Grundsatzbemerkungen zu den Anforderungen der dritten Gewalt an die Administration der Informationstechnik

Staatssekretär Harald Lemke

Vorbemerkungen

Bei allen strategischen Entscheidungen zum Ausbau der Informationstechnik in der Hessischen Landesverwaltung wird darauf hingewiesen, dass bei der konkreten technischen und organisatorischen Ausgestaltung die verfassungsrechtlichen Regelungen der Legislative und Judikative zu berücksichtigen sind.

In diesem Kontext muss auch die IT-Konfiguration der Hessischen Landesverwaltung und die Organisation der HZD betrachtet werden, die als zentrale Einheit Dienstleistungen für die Hessische Landesverwaltung mit ihren nachgeordneten Behörden, dem Hessischen Landtag und den Hessischen Gerichten erbringt.

Die in § 102 HV definierte Ressorthoheit ist nicht Gegenstand dieses Papiers. Die Nutzung der HZD beruht auf zwei Grundlagen:

- Verbindliche Querschnittsverfahren und Standards der Landesverwaltung werden nach Ressortabstimmung einvernehmlich im Kabinett beschlossen.
- Alle optionalen Dienstleistungen werden durch das jeweilige Ressort beauftragt.

In beiden Fällen ist sichergestellt, dass die eigenverantwortliche Leitung des Ressorts durch den zuständigen Minister sichergestellt ist.

Die Kumulation von operativen Aufgaben aller drei Gewalten in einem Geschäftsbetrieb wirft jedoch immer wieder die Frage auf, inwieweit diese Organisationsform die verfassungsrechtliche Unabhängigkeit von Legislative und Judikative beeinträchtigt, insbesondere, weil die HZD der Dienst- und Fachaufsicht der Exekutive, z.Zt. dem HMdF untersteht.

In der damit zusammenhängenden Diskussion wird insbesondere seitens der Richterschaft folgende Argumentationskette verwendet:

1. Vernetzte IT-Arbeitsplätze werden aufgrund des damit verbundenen Nutzens begrüßt, wenn nicht sogar gefordert.
2. Die Administration der IT-Infrastruktur birgt die **Möglichkeit** der Kontrolle der Benutzer.
3. Aufgrund seiner Dienstaufsicht hat der Hessische Finanzminister ein uneingeschränktes Recht auf Auskunft und Prüfung aller Geschäftsvorgänge und **kann** daher die richterliche Tätigkeit kontrollieren.
4. Vor diesem Hintergrund muss die Administration der durch die Richter genutzten IT-Infrastruktur im Geschäftsbereich der Gerichte angesiedelt werden.

Das vorliegende Papier setzt sich mit dieser Problematik auseinander und soll pragmatische Wege aufzeigen, wie das Management einer IT-Infrastruktur so organisiert werden kann, dass die nach § 97 GG verfassungsrechtlich geschützte Unabhängigkeit der Judikative gewahrt bleibt.

Ich halte in diesem Zusammenhang eine pragmatische Sicht im Sinne eines Interessenausgleichs für erforderlich, weil eine Fundamentaldiskussion zu absurden Ergebnissen führen würde, wie die nachfolgenden Ausführungen zeigen.

Begriffsbestimmung IT-Infrastruktur

Wenn unterstellt wird, dass die Administration der IT-Infrastruktur, z.B. das Netzwerkmanagement, ein Risiko für die Unabhängigkeit der Richter birgt, muss zunächst einmal der Begriff der IT-Infrastruktur geklärt werden.

Eine moderne IT-Infrastruktur, wie sie üblicherweise in den Hessischen Gerichten implementiert ist, besteht aus mehreren Architekturblöcken, die durch vielfältige Abhängigkeiten miteinander verbunden sind:

- Arbeitsplatzrechner mit Betriebssystem.
- Lokale Netzwerke (LAN), die in der Regel die IT-Systeme eines Hauses (Arbeitsplatzrechner, lokale Server, Drucker, usw.) miteinander verbinden.
- Das „Wide-Area-Network" (WAN), das die lokalen Netzwerke miteinander verbindet.
- Zentrale Rechnersysteme, die ausschließlich für eine bestimmte Anwendung betrieben werden, z.B. für MESTA oder POLAS.
- Zentrale Rechnersysteme, auf denen mehrere Anwendungen gleichzeitig betrieben werden, z.B. der IBM-Großrechner, auf dem JUKOS und die Steuerverfahren laufen.
- Zentrale Speichersysteme, auf denen die zentralen Rechnersysteme ihre Informationen speichern.
- Anwendungssoftware mit fachspezifischer Funktionalität.
- Systemmanagement-Systeme, mit denen der Betrieb der Einzelkomponenten überwacht und gesteuert wird.
- Systemmanagement-Systeme, die hauptsächlich der Benutzerverwaltung dienen, d.h., in denen festgelegt wird, welche Benutzer auf welche Systeme und Informationen zugreifen dürfen.

Wesentlich in diesem Zusammenhang ist: Der Anwender am PC, der z.B. JUKOS, E-MAIL, DMS oder SAP bedient, kann nicht mehr arbeiten, wenn eine der oben genannten Komponenten ausfällt. Diese funktionskritische Vernetzung hat zwei Konsequenzen:

- Für die Überwachung und Fehlerlokalisierung des Gesamtsystems werden integrierte Systemmanagementwerkzeuge benötigt, mit denen die Konfiguration der gesamten Infrastruktur überwacht werden kann.
- Die Organisation des Systemmanagements muss sicherstellen, dass jede Änderung, Entstörung usw. in abgestimmten Prozessen erfolgt.

IT-Organisation

Organisation folgt der Aufgabe. Dieser Grundsatz gilt auch für die Administration einer komplexen IT-Infrastruktur, wie sie im vorhergehenden Kapitel beschrieben ist. Es liegt auf der Hand, dass eine derartige Konfiguration nur dann sicher betrieben werden kann, wenn alle daran Beteiligten ihre Zusammenarbeit hinreichend genau geregelt haben.

Die Erfahrung zeigt, dass das Management einer IT-Infrastruktur mit einer hierarchischen Organisation und den Instrumenten der Dienstaufsicht nicht möglich ist. Das hat mehrere Gründe, z.B.:

- Weit verzweigte IT-Infrastrukturen werden in mehreren voneinander unabhängigen Organisationseinheiten genutzt. Dieses ist in der Hessischen Landesverwaltung auch der Fall, wo Judikative, Legislative und Exekutive ein gemeinsames Netz und zentrale Systemkomponenten nutzen.
- Das Eigentum an der Infrastruktur befindet sich selten in einer Hand. Auch dieses ist in der Hessischen Landesverwaltung der Fall. So wird das WAN von der Telekom, das Sprachnetz von Arcor, das Personalabrechnungssystem und das Ordnungswidrigkeitenverfahren von der eKom21 betrieben.
- Die Serviceaufgaben werden von unterschiedlichen Organisationseinheiten wahrgenommen, die z.T. außerhalb der eigenen Organisation liegen, z.B. bei Lieferanten, Netzbetreibern oder Serviceprovidern.

Es liegt auf der Hand, dass unter diesen Rahmenbedingungen die Regeln einer hierarchischen Organisation nicht ausreichen, um das Gesamtsystem zu betreiben. Insbesondere zeitkritische Entstörungs- oder Änderungsprozesse erfordern ein Regelwerk, das allen Betei-

ligten ihre Aufgaben und Kompetenzen im Gesamtsystem zuweist, unabhängig davon, in welcher Organisation sie tätig sind.

Dieses organisatorische Rahmenwerk sind die **IT-Prozesse**, für die sich weltweit die ITIL-Standards[1] etabliert haben. Die Regeln dieser IT-Prozesse binden die Beteiligten im operativen Geschäft genau so wie die jeweilige Dienstaufsicht ihrer Organisation. Solche Prozesse gibt es u.a. für

- Das Architekturmanagement,
- Das Problemmanagement,
- Das Änderungsmanagement (Benutzermanagement gehört hierzu)
- Das Sicherheitsmanagement
- Das Betriebsmanagement

Dieses Prinzip organisationsübergreifender Prozesse kann aber nur unter folgenden Bedingungen funktionieren:

1. Wenn diese Prozesse beschrieben sind und alle Beteiligten diese Regeln als Vertragsgrundlage akzeptieren,
2. Wenn die Dienstaufsicht der beteiligten Organisationen sich dem vereinbarten Prozessregime unterordnet und keine Zielkonflikte durch anders lautende Weisungen schafft.

Überwachungsrisiken einer komplexen IT-Infrastruktur

Seit Einführung der Informationstechnik weisen Datenschützer, Betriebs- und Personalräte auf die Risiken hin, die sich aus den objektiven Möglichkeiten der IT-Systeme zur individuellen Leistungs- und Verhaltenskontrolle der Mitarbeiter ergeben. Diese Kontrollrisiken sind auch einschlägig, wenn es um die Sicherstellung richterlicher Unabhängigkeit geht.

Die Kontrollrisiken lassen sich durch vier Maßnahmenbündel minimieren:

1. Ungewollte Kontrolle wird technisch ausgeschlossen oder erschwert.
2. Ungewollte Kontrolle wird durch Organisatorische Maßnahmen, wie z.B. Vieraugenprinzip oder Revision erschwert.
3. Ungewollte Kontrolle wird durch Verträge und / oder Prozesse untersagt.
4. Ungewollte Kontrolle wird durch gesetzliche Maßnahmen, z.B. Datenschutzrecht verboten und sanktioniert.

Die Kosten der oben genannten Maßnahmen sind absteigend, d.h., der technische Ausschluss eines Kontrollrisikos ist in der Regel die teuerste Maßnahme, während der Hinweis auf das Datenschutzgesetz und seine Sanktionen keine weiteren Kosten verursacht.
Vor diesem Hintergrund werden technische und organisatorische Maßnahmen auch unter ökonomischen Gesichtpunkten betrachtet, hier kann auch auf § 10 (1) HDSG verwiesen werden:

Die datenverarbeitende oder in ihrem Auftrag tätige Stelle hat die technischen und organisatorischen Maßnahmen zu treffen, die nach Abs. 2 und 3 erforderlich sind, um die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz zu gewährleisten. Erforderlich sind diese Maßnahmen, soweit der damit verbundene Aufwand unter Berücksichtigung der Art der personenbezogenen Daten und ihrer Verarbeitung zum Schutz des in § 1 Abs. 1 Nr. 1 genannten Rechts angemessen ist.

---

[1] ITIL: IT-Infrastructure-Library, ein Prozessmodell für das Management großer IT-Infrastruktur
ITIL ist ein eingetragenes Warenzeichen von OGC - The Office of Government Commerce

In diesem Zusammenhang muss noch einmal auf die oben beschriebene Systemarchitektur hingewiesen werden. Schutzmaßnahmen in einem derart vernetzten System müssen alle Objekte der Systemarchitektur umfassen, damit sie überhaupt greifen. Das folgende Beispiel soll dieses Problem verdeutlichen:

Wer von seinem Arbeitsplatzrechner auf das Internet zugreift, hinterlässt eine Spur, die sich unter dem Stichwort „Verhaltenskontrolle" auswerten ließe. So Können z.B. mehrere Systemadministratoren mit ihren speziellen Werkzeugen ermitteln, wer wann auf welche Internetseiten zugegriffen hat:

- Der Administrator für den PC
- Der Administrator für das LAN
- Der Administrator für die Verzeichnisdomäne des PCs
- Der Administrator für das WAN
- Der Administrator für den Firewall
- Der Administrator für den Internet-Zugang

Dieses ist nur ein Beispiel, die Liste ließe sich fortsetzen. Tatsächlich unterliegen aber auch die personenbezogenen Systemdaten den Vorschriften des Datenschutzgesetzes. Jeder Administrator, der die Daten missbräuchlich nutzt, begeht einen strafbewehrten Verstoß gegen das HDSG.

Wer nun, wie in der eingangs erwähnten Argumentationskette, dieses Risiko als reale Bedrohung für die richterliche Unabhängigkeit annimmt, der hat eigentlich nur drei Möglichkeiten, das Risiko nennenswert zu minimieren:

- Der Verzicht auf vernetzte Arbeitsplätze, oder
- ein extrem hoher technischer Aufwand, wie er z.B. beim BND oder beim Verfassungsschutz betrieben wird, und
- die vollständige Systemadministration der gesamten Konfiguration unter eigener Kontrolle der Richterschaft.

Eine Systemadministration von Teilkomponenten, z.B. für PC, LAN und Verzeichnisdomäne in Verantwortung der Richterschaft, wie häufig gefordert, hat nur symbolischen Wert, senkt aber nicht das Risiko untreuer Systemadministratoren.

Ein weiterer Aspekt sei noch erwähnt: Auch eine Administration der IT-Infrastruktur durch die Gerichtsverwaltung senkt nicht die Risiko, dass ein Richters durch einen rechtwidrig handelnden Systemadministrator kontrolliert wird. Hier muss die Frage erlaubt sein, wer in einem solchen Szenario ein höheres Interesse an einer Kontrolle eines Richters hat: Der Finanzminister oder der Gerichtspräsident? Meine persönliche Bewertung dieser in dieser Frage ist folgende: Das Szenario, dass ein Finanzminister oder Gerichtspräsident die Tätigkeit eines Richters über die Daten der Systemadministration unrechtmäßig kontrolliert, ist in jedem Falle absurd. Unterstellt man jedoch bei beiden die notwendige kriminelle Energie, so dürfte das Bedürfnis nach derartigen Informationen im direkten Umfeld des Richters größer sein als beim Finanzminister, der mit derartigen Informationen überhaupt nichts anfangen könnte.

Fazit:

Systemadministration ist eine treuhändlerische Aufgabe mit Missbrauchspotenzial, das sich nicht vollständig eliminieren lässt. Wenn dieses Risiko eine ernstzunehmende Bedrohung der richterlichen Unabhängigkeit darstellt, dessen Minimierung sich aus verfassungsrechtlicher Sicht einer ökonomischen Betrachtung entzieht, kann die Lösung nur in einer vollständig eigenen Infrastruktur mit verschlüsseltem WAN liegen, die unter vollständiger Kontrolle der Richterschaft administriert wird. Damit wird das Missbrauchsrisiko jedoch nur in den direkten Bereich des Gerichts verlagert.

Ungehinderter Zugriff auf die IT-Infrastruktur

Ein weiter Aspekt in diesem Zusammenhang ist der ungehinderte Zugriff des Richters auf seine Arbeitsmittel, in diesem Falle auf seinen PC mit den dazugehörigen Programmen.

Um diese Forderung zu erfüllen, sind zwei Voraussetzungen zu schaffen:

1. Die IT-Infrastruktur mit allen Komponenten muss lauffähig zur Verfügung stehen.
2. Die benutzerspezifischen Zugriffsrechte müssen in den benötigten Systemen entsprechend eingerichtet werden.

Der erste Punkt lässt sich über Verträge und Servicevereinbarungen regeln. Auch eine Infrastrukturadministration im Gericht ist nicht in der Lage, ohne fremde Hilfe einen vernetzten PC mit allen technischen Optionen zu installieren und jeden Störungsfall zu beherrschen. Man wird hier immer auf externe Lieferanten und Serviceprovider zurückgreifen müssen. Unabhängig davon, wer dem Richter die Infrastruktur installiert oder entstört, die Initiative geht immer von der Dienststelle aus, die in der Regel auch die Kosten für derartige Aufträge trägt.

Für den zweiten Punkt ist nach derzeitiger Konzeptlage eine dezentrale Benutzeradministration vorgesehen:

- Über SAP HR wird für jeden Beschäftigten ein Basisprofil angelegt, das Grundlage für die weitere Benutzeradministration ist.
- Die konkreten Benutzerprofile, in denen die Zugriffsrechte usw. für jeden Anwender hinterlegt sind, werden in den Dienststellen gepflegt, soweit dieses möglich ist. Hier muss jedoch darauf hingewiesen werden, dass einige zentrale Programme eine zusätzliche Benutzeradministration haben, die in der Regel auch durch die fachlich zuständigen Dienststellen bedient wird.

Fazit:

Auch nach derzeitiger Konzeptlage steuert jede Dienststelle den Zugriff der Anwender auf die Informationstechnik selbst:

- Durch **Aufträge**, mit denen den Anwendern die Infrastruktur zur Verfügung gestellt wird, und
- Durch die **eigene Administration** der Anwenderprofile, in denen der Zugriff der Anwender auf Programme und Daten definiert wird.

Besondere Aspekte der Vertraulichkeit

Aus der persönlichen und fachlichen Unabhängigkeit des Richters wird auch abgeleitet, dass Schriftstücke u.ä. als persönliches Eigentum des Richters zu bewerten sind, solange sie nicht Bestandteil der Gerichtsakte sind. Für die weiteren Ausführungen gehe ich von dieser Rechtsauffassung aus.

In der Konsequenz bedeutet das, dass der Richter seine persönlichen Informationen hinsichtlich der Vertraulichkeit selbst klassifiziert.

An dieser Stelle setzt die Infrastruktur der Landesverwaltung Grenzen, da sie nur für Daten bis zur Klassifikation VS-NfD ausgelegt. Ein höherer Schutz, z.B. VS-Geheim, lässt sich aus technischen, organisatorischen und finanziellen Gründen nicht implementieren.

Daraus folgt: Wenn ein Richter seine persönlichen Daten als VS-Geheim klassifiziert und jeden nicht persönlich autorisierten Zugriff ausschließen will, scheidet der dienstlich zur Verfügung gestellte PC grundsätzlich aus. Es gibt keine technische Möglichkeit, die Daten auf einem vernetzten Windows-System vor einem kriminell handelnden Systemadministrator zu schützen. Auch die verschlüsselte Ablage bietet nur vordergründigen Schutz:

- In der Regel werden bei der Bearbeitung von Dateien, z.B. mit WORD, temporäre Systemdateien angelegt, die ein krimineil handelnder Systemadministrator mit seinen Mitteln auswerten kann.
- Wenn die zu schützenden Dateien zur Bearbeitung geöffnet sind, könnte ein kriminell handelnder Systemadministrator über das Netz auf den PC und die offenen Dateien zugreifen.

Die Liste ließe sich fortsetzen.

Aus dieser Unzulänglichkeit der Technik können drei Handlungsalternativen abgeleitet werden:

1. Der Richter verzichtet vollständig auf den vernetzten PC, wenn er persönliche Dateien bearbeitet.
2. Die Gerichte bauen ein eigenes VS-Netz unter eigener Kontrolle auf.
3. Der Richter verwendet ein Verschlüsselungsprogramm für eigene Dateien, um zufällige Kenntnisnahme auszuschließen.

Die erste Alternative liegt in alleiniger und persönlicher Verantwortung des Richters und ist immer eine Option.

Die zweite Alternative scheidet aus wirtschaftlichen und organisatorischen Gründen aus. Ein VS-Netz ist zunächst sehr teuer und darf nicht mit anderen Netzen (schon gar nicht mit dem Internet) verbunden sein, d.h., die Gerichte bräuchten eine zweite Infrastruktur für den Zugriff auf landesweite IT-Ressourcen.

Die dritte Alternative wäre ein Kompromiss, der für geringe Kosten einen Grundschutz bietet, aber keine absolute Sicherheit vor unbefugtem Zugriff bietet. Eine entsprechende Verschlüsselung könnte im Zuge der Digitalen Signatur eingeführt werden, was den Vorteil hätte, dass keine besonderen Administrationskosten für die Verschlüsselung anfallen würden.

Empfehlung

Die pauschale Anforderung, dass die richterliche Unabhängigkeit eine IT-Administration unter der Dienstaufsicht der Gerichte erforderlich macht, kann nur pauschal befriedigt werden, wenn jedem Gericht eine vollständig eigene IT-Infrastruktur zur Verfügung gestellt wird, die vom Gericht allein betrieben wird. Alle Lösungen unterhalb dieser unbezahlbaren Radikallösung sind angesichts der pauschalen Anforderung beliebig.

Im übertragenen Sinne ist es wirkungslos, die Eingangstür eines Hauses mit hohem Aufwand zu sichern, während die Hintertür offen bleibt. Es kommt auch in der IT-Sicherheit auf eine vernünftige Balance aller Maßnahmen an.

Auf Grundlage der eingangs beschriebenen Argumentation hätte die geforderte Netzwerkadministration durch die Gerichte nur symbolischen Charakter, allerdings mit Türöffnerfunktion: mit der gleichen Begründung könnte sukzessive eine vollständig eigenständige und unabhängige IT-Konfiguration und Administration für jedes Gericht eingefordert werden.

Vor diesem Hintergrund scheint mir eine differenzierte Vorgehensweise angezeigt, in der das pauschale Missbrauchsszenario konkretisiert wird, um gemeinsam mit dem HMdJ und der Richterschaft eine sachgerechte und wirtschaftliche Lösung für die Problematik abzustimmen. Hierfür bieten sich die nächsten Monate an, da im Zuge einer Reorganisation der HZD die entsprechenden Serviceprozesse neu gestaltet werden. Ich kann an dieser Stelle schon ankündigen, dass in diesem Rahmen auch die Innenrevision der HZD auf dem Prüfstand steht. Ich halte es für sinnvoll und erforderlich, dass in diesem Zuge auch die Belange von Steuerverwaltung, Polizei, Staatsanwaltschaft und Rechtsprechung berücksichtigt werden.

Grundlage einer differenzierten Diskussion muss aber ein rechtlicher Rahmen sein. Der diesbezüglichen Literatur entnehme ich, dass hier es auch innerhalb der Richterschaft kont-

räre Meinungen gibt, ich zitiere hier zur Gegenüberstellung der eingangs erwähnten Auffassung aus einem Beitrag zu diesem Thema:

„ Aus dem Grundgesetz ergibt sich kein striktes Gebot der Gewaltentrennung. Es geht, wie der Präsident des BVerfG formulierte, um sachgerechte Zuordnung und Balancierung der Teilgewalten. Die Gewaltenteilung dient der Missbrauchsabwehr, nicht der Lähmung des Staates Aus der Garantie der richterlichen Unabhängigkeit in Art. 97 GG kann die Selbstverwaltung der Gerichte nicht abgeleitet werden. Sie hat eine andere Schutzrichtung als die Autonomie der dritten Gewalt. Persönliche und sachliche Unabhängigkeit kommt dem Status des Richters zu, nicht der Institution der Gerichte. ...“ (Elmar Herrler)

Ich möchte mir keine rechtliche Meinung zu diesem Thema anmaßen.

Vor diesem Hintergrund halte ich es für erforderlich, dass das HMdJ zunächst seine Rechtsposition in dieser Frage klärt, damit die Diskussion nicht in technischer und organisatorischer Beliebigkeit verläuft.

Ich versichere, dass ich mir jede Lösung vorstellen kann, die rechtliche, fachliche, technische und wirtschaftliche Interessen berücksichtigt und am Ende Verbindlichkeit für alle Beteiligten schafft. Eine fundamentale Diskussion mit pauschaler Argumentation kann aber nur in Radikallösungen oder faulen Kompromissen enden, beide Optionen wären nicht sachgerecht.