IT-Sicherheitspolitik

“Transilvania” Universität Brasov

Inhaltsverzeichnis

- Risikoanalyse
- Risikomanagement
- Sicherheitskonzept
- Sicherheitsmanagement

Inhalt

1. Einführung
2. Risikoanalyse
3. Risikomanagement
4. Sicherheitskonzept
5. Sicherheitsmanagement
6. Folgerung

Einführung

- Allgemeine Begriffe
- Corporate IT Risk Management

Allgemeine Begriffe

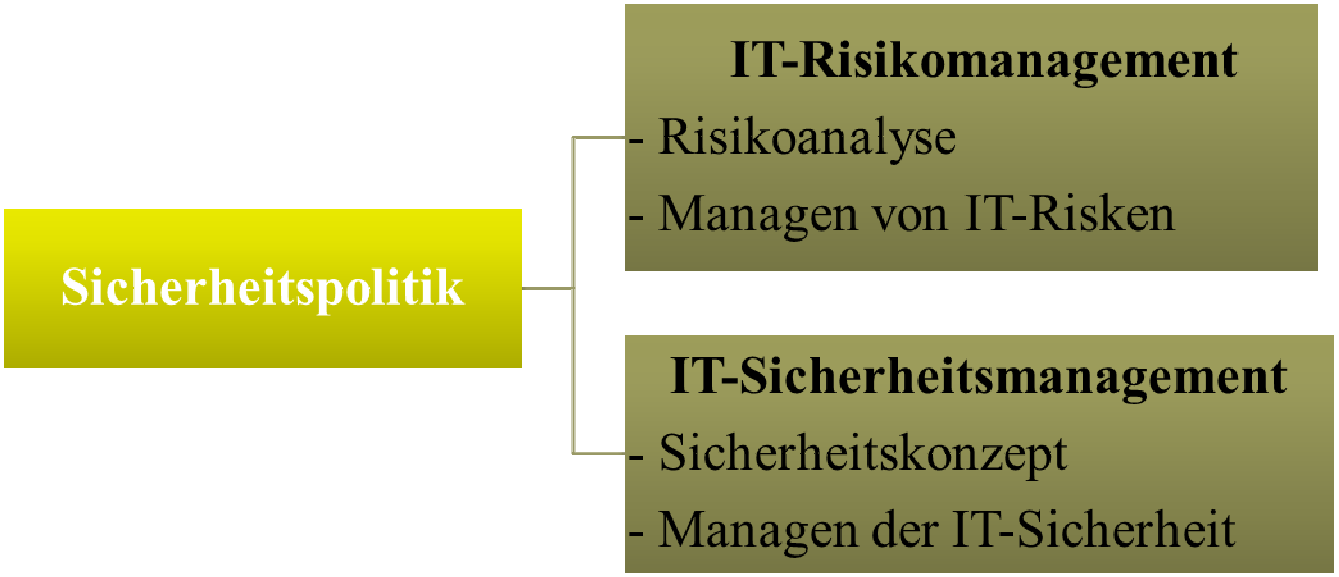
- Die Sicherheitspolitik ist die Sicherheitmaßnahme gegen die IT-Risiken
- Es gibt zwei hemmende Faktoren des Risikomanagements, und zwar:
  1) „Dafür haben wir kein Budget.“ – Werden die Kosten für die Risikomanagement zu hoch sein?; Was passiert, wenn man kein Sicherheitsmanagement hat?
  2) „Bei uns ist doch noch nie was passiert.“ - Kann man Angriffe entdecken?; Werden Schäden bilanziert?

Allgemeine Begriffe(2)

- Neben Risikomanagement und Sicherheit müssen wir auch berücksichtigen:
  1) Risikomanagement und Sicherheit müssen gemessen werden, weil nicht alles gesichert werden muss
  2) Es muss bestimmt werden, welches Risiko durch Sicherheitsmaßnahmen abgedeckt werden soll
  3) Die Existenz von Alternativtechnologien muss geprüft werden
  4) Es gibt Risiken bei denen man vorher Schutzmassnahmen nehmen soll, aber es gibt Risiken mit dem man leben kann

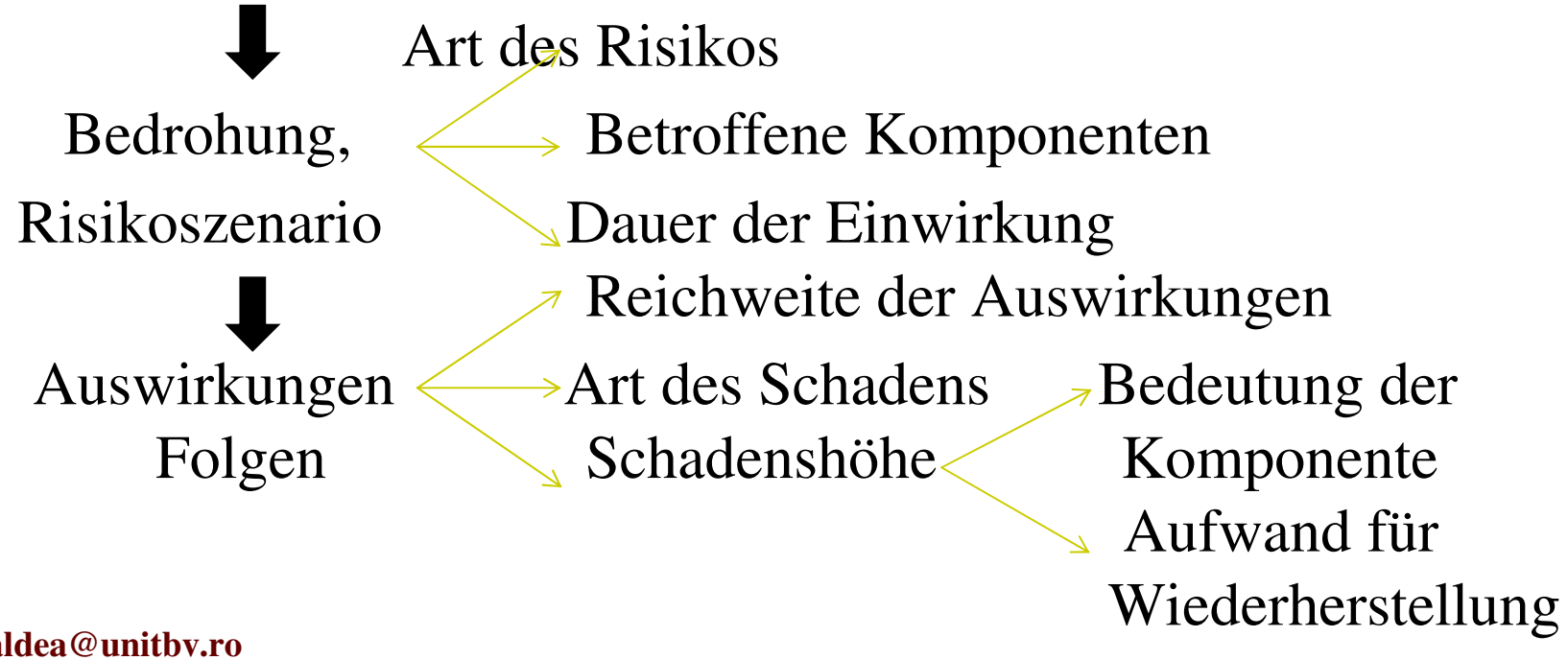
Allgemeine Begriffe(3)

- Die Branchen der Sicherheitspolitik



Corporate IT Risk Management

- IT-Risikomanagement wird zur Führungsaufgabe der Unternehmenleistung, des Fachbereichsleiter und des Netzadministrator.
- Schwachstelle + Angriffspfad + Auslöser



Risikoanalyse

- Bestandsaufnahme
- Bedrohungsanalyse
- Internet Angriffe
- Untersuchung der Schadenshöhe
- Sicherheitsanforderungen
- Ermittlung der Eintrittswahrscheinlichkeit
- Risikobewertung

Die Abschnitte der Risikoanalyse

- Die Vorgehensweise zur Bewertung potentieller Angriffsszenarien besteht aus drei Schritte:
  1) die Bestandsaufnahme
  2) die Bedrohungsanalyse
  3) die Risikobewertung

Bestandaufnahme

- In Bereichen, in denen die Rechnern verwendet sind ,sollten berücksichtigt werden:

Hardware-konfiguration	Software-komponenten	Spezifikation der Daten
• Netzstruktur (Server, Router, etc.) • Internetkopplung (Firewall, Proxy, etc.)	• Programme,etc. • Internetanwendungen und –dienste, d.h. Web-Server, E-Mail-Server, u.s.w.	• Programme,etc. • Internetanwendungen und –dienste, d.h. Web-Server, E-Mail-Server, u.s.w.

Bedrohungsanalyse

- Es gibt eine Klassifikation nach Gefahrensarten, besonders nach bewußt herbeigeführte Gefahren. Also, unterscheidet man zwei Unterkategorien: interne und externe.

Interne Gefahr	Externe Gefahr
• Sniffing: unzufriedene Mitarbeiter • Mobbing, Spionage • lokales Netz, TCP/IP-Schwächen, ARP-Spoofing	• Sniffing: ehemalige Mitarbeiter • Spionage • Internet - Angriffe

Internet Angriffe

- Spoofing: Zugriff auf geschützte Systeme und Dienste durch falsche Identitätsangaben (IP-Spoofing, UDP-Spoofing u.a.)
- Denail of Service: Herbeiführung von Systemausfällen, um Dienste für berechtigte Personen zu verhindern (SYN-Flooding, verschiedene ICMP-Angriffe)
- Sniffing
- SMTP-Server-Angriffe
- WWW-Server- Angriffe (HTTP, CGI, Java, ActiveX)

Internet Angriffe(2)

- Viren: Modifikation ausführbarer Programmsequenzen zur Funktionalitätsänderung, um dem Zielsystem Schaden zuzufügen bzw. Informationen zu entlocken Trojanische Pferde: Funktionalitätsänderung wird vom Anwender des modifizierten Programms nicht bemerkt
- TCP-Sequenznummer - Angriff
- Paßwort - Erkundung
- Portnummer - Scanning

Untersuchung der Schadenshöhe

- Welcher Geldbetrag braucht man, um den Normalzustand wieder herzustellen?

Antwort: die Bestimmung des Geldbetrages ist häufig sehr schwierig.

- Welche Auswirkungen gibt es an den laufenden Geschäftsbetrieb?
- Welche sind die Folgeschäden?

Sicherheitsanforderungen

- Resultieren aus den unternehmensstrategischen Zielen und den Ergebnissen der Risikoanalyse
- Müssen durch die Sicherheitsmaßnahmen im Sicherheitskonzept erreicht werden
- Insbesondere können organisatorische und technische Sicherheitsanforderungen formuliert werden

Ermittlung der Eintrittswahrscheinlichkeit

- Die Protokolldateien sollen ausgewertet sein
- Man kann langjähriger Statistiken von Versicherungen verwenden

Risikobewertung

- Restrisiko=Schadenshöhe * Eintrittswahrscheinlichkeit
- Für jede Bedrohung sollen das Restrisiko und die Wiederherstellungskosten für Normalzustand ermittelt werden
- Hilfreich ist eine Einteilung in tragbare und untragbare Risiken in Abhängigkeit der Geschäftsfähigkeit des Unternehmens im Schadensfall
- Man soll die Kosten für die Gefährdungen mit untragbaren Risiken schätzen

Risikomanagement

- Notfallmanagement
- Business Continuity-Management
- Wiederanlaufmanagement
- IT Risk Management Circle

Notfallmanagement

- Notfallkonzept
  1) Welche Aktionen sind im Schadensfall zu ergreifen?
  2) Wer meldet wem?
  3) Wer koordiniert die Maßnahmen?
  4) Was ist sofort zu tun?
  5) Wer spricht mit der Öffentlichkeit (Behörden, Presse)?

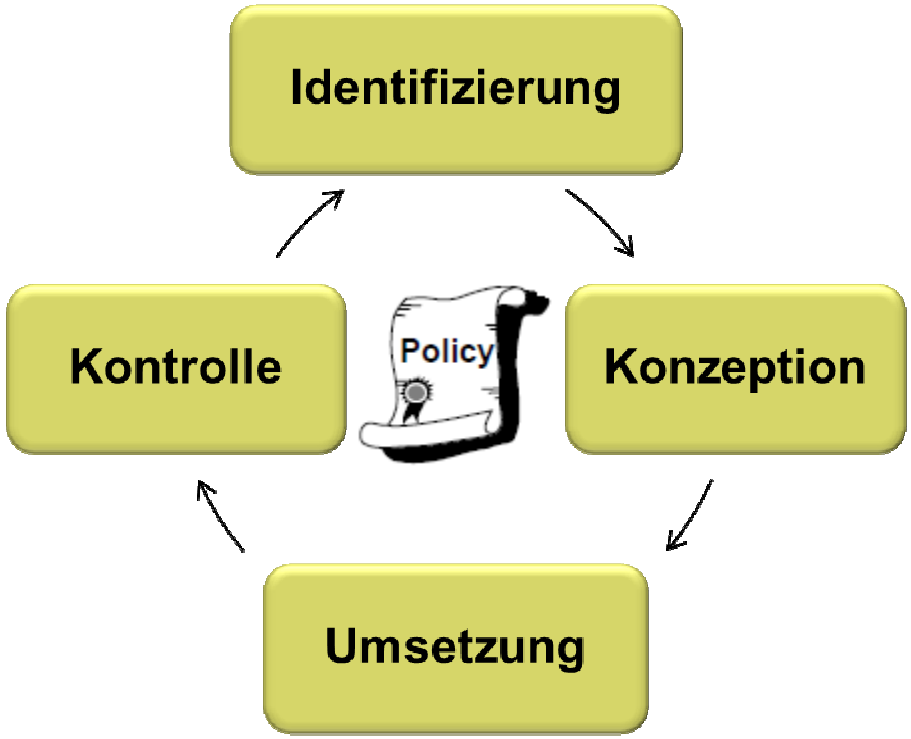
Business Continuity-Management

- Geschäftserhaltungskonzept
  1) Welche grundlegenden Geschäftsprozesse können wie aufrecht erhalten werden?
  2) Er konzentriert sich auf die Verfügbarkeit und Fallback-Fähigkeit der wesentlichen Geschäftsprozesse
  3) Wie können trotz massiver Einwirkungen existenzielle Bedrohungen abgewendet werden?
  4) Was ist sofort zu tun?

Wiederanlaufmanagement

- Wiederanlaufkonzept
  1) Welche Aktionen sind zur Wiederherstellung des Normalzustandes nach einem Schadensfall zu ergreifen?
  2) Welche Systeme sind voneinander abhängig?
  3) In welcher Reihenfolge sind die Systeme in Abhängigkeit der Systemstruktur hochzufahren?
  4) In welchem Zeitumfang ist der Normalzustand wieder erreicht?

IT Risk Management Circle



- IST-Aufnahme/Risikoanalyse
- Recherche

- Sicherheitskonzept

- Ergebnis und Ablauf der Umsetzung beachten

- Security Audits
- Continuous Risk Assesment
- Penetration tests

Sicherheitskonzept

- IT-Sicherheitskonzept

IT-Sicherheitskonzept

- Dient der Erkennung und Beseitigung von Sicherheitslücken durch geeignete Maßnahmen
- Definiert die Grenzen akzeptablen Verhaltens und die Reaktion auf Überschreitungen

IT-Sicherheitskonzept(2)

Sicherheitsmanagement

- Erstellung einer „Sicherheitspolitik“
- Umsetzung der IT-Sicherheitspolitik
- Sicherheitspolitik ist Rahmenwerk

Erstellung einer Sicherheitspolitik“

- Klassifizierung der Maßnahmen: präventive, überwachende und reaktive
- Trotz Sicherheitsmaßnahmen darf die Funktionalität der Geschäftsprozesse nicht leiden
- Klare Festlegung von personellen Zuständigkeiten, auch in der Kontrolle

Umsetzung der IT-Sicherheitspolitik

- Funktionalität und Sicherheit sind angemessen
- Sicherheitsanforderungen sind kein Produkt, sondern integraler Bestandteil der IT-Systeme
- Sicherheit wird nicht nur durch Technologie erreicht, sondern erst unter Einbindung der Unternehmensorganisation

Sicherheitspolitik ist Rahmenwerk

- Basiert sich auf den Sicherheitszielen und –anforderungen des Unternehmens
- Ist ein wichtiges Konzept für die IT-Sicherheit und die IT-Risikomanagement
- Beruht auf den identifizierten Risiken
- Betrifft technische, organizatorische und rechtliche Maßnahmen, um die Sicherheitsziele zu erreichen

Folgerung

- IT-Sicherheitspolitik ist ein muß !