Datenschutz

- Die Regelungen – für das Unternehmen – münden in einer Privacy – Policy.
- Dort werden die fundamentalen Verhaltenregeln des Unternehmens zu pDaten festgeschrieben
- Die Beschäftigten werden über diese Regelungen unterrichtet

Beispiel

- "Es wird grundsätzlich gefragt, ob der Kunde damit einverstanden ist, Werbung zu erhalten, er erhält nur dann Werbung, wenn er zustimmt"
- "Jeder MA wird zu Anfang seiner Tätigkeit auf das Datengeheimnis verpflichtet, diese Verpflichtung wird in Verbindung mit einer 30 minütigen Schulung alle 2 Jahre wiederholt.."

Datenschutz - Datensicherheit

- Anlage zu § 9 BDSG
- Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle)
- zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),

Warum Datensicherheit

- Zugriffskontrolle
- Eingabekontrolle
- Weitergabekontrolle
- Verfügbarkeitskontrolle
- Diese Anlage wird als Argumentationshilfe zu Fragen der Datensicherheit genutzt.
- Was heisst nun aber Datensicherheit ?

Datensicherheit *(data security)*

- Sachlage, bei der Daten* unmittelbar oder mittelbar so weit wie möglich vor Beeinträchtigung oder Mißbrauch bewahrt sind, und zwar unter Berücksichtigung verarbeitungsfremder Risiken wie auch im Verlauf auftrags- und ordnungsgemäßer Erbringung einer Datenverarbeitungsleistung*

Fortsetzung

- Daten dürfen also weder bei datenverarbeitenden Prozessen oder auftragsbedingten Vor- und Nacharbeiten noch in Funktionseinheiten zur Abwicklung auftragsbedingter Arbeiten , noch durch das das Handeln von an auftragsbedingten Arbeiten beteiligten Personen beeinträchtigt werden.
- Anmerkung: Beeinträchtigung von Daten umfaßt u.a. Verlust, Zerstörung, Verfälschung.

IT-Sicherheit *(it-security)*

- Sachlage, bei der *IT-Systeme oder deren Komponenten* unmittelbar oder mittelbar so weit wie möglich vor Beeinträchtigung oder Mißbrauch bewahrt sind, und zwar unter Berücksichtigung verarbeitungsfremder Risiken wie auch im Verlauf auftrags- und ordnungsgemäßer Erbringung einer Datenverarbeitungsleistung.

Daten dürfen also

- weder bei datenverarbeitenden Prozessen
- oder auftragsbedingten Vor- und Nacharbeiten noch in Funktionseinheiten zur Abwicklung auftragsbedingter Arbeiten
- noch durch das Handeln von an auftragsbedingten Arbeiten beteiligten Personen beeinträchtigt werden.

Datensicherung
(data security measures)

- Maßnahmen und Einrichtungen, die Datensicherheit herbeiführen oder aufrechterhalten.
- *Anmerkung:* Beeinträchtigung von Daten umfaßt u.a. Verlust, Zerstörung, Verfälschung.

IT Security

- The objective of security in information systems is the protection of the interests of those relying on information systems from harm resulting from failures of availability, confidentiality, and integrity.
- ***Protection of the interests*** kann sowohl als Beherrschbarkeit als auch als Verläßlichkeit verstanden werden.

IT-Sicherheit *(it-security)*

- IT-Sicherheit ist eine dem Individuum und der Gesellschaft bekannte und verständliche Sachlage, bei der das *Risiko*, das mit einem informationstechnischen Vorgang oder Zustand verbunden ist, das *Grenzrisiko* nicht überschreitet, daß jedes Individuum für sich hieraus, früher oder später, erfahren könnte: eine Beeinträchtigung oder Verlust von Geist, Körper, Seele, Freiheit, Lebenssraum, Hab und Gut.

Anmerkungen

- Die in der IT auftretenden Risiken sind sowohl Folgeschäden der **unbefugten Nutzung** von Daten und Funktionen, verursacht durch (menschliche) Fahrlässsigkeit oder Absicht, Oder Schäden, die aus **konstruktiven oder materiellen Fehlern** erwachsen.

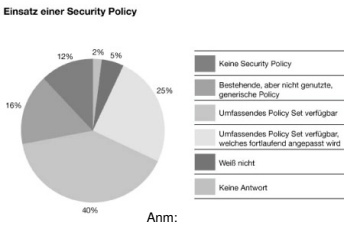
Datenschutz (*privacy protection*)

- eine *Menge von Anforderungen*, die die Zulässigkeit der Zugriffe auf Daten und die Ausführbarkeit der Informationsgewinnung aus Daten festlegen
- Def. GDD 1988
- Quelle: Dierstein „Datensicherheit Vortrag bei der GDD“

Das war die Theorie

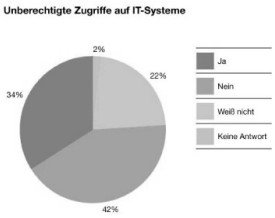
- Praxis:
  - Bei einer Studie von AA erklären 85 % aller Befragten, das sie über „ein Paket von einander ergänzender IT-Sicherheitsstrategien verfügen“
  - Nur 25 Prozent der Befragten meinen allerdings, dass dieses Paket permanent überwacht und aktualisiert wird.

Security Policy



Anm:
16 Prozent geben an, über eine Security Policy zu verfügen, sie aber nicht zu benutzen

Unberechtigte Zugriffe auf Systeme



Kernaussagen:
- 94 Prozent der Befragten bewerten die Vertraulichkeit und Integrität der Unternehmensdaten als wichtig oder sehr wichtig.
- 44 Prozent der Hackerangriffe sind unternehmensintern, 55 Prozent kommen von außen

Quelle:
„IT-Sicherheit in Europa (Andersen)“
05.2002

Datensicherheit

- Wie wird Datensicherheit eingeführt ?
- Wer definiert Datensicherheit ?
- Für was wird Datensicherheit definiert ?
- Wie geht man vor ?
- Welche Ansatzpunkte ?

Fundamentalkomponenten eines sicheren Systems

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Zurechenbarkeit
- Rechtsverbindlichkeit

Im Einzelnen

- Vertraulichkeit
  - kein Einsehen von Daten oder Erschließen von Information
  - kontrollierter Zugriff auf Daten und Funktionen
  - Informationen vor unberechtigter Kenntnisnahme schützen
- Integrität
  - keine unbemerkte Veränderung der Daten
  - keine unbemerkten Veränderungen der Funktionen
  - Schutz gegen zufällige oder absichtliche Veränderung
- Verfügbarkeit
  - Ausführung von Funktionen zum geforderten Zeitpunkt
  - und im geforderten Zeitrahmen (nix Win95 !)

Erweiterung (*)

- Zurechenbarkeit
  - Wer hat wann was veranlasst ?
- Verbindlichkeit
  - Sicherstellen von Authentizität von Kommunikationspartner und Urheberschaft von Informationen, vor allem bei Übertragung
- Rechtsverbindlich
  - Ist die durchgeführte Aktion rechtsverbindlich
  - Muss sie es sein ? (E-Commerce)
  - SigG ?
  - GOB ?

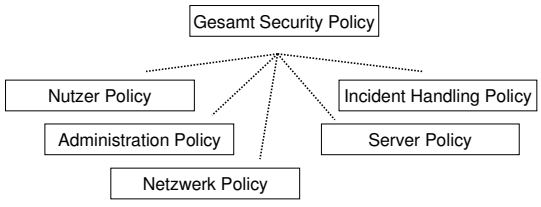
Möglicher Weg (!)

- Globale Security Policy
- Sicherheitskonzept (Policy) für die einzelnen Jobs (Dienstleistungen, Datenbanken, Web-Anbindung, ...)
- Entsorgung
- Wartungsverträge
- Auftragsdatenverarbeitung
- Produktbezogene Richtlinien

Warum Sicherheitspolicy

- Forderungen aus:
- IT-Abteilung
- Wirtschaftsprüfer
- Auditing
- Vorstand
- KontraG (Risikofrüherkennung)
- E-Business
- ...

Policy Aufbau



Inhalt einer Policy

- Formaler Teil
- Adressatenkreis
- Motivation
- Gegenstand der zu erledigen ist
- Regeln
- Anhang mit Glossar, Quellen und Abkürzungen

Probleme

- Komplexität
  - Heterogene Systeme und Netze, mehrere Betriebssysteme, Middleware etc.
- Verteilung
  - Über Standorte, Komponenten
- Änderungsrate
  - Permanente Änderungen der HW und Software

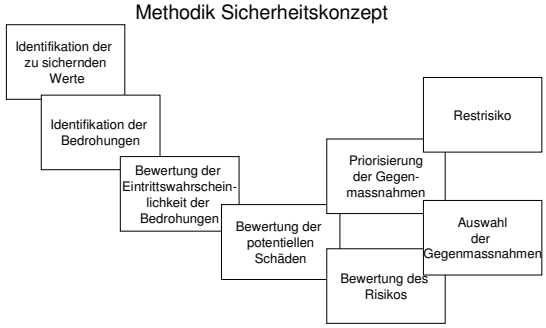
Anspruch

- Angemessenes Sicherheitsniveau
- Keine Behinderung für operatives Geschäft
- Nachweisbarkeit
- Messbar

Sicherheitskonzept

- Bezogen auf eine Anwendung oder ein Produkt
- Abgeleitet aus der Security Policy
- Spezifische Regelungen zu dieser Software
- I.d.R. nur Vorgaben was einzuhalten ist
- In enger Absprache mit dem Kunden

Methodik Sicherheitskonzept



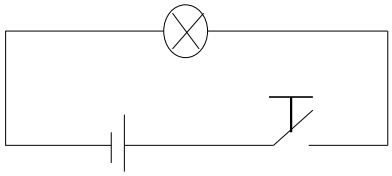
0. Analyse der Kundenwünsche

- Basierend auf den Fundamentalkomponenten wird der Kunde - der muss auch zahlen - gefragt, welche dieser Komponenten für ihn von Bedeutung sind und welche nicht
- Allgemein geht man von einem gewissen “Grundschutz” aus
- D.h. niemand erwartet heute das ein System 3 Tage ausfällt, ohne das es bemerkt wird

1. Bedrohungen

- Welche Bedrohungen gibt es für dieses System ?
- Ausgehend von der richtigen - d.h. vollständigen - Funktion, was kann nicht funktionieren ?
- Die Bedrohungen ergeben sich in erster Linie aus dem Negieren der vollständigen Funktion

Beispiel



Funktion:
Wenn der Taster gedrückt wird, brennt die Lampe
Wenn der Taster losgelassen wird, geht die Lampe aus

2. Schwachstellen

- Basierend auf den Bedrohungen des Systems, werden die Schwachstellen herausgearbeitet
- Jede Schwachstelle wird mit einer Gegenmassnahme versehen
- Das Risiko eines Eintretens der Schwachstelle wird i.d.R. mit einer Kennzahl oder einem Risikowert versehen

Risikowert

- Hier spielt das Expertenwissen eine Rolle
- Die Werte sind naturgemäß nicht nachprüfbar, sondern nur nachvollziehbar - oder auch nicht (!) -
- Der Rechenweg ist dabei von Unternehmen zu Unternehmen mehr als unterschiedlich

Risiken

- R = P * S (Risiko = Eintrittswahrscheinlichkeit * Schadenswert
- R = N * A * B (Risiko = NICHTEntdeckungswahrscheinlichkeit * Auftretenswahrscheinlichkeit * Bedeutung)
- Günstig ist es hier, den einzelnen Werten Bezugsgrößen zuzuordnen

Beispiel für A (Auftreten)

- „unwahrscheinlich": Fehler wird nicht eintreten, Auftreten ist sehr unwahrscheinlich aber denkbar - 1
- „niedrig": Auftreten ist unwahrscheinlich, aber möglich. 2-3
- „mittel": Kann auftreten, es ist damit zu rechnen - 4-6
- „hoch": Kann aus technischer Sicht auftreten, wird aus mögl. technischer Sicht auftreten 7-8
- „sehr hoch": Dieser Schaden wird auftreten 9-10

Beispiel E (Entdeckung)

- Fehler wird unmittelbar entdeckt, bevor der Schaden eintreten kann. Die Fehlerursache wird behoben. (1)
- Der Fehler äußert sich erst durch das Auftreten eines Schadens. Die Fehlerursache kann beseitigt werden. Das Schadensausmaß kann noch begrenzt werden. (4)
- Der Fehler wird erst durch den Schaden entdeckt. Die Beseitigung der Fehlerursache hilft nicht mehr. Eine Wiederholung des Fehlers kann dadurch aber verhindert werden. (7)
- Der Fehler verursacht Schäden. Der Zusammenhang mit der Fehlerursache ist nicht mehr erkennbar. Irreversible Schäden die wiederholt auftreten (10)

Beispiel B (Bedeutung)

- Auftretender Schaden niedrig, Größenordnung (Peanuts) Summe < 0,01% Jahresumsatz (1)
- Mittlere Auswirkungen des Schadens Summe < 0,1 % Jahresumsatz (4)
- Schwerwiegender Schaden Summe < 1 % (7)
- Bedrohlich für den Fortbestand des Unternehmens

Summe > 1 % (10)

Nach dieser Abschätzung

- Die gefundenen Schwachstellen werden zusammen mit dem Kunden diskutiert
- Der Kunde entscheidet, welche Schwachstellen wie behoben werden -> Priorisierung
- Die restlichen Schwachstellen gelten als Restrisiko und müssen vom Kunden getragen werden -> Restrisiken

Anwenden der Methodik

- Geg: NOZAMA - Web Buchhändler
- Anforderungen an das System:
  - Jeder Kunde soll den aktuellen Bestand an vorhandenen Büchern erkennen können
  - aus diesem Vorrat soll er eines oder mehrere Bücher aussuchen können
  - Die Auswahl soll gespeichert werden und nach der Angabe einer Adresse - Gültigkeit der Adresse (!) - zugeschickt werden

Anforderungen

- Die Übertragung von pDaten soll verschlüsselt erfolgen
- Die Nutzer sollen sich auch registrieren können (auf Wunsch)
- Jeder Kunde soll nur auf seine eigenen Bestellungen Zugriff haben
- Die Erreichbarkeit soll bei 99,9 % liegen

Alternativ

- Vorgehen nach Grundschutzhandbuch BSI
- Kastenvorgehen
- Für jedes Betriebssystem Vorschläge zur Absicherung - Welche Maßnahmen sind vorzunehmen
- Gilt auch für “bekanntere” Anwendungen wie z.B. SAP

Grundschutzhandbuch

- Einzelne Bausteine werden auf die vorhandene Infrastruktur angewendet
- Danach sollen diese Systeme nach IT Grundschutzhandbuch sicher sein