it.sec
security for your information

Data Leakage - über den unerwünschten Informationsabfluss

Holger Heimann
it.sec GmbH & Co. KG

GI Fachgruppe Management von Informationssicherheit
Frankfurt am Main, 25.2.2011

Anmerkung:

Leider hatte die PDF Erzeugung aus dem PPTX einige Formatprobleme und Artefakte zur Folge, die nicht loszuwerden sind.

Der Autor entschuldigt sich für den Umstand.

Vortragender

Dipl. Ing (FH) Holger Heimann

(CISA)

- Geschäftsführer der it.sec GmbH & Co. KG
- Mehr als 20 Jahre Berufserfahrung als Informationssicherheitsberater
- Externer Datenschutzbeauftragter
- Externer Informationssicherheitsbeauftragter
- Pentester und IT-Forensiker

it.sec GmbH & Co. KG

IT-GRCM steht für IT Governance, Risk & Compliance Management.
Hier stehen bei uns Instrumente und Führungsstrukturen des Informationssicherheits-Managements sowie Fragen der toolgestützten Modellierung von Risikomanagement und Compliance-Anforderungen im Vordergrund, sowie der zielgerichtete Einsatz von technischen und organisatorischen Maßnahmen zur passgenauen Erfüllung identifizierter Anforderungen.

Infrastruktursicherheit & Data Protection
it.sec bietet neben den klassischen Infrastrukturthemen auch umfangreiche Dienstleistungen im Bereich der SCADA Sicherheit an, hierzu zählen neben Sicherheitskonzepten auch Leittechnik-verträgliche Methoden für Vulnerability Assessments, Infrastruktur-Mappings oder Protokoll-Analysen. Natürlich gehören auch Industrial Firewalls und AAA Systeme ins Portfolio.

Penetrationstests, IT-Forensik Assessments & Audits
it.sec ist einer der führenden Anbieter von Penetrationstests. Zu unseren Kunden gehören Institutionen aller Branchen, Größen und Sicherheitsstufen, in mehr als einem Dutzend Ländern. Unser Angebot umfasst hierbei **Penetrationstests**, **Sourcecode-Reviews**, **Design-Reviews** sowie **forensische Untersuchungen** und **Beweissicherung. Im Rahmen des PCI DSS Standards führen wir Compliance Penetrationstests durch.**

Datenschutz wird im deutschen Sprachgebrauch leicht verwechselt mit Datensicherheit. Im Englischen spricht man treffender von Privacy ("Privatheit"), geht es doch beim Datenschutz um den Schutz der verfassungsgemäß garantierten Persönlichkeitsrechte beim Umgang mit personenbezogenen Daten. Dazu zählt neben dem sog. informationellen Selbstbestimmungsrecht auch das Telekommunikationsgeheimnis.

Data Leakage/Loss Prevention - DLP

Klassische IT-Sicherheit/Infrastruktursicherheit

- Erhalt von Vertraulichkeit, Verfügbarkeit, Integrität
- Design klassisch zur Abwehr von **externen** Angreifern

DLP zielt generell auf „*unerwünschten Abfluss von Daten*“ ab, also Vertraulichkeitsverlust z.B. durch

- Technische Sachverhalte, aber auch direkt durch
- Menschen
  - Externe
  - Interne
  - Halbinterne
  - durch Absicht oder Versehen

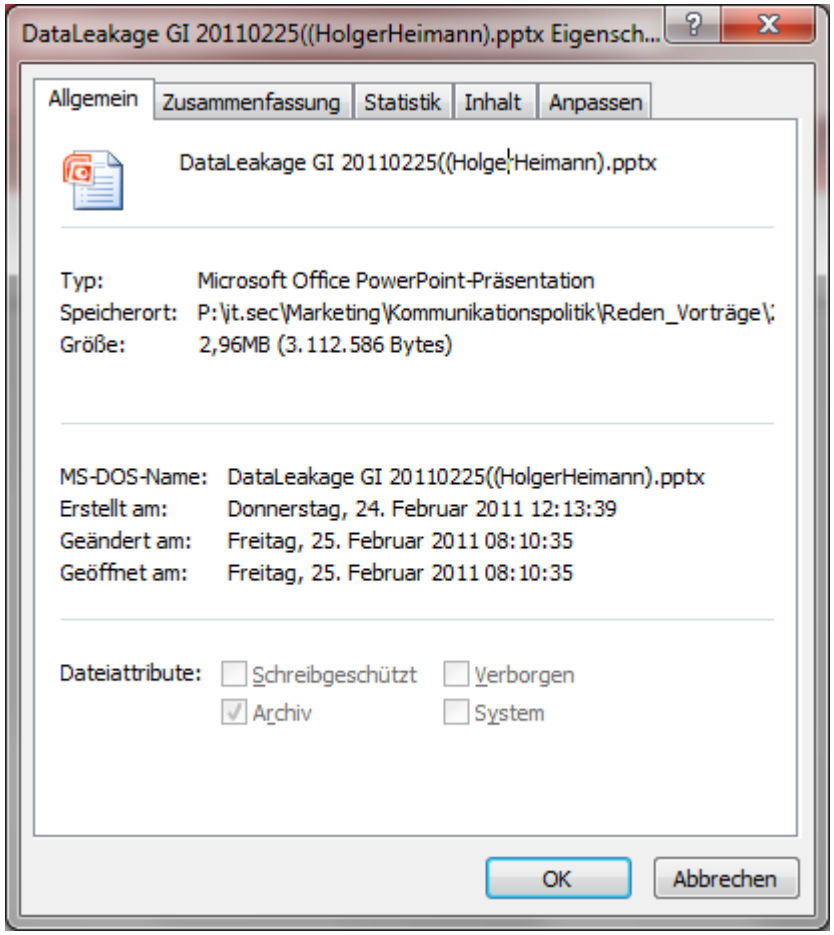
Beispiel Datenleak Protokollebene

Mailheader:

… for <hh@it-sec.de>; Thu, 24 Feb 2011 18:10:15 +0100 (CET)

:::
*X-Originating-IP: [**193.28.xxx.yyy**]*
*Received: (**qmail** 9971 invoked from network); 24 Feb 2011 17:10:14 -0000*
*Received: from **mail.nameeurope.net** (HELO **proxyxxx1.yyy.de**) (**193.28.xxx.yyy**)*
by server-9.tower-140.messagelabs.com with SMTP; 24 Feb 2011 17:10:14 -0000
*Received: from **ex04.intern.name.de** (unknown [**10.197.78.12**])*
by proxyxxx1.tds.de (Postfix) with ESMTP id 49C3110436
for <hh@it-sec.de>; Thu, 24 Feb 2011 18:10:14 +0100 (CET)
*Received: from mail pickup service by **ex04.intern.name.de** with Microsoft SMTPSVC;*
Thu, 24 Feb 2011 18:10:13 +0100
*Received: from **EX02.intern.xxx.de** ([**10.197.78.30**]) by **xxxex04.intern.XXX.de** with*
***Microsoft SMTPSVC(6.0.3790.4675)**; Thu, 24 Feb 2011 18:10:13 +0100*
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.4657

Beispiel Datenleak Metadaten



z.B. Angaben über

- Accountdaten
- Drucker
- Servernamen
- eMail Adressen
- Pfade
- Angaben zur Orga (Abteilung XY…)

In vielen gängigen Formaten enthalten

-Office
-Pdf

Beispiel Datenleaks „Foren“/SocNets

- Technische Foren
- Social Networks

→ „Google ist Dein Freund“

Datenleaks – aktuelle Highlights

- SPIEGEL 11/2009: 190.000 Bankkarten werden bei Sparkassen nach Datenleck ersetzt

WikiLeaks

- SPIEGEL: Mehr als 250.000 Depeschen aus dem internen Netz des … US-Außenministeriums sind über WikiLeaks an die Öffentlichkeit gelangt
- Stern: Trotz vehementen Protests der US-Regierung hat die Internetplattform Wikileaks in der Nacht zu Samstag fast 400.000 Geheimdokumente zum Irak-Krieg veröffentlicht

Julius Bär

- Sueddeutsche: Ein Unbekannter verkauft deutschen Behörden die Daten von Steuerhinterziehern.

www.teamshatter.com/breaches

Date	Organization	Description	Records	Industry	Type	Location
08/27/2010	Schlecker	150,000 names, addresses, genders, email addresses and customer profiles posted on the Internet by external service provider	150000	Retail Businesses	Inside - Accidental	Germany
04/28/2010	City of Olfen Germany	Website exposes confidential documents of more than 800 city and district council members	800	City (Government or Citizens)	Inside - Accidental	Olfen, Germany
04/09/2010	Wacken Open Air	Hacked server exposes customers credit card details	Unknown	Retail Businesses	Outside	Hauptstraße 47, 24869 Dörpstedt, Germany
03/29/2010	Klinikum Kassel	Documents found on street contained lists of patients medical details including dates of birth, diagnoses	21	Hospital	Inside - Accidental	Mönchebergstraße 41, 34125 Kassel, Germany
03/08/2010	Münster-Marathon e.V.	Thousands of marathon participants personal information accidentially included on a documentary dvd	3500	Organization	Inside - Accidental	Roggenmarkt 11, 48143 Münster, Germany
02/18/2010	Landkreis Teltow -Fläming	Sensitive company information, including signatures, staff details, investment info exposed on internet	Unknown	County Government	Inside - Accidental	Am Nuthefließ 2, 14943 Luckenwalde, Germany
02/11/2010	BKK Health	Third party contractors accessed and extorted millions of health subscribers sensitive medical information	1500000	Insurance	Inside - Malicious	Germany
01/19/2010	RUF Travel	SQL injection exposes 50,000 youth names, addresses, dates of birth and email addresses	50000	Retail Businesses	Outside	Boulevard 9, 33613 Bielefeld, Germany

Date	Organization	Description	Records	Industry	Type	Location
02/16/2011	Charleston Area Medical Center's Research Institute	3,655 patient names, contact details, Social Security numbers, dates of birth, along with certain basic clinical information exposed in database	3655	Medical Provider	Outside	3211 Maccorkle Ave SE, Charleston, WV 25304, USA
02/15/2011	Lush Australia	Lush Australia Website Hacked - Credit card details obtained.	Unknown	Retail Businesses	Outside	Australia
02/15/2011	Day's Jewelers	Thousands of credit cards exposed due to hackers outside of the company	2000	Retail Businesses	Outside	88 Main St, Waterville, ME 04901, USA
02/14/2011	Emory Healthcare	2,400 patients names, Social Security Numbers, addresses, date of births and limited health information stolen by hackers	2400	Medical Provider	Unknown	Atlanta, GA, USA
02/09/2011	Oregon Department of Corrections	500 employees Social Security numbers and payroll information lost on portable thumb drive	550	State Government	Inside - Accidental	2575 Center St NE, Salem, OR 97301, USA
02/04/2011	Medi-Cal	2,400 beneficiaries' names, Social Security numbers and other identifying information emailed to personal computer, two attorneys and two union representatives	2400	Medical (Non -Hospital / Provider)	Inside	San Francisco, CA, USA
01/29/2011	University of Iowa Hospitals and Clinics	13 medical records for hospitalized Iowa football players improperly accessed	13	Medical (Non -Hospital / Provider)	Unknown	200 Hawkins Dr, Iowa City, IA 52242, USA
01/26/2011	University Book Exchange	Credit and debit card information stolen	Unknown	Retail Businesses	Unknown	516 Cotanche St, Greenville, NC 27858, USA

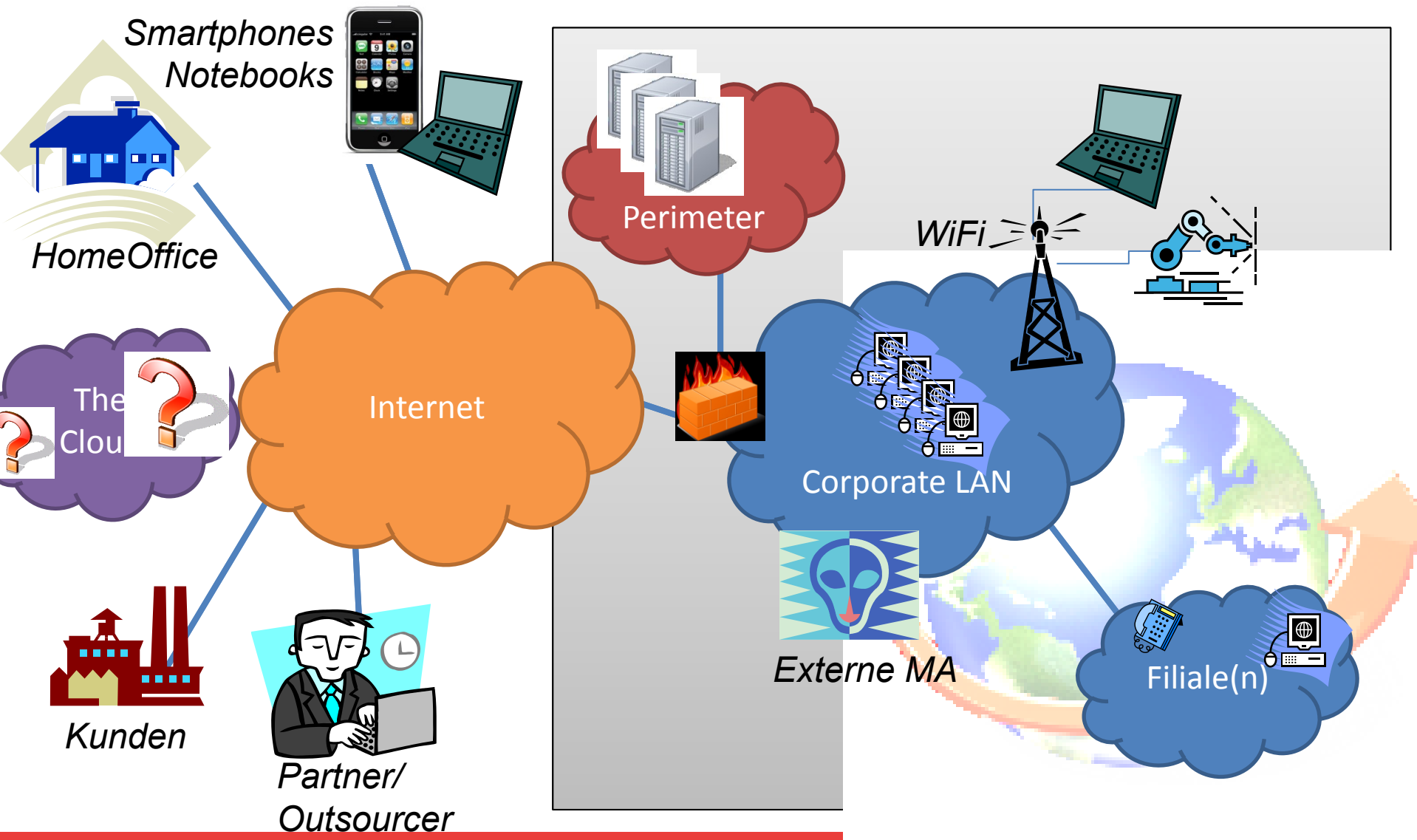
Konsequenzen

- Strafzahlungen
- Schadenersatzzahlungen
- GL Verantwortung

- Aber i.d.R. viel wichtiger: Reputationsverlust

- Verlust von wichtigen Informationen (an Konkurrenz, Gegner, etc.)

Corporate Networks anno 2011



Corporate Networks anno 2011

Was spielt alles mit (lose Stichwortsammlung)

-IP
-SMB/CIFS/NTFS
-HTTP
-HTTPS
-SMTP
-FTP
-SCP
-USB
-Firewire
-SATA/eSATA
-RAW-Daten, .doc, ascii, xls, etc…
-Gezippte Daten
-Verschlüsselte Daten
-… was noch? …

- Alte Festplatten
- Slackspace
- Temp-Dateien
- Snapshots
- Metadaten
- Vulnerabilities bei der Informations-Präsentation (WWW)

Funktionsweise „Endpoint Security“

- Abfangen von Datenflüssen
- Klassifikation *on the fly* z.B. nach
  - Herkunft
  - Ziel
  - Klassifikations-Tags („VERTRAULICH“)
- Entscheidung über Weitertransport am „Endpunkt“

Herausforderungen Endpoint-Security

- Nicht Failsafe
  - Ist eine Stelle undicht, ist es passiert
  - Verlässt ein Datum den kontrollierten Bereich, ist es auch passiert
- Klassifizierung i.d.R. *ex post*,
  - Speicherortbasiert
  - Inhaltsbasiert
  - nach Dateityp oder
  - nach „Device“
  - was aber mit
    - „*nicht* Geheim“
    - Texten als Bild
    - „rot8“
    - Unkontrollierten Übergängen
  - False Positives
- Regelbasiert
- Funktionieren nicht unter allen Umständen
  - I.d.R. in „Explorer“ integriert → Aber „CMD“?
  - Mit Outlook, nicht aber mit „xyz“
- Konflikte
  - Handling von verschlüsselten Daten?
- *Was passiert bei Partnern/Zulieferern?*
- Rechtlich *interessant*

Alternativen (Wünsch Dir was)

- Eine Lösung die (möglichst) Failsafe ist
- Sichere Klassifikation von Daten bei der Entstehung
- Dazu müssen die Informationen
  - den Schutz in/mit sich tragen („intrinsischer Schutz“)
  - Recht auf Zugriff/Nutzung **unabhängig** von „Zonen“ oder „Perimetern“ sondern User/Role-Based
  - Entscheidung über Zugriffsmöglichkeiten erfolgt zur Zeit der Nutzung, nicht bei „Transporten“ und „Zonenübergängen“
- Folge:
  - es ist egal, wo sich Daten befinden, sogar wenn sie interne, geschützte Bereiche verlassen, bleiben sie zugriffsgeschützt
  - Nicht mehr n-Einzelprobleme und –Regeln, sondern Reduktion auf Access-Model und Klassifikation

Die Zukunft (so glauben wir)

- Digital-Rights-Management (DRM) basierte Lösungen, bzw.
  - Datenobjekte, welche verschlüsselt sind und deren Nutzung (Entschlüsselung) von den entsprechenden Programme transparent und durch in-time Authentication gewährleistet wird
- Standarddatenformate werden (nativ?) unterstützt
- APIs für beliebige Formate werden verfügbar sein

DRM-basierte Systeme

Sind schon verfügbar: MS-DRM, SecureIslands, (…)

Vorteile:

- Secure by Design
- Failsafe
- Runtime-Kontrolle über Dokumente (Drucken? Cut-‘n‘-Paste? Speichern?)
- Klassifikation bei Erstellung möglich

Nachteile:

- Integration in entsprechende Produkte nötig
- PKI ähnliche Strukturen nötig

DRM Lösungen total sicher?

- Bedauerlicherweise nicht zwangsläufig
  - *Problem mit allen Daten, die NICHT DRM- enveloped sind*
  - *Low-Level-Data: select * from table | rot8 …*
  - *Absehbar nicht der gesamte Bearbeitungsprozess abdeckbar*
- So sicher wie die verfügbaren Kryptoverfahren
- Im Dokument befindliche Meta-Daten immer noch Problem
  - Eigenschaften, Redo-Logs/Versionen etc.
- Shouldersurfing, Screenshots im Internetcafé …
- Basisinfrastruktur und Lowlevel Datenhaltung muss immer noch klassisch gesichert werden

Fazit

- Klare Zielsetzungen vor Umsetzung sind nötig
  - Risikoanalyse
  - Beachtung der verschiedenen Ebenen und Bereiche

- Absolute Sicherheit bleibt schwierig (unerreichbar?)
- Konzeptionel saubere Lösungen sind
  - kaum deployed
  - „Lochabdichtungslösungen“ überlegen, aber
  - …nur dann ultimativ sicher, wenn ALLE Informationen so verwaltet werden

Das wird nicht so schnell passieren (ASCII rules!)

Realitäts-Check:

Soll ich Endpoint Lösungen zur DLP einsetzen?

- eine Frage der Schutzziele
- IMHO nicht wirklich sicher, aber abschreckend
- IMHO nicht geeignet für große Installationen

- Ohne den Menschen nützen alle technischen Lösungen nichts!

Fragen/Diskussion

it.sec GmbH & Co. KG
Einsteinstr. 55
D-89077 Ulm

USt Id Nr.: DE 225547544
Steuernummer: 88012/53709
Amtsgericht Ulm: HRA 3129

vertreten durch den **Geschäftsführer Dipl. Ing. (FH) Holger Heimann**.

Haftender Komplementär:
it.sec Verwaltungs GmbH
Amtsgericht Ulm: HRB 4593
Einsteinstr. 55
D-89077 Ulm