HOCHSCHULE
RHEIN-WAAL
Rhine-Waal University
of Applied Sciences

Elektronische Akten in der Verwaltung? Die Fundgrube für Hacker!

Kamp-Lintfort Nov. 2015

Vortrag von Prof. Dr.-Ing. Ulrich Greveler

Gedanken zu Beginn …

- Wir haben heute viel über IT-Sicherheit in der Verwaltung gehört.
- Wollen wir die E-Akte überhaupt noch?
- Wie sicher ist Behörden-IT?

Bundestag-Hack war ein Phishing-Angriff über un.org

heise online 12.09.2015 19:06 Uhr vorlesen

Die Angreifer auf den Bundestag haben wohl Mails mit gefälschter Absendeadresse verschickt, die einen Link auf Malware enthielten. Nicht nur der Bundestag, sondern mehrere internationale Organisationen seien gleichzeitig angegriffen worden.

Beim Cyberangriff auf den Bundestag haben sich die Hacker einem Medienbericht …

Bundestag will sich vor "unberechtigtem Datenabfluss" besser schützen

heise online 07.11.2015 10:41 Uhr – Stefan Krempl vorlesen

Weniger Software mit beschränkten Rechten, Zwei-Faktor-Authentisierung, längere Passwörter und zeitlich begrenzte Rechte für den IT-Support sollen das Bundestagsnetz nach dem vor sechs Monaten aufgedeckten Hack sicherer machen.

Die für Informations- und Kommunikationstechnik (IuK) zuständige Kommission des Bundestags hat am Donnerstag ein neues Konzept zur IT-Sicherheit verabschiedet. Das zum Ältestenrat gehörende Gremium will damit auf den massiven Hackerangriff auf das interne Netzwerk Parlakom reagieren, das im Sommer zur Reparatur einige Tage heruntergefahren werden musste.

Laut den heise online vorliegenden Beschlussvorlagen setzt die Kommission auf ein Paket "zeitnaher" und mittelfristiger Maßnahmen. Zu ersteren gehört ein Auftrag für die Bundestagsverwaltung, Browser-Erweiterungen "zur Darstellung multimedialer Inhalte" zu deaktivieren. Dies betrifft den größtenteils ohnehin bereits ausgeschalteten Flash Player sowie die Pendants für Shockwave, QuickTime und Silverlight.

Vorurteile oder Thesen?

- Behörden-IT ist veraltet.
- Behörden-IT ist unzureichend administriert.
- Behörden-IT unterliegt ungeeigneten Beschaffungsprozessen.
- Behörden-IT ist unflexibel bei Anforderungsänderungen.

Rem0te
@grauhut

Folgen

Kollege: "Gibt es noch eine Steigerung für 'Enterprise-Level'?"
"Government. Doppelt so teurer und funktioniert gar nicht."

RETWEETS 25 GEFÄLLT 22

13:22 - 16. Nov. 2015

Antwort an @grauhut

ciacon @ciacon · 27 Min.
@grauhut ...gibt's da was von T-Systems?

2

12 Jahre Vorbereitung reichten nicht

Microsoft hatte die technische Unterstützung für das 13 Jahre alte Betriebssystem vor einem Jahr (8. April 2014) nach langer Vorlaufphase eingestellt. Danach hat Microsoft keine Sicherheitsupdates und Aktualisierungen mehr für XP veröffentlicht. Der **Fahrplan** für das Support-Ende war von dem Konzern bereits im Jahr 2002 erstmals angekündigt worden.

Da die Berliner Verwaltung die Ablösung der betagten PCs nicht rechtzeitig umsetzen konnte, hatte das IT-Dienstleistungszentrum Berlin (ITDZ) für 300.000 Euro einen verlängerten Support mit Microsoft vereinbart. Dieser läuft am Dienstag aus. Das ITDZ will ein Virenschutzprogramm für XP noch bis Ende 2015 zur Verfügung stellen.

2014 liefen noch 28.477 Computer mit Windows XP

Der Datenschutzbeauftragte Dix sagte, er wisse nicht genau, wie viele PCs noch betroffen seien. Der Senat hatte die Zahl der XP-Rechner zuletzt im März 2015 in einer Antwort auf eine Anfrage der Piraten-Fraktion mit 28.477 angegeben (Stand 31. Oktober 2014).

Quelle: Berliner DSB 2015

IT-Fachkräftemangel im öff. Dienst

- IT-Kräfte branchenübergreifend begehrt
- Eingruppierung oft nicht konkurrenzfähig zu privaten Arbeitgebern
- Weiterqualifizierung eher schwach
- Veraltete Systeme führen zu Know-How-Mangel bei Beschäftigten („Marktwert“ sinkt)
- Beobachtung:
  „Neid“ ggü. Dienstleister-Beschäftigten.

Die **Stadt** [redacted] sucht

eine/n Mitarbeiter/in für den IT-Bereich

zur Administration und Betreuung von Netzwerken, Servern, virtueller Umgebung, Sicherheitssystemen, Datenbanken, Telefonanlagen, PC - Arbeitsplätzen und der entsprechenden Standard- und Fachbereichssoftware. Dazu gehören insbesondere auch Installationen, Anwenderunterstützung und flexible und zuverlässige Problem- und Fehlerbehebung.

Erwartet werden selbstständiges Arbeiten, Organisationstalent, Team- und Konfliktfähigkeit, Kommunikationsstärke und Einsatzbereitschaft.

Wünschenswert sind abgeschlossene IT-Ausbildung **(z. B. Fachinformatiker)** und Kenntnisse öffentlicher Verwaltungsstruktur. Gerne können sich auch **Verwaltungsfachangestellte** oder andere Fachkräfte öffentlicher Verwaltungen bewerben, die bereits Erfahrung mit EDV-Betreuung haben.

Das unbefristete Beschäftigungsverhältnis in Vollzeit mit 39 Wochenstunden richtet sich nach dem TVöD für den Bereich VkA. Die Vergütung richtet sich nach der vorhandenen Qualifikation.

Bitte schicken Sie Ihre aussagefähige Bewerbung **bis 14.12.2015** an die

[redacted]

"Wir haben in den Landesbehörden noch nicht flächendeckend IT-Sicherheitsbeauftragte."
H. Beuß, CIO NRW, 17.11.15 Vortrag @HochschuleRW

11:26 - 17. Nov. 2015

Kamp-Lintfort, Nordrhein-Westfalen

Aktuelle Zitate dazu

(Zum Thema IT-Fachkräftemangel)
"Niemand in der öffentlichen Verwaltung leidet Hunger."
H. Beuß, CIO NRW, 17.11.15 Vortrag @HochschuleRW

11:27 - 17. Nov. 2015

Kamp-Lintfort, Nordrhein-Westfalen

"Die Mitarbeiter von IT.NRW tragen alle 'Goldenen Regeln der Informationssicherheit' in der Tasche."
Vortrag @HochschuleRW

13:49 - 17. Nov. 2015

Kamp-Lintfort, Nordrhein-Westfalen

E-Akte (Beispielprospekt, Ausschnitt)

Für die Akzeptanz der E-Akte ist Softwareergonomie und Benutzerfreundlichkeit entscheidend. Die [redacted] E-Akte verfügt über zahlreiche Funktionen, die Benutzer in ihrer Arbeit unterstützen:

- Baumansicht
- Eingebettete Vorschaufunktion von Dokumenten
- Übersichtliche, individuelle Startseite mit den letzten Ereignissen und aktuellen Aufgaben
- Drag&Drop-Funktionen zum Import und innerhalb der E-Akte

Die [redacted] E-Akte fügt sich in die existierende Office-Umgebung nahtlos ein. So können die Anwender in ihrer gewohnten Umgebung arbeiten:

- Online-Bearbeitung von Office-Dokumenten
- Integration des Aktenplans in den Windows Explorer
- Integration des Aktenplans in den E-Mail Client (z.B. Microsoft Outlook) zur Ablage von E-Mails

Moment mal, bitte …
Welche Anforderungen?

- Integration in Explorer
- Bearbeitung mit Office
- Verlinkung zu Outlook

Diese Features werden zwar oft gewünscht, bedeuten aber meist, dass die E-Akten lokal am PC vorliegen und dort bearbeitet, gespeichert, kopiert, etc. werden können.

Virtuelle Desktops & Web-basierte Lösungen

- Ein virtueller Desktop wird auf einem Remote-Server gespeichert, nicht lokal.
- Web-Anwendungen erlauben die Bearbeitung allein per Browser, unabhängig von SW + OS, ggf. auch per Tablet.
- Vorteile: zentrales Backup, Archivierung, Daten-Integrität, kontrollierte Interfaces zu Druckern, Mail, Fileablagen; geringe HW-Abhängigkeit, keine lokale Administration.
  Sicherheitsgewinn für sensible Daten!
- Nachteil: Performance-Einschränkungen, insb. bei langsamen Netzverbindungen

Ausgangslage

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

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

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

Status Quo

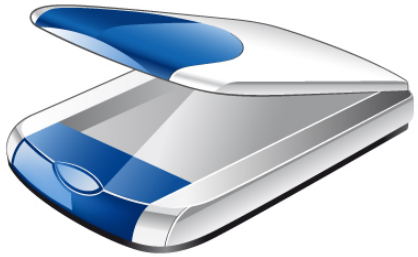
Interviewergebnis (Befragungen kommunaler Verwaltungen; Nov. 2014 - Jan. 2015):

- 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 E-Aktensystem oder 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):

- 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 E-Dokumenten wird analog zur Akte gesehen: Entweder in Benutzung – oder verstaubt in der Registratur.
- Langzeitarchivierung wird als Konzept akzeptiert.

Vorteile von E-Akten 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 System).
- 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**.

Risiken einer E-Akten-Einführung aus Sicht von Datenschutz und –sicherheit

- Lokale Kopie der Dateien wird befördert, wenn System 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.**

Angriffsziel: „Fundgrube“

Für einen Angreifer („krimineller Hacker“, schwarzes Schaf unter den Beschäftigten etc.) ist das E-Akten-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 Nichtverfügbarkeit stellt einen erheblichen Schaden da.
- Ein eigenes Hosting des Servers ordnet die Verantwortung der Organisation selbst zu!

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

- Digitalisierung von Papier schafft erst einzelne Problembereiche, die dann ein System lösen soll → daher besser gleich E-Prozesse und E-Akten von Beginn an
- 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.

Exkurs: Sprachregelungen und ihre tatsächliche Bedeutung

- „Das geht aus Datenschutzgründen nicht.“
  = „Wir wollen das nicht umsetzen oder sind technisch dazu nicht befähigt.“
- „Das muss Datenschutz-technisch überprüft werden.“
  = „Wir möchten das vielleicht umsetzen, aber es geht uns alles zu schnell. Weihnachten steht vor der Tür.“
- „Wir haben eine Projektgruppe eingerichtet und den Datenschutzbeauftragten beteiligt.“
  = „Wir werden das einführen, egal ob die User es wollen oder nicht.“

Sprachregelungen und ihre tatsächliche Bedeutung (2)

- „Das System wird nur im Pilotbetrieb eingesetzt und läuft derzeit inoffiziell.“
  = „Wir machen das, obwohl es aus Datenschutzgründen nicht geht.“
- „Die Systemeinführung wurde mit der Amtsleitung und dem Personalrat abgestimmt.“
  = „Wir fragen den Datenschutzbeauftragten erst gar nicht.“
- „Der Landesdatenschutzbeauftragte wurde involviert.“
  = „Wir werden bald wissen, ob das System den Datenschutz verletzt.“

Datenschutzbeauftragte/r

Zwischenruf

Warum es von Vorteil sein kann,
Informatiker/innen zum DSB zu machen:

- Es ist wichtiger, Daten technisch zu schützen als faktische Datenschutzverletzungen durch mehr oder weniger freiwillig geleistete Zustimmungserklärungen zu legitimieren.

Absicherung: E-Akte

- Es gibt viele gute Gründe, das Hosting des Systems abzugeben, Sicherheit gehört dazu!
- Werden eigene Server betrieben, müssen Mindestanforderungen nach IT-Grundschutz beachtet und eine Risikoanalyse durchgeführt werden.
- Dies gilt aber gleichermaßen für bisher genutzte zentrale Fileserver: E-Akten-System 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.

Sprachregelungen und ihre tatsächliche Bedeutung (3)

- „Wir orientieren uns am IT-Grundschutz.“
  = „Wir tun, was wir können und hoffen, dass es sicher ist.“
- „Wir werden nur zertifizierte Systeme in Betracht ziehen.“
  = „Wir wollen eigentlich kein neues System einführen.“
- „Wir werden nur Systeme betreiben, die wir selbst unter voller Kontrolle haben. Wir nutzen nur private Leitungen. 100%ige Sicherheit gibt es ohnehin nicht.“
  = „Wir haben keine Ahnung von IT-Sicherheit.“

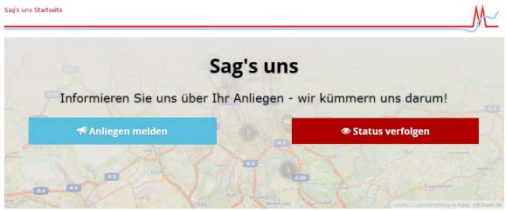
Fazit 1: Ein unsicherer Weg zur E-Akte

- Amtsleitung oder übergeordnete Behörde entscheidet: Wir wollen E-Akten einführen.
- Papierakten werden ersetzend gescannt. Akten liegen nun im DMS/E-Akte-System vor.
- System wird *inhouse* betrieben und von IT-Beschäftigten administriert.
- Backup „liegt im Keller“.
- „Private Kopien“ wichtiger Daten liegen auf Shares und Einzelplatz-PCs.
- Erfolgreiche Hacker haben zentralen Zugriff auf alle Akten bzw. große Bestände „privater Kopien“.

Fazit 2: Ein besserer Weg zur E-Akte

- E-Akten entstehen ohne Papierumweg aus elektronischen Verfahren (z. B. E-Vergabe, E-Government-Portal, Bürger-Anliegen-System / Beschwerde-App.)
- Scannen findet nicht statt. Wer PDFs ausdruckt, stempelt oder beschriftet und wieder einscannt, wird zur Amtsleitung gebeten!
- System wird außerhalb des Amtes von vertrauenswürdiger Institution gehostet (z. B. IT NRW, KRZN, Dienstleister) und administriert.
- Hacker können dann nur einzelne Zugänge (z. B. PC-Arbeitsplätze) kapern oder müssen das „große Ziel“ anvisieren.

Deutsche eVergabe



Gesamt-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 E-Akten 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* Umstellung verbessert Datenschutz und –sicherheit enorm.**
  In der Praxis schafft das aber fast (?) niemand.

Vielen Dank!

Fragen?
Meinungen?

Kontakt:

Prof. Dr.-Ing. Ulrich Greveler

Fak. Kommunikation & Umwelt

Hochschule Rhein-Waal

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