NETZWERK

GROSSBEERENSTRASSE e.V.

Sicherheit im Mittelstand 2012

IT Sicherheit

PRÄSENTATION

Bedrohungen - Schutz vor Virus, Würmer und Konsorten

tricom GmbH,
Dr. Thomas Nittka

NG NETZWERK GROßBEERENSTRAßE

Bedrohungen - Schutz vor Virus, Würmer und Konsorten

Agenda

1. Was gibt es für Bedrohungen?
2. Geschichte
3. Allgemeine Abwehrmaßnahmen gegen Viren
4. Wirtschaftliche Schäden durch Viren
5. Bedrohungen unter Windows, Linux und Mac
6. Aktuelles
7. Quellen
8. Kontaktdaten

Was gibt es für Bedrohungen?

Definition von Virus und den Grundtypen

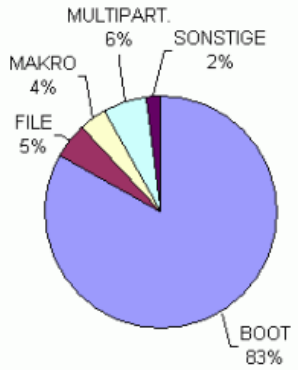
- Virus
  Nicht selbständige Programmroutine, die sich selbst reproduziert und danach vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgang vornimmt. Zusätzlich können programmierte Schadfunktionen des Virus vorhanden sein.
- Boot-Virus
- File-Virus
- Makro-Virus

Unterarten und Zusatzfunktionen von Viren

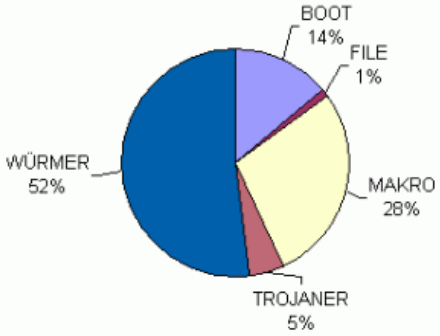
- Companion-Virus
- logische Bombe
- Multipartite-Virus
- Programm mit Schadensfunktionen (malicious software)
- residenter Virus
- selbstverschlüsselnder Virus (selbstkryptierender Virus)
- Tarnkappen-Virus (Stealth-Virus)
- Trojanisches Pferd
- Wurm

Geschichte

Verteilung der Virentypen 1996 in prozent:



Verteilung der Virentypen 2001 in Prozent:



Historie

- 1982 Elk Cloner für Apple II
- 1984 Cohen´s (1 Virus nach heutiger Def.)
- 1986 Brain (Pakistan, im Code Adresse)
- 1987 Jerusalem Virus (Freitag den 13. löschte er alle COM- u. EXE Dateien)
- 1987 Cascade Virus
- 1992 Michelangelo (Medienstar)
- 1995 Concept Virus (1. Makro Virus)
- 2000 Loveletter (45 Mio. Computer befallen)
- 2001 Lindose (Windows & Linux)
- 2004 Sasser (2 Mio. Computer befallen, Kopfgeld 250.000 US-Dollar)

Allgemeine Abwehrmaßnahmen gegen Viren

Schäden durch Viren

- Beabsichtigte, programmierte zerstörerische Schadensfunktionen
- Unbeabsichtigte Seiteneffekte bei angeblich harmlosen "Scherz-Viren„

... erfordern Zugriffe durch Spezialisten

- Inanspruchnahme von Speicherplatz im Hauptspeicher und auf Datenträgern
- Materieller und personeller Aufwand beim Suchen und Entfernen
- Zusätzlich zu ergreifende organisatorische Abwehr-Maßnahmen
- Panik-Reaktionen von Anwendern

Vorbeugende Maßnahmen

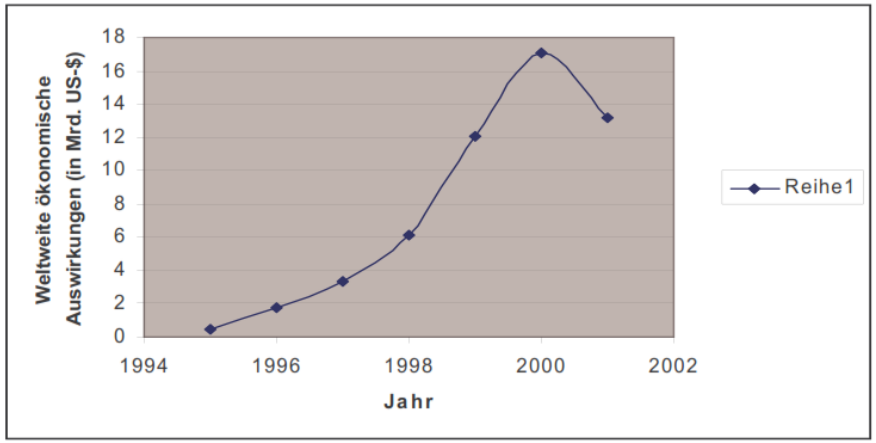
- Regelmäßig Datensicherung durchführen
- Sicherheitskopien von Datenträgern sicher aufbewahren
- Schreibschutz bei allen Disketten setzen, auf die nicht geschrieben werden muss (dies gilt insbesondere für die meisten Programm-Disketten).
- Aktuelle Viren-Schutzsoftware verwenden.
- Alle ein- und ausgehenden Datenträger auf Viren überprüfen.
- Ausgehende Datenträger mit Schreibschutz versehen.
- Vorinstallierte Neugeräte und gewartete Geräte auf Viren überprüfen. Ebenso Programme über andere Datenkanäle bei Ein- und Ausgang auf Viren überprüfen. (z.B. Mailbox oder E-Mail, Internet)
- Notfall-Diskette erstellen.
- Mehrere Partitionen (logische Laufwerke) im Rechner einrichten.
- Computer und Datenträger vor unbefugter Benutzung schützen.
- Mitarbeiter über Computer-Viren schulen.

Allgemeine Abwehrmaßnahmen gegen Viren

Verhalten bei Befall

- Bei Verdacht auf Virus-Befall Arbeit wie gewohnt aber unverzüglich beenden.
- Computer ausschalten.
- Unerfahrene Anwender sollten einen Fachmann zu Rate ziehen(z. B. Benutzerdienst)
- Von virenfreier, schreibgeschützter System-Diskette booten
- Mit aktuellem Viren-Suchprogramm die Festplatte untersuchen; dabei ein Protokoll erzeugen.
- Datensicherung durchführen (falls nicht vorhanden).
- Virus von Festplatte entfernen
- Mit Viren-Suchprogramm die Festplatte erneut überprüfen.
- Alle anderen Datenträger (Disketten, CD-ROM, Wechselplatten) auf Viren-Befall untersuchen und Viren entfernen.
- Andere Benutzer warnen (wenn Daten- und E-Mail- Austausch von infiziertem Rechner erfolgte).
- Versuchen, die Quelle der Viren-Infektion festzustellen - wenn erfolgreich, anschließend: Programm-Hersteller oder Ersteller des Datenträgers informieren.

Wirtschaftliche Schäden durch Viren



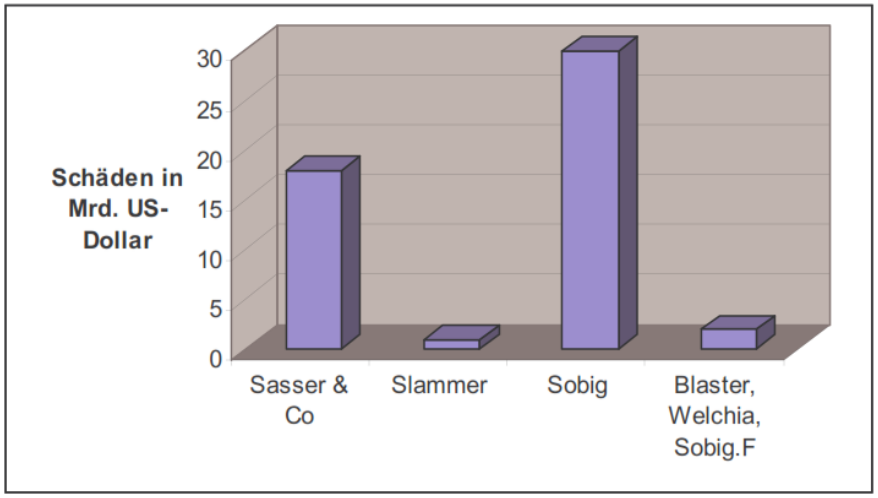
Quelle: Computer Economics 04.01.2002, www.computereconomics.com (24.05.2004)

Weltweiter wirtschaftl.Schaden v. Mailware

Trend für:

2002 auf 21 Mrd. US-Dollar

2006 auf 54 Mrd. US-Dollar



Auswirkungen in 2004 bei Mailware

In 12 Tagen 3 Viren der höchsten Bedrohungsstufe 5. Geschätzter Schaden 2 Mrd- US-Dollar.

Es ist heute keine Problem mehr, die Internet-Infrastruktur jedes Landes lahm zu legen!

Bedrohungen unter Windows, Linux, Mac usw.

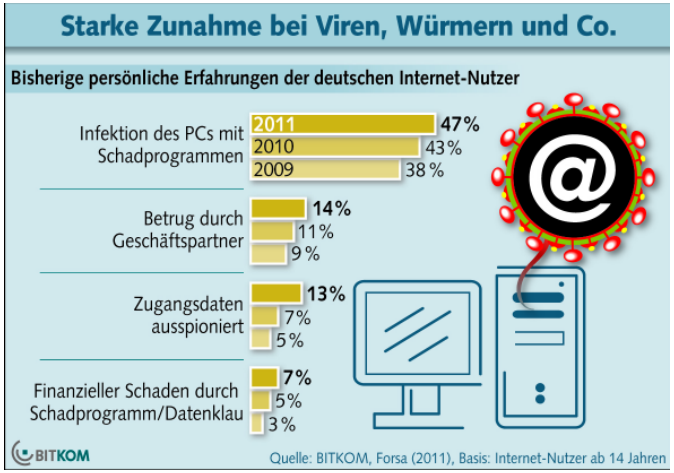
In Anbetracht der jüngsten Berichte von Befällen durch Schadsoftware auf Macs, scheint das OS X Betriebssystem sich selbst nicht genug von unzähligen im Internet zirkulierenden gefährlichen Programmen, Würmern, Trojanern und Malware schützen zu können (26. April 2012)

Schutz durch : Sophos, Intego, McAfee, Norton, Panda, BitDefender, Kaspersky

Durch das mehrstufige Rechtesystem von Linux ist die Virengefahr dort gering. Gibt es keinen Schutz können Viren z.B. durch Mails verbreitet werden.

Internetkriminalität 250.000 Fälle in 2010:
... „Insbesondere die Ausspähung von Online-Zugangsdaten, etwa für Plattformen oder Internet-Shops, ist im Vergleich zu 2010 stark angestiegen“!

Smartphone Viren liegt bei 0.4 %, vorwiegend bei Android Systemen – Warnung vor : ... der gefährlichen Banking-Viren für Android, die sich auf den Diebstahl beim Online-Banking spezialisiert haben.

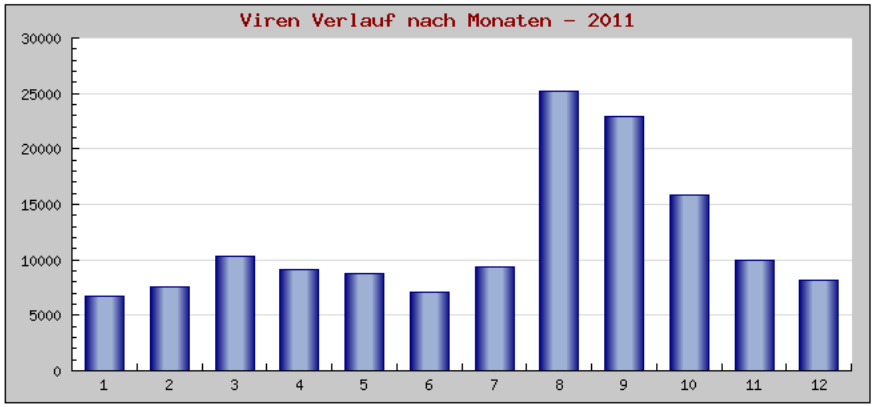


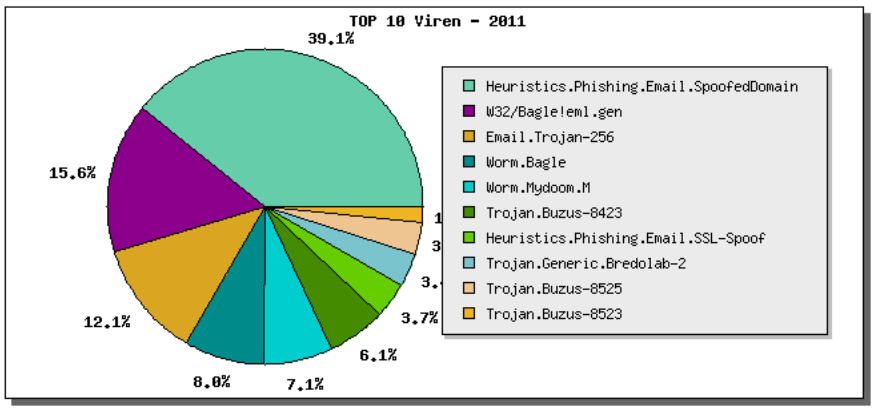
Akutelles

Virenstatistik für 2011

(Erstellt aus den Daten des zentralen Virus-Checking Clusters)

Anzahl verschiedene Viren: 489
Anzahl gefundener Viren: 140.965

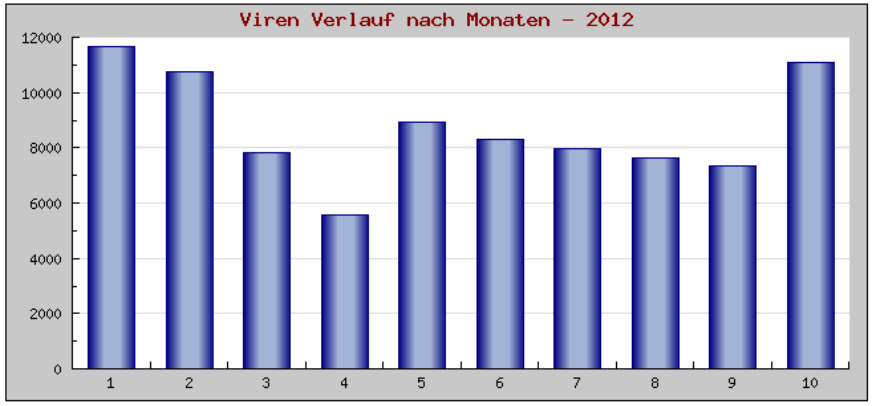


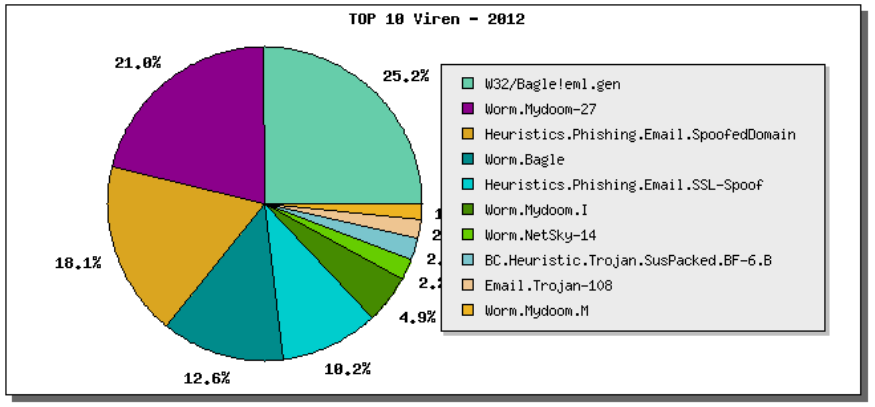


Virenstatistik für 2012

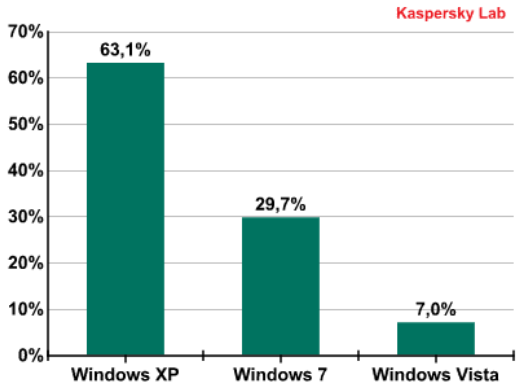
(Erstellt aus den Daten des zentralen Virus-Checking Clusters)

Anzahl verschiedene Viren: 509
Anzahl gefundener Viren: 87.084

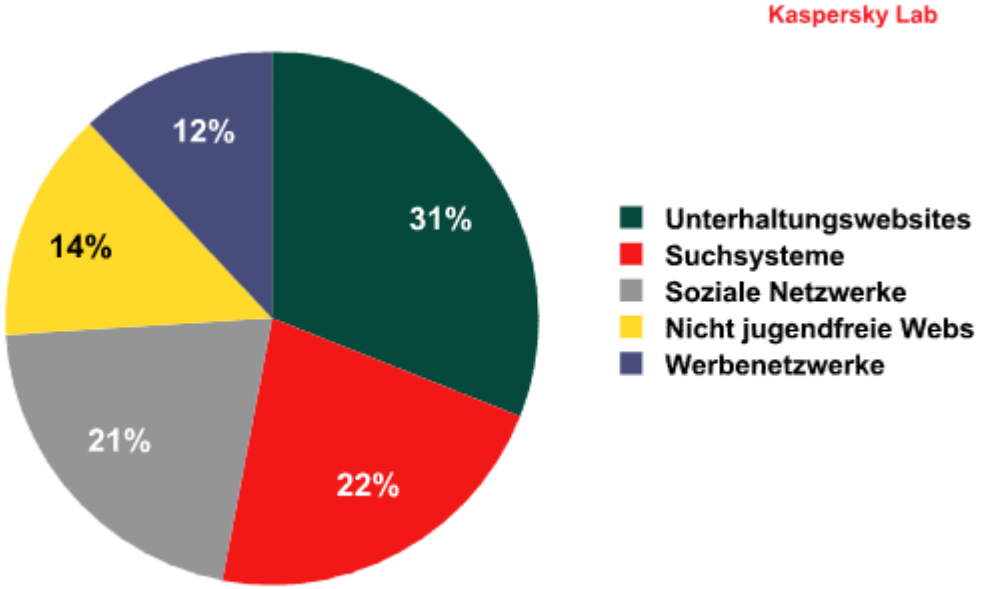




Akutelles



Jahr 2011



Kategorien von Webseiten, von denen die Anwender im Jahr 2011 am häufigsten versucht haben, schädlichen Links zu folgen

Bedrohungen - Schutz vor Virus, Würmer und Konsorten

Quellen

- Marcus Cramer:
  Viren, Würmer und Trojaner und ihre wirtschaftlichen Auswirkungen Seminar SS2004
- Marcus Schärtel:
  Praxis Viren-Glossar 01-01-112-116-VirenWuermerundKonsorten
  Internet World Januar 2001
- Virenstatistiken
  http://www.zid.tuwien.ac.at/security/virenstat/viren_stat.php
- Kaspersky Lab Security Bulletin 2011/2012. Statistik für das Jahr 2011
  http://www.viruslist.com/de/analysis?pubid=200883771
- https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Schadprogramme/schadprogramme_node.html

Bedrohungen - Schutz vor Virus, Würmer und Konsorten

tricom
Dr. Thomas Nittka
Löptener Str. 5
Tel.: 030 – 45086145
Fax: 030 – 45086144
Nittka@tricom-edv.de

IT Consulting

Analysen + Prozesse + Lösungen

IT-Sicherheit im Mittelstand

Berlin am 29.11.2012

Ute Zorn

IT Consulting

Analysen + Prozesse + Lösungen

Angaben zur Referentin

Ute Zorn

Staatlich geprüfte Betriebswirtin (Datenverarbeitung/Organisation)

Seit 1971 in der IT (IT-Organisation, IT-Sicherheitsmanagement, IT-Projektmanagement, IT-Controlling, IT-Training)

Seit 2009:

IT-Freelancerin am Markt aktiv tätig (IT-Consulting-Zorn.de)

Kompetenzen:

- Projektaufgaben im Bereich der IT-Organisation
- Langjährige Erfahrungen im Bereich der IT-Sicherheit als IT-Sicherheitsbeauftragte
- Langjährige Erfahrungen im Bereich des IT-Risikomanagements
- Erfolgreiche Zuarbeiten für die IT-Revision (gem. Anforderungen vom BaFin) Ansprechpartnerin gem. KWG § 24a
- IT-Trainerin (individuell, unternehmensintern und in Schulungscentern)

29.11.2012 IT-Sicherheit im Mittelstand 2

IT Consulting
Analysen + Prozesse + Lösungen

Themen-Übersicht

1. BSI IT-Grundschutz
2. Neues vom IT-Grundschutz
3. Zertifizierung
4. Aktuelle Sicht und Unterstützung der Behörden

IT Consulting
Analysen + Prozesse + Lösungen

Rechtliche Vorgaben in Deutschland …

… zur Informationssicherheit sind beispielsweise geregelt in:

- Bundesdatenschutzgesetz (BDSG)
- Aktiengesetz
- Bilanzrechtsmodernisierungsgesetz (BilMoG)
- Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (G
- GDPdU – Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
- Common Criteria - Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik
- MaRisk - Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informations- und Kommunikationstechnik (IuK – Mindestanforderungen)

IT Consulting
Analysen + Prozesse + Lösungen

Bundesamt für Sicherheit in der Informationstechnik (BSI)

- IT-Grundschutz
  die Basis für Informationssicherheit mit IT-Grundschutz-Katalogen (aktuell 12-EL) mit Bausteinen, Gefahren und Maßnahmen u.a. Hilfsmitteln

- Unterstützung bei der Vorgehensweise mit Leitfäden sowie anderen Dokumenten und Checklisten

IT Consulting
Analysen + Prozesse + Lösungen

IT-Grundschutzkataloge

IT-Grundschutz - Basis für Informationssicherheit

Schichtenmodell und Modellierung

Bausteine

Gefährdungskataloge

Maßnahmenkataloge

Hilfsmittel

Dokumente

- Überblickspapier Smartphones
- Überblickspapier Netzzugangskontrolle
- Überblickspapier Online-Speicher
- Grundlagenpapier Cloud Computing

IT-Krisenmanagement

BSI-Publikationen:
BSI-Broschüren
BSI-Kurzinformationen im Faltblattformat
Technische Richtlinien
u.v.m.

IT Consulting
Analysen + Prozesse + Lösungen

IT-Grundschutz-Standards

Bundesamt für Sicherheit in der Informationstechnik

- BSI-Standard 100-1:
  Managementsysteme für Informationssicherheit (ISMS)
- BSI-Standard 100-2:
  IT-Grundschutz-Vorgehensweise
- BSI-Standard 100-3:
  Risikoanalyse auf der Basis von IT-Grundschutz

  Zusätzlich:
  Risikoanalysen mittels elementarer Gefährdungen
- BSI-Standard 100-4:
  Notfallmanagement

29.11.2012 IT-Sicherheit im Mittelstand 7

IT Consulting
Analysen + Prozesse + Lösungen

Warum IT-Grundschutz?

Unerlässlich

- benötigte Informationen müssen korrekt für wesentliche Geschäftsprozesse (GP) vorliegen
- Diese GP sind vertraulich zu behandeln.
- Einheitliches Vorgehen ermöglicht Vergleichbarkeit

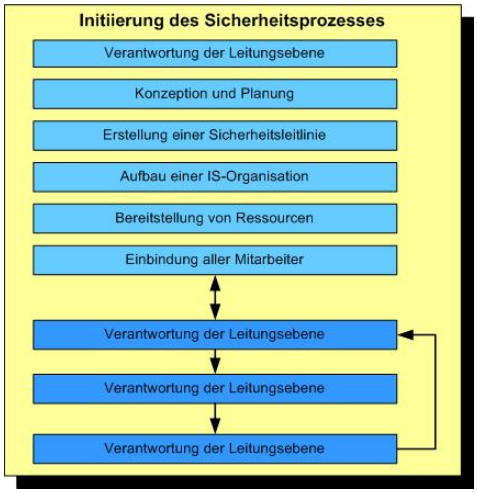
Wichtig ist daher

- unterstützende Informationstechnik muss reibungslos funktionieren
- Wirksame Schutzvorkehrungen gegen vielfältige und neuartigen Gefährdungen
  - Sicherheit von Informationen, Anwendungen, IT-Systemen und Kommunikationsnetzen

29.11.2012 IT-Sicherheit im Mittelstand 8

IT Consulting
Analysen + Prozesse + Lösungen

Initiierung des Sicherheitsprozesses

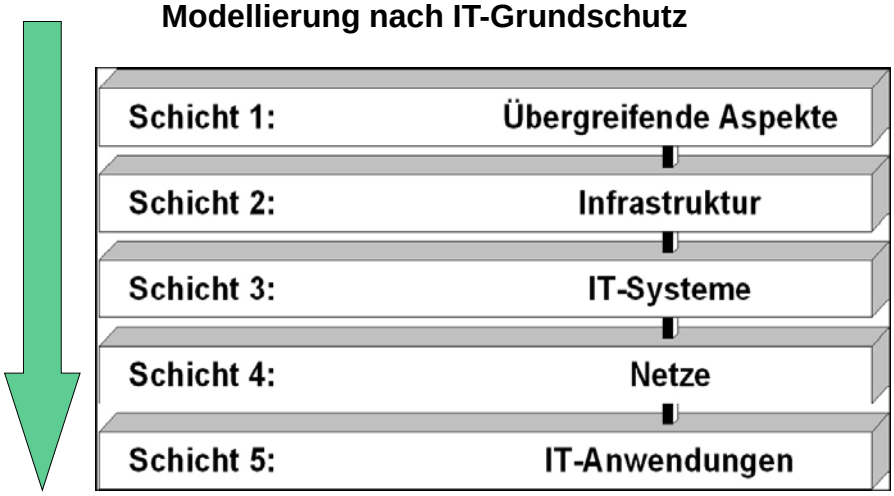


→ Gemäß BSI-Leitfaden 100-1 - ISMS

IT Consulting
Analysen + Prozesse + Lösungen

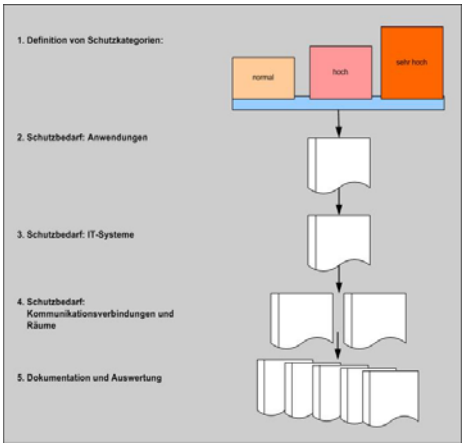
Schichtenmodell der IT-Sicherheit
1. IT-Strukturanalyse

Modellierung nach IT-Grundschutz



IT Consulting
Analysen + Prozesse + Lösungen

ISMS - Pkt. 2. Schutzbedarfsfeststellung



Ziel der Schutzbedarfsfeststellung:

- Ermittlung benötigten Schutzbedarfs für den Informationsverbundes und seiner zugehörigen Objekte?
- Weg zur begründeten und nachvollziehbaren Einschätzungen des Schutzbedarfs?
- Welche Objekte benötigen mehr Sicherheit, bei welchen genügen elementare Schutzmaßnahmen?

Auswahl **angemessener Sicherheitsmaßnahmen** für die einzelnen Objekte des betrachteten Informationsverbundes sind zu steuern.

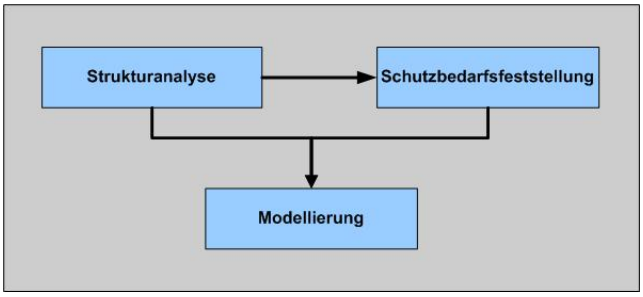
IT Consulting
Analysen + Prozesse + Lösungen

ISMS - Pkt. 3. Modellierung

1. **Strukturanalyse** nutzt Übersichten über die einzelnen Komponenten des betrachteten Informationsverbundes
2. **Ergebnisse** der **Schutzbedarfsfeststellung**
   Bausteine, deren Anwendung mit höherem Schutzbedarf, die einen höheren Schutzbedarf in einem der drei Grundwerte haben, werden genutzt
   → z.B. für den Baustein B 1.7 *Kryptokonzept*, der vor allem für solche Objekte wichtig ist, deren Bedarf an Vertraulichkeit hoch oder sehr hoch ist.
3. **Modellierung**
   → Abbilden Informationsverbund, seiner Komponenten gem. BSI-Bausteinen
   → Ergebnis ist ein IT-Grundschutz-Modell.
   → Einbeziehung auf Ergebnisse der beiden vorangegangenen Schritte

IT Consulting
Analysen + Prozesse + Lösungen

Modell als Prüfplan nutzen



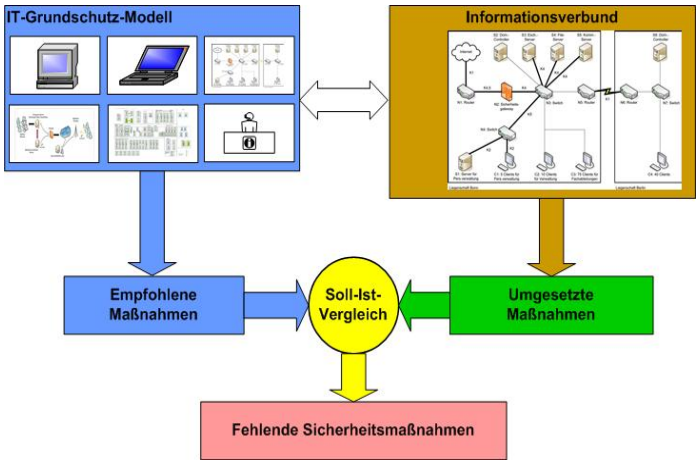
Dieses Modell können Sie für die bestehenden Teile Ihrer Informationstechnik als Prüfplan **verwenden und für geplante Teile als** Entwicklungskonzept**.**

29.11.2012 IT-Sicherheit im Mittelstand 14

IT Consulting
Analysen + Prozesse + Lösungen

ISMS - 4. Basis-Sicherheitscheck

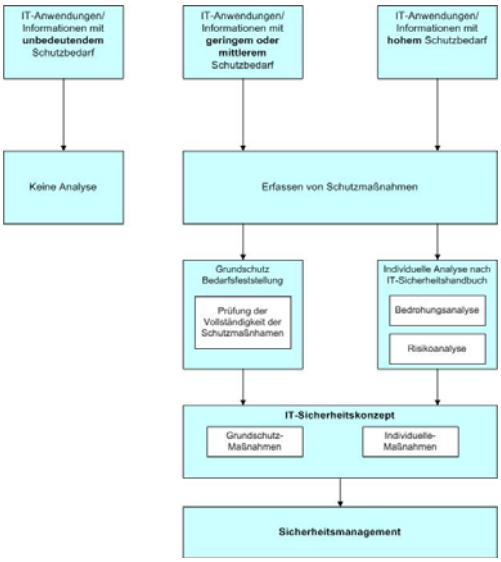
Prüfung ob die Informationen und die Informationstechnik hinreichend geschützt ist



29.11.2012 IT-Sicherheit im Mittelstand 15

IT Consulting
Analysen + Prozesse + Lösungen

Ablauf Ermittlung der Schutzbedürftigkeit

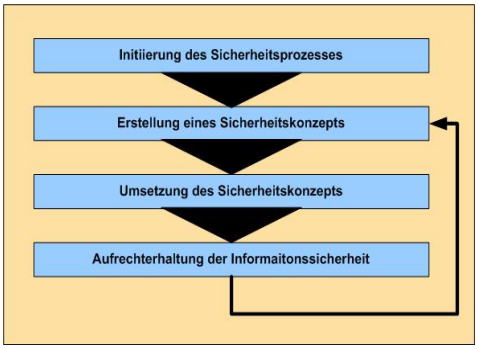


29.11.2012 IT-Sicherheit im Mittelstand 17

IT Consulting
Analysen + Prozesse + Lösungen

Aufrechterhaltung der Informationssicherheit

Kriterien zur Aufrechterhaltung der Sicherheit sind:



- regelmäßig kontrollieren (Prozess)
- Sicherheitsrevision
- Vollständigkeits- oder Aktualisierungsprüfung

29.11.2012 IT-Sicherheit im Mittelstand 20

Wichtige umzusetzende Regelungen

- Zu **festgelegten Zeitpunkten** sollte das Sicherheitskonzept (mindestens alle zwei Jahre) **überprüfen**, bei Bedarf aber auch vorzeitig
  → zum Beispiel nach Sicherheitsvorfällen.

Voraussetzung für die Aufrechterhaltung und Verbesserung der Informationssicherheit ist, eine Regelung:

- Zuständigkeit für die Überprüfung der Wirksamkeit und Angemessenheit der Sicherheitsmaßnahmen
- Tätigkeiten des IT-Sicherheitsbeauftragten und des IS-Management-Teams haben eine besondere Bedeutung

29.11.2012 IT-Sicherheit im Mittelstand 21

Risikoanalyse erstellen

IT-Grundschutz bedeutet das Sicherheitsniveau ist zu prüfen

- **normaler Schutzbedarf**
  ein **angemessenes und kostengünstiges Sicherheitsniveau** für **typische Infrastrukturen**
- **hohen oder sehr hohen Bedarf** an Vertraulichkeit, Integrität oder Verfügbarkeit,
- IT-Grundschutz-Kataloge enthalten (noch) **keinen passenden Baustein** (Beispiel: Labormessgerät mit direkter Netzanbindung
  oder
  ein solcher Baustein ist vorhanden,
  die Komponente wird in einer für das Anwendungsgebiet des IT-Grundschutzes **untypischen Weise** oder Einsatzumgebung betrieben?

29.11.2012 IT-Sicherheit im Mittelstand 22

IT Consulting
Analysen + Prozesse + Lösungen

Verfahren BSI-Standard 100-3

Bundesamt für Sicherheit in der Informationstechnik

Risikoanalyse auf Basis von IT-Grundschutz (Version 2.5)

1. Erstellen der Gefährdungsübersicht
2. Ermittlung zusätzlicher Gefährdungen
3. Gefährdungsbewertung
4. Behandlung von Risiken
5. Konsolidierung des IT-Sicherheitskonzepts
6. Rückführung in den IT-Sicherheitsprozess

IT Consulting
Analysen + Prozesse + Lösungen

Risikobewertung

- **sehr hohes Risiko** = Sofort-Maßnahmen unverzichtbar
- **hohes Risiko**
  = auf Dauer untragbar, Maßnahmen baldmöglichst realisieren
- **mittleres Risiko**
  = Reduzierung durch Maßnahmen des Grundschutzes angeraten
- **tragbares Risiko**
  = keine Maßnahmen erforderlich

IT Consulting
Analysen + Prozesse + Lösungen

Nutzen einer Risikoanalyse

- Identifizierung aller Werte und Schwächen
  → Bessere Entscheidungen bezüglich der Schutzmaßnahmen
- Gesteigertes Sicherheits-Bewusstsein unter Angestellten
- Rechtfertigung für Sicherheitsausgaben

IT Consulting
Analysen + Prozesse + Lösungen

Verfahren BSI-Standard 100-3

Bundesamt für Sicherheit in der Informationstechnik

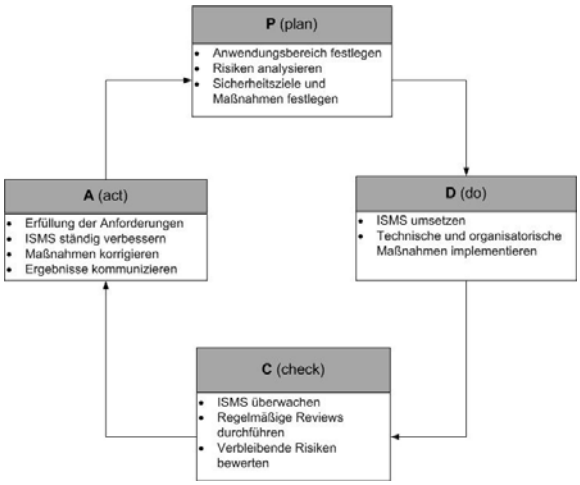
Rückführung in den

IT-Sicherheitsprozess

Umsetzung

und

Ständige Überwachung, Verbesserung



→ Werkzeuge können Risk Assessment Tools zur Überwachung sein.

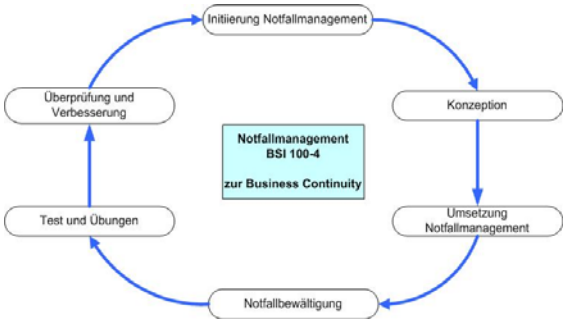
IT Consulting
Analysen + Prozesse + Lösungen

Notfallmanagement

Bundesamt für Sicherheit in der Informationstechnik

BSI-Standard 100-4 *Notfallmanagement* trägt zur Beantwortung derartiger Fragen bei.

- **Vorgehensmodell** für die Einführung, den Betrieb und die Weiterentwicklung eines Notfallmanagements in einer Institution.
- **Empfehlungen** für die anstehenden Aufgaben in den jeweiligen Phasen werden gegeben..



29.11.2012 IT-Sicherheit im Mittelstand 27

IT Consulting
Analysen + Prozesse + Lösungen

Neues vom IT-Grundschutz

Bundesamt für Sicherheit in der Informationstechnik

IT-Grundschutz-Kataloge
12. Ergänzungslieferung

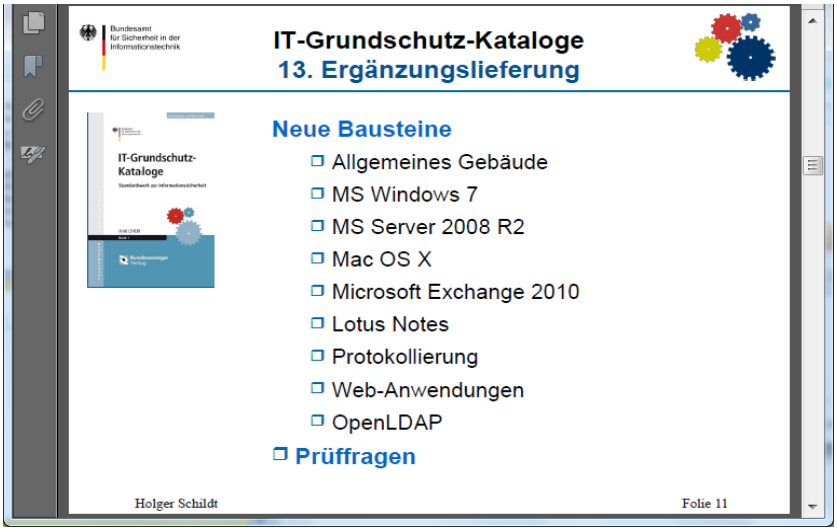
- Neue Bausteine
  - B 3.304 Virtualisierung
  - B 3.305 Terminal-Server
  - B 4.8 Bluetooth
  - B 5.3 Groupware
  - B 5.18 DNS-Server
  - B 5.19 Internet-Nutzung
- Überarbeitete Bausteine
  - B 3.401 TK-Anlage
  - B 5.4 Webserver
- Gestrichene Bausteine
  - B 3.403 Anrufbeantworter
  - B 5.10 Internet Information Server
  - B 5.11 Apache Webserver

29.11.2012 IT-Sicherheit im Mittelstand 28

IT Consulting
Analysen + Prozesse + Lösungen

Neues vom IT-Grundschutz

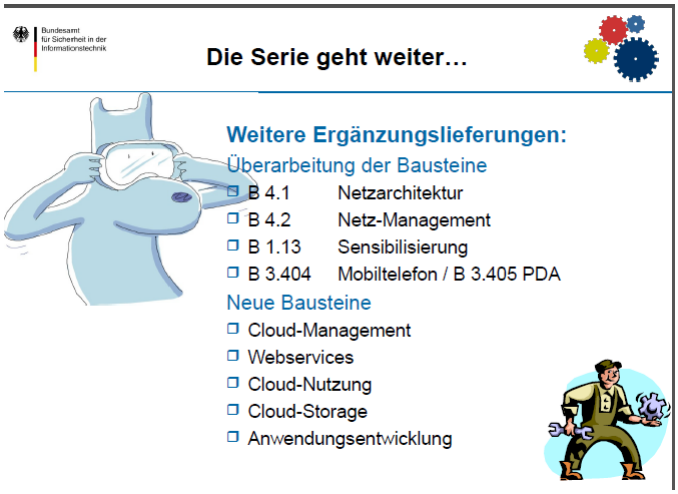
Bundesamt für Sicherheit in der Informationstechnik



IT Consulting
Analysen + Prozesse + Lösungen

Neues vom IT-Grundschutz

Bundesamt für Sicherheit in der Informationstechnik



IT Consulting
Analysen + Prozesse + Lösungen

Neues vom IT-Grundschutz

Bundesamt für Sicherheit in der Informationstechnik

IT Consulting
Analysen + Prozesse + Lösungen

Zertifizierung

- Zertifizierungsstellen (Beispiele)

Bundesamt für Sicherheit in der Informationstechnik

SAAR CERT TÜV

PERSICON cert

- Alle Zertifizierungsstellen orientieren sich an der Norm ISO/IEC 17021 für Zertifizierungsstellen.
- Es gibt Spielräume für Unterschiede.
- Es gibt verschiedene Zertifizierungsverfahren.
- BSI hat als staatliche Zertifizierungsstelle die meisten Spezifika und ist in erster Linie für den nationalen Raum geeignet.

Zusammenfassung

- IT-Sicherheit dient nicht dem Selbstzweck, sondern ist in der modernen Zeit unbedingte Notwendigkeit.
- Sie dient der Sicherung der Arbeitsfähigkeit im Unternehmen.
- Regeln zur IT-Sicherheit sind von allen Mitarbeitern zu beachten.
- Das Management der IT-Sicherheit kann man offiziell zertifizieren lassen.

„IT-Sicherheit kostet Zeit und Geld – Fehlende IT-Sicherheit die Zukunft“

Stefan Kronschnabel

Aktuelle Aktivitäten zur IT-Sicherheit der Regierung

Auswahl interessanter Informationen zum bedarfsgerechten Sicherheitsmanagements:

- Netzwerken für IT-Sicherheit - Interview Prof. Kempf –BITKOM

https://www.sicher-im-netz.de/unternehmen/2195.aspx

- Machen Sie den DsiN-Sicherheitscheck

https://www.sicher-im-netz.de/unternehmen/DsiN-Sicherheitscheck.aspx

- Neue Checkliste zum Thema Website-Sicherheit online

https://www.sicher-im-netz.de/wir_ueber_uns/News_2196.aspx

- IT-Sicherheitsnavigator

http://www.it-sicherheit-in-der-wirtschaft.de/IT-Sicherheit/Navigation/root.html

IT Consulting
Analysen + Prozesse + Lösungen

Wichtige Linksammlung zu Videos

Richtiges Passwort
http://www.youtube.com/watch?v=bRKEhr1TSLg&feature=plcp

Wie schütze ich mein Smartphone vor digitalen Bedrohungen?
http://www.youtube.com/watch?v=DofNGV1kCy0&feature=relmfu

Wie schütze ich mich vor Phishing?
http://www.youtube.com/watch?v=2gO0Fr3hssc&feature=relmfu

IT Consulting
Analysen + Prozesse + Lösungen

Haben Sie noch Fragen …