



Security Management in einem Großkonzern

am Beispiel der Deutschen Telekom AG

Thomas Königshofen, Sicherheitsbevollmächtigter, Deutsche Telekom AG
Rheinlandtreffen, 12. November 2008

Gliederung

- Bedrohungsanalyse /modi operandi der Infobeschaffung
- Ursachen für den ungewollten Informationsabfluss
- Strategische Steuerungsinstrumente zur Informationssicherheit
- Die Group Business Security und ihre Aufgaben
- Klassische operative Informationsschutz-Maßnahmen und ihre Grenzen
- Awareness-Kampagnen und Abschreckungskonzepte in der Praxis
- Fazit

Bedrohungsanalyse

- **Komplexität/Vernetzung der Systeme mit schutzwürdigen Informationen wächst**
 - Beispiele: Email/Mobilfunk; Internet/Festnetztelefonie; Elektronische Personalakte
 - Dynamische Veränderungen der Unternehmensstrukturen/ -netzwerke durch Globalisierung und neue strategische Fokussierung (Beispiel: Verkauf VTS in Deutschland, Erwerb Orange in den Niederlanden)
- **„Nachfrage“ nach vertraulicher Information wächst (aber auch das „Angebot“)**
 - Nachrichtendienste
 - Konkurrenz-Unternehmen
 - „Informationsbeschaffer“ und „Informations-Händler“
- **Kriminelle Energie und Professionalität der Angreifer wächst**
 - Vom „Script-Kiddy“ zum Trojaner-Baukastenersteller
 - Vom Hacker zum Cracker (Phishing, PBX-Fraud, Prepaid-Boxes, Less-Than-0-Day Exploits)
 - Von der Gelegenheitsverwertung zum Geschäftsmodell (Competitive Intelligence)

modi operandi der Informationsbeschaffung

- **Gezielte Beschaffung von Datenträgern**
 - Diebstahl von Informationsträgern (Notebook, USB-Stick, Dokumente ...)
 - Mitnahme von Hardcopies (Kopien von Dokumenten im Mülleimer; gebrauchte Datenträger (zB beschriebene CD-ROM, ausgetauschte PC´s [Festplatten] ...)
- **Direkte Beschaffung von Informationen**
 - Eindringen in IT-Systeme (Viren, Würmer, Trojaner, sonstige Hacking-Attacken)
 - Einsatz von Abhörtechnik (technischer Lauschangriff)
 - Agenten-Anwerbung und Agenten-Einsatz beim Opfer
- **Indirekte Beschaffung von Informationen**
 - Social Engineering,
 - Informationsbeschaffung bei ehemaligen Mitarbeitern des Opfers
 - Human Intelligence
 - Analyse offener Quellen

Ursachen für den ungewollten Informationsabfluss

■ Ursachen beim „Opfer“

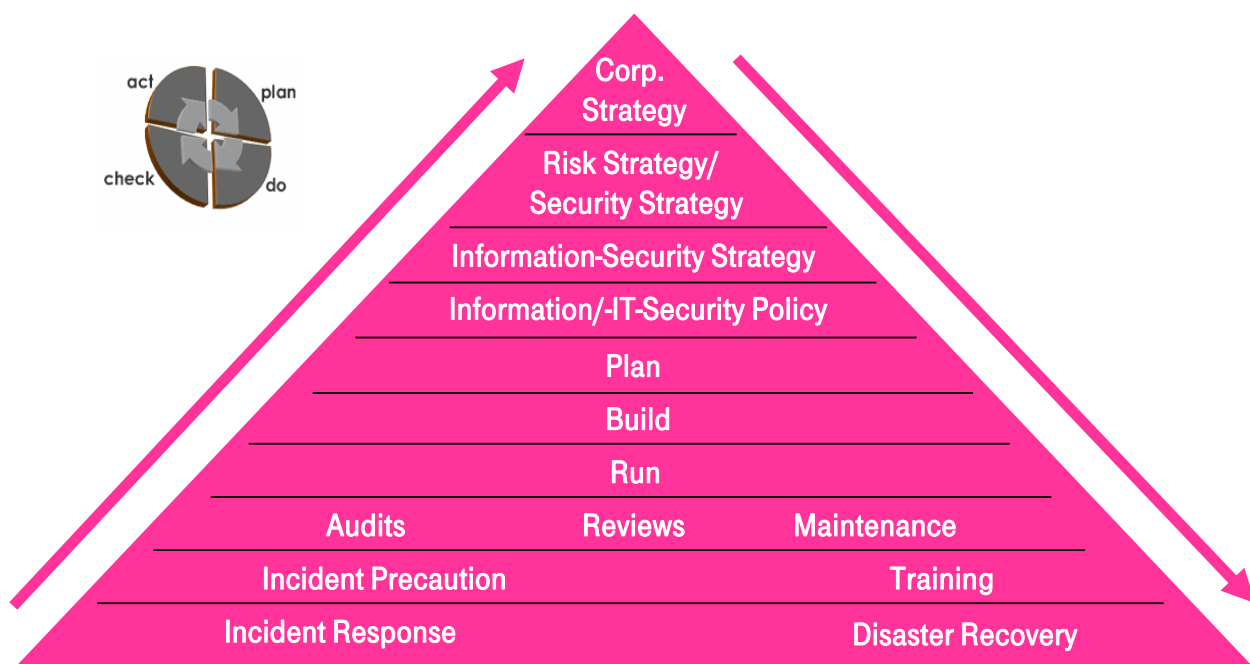
- Keine gute IT-Sicherheit (Firewall, Antivirenschutz, Verschlüsselung, Patch-Management ...)
- Fehlende Lauschabwehr (organisatorische und technische Prävention)
- Fehlendes Gefahrenbewusstsein, mangelhaftes Screening ...

■ Ursachen beim Mitarbeiter

- Fahrlässigkeit im Umgang mit Firmeneigentum (Beispiel: Laptopverlust)
- Mangelnde Sensibilität, kein Unrechtsbewusstsein
- Fehlende Werkzeuge oder fehlendes Know-How (zB Verschlüsselung; Daten-Entsorgung; Funktionalitäten für sicheres Löschen usw.)
- Innere Kündigung
- Charakterschwäche (Geltungssucht, Geldgier, Rachegeleüste)
- persönliche Notlagen (z.B. Erpressbarkeit, Überschuldung usw.)

Information Security Management

Die Corporate Information-Security Strategy im Information-Security Management Prozess



Strategische Steuerungskonzepte zur Informationssicherheit

- **Strategische (langfristige) Ziele der Informationssicherheit (Information Security Strategy)**
 - Verfügbarkeit der Information an den notwendigen Stellen
 - Schutz vertraulicher Informationen vor unbefugter Kenntnisnahme
 - Integrität der Informationen (Vollständigkeit, Authentizität, Zurechenbarkeit)
- **Klassifizierung von Informationen; Zugang zu Informationen; Umgang mit Informationen, Behandlung von Informationen (Information Security Policy = Sollzustand) im Hinblick auf**
 - offene Informationen
 - interne / vertrauliche Informationen
 - streng vertrauliche / geheime / streng geheime Informationen
- **Unterschiedliche operative Maßnahmen**
 - Werkzeuge (PKI, Zugangsschutz, Verschlüsselung, ...)
 - Unternehmensregelungen (Infoschutz-Richtlinien; Anweisungen)
 - Audits, Reviews
 - Schulungs- und Sensibilisierungsmaßnahmen, repressive Maßnahmen (Ermittlungen etc.)

Strategische Steuerungskonzepte zur Informationssicherheit

- **ISMS (Information Security Management System)**
 - ISO-Standard 27.000 ff. (ehemals Britischer Standard 7799)
 - Umfasst alle Maßnahmen der Informationssicherheit
 - Umsetzung führt zu einem Sicherheitsniveau „aus einem Guss“
- **ITIL (Information Technology Infrastructure Library), Kapitel: Security Management**
 - ISO-Standard 20.000 ff. (ehemals Britischer Standard 15.000)
 - Beschreibt die Organisation von IT-Prozessen (was muss getan werden)
 - Umsetzung erleichtert die Fragmentierung von Aufgaben (SLA, Outsourcing etc.)
- **Key Performance Indicators – KPI´s (Balanced Scorecard, TQM nach ISO 9000 ff. etc.)**
 - Dienen der strategischen Steuerung (Zielvorgaben)
 - Beschreiben die Soll-/Ist-Abweichung
 - Objektivieren die Ressourcenverwendung

Die Group Business Security (Konzernsicherheit)

- **Aufgaben**
 - Gewährleistung eines hohen Sicherheitsniveaus im Konzern
 - Regelungsgeber für den Gesamtkonzern
 - Operative Aufgaben (Beratung, Unterstützung, Kontrolle)
- **Mission**
 - Sicherheit in die Prozesse
 - Sicherheit in die Systeme
 - Sicherheit in die Köpfe
- **Herausforderungen**
 - Image
 - Compliance
 - Neuorganisation (Stichwort: Datensicherheit)

Klassische operative Informationsschutz-Maßnahmen

- **Maßnahmen gegen ungewollte Weitergabe**
 - Personalauswahl unter Sicherheitsgesichtspunkten: Knowledge, Skill, Attitude
 - Personalsensibilisierungs- und Schulungsaktivitäten
 - Produktauswahl unter Sicherheitsgesichtspunkten: Software, Hardware
(z.B. Verschlüsselungstools, Datenlöschungs-Tools)
- **Maßnahmen gegen offene und verdeckte Beschaffung durch Dritte**
 - IT-Sicherheits-Management (Firewall, Antivirenprogramme, Daten-Verschlüsselung ...)
 - Regelmäßige Prävention gegen Lauschangriffe
 - Sensibilisierung von Wissensträgern, Personal Screenings ...
- **Maßnahmen gegen die gezielte Weitergabe durch „Innentäter“ bzw. Wissensträger**
 - Einengung des Kreises der Wissensträger (Need-to-know-Prinzip)
 - Erhöhung des Risikos, entdeckt zu werden (Kontrollen)
 - Abschreckung (präventiv: Vertragsstrafenvereinbarungen und kommunizierte/praktizierte Regeln bei Geheimnisverrat [z.B. Strafverfolgung] ...)

Grenzen von Präventions- und Kontrollinstrumenten

■ Betriebsverfassungsrecht

- Logdateien-Systeme sind technische Einrichtungen, die nach der Rechtsprechung der Arbeitsgerichte dazu bestimmt (weil objektiv geeignet) sind, das Verhalten der Arbeitnehmer zu überwachen; daraus ergibt sich ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG
- Betriebsvereinbarungen sollten regeln,
 - welche Ereignisse (zB Zugang zu einem System, versuchter Zugang zu einem System) grundsätzlich geloggt werden (zB Firewall-Administration)
 - welche dieser Logdaten wann, von wem und für welche Zwecke ausgewertet werden dürfen (zB bei Verdacht auf Geheimnisverrat: Wer hat wann wem eine Email geschickt?)
 - in welchen Fällen datenforensische Untersuchungen (zB was ist/war auf der Festplatte des Dienstrechners gespeichert?) durch wen durchgeführt werden dürfen

Grenzen von Präventions- und Kontrollinstrumenten

■ Datenschutzrecht, Post- und Fernmeldegeheimnis, allgemeines Persönlichkeitsrecht

- Die Auswertung personenbezogener Daten (zB Zugriffe auf Systeme oder Dateien) ist im Einzelfall abhängig von dem Ergebnis einer Interessenabwägung zwischen den geschützten Interessen des Arbeitgebers (zB Eigentum) und denen des Arbeitnehmers (zB informationelles Selbstbestimmungsrecht, Fernmelde- und Postgeheimnis)
- Eine präventive vollständige Überwachung (zB Emails, Internetnutzung, Videoüberwachung am Arbeitsplatz) durch den Arbeitgeber ist nach der Rechtsprechung grundsätzlich unzulässig und auch nicht durch eine Betriebsvereinbarung regelbar.
- Eine repressive Überwachung bzw. Kontrolle (zB Auswertung der Daten auf dem dienstlichen PC oder Handy) ist nur mit Zustimmung des Betriebsrats und nur in besonders gravierenden Fällen (Interessenabwägung) zulässig. Bei zulässiger privater Mitnutzung der Kommunikationssysteme scheidet eine Kontrolle der Kommunikation (zB Email-Verkehr) durch das Unternehmen aus – das dürfen nur die Strafverfolgungsorgane im Rahmen ihrer gesetzlichen Befugnisse (Strafprozessordnung).

Awareness-Kampagnen und Abschreckungskonzepte

■ Die vier Phasen von Awarenesskampagnen

■ Die Aufmerksamkeitsphase

Ziel: Mitarbeiter und Führungskräfte werden auf das Thema gelenkt und motiviert, sich damit auseinanderzusetzen

■ Die Wissensvermittlungs- und Veränderungsphase

Ziel: Know-How-Vermittlung, Motivation zur Verhaltensänderung

■ Die Phase der „Verstärkung“

Ziel: Festigung der Verhaltensänderung im Sinne einer dauerhaften Veränderung der Einstellung

■ Die Phase der „Öffentlichkeit“

Ziel: Imageverbesserung, Steigerung des Kundenvertrauens; damit zusätzlicher „payback“

■ Notwendige Begleitung:

- Messungen des Know-Hows und der Skills vor, während und nach der Kampagne

Abschreckungskonzepte in der Praxis

■ Voraussetzungen für ein wirksames Abschreckungskonzept

■ Klare Regelungen, was erlaubt ist und was nicht

Beispiele: Weitergabe / Mitnahme vertraulicher Informationen; Umfang der erlaubten privaten Mitnutzung dienstlicher Hard- und Software; Umfang „privater“ Aufzeichnungen

■ Klare Kommunikation und Commitment

Beispiel: Bestätigung der Kenntnisnahme der Regeln durch Unterschrift

■ Klare Sanktionsankündigungen

Beispiel: Fristlose Entlassung, Strafanzeige und Schadensersatzklage bei Geheimnisverrat

■ Hohes Risiko des „Erwischtwerdens“

- Professionelle und unternehmensintern bekannte forensische Prozesse

- AFM (Anti-Fraud-Management) / BKMS (Business Keeper Management System)
- Whistleblowing (Hotlines für anonyme Hinweise)
- Datenspeicherung und -auswertung (ITK-Forensik)

Abschreckungskonzepte in der Praxis

- **Conditio sine qua non: Kommunikation von Repressionsmaßnahmen**
 - **Keine Scheu vor großen Namen**

Bei nachgewiesenen Verstößen (auch des Top Managements):



An den Pranger!

Fazit:

- Der ungewollte Abfluss vertrauenswürdiger Informationen ist ein Risiko, das bei vielen Unternehmen mit schützenswertem Know-How oder schützenswerten Informationen (zB Strategien, Wirtschafts-, Vertriebspläne, FuE-Ergebnisse, Marketingpläne, Kunden- und Personaldaten) größer wird. Auch die Image-Schäden können enorm sein.
- Präventionskonzepte zum Informationsschutz mit dem Ziel, unter Beachtung einer sinnvollen Kosten-Nutzen-Relation die Risiken deutlich und nachhaltig zu minimieren, bedürfen einer ganzheitlichen Betrachtungsweise, die nur im Sinne eines strategischen Ansatzes zum Management der schützenswerten Informationen und der Informations- und ITK-Sicherheit „state of the art“ gelingen kann.
- Unsicherheitsfaktor und größtes Risiko für den unerwünschten Abfluss von schützenswerten Informationen ist der Mensch; dieser menschliche Faktor sollte immer im Mittelpunkt aller Schutzkonzepte stehen. (Stichwort: Awareness):
- Die interne Aufklärung von „Datendiebstahl“ sollte unter dem Gesichtspunkt der Einhaltung rechtlicher Grenzen (Datenschutz) immer im Vier-Augen-Prinzip erfolgen.

Vielen Dank für Ihre Aufmerksamkeit!



e-mail: Thomas.Koenigshofen@telekom.de



Informationssicherheit
Thomas Königshofen
Stand: November 2008, Seite 17