Ihr Partner für IT Lösungen

Konformität der IT in Ihrem Betrieb mit gesetzlichen und unternehmerischen Vorgaben

Dr. Michael Schiffmann, SINTEC Informatik GmbH

IGZ Bamberg, 11.07.2012

Ziele

- Überblick über die einzelnen durch Compliance-Regelungen betroffenen Bereiche der Informationstechnologie
- Gefahren und Risiken durch eine nicht compliance-gerechte IT
- Anforderungen der Compliance an die IT
- Möglichkeiten zur Sicherstellung der Konformität der IT in Ihrem Betrieb mit gesetzlichen und unternehmerischen Vorgaben

Inhalte

- Überblick über die verschiedenen gesetzlichen Regelungen und Standards
- Themen in Bezug auf IT-Compliance
- Organisation (der IT-Abteilung)
- Lizenzmanagement
- Berechtigungen
- Virenschutz und Patches
- Netzwerküberwachung
- Sicherung / Desaster Recovery
- Internet und e-Mail
- Archivierung
- Notfallplanung

Definition Compliance

- **Compliance = Regeleinhaltung**

- **Corporate Compliance:**

  Alle Maßnahmen zur Sicherstellung der Einhaltung von gesetzlichen und unternehmensinternen Regelungen durch Manager und Mitarbeiter

Gesetzliche Standards

- KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich)
- Telekommunikationsgesetz (TKG)
- Bundesdatenschutzgesetz (BDSG)
- Grundsätze zum Datenzugriff und Prüfbarkeit digitaler Unterlagen (GDPdU)
- UrhG (Urhebergesetz)
- …

Europäische Richtlinien

- Basel II
- Sarbanes-Oxley Act (SOX)
- IFRS
- Problem:

  Keine konkreten Forderungen und Hinweise zur Einhaltung der IT-Compliance

Standards mit IT-Sicherheitsaspekten

- ISO 27001 ff (Informationssicherheits-Management-Systeme (ISMS)
  Überblick: http://en.wikipedia.org/wiki/ISO/IEC_27001
  http://de.wikipedia.org/wiki/ISO_27001

- ISO **27033** (Sicherheitsmaßnahmen und Monitoring)
  http://de.wikipedia.org/wiki/ISO_27001

- IT Grundschutzhandbuch (BSI)
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

- Standards mit IT-Sicherheitsaspekten
  - Cobit http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx
  - ITIL http://www.itil.org/de/vomkennen/itil/index.php
  - IDW

- Übersicht im Kompass der IT-Sicherheitsstandards V3.0 (BITKOM)
  http://www.bitkom.org/de/publikationen/38337_40496.aspx

Organisation der IT

- Verantwortlichkeiten und Regelungen für den IT-Einsatz sind verbindlich festzulegen
  - Vergabe von Zutritts-, Zugangs- und Zugriffsberechtigungen
  - Regelungen bei möglichen Verletzungen der IT-Sicherheitspolicy
- Abweichungen sind zu kontrollieren und dokumentieren

Organisation der IT

- Aufbauorganisation
  - nach Verantwortlichkeit
  - Arbeitsplatzbeschreibungen
  - Vertreterregelungen

- Ablauforganisation
  - Prozessdokumentation unterstützt durch
    - Richtlinien (4-Augenprinzip, Erstellung – Zuweisung von Berechtigungen, Passwortweitergabe)
    - Arbeitsanweisungen
    - Handbücher

Lizenzmanagement

- Unterlizenzierung – Überlizenzierung
- Umfang
  - Planung,
  - Beschaffung,
  - Installation,
  - Deinstallation,
  - Software- Lizenzdatenbank,
  - Controlling der Maßnahmen,
  - Zuständigkeit und Kompetenzen
- Überwachung
  - Nicht lizenzierte SW auf Rechnern
  - Nicht autorisierte Verwendung von Software (Tools!!)
  - Downloads (Urheberschutzverletzungen)

Lizenzmanagement

- Rechtsfolgen
  - Unterlizenzierung:
    - Urheberrechtsverletzung gemäß § 69 UrhG -> Unterlassung, Auskunft, Schadensersatz
    - Straftatbestand des § 106 UrhG (Mitarbeiter, IT-Administratoren, Unternehmensleitung)
- Wirtschaftliche Konsequenzen
  - Unterlizenzierung:
    - Nachkauf von Lizenzen zu Listenpreisen, ggf. rückwirkend
  - Überlizenzierung:
    - zu hohe Wartungskosten

Virenschutz und Patchmanagement

- Virenschutz:
  - Schutz der Rechner und Netzwerke vor schädlichen Programmen

- Patchmanagement:
  - Schließung erkannter Sicherheitslücken
  - Beseitigung von Fehlern in Programmen

Virenschutz und Patchmanagement

93%
Increase in Web Attacks

A growing proliferation of Web-attack toolkits drove a 93% increase in the volume of Web-based attacks in 2010 over the volume observed in 2009. Shortened URLs appear to be playing a role here too. During a three-month observation period in 2010, 65% of the malicious URLs observed on social networks were shortened URLs.

260,000
Identities Exposed per Breach

This was the average number of identities exposed in each of the data breaches caused by hacking throughout the year.

42%
More Mobile Vulnerabilities

In a sign that the mobile space is starting to garner more attention from both security researchers and cybercriminals, there was a sharp rise in the number of reported new mobile operating system vulnerabilities—up to 163 from 115 in 2009.

6,253
New Vulnerabilities

Symantec recorded more vulnerabilities in 2010 than in any previous year since starting this report. Furthermore, the new vendors affected by a vulnerability rose to 1,914, a 161% increase over the prior year.

14
New Zero-Day Vulnerabilities

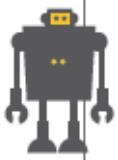
The 14 zero-day vulnerabilities in 2010 were found in widely used applications such as Internet Explorer, Adobe Reader, and Adobe Flash Player. Industrial Control System software was also exploited. In a sign of its sophistication, Stuxnet alone used four different zero-days.

74%
Pharmaceutical Spam

Approximately three-quarters of all spam in 2010 was related to pharmaceutical products—a great deal of which was related to "Canadian Pharmacy" websites and related brands.

1M+
Bots

Rustock, the largest botnet observed in 2010, had well over 1 million bots under its control. Grum and Cutwail followed, each with many hundreds of thousands of bots.



$15
per 10,000 Bots

Symantec observed an underground economy advertisement in 2010 promoting 10,000 bots for $15. Bots are typically used for spam or rogueware campaigns, but are increasingly also used for Distributed Denial of Service attacks.

$0.07 to $100
per Credit Card

This was the range of prices seen advertised in the underground economy for each "stolen" credit card number, and, as in the real economy, bulk buying usually gets the buyer a significant discount.

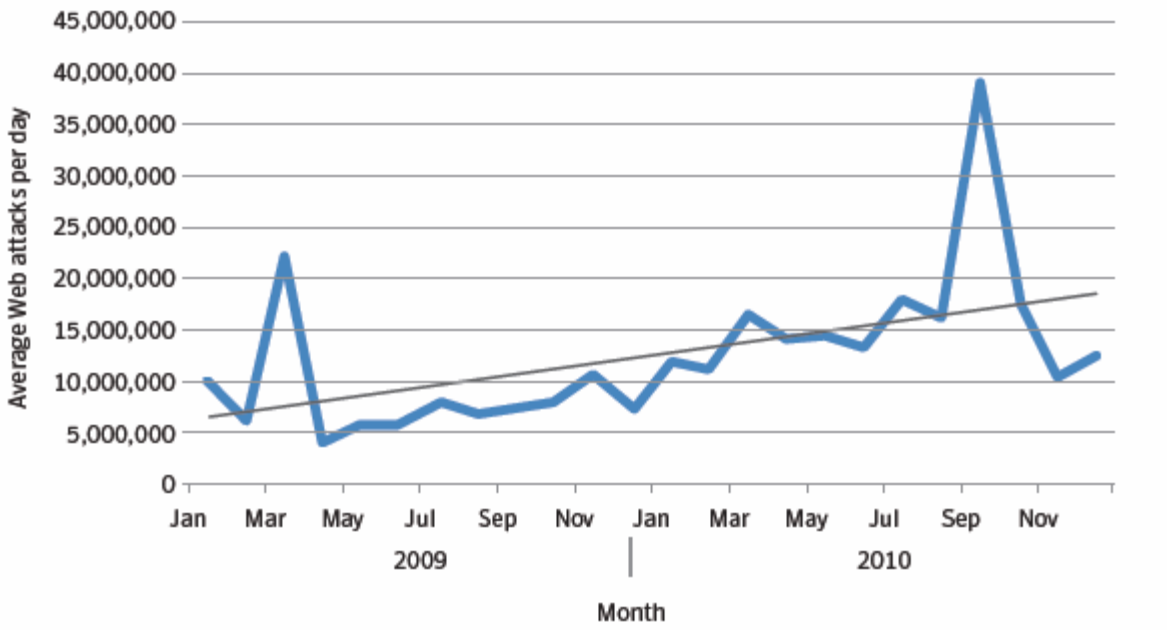
Source: Symantec Corporation

Virenschutz und Patchmanagement

Rank	Propagation Mechanisms	2010%	2009%
1	**Executable file sharing.** The malicious code creates copies of itself or infects executable files. The files are distributed to other users, often by copying them to removable drives such as USB thumb drives and setting up an autorun routine.	74% ↑	72%
2	**File transfer, CIFS.** CIFS is a file-sharing protocol that allows files and other resources on a computer to be shared with other computers across the Internet. One or more directories on a computer can be shared to allow other computers to access the files within. Malicious code creates copies of itself on shared directories to affect other users who have access to the share.	47% ↑	42%
3	**Remotely exploitable vulnerability.** The malicious code exploits a vulnerability that allows it to copy itself to or infect another computer.	24%	24%
4	**File transfer, email attachment.** The malicious code sends spam email that contains a copy of the malicious code. Should a recipient of the spam open the attachment, the malicious code will run and the recipient's computer may be compromised.	18% ↓	25%
5	**File sharing, P2P.** The malicious code copies itself to folders on an infected computer that are associated with P2P file-sharing applications. When the application runs, the malicious file will be shared with other users on the same P2P network.	8% ↑	5%
6	**File transfer, HTTP, embedded URI, instant messenger.** The malicious code sends or modifies instant messages with an embedded URI that, when clicked by the recipient, will launch an attack and install a copy of the malicious code.	4% ↓	5%
7	**File transfer, instant messenger.** The malicious code uses an instant messaging client to initiate a file transfer of itself to a recipient in the victim's contact list.	2% ↑	1%
8	**SQL** The malicious code accesses SQL servers, by exploiting a latent SQL vulnerability or by trying default or guessable administrator passwords, and copies itself to the server.	1% ↓	2%
9	**File transfer, HTTP, embedded URI, email message body.** The malicious code sends spam email containing a malicious URI that, when clicked by the recipient, will launch an attack and install a copy of the malicious code.	< 1%	< 1%
10	**File transfer, MMS attachment.** The malicious code uses Multimedia Messaging Service (MMS) to send spam messages containing a copy of itself.	< 1%	< 1%

Propagation mechanisms in 2010
Source: Symantec Corporation

Virenschutz und Patchmanagement



Average Web-based attacks per day, by month, 2009–2010

Source: Symantec Corporation

Virenschutz und Patchmanagement

Virenschutz: Lfd. Aktualisierung (4 Std.) der Virenpattern

3-stufiges Virenschutzkonzept:

- Zugänge zum Unternehmen (Mail-Gateway, Internet, Standleitungen, VPN)
- IT-Systeme (Server)
- Endpunkte (PC´s, Notebooks, mobile Geräte)
- Verwendung von Virenschutzprogrammen unterschiedlicher Hersteller
- Zentrale Installation und Überwachung
- Notfallkonzept für Vireneinbruch
- **Sicherheitsbewusstsein im Unternehmen**

Patchmanagement:

- Definition der Intervalle in denen regelmäßig gepatcht wird
- Regelung mit kritischen Patches
- Regelung für Tests, Freigabe und Übernahme der Patches in die produktiven Systeme

Virenschutz und Patchmanagement

Risiken und Rechtsfolgen:

- Versenden von virenbehafteten Daten und Schädigung der Systeme der Geschäftspartner
- Imageverlust

- Grundsätzlich: Schadensersatz aus § 823 BGB
- Der gewerbliche e-Mail Versender ist verpflichtet zumutbare und angemessene Sicherheitskonzepte, die den aktuellen Stand der Technik entsprechen, einzusetzen.

- Bei Geschäftspartnern mit vertraglicher Bindung: Schutzpflichten innerhalb des Vertrags

- Ggf.: Datenschutzverstoß
- Mitverschulden des Empfängers

Netzwerküberwachung

- lfd. Überwachung der Hardware auf fehlerfreie Funktion
  - Proaktive Überwachung möglich
    (z.B. Fehlfunktion eines Lüfters kann vor dem Ausfall erkannt werden)
  - Überwachung des Netzverkehrs
  - Erkennung von Unregelmäßigkeiten im Netzwerk
- Definition was (Geräte, Ereignisse) überwacht werden soll
- Priorisierung von Meldungen
- Definition von Reaktionen auf Meldungen und Eskalationsstufen

Netzwerküberwachung

Risiken und Rechtsfolgen:

- Erforderlich zum Datenschutz (§9 BDSG)
  - Zugangskontrolle
  - Protokollierung aller Zugriffe auf das System (auch der erfolgreichen Zugriffe) (Intrusion Detection System)

- aber auch Datenschutzverstoß
  - bei Erhebung und Verwendung personenbezogener Daten

- Sind die Überwachungsmaßnahmen geeignet das Verhalten und die Leistung von Arbeitnehmern zu überwachen, ist das Mitbestimmungsrecht des Betriebsrates zu beachten.

- Bußgelder
- Schadensersatz

- Betroffene: Unternehmensleitung und Administration

Sicherung / Desaster Recovery

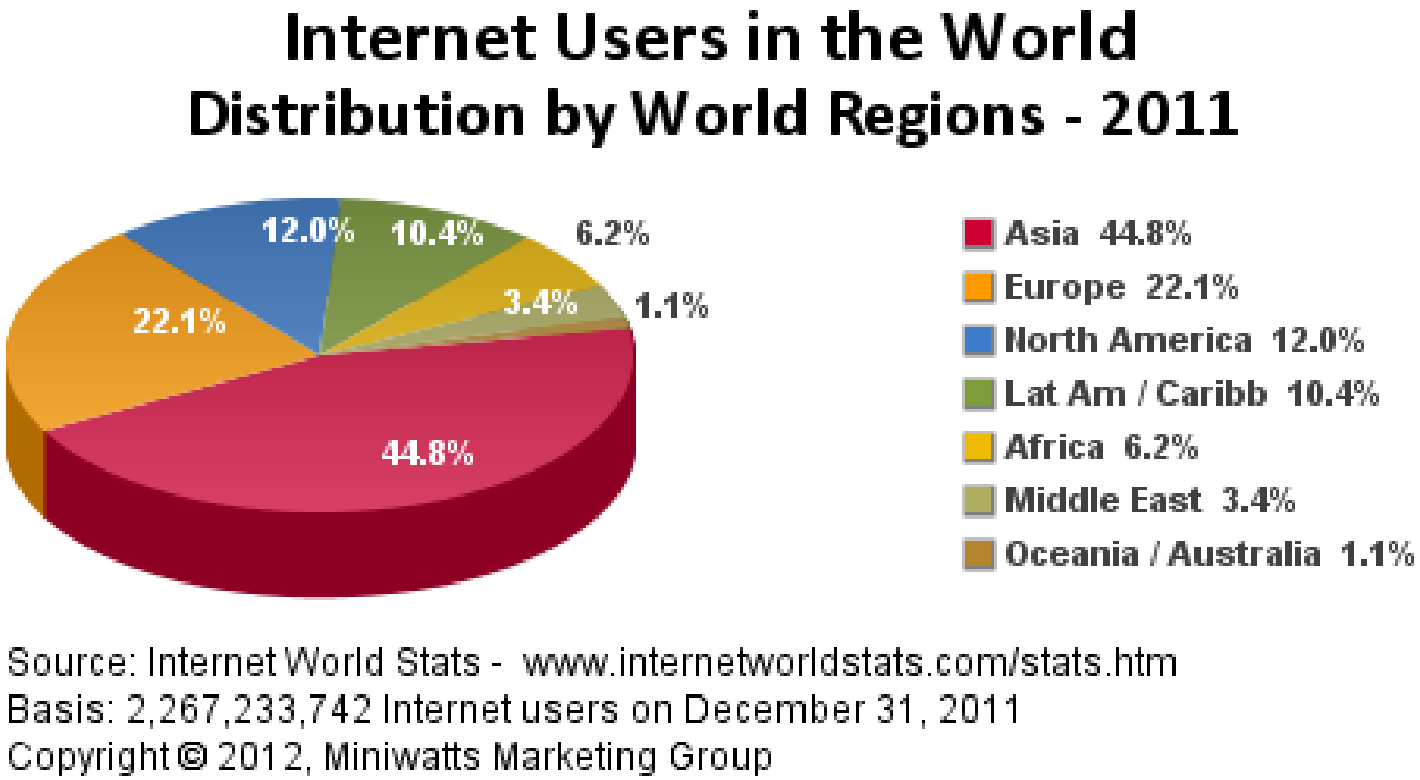
- Schutz vor:
  - Datenverlust
  - Dateninkonsistenz
- Unterscheidung zwischen:
  - dateibasierten und
  - datenbankbasierten Informationen
- Zeitpunkte und Intervalle der Sicherung
- Kontrolle der Sicherung
- Recovery
- Lagerung
- Speichermedien
- Wechsel des Sicherungsmediums
- Gesetzliche Aufbewahrungsfristen
- Archivierung

Sicherung / Desaster Recovery

Risiken:

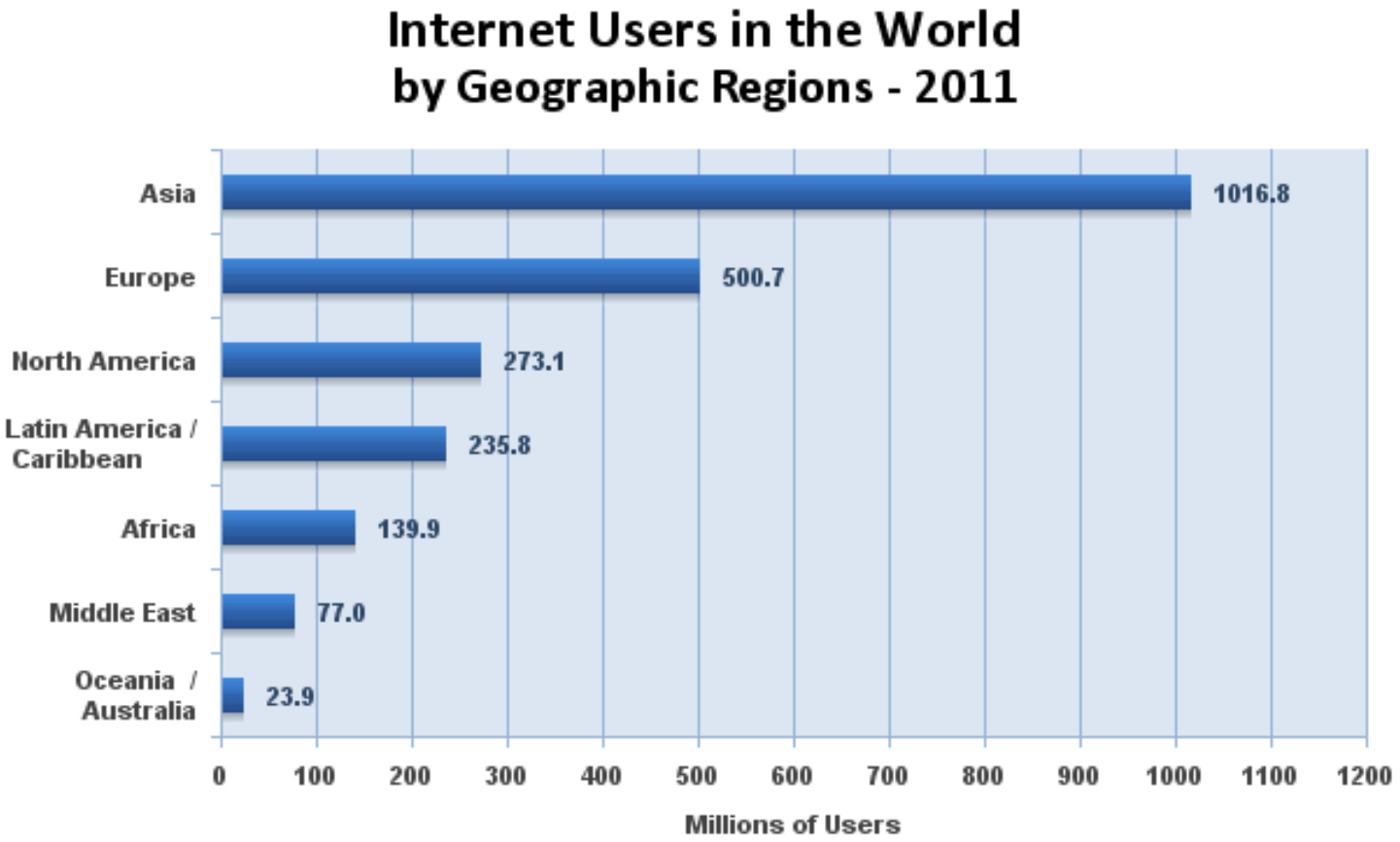
- Verlust von Schadensersatzansprüchen
- Verstöße gegen Archivierungspflichten
- Verstoß gegen die Verfügbarkeitskontrolle gem. Nr. 7 der Anlage zu § 9 BDSG

Internet und e-Mail



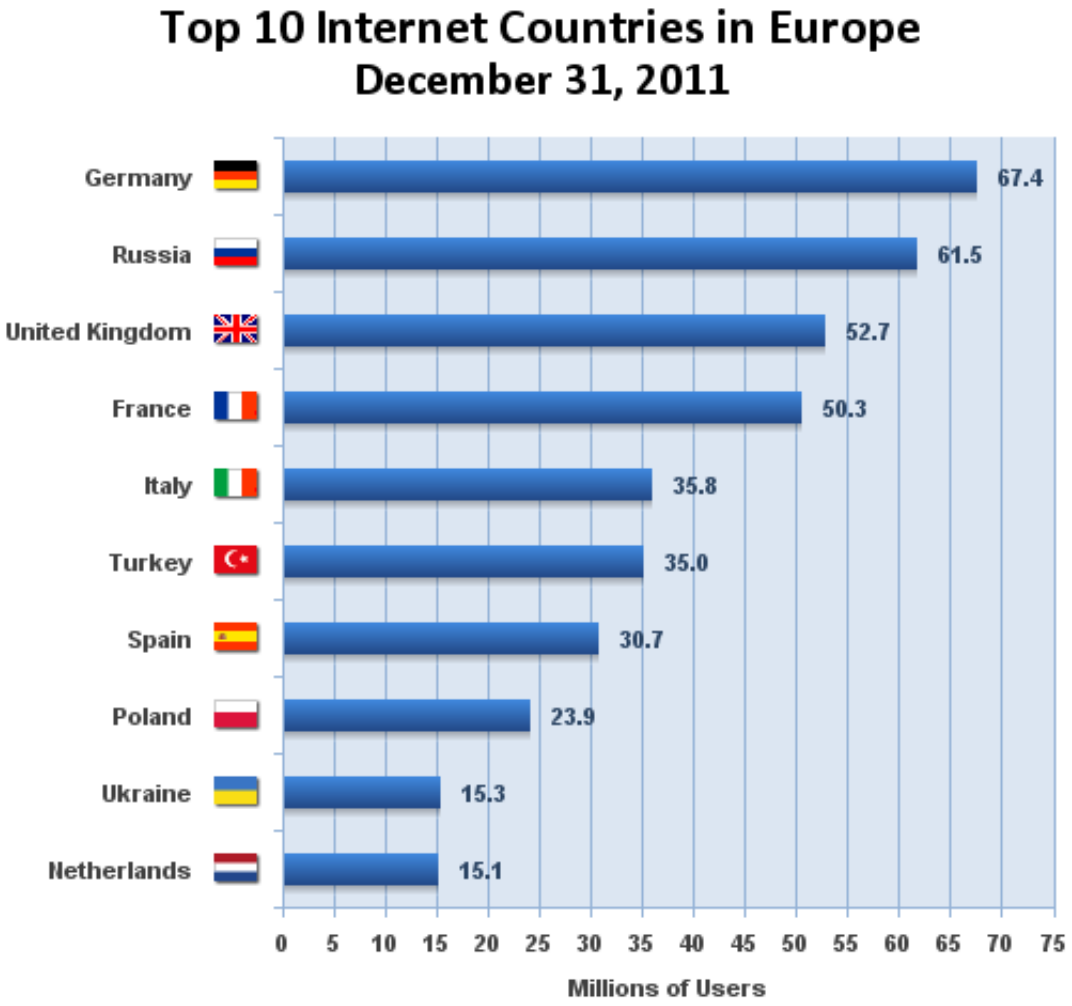
Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 2,267,233,742 Internet users on December 31, 2011
Copyright © 2012, Miniwatts Marketing Group

Internet und e-Mail



Source: Internet World Stats - www.internetworldstats.com/stats.htm
Estimated Internet users are 2,267,233,742 on December 31, 2011
Copyright © 2012, Miniwatts Marketing Group

Internet und e-Mail



Source: Internet World Stats - www.internetworldstats.com/stats4.htm
Basis: 500,723,686 estimated Internet Users in Europe on 2010Q4
Copyright © 2001-2012, Miniwatts Marketing Group

Internet und e-Mail

- keine Verpflichtung des Arbeitgebers seinen Mitarbeitern die private e-Mail und Internetnutzung zu ermöglichen
- stillschweigende Duldung führt zur betrieblichen Übung
- Regelung notwendig

Internet und e-Mail

- Erlaubte Internetnutzung:
  - Arbeitgeber wird zum Diensteanbieter von Telekommunikationsdiensten gem. § 3 Nr. 6 TKG
  - -> Fernmeldegeheimnis und die strengen Datenschutzvorgaben sind zu berücksichtigen (§ 88 TKG) insb. in Bezug auf
    - Inhalt
    - Beteiligte
    - aber Daten dürfen erhoben werden, wenn dies zum Schutz der Systeme notwendig ist
    - beim Vorliegen dokumentierter, tatsächlicher Anhaltspunkte in Bezug auf rechtswidriges Verhalten durch Bestand- und Verkehrdaten erhoben und verwendet werden.
  - Im Prinzip aber: Kein Zugriff des Arbeitgebers auf e-Mails

Internet und e-Mail

- Verbot der privaten Internetnutzung:
  - Arbeitgeber ist nicht an das Fernmeldegeheimnis und die strengen Datenschutzvorgaben des TKG gebunden
  - „lediglich“ die Persönlichkeitsrechte und die allgemeinen datenschutzrechtlichen Vorgaben des BDSG sind zu berücksichtigen
  - Weitgehende Zugriffsrechte des Arbeitgebers auf e-Mail und Internetverkehr

Internet und e-Mail

Risiken:

- Spam
- Phishing
- Malware
- Datendiebstahl durch Mitarbeiter

- Verstöße gegen das Fernmeldegeheimnis: Strafbarkeit gem. § 206 StGB in Betracht (Freiheitsstrafe bis zu fünf Jahre oder Geldstrafe)
- Schadensersatz
- Beweisverwertungsverbot

- Der Betreiber eines unverschlüsselten WLANS haftet für Rechtsverletzungen, die darüber erfolgen

Archivierung

- die Aufbewahrungspflicht für Handelsbriefe und die in § 257 Abs. I Nr. 1 genannten Unterlagen gelten auch für e-Mails
- in steuerlicher Hinsicht müssen Unterlagen innerhalb der Aufbewahrungspflicht “unverzüglich” lesbar und “maschinell auswertbar” sein
- die inhaltliche und bildliche Übereinstimmung ist vorgeschrieben
- elektronisch archivierte Dokumente müssen mit einem unveränderbaren Index versehen werden
- eine historisierte, aber auch aktuelle Verfahrensdokumentation ist notwendig
- die Revisionssicherheit MUSS gegeben sein

Archivierung

Risiken:

- unzureichende Archivierung ist eine Verletzung der Buchführungspflichten (Freiheitsstrafe bis zu 2 Jahren, oder Geldstrafe)
- Strafbarkeit gem. §274 StGB wegen Beseitigung beweiserheblicher Daten (Freiheitsstrafe bis zu 5 Jahren, oder Geldstrafe)
- Schätzung durch die Finanzbehörden
- Zwangsgeld

- für Vorstand oder Geschäftsführer

Notfallplanung

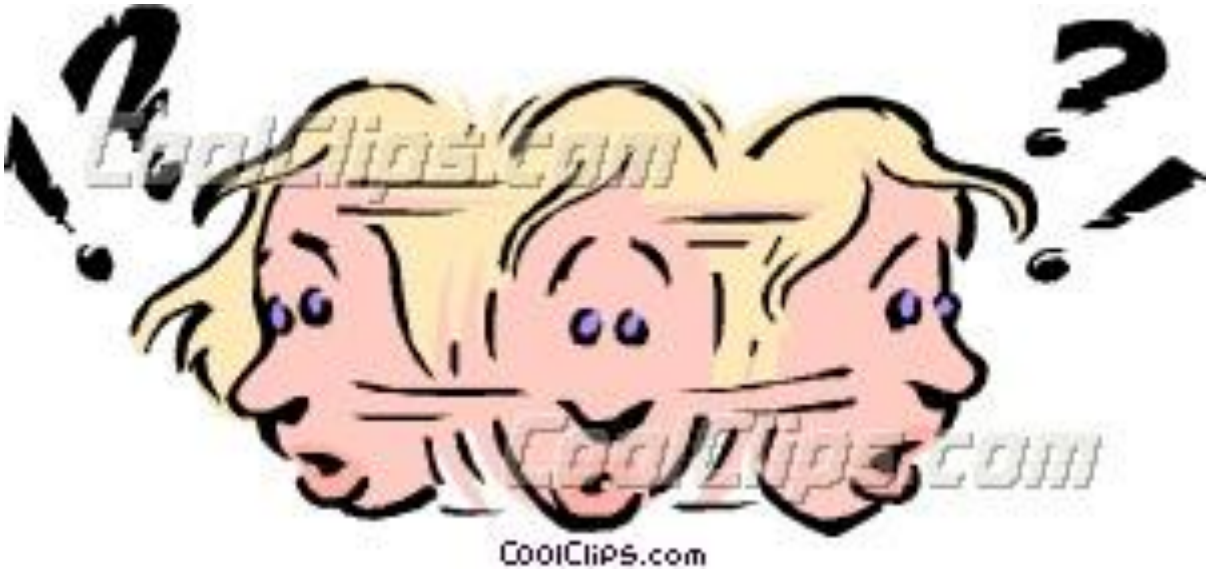
- **Notfallvorsorge**
  - Übersicht über die Verfügbarkeitsanforderungen der Systeme
  - Definition des Notfalls (Überschreitung der maximal tolerierbaren Ausfallzeit und Überschreitung einer zuvor definierten Schadenshöhe)
  - Definition von Maßnahmen für den Notfall

- **Notfallhandbuch**
  - Aufzählung möglicher Notfälle
  - Bewertung
  - Eintrittswahrscheinlichkeit
  - Alarmierungsplan
  - Sofortmaßnahmen
  - Wiederanlaufpläne für kritische Systeme
  - Dokumentation der Systeme
  - ggf. Ausweichmöglichkeiten

Notfallplanung

- Risiken: siehe Sicherungen, Archivierung

????


CoolClips.com

Herzlichen Dank für Ihre Aufmerksamkeit

SINTEC Informatik GmbH
Ludwig-Quellen-Str. 18
90762 Fürth
Tel. +49 911 979 93 0
www.sintec.de

Dr. Michael Schiffmann
Tel. +49 911 979 93 23
Fax +49 911 979 93 30
michael.schiffmann@sintec.de