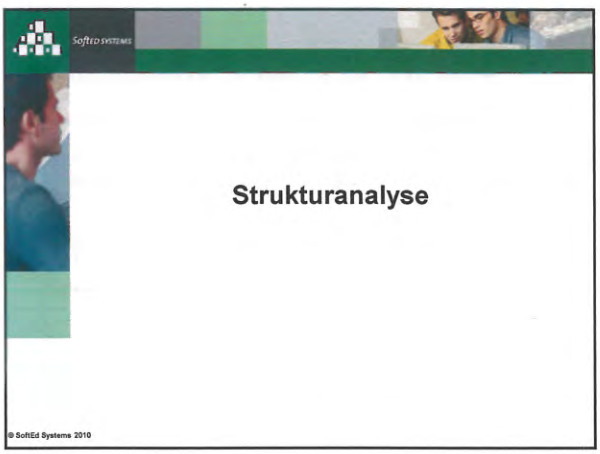
1. **Bedeutung der IT für die Arbeiten der Organisation**
2. **Sollziele für die ITSicherheit**
3. **Strategie zur Erreichung der Ziele**
4. **Dafür notwendige interne Organisationsstrukturen, Richtlinien, Regeln und Vorgaben**

Kurs der Leitlinie auf BSI-Internetseite
IT-Grundschutz
-> Download
-> alle Hilfsmittel
-> Muster
-> Muster Richtlinien

Sicherheitskonzept nach IT-Grundschutz-Vorgehensweise

Leitlinie soll eher unkonkret sein (ohne Namen, techn. Anlagen, Produkte) -> Ziele sollen definiert werden aber nicht zu genau, da diese sonst zu häufig angepasst werden muss.



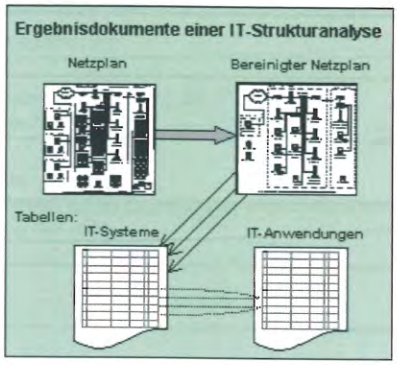


IT-Strukturanalyse

Teilaufgaben

- Erstellung bzw. Aktualisierung eines Netzplans (grafische Übersicht)
  - Komplexitätsreduktion durch Gruppenbildung
- Erhebung der IT-Systeme (Tabelle)
- Erfassung der IT-Anwendungen und der zugehörigen Informationen (Tabelle)

Netzplan



Strukturanalyse

Bei der IT- Strukturanalyse geht es darum, die erforderlichen Informationen zusammenzustellen und so aufzubereiten, dass sie die weiteren Schritte bei der Anwendung der Grundschutz-Kataloge unterstützen.

IT-Strukturanalyse

Komplexitätsreduktion im Netzplan

Gleichartige Komponenten sollten zu einer Gruppe zusammengefasst werden.

Voraussetzungen:

- gleicher Typ
- gleiche oder nahezu gleiche Konfiguration
- gleiche oder nahezu gleiche Netzanbindung (z. B. Anschluss am gleichen Switch)
- gleiche Rahmenbedingungen (Administration und Infrastruktur)
- gleiche Anwendungen

Bereinigung des Netzplans

Folgende Clients sollten **nicht zusammengefasst** werden:

- Bei den Rechnern der **Geschäftsführung** kann man von einem höheren Schutzbedarf ausgehen.
- Eine hohe Vertraulichkeit besitzen ferner auch die Daten, die in der **Personalabteilung** bearbeitet werden, sowie die Daten der **Finanz- und Lohnbuchhaltung**.
- Auf Rechnern der **IT- Administratoren** laufen Anwendungen, die für die Verwaltung des Netzes erforderlich sind. Von daher verlangen auch diese Rechner eine besondere Aufmerksamkeit.

IT-Strukturanalyse Darstellung der IT-Systeme

Nr.	Beschreibung	Plattform	Anz.	Standort	Status	Anwender/ Admin.
S1	Server für Personal-verwaltung	Windows NT Server	1	Bonn, R 1.01	in Betrieb	Personal-referat
S2	Primärer Domänen-Controller	Windows NT Server	1	Bonn, R 3.10	in Betrieb	alle IT-Anwender
C6	Gruppe der Laptops für den Standort Berlin	Laptop unter Windows 95	2	Berlin, R 2.0 1	in Betrieb	alle IT-Anwender in Berlin
N1	Router zum Internet-Zugang	Router	1	Bonn, R 3.09	in Betrieb	alle IT-Anwender
T1	TK-Anlage für Bonn	ISDN-TK-Anlage	1	Bonn, B.02	in Betrieb	alle Mitarb. in Bonn

IT-Strukturanalyse
Erfassung der IT-Anwendungen

Diejenigen IT-Anwendungen des jeweiligen IT-Systems,

- deren Daten bzw. Informationen und Programme den höchsten Bedarf an Geheimhaltung (Vertraulichkeit) besitzen,
- deren Daten bzw. Informationen und Programme den höchsten Bedarf an Korrektheit und Unverfälschtheit (Integrität) besitzen,
- die die kürzeste tolerierbare Ausfallzeit (höchster Bedarf an Verfügbarkeit) haben,

müssen erfasst werden.

Es ist nicht sinnvoll, alle IT-Anwendungen zu erfassen.

Tipp:

statt „IT-Anwendung" besser „IT-Verfahren" erfassen!

IT-Strukturanalyse
Beispiel: Liste der IT-Anwendungen

Beschreibung der IT-Anwendungen			IT-Systeme						
Anw.-Nr.	IT-Anwendung/ Informationen	Pers.-bez. Daten	S1	S2	S3	S4	S5	S6	S7
A1	Personaldaten-verarbeitung	X	X						
A4	Benutzer-Authentisierung	X		X				X	
A5	Systemmanagement			X					
A7	zentrale Dokumentenverwaltung					X			

Schutzbedarfsfeststellung

Schutzbedarfsfeststellung

Teilaufgaben

- Definition der Schutzbedarfskategorien
- Schutzbedarfsfeststellung für
  - IT-Anwendungen einschließlich ihrer Daten
  - IT-Systeme
  - Kommunikationsverbindungen
  - IT-Räume

  anhand von typischen Schadensszenarien
- Dokumentation der Ergebnisse

Schutzbedarf ist meist nicht quantifizierbar.
⇨ Beschränkung auf drei Kategorien

Schutzbedarfskategorie	
normal (niedrig bis mittel)	Die Schadensauswirkungen sind begrenzt und überschaubar.
hoch	Die Schadensauswirkungen können beträchtlich sein. (ca. das IT-Budget eines Jahres)
sehr hoch	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen. (> Jahres-IT-Budget oder > 10% Jahresumsatz)

Schutzbedarfsfeststellung - Schutzbedarfskategorien

- Schutzbedarfsfeststellung erfolgt immer bezüglich der Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit.
- Betrachtung von typischen Schadensszenarien aus Sicht der Anwender ("Was wäre, wenn... ?")
  - Verstoß gegen Gesetze, Vorschriften, Verträge
  - Beeinträchtigung des informationellen Selbstbestimmungsrechts
  - Beeinträchtigung der persönlichen Unversehrtheit
  - Beeinträchtigung der Aufgabenerfüllung
  - negative Außenwirkung
  - finanzielle Auswirkungen
- Individualisierung der Zuordnungstabelle!

Analyse Schutzbedarf

Sinnvoll ist es, die **Bedeutung** der einzelnen IT- Anwendungen **für die Geschäftsprozesse** anzugeben, ob also eine Aufgabe bei Ausfall der Anwendung gar nicht erledigt werden kann oder ob sie mit gewissem zusätzlichem Aufwand z. B. manuell durchgeführt werden kann.

Auswirkungen von Schäden

Niedriger bis mittlerer Schutzbedarf (normal):

"Der finanzielle Schaden ist kleiner als 50.000 Euro."

"Die Abläufe in der Firma werden allenfalls unerheblich beeinträchtigt. Ausfallzeiten von mehr als 24 Stunden können hingenommen werden."

Auswirkungen von Schäden

Hoher Schutzbedarf:

"Der mögliche finanzielle Schaden liegt zwischen 50.000 und 5.000.000 Euro."

"Die Abläufe in der Firma werden erheblich beeinträchtigt. Ausfallzeiten dürfen maximal 24 Stunden betragen."

Auswirkungen von Schäden

Sehr hoher Schutzbedarf:

"Der mögliche finanzielle Schaden beträgt mehr als 5.000.000 Euro.„

"Die Abläufe in der Firma werden so stark beeinträchtigt, dass Ausfallzeiten, die über 2 Stunden hinausgehen, nicht toleriert werden können."

Analyse Schutzbedarf

Der Schutzbedarf der drei Grundwerte *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* wird getrennt ermittelt und bleibt getrennt stehen, er wird nicht zusammengefasst.

Schutzbedarfsfeststellung Beispiel: IT-Anwendungen

IT-Anwendung			Schutzbedarfsfeststellung		
Nr.	**Bezeichnung**	**pers. Daten**	**Grund-wert**	**Schutz-bedarf**	**Begründung**
A1	Personaldaten-verarbeitung	×	Vertr.	hoch	schutzbedürft., personenbez. Daten, Gehaltsinformationen
			Integr.	mittel	Fehler werden rasch erkannt und korrigiert.
			Verf.	mittel	Ausfälle bis zu einer Woche können mittels manueller Verfahren überbrückt werden.
A2	Beihilfeab-wicklung	×	Vertr.	hoch	schutzbedürft., personenbez. Daten, z.T. Hinweise auf Erkrankungen etc.
			Integr.	mittel	Fehler werden rasch erkannt und korrigiert.
			Verf.	mittel	Ausfälle bis zu einer Woche können mittels manueller Verfahren überbrückt werden.

Schutzbedarfsfeststellung IT-Systeme

- **Maximumprinzip**
  Auf einem IT-System können mehrere Anwendungen laufen. Im Wesentlichen bestimmt der Schaden mit den schwerwiegendsten Auswirkungen den Schutzbedarf des IT-Systems.
- **Kumulationseffekt**
  Durch Kumulation mehrerer (z.B. kleinerer) Schäden entsteht ein insgesamt höherer Gesamtschaden. Der Schutzbedarf des IT-Systems erhöht sich dann entsprechend.
- **Verteilungseffekt**
  - Eine IT-Anwendung überträgt ihren hohen Schutzbedarf nicht auf ein IT-System, weil auf diesem IT-System nur unwesentliche Teile der IT-Anwendung laufen.
  - Bei redundanter Systemauslegung ist der Schutzbedarf der Einzelkomponenten niedriger als der Schutzbedarf der Gesamtanwendung.

Schutzbedarfsfeststellung Beispiel: IT-Systeme

IT-System		Schutzbedarfsfeststellung		
Nr.	Bezeichnung	Grund-wert	Schutz-bedarf	Begründung
S1	Server für Personalverw. alt	Vertr.	hoch	Maximumprinzip
		Integr.	mittel	Maximumprinzip
		Verf.	mittel	Maximumprinzip
S2	Primärer Domänen-Controller	Vertr.	mittel	Maximumprinzip
		Integr.	hoch	Maximumprinzip
		Verf.	mittel	Verteilungseffekt: mehrere Domänencontroller im Einsatz

Schutzbedarfsfeststellung Kommunikationsverbindungen

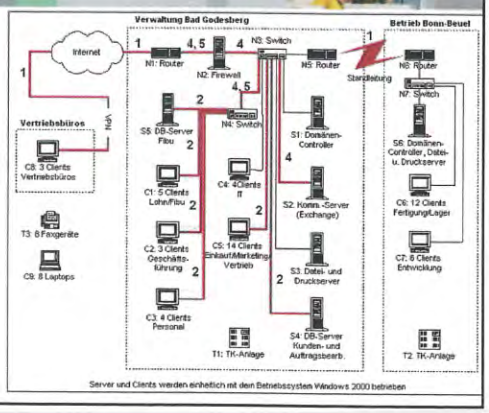
Folgende Kommunikationsverbindungen sind kritisch:

- Außenverbindungen (1)
- Übertragung von hochschutzbedürftigen Informationen
  - Schutzbedarf resultiert aus Vertraulichkeit (2)
  - Schutzbedarf resultiert aus Integrität (3)
  - Schutzbedarf resultiert aus Verfügbarkeit (4)
- Hochschutzbedürftige Informationen dürfen auf keinen Fall übertragen werden. (5)

➔ Verbindungen im Netzplan grafisch hervorheben

➔ tabellarische Dokumentation

Bsp.:

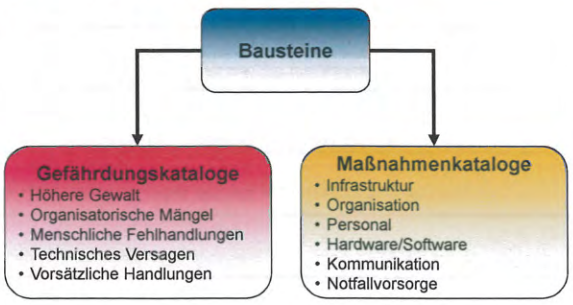


Schutzbedarfsfeststellung
Beispiel: IT-Räume

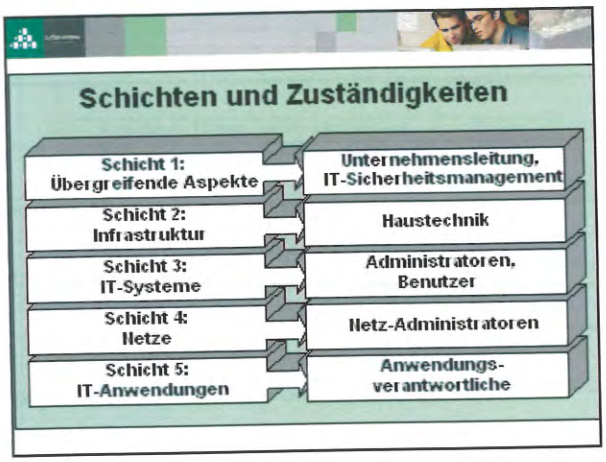
Raum			IT	Schutzbedarf		
Bez.	Art	Lokation	IT-Syst./ Datentr.	Vertr.	Integr.	Verf.
R U.02	Datenträger-archiv	G. Bonn	Backup-Datentr.	hoch	hoch	mittel
R B.02	Technikraum	G. Bonn	TK-Anlage	mittel	mittel	hoch
R E.03	Serverraum	G. Berlin	S6, N6, N7	mittel	hoch	hoch
R 2.01 - R 2.40	Büroräume	G. Berlin	C4	mittel	mittel	mittel

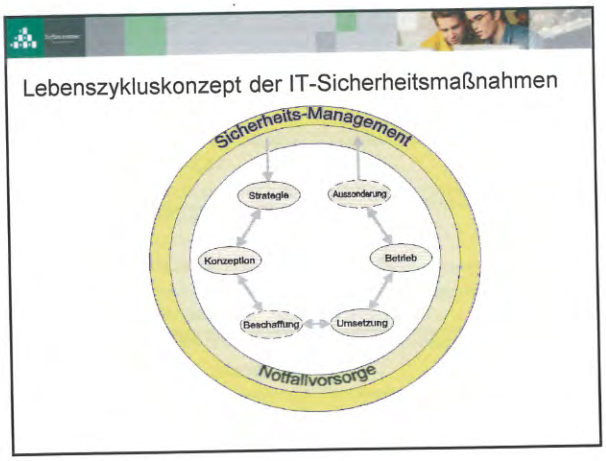
Modellierung

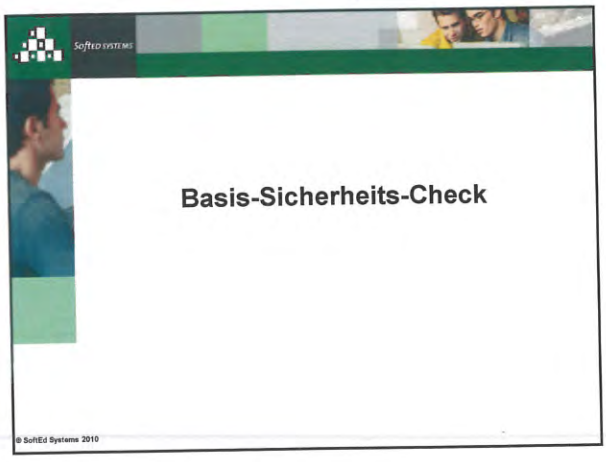
Struktur der Grundschutzkataloge



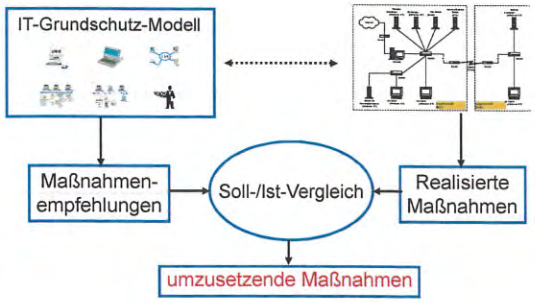
BSI Grundschutz
→ Kataloge
→ Bausteine


Schichten und Zuständigkeiten
Schicht 1: Übergreifende Aspekte
Unternehmensleitung, IT-Sicherheitsmanagement
Schicht 2: Infrastruktur
Haustechnik
Schicht 3: IT-Systeme
Administratoren, Benutzer
Schicht 4: Netze
Netz-Administratoren
Schicht 5: IT-Anwendungen
Anwendungs-verantwortliche


Lebenszykluskonzept der IT-Sicherheitsmaßnahmen
Sicherheits-Management
Strategie
Aussonderung
Konzeption
Betrieb
Beschaffung
Umsetzung
Notfallvorsorge


Basis-Sicherheits-Check
© SoftEd Systems 2010

Basis-Sicherheitscheck



Basis-Sicherheitscheck
Umsetzungsstatus

Mögliche Umsetzungsstatus einzelner Maßnahmen:

- "ja"
  - Alle Empfehlungen sind vollständig und wirksam umgesetzt.
- "entbehrlich" – Begründung erforderlich:
  - Umsetzung ist nicht notwendig, da Gefährdungen durch andere adäquate Maßnahmen entgegengewirkt wird.
  - nicht relevant, weil z. B. Dienste nicht aktiv
- "teilweise"
- "nein"

Siegelstufen

- A – Einstiegsstufe
- A, B – Aufbaustufe
- A, B, C – Zertifikat
- Z – Optional, bei höherem Schutzbedarf eventuell erforderlich
- W – Wissen, dient nur zur Information und ist nicht zertifizierungsrelevant

Realisierung von IT-Sicherheitsmaßnahmen I

Schritt 1: Sichtung der Untersuchungsergebnisse
- Welche Maßnahmen sind nicht oder nur teilweise umgesetzt?

Schritt 2: Konsolidierung der Maßnahmen
- Welche IT-Grundschutzmaßnahmen werden durch höher- oder gleichwertige Maßnahmen ersetzt?
- Welche Maßnahmenempfehlungen müssen noch an die individuellen Gegebenheiten angepasst werden?

Schritt 3: Kosten- und Aufwandsschätzung
- Welche einmaligen/wiederkehrenden Investitions- bzw. Personalkosten entstehen?
- Wenn das zur Verfügung stehende Budget nicht ausreicht, sollten Ersatzmaßnahmen ergriffen werden und das verbleibende Restrisiko für die Leitungsebene dokumentiert werden.

Realisierung von IT-Sicherheitsmaßnahmen II

Schritt 4: Festlegung der Umsetzungsreihenfolge
- Welche fehlenden Maßnahmen sollten zuerst umgesetzt werden?
- Breitenwirkung beachten!

Schritt 5: Festlegung der Verantwortlichkeit
- Wer setzt welche Maßnahme bis wann um?

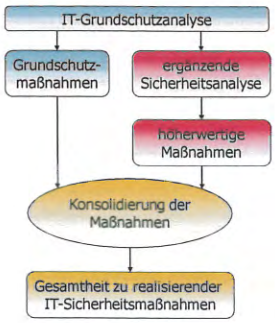
Schritt 6: Realisierungsbegleitende Maßnahmen
- Schulung der Mitarbeiter
- Sensibilisierung der Mitarbeiter zur Erhöhung der Akzeptanz der IT-Sicherheitsmaßnahmen

Wenige fehlende Maßnahmen? Wenig personelle oder finanzielle Ressourcen erforderlich? => Schritte 1,3,4 können entfallen

Ergänzende Sicherheitsanalyse

Eine ergänzende Sicherheits-analyse ist durchzuführen, wenn

- hoher oder sehr hoher Schutzbedarf vorliegt,
- zusätzlicher Analysebedarf besteht oder
- für bestimmte Aspekte kein geeigneter Baustein existiert.



BSI-Standard 100-3

Risikoanalyse auf der Basis von IT-Grundschutz

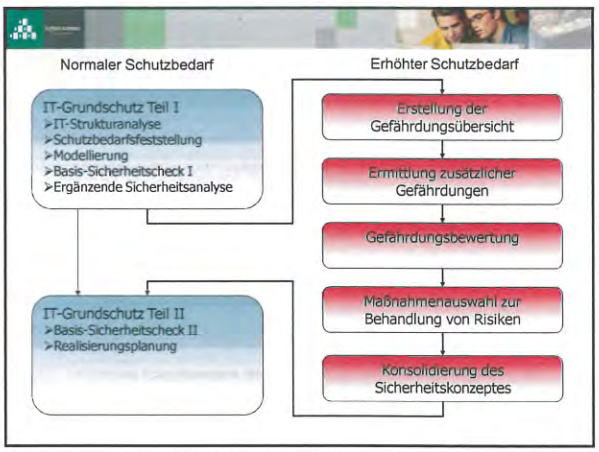
Einsatzbereich

- für Systeme, die einen **hohen** oder **sehr hohen** Schutzbedarf bezüglich eines der drei Grundwerte Vertraulichkeit, Verfügbarkei oder Integrität haben
- für Systeme, die mit Bausteinen nicht abgebildet werden können
- für spezielle Einsatzszenarien

Grundschutz-Maßnahmen A,B,C

Schutzwirkung von Standard-Sicherheitsmaßnahmen nach IT-Grundschutz sind

- für die Schutzbedarfskategorie „normal"
  - im Allgemeinen ausreichend und angemessen,
- für die Schutzbedarfskategorie "hoch"
  - Basisschutz,
  - unter Umständen nicht ausreichend; ergänzende Sicherheitsanalyse bestimmt, ob zusätzliche Sicherheitsmaßnahmen durch Risikoanalyse ermittelt werden müssen,
- für die Schutzbedarfskategorie "sehr hoch"
  - Basisschutz,
  - im Allgemeinen nicht ausreichend, so dass eine Risikoanalyse notwendig ist.



Gefährdungsübersicht

- Streichen aller nicht relevanten Objekte und Bausteine
- Ermittlung der Gefährdungen und thematische Sortierung
- Ermittlung zusätzlicher Gefährdungen
  - Dokumentation des Herstellers
  - Schwachstellenpublikation im Internet
  - Bedrohungsanalysen

BSI
Downloads
↳ Gefährdungskatalog

Gefährdungsbewertung

Bewertung der vorhandenen Sicherheitsmaßnahmen auf

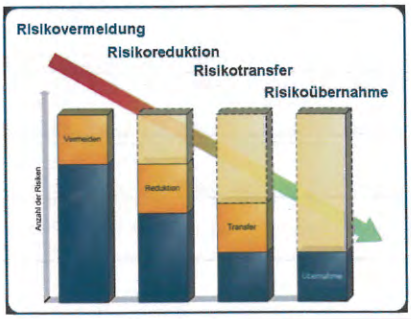
- Vollständigkeit
  - Alle Türen sind verschlossen.
- Mechanismenstärke
  - Die Türen haben eine ausreichende Festigkeit.
- Zuverlässigkeit
  - Ich kann nicht durch das Fenster einsteigen.

Bestimmung der bisher nicht ausreichend abgesicherten Gefährdungen

Behandlung von Risiken

- Risiko-Vermeidung
  - durch Umstrukturierung
- Risiko-Reduktion
  - durch weitere Sicherheitsmaßnahmen
- Risiko-Transfer
  - Versicherungen
  - Outsourcing
- Risiko-Übernahme

Behandlung von Risiken



Konsolidierung des
IT-Sicherheitskonzeptes

- Eignung der Maßnahmen zur Abwehr der Gefährdungen
- Zusammenwirken der Maßnahmen
- Benutzerfreundlichkeit der Maßnahmen
- Angemessenheit der Maßnahmen

- Rückführung in den IT-Sicherheitsprozess

BSI
↳ Kataloge
↳ übergreifende Aspekte
↳ Notfallmanagement

BSI-Standard 100-4

Notfallmanagement

Informationssicherheit ⇔ Business Continuity

- Ziel von ISM: Gewährleisten von **Vertraulichkeit, Integrität und Verfügbarkeit von Informationen,** Anwendungen und IT-Systemen in einem für das Geschäft angemessenen Niveau ⇒ Schaden verhindern / minimieren
- Paradigmenwechsel IT → Informationssicherheit und Ganzheitlichkeit

- Ziel von BCM: Gewährleisten der **Verfügbarkeit kritischer Prozesse** auf einem akzeptablen Niveau ⇒ Schaden verhindern / minimieren
- Steigende Abhängigkeit von der IT
- Steigende Vernetzung

Gemeinsamkeiten

- Gemeinsame Verantwortung im Top-Management
  - Verankerung in den Fachbereichen
  - Abstimmung der Funktionen, Verantwortlichkeiten und des Berichtswesens
- Ressourcen und Investitionen (ROI)
  - Abstimmung der Methoden Schutzbedarfsfeststellung, BIA und Risikoanalysen
- Auswahl der Maßnahmen optimiert für ISM und BCM

Kritikalitätskategorien

Notfallmanagement IT-Sicherheit

Kritikalitätskategorien		Schutzbedarfskategorien	
Unkritisch	Ausfall hat keine oder nur minimale Auswirkungen		
Wenig kritisch	Ausfall hat Auswirkungen	Normal	Die Schadensauswirkungen sind begrenzt und überschaubar.
Kritisch	Ausfall hat beträchtliche Auswirkungen	Hoch	Die Schadensauswirkungen können beträchtlich sein.
Hoch kritisch	Ausfall oder Beeinträchtigung führen zu existenziell bedrohlichen Auswirkungen	Sehr hoch	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Kritikalitätsanalyse eines Geschäftsprozesses

	< 12 h	12 h – 3d	3 – 10 d	11 – 30 d	> 30 d
Finanzielle Auswirkungen	Unkritisch	Kritisch	Hoch kritisch	Hoch kritisch	Hoch kritisch
Beeinträchtigung der Aufgabenerfüllung	Unkritisch	Unkritisch	Wenig kritisch	Kritisch	Hoch kritisch
Verstoß gegen Gesetze	Unkritisch	Unkritisch	Unkritisch	Unkritisch	Unkritisch
Negative Innen- und Außenwirkung	Unkritisch	Unkritisch	Unkritisch	Wenig kritisch	Wenig kritisch

Priorisierung der Geschäftsprozesse

- Prozessabhängigkeiten
- Geschäftsziele
  - „Top-Down"-Ansatz
- Beachtung besonderer Termine
- Abgleich der Wiederanlaufzeiten → Abhängigkeiten im Ablauf

BIA – Bericht (Business Impact Analyse)

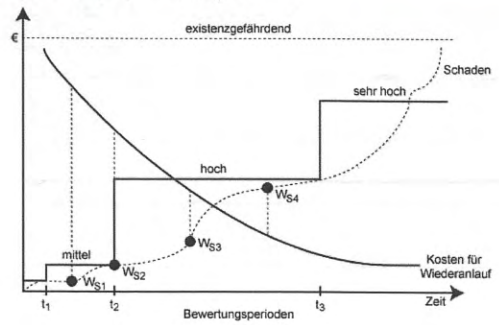
Strategieoptionen für Prozesse

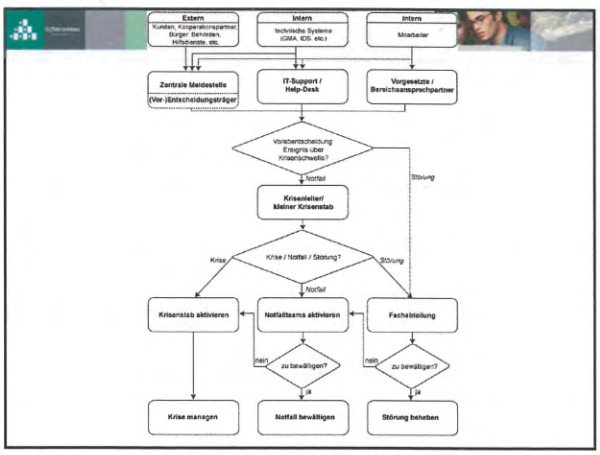
	Prozess: Rechenzentrumsbetrieb
Minimale Lösung	Dienstleistungsvertrag für den Notbetrieb
Kleine Lösung	„Cold-standby"-Ausweich-Rechenzentrum
Mittlere Lösung	„Warm-standby"-Ausweich-Rechenzentrum
Große Lösung	„Hot-standby"-Ausweich-Rechenzentrum

Strategieoptionen für Prozesse

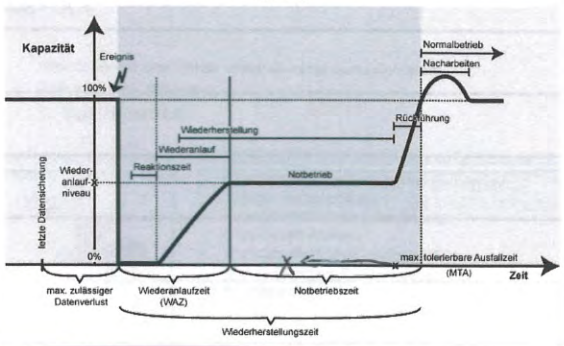
	Prozess: Arbeitsplatz-Management
Minimale Lösung	Interne Lösung: Freisetzung und Heimarbeitsplätze für die Arbeitsplätze mit höchster Priorität
Kleine Lösung	Lösung mit kooperierenden Partnerschaften
Mittlere Lösung	Kommerzieller Dienstleistungsvertrag „bezugsfertiges Bürogebäude"
Große Lösung	Zweites eigenes Bürogebäude

Kosten – Nutzen – Analyse





Phasen der Notfallbewältigung



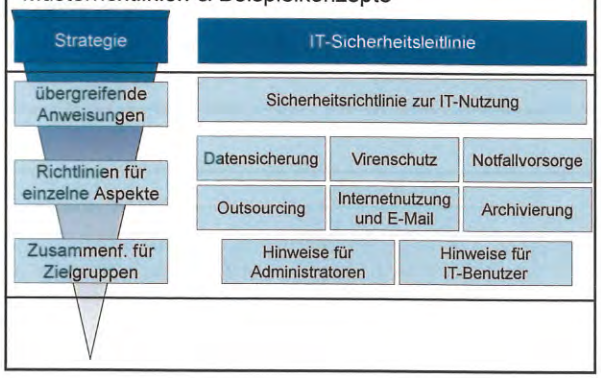
Krisenkommunikation

Werkzeuge

Leitfaden IT-Sicherheit

- **Zielgruppe:** Einsteiger, Management, eilige Leser, kleine und mittlere Unternehmen und Behörden
- **Idee:** Die wichtigsten Fakten zur IT-Sicherheit komprimiert auf wenigen Seiten
- **Darstellung:** nachvollziehbar, nah an der Realität
- **Schwerpunkt:** Organisation und Prozesse, technische Hinweise, doch ohne Details
- Kein "IT-Grundschutz light"
- Kurzüberblick über IT-Grundschutz und Motivation zur vertieften Beschäftigung mit IT-Sicherheit

Musterrichtlinien & Beispielkonzepte



Weitere Hilfsmittel

- Formblätter, Maßnahmenlisten etc.
- Kreuzreferenztabellen (Zuordnung von Maßnahmen zu Gefährdungen)
- Technische Zusatzinformationen zu Bausteinen
- Beispiele von Grundschutz-Anwendern, z. B.:
  - Muster für Dienstvereinbarungen
  - Richtlinien
  - Sicherheitsleitlinien
  - Bausteine für Themen, die nicht in den Grundschutz-Katalogen behandelt werden

BSI
1) Download
↳ Formblätter für die Grundschutzerhebung
2) ↳ Grundschutzkataloge

GSTOOL

- Informationen und Preise unter www.bsi.bund.de/gstool
- Bezugsquelle: Download
- 30 Tage Testversion

Funktionalität
- Erfassung von IT-Systemen, Anwendungen usw.
- Schutzbedarfsfeststellung
- Auswahl der Bausteine (Modellierung)
- Basis-Sicherheitscheck
- unterstützt die IT-Grundschutz-Zertifizierung
- Kostenauswertung, Revisionsunterstützung
- Berichterstellung

(PRO mit Einschränkungen)
Verinice = Alternative
↳ Link anderer Tools
bei BSI unter GSTOOL
Andere Tools lesbar
(Kronsoft + IT-Scout nicht unbedingt empfohlen (teuer bzw. ohne Updates)
↳ GSTOOL selbst als Projekt beendet

Windows 2003 Server werden ab 2015 nicht mehr supported

Schichtmodell

1.11 Outsourcing → Lohn- u. Gehaltsabr. zählt dazu

Reihenfolge

1) Leitlinie
2) vereinfachter Netzplan
3) Schutzbedarfsermittlung
4) Umsetzgs.-grad (grafisch) ← GF zur Kenntnisnahme)
5) Ergänzende Sicherheitsanalyse für „Hoch" u. ~~Sehr~~ „Sehr Hoch"
   ↳ Risikoanalyse
      ↳ zusätzliche Gefährdungen abschätzen anhand vorschlägen oder Einspielen eigener Gefährdungen → Maßnahmen feststellen und Umsetzg. kontrollieren

Weitere Infos

www.BSI.bund.de → IT-Grundschutz → Download
→ Sonstige Veröffentlichungen
→ IT-Grundschutz-Profile (Bsp. für div. Unternehmensgrößen)

→ IT-Grundschutz-GSTOOL → Download
→ Beispieldatenbanken
→ ~~in Vollversion über Import/Exp. einlesbar~~
→ ~~[illegible]~~ anonymisiert
Texte z. Ablauf vorh.
(Erläuterungen z. Beispiel)