Deutsch Wyss
& Partner

Anwaltsforum des Zürcher Anwaltsverbandes

12. März 2008

IT-Sicherheit für die Anwaltskanzlei
Sicht des Anwalts

Dr. Wolfgang Straub

Übersicht

- Geheimhaltungs- und Datenschutzpflichten
- Versand und Aufbewahrung von E-Mails
- Praktische Erfahrungen

2

Ziele

Generelle Sicherheitsziele

- Verfügbarkeit von Daten und Infrastruktur
- Vertraulichkeit/Integrität von Daten
- Beweisbarkeit der Integrität von Daten
- Effizienz der Datenverarbeitung

3

Ziele

Praktische Sicherheitsziele

- Vermeidung von Schäden (auch Reputations-schäden) mit vernünftigem Aufwand
- Dokumentation der eigenen Sorgfalt im Hinblick auf Haftung

4

Ziele

IT-Sicherheitslücken sind nur eine von verschiedenen Gefahren (Social Engineering, Indiskretionen, unbeabsichtigte Falschadressierung).

5

Anwaltsgeheimnis

Art. 321 StGB

- mindestens Eventualvorsatz nötig
- nur geheime Tatsachen

Art. 13 BGFA/Art. 15 Standesregeln SAV

Auftragsrechtliche Sorgfaltspflichten

Datengeheimnis nach Datenschutzrecht?

6

Datenschutz

Automatisierte Bearbeitung besonders schützenswerter Daten in Branchensoftware?

- Meldung an EDÖB (Art. 11a Abs. 3 lit. a DSG) oder Ernennung eines Datenschutzverantwortlichen (Abs. 5 lit. e)
- Strenge technische und organisatorische Massnahmen (Art. 9 und 10 VDSG)

→ Antrag SAV an Bundesrat für Ausnahmebestimmung in Verordnung

7

E-Mail

Potenzielle Gefahren beim E-Mail allgemein bekannt.

Systematische E-Mail-Verschlüsselung ist immer noch mit praktischen Problemen verbunden.

Bei besonders sensiblen Daten sollten Attachments verschlüsselt werden (Achtung: Dokumentnamen bleiben meist sichtbar).

8

Aufbewahrungspflichten

Aufbewahrungspflichten für Geschäftskorrespondenz (Art. 957ff. OR)

- Eintragungspflichtige Anwaltsfirmen
- Abwicklung von Firmenaktivitäten mit Büroinfrastruktur

Standesrechtliche Aufbewahrungspflichten: Analoge Anwendung von Art. 9 GeBüV

Auftragsrechtliche Nebenpflichten?

9

Aufbewahrungspflichten

Art. 9 GeBüV

Speicherung auf unveränderbaren Datenträgern oder:

- Beweisbarkeit der Integrität (Signatur)
- Beweisbarkeit des Speicherungsdatums (Zeitstempel)
- Dokumentation des Prozesse

10

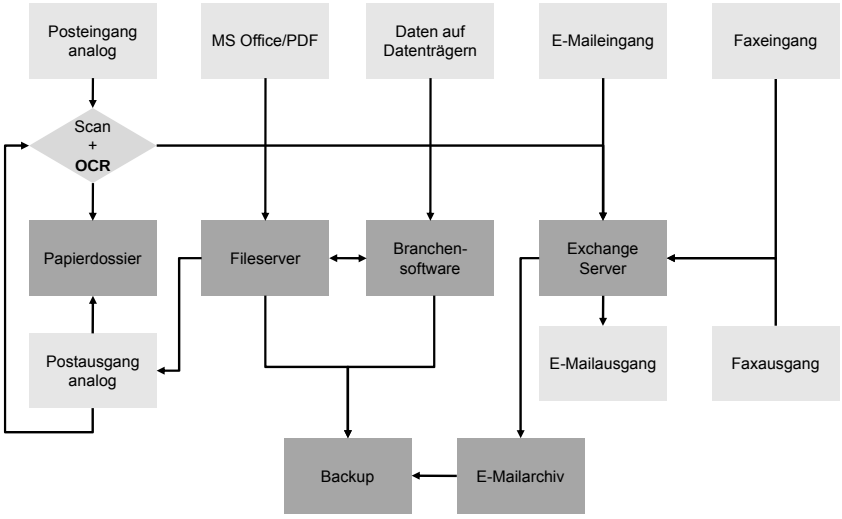
Aufbewahrungspflichten

Strategien

- Ausdrucken aller E-Mails?
- Ablage auf Exchange Server →Problem: Beweissicherheit
- Spezifische Mailarchivierungssoftware →Periodische Migration auf neue Software erforderlich

11

Aufbewahrungspflichten



12

Vorgehensempfehlungen

IT-Sicherheit ist ein Querschnittproblem, welches sich nicht mit der Implementierung punktueller Massnahmen lösen lässt.

→Sorgfaltspflichten erfordern systematische Analyse des konkreten Risikopotenzials, erlauben aber auch die bewusste Akzeptanz gewisser Risiken.

13

Sicherheitsanalyse

Beispielausschnitt Sicherheitsanalyse

Risiko	Singe Points of Failure (SPOF)	Proba-bility	Impact	Gewicht	Implementierte Massnahmen	Mögliche Zusatz-massnahmen	Kosten einma-lig	Kosten jährlich
Server	Defekt Festplatten	2	2	4	• RAID 5 • Backup von Daten	• Periodische Snapshots zur Si-cherung der Kon-figuration	-	500
	Defekt RAID-Controller	1	3	3	• Verlängerte Her-stellergarantie	• Vollständige Re-dundanz aller Server	8000	-
	Defekt Mother-board	1	3	3	• Verlängerte Her-stellergarantie	• Vollständige Re-dundanz aller Server	8000	-
	Netzteile in Servern	2	1	2	• Redundante Netz-teile	• Vollständige Re-dundanz aller Server	8000	-
	UPS	2	2	4	• Alerts • Periodische Tests	• Redundante UPS	2000	-
	SQL Server	1	2	2	• Backup Daten und Konfiguration	• Redundanter SQL Server	4000	500
	Exchange Server	1	3	3	• Backup Daten und Konfiguration	• Backup-Mailserver	-	500

14

Vorgehensempfehlungen

- Sorgfaltsnachweis durch Erarbeitung und Implementierung eines Sicherheitskonzepts
- Periodische externe Überprüfungen
- Regelmässige Sensibilisierung

15

Fragen? Kritik? Anregungen?

Wolfgang Straub
Deutsch Wyss & Partner
Effingerstrasse 17/Postfach 5860
CH-3001 Bern

+41 31 381 44 25

wolfgang.straub@advobern.ch
www.advobern.ch

16