

(Un)Sicherheit in der Informationsgesellschaft

IT-Sicherheit – Risiken und Handlungsempfehlungen
Marietta Spangenberg
Vortrag Februar 2010

Schwerpunkte

- Situation und Motivation
- IT-Sicherheitsrisiken
- Aktuelle Beispiele
- Schäden durch Sicherheitsvorfälle
- Gesetzliche Erfordernisse
- Was tun? – Empfehlungen zur Entwicklung einer IT-Sicherheitsstrategie
- Maßnahmen zur Gewährleistung von IT-Sicherheit und Datenschutz
- Fazit

Situation

Informationsgesellschaft

Moderne IT überall

E-Commerce, E-Banking,
E-Business, E-Learning,
... soziale Netzwerke

Kosten für Beseitigung der
Folgen eines Angriffs: im
Mittel 350.000€

Kosten für
Datenbankabsturz: im
Mittel 1750€/h

Risikogesellschaft

Abhängigkeit

Existenzbedrohte
Unternehmen

Verunsicherte Nutzer

Kosten für IT-Sicherheit?

Anforderungen im Geschäftsleben

- Sie müssen immer auf dem aktuellen Stand sein
- Sie müssen immer auf die Informationen ihres Unternehmens zugreifen können
- Sie müssen immer erreichbar sein
- Sie müssen immer im Internet präsent sein
- Sie müssen immer und sofort auf eingehende Emails reagieren
- ...

Kein Problem



Was ist bei Ihnen zutreffend?

- Sie verarbeiten personenbezogene Daten
- Ihre Kalkulation ist geheim
- Sie haben ein innovatives Produkt entwickelt
- Sie haben ein sehr gutes Image bei Ihren Kunden aufgebaut
- Sie haben mehr oder weniger Geld auf der Bank und eine Menge Kreditkarten
- ...
- → Das alles macht Sie zu einem interessanten Ziel und vielleicht sind Sie ja angreifbar?

Wovon man nicht ausgehen sollte

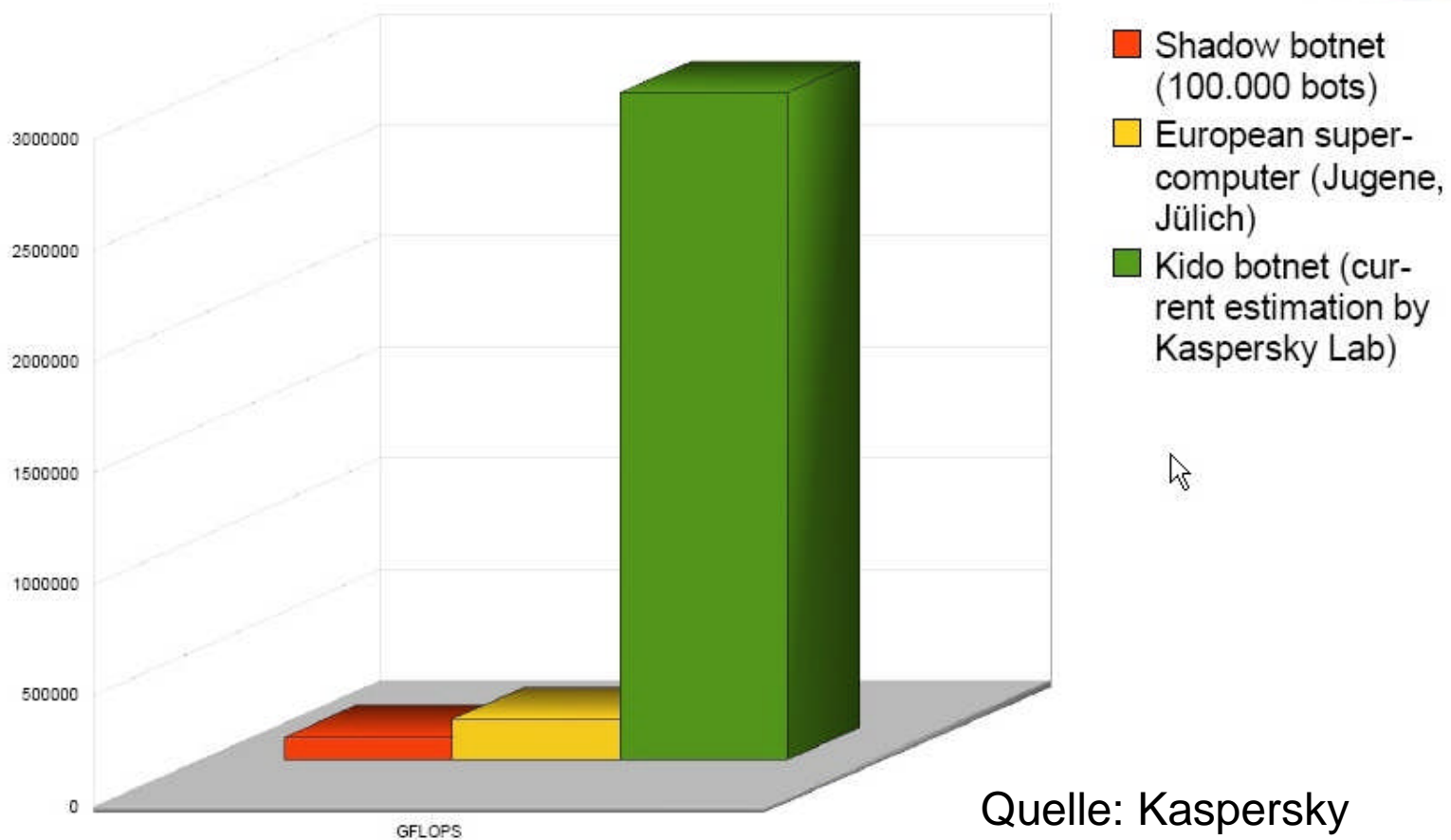
- Uns ist noch nie etwas passiert
- Unsere Daten sind nicht so geheim
- Keine Zeit für IT-Sicherheit
- IT-Sicherheit kostet zu viel Geld
- Das ist Sache von Spezialisten oder der IT-Abteilung
- Sicherheit ist nicht mein/unser Problem
- Probleme hat nur der Wettbewerber

Mögliche IT-Sicherheitsrisiken

- Malware
- Phishing
- Identitätsdiebstahl
- Datenverlust
- Hackerangriffe
- DoS-Attacken
- Betrug
- Spionage
- Social Engineering
- Diebstahl des Systems oder der Medien
- Irrtum und Nachlässigkeit der Mitarbeiter
- Systemausfälle
- ...



Das größte Botnet aller Zeiten



Sicherheitsvorfälle in Unternehmen

	Bedeutung heute		Prognose		Schäden	
	Rang	Priorität	Rang	progn. Priorität	Rang	ja, bei
Irrtum und Nachlässigkeit eigener Mitarbeiter	1	1,52	2	1,17	1	49%
Malware (Viren, Würmer, Troj. Pferde,...)	2	1,06	1	1,51	4	35%
Software-Mängel-/Defekte	3	0,60	5	0,58	2	46%
Hardware-Mängel-/Defekte	4	0,55	6	0,34	3	45%
unbefugte Kenntnisnahme, Informationsdiebstahl, Wirtschaftsspionage	5	0,50	3	0,63	7	12%
unbeabsichtigte Fehler von Externen	6	0,39	7	0,32	5	30%
Hacking (Vandalismus, Probing, Missbrauch,...)	7	0,37	4	0,59	8	12%
Mängel der Dokumentation	8	0,27	9	0,27	6	20%
Manipulation zum Zweck der Bereicherung	9	0,26	8	0,29	10	11%
höhere Gewalt (Feuer, Wasser,...)	10	0,21	11	0,03	9	12%
Sabotage (inkl. DoS)	11	0,17	10	0,22	11	10%
Sonstiges	12	0,02	12	0,00	12	3%

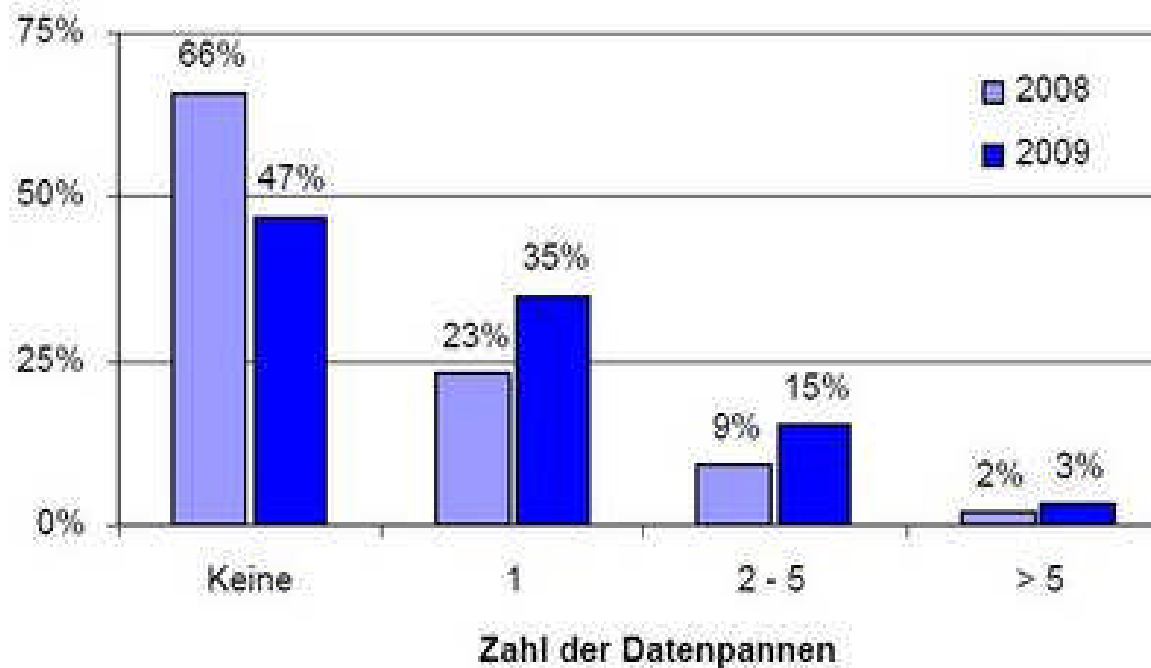
*Tabelle 1:
Bedeutung der
verschiedenen
Gefahren-
bereiche*

Basis: 155 Antworten (Bedeutung), Ø 130 (Prognose), Ø 127 (Schäden)

Table 1	2004	2005	2006	2007	2008
Denial of service	39%	32%	25%	25%	21%
Laptop theft	49%	48%	47%	50%	42%
Telecom fraud	10%	10%	8%	5%	5%
Unauthorized access	37%	32%	32%	25%	29%
Virus	78%	74%	65%	52%	50%
Financial fraud	8%	7%	9%	12%	12%
Insider abuse	59%	48%	42%	59%	44%
System penetration	17%	14%	15%	13%	13%
Sabotage	5%	2%	3%	4%	2%
Theft/loss of proprietary info	10%	9%	9%	8%	9%
from mobile devices					4%
from all other sources					5%
Abuse of wireless network	15%	16%	14%	17%	14%
Web site defacement	7%	5%	6%	10%	6%
Misuse of Web application	10%	5%	6%	9%	11%
Eots				21%	20%
DNS attacks				6%	8%
Instant messaging abuse				25%	21%
Password sniffing				10%	9%
Theft/loss of customer data				17%	17%
from mobile devices					8%
from all other sources					8%

Quelle:
CSI Sicherheitsumfrage

Datenskandale und Datenpannen



Quelle: Studie PGP

2010 Fortsetzung der Datenpannen

News vom 13.01.2010

- Microsoft warnt vor Lücke in alter Flash-Player-Version
- UMTS-Verschlüsselung angeknackst
- Oracle patcht 24 Lücken
- Sicherheits-Update für Adobe-Produkte verfügbar

News vom 15.1.2010

- Angriffe auf Google und Co. durch bislang unbekannte Lücke im Internet-Explorer
- Sicherheitslücke an Flughäfen durch ID-Chipkarten
- Laut BSI existiert im Internet Explorer eine bisher unbekannte kritische Sicherheitslücke. Die Schwachstelle ermöglicht Angreifern, über eine manipulierte Webseite Schadcode in einen Windows-Rechner zu schleusen und zu starten. → Empfehlung, den Internet Explorer vorerst nicht zu nutzen

Mitarbeiter als „Schwachstelle“

- Ursache menschliches Fehlverhalten zwischen 25 und 84%
- Virus wird anderweitig zugeordnet, aber oft hat auch hier die „menschliche Firewall“ versagt
- Zunehmende Wirksamkeit von Social Engineering
- Passwortverrat, Mitteilung PW über Email
- Gespräch unter Kollegen → Wettbewerber hört mit
- Ergebnisse einer Studie:
 - Jeder zweite Arbeitnehmer entwendet Daten beim Jobwechsel
 - 57% sagten, es sei leicht auf vertrauliche Daten zuzugreifen
- Nachlässigkeit, Bequemlichkeit (warum soll ich denn andauernd das Passwort wechseln?), Unkenntnis, fehlendes Sicherheitsbewusstsein, schlechte Vorbilder

Gesetzliche Erfordernisse und unternehmerische Vernunft

- BDSG
- Datenschutzgesetze der Länder
- Sozialgesetzbuch
- KonTraG
- GoBS
- Basel II
- ...
- Gefährdung der Aufgabenerfüllung
- Verstoß gegen Verträge (Geheimhaltung)
- Finanzielle Schäden bzw. Auswirkungen
- Vernichtung von Arbeitsplätzen
- Fortbestand des Unternehmens
- Imageschäden
- ...

Was ist zu tun?

Bei der Verbesserung der ISi behindern am meisten:	
Es fehlt an Geld	55%
Es fehlt an Bewusstsein bei den Mitarbeitern	52%
Es fehlt an Bewusstsein und Unterstützung im Top-Management	45%
Es fehlt an Bewusstsein beim mittleren Management	37%
Es fehlen verfügbare und kompetente Mitarbeiter	32%
Es fehlt an Möglichkeiten zur Durchsetzung sicherheitsrelevanter Maßnahmen	31%
Es fehlen die strategischen Grundlagen / Gesamt-Konzepte	29%
Die Kontrolle auf Einhaltung ist unzureichend	27%
Anwendungen sind nicht für ISi-Maßnahmen vorbereitet	25%
Die vorhandenen Konzepte werden nicht umgesetzt	22%
Es fehlen realisierbare (Teil-)Konzepte	19%
Es fehlen geeignete Methoden und Werkzeuge	16%
Es fehlen geeignete Produkte	13%
Es fehlt an praxisorientierten Sicherheitsberatern	8%
Sonstiges	5%
keine Hindernisse	3%

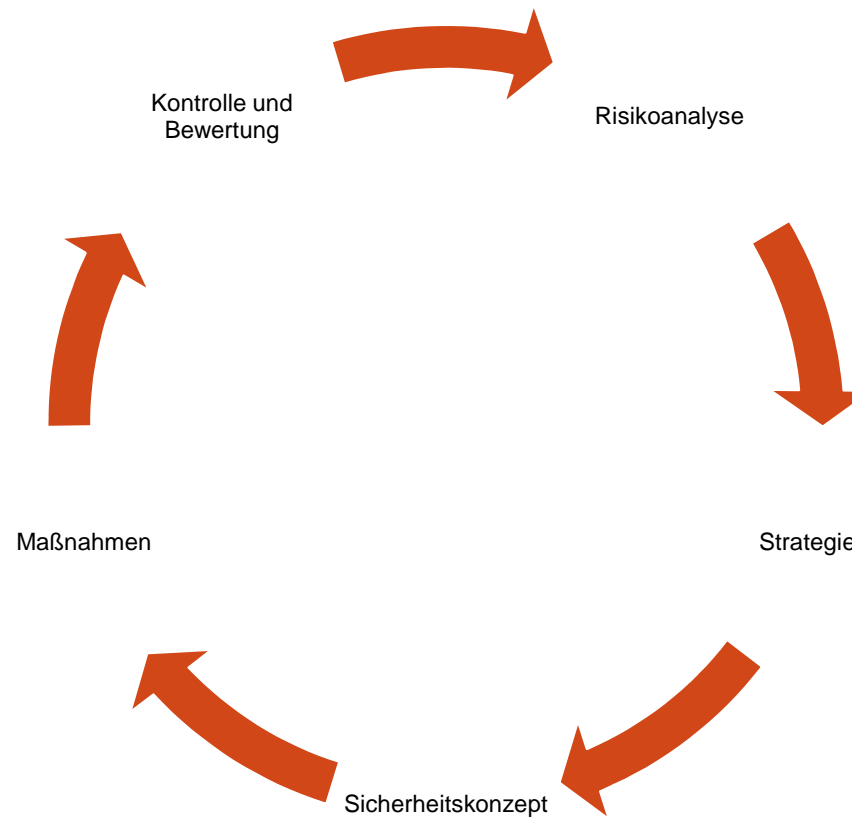
Basis: 158 Antworten

*Tabelle 8:
Hindernisse
für bessere
Informations-
Sicherheit*

Quelle: KES 2006

IT-Sicherheitsstrategie

Notwendigkeit zum Handeln → Sicherheitsbedürfnis



Sicherheit ist ein Ziel

- Ständige Anpassung, denn Systeme entwickeln sich weiter
- Strukturen verändern sich
- Angriffsmethoden entwickeln sich weiter

Auswahl Maßnahmen von A bis Z

- Antivirensoftware
- Backup, bauliche Maßnahmen
- Elektronische Unterschriften
- Firewall
- Intrusion Detection
- Notfallvorsorge (Disaster Recovery)
- Organisatorische Maßnahmen
- Personelle Maßnahmen
- Sicherheitsbewusstsein
- Verschlüsselung, VPN
- Zertifikate
- Zugang, Zugriff zum System, zu den Informationen

Wirtschaftliche Aspekte und Wettbewerbsvorteile

- IT-Sicherheit ist mehr als bloße Absicherung der Daten und Schutz gegen Hacker- und Virenangriffe
- Return on Security Investment
- Enge Verknüpfung von Sicherheit und Geschäftsprozessen

- Zuverlässige Arbeit mit verfügbarer Hard-, Software und richtigen Daten
- Keine Ausfälle
- Kein ständiger Kampf mit den Folgen eines Virenbefalls
- Kein Zugriff durch Unbefugte → Vertrauen der Kunden
- Keine Konflikte mit dem Gesetz (z.B. BDSG)

Fazit

- Einzelne Maßnahmen bedeuten keine Sicherheit
- Viele Maßnahmen sind kein Konzept
- IT-Sicherheit ist kein Zustand, sondern ein Ziel
- Sicherheit kostet Geld, fehlende Sicherheit kann viel mehr kosten
- Angemessenheit → Sicherheit rechnet sich
- Sichere Systeme sind effiziente Systeme

Fragen ? ? ?

Vielen Dank für Ihre
Aufmerksamkeit!