

Sicherheitskonzepte in Unternehmen

VDI Arbeitskreis IT

Düsseldorf

13.10.2005

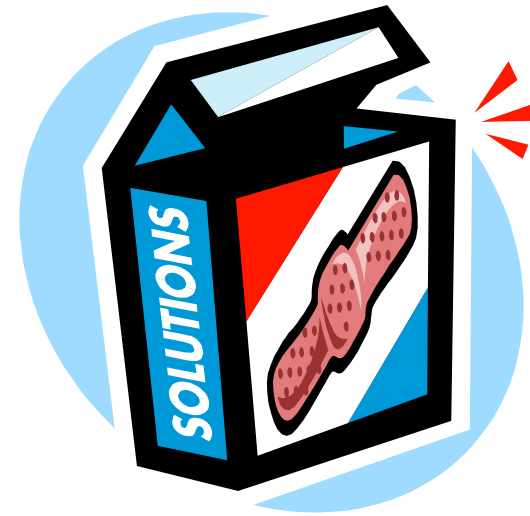
Dr. Michael Gehrke (TTS GmbH)



- Geb. 1960, verheiratet, 2 Kinder, Wohnort Essen
- Ausbildung
 - Diplom-Informatiker
 - Promotion über Informationssicherheit
- Berufliche Tätigkeiten
 - Technische Universität Berlin
 - Lehre und Forschung im Bereich Informationssicherheit
 - Deutsche Telekom AG
 - Projektmanagement Informationssicherheit
 - Sicherheitskonzepte für Netze, Anwendungen, Systeme
 - secunet AG
 - Projektleitung
 - Leiter Technik, Niederlassungsleitung
 - Vorstand Vertrieb und Marketing
 - TTS GmbH
 - Beratung, Geschäftsführung
- Publikationen
 - Zahlreiche Vorträge und Veröffentlichungen zum Thema Informationssicherheit
- Arbeitsschwerpunkte
 - Projektmanagement, -leitung
 - Sicherheitsstrategien
 - Sicherheitsaudits
 - Security Policies
 - Sicherheitsmanagement
 - Kritische Infrastrukturen
 - Trust Center (SigG)
 - Netzwerkmanagement
 - Organisatorische Sicherheit
- Handicap
 - Führung von 240 Mitarbeitern
 - Umsatzverantwortung über 20 Mio. €
 - Projektverantwortung IT-Sicherheit über 4 Mio. €



- Beratung zur Informationssicherheit
 - Sicherheitsstrategien
 - Aufbau von Sicherheitsorganisationen
 - Sicherheitsanalysen
 - Security Reviews, Benchmarking, Penetrationstests
 - Security Documents Framework
 - Information Security Policy
 - Sicherheitsrichtlinien
 - Sicherheitssystemstandards, Handlungsanweisungen
 - Sicherheitskonzepte und -architekturen
 - Risikomanagement
 - Schutzbedarfs- und Risikoanalysen
 - Notfallplanung
 - Studien, Gutachten, 2nd opinion
 - Identity- und Accessmanagement
 - SSO, Berechtigungsmanagement, PKI
 - Netzwerk- und Systemsicherheit
 - IP, DNS, IPSEC, VPN, Windows, UX, WWW, Portale



- Leitung und Management komplexer IT-Projekte



- Übersicht
 - Zum Stellenwert der Informationssicherheit
 - Was ist ein Sicherheitskonzept?
 - Standards und Methoden
 - Gelebte Praxis – zum Lachen oder Weinen

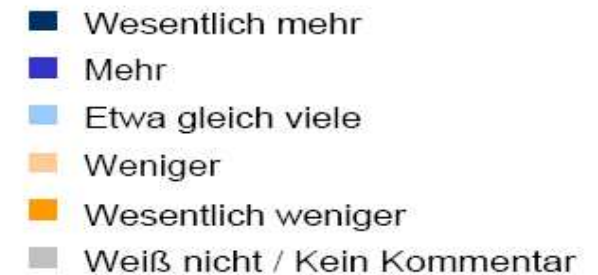
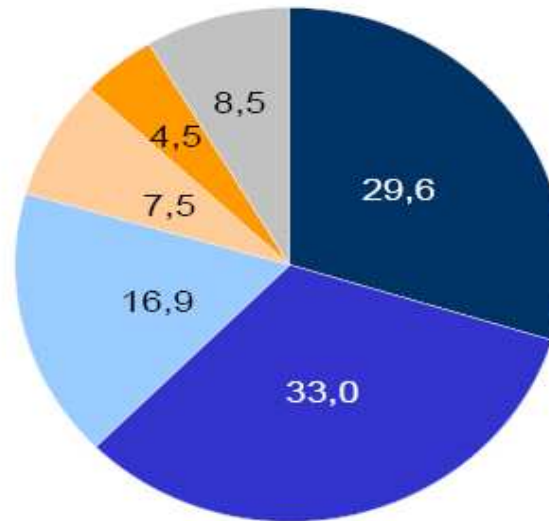


- Die O-Ton Charts
 - „Dafür haben wir jetzt keine Zeit.“
 - „Das ist im Augenblick kein Thema für uns.“
 - „Wir haben schon eine Firewall.“
 - „Da sprechen Sie am Besten mal mit unserem Systemadministrator.“



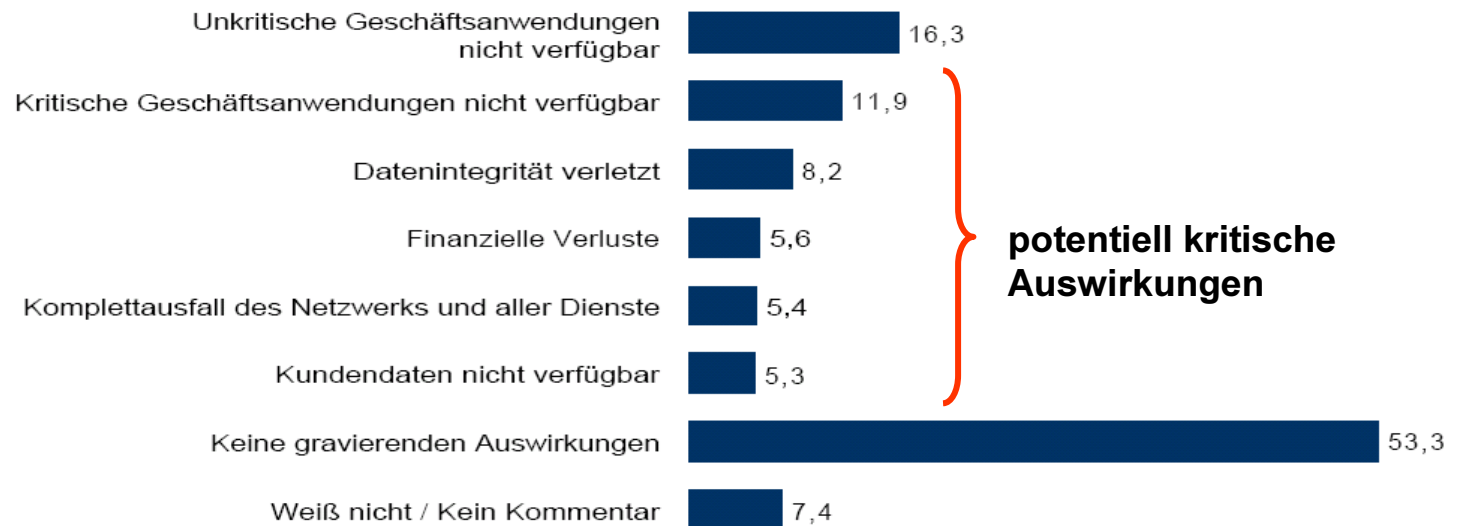
Zum Stellenwert der Informationssicherheit

Frage: Hatten Sie im Vergleich zu 2003 mehr oder weniger Verstöße (bspw. Viren, Würmer, Netzangriffe) zu verzeichnen? (Quelle: InformationWeek „IT-Security 2004“)



- Mögliche Diskussionspunkte
 - Eingeschränkter Begriff von „Sicherheitsverstoß“ (zudem unbefugtes Betreten, Entwendung von Akten, Weitergabe von vertraulichen Informationen, etc.)
 - Verfügen alle befragten Unternehmen auch über ein Berichtswesen für Sicherheitsverstöße
- Aber immerhin: bei ca. 63% ist eine Zunahme zu verzeichnen
 - Das deckt sich mit den Ergebnissen des CERT
 - Attacken werden in 2005 aber fokussierter

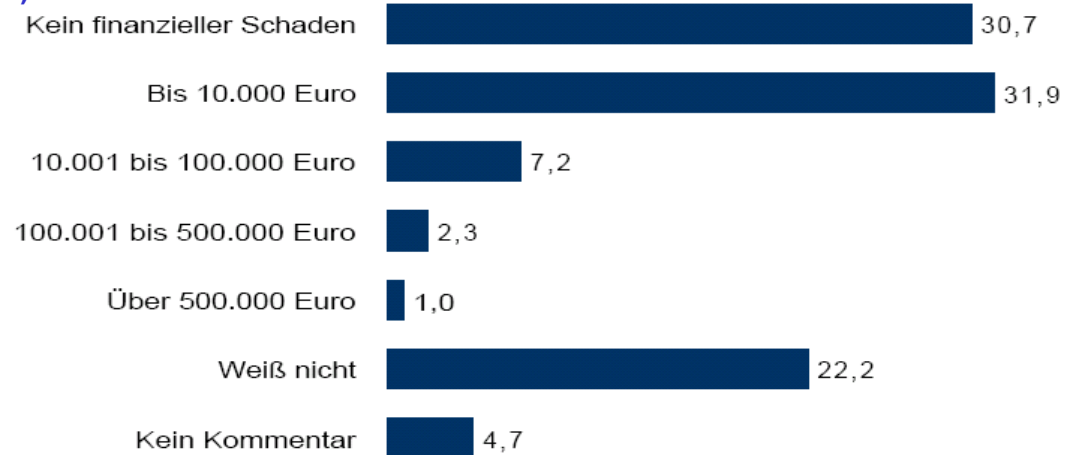
Frage: Welche Auswirkungen hatten diese Angriffe? (Quelle: InformationWeek „IT-Security 2004“)



- Mögliche Diskussionspunkte
 - Potentiell kritische Auswirkungen bei etwa 38% der Fälle
 - Wissen immerhin 11,9% der Unternehmen, welches ihre kritischen Geschäftsanwendungen sind?

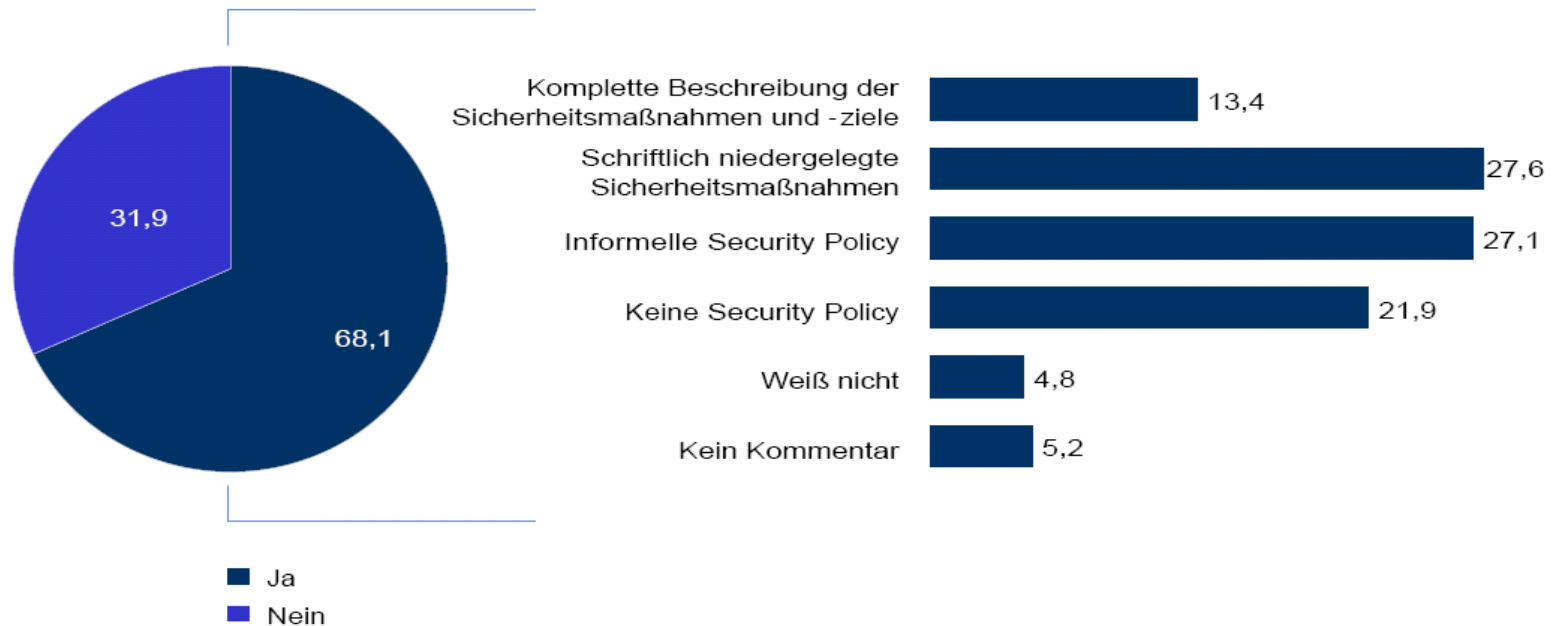


Frage: Wenn überhaupt, wie hoch schätzen Sie den Gesamtwert bzw. –schaden der Verstöße bzw. Spionagefälle gegen die Informationssicherheit in Ihrem Unternehmen in den letzten 12 Monaten?
(Quelle: InformationWeek „IT-Security 2004“)



- Mögliche Diskussionspunkte
 - Auch hier ist fraglich, ob die Unternehmen, den entstandenen Schaden tatsächlich bewertet haben?
 - Was kostet bspw.
 - ein Virenvorfall oder
 - ein Manager, der mit wettbewerbsrelevanten Informationen das Unternehmen verlässt
 - Durch BASEL II werden erst jetzt Lösungen zur Erfassung von Erfahrungswerten für operational Risks aufgebaut

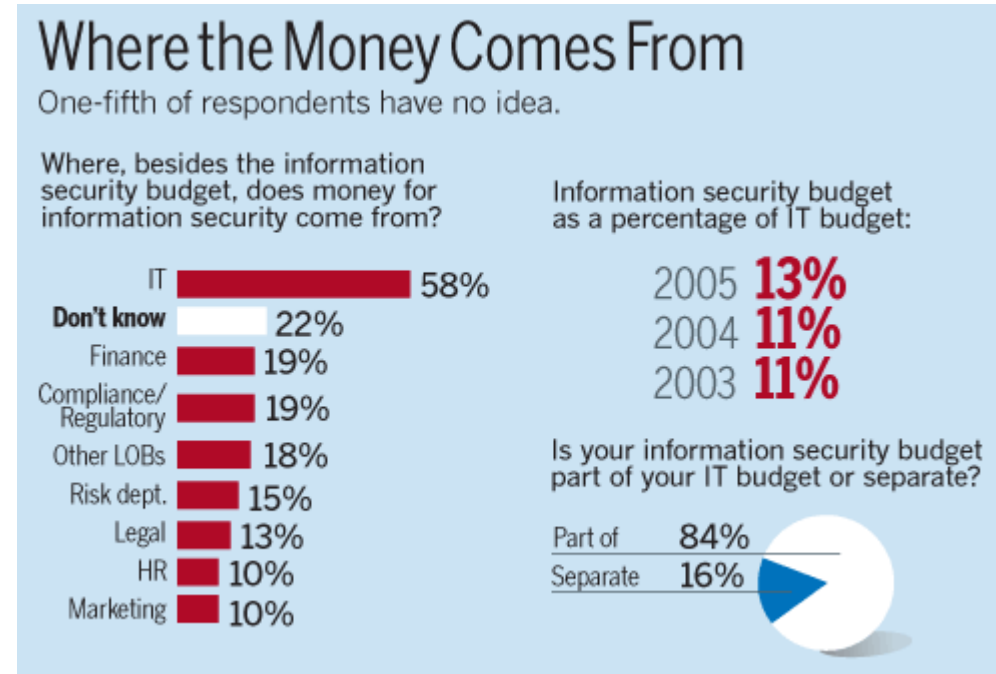
Frage: Verfügt Ihr Unternehmen über eine Security Policy, und wenn ja, in welcher Form?
(Quelle: InformationWeek „IT-Security 2004“)



- Mögliche Diskussionspunkte
 - Was bedeutet es eine „informelle Security Policy“ zu haben?
 - Immerhin verfügen 49% der befragten Unternehmen nicht über eine schriftlich fixierte Security Policy



- Budgetfragen
 - 13% des IT-Budgets ist Informationssicherheit!
 - 22% wissen nicht, wie ihre Informationssicherheit finanziert wird
 - Obwohl anders gefordert, ist IS bei IT aufgehängt



Quelle: PWC/CSO „The Global State of Information Security 2005“

Das Spektrum der Angriffsmöglichkeiten wird größer

- Komplexe Technologien ...
 - CGI, ActiveX, Java, Javascript, Server Side Includes, Cookies, ...
- ... ermöglichen komplexe Angriffe
 - page jacking, web spoofing, cookie poisoning, ...

Quelle: Vortrag M. Gehrke, 2000!



- Die heutigen moderne Komponentenarchitekturen
 - Java applets, Plug-Ins, DLL / shared libraries, Makros, ...
- Garantieren kein fehlerfreies Zusammenspiel
- können nicht die Vertrauenswürdigkeit aller Komponenten sicherstellen (z.B. Laden eines neuen Plug-Ins)

Quelle: Vortrag M. Gehrke, 2000!



- Was wir wissen
 - Unsere Geschäftsprozesse sind mehr und mehr von IT abhängig
 - Die Komplexität der IT steigt
 - „Angriffe“ auf die Informationssicherheit nehmen zu
 - Zudem hat sich die Bedrohungslage seit dem 11.9.2001 geändert
- Was ich glaube
 - Die Wirklichkeit ist komplexer als alle Studien zur Informationssicherheit
 - Von den Experten wird die Notwendigkeit von Aktivitäten zur Informationssicherheit erkannt
 - Es fehlt aber an Personalressourcen zur Umsetzung
 - Security wird zu häufig als IT-Thema gesehen, mit allen negativen Auswirkungen
 - Geschäftsprozesseigentümer müssen stärker einbezogen werden



- Übersicht
 - Zum Stellenwert der Informationssicherheit
 - Was ist ein Sicherheitskonzept?
 - Methoden und Standards
 - Gelebte Praxis – zum Lachen oder Weinen



Was ist ein Sicherheitskonzept?

- Darstellung der Maßnahmen, um für den Betrachtungsgegenstand ein adäquates Maß an Informationssicherheit zu gewährleisten
- Ein Sicherheitskonzept wird für ein Unternehmen, ein System (z. B. SAP, Portal oder Fileserver), ein Projekt oder auch eine Technologie (z. B. WLAN, Blackberry) erstellt
- Weitere Anforderungen an SiKos
 - Nachvollziehbarkeit
 - Systematisch
 - Wartbar



- Abgrenzung des Betrachtungsbereiches
- Darstellung / Ableitung der Sicherheitsanforderungen
- Sicherheitsarchitektur
- Sicherheitsmaßnahmen
 - Technisch
 - Organisatorisch
 - Baulich
- Ergänzende Risikoanalyse
- Relevante Betriebsprozesse



- Warum sollte ich den Betrachtungsbereich abgrenzen?
- Wie leite ich Sicherheitsanforderungen ab?
- Wie geht eigentlich eine Risikoanalyse?
- Was sind denn relevante Betriebsprozesse?
- Und überhaupt ...
- Warum muss man das alles dokumentieren?



- Übersicht
 - Zum Stellenwert der Informationssicherheit
 - Was ist ein Sicherheitskonzept?
 - Standards und Methoden
 - Gelebte Praxis – zum Lachen oder Weinen



- Übersicht Standards
 - Sicherheitsmanagement und Kriterienkataloge (Fokus)
 - Technik und Protokolle
- Übersicht Methoden
 - Sicherheitsanforderungen
 - Business Impact Analyse
 - Risikoanalyse



Grundschutzhandbuch
ISO / IEC 17799 und BS 7799
ISO TR 13335
ITSEC / Common Criteria
FIPS 140-1/2
Task Force Sicheres Internet
CobiT
Gütesiegel / Produktaudit Schleswig Holstein
ISO 9000
CRAMM (Comprehensive Risk Analysis and Management Method)
OECD Guidelines on Information Security, Privacy Guidelines, Cryptography Guidelines
GASSP (Generally Accepted System Security Principles)
Computer Security Techniques
ANSI Standards
Orange Book (TCSEC)
U.S. NIST Computer Security Handbook



Übersicht Standards und Kriterienwerke

Größte Praxisrelevanz

Grundschutzhandbuch
ISO 17799 / BS 7799
ISO TR 13335
ISF Standard of Good Practice for Information Security
NIST Framework



- Rechtliche Anforderungen
- Vorgaben der Organisation
- Geschäftliche Anforderungen



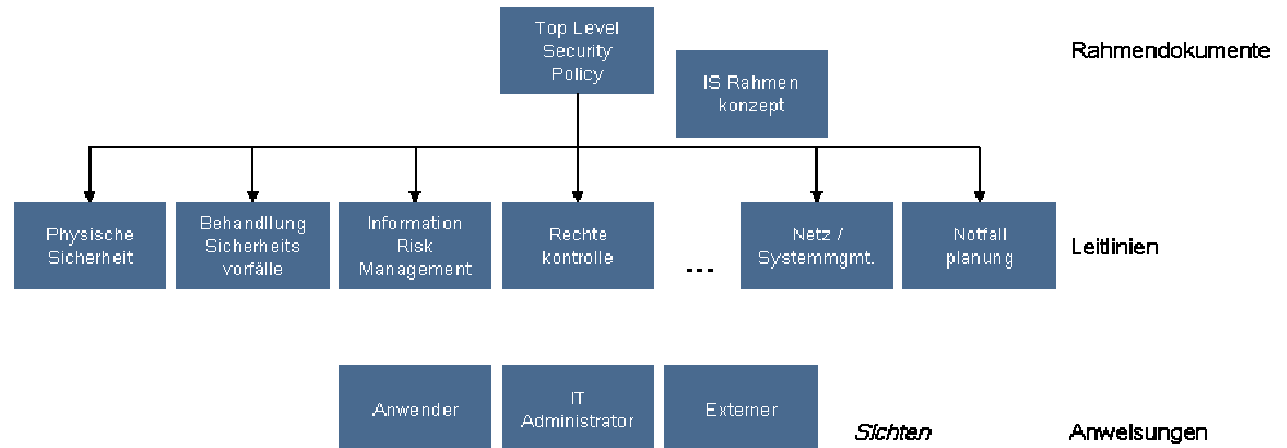
Anforderungen aus Gesetzen und Verträgen (Auszug)

- **BDSG: Technische und organisatorische Maßnahmen zum Datenschutz**
 - Teledienstschutzgesetz (TDDSG), Telekommunikationsgesetz (TKG), Telekommunikations-Datenschutzverordnung (TDSV), Teledienstgesetz (TDG)
 - Patientendatenschutz
- **Handelsgesetzbuch (HGB), Abgabenordnung (AO), Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)**
- **AktG / GmbHG, KonTraG, Sarbanes Oxley Act**
 - z. B. Anforderungen an Risikomanagement, rechnungslegende Prozesse
- **MaH: Allgemeine Anforderungen, Betriebsrisiken, Kreditwesengesetz (KWG), etc.**
 - z. B. Business Continuity
- **Basel II**
- **Pharma: 21 CFR Part 11 (Federal Drug Administration, FDA)**
- **Spezielle vertragliche Regelungen in Kundenverträgen**



- Der Sarbanes-Oxley Act fordert von an US-Börsen notierten Unternehmen die Dokumentation aller Prozesse und Kontrollen, die die Qualität der Finanzberichterstattung beeinflussen
- Darüber hinaus wird verlangt, die Abläufe auf ihre Wirksamkeit zu testen und dies auch nachzuweisen
- SOx selbst enthält keine direkte Anforderung nach „information security“
- In Projekten zur SOx-Compliance spielt die Informationssicherheit aber eine wichtige Rolle, u. a.
 - Berechtigungsprozesse
 - 4-Augen-Prinzip
 - Notfallplanung
 - Sicherheitskonzepte
- Sicherheitsanforderungen müssen also aus den gesetzlichen Vorgaben erarbeitet werden!

Anforderungen aus Vorgaben der Organisation



- Beispiel Kunde A
 - Modulare Security Policy
 - Top-Level Security Policy auf Managementebene
 - Sicherheitsstandards für weitere Detaillierung
 - Handlungsanweisungen / Sichten nach Zielgruppe



- Beispiel Kunde aus der Logistik

- Vorgaben aus der Top Level Security Policy
- Vorgaben aus dem Infrastrukturstandard

All information processing facilities used at the premises of the XXXX group have to be formally approved

Access to information and information systems has to be restricted according to the “Need-to-Know”-principle.

Constructional fire protection measures shall be designed in accordance with fire protection class F180¹. This includes the encapsulation of cables, cable tunnels and piping-holes as well as air entries, exit ducts, fire protection flaps and the encapsulation of steel girders (fire sealing of trays).

- Beispiel Finanzdienstleister

- Vorgabe aus der Top Level Policy

Diese Informationssicherheits-Leitlinie muss von allen Mitarbeiter der Firma A unterzeichnet werden.

Die Absicht ist gut,
aber wird die
Wirkung auch
erzielt?



- Geschäftliche Anforderungen
 - entstehen aus dem Schutzbedarf der in Geschäftsprozessen genutzten Informationen und Systemen
 - Sicherheitsanforderungen sollten von den Geschäftsprozesseigentümern definiert werden
 - Unterstützung durch die Sicherheitsorganisation
- Mittel zur Definition der Sicherheitsanforderungen
 - Informelle Analyse
 - Business Impact Analyse
 - Risikoanalyse
 - Sicherheitsanalysen
 - Schwachstellenanalyse
 - Penetrationstests



- **Beispiel Business Impact Analyse**
 - Im Rahmen einer Business Impact Analyse wurde der Schutzbedarf der verschiedenen Assets ermittelt
 - Der Schutzbedarf ist nun adäquat durch Maßnahmen der Informationssicherheit zu gewährleisten
 - Hohe Integritätsanforderungen könnten durch Überwachung der Zugriffe implementiert werden
 - Bei hohen (3) Vertraulichkeitsanforderungen ist eine Verschlüsselung der Informationen zu überlegen
 - etc.

| Informationsobjekt | Vertraulichkeit | Integrität | Verfügbarkeit | | | | |
|------------------------------|-----------------|------------|---------------|----|------|----|----|
| | | | 1h | 1d | 2-3d | 1w | 1m |
| Kontrolle Bewertung | 1 | 1 | 1 | 1 | 2 | 3 | 3 |
| Konzerninterne Verträge | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Korrespondenz BAFin, BB, ... | 3 | 3 | 1 | 1 | 1 | 2 | 3 |



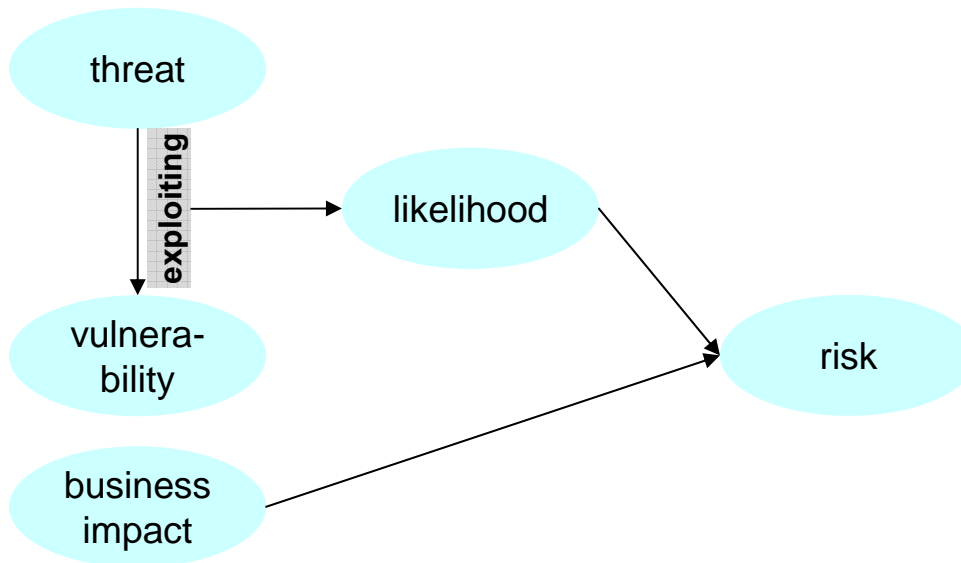
- Beispiel Risikoanalyse
 - Das IS Budget ist immer begrenzt, deswegen ist es wichtig, jedes IT System exakt entsprechend seiner Bedeutung für die Geschäftsprozesse abzusichern
 - Diese Ausrichtung erreicht man durch Risikoanalyse / -management
 - Minimierung negativer Auswirkungen auf eine Organisation und eine stabile Basis zur Entscheidungsfindung sind die wesentlichen Gründe für Risikomanagement



Bedrohungen, Risiken, Schwachstellen, Schäden



Example: The risk of a fire damaging an office building



- Übersicht

- Zum Stellenwert der Informationssicherheit
- Was ist ein Sicherheitskonzept?
- Methoden und Standards
- Gelebte Praxis – zum Lachen oder Weinen



- Dateien werden auf dem Fileserver verschlüsselt, die Backupmedien mit Klartextdaten liegen aber offen herum
- Der Hauptzugang wird mit einem Rammschutz versehen, man kann aber auch von hinten „an“ das Gebäude fahren
- In einem Terabyte-SAN wird kein Virenschutz installiert, weil der Hersteller diesen nicht zertifiziert hatte
- Die offiziellen Eingänge werden von einer Sicherheitsfirma betreut, ein Hintereingang wird aber mit einem Papierkorb offen gehalten
- Die wesentlichen Anwendungen wurden von einem Mitarbeiter entwickelt. Eine Dokumentation existiert nicht, man würde sich aber gerne von diesem Mitarbeiter trennen.
- Und natürlich ungezählte Sicherheitslücken aus verschiedenen Security Reviews
 - Ungeschützte Adminkonten
 - Nicht gehärtete / gepatchte Systeme
 - etc.

- Die Verantwortung für den Schutz unternehmenskritischer Informationen liegt letztendlich immer beim Management
- Informationssicherheit wird vom Geschäft abgeleitet, nicht anders herum
- Anforderungen, Standards und Compliance Management zentral – Implementierung dezentral
- Rollen werden auf Mitarbeiter abgebildet entsprechend der Unternehmensgröße
- Prozesse und Verantwortlichkeiten sind klar zu definieren
- Schnittstellen zu anderen Unternehmensfunktionen müssen etabliert werden
 - Risikomanagement
 - Datenschutz
 - Audit
 - IT Projekte
 - Recht

- Einführung von technischen Sicherheitsvorkehrungen ohne Konzept (Firewall, Verschlüsselung)
- Übertriebene Maßnahmen, Überbetonung von Teilaspekten
 - Verschlüsselte Übertragung, aber unsichere Systeme
 - Sicherheit ist mehr als Viren
 - Einbrüche werden nicht nur vom CCC durchgeführt
- Fehlende Kontrolle, ob Sicherheitsvorkehrungen auch das leisten, was der Prospekt verspricht



- Das Budget erlaubt den Kauf von Lösungen, aber nicht den Betrieb
 - Fehlkonfigurationen, Missmanagement sind absehbar
 - fehlendes Personal, der Betrieb einer Firewall bedeutet mindestens 2 Personen und deren Ausbildung
 - alle High-Tech Vorkehrungen helfen wenig, wenn der Rechner einfach entwendet wird
- Komplexität der heutigen Systeme ermöglicht Schwachstellen
 - Implementierungsfehler sind die Regel
 - Patches werden nicht schnell genug eingespielt



- Keine Aktualisierung der Konzeption
 - die Sicherheit wächst nicht mit den Unternehmensanforderungen mit
- Grösstes Problem
 - Überbetonung von Produkten
 - Hersteller: „Dieses Produkt sichert Ihren E-Commerce“
 - Sichern gegen wen / gegen was?
- Einzellösungen erhöhen die Gefahr, da sie eine Sicherheit vortäuschen, die sie so nicht realisieren können



- Kritische Erfolgsfaktoren
 - Sicherheitsleitlinie, Ziele und Aktivitäten im Einklang mit geschäftlichen Anforderungen
 - Implementierungsansatz muss in die Organisationskultur passen
 - sichtbare Unterstützung von allen Managementebenen
 - gutes Verständnis über Sicherheitsanforderungen, Risikoanalyse und -management
 - interne Vermarktung der Aktivität an alle Mitarbeiterebenen und Geschäftspartner
 - Unterstützung bei der Umsetzung der Sicherheitsleitlinien
 - Verfahren Sicherheitsaktivitäten zu budgetieren
 - Training und Ausbildung
 - Ansatz, um Fortschritte und Veränderungen zu messen



Vielen Dank für Ihre Aufmerksamkeit

“The wonderful thing about the Internet is that you’re
connected to everyone else.

The terrible thing about the Internet is that you’re connected
to everyone else.”

Vint Cerf



- Über Feedback jeglicher Art freue ich mich
- Dr. Michael Gehrke
 - Phone: +49 (2054) 873579-14
 - Mobile: +49 (171) 8916081
 - Email: michael.gehrke@tts-security.com
 - Internet: www.tts-security.com

The screenshot shows the TTS website homepage. At the top left is the TTS logo with the tagline 'trusted technologies and solutions'. Below the logo is a navigation menu with 'HOME', 'KONTAKT', and 'SITEMAP'. To the right of the navigation menu, it says 'Aktualisiert: 20.05.2005'. The main content area is divided into several sections:

- Home:** A vertical menu with links to 'Unternehmensprofil', 'Philosophie', 'Alleinstellungsmerkmale', and 'Designkriterien'.
- News:** A section for news updates.
- Leistungen:** A section for services.
- Informationssicherheit:** A section for information security.
- Publikationen:** A section for publications.
- Karriere:** A section for career opportunities.
- Kontakt:** A section for contact information.
- Vision:** A section with the text: 'In 5 Jahren werden Unternehmen weltweit auf die Beratungskonzepte der TTS vertrauen, um jegliche Art von Angriffen auf die Informationssicherheit beherrschen zu können.' accompanied by an image of a glowing lightbulb.
- Mission:** A section with the text: 'Die Berater der TTS entwickeln Strategien, Pläne, Architekturen und Konzeptionen, damit unsere Kunden Informationssicherheit beherrschen. Dabei setzen wir die besten Organisationskonzepte und Technologien ein, und passen diese an die Kundenbedürfnisse an. Professionalität, Qualität und Kompetenz sind die wesentlichen Eigenschaften unserer Arbeit und gleichzeitig das höchste Ideal für unsere Mitarbeiter.'
- In bin interessiert an ...:** A section listing various services:
 - Antivirus
 - Firewall
 - Grundschutz
 - Identity & Access Management
 - Incident Handling
 - Intrusion Detection
 - ISO 17799/ BS7799
 - Kontrag
 - Notfallplanung
 - Penetrationstest
 - Provisioning
 - Risikoanalyse
 - Risikomanagement
 - Rollenbasierter Zugriffsschutz - RBAC
 - Security Awareness
 - Security Guidelines
 - Security Policy
 - Security Review
 - Sicherheitshandbuch
 - Sicherheitslösungen
 - Sicherheitsorganisation
 - Sicherheitsprozesse
 - Single Sign-On
 - Verschlüsselung
 - Vertrauenswürdige Geschäftsprozesse

At the bottom right of the page, it says 'Copyright © 2005 TTS GmbH'.