

Orientierung im Paragraphendschungel: Rechtssicher im Internet unterwegs



Datenschutz im Netz – Was muss ich beachten?

Gilbert Staffler

Betriebswirt (VWA)

Zertifizierter Datenschutzbeauftragter
durch die FH Südwestfalen

EDV-Sachverständiger

Inhaber EHS-Datentechnik

März 2010

IT-Sicherheit und Datenschutz

■ IT-Sicherheit in Ihrem **eigenen** Interesse



- Schutz von Daten vor Beeinträchtigungen bei der Verarbeitung
- nicht nur personenbezogen

■ Datenschutz im Interesse der **Betroffenen**

- Schutz vor Missbrauch personenbezogener Daten
- Schutz vor Persönlichkeitsrechts-Beeinträchtigungen durch die automatisierte Verarbeitung

■ Aber: **Ohne** IT-Sicherheit **kein** Datenschutz!

Von Daten zu Informationen

- **Information** = Wissen aus **Daten**, die beim Empfänger noch nicht bekannt waren
- Prozess: aus Daten  Information mit moderner EDV  Triebfeder der modernen Informationsgesellschaft (Data-Mining / Data-Warehousing / Data-Grabbing)

BDSG Grundsätze

- so genannte Verbotprinzip mit Erlaubnisvorbehalt
- Grundsatz der Datenvermeidung und Datensparsamkeit

„Payback“ und Co.

„Tausche Privatsphäre gegen Rabatt“



Um welche Daten geht es eigentlich?

■ Personenbezogene Daten

- Mitarbeiterdaten, z.B.: Bildungsstand, Kenntnisse, Fähigkeiten, Erfahrungen, („...Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens...“), rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualeben, Lohn- und Gehaltsdaten, Zeugnisse, Surf- und Mailverhalten, installierte Software auf zugewiesenem PC, Personalnummer, Benutzerkennung (User-ID), IP-Adresse
- Informationen zu einer Person z.B. Produktnutzung, Einkaufsverhalten, Kontaktdaten, Hobby, Interessen, Werbeaffinität, Wohnumfeld, Haushaltsgröße
- Kunden- oder Mandantendaten, Lieferantendaten

Um welche Daten geht es nicht?

Nicht Aufgabe gem. BDSG:

- Technologiedaten
- Betriebswirtschaftliche Daten
- Strategische Daten

Seit wann gibt's Datenschutz?

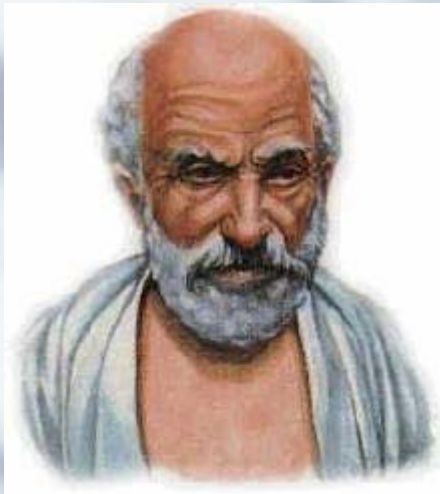
- Was meinen Sie?



D
M
C
IV
II
L
VII
VIII
VII

Hippokrates

- „Was ich bei der Behandlung sehe oder höre oder auch außerhalb der Behandlung im Leben der Menschen, werde ich, soweit man es nicht ausplaudern darf, verschweigen und solches als ein Geheimnis betrachten.“



Hippokrates von Kòs

(* um ca. 460 v. Chr. + um 375 v. Chr.)

Wichtige Rechtsnormen zum Datenschutz in der EDV, Telekommunikation und für Websites

**Bundesdatenschutzgesetz
(BDSG)**

**Betriebsverfassungsgesetz
(BetrVG)**

**Telekommunikationsgesetz
(TKG)**

**Telemediengesetz
(TMG)**

**Gesetz gegen den unlauteren Wettbewerb
(UWG)**

...

Website /Shop

- **Anbieterkennzeichnung (Impressum)**
- **Unterrichtung des Nutzers**
- **Einwilligung**
- **Profilbildung**
- **Hinweis auf Weiterleitung an Dritte (Verlinkung)**
- **Technisch-organisatorischer Datenschutz**
- **E-Mail-Newsletter**
- **Preisausschreiben oder Gewinnspiele**
- **Mitarbeiterdaten auf der Website**

Mitarbeiterdaten auf der Website

■ Mitarbeiterdaten auf der Website sind **zulässig**

- insoweit, als dies zur **Erfüllung des Arbeitsvertrags** erforderlich ist (z.B. Name des Kundenberaters, seine Telefonnummer und seine E-Mail-Adresse)
- im Rahmen **gesetzlicher Verpflichtungen** (z.B. Name des Geschäftsführers im Impressum)
- bei (freiwilliger) **Einwilligung** des Mitarbeiters (z.B. auch für das Foto) – Achtung: Einwilligung können jederzeit widerrufen werden!



Technisch-organisatorischer Datenschutz (1)

- Es sind **angemessene** Sicherheitsmaßnahmen umzusetzen:
 - Firewall, Antivirensoftware und Intrusion-Detection-System sollten Standard sein.
 - Bei der Verwaltung des Internet-Angebots durch einen Dienstleister handelt es sich i.d.R. um Datenverarbeitung im Auftrag (erfordert nach § 11 BDSG entsprechende vertragliche Regelungen (mind.10 Punkte) auch über die technischen und organisatorischen Sicherheitsmaßnahmen).

„Auftragsdatenverarbeitung“ (§ 11): Dokumentations- und Prüfungspflicht

50.000,- EUR

■ Der Auftrag ist schriftlich zu erteilen und muss folgenden Mindestinhalt haben:

1. der **Gegenstand und die Dauer** des Auftrags,
2. der **Umfang, die Art und der Zweck** der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die **Art der Daten** und der **Kreis der Betroffenen**,
3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm **vorzunehmenden Kontrollen**,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die **Kontrollrechte des Auftraggebers** und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. **mitzuteilende Verstöße des Auftragnehmers** oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. der **Umfang der Weisungsbefugnisse**, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. die **Rückgabe überlassener Datenträger** und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Der Auftraggeber muss **vor** Beginn der Datenverarbeitung und dann regelmäßig die Einhaltung der Datenschutzvorschriften beim Auftragnehmer prüfen. Das Ergebnis ist jeweils **schriftlich** zu dokumentieren.

Technisch-organisatorischer Datenschutz (2)

- Der Nutzer muss jederzeit den Zugriff auf oder die Nutzung des Webdienstes abbrechen können. Technische Maßnahmen, die genau das verhindern, sind unzulässig.
- Anfallende personenbezogene Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung sind unmittelbar nach deren Beendigung zu löschen

Technisch-organisatorischer Datenschutz (3)

- Die Daten müssen vor **unberechtigter Kenntnisnahme** während des **gesamten Übertragungsvorgangs** geschützt werden.
- Bezogen auf das offene Internet bedeutet das, dass bei sensibler Datenkommunikation eine hinreichende SSL-Verschlüsselung vorzusehen ist,
 - z.B. bei Bewerbungsdaten, Bankverbindung, Kreditkartendaten, Benutzerkennungen und Passwörtern.

Wie sicher ist eigentlich Ihr Passwort?

- **So lange dauert das Passwort-Knacken**
 - Rechenbeispiel: Ein 6-stelliges Passwort
 - wie oft der Fall - nur aus Kleinbuchstaben besteht.
 - 26 verschiedenen Zeichen bestehen
 - insgesamt 308.915.776 (also fast 309 Millionen) Kombinationen zulässt.

- Benötigt zum Knacken des Passwortes

Passwort geknackt in ...

- bei handelsüblicher Core 2 Quad Q6600, mit 45.423.600 „Tastenanschläge“ pro Sekunde: **6,8 Sekunden.**
- **Besser wird es bei**
- Kennwort aus **Klein- und Großbuchstaben und Zahlen** ergibt bei **6 Zeichen schon** rund **21 Minuten** Rechenzeit.
- Bei **7-stelligen** Passwörtern werden fast **22 Stunden.**
- Für **8 Zeichen** fast **2 Monate** brauchen;
- für **10 Zeichen** fast **600 Jahre.**
- Sonderzeichen und jede weitere Stelle verlängern die Berechnung um ein Vielfaches.

Quelle: http://www.pcwelt.de/start/sicherheit/backup/praxis/197778/so_knacken_sie_ihr_vergessenes_passwort/index2.html

Passwortrichtlinie

- Änderungsaufforderung, Verfallszeit
- Nutzungsfenster (z.B. nur während der Arbeitszeit?)
- Verbotene Passwörter (Trivialpasswörter wie z.B.: 4711, Username, OTTO, ATA....)
- Passwortlänge, -gestaltung, -historie, -protokollierung
- (Bsp.: „Ich bin das 1. Kind meiner Eltern! Ibd1KmE!“)

E-Mail-Newsletter

- Werbe-E-Mails sind Spam, wenn der Empfänger diese Mails unerwünscht erhält.
- Um beweisen zu können, dass eine bestimmte Person/Firma den Newsletter tatsächlich bestellt hat, genügt nicht die Protokollierung der Daten. Erforderlich ist ein „double opt-in“.
- Ein Werbecharakter darf nicht verschleiert werden.
- Kopf- und Betreffzeile dürfen nicht so gestaltet werden, dass der Empfänger vor Einsichtnahme in den Inhalt der Kommunikation keine oder irreführende Informationen über den kommerziellen Charakter der Nachricht erhält.
- Selbst, wenn durch BDSG erlaubt, ggf. durch UWG immer noch verboten!

Persönlichkeitsschutz durch Telekommunikationsgesetz (TKG)

■ Nach § 88 TKG

unterliegen Inhalt und die näheren Umstände einer Telekommunikation dem Fernmeldegeheimnis

Verpflichtet ist jeder Diensteanbieter!

Diensteanbieter ist, wer für Dritte - z.B. verbundene Unternehmen, oder die private Nutzung von Internet und E-Mail durch Mitarbeiter wird geduldet/erlaubt - Telekommunikationsdienste anbietet (unabhängig von einer Gewinnerzielungsabsicht).



Telekommunikationsdienste

- sind nicht nur die Telefonie, sondern auch das E-Mail-System, ggf. aber auch der Internetzugriff sowie die Nutzung der EDV bzw. des Netzwerks.



Verstöße gegen das Fernmeldegeheimnis werden nach dem Strafgesetzbuch (StGB) mit Freiheitsstrafe bis zu 5 Jahren geahndet.

Persönlichkeitsschutz durch Telemediengesetz (TMG) und Telekommunikationsgesetz (TKG)

Diensteanbieter (= Provider) bei

- Internetangebot (Homepage) oder wenn
- Mitarbeitern zu privaten Zwecken der Internetzugang ermöglicht wird.
(Vorsicht: Verbote müssen aktiv kontrolliert werden)



§ 88 Abs. 3 TKG Fernmeldegeheimnis

■ ... ist es untersagt, sich oder anderen ... Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen ...

■ **§ 206 StGB Verletzung des Post- oder Fernmeldegeheimnisses**

Wer unbefugt ... wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft ...



Der Zulässigkeitsrahmen ergibt sich aus der Einwilligung und Betriebsvereinbarung.

Löschen von Spam ohne Einwilligung des Mitarbeiters kann strafbar sein

■ § 303 a StGB Datenveränderung

(1) Wer rechtswidrig Daten ... löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.



*Der Zulässigkeitsrahmen ergibt sich aus der Einwilligung der Mitarbeiter und Betriebsvereinbarung.
(Virensan ist nach § 88 TKG zulässig.)*

Beispiel Telekommunikationsanlage

- Registrierung der ein- und ausgehenden Anrufe inkl. Teilnehmernummer, Dauer und Kosten jedes Gesprächs

Wenn private Telefongespräche erlaubt sind, dürfen die angerufenen Nummern nicht registriert werden - es sei denn, es erfolgt eine Gebührenabrechnung. Einzelheiten ergeben sich aus der Betriebsvereinbarung.

Neue Datenverarbeitungsprozesse

- Der Datenschutzbeauftragte ist über Vorhaben zu neuen Datenverarbeitungsprogrammen rechtzeitig zu unterrichten (§ 4g Abs. 1 Nr. 1 BDSG).

Der Datenschutzbeauftragte prüft dann, ob dieses neue Verfahren zulässig und eine Meldung für die Übersicht über die Verfahren erforderlich ist (§ 4g Abs. 2 BDSG). Er führt ggf. die gesetzlich erforderliche Vorabkontrolle durch.

Gefahren im Internet

- Internetseiten mit ungeeigneten Inhalten (Kinder und Jugendliche)
- Internetchats als Kontaktbörse
- Ungeeignete Computerspiele
- Spam
- Computerschädlinge
- Verbreitung ungeeigneter Inhalte über Bluetooth
- Teure Downloads über Internet oder Handy
- Kostenfallen Dialer und Handy-Payment
- Marketing – Beeinflussung durch verschleierte Botschaften
- Fehlendes Unrechtbewusstsein
- Soziale Netzwerke

Soziale Netzwerke

- ... wie **Facebook**, **Myspace**, **StudiVZ** oder **SchülerVZ**, **Spick Mich**, **YouTube** aber auch **XING**
- z.B.: StudiVZ hat im deutschsprachigen Raum bereits über 4 Millionen Nutzer.
- SchülerVZ ist zur Zeit, mit 6,4 Milliarden Seitenaufrufen pro Monat, die meist geöffnete Seite im gesamten deutschsprachigen Raum.
- StudiVZ liegt mit 6 Milliarden Seitenaufrufen knapp dahinter.



Polizeiermittler in sozialen Netzwerken

- Soziale Netzwerke sind "wahre Fundgruben für Ermittlungs- und Fahndungszwecke".
- gem. BVerfG: ein neues Grundrecht auf "Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme"

Quelle: <http://www.heise.de/newsticker/meldung/Polizeiermittler-in-sozialen-Netzwerken-924378.html>

Personensuchmaschinen – Unterschätzte Gefahr für die Karriere

- regelmäßige „Ego-Googeln“
- Studie „Etwa einem Drittel gefiel nicht, was sie im Internet über den Bewerber fanden, und erteilten ihm deshalb eine Absage.“ *
- z.B. <http://www.yasni.de/>
- Yasni verschickt zusätzlich E-Mails, sobald neue Ergebnisse zu seiner Person im Internet auftauchen.

* CareerBuilder-Studie 2008, USA

Datenschutz bei Suchmaschinen

- Üblicherweise werden bei Google alle Sucheingaben mindestens neun Monate lang inklusive ausgehender Internet-Adresse (IP) gespeichert. Über die IP ist beim Provider eine Rückverfolgung des Users (zumindest theoretisch) möglich.
- Nach neun Monaten wird nur ein Teil der IP anonymisiert. Der Rest des Datensatzes kann dann bis in alle Ewigkeit vorgehalten werden.
- z.B. Google begründet das mit der Nutzung für mögliche Optimierungen seiner Technik begründet.
- Abhilfe: Dienst zum Anonymen Surfen **Scroogle Scraper**

Browser & Browsereinstellungen

- Cookies
- Formulardaten
- Passwörter
- Technologie Active X
- Java
- JavaScript
- Die Chronik/ Verlauf/ History
- Browsercache

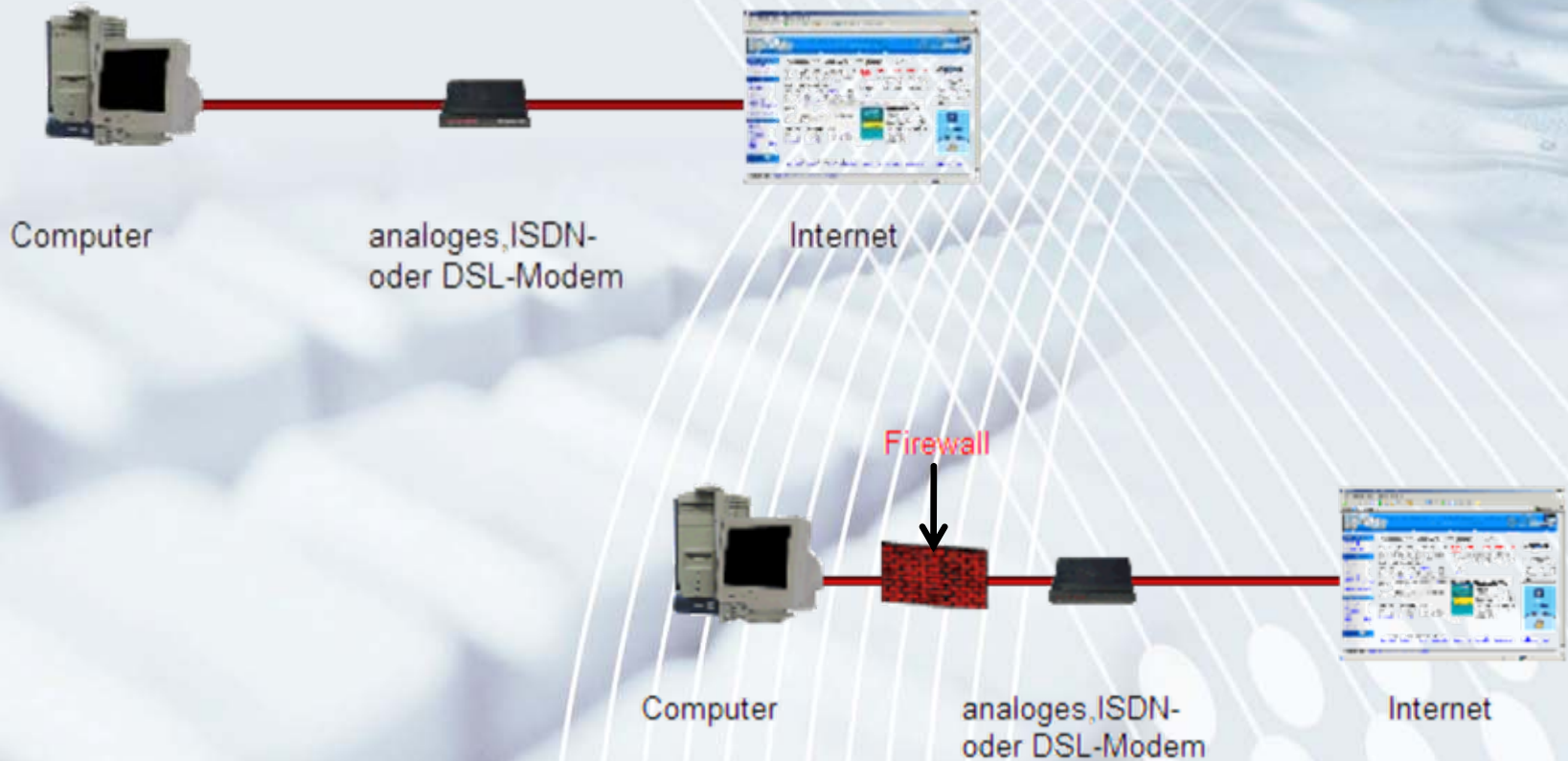
Mindestens aber:

- Für jedes Betriebssystem, egal ob Windows, Linux oder Mac OS, gilt:
 - Jede nicht in Gebrauch befindliche Software deinstallieren.
 - Jeden nicht benötigten Server-Dienst abschalten.
 - Anzahl der Software-Fehler durch regelmäßige Updates reduzieren.
 - Bei Software-Alternativen diejenige mit den geringsten Fehlern wählen.
 - Tendenziell die weniger komplexe Lösung verwenden.

Internet-Telefonie

- Durch die Übertragung über das Internet wird die Internettelefonie anfälliger für Angriffe und kann leichter abgehört werden.
- Sicherheitsproblemen durch Viren, Würmer, Trojaner und zu sogenannten „Denial of Service“ (DOS)-Attacken
- Oft keine ausreichende Verschlüsselung der Datenübertragung.
- Werbeindustrie: Spit (Spam over Internet Telephony) ist das Telefon-Pendant zum E-mail-Spam.

Firewall, Router, Modem und Co.



Bilder von: http://www.its05.de/computerwissen-computerhilfe/pc-sicherheit/firewall_software/firewall_software.html

Firewall

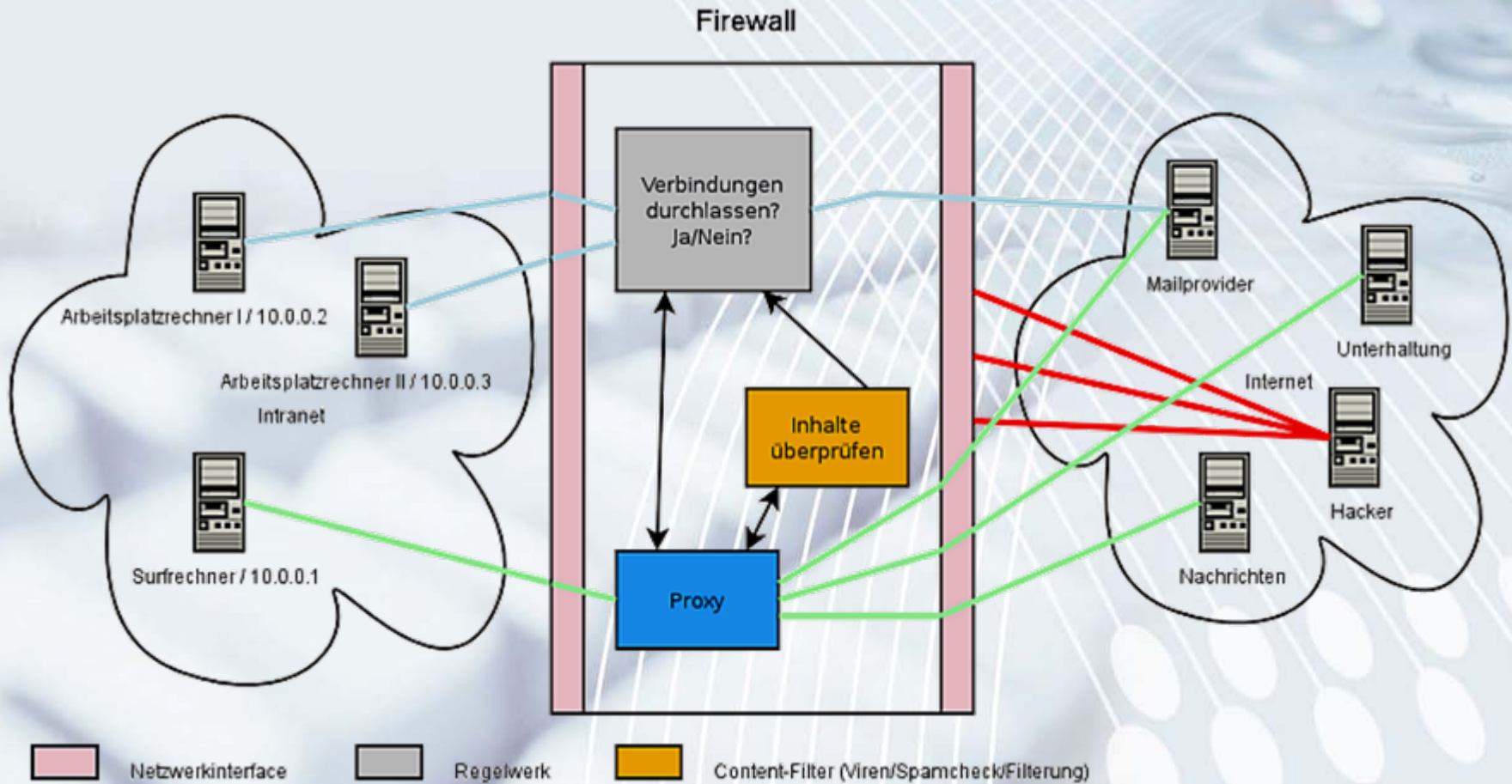


Bild-Quelle: http://de.wikipedia.org/wiki/Datei:Konzeptioneller_Aufbau_einer_Firewall.png

Interessante Unterstützung

■ <https://www.bsi-fuer-buerger.de/>



IT-Sicherheit

- Das Internet
- Der Browser
- Datensicherung
- Viren & andere Tiere
- Abzocker & Spione
- Infiziert - und nun?
- Schützen - aber wie?

Themen

- Kinderschutz
- Computerspiele
- Chat - aber sicher?
- Der Staat online
- Online-Banking
- Einkaufen im Internet
- WLAN
- Phishing
- Benutzerkonten / Netzwerk
- Handy
- Internettelefonie
- Suchmaschinen
- Open Source Software
- Recht im Internet

Aktuelles

- Newsletter
- Brennpunkt

Downloads

- Programme
- Bildschirmschoner
- Druckversion
- Linkbanner

Bußgelder bis zu **50.000,00 €** drohen in folgenden Fällen

- Auftragsdatenverarbeitungsauftrag falsch erteilt,
- Meldepflicht nach § 4 d BDSG nicht nachgekommen
- nicht rechtzeitige Bestellung eines DSB
- Widerspruchsrecht nicht , nicht richtig bzw. nicht rechtzeitig aufgeklärt
- Daten in elektronische oder gedruckte Adress-, Rufnummer-, Branchen- oder vergleichbare Verzeichnisse aufzunehmen, wenn bereits der entgegenstehende Wille ersichtlich ist.

Bußgelder bis zu **300.000,00 €** drohen in folgenden Fällen

- Wer personenbezogene Daten, die **nicht allgemein zugänglich sind, erhebt oder verarbeitet und dazu nicht befugt ist**
- oder befugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisiertem Verfahren **bereithält**
- oder entgegen dem Gesetz den Abschluss eines Vertrages von der **Einwilligung** des Betroffenen **abhängig macht**,
- **entgegen** dem ausdrücklichen **Willen** des Betroffenen, dass seine Daten nicht für Zwecke und Werbung und/oder der Markt- und Meinungsforschung verwendet werden, dennoch verwendet
- oder bei einer sogenannten „**Datenpanne**“, dazu **sogleich später, eine Mitteilung** nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.

Vielen Dank!
Jetzt ist noch Zeit für
Fragen
Anregungen
Kritik.

Kundenorientierung

Komplettangebot

Kompetenz

comTeam
SYSTEMHAUS-VERBUND

- VERSTEHEN
- PLANEN
- UMSETZEN

KNOW HOW

Effizienz

Sicherheit

Kundennähe