Datenklau – Ein Risiko auch für mein Unternehmen

Secuware Deutschland GmbH
Jürgen Saamen
53111 Bonn
www.secuware.de

Agenda

1. Datenschutz im Unternehmen
2. Tägliche Anforderungen
3. Finanzielle Anforderungen
4. Konzepterstellung
5. Fragen

Datenschutz im Unternehmen

Beispiele

- Programm- und Geräteüberwachung
- Schulung der Mitarbeiter
- Personalaktenkontrolle
- Überwachung der Kundendaten, auch bei der Werbung
- Auskunftserteilung an Betroffene

Schutzgegenstand des BDSG

- § 1 BDSG

„Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem **Persönlichkeitsrecht** beeinträchtigt wird.“

=

Definition des Datenschutzes

Wessen Daten werden geschützt?

- jede natürliche oder juristische Person außerhalb des datenverarbeitenden Betriebs
- Mitarbeiter, seit 9/2009,§ 32 BDSG
- **Datenverarbeitung**
- **Gesetzliche Definition, § 3 II BDSG**
- „Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen“
- Begriffsbestimmungen in § 3 Abs. 3-5 BDSG

Grundsätze der Datenverarbeitung

- Datenvermeidung und Datensparsamkeit, § 3a BDSG
- Verhältnismäßigkeit
- Zweckbindung
- Vorrang anonymer oder pseudonymer Datenverarbeitung, Begriffsbestimmung in § 3 Abs. 6 und 6a BDSG
- Durchschaubarkeit der Datenverarbeitung
- Organisatorische und verfahrensrechtliche Absicherung

Tägliche Anforderungen

Das Daten-Problem

Daten sind allgegenwärtig und beweglich:

- Desktops und Laptops
- Computer-Festplatten
- Mobile Speichergeräte, wie CDs oder USB-Laufwerke
- Netzwerk-Ordner (Speicher) und Email

Risiko für Unternehmen und Mandanten:

- Datenverlust und die damit verbundenen Aufwendungen



Unsichere Daten machen Ihr Geschäft unsicher


Security
Forrester Loses Laptop Containing Personnel Data
Home > News > Fidelity: Employee stole, sold 2.3 million consumer records
Fidelity: Employee stole, sold 2.3 million consumer r
Jim Carr
JUMP TO More Resources
Home
News
Newsfeeds/XML
Knowledge Centers
Business
COMPUTERWORLD
Security
Wells Fargo Loses Compute
Data -- Again
Incident is
c|net NEWS.com
Today on CNET
News
Reviews
Compare prices
Today on News | Business Tech | Cutting Edge | Access | Threats | Media 2.0
Search:
Veterans' data swiped in th
By Greg Sandoval
Staff Writer, CNET News.com
Published: May 22, 2006, 2:50 PM PDT
TalkBack
abc NEWS
start here
Home | News Brief | World | U.S. | Investigative | Politics | Money |
Good Morning America | World
Wednesday, January 09, 2008
Register | Sign In
Technology & Science
Home > Technology & Science
Disk With Ohio State W
Disk With Personal Data on All
COLUMBU
Stolen
GCN
Government Computer News
Search GCN
Advanced Search
Monday January 7, 2008 | Upc
GCN Hot Topics:
Tech/Products Home
Authentication/ID Mgt.
Hardware
Homeland Security
IPv6
IT Mgt.
Content/Rec
State & Loca
GCN Home > 11/21/07 web stories
U.K. rocked by loss of 25m records
By Joab Jackson
Story Tools: Print this | Email this | Purchase a Reprint | Link to this page
U.S. agency officials stung by data loss can take some solace
struggling with data security issues. A
Customs department
USA TODAY
Home
News
Travel
Money
Sports
Life
Money
Markets
Economy
Company News
Media
Cars
Managing Your Mo
GET A QUOTE:
Enter symbol(s) or Keywords
GO
DJIA 13,432.77
-294.26
NASDA
Gap loses laptop with 800,000 job se
data
Posted 74d ago | Comments 29 | Recommend 15
(GPS) said Friday that a laptop comp
was stolen from

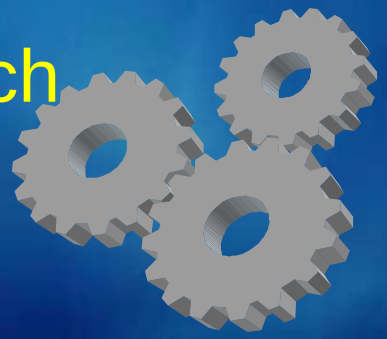
Datenklau Bonner Unternehmertag 2010

Prozess um Datendiebstahl vor Bonner Arbeitsgericht
Von Benjamin Jeschor
(Auszug)
Bonn. Vor dem Bonner Amtsgericht muss sich demnächst ein 34-Jähriger verantworten, weil er Geschäfts- und Betriebsgeheimnisse verraten und gegen das Bundesdatenschutzgesetz verstoßen haben soll.
…….

….. zwischen März und Juli 2009 insgesamt ***143 000 Datensätze*** von (FIRMEN) -Kunden auf seinem privaten Netbook zu speichern. Laut Anklage hatte der Beschuldigte zwei Komplizen, die neben ihm auf der Anklagebank sitzen werden. Auch den 36 und 37 Jahre alten Männern wird vorgeworfen, gegen das Datenschutzgesetz verstoßen und Beihilfe zum Geheimnisverrat geleistet zu haben …..
Das Unternehmen erstattete Anzeige, die Staatsanwaltschaft ermittelte die Verdächtigen. Bei dem 37-Jährigen wurden Daten gefunden, die eindeutig der FIRMA zugeordnet werden konnten. Über die Höhe der Bezahlung des Datenlieferanten hatten die Beteiligten offenbar noch keine Vereinbarung getroffen.
Artikel BONNER GENERALANZEIGER vom 24.09.2010

Angriffsvektoren

Wirtschafts- und damit Computerkriminalität ist eine absolut blühende Branche. Laut einer Untersuchung im Auftrag der Euler Hermes Kreditversicherung haben nicht weniger als 86 Prozent aller deutschen Unternehmen Probleme mit Wirtschaftskriminalität. Der gesamtwirtschaftliche Schaden beläuft sich auf über 100 Milliarden (!) Euro.



Angriffsvektor Mitarbeiter

Warum mein Unternehmen ?
"Hauptursache für Wirtschaftskriminalität ist der immer härter werdende Konkurrenzkampf der Unternehmen"

In der Folge wurde nach immer neuen Wegen gesucht, an unternehmensrelevante und -entscheidende Daten des Wettbewerbers zu kommen.

Angriffsvektor (2)

Wer kommt als Täter in Frage und wie geht er vor?

Eigene Mitarbeiter

Malware, zunehmend maßgeschneidert

- **Botnetze, Webangriffe, soziale Angriffe**

Kleine Wirtschaftsspionage

- **Mitbewerber, Hacker, kriminelle Banden**

Große Wirtschaftsspionage

- **Fremde Nationen, hier China.**

Angriffsvektor Mitarbeiter

Menschen mit existenziellen Problemen

Menschen mit dem Wunsch sich beruflich beim Mitbewerber zu verbessern.

Der einfache Wunsch Geld zu verdienen

Kein Unrechtsbewusstsein, illoyal

Angriffsvektor Mitarbeiter

Anhang 1: Aktuelle Bedrohungslage / Beispiel Passwort

Studie mit IT-Mitarbeitern: „Welche Information würden Sie entwenden?“

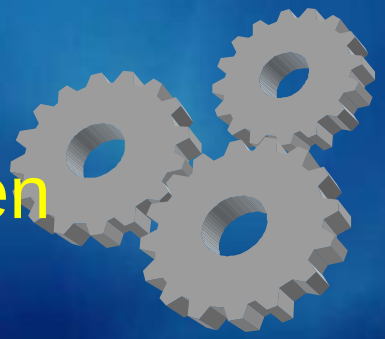
Art der Information	2008	2009
Kundendatenbanken	35 %	47 %
Admin-Accounts für E-Mail-Server	13 %	47 %
M&A-Pläne	7 %	46 %
R&D-Informationen	13 %	46 %
CEO-Passwörter	11 %	46 %
Finanzpläne	11 %	46 %
Privilegierte Passwörter	31 %	42 %

Quelle: Cyber-Ark „2009 Trust, Security Passwords Survey Research Brief“ 10. Juni 2009

Angriffsvektor Malware

"Was Firmen früher gesichert im Tresor aufbewahrten, liegt heute nicht selten ungesichert im Firmennetzwerk herum„

Zugriff durch:
10.000 neue Viren pro Tag (Quelle AV-Test)
Rasch wachsenden Bot Netze
Maßgeschneiderte Trojaner, Keylogger.
Kosten von:
39 EURO – 35.000 EURO für unbekannten Exploid mit Malware.



Angriffsvektor kleine Spionage

"Was Firmen früher gesichert im Tresor aufbewahrten, liegt heute nicht selten ungesichert im Firmennetzwerk herum„

Cyber Kriminelle Preisliste:

20 Millionen Spam Mails	350 EURO
Log on für Computer Portal/Spiele	6 EURO
Kreditkartendaten	3 EURO
Identität mit Pass u. Kredit Karten	2500 EURO

Angriffsvektor Spionage

„Es gibt Länder, in denen die Informationsbeschaffung nicht strafbar ist und zum Auftrag eines jeden Bürgers gehört„

Auch der deutsche Mittelstand ist verstärktes Ziel von Hackerangriffen. "In letzter Zeit haben wir verstärkt chinesische Hackerangriffe festgestellt", sagte der Vizepräsident des Bundesamtes für Verfassungsschutz, Hans Elmar Remberg, im Februar in einem Zeitungsinterview. China betreibe Wirtschaftsspionage in Deutschland "hauptsächlich auf dem elektronischen Sektor". (Spiegel 2007)

Finanzielle Anforderungen an Firmen

Kosten der Offenlegung

- **Die Offenlegung ist Pflicht, die Kosten sind gigantisch**
  - USA: SB1386 — 36 State laws, 5 Federal bills, DE neuer §42 BDSG
  - **Verschlüsselung ist der einzige "sichere Hafen"**

Strengere Sicherheitsmaßnahmen

- **Wachsende Richtlinien, Sanktionen**
  - FSA, BASEL-II, Data Protection Act (UK / EU), EU Directive 95/46/EC
  - SOX, HIPAA, GLBA

Erhöhte Mobilität

- **Rasant steigende Zahl mobiler Arbeitskräfte**
  - 93M Laptops, 2008 - 170M USB dev., 50% CAGR

Durchschnittliche Kosten pro aufgedecktem Verstoß: ~$7.5 Mio.
Ein Bruchteil der Kosten durch Schutz

Ist der Kampf verloren ?

NEIN ! Erstellen Sie ein Konzept

Methodik des ISMS zur risikoorientierten Steuerung

Das ISMS (InformationsSicherheitsManagementSystem) leitet sich aus der ISO2700x ff. ab.

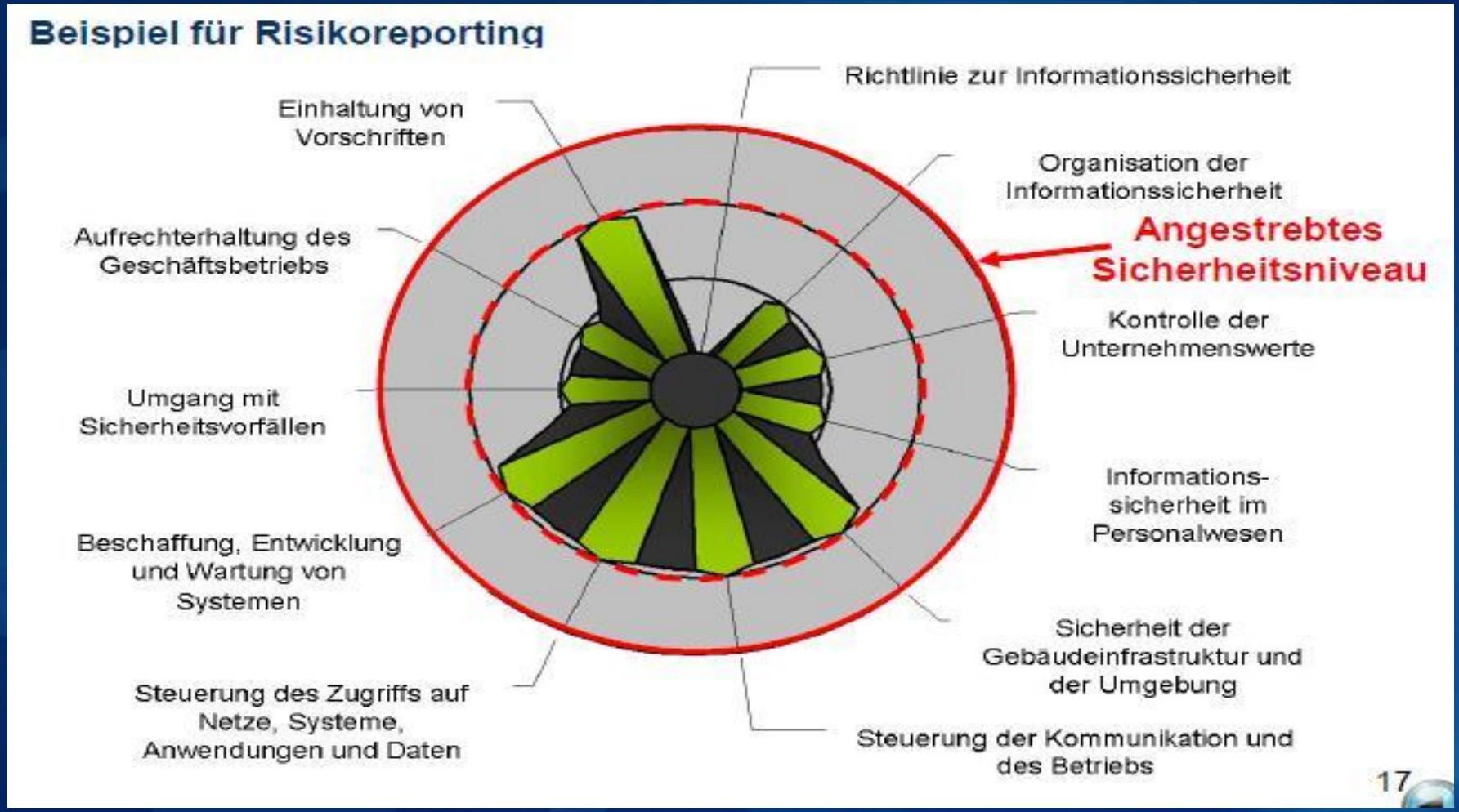
Gegenüber dem klassischen IT-Grundschutz verfolgt dieser ISO-Standard einen risikoorientierten Ansatz.

Im ISMS müssen grundlegende Parameter für einen sicheren IT-Betrieb geklärt oder definiert sein:

(1) Wie lauten die Informationssicherheitsziele des Unternehmens?
(2) Welche Voraussetzungen müssen für eine funktionierende Informationssicherheit im Unternehmen geschaffen sein?
(3) Wie sieht der (übergeordnete) Informationssicherheitsprozess aus?
(4) Wie muss die Informationsicherheitsorganisation gestaltet sein, welche beteiligte Rollen und Verantwortlichkeiten müssen existieren?

IS-Dokumentenhierarchie

Verfolgen Sie einen Plan



Technische Hilfen

Nutzen Sie Outpost24 zur Bestandsaufnahme der Lücken

Schwachstellenanalyse und Haftungsfreistellung

Nutzen Sie Verschlüsselung

Stoppen Sie alle offene und private Internetnutzung

Verzichten Sie auf IM, Twitter, Facebook etc.

Kontrollieren Sie mit ARP Guard Ihre IT Geräte

Kontrollieren Sie WIRKLICH ihre ITK Landschaft.

Beispiel Client

Oft sieht der Client intern so aus

Alles mögliche ist dort abgelegt ohne Struktur

Wer weiß dann was wo ist ?

Kann sein dass was fehlt, weiß ich nicht.

Lösung Client

- Antivirus ist ein muss ! Haftung beachten
- Clients verschlüsseln ! Haftung beachten
- Anwender schulen im Umgang mit Daten und Sicherheit
- Schnittstellen beschränken (USB, CD /DVD)
- Nur Benutzer, keine lokalen „Admins“ einrichten.
- Software Installation beschränken
- Nur benötigte Ports und Portale öffnen.
- Ordnung vorgeben und vorleben

Externe Endgeräte

- Erlauben Sie kaum bis keine externe Endgeräte
- Kontrollieren Sie den Einsatz
- Blocken Sie durch Verschlüsslung den Einsatz von „mitgebrachten“ Geräten
- Erlauben Sie nur die Speicherung und den Datenaustausch auf Verschlüsselten Endgeräten.

Zusammenfassung

- IT Sicherheit und Datenschutz ist kein statischer Bereich.
- Machen Sie sich klar, es gibt keine 100 % Lösung.
- Analysieren Sie Ihre Situation im Betrieb und erstellen eine Schwachstellenanalyse.
- Erledigen Sie Punkt für Punkt und kontrollieren Sie die Ergebnisse.
- Beginnen Sie von vorne.

Vielen Dank für Ihre Aufmerksamkeit.

Fragen Sie jetzt oder senden Sie mir eine Email:

juergen_saamen@secuware.de