KPMG
cutting through complexity™

Behandlung von Sicherheitsvorfällen und Beweisverwertung von gesicherten Daten

BSI Grundschutztag, Bremen, 13.6.2012

Barbara Scheben
Alexander Geschonneck

Sicherheitsvorfälle

- Unbewusste Offenlegung vertraulicher Daten
- Sicherheitslücken durch Hard- oder Softwarefehler
- Schadsoftware
- Dolose Handlungen, die zu Datendiebstahl führen
  - Von extern, z. B. Hacking (Bsp.: Kreditkartendaten)
  - Von intern, z. B. Verrat von Geschäfts- und Betriebsgeheimnissen durch Mitarbeiter
- Etc.

© 2012 KPMG AG Wirtschaftsprüfungsgesellschaft, a subsidiary of KPMG Europe LLP and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name, logo and "cutting through complexity" are registered trademarks of KPMG International Cooperative. Printed in Germany.

Ursachen

- Fehlkonfigurationen, Überberechtigungen
- Insuffizientes Berechtigungskonzept
- Ungesicherte Schnittstellen
- Unzureichende technische und organisatorische Maßnahmen bzgl. Hardware, Software, IT-Infrastruktur
- Unzureichende technische und organisatorische Maßnahmen im Hinblick auf Gebäude, Räume
- Etc.

© 2012 KPMG AG Wirtschaftsprüfungsgesellschaft, a subsidiary of KPMG Europe LLP and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name, logo and "cutting through complexity" are registered trademarks of KPMG International Cooperative. Printed in Germany.

Managementverantwortung

§ 91 Abs. 2 AktG: *„Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen frühzeitig erkannt werden“*

§ 93 Abs. 1 S. 1 AktG: *„Die Vorstandsmitglieder haben bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden.“*

§ 116 S. 1 AktG: *„Für die Sorgfaltspflicht und Verantwortlichkeit der Aufsichtsratsmitglieder gilt § 93 …“*

§ 43 Abs. 1 GmbHG: *“Die Geschäftsführer haben in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden.“*

§ 130 Abs. 1 und 3 OwiG: *„Wer als Inhaber eines Betriebes oder Unternehmens vorsätzlich oder fahrlässig die Aufsichtsmaßnahmen unterlässt, die erforderlich sind, um in dem Betrieb oder Unternehmen Zuwiderhandlungen gegen Pflichten zu verhindern, die den Inhaber treffen und deren Verletzung mit Strafe oder Geldbuße bedroht ist, handelt ordnungswidrig, wenn eine solche Zuwiderhandlung begangen wird, die durch gehörige Aufsicht verhindert oder wesentlich erschwert worden wäre.“*

© 2012 KPMG AG Wirtschaftsprüfungsgesellschaft, a subsidiary of KPMG Europe LLP and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name, logo and "cutting through complexity" are registered trademarks of KPMG International Cooperative. Printed in Germany.

Abzuleitende Maßnahmen

- Festlegung einer Soll-Vorgabe für IT-Infrastruktur, Sicherheitsniveau; Berechtigungskonzept, etc.
- Definition von Sicherheitsvorfällen, die abzuwenden oder zu minimieren sind
- Definition eines Prozesses und korrespondierender Zuständigkeiten für den Fall des Eintritts von Sicherheitsvorfällen
  - Zuständigkeiten definieren (Expertenteam, Eskalations- und Meldewege, Head of)
  - Prioritäten (Welche Sicherheitsvorfälle sind wie wesentlich: z. B. interne Überberechtigung im Bereich HR oder ungehinderter Zugriff auf wesentliche Geschäftsgeheimnisse wie Kundendaten)
  - Modus für Erkennung, Erfassung, Qualifizierung, Beweismittelsicherung, Reporting
  - Behebung/Wiederherstellung
  - Nachbereitung: Beweisverwertung und lessons learned
- Roll-out (Bekanntmachung, Schulungen, Updates, etc.)

© 2012 KPMG AG Wirtschaftsprüfungsgesellschaft, a subsidiary of KPMG Europe LLP and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name, logo and "cutting through complexity" are registered trademarks of KPMG International Cooperative. Printed in Germany.

Compliance-Framework

Compliance-Überwachung und Verbesserung

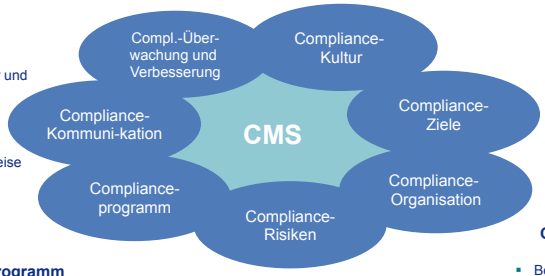
- Überwachung der Angemessenheit und Wirksamkeit
- Voraussetzung: ausreichende Dokumentation
- Berichterstattung von Schwachstellen und Verstößen
- Management trägt Verantwortung

Compliance-Kultur

- Bewusstsein für die Bedeutung von Regeln als Grundlage für die Angemessenheit und Wirksamkeit des CMS
- Wesentlicher Einflussfaktor: Grundeinstellung und Verhaltensweisen des Managements („Tone at the Top")

Compliance-Kommunikation

- Information betroffener Mitarbeiter und ggf. Dritter über das Compliance Programm sowie der Rollen/ Verantwortlichkeiten
- Festlegung der Berichtswege für Compliance-Risiken und für Hinweise auf Regelverstöße



Compliance-Ziele

- Festlegung wesentlicher zu erreichender CMS-Ziele auf Grundlage der allgemeinen Unternehmensziele
- Festlegung der relevanten Teilbereiche und der darin einzuhaltenden Regeln

Compliance-Organisation

- Bestimmung der Aufbau- und Ablauforganisation
- Festlegung von Rollen, Verant-wortlichkeiten und Berichtswegen
- Zur Verfügung stellen notwendiger Ressourcen

Compliance-Programm

- Einführung von Grundsätzen und Maßnahmen zur Begrenzung von Risiken und Vermeidung von Verstößen
- Dokumentation

Compliance-Risiken

- Identifikation wesentlicher Compliance-Risiken
- Einführung systematischer Verfahren zur Risikoerkennung und -berichterstattung

© 2012 KPMG AG Wirtschaftsprüfungsgesellschaft, a subsidiary of KPMG Europe LLP and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name, logo and "cutting through complexity" are registered trademarks of KPMG International Cooperative. Printed in Germany.

Auf dem Weg zur Beweisverwertung der gesicherten Daten
Besondere gesetzliche Vorgaben - BDSG

Personenbezogene Daten?

- Legaldefinition in § 3 Abs. 1 BDSG:
- „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person."
- Hierzu zählen:
  - Name, Alter, Geschlecht, Staatsangehörigkeit, Beruf, Beziehungen zu Dritten, soweit diese Daten auf eine bestimmte oder bestimmbare Person bezogen werden können.
  - Auch User-ID
  - Auch (dynamische) IP-Adressen werden teilweise als personenbezogene Daten angesehen
    (so etwa: AG Berlin-Mitte v. 27. März 2007 – 5 C 314/06).
  - Ebenfalls: In E-Mail-Logfiles enthaltene Daten (z.B. Absender, Empfänger, Betreff, Uhrzeit, etc.).

© 2012 KPMG AG Wirtschaftsprüfungsgesellschaft, a subsidiary of KPMG Europe LLP and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name, logo and "cutting through complexity" are registered trademarks of KPMG International Cooperative. Printed in Germany.

Grundsätze der Erhebung, Verarbeitung und Nutzung personenbezogener Daten

- Verbot mit Erlaubnisvorbehalt:
  - § 4 Abs. 1 BDSG:

    „Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat."
  - Folge:

    Erlaubnistatbestand oder Einwilligung des Betroffenen erforderlich

- Grundsatz der Datenvermeidung und Datensparsamkeit, § 3a BDSG
  - So wenig personenbezogene Daten wie möglich
  - Anonymisieren oder pseudonymisieren, wo nach Verwendungszweck möglich und kein unverhältnismäßiger Aufwand

- TKG vorrangig zu beachten

© 2012 KPMG AG Wirtschaftsprüfungsgesellschaft, a subsidiary of KPMG Europe LLP and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name, logo and "cutting through complexity" are registered trademarks of KPMG International Cooperative. Printed in Germany.

Erlaubnistatbestände im Hinblick auf Sicherheitsvorfälle
Bsp.: Sicherstellung eines ordnungsgemäßen Betriebs

§ 31 BDSG: Besondere Zweckbindung

"Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden."

Dieser Zweck muss bei Erhebung der Daten festgelegt werden, § 28 Abs. 1 S. 2 BDSG.

Demnach erlaubt, z. B. :

- Auswertung zur Mißbrauchsbekämpfung
- Eingabekontrolle
- Ermittlung unbefugter Datenverarbeitung
- Ermittlung von Systemschwächen

Demnach nicht erlaubt, z. B.:

- Nachträgliche Zweckänderung
- Verarbeitung zu Zwecken der Leistungskontrolle von AN
- Verfolgung allgemeiner Complianceziele, die nicht mit Datenschutz in Verbindung stehen

© 2012 KPMG AG Wirtschaftsprüfungsgesellschaft, a subsidiary of KPMG Europe LLP and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name, logo and "cutting through complexity" are registered trademarks of KPMG International Cooperative. Printed in Germany.

Erlaubnistatbestände im Hinblick auf Sicherheitsvorfälle
Bsp.: Dolose Handlungen

§ 32 BDSG

Abs.1 S. 1

"Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses (…) für dessen Durchführung oder Beendigung erforderlich ist."

Abs. 2 S.1:

"Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, (…) erforderlich ist (…)."

Demnach erlaubt, z. B.:

- Ggf. Maßnahmen zur Arbeitszeitkontrolle, wie z.B. elektronische Stempelkarten, etc., wenn keine weniger einschneidende Maßnahme sinnvoll durchführbar
- Aufdeckung eines konkreten Straftatverdachts z. B. Verrat von Geschäfts- und Betriebsgeheimnissen

Demnach nicht erlaubt, z. B.:

- Erstellung von Arbeitnehmerprofilen (BAG NZA 1986, 643)
- Umfassende Präventivüberwachung
- Leistungs- /Verhaltenskontrolle unter Missachtung der Mitbestimmung

© 2012 KPMG AG Wirtschaftsprüfungsgesellschaft, a subsidiary of KPMG Europe LLP and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name, logo and "cutting through complexity" are registered trademarks of KPMG International Cooperative. Printed in Germany.

Verwertbarkeit von gesicherten Daten im Rechtsstreit
1/3

- Beispiel: Verdacht des Informationsabflusses durch Mitarbeiter und/oder von außen
- Beweismittel: Richterlicher Augenschein, Urkunde, Sachverständiger, Zeuge, Parteivernehmung
- Einführung in den Prozess i.d.R. als Urkundsbeweis oder Inaugenscheinnahme; ggf. auch im Rahmen eines Sachverständigengutachtens
- Aussagegehalt z. T. begrenzt. Bsp.: Protokolldatei: I.d.R. nur Indiz / Anscheinsbeweis
- Herausforderung: Zweckbindung
- Zweckwidrige Verwendung i.d.R. zumindest Verstoß gegen Datenschutzrecht (Ausnahme ggf.: Festlegung mehrerer Zwecke vor Datenerhebung)
- Frage der Zulässigkeit der Verwertung als Beweismittel i. d. R. anhand einer Abwägung der betroffenen Rechtsgüter zu treffen
- Bei rechtmäßiger und zweckgerechter Verwendung regelmäßig kein Beweisverwertungsverbot

© 2012 KPMG AG Wirtschaftsprüfungsgesellschaft, a subsidiary of KPMG Europe LLP and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name, logo and "cutting through complexity" are registered trademarks of KPMG International Cooperative. Printed in Germany.

Verwertbarkeit von gesicherten Daten im Rechtsstreit
2/3

Datenerhebung rechtswidrig

- Führt regelmäßig zu Verwertungsverbot, wenn allgemeines Persönlichkeitsrecht gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verletzt (z. B. Umfassende Erstellung eines Nutzerprofils)
- Verletzung einfachgesetzlicher Datenschutzvorschriften stellt i.d.R. einen solchen Verstoß dar, ist aber im Einzelfall zu prüfen (Interessenabwägung, z.B. Umwidmung der zu Zwecken der Anlagensicherheit erstellten Protokolldateien)
- Möglicherweise aber verwertbar, wenn sich Partei in Notwehrlage gem. § 227 BGB befindet (z.B. zur Abwehr eines versuchten Prozessbetruges und Fehlen anderer Beweismittel; Interessenabwägung)

Datenerhebung rechtmäßig, aber Verarbeitung zweckwidrig

- Beweisverwertungsverbot i.d.R., wenn Verwertung durch das Gericht in grundrechtlich geschützte Positionen eingreift
- Wohl kein generelles Verwertungsverbot bei zweckwidriger Nutzung von Daten, solange nicht in Grundrechtsposition des Prozessgegners (AN) eingegriffen wird (BAG v. 13.12.2007 – 2 AZR 537/06 bei Verletzung von Zweckbestimmung in Betriebsvereinbarung)
- Stellt zweckwidrige Verwendung Verletzung von Datenschutzvorschriften dar (z.B. § 100 TKG), so kann dies auch zur Unverwertbarkeit führen (vgl. OLG Karlsruhe v. 4.12.2008 – 4 U 86/07)

Fernwirkung von Beweisverboten

- Grundsätzlich keine umfassende Fernwirkung von Beweisverwertungsverboten („Fruit-of the-poisonous-tree-doctrine“ in BRD nicht anwendbar)
- Möglich daher: Erlangung weiterer Beweismittel durch Auswertung von Protokollen (z.B.: Hinweise auf mögliche Zeugen, weitere Beweismittel)
- Nicht zulässig jedoch Ersetzung des verbotenen Beweismittels durch anderes Beweismittel (z.B.: Vernehmung eines Zeugen über den Inhalt der rechtswidrig erhobenen Protokolldatei) s. BVerfG NZA 2002, 284; OLG Karlsruhe v. 4.12.2008 – 4 U 86/07

© 2012 KPMG AG Wirtschaftsprüfungsgesellschaft, a subsidiary of KPMG Europe LLP and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name, logo and "cutting through complexity" are registered trademarks of KPMG International Cooperative. Printed in Germany.

Verwertbarkeit von gesicherten Daten im Rechtsstreit 3/3

Zivilprozess (ZPO)	Kündigungsschutzprozess (ArbGG)	Strafprozess (StPO)
• Keine ausdrückliche Regelung zu Beweisverwertungsverboten	• Keine ausdrückliche Regelung zu Beweisverwertungsverboten	• Diverse Vorschriften zu Beweisverwertungsverboten (z.B. § 136a StPO), aber keine spezielle Regelung bezüglich rechtswidrig erhobener / verwendeter (Protokoll)dateien
• Abwägung zwischen Rechtsverletzung des Betroffenem und Interesse der beweisbelasteten Partei	• Kein Verwertungsverbot, wenn nur allgemeines Persönlichkeitsrechts Dritter verletzt wird; Eingriff muss Rechte des Prozessgegners verletzen (Beispiel: Videoüberwachung im öffentlichen Raum -> zulässig gegenüber AN, obwohl unzulässig gegenüber Kunden)	• Bestimmte, möglicherweise rechtswidrig erlangte Beweismittel, verwertbar. Z. B. Verstoß gegen datenschutzrechtliche Formvorschriften.
• Verwertungsverbot wohl auch bei Eingriff in Grundrechte Dritter (vgl.: OLG Karlsruhe NJW 2000, 1577; OLG Karlsruhe v. 4.12.2008 – 4 U 86/07)	• Kein Verwertungsverbot bei Verletzung von Mitbestimmungsrechten (BAG v. 13.12.2007 = NJW 2008, 2732)	• Grundsätzlich auch hier: Abwägung der verletzten Individualinteressen und öffentlichem Interesse an Strafverfolgung (Merke: Je intimer die erhobenen Daten, umso eher führt dies zum Verwertungsverbot)
• Grundsatz der prozessualen Wahrheit: Rechtswidrig erlangte (Protokoll)daten dürfen nicht mit wahrheitswidrigem Tatsachenvortrag bestritten werden, Rechtsverletzung kann aber gerügt werden.	• Grundsatz der prozessualen Wahrheit	

© 2012 KPMG AG Wirtschaftsprüfungsgesellschaft, a subsidiary of KPMG Europe LLP and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name, logo and "cutting through complexity" are registered trademarks of KPMG International Cooperative. Printed in Germany.

Vielen Dank für Ihre Aufmerksamkeit

Kontakt:

Barbara Scheben
Rechtsanwältin

KPMG AG Wirtschaftsprüfungsgesellschaft
Forensic
T +49 69 958 737 37
M +49 174 307 89 70
bscheben@kpmg.com

Alexander Geschonneck
Partner

KPMG AG Wirtschaftsprüfungsgesellschaft
Forensic
T +49 30 2068 1520
M +49 174 3201475
ageschonneck@kpmg.com

© 2012 KPMG AG Wirtschaftsprüfungsgesellschaft, a subsidiary of KPMG Europe LLP and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name, logo and "cutting through complexity" are registered trademarks of KPMG International Cooperative. Printed in Germany.