

# CHSH

Cerha Hempel Spiegelfeld Hlawati

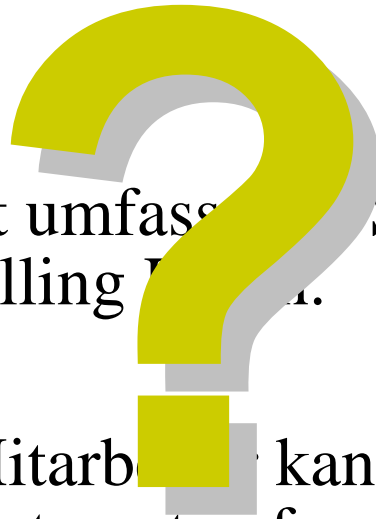
---



Zugriffskontrolle &  
Archivierung

## Zugriffsbeispiele

- Der Mitarbeiter aus dem Einkauf hat Einsicht in alle HR relevanten Daten.
- Der Praktikant hat umfassende Schreib- und Löschrechte an relevanten Controlling Daten.
- Der gekündigte Mitarbeiter kann nach Ausscheiden von daheim über das Internet auf unternehmensinterne Daten zugreifen.



## Zugriffskontrolle

*§ 14 Z 5 DSG verlangt:*

*„...die **Zugriffsberechtigung** auf Daten und Programme zu **regeln** und **Schutz der Datenträger** vor der **Einsicht** und **Verwendung durch Unbefugte**“*

→ Zugriffskontrolle durch Vergabe von Zugriffsberechtigungen

## Ziel der Zugriffskontrolle

- **Vertraulichkeit**  
nur Berechtigte sollen Kenntnis vom Inhalt erlangen
- **Verfügbarkeit**  
Berechtigten sollen die Daten nach Identifikation zur Verfügung stehen
- **Integrität**  
Daten sollen vollständig und unverändert bleiben

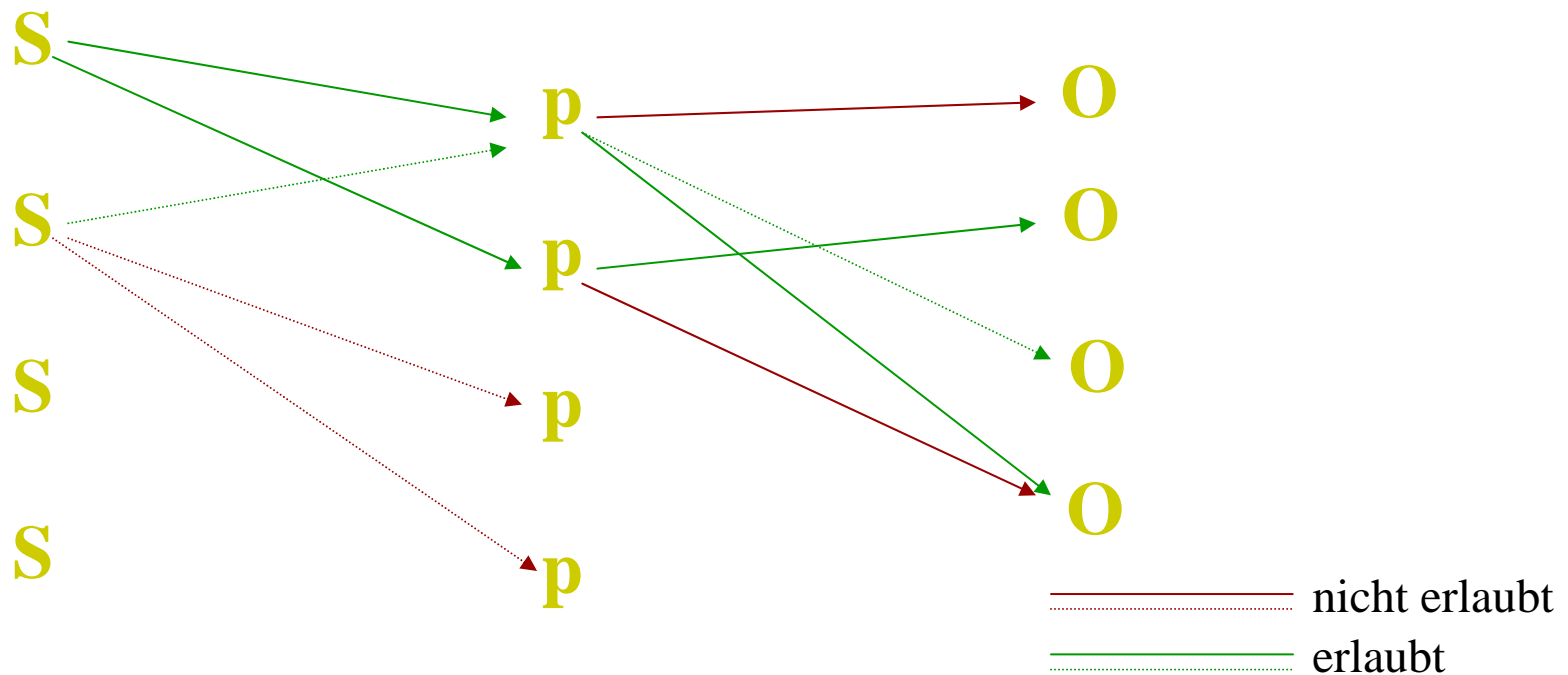
## Festlegung der Zugriffsberechtigung

Zugriffsberechtigungen festlegen durch Regelung

- welche Person → **S** (Subjekt)
- auf welche Daten → **O** (Objekt)
- in welchem Ausmaß → **p** (Operator)

Zugriff hat.

## Festlegung der Zugriffsberechtigung



## Mögliche Maßnahmen

- **technisch**

Festlegung von Passwörtern, Verschlüsselungen, biometrische Verfahren

- **organisatorisch**

umfassende User-Verwaltung, regelmäßiger Wechsel von Passwörtern, Festlegung von Richtlinien - technische Weitergabe zwar möglich aber verboten!! Zugriffsbeendigung bei Ausscheiden des Mitarbeiters

- **personell**

Zuständigkeitsfestlegung für Mitarbeiter, Handhabe gegen unbefugten Zugriff

## Protokollierung

Steht in engem Zusammenhang mit der Zugriffskontrolle:

§ 14 Z 7 DSG - Verpflichtung:

*„Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können.“*

## Protokollierung

Von Protokollierung spricht man dann wenn mindestens:

- der Zeitpunkt des Zugriffs
- die ausgeführte Handlung (Löschen, Verändern, etc.) und
- die Identität des Handelnden

aufgezeichnet werden

## Ziel der Protokollierung

- Überprüfbarkeit der datenschutzrechtlichen Zulässigkeit von Änderungen, Abfragen oder Übermittlungen
- Kontrolle der Datensicherheit (Auffinden von Sicherheitslücken und evtl. Anpassung des Systems)
- Sicherstellung des ordnungsgemäßen Betriebes
- Wahrung der Rechte von Betroffenen



**NICHT: Kontrolle der Zugreifenden und Betroffenen** aus anderen Gründen  
(Ausnahmen im strafrechtlichen Bereich)

## Aufbewahrungsdauer

- Protokolldaten - **drei Jahre**
- außer: betroffene Datenbestand wird zulässigerweise früher gelöscht oder länger aufbewahrt.
  - Protokolldaten folgen dem Schicksal ihres zugrundeliegenden Datenbestandes

## Archivierungspflichten



## Archivierungspflichten nach UGB

- § 212 : Bücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse samt den Lageberichten, Konzernabschlüsse samt den Konzernlageberichten, empfangene Geschäftsbriefe, Abschriften der abgesendeten Geschäftsbriefe und Belege für Buchungen sind **sieben Jahre** lang aufzubewahren;
- **Verlängerte Aufbewahrungsfrist:** darüber hinaus noch solange, als sie für ein anhängiges gerichtliches oder behördliches Verfahren, in dem der Unternehmer Parteistellung hat, von Bedeutung sind.

## Archivierungspflichten nach UGB

Bei elektronischer Archivierung ist insbesondere zu beachten (§ 190):

- Nachweis der vollständigen, richtigen, zeitlich geordneten und zeitgerechten Erfassung
- Das Veränderungsverbot
- Jederzeitige inhaltsgleiche, vollständige, geordnete und urschriftgetreue Wiedergabe
- Nachvollziehbarkeit der Veränderungen (Historie)

## Steuerrechtliche Archivierungspflichten

- § 132 Bücher und Aufzeichnungen, Belege, Geschäftspapiere und sonstige Unterlagen für die Abgabenerhebung von Bedeutung sind: **sieben Jahre** aufzubewahren;
- **Länger:** darüber hinaus sind sie noch so lange aufzubewahren, als sie für die Abgabenerhebung betreffende anhängige Verfahren von Bedeutung sind, in denen diejenige Parteistellung haben.

## Steuerrechtliche Archivierungspflichten

Zulässigkeit der Archivierung auf Datenträgern wenn:

- vollständige, geordnete, inhaltsgleiche und urschriftgetreue Wiedergabe bis zum Ablauf der gesetzlichen Aufbewahrungsfrist jederzeit gewährleistet ist
- auf eigene Kosten innerhalb angemessener Frist notwendige Hilfsmittel zur Verfügung gestellt werden um Unterlagen lesbar zu machen

## Weitere Archivierungsvorgaben

- § 18 UStG: Unterlagen die Grundstücke betreffen sind mind. **12 Jahre** aufbewahrungspflichtig; bei tw. privater Nutzung: **22 Jahre**
- Weiter sondergetzliche Bestimmungen (AZG, AMG, ÄrzteG, PrR-G, etc.)
- **Sorbanes-Oxley Act (SOX)** für US-börsennotierte Unternehmen
- Archivierung im Eigeninteresse – für Vorlage in Prozessen, Gebrauch im täglichen Geschäftsalltag

Vielen Dank für Ihre Aufmerksamkeit!

**Kontakt:**

Mag. Claudia Bernhard


Tel.: + 43/1 514 35 – 191

[claudia.bernhard@chsh.com](mailto:claudia.bernhard@chsh.com)

# CHSH

Cerha Hempel Spiegelfeld Hlawati

---

A close-up photograph of a fountain pen nib, likely gold or brass, touching a surface of water. The nib is positioned diagonally from the upper right towards the center. The point of contact has just created a series of concentric ripples that spread outwards. The background is dark and out of focus, with some light-colored, misty or smoke-like patterns. The overall mood is elegant and precise.

## Datenmissbrauch - Arbeitsrechtliche Konsequenzen

Mag. Barbara Klinger

30.09.2010

## Datengeheimnis im Arbeitsverhältnis

§ 15 Abs 1 DSGVO lautet:

*Auftraggeber, Dienstleister und ihre Mitarbeiter - Arbeitnehmer und Personen in einem arbeitnehmerähnlichen Verhältnis - haben Daten aus Datenanwendungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen Daten besteht (Datengeheimnis).*

## Datengeheimnis im Arbeitsverhältnis

§ 15 Abs 2 DSGVO lautet:

*„Mitarbeiter dürfen Daten nur auf Grund einer ausdrücklichen Anordnung ihres Arbeitgebers übermitteln. Auftraggeber und Dienstleister haben, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, diese vertraglich zu verpflichten, dass sie Daten aus Datenanwendungen nur auf Grund von Anordnungen übermitteln und das Datengeheimnis auch nach Beendigung des Arbeitsverhältnisses zum Auftraggeber oder Dienstleister einhalten werden“.*

## Fälle von Datenmissbrauch

- Arbeitnehmer missachtet Weisung/Vorschrift des Arbeitgebers aus
  - Betriebsvereinbarung (gemäß § 97 Abs 1 Z 6 ArbVG)
  - Richtlinie
  - Dienstvertrag
  - Schulungund schädigt damit das System bzw fängt Virus ein
- Arbeitnehmer entwendet oder löscht Daten des Unternehmens
- Arbeitnehmer verwendet Daten des Unternehmens oder das System missbräuchlich

## Prävention durch den Arbeitgeber

- Vorschriften in
  - Einzelarbeitsvertrag
  - Betriebsvereinbarung
  - Richtliniepräzise und verständlich gestalten
- Sensibilisierung durch Schulungen
- Durchgreifen bei Missbrauch/arbeitsrechtliche Konsequenzen

## Konsequenzen bei Datenmissbrauch

- Verwarnung (mündlich/schriftlich)
- Beendigung des Arbeitsverhältnisses:
  - Ordentliche Kündigung (mit sofortiger Dienstfreistellung)
  - fristlose Entlassung
  - Einvernehmliche Auflösung

## Kündigung

- Einhaltung von Kündigungsfristen und –terminen
  - Sonderfall befristetes Dienstverhältnis
- Angabe eines Kündigungsgrundes nicht erforderlich
- Betriebliches Vorverfahren unter Einbindung des Betriebsrates vor Ausspruch der Kündigung
- Kosten einer Kündigung (Abfertigung alt, Urlaubersatz)
- Arbeitsverhältnis endet erst mit Ablauf der Kündigungsfrist
- Möglichkeit der sofortigen Dienstfreistellung und Zugangssperre unter fortlaufender Entgeltzahlung

## Risiken einer Kündigung

- Anfechtung des Mitarbeiters der Kündigung vor dem Arbeits- und Sozialgericht
  - wegen verpönten Kündigungsmotiv
  - wegen Sozialwidrigkeit (wenn der Mitarbeiter seit mind. 6 Monaten im Unternehmen ist)
- bei erfolgreicher Anfechtung des Mitarbeiters Entgeltnachzahlung und Rückkehr an den Arbeitsplatz

## Kündigungsanfechtungsverfahren

- Im Verfahren hat der Arbeitgeber den Kündigungsgrund darzulegen
- Datenmissbrauch ist ein persönlicher Kündigungsgrund gemäß § 105 Abs 3 Z 2 lit a ArbVG:
  - *„Die Kündigung ist durch Umstände begründet, die in der Person des Arbeitnehmers gelegen sind und die betrieblichen Interessen nachteilig berühren.“*

## Entlassung

- Fristlose Entlassung immer unverzüglich aussprechen – sonst ist Entlassungsgrund verwirkt
- Betriebliches Vorverfahren unter Einbindung des Betriebsrates erst nach Ausspruch der Entlassung
- Arbeitsverhältnis endet sofort
- Arbeitnehmer hat keine Ansprüche mehr aus dem Arbeitsverhältnis
- Entlassungsgrund der Untreue bzw. des Vertrauensverlust gemäß § 27 Z 1 AngG

## Risiken einer Entlassung

- Entlassungsanfechtung des Mitarbeiters vor dem Arbeits- und Sozialgericht
- Bei erfolgreicher Anfechtung des Mitarbeiters Unwirksamkeit der Entlassung unwirksam, Entgelt nachzahlung und Rückkehr an den Arbeitsplatz

## Beispiele aus der Judikatur 1

- Das Gericht bestätigt die Entlassung eines Angestellten nach § 27 Z 1 AngG wegen Vertrauensunwürdigkeit, weil dieser entgegen der Anweisung des Vorgesetzten eine privat auf den Dienstrechner überspielte Datei gelöscht hatte. Die Datei enthielt ein während der Arbeitszeit verfasstes privates Dokument des Arbeitnehmers (OGH, Urteil 25.10.2001, 8 Ob A 218/01v). Der Arbeitnehmer hatte sich dabei nicht nur der Weisung widersetzt, während seiner Arbeitszeit auf dem PC keine Privatarbeiten zu verrichten, sondern auch der Anweisungen, die der Kontrolle und Verhinderung solcher Aktivitäten diene.

## Beispiele aus der Judikatur 2

- Kein Verrat eines Betriebs- oder Geschäftsgeheimnisses durch vom Dienstnehmer erstellte Seminararbeit. Es liegt auch keine grobe Pflichtverletzung iSd § 27 Z 1 AngG bei bloß geringfügiger Privatnutzung des PC vor. (OLG Wien, Urteil vom 17.3.1999, 7 Ra 45/99k).
- Entlassung wegen Erledigung privater Korrespondenzen auf Computer des Arbeitgebers in Dienstzeit und grobe Beleidigung des Arbeitgebers nach Wegnahme der privaten Diskette und erfolgter Dienstfreistellung (OLG Wien, Urteil vom 17.12.1999, 9 Ra 280/99h).

## Beispiele aus der Judikatur 3

- Das Überspielen fremder Daten auf einen eigenen Datenträger des Arbeitnehmers, rechtfertigt die Entlassung gemäß § 27 Z 1 letzter Fall AngG, da das arbeitsvertragswidrige und schuldhafte Kopieren auf nahezu gleicher Stufe mit der rechtswidrigen und schuldhaften Entwendung einer Sache steht ( OLG Wien 28. 11. 2001, 9 Ra 349/01m).
- Die Entlassung ist gerechtfertigt, wenn der Arbeitnehmer Privatsoftware auf Unternehmens PC installiert, da auch ohne Schädigungsabsicht und ohne Gefahr von "Viren"-Import die Befürchtung objektiviert wird, dass der Dienstnehmer seine Pflichten nicht gehörig erfüllen wird (OGH 5. 11. 1997, 9 Ob A 315/97g).

# CHSH

Cerha Hempel Spiegelfeld Hlawati

---

Vielen Dank für Ihre Aufmerksamkeit!



# CHSH

Cerha Hempel Spiegelfeld Hlawati

---

## Datenverlust und Meldepflichten

Hans Kristoferitsch

A close-up photograph of a fountain pen nib, likely made of gold, just touching the surface of water. The contact point creates a series of concentric ripples that spread outwards. A plume of white steam or smoke rises from the point of contact, suggesting the water is very hot. The background is dark, making the pen and the water's surface the central focus.

# CHSH

Cerha Hempel Spiegelfeld Hlawati

---

**wochenblatt**

Die Zeitung für alle

**Skandal bei GEZ-Fahndern: Daten lagen auf der Straße**

**DER TAGESSPIEGEL**



*Das Geld in Liechtenstein*

**Neue Steuer-CD aufgetaucht**

**SPIEGEL ONLINE**

**1,6 Millionen Daten bei SchülerVZ  
abgegriffen**

**WELT ONLINE**

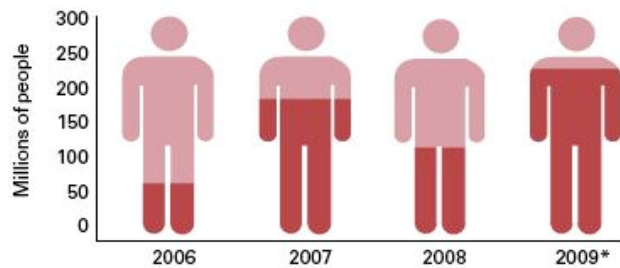
**Schlecker-Kundendaten kursierten im Internet**

## Aktuelle Fälle

- Deutsche Bundesländer kaufen CDs mit Daten deutscher Steuerbetrüger in der Schweiz und Liechtenstein.
- MTV Networks: Der Sender informierte 5000 Mitarbeiter, dass ihre persönlichen Daten teilweise mit Gehaltsangaben aus dem Firmen-Netzwerk gestohlen wurde.
- Hannaford Brothers: Datendiebe entwendeten 4,2 Millionen Kreditkarten-Nummern aus dem System der Supermarkt-Kette in New England, USA.
- Royal Navy: Einem britischen Offizier wurde der Laptop mit persönlichen Daten von 600.000 Armee-Angehörigen und -Bewerbern gestohlen.
- Britische Krankenkassen: mehrere 100.000 Datensätze mit Sozialversicherungsnummern und persönlicher Krankengeschichte in den Health Centern gehen verloren.
- Großbritannien: Vertrauliche Daten von drei Millionen Führerschein-Anwärtern gingen verloren. Ein Outsourcing-Unternehmen aus den USA war dafür verantwortlich.

## Datenverlust in Zahlen

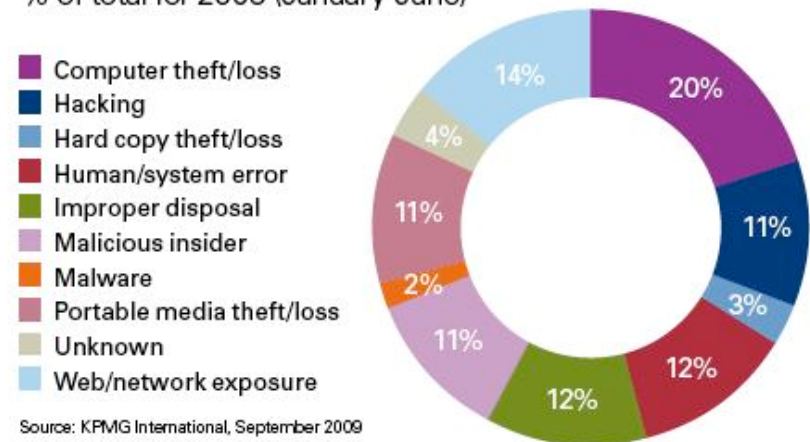
Number of people affected over the years



\*Estimate based on figures for January-June 2009 (110m affected)  
Source: KPMG International, September 2009

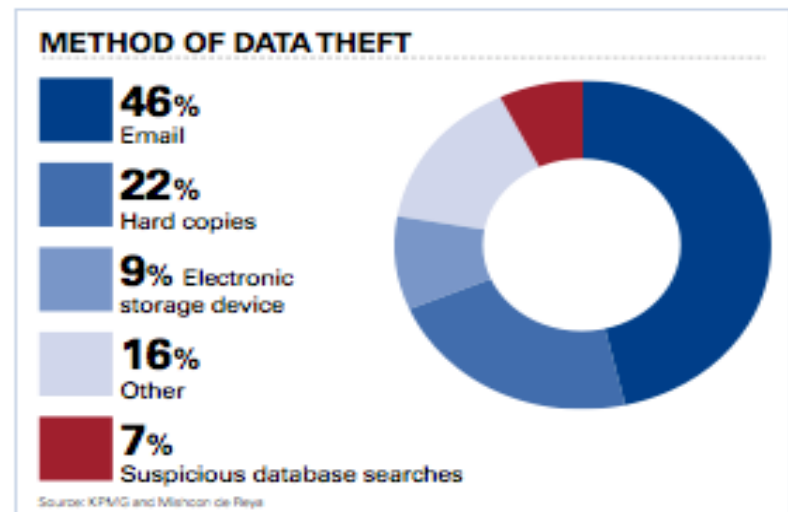
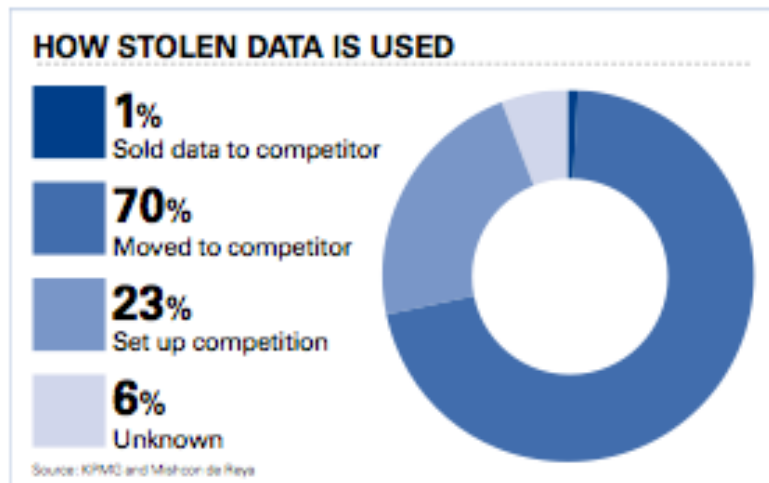
...die Mehrheit der Fälle wird aber gar nicht publik...

Cause of data loss: number of incidents as % of total for 2009 (January-June)



Source: KPMG International, September 2009

## Datendiebstahl in Zahlen



## Meldepflicht bei Datenverlust / Data Breach Notification

- Stammt aus den USA (in mehr als 30 Bundesstaaten eingeführt).
- In Europa bislang nur in Deutschland umgesetzt.
- Entwurf zur EU-Datenschutzrichtlinie für elektronische Kommunikation (2009/136/EG) sieht ebenfalls data breach notification vor.
- Mit DSGVO-Novelle 2010 nunmehr auch in Österreich eingeführt.

## § 24 Abs 2a DSGVO (DSG-Novelle 2010)

*„Wird dem Auftraggeber bekannt, dass Daten aus einer seiner Datenanwendungen systematisch und schwerwiegend unrechtmäßig verwendet wurden und dem Betroffenen Schaden droht, hat er darüber unverzüglich die Betroffenen in geeigneter Form zu informieren. Diese Verpflichtung besteht nicht, wenn die Information angesichts der Drohung eines nur geringfügigen Schadens der Betroffenen einerseits oder der Kosten der Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordert.“*

## Elemente (1)

- „Daten“ – vgl. Definition § 4 Z 1 DSGVO
  - ⇒ keine Informationspflicht bei
    - anonymisierten Daten
    - nicht-personenbezogenen Daten
    - verschlüsselten Daten

## Elemente (2)

- „wird dem Auftraggeber bekannt“
  - ⇒ keine Informationspflicht, falls Hacking-Attacke unbemerkt bleibt;
  - ⇒ keine Informationspflicht, falls Hacking-Attacke bemerkt wird, nicht aber, ob und welche Daten von der Attacke betroffen waren;
  - ⇒ keine Informationspflicht, falls Dienstleister betroffen und Auftraggeber keine Kenntnis erlangt?
- „aus einer Datenanwendung“
  - ⇒ keine Informationspflicht bei Phishing (vgl. Literatur)?

## Elemente (3)

- „systematisch und schwerwiegend“
  - ⇒ sehr unbestimmte Gesetzesbegriffe;
  - ⇒ keine Informationspflicht bei bloß zufälligem, einmaligem und punktuellen Datenverlust?
  - ⇒ keine Informationspflicht bei nur wenigen Betroffenen?
- „verwendet wurden“
  - ⇒ keine Informationspflicht (laut Literatur) bei fahrlässigem Datenverlust, außer es muss mit Datenmissbrauch gerechnet werden?

## Ausnahmen von der Informationspflicht

- „geringfügiger Schaden“:
  - ⇒ sehr vage
  - ⇒ Was ist ein geringfügiger Schaden?
- „unverhältnismäßiger Aufwand“:
  - ⇒ sehr vage
  - ⇒ Was ist ein unverhältnismäßiger Aufwand?
- Standardanwendungen (§ 24 Abs 4 DSGVO)?
  - ⇒ wohl vom Gesetzgeber nicht gewollt;

## Rechtsfolgen

- Informationspflicht (über alle zur Vermeidung von Vermögensschäden relevanten Aspekte) „in geeigneter Form“;
- keine Pflicht zur Verständigung der DSK;
- Verwaltungsstrafen bis zu EUR 10.000,00 (§ 52 Abs 2 Z 4 DSG);
- bereits Versuch ist strafbar (§ 52 Abs 3 DSG);
- Verfall von Datenträgern und Programmen (§ 52 Abs 4 DSG);
- zivilrechtliche Folgen:
  - § 24 (2) DSG als Schutzgesetz; aber: wohl meistens kein Schaden nachweisbar;
  - Verständigungspflicht als Ausfluss nebenvertraglicher Schutz- und Sorgfaltspflichten und der Schadensminderungspflicht;
  - Risiko von UWG-Klagen;

## Analyse

- wohl nur wenige Fälle;
- viele vage Begriffe – Konkretisierung durch Entscheidungspraxis bleibt abzuwarten;
- Hauptrelevanz wohl „Reflexwirkungen“ im Zivilrecht;

## Vielen Dank für Ihre Aufmerksamkeit!



**Kontakt:**

**Dr. Hans Kristoferitsch**

Tel. +43/1/514 35-291

[hans.kristoferitsch@chsh.com](mailto:hans.kristoferitsch@chsh.com)

**CHSH Vienna**

**Cerha Hempel Spiegelfeld**

**Hlawati**

Parkring 2

A-1010 Wien

telephone: +43/1/514 35 0

fax: +43/1/514 35 35

e-mail: [office@chsh.com](mailto:office@chsh.com)

# CHSH

Cerha Hempel Spiegelfeld Hlawati

---



## Datensicherheitsmaßnahmen

Karin Lehner  
Stefan Panholzer

## Datenschutz vs. Datensicherheit

- „*Datenschutz*“ = den Schutz des Betroffenen vor der unrechtmäßigen Verwendung seiner Daten
- „*Datensicherheit*“ die Sicherung der Datenbestände und des Datenverarbeitungsbetriebs gegen Preisgabe, Verfälschung, Unterbrechung und Verlust aller **„unternehmenswerten Informationen“**

## Risiken & Bedrohungen



Unauthorisierter Zugriff

Missbrauch durch IT-Personal

Verlust mobiler Geräte

Angriffe von Außen & Innen

Ausfall von IT-Systemen

Ändern von Daten

Änderung Sicherheitseinstellungen

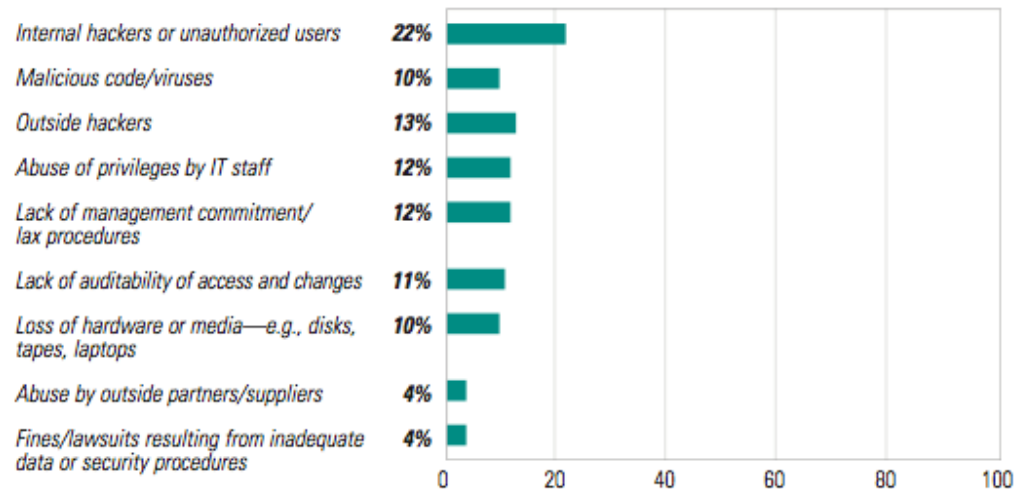
## Risiken & Bedrohungen in Zahlen...

- Diebstahl oder Verlust eines Computers 20 %
- Netzwerke und das Internet 14 %
- menschliches Verhalten 12 %
- unsachgemäße Entsorgung 12 %
- Hacker 11 %
- kriminelle Insider 11 %

Quelle: KPMG, Data Loss Barometer, 1 Hj. 2009

**Figure 20: Greatest Risks, Threats, Vulnerabilities**

*(Respondents rating vulnerability as "high")*



Quelle: Data Security Survey, UnisphereResearch, September 2010

## IT-Compliance – nur ein Modewort?

- Aufgabe der Geschäftsleitung
  - Informationssicherheit
  - IT-Sicherheit
  - Physikalische Sicherheit
- Vielzahl von regulativen Anforderungen
- Einführung eines „Sicherheitsmanagements“



Schutz der Daten vor zufälliger oder unrechtmäßiger Zerstörung

Schutz der Daten vor Verlust

ordnungsgemäße Verwendung von Daten

Kein Zugriff auf Daten durch Unbefugte


→ **Mindestanforderungen nach § 14 DSGVO**

## Datensicherheit

§ 14 Abs 1 DSGVO sieht vor, dass

**... für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden, entsprechende Maßnahmen zur Gewährleistung der Datensicherheit zu treffen sind.**

## Gesetzlicher „Pflichtenkatalog“ (§ 14 DSGVO)

- Funktionstrennung
  - Auftragsprinzip
  - Schulungspflicht
  - Zutrittskontrolle
- 
- Zugriffsbeschränkung
  - Betriebsbeschränkung
  - Protokollierung
  - Dokumentation

## Bedarfsanalyse

- Welche Anforderungen bestehen im Unternehmen?  
(Risikoanalyse)
- Verhältnismäßigkeitsabwägung:
  - Art der verwendeten Daten
  - Umfang und Zweck der Verwendung
  - Stand der technischen Möglichkeiten
  - wirtschaftliche Vertretbarkeit

## Warum Security-Audits

- 1: Absicherung der eigenen Verantwortung  
(IT-Leiter, GF, Vorstand)
- 2: Kontrolle von Lieferanten und Dienstleistern  
(Outsourcing RZ-Thema Linz)
- 3: Regelmäßige Kontrolle für rechtskonformes  
Security-Management

## Unterschiedliche Security-Audits

- Externes Security Audit - ablegen von verbotenen Daten
- WAS - Web Application Scan - hacking und shopthematik
- Internes Security Audit - conficker thema Batching
- WLAN Audit - home-user mit VPN und wlan
- Social Engineering - usb-stick

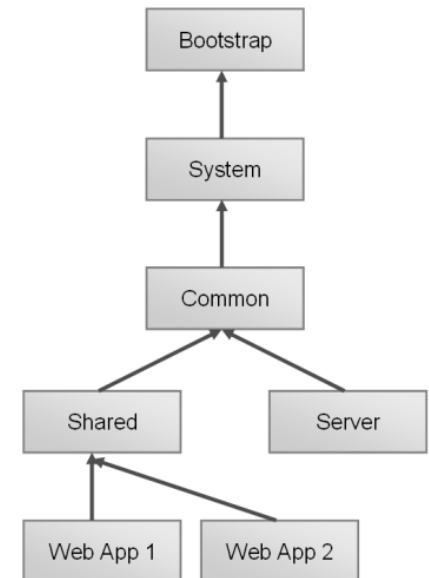
## Externes Security Audit

- 1.1 Informationssammlung (Öffentliche IP Adressbereiche, Standorte, Webauftritte, Mailkommunikation, B2B Partner- und Lieferantenzugänge, Onlineportale usw.)
- 1.2 Scan der Adressbereiche welche über die Informationssammlung gefunden wurden und in die Permission to Attack übergeben wurden.
- 1.3 Auswertung der identifizierten Dienste
- 1.4 Manuelle Überprüfung der gefundenen Dienste
- 1.5 Automatisierte Überprüfung dieser Dienste mittels Scansystemen mit aktuellen Vulnerability-Signaturen
- 1.6 Penetration Testing
- 1.7 PCI Payment Card Industry Scan
- 1.8 SANS Top 20 Vulnerability Scan



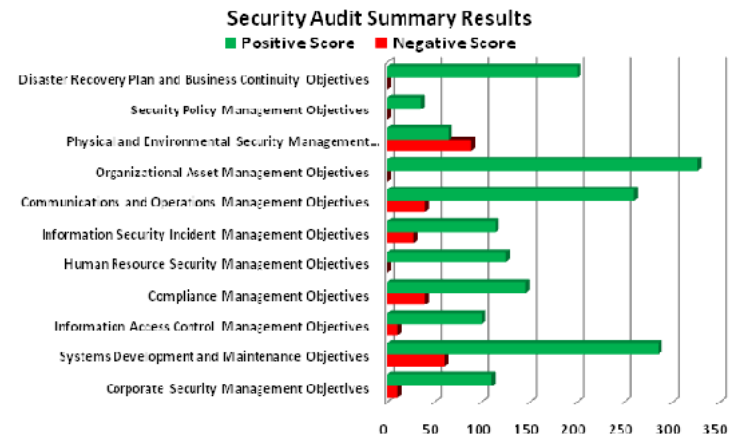
## WAS - Web Application Scan

- 2.1 Informationssammlung (Webservice und Webapplikation)
- 2.2 Testen des Webservers (OS, Patches, usw.)
- 2.3 Testen der Webapplikation auf Cross Site Scripting, Reflected Cross Site Scripting, SQL Injection, XML und XPath Injection
- 2.4 Cookie Diebstahl und Session Hopping
- 2.5 Password Brute Force (Minimal, Limited, Standard, Exhaustive oder Customer Settings)
- 2.6 Scan for Credit Card Numbers
- 2.7 Scan for Security Numbers  
(für Kunden mit Standorten in den US notwendig)



## Internes Security Audit

- 3.1 Vorbereitungsworkshop mit den verantwortlichen Personen der IT Security Abteilung
- 3.2 Netzwerküberprüfung (Zugriffskontrolle, 802.1x, usw.)
- 3.3 Interner Portscan unterschiedlicher Bereiche (Server, Client, MGMT, Außenstellen,..)
- 3.4 Detailanalyse der Serverbereiche
- 3.5 Stichprobenartige Analyse der Clientsysteme
- 3.6 Auswertung der gefundenen Dienste
- 3.7 Manuelle Überprüfung der identifizierten Dienste



## Internes Security Audit

- 3.8 Automatisierte Überprüfung dieser Dienste mittels Scansystemen mit aktuellen Vulnerability-Signaturen
- 3.9 Penetration Testing
- 3.10 Überprüfung AD Infrastruktur und Policykonfiguration
- 3.11 Überprüfung Firewall-Regelwerk (Cisco, Checkpoint, Fortinet, MS ISA)
- 3.12 Überprüfung Storagekonzept
- 3.13 Überprüfung Ausfallsicherheit
- 3.14 Überprüfung Backup und Restore
- 3.15 Überprüfung Netzwerkkomponenten (Topologie, Spanning-Tree,..)



## WLAN Audit

- 4.1 Security Audit über die eingesetzte WLAN Infrastruktur
- 4.2 Brute Force Angriffe auf die verschlüsselten Pakete
- 4.3 Überprüfung auf RAW Access Points
- 4.4 Konfigurationsüberprüfung von WLAN Controllern
- 4.5 WLAN Ausmessung über Reichweite und Überschneidung
- 4.6 Wardriving am Firmengelände



## Social Engineering

- 5.1 Informationssammlung und gezielte Vorbereitung
- 5.2 Überprüfung der Zugangskontrolle (Firmengelände, Firmenzutritt,...)
- 5.3 Auftreten als firmeninterne Person um zu Informationen zu gelangen
- 5.4 Auftreten als Person von externen Dienstleistern (Telekom, IT Dienstleister,...)
- 5.5 Wardialing
- 5.6 Verteilen von USB Sticks mit „spezieller Software“
- 5.7 Detaillierte Vorgehensweise nach Kundenwunsch



## Add ON's

- Audit-Report
- Management Report
- Automatisierte Audits
- Periodische Audits
- Qualis-Scan-Demoreport
- Mitarbeiter Sensibilisierung
- Security-Policy



## Wer ist verantwortlich?

- Verantwortung der Geschäftsführung
  - § 347 UGB - „Sorgfalt des ordentlichen Unternehmers“
  - § 6 DSG – “Einhaltung der Datenschutzgrundsätze”
  - § 9 VStG – “Einhaltung der Verwaltungsvorschriften”
- Einführung eines „Internen Kontrollsystems“
  - §§ 70, 82 AktG, § 22 GmbHG (§ 243a/243b UGB)
- Rechtsfolgen: Schadenersatz, Bußgelder, Reputationsverlust



DANKE FÜR IHRE  
AUFMERKSAMKEIT!

[karin.lehner@chsh.com](mailto:karin.lehner@chsh.com)  
[stefan.panholzer@s-db.at](mailto:stefan.panholzer@s-db.at)