HOCHSCHULE
RHEIN-WAAL
Rhine-Waal University
of Applied Sciences

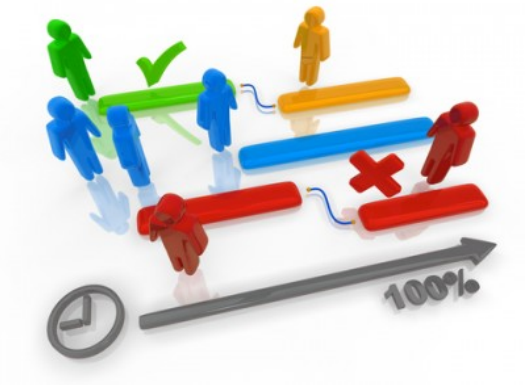
Ein Dokumentenarchiv für Hacker?
IT-Sicherheit von DMS

Kamp-Lintfort 11.02.2015

Vortrag von Prof. Dr.-Ing. Ulrich Greveler

Ausgangslage

Berechtigte Frage: „Wie beurteilen Sie eine DMS-Einführung aus IT-Sicherheitssicht?“



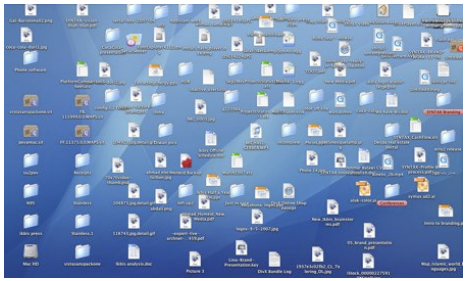
Ehrliche Antwort: „Schlimmer als der Status Quo wird es wohl nicht mehr kommen.“

Eine Sicherheitsbetrachtung von DMS in der öffentlichen Verwaltung sollte berücksichtigen, welche Altlasten beseitigt werden können.

Status Quo

Interviewergebnis (Kommunale Verwaltung):

- Wir halten Akten und wir verwalten Dateien.
- Dateien werden zu Ordnern zusammengefasst: Referate, Teams, Abteilungen; darunter: Sachgebiete, Personen, Jahreszahlen oder Vorgänge als Name.

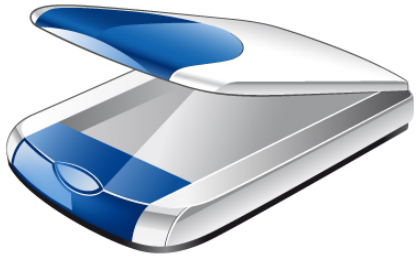


- „Jeder hat da sein System.“
- Die Zuordnung zwischen Akten und Dateien erfordert Sachkenntnis, jahrelange Erfahrung oder einfach großes Glück.

Status Quo (2)

Interviewergebnis (Kommunale Verwaltung):

- DMS haben wir schon lange. Aber nicht für unsere Akten und Dateien.
- (ausgehender) Schriftwechsel wird als Word-Dokument gespeichert.
- Neue Briefe sollten Dateien alter Briefe nicht überschreiben. Meist findet man neuere Versionen eines Dokumentes im selben Ordner.
- PDFs sind bei uns Scans eingehender Schriftstücke.
- Irgendwann soll die Ordnerstruktur reformiert werden.



Status Quo (3)

Interviewergebnis (Kommunale Verwaltung):

- Ein DMS, das eine Suche nach Stichworten, sachbezogenen Labels oder Semantiken ermöglicht, wäre toll.
- Wenn das bei uns eingeführt wird, funktioniert es aber ohnehin nicht und wir werden weiter die Ordner nebenher benutzen.
- Dateien gehen schon hin und wieder verloren, aber Akten auch. (Vieles taucht wieder auf.)

Status Quo (4)

Interviewergebnis (Kommunale Verwaltung):

- Datenschutz ist wichtig: Ausdrucke werden veraktet oder geschreddert.
- Löschfristen oder Löschvorgaben nach Wegfall des Erhebungszweckes bleiben unbeachtet.

- Auskunftsersuchen würde Justiziariat bearbeiten. Die kennen unsere Ordner nicht. (Besser so.)
- Zugriffsschutz über Ordnerprivilegien.
- Zugriffsprotokollierung unbekannt – oder wäre Fall für den Personalrat.

Status Quo (5)

Interviewergebnis (Kommunale Verwaltung):

- Vollständiges Ersetzen der Papierakte durch elektronische Akte / DMS erst, „wenn alle in Rente sind“.
- Löschen von Dateien zentral sinnvoll, aber mit Vorwarnung, um lokale Kopien zu ermöglichen.
- Lebenszyklus von Dokumenten wird analog zur Akte gesehen: Entweder in Benutzung – oder verstaubt in der Registratur.
- Langzeitarchivierung wird als Konzept akzeptiert.

Zwischenfazit

Der Amtsleiter, der den hier erhobenen Status Quo vorsätzlich herbeiführt oder duldet, steht (fast) „mit einem Bein im Gefängnis“.

(Nach BDSG „Freiheitsstrafe bis zu zwei Jahre oder eine Geldstrafe.“)

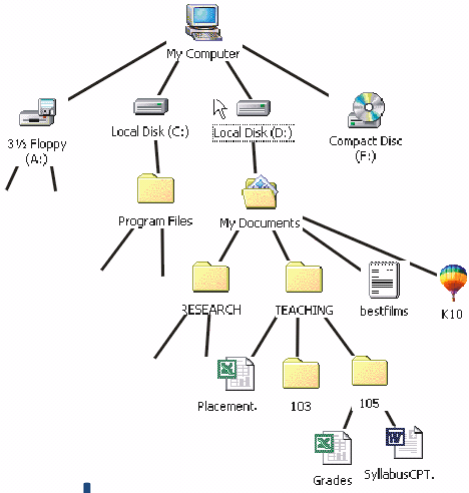
Voraussetzung für Strafbarkeit aber i. d. R. nicht erfüllt: „vorsätzliche Handlung gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern (…)“.

Zwischen-Folgerung

Eine Einführung von DMS ist bereits angezeigt, um den Status Quo hinsichtlich Datenschutzvorgaben, Integrität und Revisionssicherheit zu „reparieren“ und mangelnde Technikkompetenz auszugleichen.

Eine Alternative wäre:

- Strikte Vorgaben zur Dateihaltung (z. B. Benennung, Ordnerstruktur, Verschlagwortung, Konvertierung)
- Großprojekt: Reform des Datenbestandes (Aufheben der bisherigen Struktur)



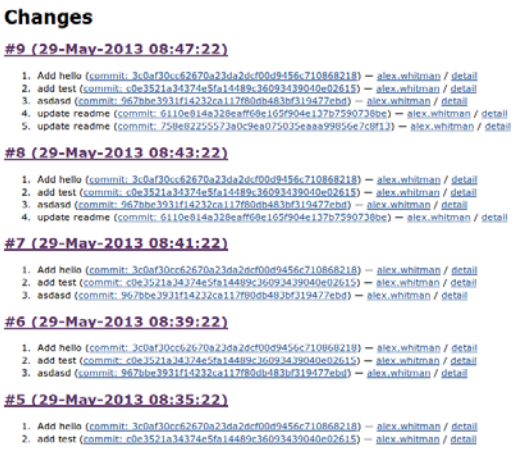
Vorteile einer DMS-Einführung aus Sicht von Datenschutz und –sicherheit

- (Besonders) Schutzwürdige Daten können ausgezeichnet werden (Zugriffsbeschränkung, Protokollierung, 4-Augen).
- Löschvorgabe oder Zweckbindungen können zugeordnet werden, ggf. automatisch durchgesetzt werden (Löschbarkeit, Löschvornahme durch DMS).
- Protokollierung des Zugriffs schafft Nachvollziehbarkeit und dämpft Missbrauchsverhalten.
- Mehrfachkopie des Datenbestandes kann vermieden werden.
- Geordneter, abgesicherter Zugriff über Netzgrenzen oder vom Heimarbeitsplatz wird möglich.

Aber: All das **kann** geschehen. Es geschieht in der Praxis **nicht**.

Vorteile einer DMS-Einführung aus Sicht von Datenschutz und –sicherheit (2)

- Recht auf Selbstauskunft / Akteinsicht kann nun technisch abgebildet werden.
- Änderungshistorie ermöglicht Korrekturen (Recht auf Berichtigung) und vermeidet Datenverlust.
- Rollen- und Rechtekonzepte filigraner als bei „Teamordnern“.
- Durchgehende Verschlüsselung (Speicherung, Transportweg) schutzwürdiger Daten wird möglich.
- Informationsfreiheitsrechte und Open-Data-Lösungen erhalten einen technischen Rahmen.



Risiken einer DMS-Einführung aus Sicht von Datenschutz und –sicherheit

- Lokale Kopie der Dateien wird befördert, wenn DMS die Nutzererwartungen nicht erfüllt.

- Missbrauch des Zugriffslogs durch Vorgesetzte oder Controller (Leistungskontrolle).
- Zusammenführen von Daten ermöglicht weitreichende Auswertung und Volltextrecherchen (bei Akten zu teuer).

- Diebstahl oder Verlust des Gesamtdatenbestandes in einem Vorgang.

Risiken einer DMS-Einführung aus Sicht von Datenschutz und –sicherheit (2)

- Digitalisierung schafft erst einzelne Problembereiche, die dann das DMS lösen soll → daher besser gleich eine Digitalisierung inkl. DMS-Einführung
- Eine vollständige Umstellung auf elektronische Akten / DMS trauen sich Verwaltungen nicht zu: Teilumstellungen führen aber zu mehr Risiken.
- Datenschutz wird schnell als „Showstopper“ verunglimpft, was den berechtigten Interessen zuwiderläuft.

Angriffsziel DMS

Für einen Angreifer („krimineller Hacker“, schwarzes Schaf unter den Beschäftigten etc.) ist das DMS-Backend (Datenbank) ein ideales Ziel:

- Alle Daten (Dateien, Dokumente) können als Gesamtbestand gestohlen oder vernichtet werden.
- Es genügt bspw., an ein unverschlüsseltes Tape zu gelangen.
- Die Auswirkungen (*Incident Impact*) wären ruinös.
- Bereits die Nichtverfügbakeit stellt einen erheblichen Schaden da.
- Ein eigenes Hosting des Servers ordnet die Verantwortung der Organisation selbst zu!

Absicherung: DMS

- Es gibt viele gute Gründe, das Hosting des DMS abzugeben, Sicherheit gehört dazu!
- Werden eigene DMS-Server betrieben, müssen Mindestanforderungen nach IT-Grundschutz beachtet und eine Risikoanalyse durchgeführt werden.
- Dies gilt aber gleichermaßen für bisher genutzte zentrale Fileserver: DMS ist hier nicht „das Problem“.
- Ein Client-/Web-basierter Zugriff mit Sicherheitstoken ermöglicht einen hohen Standard intern und bei Heimarbeitsplätzen / verteilten Beschäftigten.
- Es sollten Mechanismen greifen, die bei erheblichem Transaktionsvolumen den Zugriff sperren.

Fazit

- Der Status Quo (Akten plus „wilde“ Dateisammlung) ist nicht tragbar und zwingt zum Handeln (auch aus Gründen von Datenschutz und –sicherheit).
- Eine Einführung von DMS schafft oft neue Insellösungen mit weiteren Chancen **und Risiken**.
- Eine vollständige Umstellung auf DMS / E-Akten ist ein Projekt enormer Tragweite, das sich Verwaltungen i. a. nicht zutrauen oder das mit Fachverfahren (mit Systemvorgaben) kollidiert.
- Eine von den Anforderungen her *durchdachte* und hinsichtlich der Implementierung *gelungene* DMS-Umstellung verbessert Datenschutz und –sicherheit enorm. In der Praxis schafft das aber niemand (?).
- Für das DMS-Backend bzw. für die Serverinfrastruktur gelten erhöhte Sicherheitsanforderungen.

Vielen Dank!

Fragen?
Meinungen?

Kontakt:

Prof. Dr.-Ing. Ulrich Greveler

Fak. Kommunikation & Umwelt

Hochschule Rhein-Waal

http://www.hochschule-rhein-waal.de