4/2011 Verwaltung INNOVATIV

Herausgegeben vom Führungsforum Innovative Verwaltung

EDITORIAL
Heidrun Strohmeyer

Fotostudio Willibald Haslinger

Hackerangriffe versus Verwaltungs-Apps — der Umgang mit Informationen als Führungsaufgabe?

Verwaltung INNOVATIV ist diesmal dem Schwerpunkt Daten – ihrer Sicherheit, aber auch ihrer kreativen Verwertung – gewidmet. Das ist keine Frage der Technik, sondern durchaus ein Thema für innovatives Verwaltungsmanagement: Transparenz und Effizienz sind die Grundlage für die Schaffung einer europaweit einheitlichen Geodateninfrastruktur. Was so knochentrocken klingt, birgt als INSPIRE-Richtlinie enormes Potenzial für Serviceleistungen am Bürger. Wer wünscht sich nicht, per App am Smartphone über die aktuelle Umweltbelastung (z. B. Feinstaubwerte) informiert zu sein oder während des Sonntagsausflugs Details über denkmalgeschützte Objekte in der Umgebung zu erfahren?

Der Freiheit der Nutzung offener Daten steht der Anspruch nach Sicherheit und Schutz, vor allem von personenbezogenen Daten, gegenüber. Die technischen Anforderungen sind meist unschwer zu erfüllen, organisatorische Aspekte und der Faktor „Mensch" müssten in der aktuellen Diskussion um Datensicherheit aber stärker berücksichtigt werden. Bei näherer Betrachtung sind es oft keine technischen Gründe, dass interne Informationen und schützenswerte Daten öffentlich werden. Achtlosigkeit oder absichtliche Weitergabe als häufige Ursache zeigen, dass hier die Führungskräfte verstärkt gefordert sind. Loyalität und Verantwortungsbewusstsein der MitarbeiterInnen kennzeichnen schließlich eine gute Unternehmenskultur.

Apropos Kultur: Das FIV hat selbst Neuland betreten und sich kulturell betätigt: Jan Banning, ein niederländischer Künstler, hat BeamtInnen rund um den Erdball in ihrer Arbeitsumgebung fotografiert. Das FIV zeigt diese sozialdokumentarischen Bilder in einer eigenen Ausstellung. Bitte anschauen und weitersagen!

Ihre

Heidrun Strohmeyer
Präsidentin des Führungsforums Innovative Verwaltung
heidrun.strohmeyer@bmukk.gv.at

Informationssicherheit im Fokus

Die Aktivitäten der Hackergruppe „AnonAustria" haben ein erstaunliches mediales Echo erhalten. Viele Entscheidungsträger stellen sich nun die Frage, was sie tun können, um Informationen vor möglichem Fremdzugriff und ungewollten Veröffentlichungen zu schützen.

TEXT: A MIN TJOA, MARKUS KLEMEN

PHOTOS.COM

Vereinfacht dargestellt, müssen drei Ebenen adressiert werden: die menschliche, die organisatorische und die technische Ebene. In der Praxis wird die technische Ebene in ihrer Bedeutung häufig überbewertet, die menschliche und organisatorische Ebene eher unterbewertet, wie wir nachfolgend darstellen werden.

Ein weiterer ganzheitlicher systematischer Ansatz dieser Fragestellung kann durch Klassifikationen vorgenommen werden: Klassifikationen nach Urheber bzw. Ursache („wer"), nach Motivation, Intention, Absicht („warum"), nach Tätigkeit („wie"), nach Wahrscheinlichkeit und Häufigkeit („wie oft"), nach bedrohtem Objekt („was"), nach Schadenshöhe („wie viel") oder nach Art der Grundbedrohung. In einer umfassenden Bedrohungsanalyse sollten alle Ausgangspunkte

Zu adressierende Ebenen bei Institutionen und Unternehmen

- Menschliche Ebene
- Organisatorische Ebene
- Technische Ebene

Interne Urheber

- Benutzer
- Privilegierte Benutzer
- Administratoren
- Entscheidungsträger

Externe Urheber

- Hacker
- Partner, Kunden
- Konkurrenten
- Nachrichtendienste

berücksichtigt werden, an dieser Stelle sollen nur die drei relevantesten Punkte näher beleuchtet werden:

Urheber einer Bedrohung

Auch wenn in den letzten Wochen der „Hacker" zum Hauptverursacher von Datenverlusten medial stilisiert wurde, ist dies zu relativieren. Zwar gibt es wenig belastbare Studien zu diesem Thema, da die meisten Institutionen und Unternehmen dazu auch nur sehr ungern Auskunft geben, aber ohne Zweifel geht ein Großteil der Datenverluste auf Fehler oder absichtliche Fehlhandlungen von Mitarbeitern zurück. Dieser Umstand wird von Institutionen und Unternehmen immer noch häufig tabuisiert, nach dem inhärenten Dogma „Unsere Mitarbeiter machen keine Fehler und sind vertrauenswürdig". Da Datenveröffentlichungen durch Insider auch medial nur wenig Aufmerksamkeit erregen, wird dieser wichtige Aspekt in der Praxis extrem unterschätzt. Das ist insofern interessant, als auch die jüngsten Aktivitäten von AnonAustria wenig mit technisch ausgefeilten externen Angriffen zu tun hatten und mehr mit dem Auffinden von Informationen, die über verschiedene Kanäle in die weite Welt der öffentlich zugänglichen Datennetze gelangt waren. Mehrere „Hackerangriffe" stellen sich bei genauerer Analyse als Veröffentlichung durch Insider dar. So war die Veröffentlichung von Namen und Adressen von zahlreichen Unterstützern der Polizei kein Hackerangriff, vielmehr wurden diese Informationen AnonAustria „zugespielt". Trotzdem wurde dies in den Medien zunächst als „Hackerangriff" dargestellt.

Die Bewusstseinsbildung bei den Mitarbeitern ist daher eine wichtige Weiterbildungsmaßnahme, um den Wert der Daten zu verdeutlichen, um mögliche Fehlerquellen durch Benutzer zu minimieren und um die Aufmerksamkeit im Umgang mit vertraulichen Daten zu schärfen.

Ursache einer Bedrohung

Das Hinterfragen der Ursache einer Bedrohung von Informationssystemen lässt sich gut den bereits erwähnten drei Ebenen zuordnen: Eine Ursache können Fehleingaben (z. B. irrtümliches Veröffentlichen), unbewusste Fehlhandlungen (Reagieren auf ein Phishingmail, Klicken auf einen falschen Link, falsche Reaktion auf eine Social-Engineering-Attacke) oder bewusste Fehlhandlungen (Zuspielen von Informationen, Verkauf von Informationen) von Insidern sein – dies ist auf der menschlichen Ebene angesiedelt.

Eine weitere Ursache können schlecht definierte oder unvollständige Organisationsprozesse sein (Beispiel: Ist ein Prozess definiert, der vor einer Entsorgung von Massenspeichern die vollständige Löschung sicherstellt? Gibt es ein Vier-Augen-Prinzip bei Zugriffen von Systemadministratoren auf Datenbanken mit sensiblen Daten?). Hier können Informationssicherheitsaudits helfen, Lücken zu schließen. Diese sollten sich an etablierten Standards orientieren, wie etwa dem Österreichischen Sicherheitshandbuch, dem deutschen Grundschutzhandbuch oder dem ISO-27001-Standard.

Als dritte Ursache sind technische Schwachstellen und Fehler zu adressieren. Das können fehlerhafte (Sicherheits-) Einstellungen auf Arbeitsstationen, Servern oder Netzwerkinfrastrukturgeräten, schlecht programmierte Webseiten oder fehlerhafte Software sein. Dabei ist in der Regel das Problem der fehlerhaften Software als Grundursache einzustufen, die mit anderen technischen Hilfsmitteln (z. B. Web-Application-Firewalls zum Schutz von Webseiten) überdeckt wird. Hier sind zwei Arten von Gegenmaßnahmen anzuführen:

Was voreilig als „Hackerangriff" gilt, ist nicht selten eine Veröffentlichung durch Insider.

Einerseits können die Anbieter von Softwareprodukten versuchen, ihre Software möglichst frei von ausnützbaren Schwachstellen zu entwickeln. Aufgrund von Kostendruck, Zeitdruck und anderer Fehler, die unmittelbar als wichtiger angesehen werden, werden Sicherheitsaspekte bei Software leider noch viel zu häufig vernachlässigt. Hier liegt es primär an den Kunden, Sicherheit bei der Entwicklung einzufordern. Österreich ist insofern international führend, als es eine Önorm gibt, die die Sicherheitsqualität von webbasierter Software durch externe Audits sicherstellen soll (A7700). Bislang hat sich diese Norm aber leider noch nicht ausreichend etabliert.

Andererseits können Softwaresicherheitsüberprüfungen (z. B. externe Penetrationstests von Webseiten, bei denen ein Sicherheitsdienstleister in der Rolle eines Hackers versucht, in ein System einzudringen und dieses im Extremfall zu übernehmen) helfen, Schwächen und Probleme aufzufinden und damit den Herstellern die Möglichkeit zu geben, diese zeitgerecht auszumerzen. Dieser Ex-Post-Ansatz ist zum momentanen Zeitpunkt das Hauptinstrument der Firmen und Institutionen, um ihre Sicherheitslage und den „exposure factor", also das Ausmaß, in dem sie nach außen datensicherheitsmäßig exponiert sind, einzuschätzen und Gegenmaßnahmen einzuleiten.

Das bedrohte Objekt

Welche Informationen sind in einer Institution eigentlich schützenswert? Diese einfach klingende Frage stellt sich in der Praxis als komplexes Problem heraus. Zwar sind einige Datenbestände schnell als vertraulich klassifizierbar (z. B. Lohn- und Gehaltsdaten, Patientendaten). Den gesamten Datenbestand einer größeren Institution durchzuarbeiten und entsprechend zu klassifizieren ist hingegen eine organisatorische und aufwandstechnische Herausforderung, bei der auch die Forschung Aufholbedarf hat. Dabei ist gerade dieser Schritt eine wichtige organisatorische Maßnahme, um darauf folgende technische Maßnahmen erfolgreich umzusetzen. So finden sich seit nunmehr einigen Jahren Softwarelösungen zum Schutz vor Datenlecks unter dem Schlagwort „Data Leakage Prevention". Doch bislang finden sich wenige Success-Storys. Geht man den Ursachen genauer auf den Grund, stellt sich meistens heraus, dass die Frage, welche Daten in welchem Ausmaß mit welchen technischen Maßnahmen beschränkt werden sollen, im Vorfeld nicht ausreichend geklärt wurde. Damit müssen in der Folge so viele Ausnahmeregeln geschaffen werden, dass die Sicherheitswirkung der Maßnahme wieder erheblich reduziert wird.

Fazit

Auch wenn die mediale Aufmerksamkeit der letzten Monate den „Hacker" als primäre Gefahr darstellt, so ist dies eine zu starke Reduktion auf einen einzelnen Verursacher. Vielmehr muss eine Organisation sicherheitstechnisch ganzheitlich analysiert werden, um langfristig eine deutliche Verbesserung des Informationssicherheitsniveaus zu erreichen.

PROF. DR. A MIN TJOA ist Obmann des Forschungszentrum Secure Business Austria Research (SBA Research) und Leiter des Instituts für Softwaretechnik der TU Wien.

MAG. MARKUS KLEMEN ist seit der Gründung des Forschungszentrums SBA Research Geschäftsführer und hat davor an der TU Wien Vorlesungen zu technischen und organisatorischen Sicherheitsaspekten gehalten.

Achtung, Attacke!

Die Aktionen der Gruppe „Anonymous" haben auch in Österreich für Aufmerksamkeit gesorgt: Hacker-Attacken und Datenverlust können nur durch vorbeugende Datensicherheitsmaßnahmen verhindert werden. Die datenschutzrechtlichen Auftraggeber – öffentliche wie private – sollten diesbezüglich in die Pflicht genommen werden.

TEXT: EVA SOUHRADA-KIRCHMAYER

PHOTOS.COM

Aufruhr verursachte die Gruppe AnonAustria durch Hacking-Angriffe.
Für die DSK ist klar: Die Einhaltung der Datensicherheit ist eine Verpflichtung!

Die österreichische Gruppe AnonAustria bekannte sich auf der einen Seite zu einigen Hacking-Angriffen, zum Beispiel auf die Websites einiger politischer Parteien, aber auch die der Gebühren Info Service GmbH (GIS); andererseits gelangte sie vermutlich auch auf andere Weise in den Besitz von Daten: So veröffentlichte AnonAustria Daten von Exekutivbeamten, die der Gruppe angeblich zugespielt worden waren. Wenige Tage später teilte die Gruppe mit, dass man über eine Datenbank der Tiroler Gebietskrankenkasse „gestolpert" sei. Zu Beunruhigung führte in weiterer Folge auch die Tatsache, dass sich Hacker Zugang zu Webseiten, die von der Bundesrechenzentrum GmbH gehostet wurden, verschafft hatten. Weiters veröffentlichte AnonAustria Kundendaten der Wirtschaftskammer Österreich.

Was sagt das Gesetz?

Das österreichische Datenschutzgesetz (DSG 2000) enthält in § 14 Bestimmungen zur Datensicherheit. Zur Ergreifung von Datensicherheitsmaßnahmen sind sowohl der Auftraggeber einer Datenanwendung als auch allenfalls herangezogene Dienstleister verpflichtet. Gemäß § 14 Abs. 1 DSG 2000 sind für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden, Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. „Dabei ist je nach der Art der verwendeten Daten und nach Umfang und Zweck der Verwendung sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit sicherzustellen, daß die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind." Des Weiteren werden in § 14 auch Maßnahmen ausgeführt, die zu treffen sind (wie z. B. die Regelung der Zutrittberechtigungen zu den Räumlichkeiten und der Zugriffsberechtigungen und die Protokollierungen von Verwendungsvorgängen).
Mit Leben erfüllt wurde nunmehr auch die seit 2010 im Datenschutzgesetz 2000 verankerte Verpflichtung zur Meldung von Datensicherheitsverletzungen („data breach notification") beim Vorliegen von systematisch und schwerwiegend unrechtmäßigen Datenverwendungen, wenn den Betroffenen Schaden droht.
Davon abgesehen kann hier auch strafbares Verhalten vorliegen: Neben gerichtlich strafbaren (Computerkriminalitäts-) Tatbeständen im Strafgesetzbuch und im DSG 2000 (Datenverwendung in Gewinn- oder Schädigungsabsicht) existiert eine Verwaltungsstrafbestimmung (§ 52 Abs. 2 Z 5 DSG 2000), nach der das gröbliche Außer-Acht-Lassen der erforderlichen Datensicherheitsmaßnahmen strafbar ist.

Geheimhaltung wahren

Die Datenschutzkommission hat zwar Prüfverfahren eingeleitet, kann aber im Bereich der informellen Verfahren bestenfalls Empfehlungen aussprechen. Verbindliche Entscheidungen kann die Datenschutzkommission etwa dann treffen, wenn ein Betroffener wegen Verletzung seines Grundrechts auf Datenschutz gegen einen öffentlichen Auftraggeber Beschwerde erhebt.
Eine nachprüfende Kontrolle kann vorbeugende Datensicherheitsmaßnahmen nicht ersetzen. Die Einhaltung der Datensicherheit ist eine Verpflichtung, die Auftraggeber und Dienstleister einer Datenanwendung trifft. Diese müssen sich über ihre Verantwortung im Klaren sein und sollten auch nachvollziehbar machen, dass sie alles getan haben, um die Geheimhaltungsinteressen der Betroffenen zu wahren.

DR. EVA SOUHRADA-KIRCHMAYER ist geschäftsführendes Mitglied der Datenschutzkommission und Leiterin der Geschäftsstelle der Datenschutzkommission. Sie ist Juristin und seit 1991 im Datenschutzbereich tätig.

BSK

Schutz vor Hacktivismus

Große Konzerne, Verwaltungsdienststellen, das Militär und politische Parteien – sie alle waren in den vergangenen Monaten vor Angriffen auf IT-Systeme nicht gefeit. Einen wesentlichen Teil der Datenverluste verursachen Insider. Warum ist das so? Und warum ist es so gefährlich? Johannes Mariel vom Bundesrechenzentrum gibt Antworten.

TEXT: JOHANNES MARIEL

Zahlreiche Angriffe auf IT-Systeme sorgten in den vergangenen Monaten für Schlagzeilen. Die Veröffentlichung von Angriffen, meist verbunden mit der Preisgabe von gestohlenen Daten, wird mit dem Begriff „Hacktivismus" bezeichnet. Diese Angriffe werden häufig mit einem politischen oder sozialen Anliegen verknüpft, das zur Rechtfertigung der kriminellen Vorgangsweise benutzt wird. Tatsächlich erzielt die organisierte Kriminalität in diesem Geschäftszweig ähnliche Umsätze wie beim Drogenhandel.

Schützen – aber was?

Der Schutz der Sicherheit in einem Rechenzentrum beginnt idealerweise bei der Informationssicherheit. Mit diesem Begriff wird die Information in jeder Form in den Mittelpunkt der Sicherheitskonzepte gestellt. Information kann in technisch lesbarer Form als Daten in IT-Systemen, aber auch auf Datenträgern wie Festplatten, USB-Sticks oder Smartphones vorliegen. In der Welt von Web 2.0 und Cloud-Computing, die auch für E-Government und E-Business eingesetzt werden, sind zunehmend auch die Daten auf Webservern im Fokus der Attacken.

„Data-Leakage", also Veröffentlichungen von internen Informationen, stellen ein weiteres Sicherheitsproblem dar. Die Ursachen reichen von achtlos weitergeleiteten vertraulichen E-Mails über unbedachte Aussagen auf öffentlichen Präsentationen bzw. bei Interviews bis zu euphorischen Presseaussendungen. Aber auch das Wissen der Mitarbeiter stellt eine enorme Datenmenge dar, die durch Angriffsmethoden wie „Social Engineering" (auf gut wienerisch „Aushorchen") angezapft wird, um beispielsweise Passwörter auszukundschaften. Die sehr häufig freizügig angebotenen persönlichen Informationen in Facebook und Co erleichtern Kontakte mit Mitarbeitern, die dann oft in bester Absicht vertrauliche Informationen weitergeben.

Schützen – aber wie?

Die Gewährleistung der Sicherheit erfordert präventive und reaktive Maßnahmen, die abgestimmt zusammenwirken. In der Vorbeugung sind technische Maßnahmen einzusetzen, die durch geeignete Prozesse laufend aktualisiert und überwacht werden. Dazu zählen bekannte Grundschutzmaßnahmen wie Virenschutz oder Firewalls. Neben der technischen Implementierung muss sichergestellt werden, dass täglich Updates erfolgen. High-Level-Maßnahmen wie Intrusion-Prevention-Systeme für Netze und Server überwachen aufgrund von bekannten Mustern, die Angreifer verursachen, den Netzwerk- und Serverbetrieb. Sie können entweder alarmieren oder in definierten Fällen sogar automatisch abschalten. Ein wesentlicher Baustein im Sicherheitskonzept bildet das Berechtigungssystem, das die Zugriffe auf die Informationen erlaubt. Der Grundsatz „Need to Have" bildet die Leitlinie. In der Praxis stellt uns die Gratwanderung zwischen Flexibilität der Organisation und Komfort des Benutzers versus Sicherheit der Informationen täglich vor neue Herausforderungen.

PHOTOS.COM

Die genannten Beispiele und viele weitere Sicherheitsmaßnahmen können keinen absoluten Schutz bieten. Deshalb umfasst ein Sicherheitskonzept auch Maßnahmen zur aktiven Abwehr von Angriffen. Zur raschen Wiederherstellung von beschädigten IT-Systemen braucht es in erster Linie einen Business-Continuity-Plan.

Die BRZ GmbH verwendet als Grundlage des Sicherheitskonzepts den internationalen Sicherheitsstandard ISO 27001. Das Informationssicherheits-Managementsystem der BRZ GmbH ist seit 2005 zertifiziert und wird jährlich durch ein umfassendes Audit geprüft.

Magisches Dreieck

Veränderungen im Userverhalten – wie dies mit der Anforderung an mobile Arbeitsplätze zurzeit aktuell ist – gehen mit technologischen Änderungen (z. B. Smartphones) einher.

Im „magischen Dreieck der Sicherheit", dem Spannungsfeld zwischen Usability, Kosten und Sicherheit, ist daher auch mit Kompromissen und Restrisiken zu agieren. In der Vergangenheit wurden Entscheidungen immer wieder kostendominiert getroffen, aber die Lernkurve führt durch die Vorfälle zur Reduktion des Risikopotenzials. Bei der Cyberconference in London am 1. 11. 2011 brachte Howard Schmidt, der Cyber Security Coordinator der Obama Administration, diese Erkenntnis mit knappen Worten auf den Punkt: „Cyber Security kostet Geld. Fehlende Cyber Security kostet mehr Geld."

www.brz.gv.at

ING. JOHANNES MARIEL ist Chief Security Officer (CISCO) und Leiter der Stabsstelle Sicherheit und Qualität im Bundesrechenzentrum (BRZ). Zuvor war er zwei Jahre als Referent in der Stabsstelle für IKT-Strategien des Bundes im Bundeskanzleramt tätig.

BRZ

Die INSPIRE-Richtlinie soll die Nutzung von Geodaten erleichtern. Sie ist damit ein Schritt zur transparenten Verwaltung.

Einheitliche Geodateninfrastruktur dank INSPIRE

Datenlücken, fehlende Dokumentation und unterschiedliche räumliche Bezugssysteme soll es dank INSPIRE-Richtlinie nicht mehr geben. Doch INSPIRE schafft nicht nur eine einheitliche Geodateninfrastruktur. Sie ist auch ein Beitrag zur Open-Government-Initiative.

TEXT: REINHARD MANG, ANDREAS REITHOFER

Mit der Ratifizierung der Richtlinie 2007/2/EG durch das Europäische Parlament am 13. 2. 2007 trat am 15. Mai des gleichen Jahres die INSPIRE-Richtlinie zur Schaffung einer einheitlichen Geodateninfrastruktur in Kraft. Ihr erklärtes Ziel ist es, qualitativ hochwertige Geodaten aus den Behörden der einzelnen Mitgliedstaaten unter einheitlichen Bedingungen zur Unterstützung der Formulierung, Umsetzung und Bewertung europäischer und nationaler Politikfelder zugänglich zu machen. Im Umweltbereich, aus dem die Initiative hervorging und welcher auch heute noch den Schwerpunkt bildet, schafft dies die Voraussetzungen für eine proaktive grenzüberschreitende Gestaltung des Umwelt- und Naturschutzes sowie das Monitoring der ergriffenen Maßnahmen und deren Erfolge. Auch eine kurzfristige, abgestimmte Reaktion auf grenzüberschreitende Katastrophen soll durch INSPIRE vereinfacht werden.

Publish – find – bind

Die Ausgangsproblemstellung lag vor allem in bestehenden Datenlücken, fehlender Dokumentation, inkompatiblen Datenformaten sowie unterschiedlichen räumlichen Bezugssystemen, welche eine grenzüberschreitende Aufbereitung und Weitergabe von Geodaten behinderten. Diese Mängel sollen durch die INSPIRE-Richtlinie schrittweise behoben werden. Nach dem von INSPIRE postulierten Prinzip des „publish – find – bind" sollen Metadaten und Geodaten publiziert, gesucht und ins eigene System eingebunden werden.

Ein erster großer Schritt dazu ist die Einrichtung eines EU-weiten Geodatenportals, in das sämtliche von der INSPIRE-Richtlinie in den Annexen I, II und III geregelten Metadaten verfügbarer Geodatensätze der EU-27 eingepflegt bzw. verfügbar gemacht werden. Diese Metadaten (nicht jedoch die Geodaten selbst) müssen allen Verwaltungsinstitutionen sowie auch privaten Firmen und Bürgern kostenlos zur Verfügung gestellt werden.

Die Prinzipien für die Umsetzung folgen einerseits dem Subsidiaritätsprinzip und andererseits dem Transparenz- und Effizienzprinzip. Danach ist jede INSPIRE-pflichtige datenführende Stelle selbst für die richtlinienkonforme Aufbereitung zuständig und hat sowohl die Daten selbst als auch die Informationen darüber in geeigneter Weise öffentlich zugänglich zu machen. Dabei sollen nicht zwingend neue Daten erhoben, sondern insbesondere die vorhandenen Daten interoperabel gemacht werden. Als Meilenstein im Umsetzungszeitplan kann dabei der 9. November 2011 gesehen werden, ab dem die volle Betriebsfähigkeit der Such- und Darstellungsdienste der Themen aus Annex I und II gewährleistet sein muss.

Freie Datennutzung

Ungeachtet aller Bestrebungen vonseiten der EK, den Zugang zu und die Verwen-

dung von öffentlichen Daten zu erleichtern, existiert ausgehend vom US-amerikanischen Raum seit einigen Jahren das Open-Data-Konzept, welches im Zusammenhang mit Daten aus Institutionen der öffentlichen Verwaltung zum Paradigma des Open Government Data (kurz OGD) erweitert wurde. Zusammengefasst bezeichnet OGD die Idee, die Datenbestände des öffentlichen Sektors, die im Interesse der Allgemeinheit gesammelt wurden, ohne jedwede Einschränkung zur freien Nutzung, zur Weiterverbreitung und zur freien Weiterverwendung frei zugänglich zu machen[1]. Diese Daten sollen der Bevölkerung in maschinenlesbarer Form (also digital) zur Verfügung gestellt werden, sodass die Daten auch automatisiert verarbeitet werden können. Dazu sollen offene Standards und Schnittstellen verwendet werden[2]. Neben den technischen Schnittstellen muss seitens der Verwaltung ein rechtlicher Rahmen geschaffen werden.

Top-down-Initiative

Tatsächlich existieren zwischen INSPIRE und OGD eine Reihe an Gemeinsamkeiten, aber auch grundlegende Unterschiede. Neben dem unterschiedlichen Umfang (Geodaten bei INSPIRE versus sämtliche Daten bei OGD) betrifft dies auch die Entstehung, das Begriffsverständnis, die Zielsetzung sowie die Art der Umsetzung. OGD ist eine Bottom-up-Initiative vonseiten der Zivilgesellschaft, welche sich auf den Verwaltungsapparat als Ganzes bezieht, während INSPIRE eine durch die Verwaltung selbst initiierte (Top-down-) Initiative zur Erleichterung des Austausches und des Zugangs zu raumbezogenen Daten ist. Dementsprechend unterscheiden sich auch Begriffsverständnis, Zielsetzung und Herangehensweise.

Explizit soll im Verständnis von OGD auch eine kostenfreie kommerzielle Nutzung durch Privatpersonen und -firmen sowie die unbegrenzte Weiterverarbeitung für eigene Zwecke und die Weitergabe an Dritte erlaubt sein, ohne Zwang zur vorhergehenden namentlichen Registrierung und Akzeptieren von Nutzungsbedingungen. Die INSPIRE-Richtlinie zielt hingegen lediglich auf die Verfügbarkeit und Interoperabilität von raumbezogenen Daten ab, wobei dies nicht die generelle Kostenfreiheit inkludiert. Auch darf es sehr wohl Beschränkungen hinsichtlich der Nutzung und des Zugangs zu den Daten geben (Registrierung):

	INSPIRE	OGD
Umsetzung	Top-down (ausgehend von Europäischer Kommission)	Bottom-up (ausgehend von der Zivilgesellschaft)
Umfang	Geodaten	alle (öffentlichen) Daten
Zielsetzung	Erleichterungen in Interoperabilität, Suche und Nutzung von Geodaten, möglichst kostenfreie Nutzung für den Privatgebrauch	Kosten- und lizenzfreie Nutzung sämtlicher Daten, auch für kommerzielle Zwecke
Verständnis	Schritt zu einer effizienten und transparenten Verwaltung mit Verbesserungen für Verwaltungsinstitutionen und Bürger	Gesellschaftlicher Paradigmenwechsel von der hoheitlichen Verwaltung zum Dienstleister einer Zivil- und Wissensgesellschaft

Doch so unterschiedlich die beiden Initiativen auf den ersten Blick auch sein mögen, gibt es auch Synergien und Überschneidungen. So öffnen beispielsweise die INSPIRE-Suchdienste mittels eines Metadatenkatalogs die Sicht auf sämtliche verfügbare Geodaten öffentlicher Stellen, welche nicht der militärischen Geheimhaltung unterliegen[3]. Alle INSPIRE-relevanten Daten müssen schrittweise zur Darstellung und in weiterer Folge auch zum Download zur Verfügung gestellt werden. Dazu wird auf die kostspielige Umsetzung von Webshop-Lösungen zur Förderung der freien Datenabgabe teilweise verzichtet.

Als Beispiele OGD-naher Umsetzungen können vonseiten des Lebensministeriums sowohl der zur nichtkommerziellen Nutzung kostenfrei angebotene Orthophotodienst Geoimage als auch die zahlreichen WebGIS-Applikationen genannt werden, welche mit den einzelnen Ressortdaten gespeist werden und diese neben der bloßen Darstellung teilweise auch direkt zum Download anbieten. Auch Smartphone-Applikationen wie jene zur Darstellung des aktuellen Ozonwerts der nächstgelegenen Messstation konnten dadurch von privater Seite bereits realisiert werden.[4]

Obgleich nicht von den gleichen Wurzeln wie OGD, trägt die EU-Richtlinie INSPIRE somit auch dem Prinzip einer offenen, transparenten Verwaltung Rechnung, mit dem Verständnis eines modernen Dienstleisters der Zivilgesellschaft.

http://www.inspire.gv.at/

MAG. DIPL.-ING DDR. REINHARD MANG ist Generalsekretär sowie Leiter der Sektion II „Nachhaltigkeit und ländlicher Raum" im Lebensministerium.


LEBENSMINISTERIUM

MAG. ANDREAS REITHOFER ist Mitarbeiter im Projekt INSPIRE/AT, welches am Land-, forst- und wasserwirtschaftlichen Rechenzentrum im Auftrag des Lebensministeriums umgesetzt wird.


PRIVAT

[1] Siehe auch: VON LUCKE, Jörn [2010]: Open Government Data. Frei verfügbare Daten des öffentlichen Sektors. Gutachten für die dt. Telekom AG zur T-City Friedrichshafen

[2] http://sunlightfoundation.com/policy/documents/ten-open-data-principles/

[3] Im Einzelfall können auch datenschutzrechtliche Bestimmungen die Nutzung einschränken, dies ist jedoch kein Teil des Richtlinientextes und damit Auslegungssache.

[4] http://www.ozon-info.at

Leistungsmotivation statt Ehrgeiz

Wenn Toni Innauer über seine Karriere als Athlet spricht, geht es nicht um nur um Sport. Häufig ist die Rede von Motivation und Funktionslust. Doch wie ist das auf den „Normalbürger" übertragbar? Und warum sind Denken und Bewegung so eng miteinander verknüpft? Toni Innauer im Gespräch mit dem FIV.

INTERVIEW: GERTRAUD EIBL

ICG

Toni Innauer, Jahrgang 1958, ist Olympiasieger und Weltmeister im Skispringen, war Trainer, Sportmanager und nordischer Sportdirektor im ÖSV. Nach seiner sportlichen Karriere studierte er Philosophie, Psychologie und Sportwissenschaften und ist heute als Autor und Referent tätig.

Sie waren Jahrzehnte als Athlet und Manager im Spitzensport aktiv. Inwieweit prägt eine Sportlerkarriere das Leben nach dem Spitzensport?
Es war kein Zufall, dass ich zum Spitzensport gekommen bin. Ich bin ein Bewegungsmensch, auch heute noch. Der Spitzensport prägt auch das Qualitätsbewusstsein und den persönlichen Leistungsbezug. Vielleicht wird man ein bisschen verdorben, weil vieles mit Können, Leistung und Wettbewerb in Verbindung gebracht wird. Dabei gibt es Dinge, die damit nicht fassbar sind. Ich habe deshalb versucht, meine Grenzen und meine Interessen zu erweitern.

Wie beschreiben Sie den Zusammenhang zwischen Bewegung und Motivation?
Körperlichkeit und Bewegung hat sehr viel mit unserer Identität und unserer Selbstwahrnehmung zu tun, das hat Einfluss auf unsere kognitiven und emotionalen Abläufe. Der Zusammenhang wird meines Erachtens sträflich unterschätzt, auch im Schulwesen. Man weiß, dass verschiedene Prozesse, die im Hirn ablaufen, von physiologischen Dimensionen gespeist und gesteuert sind. Es muss nicht Spitzensport sein, aber es ist nicht alles „Hirn".

Glauben Sie, dass dieses Bewusstsein noch mehr an Bedeutung gewinnen wird?
Man wird sich neue Strategien überlegen müssen, damit der Mensch zu der Bewegung kommt, die er von Natur aus braucht. Nicht nur, um leistungsfähig zu sein, sondern auch um nicht krank oder depressiv zu werden.

Denken Spitzensportler anders, was Leistungsfähigkeit anbelangt?
Mir ist schon bewusst, dass Spitzensport eine extreme Ausprägung ist, die man nur bedingt modellhaft vorführen kann. Leider gibt es Entartungen in manchen Bereichen des Spitzensports, man denke an Doping und Korruption. In Bezug auf globale Herausforderungen sind Politik und Wirtschaft dennoch mit Sport vergleichbar: Es geht um klare Spielregeln. Wenn es keine international standardisierten Regeln gibt, funktioniert ein Wettbewerbssystem nicht. Außerdem zeigt der Sport modellhaft, dass es nicht nur um Wettbewerb geht, sondern auch um Kooperationen. Kooperation ist wichtig, um überhaupt wettbewerbsfähig zu sein.

Welche Rolle spielt Feedback für die eigene Persönlichkeit?
Erfahrungsgemäß ist man als Mensch leicht überfordert, wenn man sich selber beurteilen muss. Rückmeldungen und Supervision systematischer Art sind sehr hilfreich. Menschen, die unter großer Belastung stehen, sind gut beraten, sich coachen zu lassen. Es ist motivierend, weil man viel über sich selbst lernt.

In Ihrem Vortrag haben Sie viel von Erfolg und Leistung gesprochen. Wann wird Ehrgeiz bedrohlich?
Den Begriff „Ehrgeiz" gibt es im Spitzensport nicht mehr. Es gibt Leute, die höchst leistungsmotiviert sin. Sie sind risikofreudiger, wettbewerbsorientiert und messen sich gerne an anderen. Die sind richtig verknallt in die Schwierigkeit einer Aufgabe. Im Sport passiert es oft, dass man plötzlich dieses Gefühl kriegt: Im Gehirn tut sich was. Was sich da tut, ist noch nicht automatisiert, man muss sich noch wahnsinnig anstrengen, damit es halbwegs funktioniert. Aber man merkt: Langsam entwickelt sich eine Automatik, weil sich synaptische Verbindungen festigen. Da kommt die Funktionslust ins Spiel. Man freut sich über diese Erweiterung der Identität, des eigenen menschlichen Radius. Das hat aber viel mehr mit unserem Hirn, mit unserem Bewusstsein zu tun als mit bloßem Ehrgeiz.

www.toni-innauer.at

Geschlechter- statt rollenspezifisch

2011 erhielt die Arbeitsinspektion den BKA-Verwaltungspreis „Management von Diversity, Integration und Gender-Potenzial für die Verwaltung von morgen". Ein Beispiel, wie Gender-Mainstreaming und Diversity in der Praxis funktionieren können.

TEXT: RENATE NOVAK

Bei der Verwaltungspreisverleihung 2011 im Wiener Rathaus wurde die Arbeitsinspektion gekürt. V. l. n. r.: SC Dr.in Eva-Elisabeth Szymanski, DI Günter Schinkovits* (Amtsleiter Eisenstadt), Dr.in Renate Novak (BMASK/A – ZAI/3)*, BM Gabriele Heinisch-Hosek, DI Franz Jäger (Amtsleiter Krems), Dr.in Elsbeth Huber (BMASK/A-ZAI-4) – * GMD-Beauftragte AG-GM des BMASK/Arbeitsinspektion

BKA

Die Jury war überzeugt: Mit dem fundierten Organisationsentwicklungsprozess können vielfältige Geschlechtergerechtigkeitsaspekte in der internen Organisationsstruktur und in den Kernaufgaben im Arbeitnehmerschutz verankert werden. Besonders betont wurde der Umstand, dass mit der Projektentwicklung weitere soziale Merkmale wie Alter oder Herkunft verbindlich Berücksichtigung finden.

Diversitygerechte Arbeit

Als Aufsichts- und Kontrollbehörde muss die Arbeitsinspektion auch auf die Weiterentwicklung des Arbeitnehmerschutzes achten (ArbIG 1993). So wurde die Genderperspektive 2003 im TQM der Arbeitsinspektion einbezogen. Die weitere Implementierung im Auftrag von SC Dr.in Szymanski erfolgte ab 2004 schrittweise mit Schulungs-, Strukturmaßnahmen (GM-Arbeitsgruppe, Netzwerk) und genderrelevanten Arbeitsschwerpunkten (Alten-/Pflegeheime, Reinigung, Gastgewerbe). Mit der Arbeitsschutzstrategie 2007–2012 folgten die Erweiterung um den Aspekt „Diversity" und ein dementsprechender Austausch, u. a. mit AUVA, Interessenvertretungen, Forschungs- und Gesundheitseinrichtungen. Wesentlich für den Projekterfolg war die Integration der Genderperspektive in die externe Beratungs- und Kontrolltätigkeit der Arbeitsinspektoren. Besonders hervorgehoben wurde die Bedeutung von Genderfragen im Arbeitnehmerschutz.

Rollenstereotype

Frauen und Männer sind nach wie vor jeweils häufiger in bestimmten Branchen beschäftigt und damit typischen Sicherheits- und Gesundheitsschutzgefahren ausgesetzt. Oft bestimmen Geschlechtsrollenbilder, was als Gefahr und Belastung am Arbeitsplatz wahrgenommen und für Frauen/Männer als normal oder problematisch angesehen wird. Häufig passiert es, dass Schutz- und Präventionsmaßnahmen unterbleiben. Genderfragen bleiben auch ungelöst, wenn nur auf biologische Faktoren abgestellt wird. Auch geschlechtsspezifisches Risikoverhalten, Umgang mit Belastungen, mangelnde Arbeitsorganisation und Beteiligung sind relevante Faktoren. Um allen gerechte Arbeitsbedingungen und wirksame Schutzmaßnahmen gewährleisten zu können, ist ein Perspektivenwechsel erforderlich:

- Der genderneutrale Arbeitsschutz stellte den männlichen Durchschnittsarbeitnehmer in den Mittelpunkt und wurde damit weder Frauen noch Männern, die diesem Bild nicht entsprechen, gerecht – z. B. bei Auswahl der Schutzkleidung, Lastenhandhabung und der ergonomischen Arbeitsplatzgestaltung.
- Ein gendergerechter Ansatz nimmt auf unterschiedliche Arbeitssituationen von Frauen und Männern und Geschlechterverhältnisse am Arbeitsplatz Bedacht. Er berücksichtigt die Vielfältigkeit innerhalb der Gruppen und reflektiert Rollenstereotype.
- Diversität im Arbeitnehmer/innenschutz bedeutet u. a., Arbeitsorganisation, Schutzmaßnahmen, Prävention und betriebliche Gesundheitsförderung diversitygerecht zu gestalten. Dazu gehören eine verständliche Unterweisung, adäquate Beteiligung und Funktionsbestellung, z. B. von Migranten. Wichtig ist es, in allen Diversitäten auch die Genderperspektive einzubeziehen.

Die Erfahrung zeigt, dass Arbeitsschutzstandards für alle Beschäftigten steigen, wenn Arbeitsplätze und Arbeitsvorgänge gender- und diversitygerecht für alle am Arbeitsplatz tätigen Menschen gestaltet werden.

DR.in RENATE NOVAK ist Gender-Mainstreaming-Beauftragte der Arbeitsinspektion und in der AG-GM des BMASK (Sektion VII), Juristin in der Rechtsabteilung des Zentral-Arbeitsinspektorats im BMASK (VII/A/3), Projektleiterin der GM-Implementierung in der Arbeitsinspektion. Arbeitsschwerpunkt: ArbeitnehmerInnenschutz, Gender und Diversity im Sicherheits- und Gesundheitsschutz am Arbeitsplatz.

BMASK

Eine Archivarin im indischen Patna, die ihren Job aus humanitären Gründen nach dem Tod ihres Mannes „geerbt" hat.

Staatsdiener aus aller Welt

Acht Länder hat der niederländische Fotograf Jan Banning für sein Projekt „Bureaucratics" bereist. Entstanden sind Bilder, die Geschichten erzählen: über das Leben und die Kultur des Porträtierten. Aber auch über Bürokratie im globalen Kontext.

TEXT: GERTRAUD EIBL

„Die Bilder verraten, dass die porträtierten Menschen stolz sind auf ihren Arbeitsplatz. Und doch möchte wohl kaum jemand von uns mit den Porträtierten tauschen", so die Worte von FIV-Vizepräsident Mag. Klaus Hartmann bei der Eröffnung der Ausstellung „Bureaucratics" im Palais Porcia, dem Kunstraum des BKA. Tatsächlich entführen die Bilder sowohl in das Arbeits- als auch das kulturelle Umfeld von Staatsdienern, deren Job dem des öffentlich Bediensteten hierzulande nur bedingt gleicht.

50 Fotografien umfasst die Ausstellung „Bureaucratics" des niederländischen Fotografen Jan Banning. Es sind Bilder, die neugierig machen, weil sie Details verraten. Nicht nur über Schreibtische und Amtsstuben, sondern über jene Menschen, die sie mit Leben erfüllen. Begonnen hat Banning das Projekt im Jahr 2003 in Indien. Es folgten Reisen nach Russland, Bolivien, Frankreich, Liberia, China, in den Jemen und die USA. Nach offizieller Genehmigung seien Banning und sein Kollege Will Tinnemans jeweils unangekündigt bei den porträtierten Personen erschienen. Während Journalist Tinneman interviewte, entstanden Bannings Porträtfotografien. Egal ob Finanzbeamter, Polizist, Gemeindebeamter oder Direktor: Die Bilder zeigen, dass die Porträtierten stolz auf ihre Arbeit sind. „In den Fotografien kann sehr viel entdeckt werden. Wenn du sie genau studierst, verraten sie dir etwas über das Land, aber vielleicht auch etwas über Bürokratie im Allgemeinen", resümiert Jan Banning.

Vielfalt der Bürokratie

Ja, sie hat viele Gesichter, die Bürokratie. Sushma Prasad (Jahrgang 1962) arbeitet im indischen Patna als Archivarin. Ihren Job hat sie durch den Tod ihres Mannes im Jahr 1997 „geerbt".

Ein Abteilungsleiter in seinem Büro in der Provinz Cornelio Saavedra, Bolivien.

Jan Banning wurde im Jahr 1954 in den Niederlanden geboren. Er studierte Sozial- und Wirtschaftsgeschichte, bevor er 1981 als freier Fotograf tätig wurde. Sein Schwerpunkt liegt im Bereich der sozialdokumentarischen Fotografie. Für seine Arbeit, die regelmäßig in internationalen Zeitungen und Magazinen erscheint, erhielt er zahlreiche Auszeichnungen, darunter einen World Press Photo Award 2004, den Lead Award 2007 sowie insgesamt zehn Auszeichnungen und Nominierungen bei der Vergabe der „Zilveren Camera" für das beste niederländische Pressefoto des Jahres.

FIV-Präsidentin Heidrun Strohmeyer und
FIV-Vizepräsident Klaus Hartmann eröffneten die Ausstellung.

Rudolfo Vilca Flores (Jahrgang 1958) ist Abteilungsleiter für „Market and Sanitary Services" in der Kommune Betanzos der Provinz Cornelio Saavedra. Vor seinem Job im öffentlichen Dienst hat er sein Geld als Maurer, Elektriker, Installateur und Heimwerker verdient.

Dass die Ausstellung derzeit in Wien gastiert, ist auf die Initiative des FIV mit Unterstützung des BKA, der Königlich Niederländischen Botschaft und der Raiffeisen Centro Bank zurückzuführen.

Eröffnet wurde „Bureaucratics" am 16. 11. durch FIV-Präsidentin Heidrun Strohmeyer und FIV-Vizepräsident Klaus Hartmann. Rund 70 interessierte Besucher folgten bereits bei der Vernissage den „Bild-Geschichten" des niederländischen Künstlers. Bis 5. 1. ist noch Zeit, der Vielfalt der Bürokratie vor Ort in Wien zu begegnen.

BUREAUCRATICS
Kunstraum Palais Porcia,
Bundeskanzleramt
Wien I, Herrengasse 23
Die Ausstellung ist
bis 5. Jänner 2012 geöffnet.
Öffnungszeiten: Montag bis Freitag
8.00 – 16.00 Uhr, Einlass bis 15.45 Uhr,
feiertags geschlossen.
Der Eintritt ist frei!

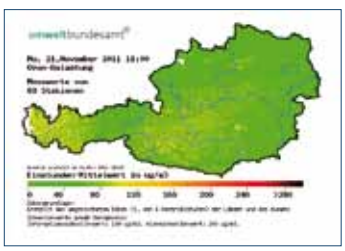
Ozon-App fürs Smartphone

„Apps sind das Symbol für den Erfolg des mobilen Internet" – so zu lesen in einem Blog der Frankfurter Allgemeinen Zeitung. Ein Zeichen des Erfolgs sind Apps zweifelsohne auch für die Open-Data-Szene. Und für jene, die von deren Entwicklungen profitieren: die Bürger.

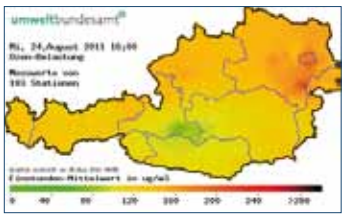
TEXT: GERTRAUD EIBL

PHOTOS.COM

Wenn die Temperaturen sinken, der Nebel tief hängt und alles grau in grau erscheint, ist die Sehnsucht nach Sonne und Badewetter wieder da. Mit den hohen Temperaturen steigt allerdings die Gefahr einer erhöhten Ozonbelastung. Ein Thema, dem sich das Umweltbundesamt zusammen mit open3.at und echonet 2011 angenommen hat: Sie haben – ganz im Sinne des Open Government – eine Ozon-Warnung für das Smartphone entwickelt.



UMWELTBUNDESAMT



UMWELTBUNDESAMT

Das Ozon-App visualisiert aktuelle Ozondaten auf dem Smartphone. Hier ein Vergleich der Ozonbelastung von August und November.

Derzeit lassen die winterlichen Temperaturen keinen daran denken: an erhöhte Ozonbelastung. Die Ozonschicht, die im Sommer vor schädlicher UV-Strahlung schützt, schwindet jeden Winter über der Antarktis. Im Winter verringert sich die Ozonschicht normalerweise um 30 Prozent. Durch FCKWs und die eisigen Temperaturen in der Höhe hat diese Schicht im vergangenen Winter rund 40 Prozent eingebüßt. Hervor geht dies aus Boden- und Satellitenbeobachtungen der World Meteorological Organization (WMO).

UMWELTBUNDESAMT

Spätestens nächsten Sommer wird die Ozon-Warnung auf vielen Smartphones wieder aktiviert. Unter www.ozon-info.at kann sie aufgerufen werden. Für die Warnfunktion werden die stündlich aktualisierten Ozonmesswerte für ganz Österreich von den Ämtern der Landesregierungen und dem Umweltbundesamt zur Verfügung gestellt. In Österreich werden derzeit über 100 Ozonmessstellen betrieben. Zum Schutz der Bevölkerung vor überhöhter Ozonbelastung sind im Ozongesetz eine Informations- und eine Alarmschwelle festgesetzt. Werden diese überschritten, ist in den Medien darüber zu informieren. Die Informationsschwelle wird bei einer einstündigen Ozonkonzentration von mehr als 180 µg/m³, die Alarmschwelle wird bei einer einstündigen Ozonkonzentration von mehr als 240 µg/m³ erreicht. Zum Schutz der menschlichen Gesundheit legt das Ozongesetz darüber hinaus auch einen Zielwert fest. Dieser ist als höchster Achtstundenmittelwert eines Tages festgelegt. Er beträgt 120 µg/m³ und darf an nicht mehr als 25 Tagen pro Jahr, gemittelt über drei Jahre, überschritten werden.

Ideen für weitere Apps gäbe es genug: Zum Beispiel eine Application, die über Feinstaub-Werte informiert. Bleibt abzuwarten, welche mobilen Überraschungen Open Government weiter bringt.

Mythos einheitliche Verwaltung

Die Vielfalt von Verwaltungsstrukturen war Thema der diesjährigen Herbsttagung der Verwaltungswissenschaftlichen Gesellschaft (ÖVG). Gregor Wenda war dabei und berichtet zusammenfassend.

TEXT: GREGOR WENDA

Verwaltungsorganisationen sind schon lange nicht mehr ausschließlich auf die in hierarchische Strukturen eingebetteten Behörden und Ämter beschränkt; auch in neuen Organisationsformen wie weisungsfreien Einrichtungen, „teilrechtsfähigen" Strukturen, privatrechtlich organisierten Ausgliederungen oder kooperativen Zusammenschlüssen agiert die Verwaltung. Die Österreichische Verwaltungswissenschaftliche Gesellschaft (ÖVG) widmete sich daher in ihrer diesjährigen zweitägigen Herbsttagung der Thematik „Unabhängigkeit und Steuerbarkeit von Verwaltungseinheiten". Auf Einladung des Landes Steiermark unternahm die ÖVG im festlichen Rahmen des „Weißen Saales" der Grazer Burg den Versuch einer aktuellen Systematik und Einordnung in das Rechtssystem, gefolgt von der Darstellung praktischer Beispiele und verwaltungswissenschaftlicher Analysen. Landeshauptmann Mag. Franz Voves eröffnete die Veranstaltung und betonte vor dem Hintergrund aktueller Verwaltungsstrukturreformen in der Steiermark die Wichtigkeit des Austausches zwischen Politik und Wissenschaft.

Dozent Dr. Bernhard Müller diskutierte verfassungsrechtliche Fragen rund um die Durchbrechung des Weisungszusammenhanges. Es sei kein Widerspruch zum Demokratieprinzip, wenn Legitimationsdefizite durch eine Form von „Ingerenz" ersetzt würden. Univ.-Prof. Dr. Nicolas Raschauer befasste sich mit der „Agency-Verwaltung" aus unionsrechtlicher Sicht und beschrieb den neuen Trend zu EU-Regulierungsagenturen. Zu deren Ausgestaltung biete insbesondere eine Entscheidung des EuGH von 2010 wichtige Leitlinien. Weitere europarechtliche Aspekte zu EU-Agenturen und Details aus dem Arbeitsalltag der EU-Grundrechteagentur (FRA) präsentierten Dr. Andreas J. Kumin vom Außenministerium und Dr. Gabriel N. Toggenburg von der FRA. Die Realität selbstständiger Verwaltungseinrichtungen in Österreich bildete den Schwerpunkt des Nachmittags: Univ.-Prof. Dr. Bernhard Raschauer notierte den steten Anstieg ausgegliederter Rechtsträger und erläuterte, dass mutmaßliche Kontrolldefizite nicht immer als solche zu werten seien: Die Unzuständigkeit der Volksanwaltschaft bei privatrechtlichen Aktivitäten von Ausgegliederten sei beispielsweise eine Systementscheidung des Verfassungsgesetzgebers gewesen; bei Ausgegliederten müsse eine entsprechende Weisungsbindung gesetzlich vorgesehen werden – hier gelte die „Ingerenz". Die Evaluierung bisheriger Ausgliederungen im Bundesbereich erläuterte Dr. Alois Schittengruber vom Bundeskanzleramt; der Grazer Steuerberater und Wirtschaftstreuhänder Dr. Peter Pilz berichtete über die Evaluierung von Ausgliederungen auf Landes- und Gemeindebene. Derzeit bestehen rund 800 ausgegliederte Einrichtungen im Bundes- und Landesbereich; von April 2010 bis Mai 2011 wurden 40 dieser Einrichtungen durch das Bundeskanzleramt untersucht.

Das dritte Modul der ÖVG-Herbsttagung diskutierte Einheit und Vielfalt von Verwaltungsstrukturen: Prof. Werner Jann, Universität Potsdam, zeigte, dass die Verwaltung keine monolithische Struktur aufweise und sich das starre Organisationsbild der Verwaltung zugunsten neuer Organisationsformen auflöse. Die „Einheit der Verwaltung" sei für ihn immer ein Mythos gewesen. Seit den 1980er-Jahren bestehe ein „Agency-Fever" nach dem Modell eines „Prinicipal-Agent"-Verhältnisses. Rechnungshofpräsident Dr. Josef Moser verdeutlichte Doppelgleisigkeiten in der Verwaltung und unterstrich die Notwendigkeit nachhaltiger Reformen. SC Dr. Hans-Günter Gruber vom Lebensministerium beschrieb zum Abschluss der Tagung Ausgliederungen aus der Sicht eines „Mutterressorts", während Dr. Wolfgang Urbantschitsch von der E-Control Austria aus der Sicht eines ausgegliederten Rechtsträgers referierte. Sektionschef Dr. Manfred Matzka, Präsident der ÖVG, bilanzierte, wie notwendig es sei, die Instrumente der Steuerung in der Realität der österreichischen Verwaltung weiterzuentwickeln. „Wir müssen den Werkzeugkasten, den uns das Verfassungsrecht und das Unternehmensrecht geben, in vollem Umfang auszunutzen, um Standards zu setzen und Strukturen zu verfestigen."

ÖVG / GREGOR WENDA

Es gibt keine einheitliche Verwaltung, vielmehr eine Vielfalt an Strukturen. Darüber waren sich die Teilnehmer der ÖVG-Herbsttagung einig.

Präsentationen:
http://www.oevg.info/download/

MAG. GREGOR WENDA, MBA, ist seit 2007 Generalsekretär der Österreichischen Verwaltungswissenschaftlichen Gesellschaft (ÖVG); im Bundesministerium für Inneres ist der studierte Jurist als stv. Leiter der Abteilung für Wahlangelegenheiten und als stv. Chefredakteur des Magazins „Öffentliche Sicherheit" tätig.

BMI / EGON WEISSHEIMER

Von Ruhestandsversetzungsverfahren und konfliktbelasteter Kommunikation am Arbeitsplatz

TEXT: RUDOLF HASCHMANN

VERWALTUNGSGERICHTSHOF

Ruhestandsversetzungsverfahren wegen Dienstunfähigkeit – Sekundärprüfung (VwGH v. 30.5.2011, 2010/12/0136)

Im Ruhestandsversetzungsverfahren spielt im Rahmen der Sekundärprüfung unter anderem auch die gesundheitliche Verfassung des Beamten und die Gleichwertigkeit des Verweisungsarbeitsplatzes eine Rolle. Dabei sind grundsätzlich alle Tätigkeiten der betreffenden Verwendungsgruppe und deren Anforderungen in physischer und psychischer Hinsicht im Wirkungsbereich der jeweiligen obersten Dienstbehörde anzuführen und anzugeben, ob der Beamte aufgrund der festgestellten Restarbeitsfähigkeit imstande ist, diese Tätigkeiten auszuüben. Von dieser Verpflichtung könnte die Dienstbehörde dann entbunden sein, wenn entweder überhaupt keine Restarbeitsfähigkeit des Beamten besteht oder dargelegt wird, dass überhaupt keine Arbeitsplätze seiner Verwendungsgruppe frei sind, bzw., dass sämtliche freien Arbeitsplätze seiner Verwendungsgruppe der bisherigen Verwendung nicht gleichwertig oder aber nicht im Sinne des § 14 Abs. 3 BDG 1979 zumutbar sind.

Die Behörde irrt, wenn sie die Auffassung vertritt, „dass die Richtigkeit von ärztlichen Gutachten niemals von einer Dienstbehörde in Zweifel gesetzt werden könne bzw. dürfe". Vielmehr ist die Behörde verpflichtet, sich mit den unterschiedlichen Ergebnissen der Gutachten der beteiligten Ärzte beweiswürdigend auseinanderzusetzen und darzulegen, aufgrund welcher Erwägungen sie als Ergebnis ihrer Beweiswürdigung dem einen oder dem anderen Gutachten folgt.

OBERSTER GERICHTSHOF

Grundlage des Anspruchs auf Erteilung einer betrieblichen Pensionskassenzusage, Wurzel in der öffentlich-rechtlichen Stellung der Beamten (OGH 28.6.2011, 9ObA66/11p)

Die Rechtsansicht des Rekurswerbers, dass die sich aus § 22a Abs. 1 GehG ergebende Verpflichtung der Beklagten einen Anspruch zivilrechtlicher Natur begründe, ist unzutreffend. Nach stRsp waren Streitigkeiten aus öffentlich-rechtlichen Dienstverhältnissen, soweit es sich um Besoldungen und Gebühren handelte, im administrativen Weg auszutragen. Daran hat sich auch durch die Aufhebung des genannten Hofdekrets mit dem Ersten Bundesrechtsbereinigungsgesetz BGBl I 1999/191 im Hinblick auf § 1 Abs. 1 DVG nichts geändert. Die Unzulässig-

keit des Rechtswegs bezieht sich daher auf Ansprüche, welche auf der öffentlich-rechtlichen Stellung des Beamten zu der Gebietskörperschaft beruhen. Nur dann, wenn von oder gegen Beamte Ansprüche zivilrechtlicher Natur geltend gemacht werden, sind für solche Rechtsstreitigkeiten die Arbeits- und Sozialgerichte zuständig.

Ziel der Bestimmung des § 22a GehG war die Schaffung einer Rechtsgrundlage für die Einbeziehung auch von Beamtinnen und Beamten in eine entsprechende Pensionsvorsorge durch Abschluss eines Kollektivvertrags. Das GehG regelt demnach die Grundlage des Anspruchs auf Erteilung einer betrieblichen Pensionskassenzusage, der daher unzweifelhaft seine Wurzel in der öffentlich-rechtlichen Stellung der von dieser Bestimmung erfassten Beamten hat. Dabei handelt es sich aber nicht um eine direkt auf § 2 Z 1 BPG beruhende Leistungszusage, sondern nach dem klaren Wortlaut des § 22a Abs 1 Satz 1 GehG um eine in dieser – das öffentlich-rechtliche Dienstverhältnis von (bestimmten) Beamten betreffenden – Bestimmung geregelte Verpflichtung des Bundes, diesen Beamten eine betriebliche Pensionskassenzusage iSd § 2 Abs. 1 BPG zu erteilen, die daher keinesfalls zivilrechtlicher Natur ist.

Nach stRsp ist bei der Zulässigkeit des Rechtswegs ausgehend von den Klagebehauptungen nicht allein der Wortlaut des Klagebegehrens, sondern die Natur bzw. das Wesen des geltend gemachten Anspruchs maßgebend. Daher ist nicht entscheidend, wie der Kläger seinen Anspruch formt, sondern ob nach dem Inhalt der Klage ein privatrechtlicher Anspruch erhoben wird. Dabei ist zu beachten, dass die aus einem öffentlich-rechtlichen Dienstverhältnis abgeleiteten Rechte und Pflichten bzw. die Arbeitsbedingungen – mangels eines ausdrücklich eingeräumten gesetzlichen Gestaltungsrechts – weder vom Dienstgeber noch vom Dienstnehmer rechtswirksam gestaltet werden können.

Es trifft zwar zu, dass es den an einem öffentlich-rechtlichen Dienstverhältnis beteiligten Rechtssubjekten schon aufgrund ihrer Privatautonomie nicht verwehrt ist, über Gegenstände und Leistungen außerhalb der gesetzlich abgesteckten dienstrechtlichen Beziehungen privatrechtliche Verträge abzuschließen. Ansprüche, die auf eine solche, neben dem öffentlich-rechtlichen Dienstverhältnis zwischen Dienstnehmer und Dienstgeber getroffene privatrechtliche Vereinbarung gestützt werden, sind auch vor den ordentlichen Gerichten geltend zu machen.

Ein solcher Anspruch wird hier aber nicht geltend gemacht. § 22a Abs. 1 GehG verpflichtet die Beklagte zur Erteilung einer betrieblichen Pensionskassenzusage. Der Abschluss eines Kollektivvertrags dient lediglich der Umsetzung dieser gesetzlichen Verpflichtung. Mag dieser Kollektivvertrag auch nicht vom Staat als Träger von Hoheitsrechten abgeschlossen worden sein, so begründet er dennoch keine eigene, neben dem Gesetz bestehende Verpflichtung zivilrechtlicher Natur.

Es besteht daher neben der gesetzlichen Verpflichtung auch nicht eine – durch den Kollektivvertrag begründete – privatrechtliche Verpflichtung der Beklagten zur Erteilung einer Pensionskassenzusage.

DISZIPLINAROBER-KOMMISSION

Mobbingverbot, persönlicher Geltungsbereich, konfliktbelastete Kommunikation am Arbeitsplatz, systematische Verhaltensweise über längeren Zeitraum (14.7.2011, 1/17-DOK/11 und 2/17-DOK/11)

Mangels des vom Gesetz geforderten unmittelbaren dienstlichen Bezuges der beiden konkreten Bediensteten zueinander unterliegt der beschuldigte Beamte hier nicht dem persönlichen Geltungsbereich des § 43a BDG.

Es lag zudem aber auch keine oftmalige, systematische, während eines längeren Zeitraumes angedauert habende, direkt oder indirekt angreifende Verhaltensweise des Beschuldigten der X. gegenüber vor, mit dem Ziel oder Effekt des Ausstoßens der genannten Sachbearbeiterin aus dem Arbeitsverhältnis, die vom (unterlegenen) Opfer als Diskriminierung empfunden worden wäre.

Der inkriminierte Sachverhalt kann daher schon aus diesen Gründen nicht unter die Bestimmung des § 43a BDG subsumiert werden. Da der im Einleitungsbeschluss im Verdachtsbereich erhobene disziplinäre Vorwurf eindeutig auf eine schuldhafte Verletzung der Dienstpflichten gemäß § 43a BDG (Mobbingverbot) lautete, hat sich die Disziplinarkommission diesbezüglich festgelegt und den Gegenstand des Disziplinarverfahrens abgegrenzt. Der DOK ist es daher verwehrt, im Berufungsverfahren erstmals die Frage zu prüfen, ob die vom Beschuldigten inkriminierten schriftlichen Äußerungen allenfalls eine Verletzung seiner in § 43 Abs. 2 BDG normierten Dienstpflichten darstellen und somit einen anderen disziplinarrechtlichen Tatbestand erfüllen oder ob diese Äußerungen als gerade noch ausreichend sachliche Kritik zu werten seien, die als vom Grundrecht auf Freiheit der Meinungsäußerung gemäß Art. 10 EMRK umfasst angesehen werden müsse.

MAG. RUDOLF HASCHMANN
ist Referatsleiter in der Sektion III des Bundeskanzleramts und hat die abgedruckten Rechtsentscheidungen zusammengestellt.

FIV

IMPRESSUM
Medieninhaber und Herausgeber: FIV Führungsforum Innovative Verwaltung (1010 Wien, Rockhgasse 6, Tel.: +43 1 533 86 36-49)
Anzeigen und Verleger: Österreichischer Wirtschaftsverlag GmbH (1051 Wien, Wiedner Hauptstraße 120–124, Tel.: +43 1 54664-0)
Anzeigenkontakt: Michael Glatz, Tel.: +43 1 54665-281, m.glatz@wirtschaftsverlag.at
Redaktion: Mag. (FH) Gertraud Eibl, MAS (Österreichischer Wirtschaftsverlag), Mag. Heidrun Strohmeyer, Mag. Klaus Hartmann, Andrea Bock (alle FIV)
AutorInnen dieser Ausgabe: Gertraud Eibl, Rudolf Haschmann, Markus Klemen, Reinhard Mang, Johannes Mariel, Renate Novak, Andreas Reithofer, Eva Souhrada-Kirchmayer, A Min Tjoa, Gregor Wenda
Grafik-Design: Antonia Stanek **Druck:** Friedrich VDV GmbH, 4020 Linz **Erscheinungsweise:** 4 x jährlich.
Aus Gründen der Textökonomie verzichten wir auf geschlechtsspezifische Ausformulierung und den Verweis auf (nicht)akademische Titel.

Herzlichen Dank für die kostenlose Schaltung!

Foto: Alex Wynter/International Federation

DÜRRE IN AFRIKA

HILFE FÜR DIE BETROFFENEN MENSCHEN.

Helfen Sie uns helfen!

PSK 2.345.000, BLZ 60000, Kennwort: „Dürre in Afrika“
Online: spende.roteskreuz.at | SMS: 0664/660 00 20

ÖSTERREICHISCHES ROTES KREUZ

Aus Liebe zum Menschen.

www.roteskreuz.at