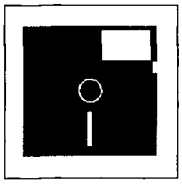
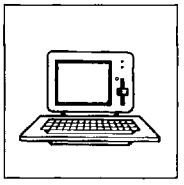



Anforderungen an ein gerichtliches Sicherheitssystem

Friedrich Albrecht

Rechtliche Grundlagen

Rechtliche Grundlagen für das Sicherheitssystem eines Gerichts in einer offenen EDV-Welt, etwa in einer Client-Server-Architektur, sind die Datenschutzgesetze des Bundes, der Länder, sowie die Art. 1 und 2 GG in ihrer Interpretation durch das Bundesverfassungsgericht[1] sowie einschlägige bereichsspezifische Normen.

Stand-alone PC oder im Netz: Wo sind die Gefahren größer?

Daß in einer modernen Systemarchitektur Server, meist unter UNIX, und PCs, meist unter DOS, gekoppelt werden, macht gegenüber reinen PC-Netzen und sogar gegenüber Stand-alone-PCs kaum noch einen rechtlichen Unterschied. Die Verarbeitungskapazität vieler PCs reicht heute an das heran, was vor einigen Jahren noch Großrechenanlagen vorbehalten war. Nicht zuletzt deshalb hat sich der Gesetzgeber[2] dafür entschieden, daß die Regeln des Bundesdatenschutzgesetzes auch für die Datenverarbeitung auf dem PC Anwendung finden. Die ständig weiter um sich greifenden Vernetzungsmöglichkeiten und damit der Zugriff auf immer größere Datenmengen lassen es zwar auf den ersten Blick so aussehen, als müßten die datenschutzrechtlichen Probleme bei Vernetzung noch drückender sein. Dem ist aber gar nicht so. Gerade in vernetzten Systemen bieten sich nämlich viel mehr Möglichkeiten, Datenschutz und Datensicherheit zu realisieren, als an Stand-alone-PCs.

Schutzmaßnahmen müssen verhältnismäßig sein!

Den Schutzzweck des Datenschutzrechts legt § 1 BDSG fest. Der Einzelne ist danach davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Dabei kann es nicht um den Schutz vor der kleinsten Beeinträchtigung um jeden Preis gehen. Das macht § 9 Satz 2 BDSG deutlich, der nur solche Maßnahmen für erforderlich erklärt, deren Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Damit eröffnet § 9 Satz 2 BDSG ein flexibles Reaktionspotential, in dem unter Berücksichtigung der Verhältnismäßigkeit die Schwere der Beeinträchtigung, die Sensitivität der gespeicherten personenbezogenen Daten und die Wahrscheinlichkeit des Eintritts einer Beeinträchtigung gegen den Schutzaufwand zur Verhinderung der Beeinträchtigung abzuwägen sind.

Auch der allgemeine Grundsatz der Verhältnismäßigkeit besagt, daß die datenverarbeitende Stelle in zulässiger Weise erhobene Daten mit angemessenen Mitteln auf einem möglichst niedrigen Gefährdungsniveau zu halten hat. Dabei sind die dem jeweiligen Gefährdungsniveau adäquaten technischen und organisatorischen Maßnahmen zu treffen. Ein höheres Gefährdungsniveau führt naturgemäß zu höheren Anforderungen an technische und organisatorische Datensicherungsvorkehrungen, deren Kosten dann weniger ausschlaggebend sein dürfen. Zunächst sind also die tatsächlich drohenden Gefahren festzustellen.

Gefahren und Risiken

Persönlichkeitsrechte

Im Umgang mit personenbezogenen Daten könnte das Persönlichkeitsrecht des Betroffenen in dreierlei Hinsicht verletzt werden:

- Datenintegrität,
- Datenvertraulichkeit und
- Zweckbindung im Umgang mit den Daten.

Verfügbarkeit

Zur Datensicherheit im allgemeinen gehört auch die Verfügbarkeit der Daten für den berechtigen Nutzer, die für den Anwender so wichtig ist, aber von § 9 BDSG nicht umfaßt wird.

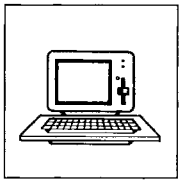
Datenintegrität

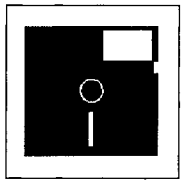
Die Datenintegrität spricht den Schutz vor der Verfälschung personenbezogener Daten an. Daten können sowohl durch nicht berechtigte Nutzer, die in das System einbrechen, wie durch berechtigte Nutzer bedroht werden. Die Wahrscheinlichkeit, daß der berechtigte

Friedrich Albrecht ist Richter am Bundespatentgericht und Referatsleiter für Informationstechnik.

[1] vgl. BVerfGE 65, 1 ff (Recht auf informationelle Selbstbestimmung)

[2] vgl. Materialien zur Novellierung des Bundesdatenschutzgesetzes





Nutzer eines Programms falsche Daten einträgt, erscheint indessen gering. Maßnahmen zum Schutz der Datenintegrität sind daher hauptsächlich mit Blick auf unberechtigte Nutzer ins Auge zu fassen.

Datenvertraulichkeit

Geheimhaltung

Die Datenvertraulichkeit gebietet die Geheimhaltung der zulässigerweise erhobenen und verarbeiteten personenbezogenen Daten und damit den Schutz vor der Kenntnisnahme und vor Nutzung durch Unbefugte.

Zweckbindung

Schutz gegen zweckwidrige Verarbeitung

Die Zweckbindung schützt vor der Verarbeitung und Nutzung zu anderen Zwecken als denen, zu denen die personenbezogenen Daten erhoben worden sind und zu denen ihre Verarbeitung erlaubt ist. Für diesen Bereich sind nicht nur die generell Unbefugten, sondern auch die ursprünglich Befugten ins Auge zu fassen.

Kontrollmöglichkeiten

Kontrolle des Arbeitsverhaltens

Die Verantwortlichen für die Informationstechnik haben aber nicht nur die Belange der Bürger und Anwälte zu berücksichtigen, sondern auch, daß die Anwender Datenschutz für sich selbst beanspruchen. Unbestritten dürfte es dabei sein, daß die Speicherung, Verarbeitung und Verwertung von Personaldaten mitbestimmungspflichtig[3] ist. Insoweit gelten die oben gezeigten Belange. Wegen der Empfindlichkeit gerade der Personaldaten ist ihre Zusammenführung mit anderen Daten, insbesondere Statistikdaten, auszuschließen. Hinzu kommt nun noch die Gefahr unzulässiger Erhebungen und Auswertungen des Arbeitsverhaltens. Sie beruht unter anderem auf folgenden Möglichkeiten in einem informationstechnischen System:

- Es kann festgehalten werden, wer sich wann ein- bzw. ausloggt.
- Es kann festgestellt werden, wer im Zeitpunkt der Feststellung eingeloggt ist.
- Es könnte jeder Tastendruck jedes Benutzers aufgezeichnet werden.
- Die Systemverwalter könnten jede Datei jedes Benutzers einsehen.

Wer loggt sich wann ein und aus?

Wer arbeitet gerade im System?

Die Aussagekraft der ersten beiden Erhebungen erscheint mir gering, zumal die wenigsten Arbeitsplätze so eingerichtet sind, daß an ihnen nur und dauernd am PC gearbeitet werden müßte. Richter- und Rechtspflegerarbeitsplätze fallen hierunter sicher nie.

Wer arbeitet gerade?

Die zweite Erhebung liefert ohnehin nur eine Momentaufnahme. Trotzdem muß die Erfassung solcher Daten so weit als möglich ausgeschlossen werden. Technisch ist dies wie auch die Verhinderung der Aufzeichnung aller Tastenbedienungen eines Anwenders nicht möglich, da ein Systemverwalter als sog. Super-User sich selbst die Rechte zu solchen Erhebungen einräumen könnte. Hier bleibt nur die Möglichkeit, durch Dienstvereinbarungen, Anweisungen etc. die Bediensteten zu verpflichten, derartiges zu unterlassen.

Zum Erfassen jedes Tastendrucks müßte ein erheblicher technischer Aufwand betrieben werden, der den anderen Systembetreuern auffallen würde. Insoweit gibt auch das Vier-Augen-Prinzip einen Schutz. Somit bleibt als später noch zu behandelndes Risiko die uneingeschränkte Einsichtnahme der Systemverwalter.

Im Rahmen von Lizenzrechten wird oftmals überprüft, wieviele Anwender gleichzeitig auf eine Software zugreifen. Auch diese Erhebung ist meines Erachtens nicht zu fürchten, gibt sie doch nur Momentaufnahmen. Man kann allerdings sogar dies vermeiden, wenn man lediglich weitere Benutzer solange nicht auf die Software zugreifen läßt, bis sich die Zahl der Benutzer wieder verringert. Eine Speicherung der jeweiligen Anzahl oder der Höchstzahl gäbe aber ohnehin keine Aussagen über das Arbeitsverhalten einzelner.

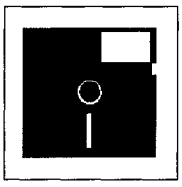
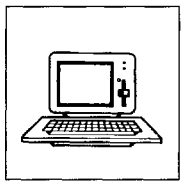
Weitere Gefahren

Gefahren über Gefahren

Um weitere Gefährdungen der Datensicherheit und des Datenschutzes zu erkennen, verwende man Listen, die ich im folgenden nur schlaglichtartig darstellen kann. Nach ihnen ließen sich beispielsweise folgende Punkte untersuchen:

---

[3] vgl. Novellierung des Personalvertretungsgesetzes

Organisation
organisatorische Mängel
Regelungen, Betriebsmittel, Kontrolle, Wartung
Personal
Menschliche Fehlhandlungen
Notfallvorsorge
Gebäude
Blitz, Feuer etc.
Zutritt
Stromversorgung, Spannungsschwankungen
Überspannung/Unterspannung
Vorsätzliche Handlungen: Einbruch, Anschlag
Gefährdung durch Reinigungs- oder Fremdpersonal
Verkabelung
Kabelbrand
Kapazitätsengpaß, Verteiler
Menschliche Fehlhandlungen: unzulässige Kabelverbindungen, Beschädigung
Vorsätzliche Handlungen: Abhören, Manipulation an Leitungen
DOS-PC
Diebstahl, Computerviren
und vieles andere mehr – jeweils für jede Anwendung, jedes Modul usw.

Gefahren beim Einsatz privater Software

Folgende Gefährdungen sehe ich bei der so umstrittenen Nutzung nicht dem Standard entsprechender Software:

- unerlaubte Ausübung von Rechten, unberechtigte Nutzung
- unkontrollierter Einsatz von Betriebsmitteln
- mangelhafte Anpassung an Veränderungen
- Nichtbeachtung von Sicherheitsmaßnahmen
- Manipulation an Daten oder Software
- fahrlässige Zerstörung von Gerät oder Daten
- fehlerhafte Nutzung des Systems
- Übertragung von Fehlern auf das System
- Computerviren

Kriterien

Verhältnismäßigkeit von Schutzmaßnahmen

Um festzustellen, welche Maßnahmen angebracht sind, bestimmte Gefährdungen auszuschließen, können folgende Kriterien Hilfe sein:

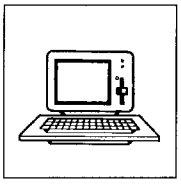
Verstoß gegen Gesetze, Rechtsverordnungen und andere Vorschriften
Es ist zu fragen, ob Gesetze, Rechtsverordnungen und andere Vorschriften (Richtlinien, Dienstanweisungen etc.) verletzt werden.

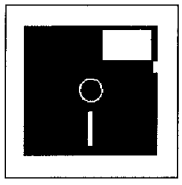
Beeinträchtigung der Aufgabenerfüllung
Hier wird die Bedeutung der IT-Anwendung und Informationen in bezug auf die Gesamtaufgabe der Behörde betrachtet. (z. B.: Bei fehlerhaftem Verhalten der eingesetzten Software muß sicher gestellt sein, daß korrekt arbeitender Ersatz installiert werden kann.)

Außenwirkung, Ansehens- und Vertrauensbeeinträchtigung

Datenschutz und Datensicherheit: Nicht 'störender Sand im Getriebe'

Zu betrachten ist nunmehr die Wirkung eines Schadens außerhalb der Behörde, wie z.B. Vertrauens- oder Ansehensverlust in der Öffentlichkeit, Schädigung politischer oder gesellschaftlicher Gruppen, Beziehungen zu Klienten und anderen Behörden. Betont werden muß in diesem Zusammenhang, daß Mängel hinsichtlich Datenschutz und Datensicherheit in der Justiz besonders belastende Auswirkungen auf Rechtssuchende und Anwaltschaft haben. Maßnahmen des Datenschutzes und der Datensicherheit werden aber trotzdem innerhalb der Justiz vielfach noch – insbesondere von den sich auf ihre Unabhängigkeit berufenden Richtern – als störender "Sand im Getriebe" angesehen. Nicht wenige Richter argwöhnen, ihre Unabhängigkeit werde durch Sicherheitsmaßnahmen beeinträchtigt. Sie übersehen dabei, daß zwischen datenschutzrechtlichen Grundprinzipien und Grundprinzipien gerichtlicher Verfahren ohnehin "Ähnlichkeiten" bestehen. Die Einhaltung der Gebote des Datenschutzes braucht also keinesfalls zu einer Verhinderung eines aufgabenadäquaten Einsatzes von Informationstechnik zu führen. Sie gebieten es lediglich, die datenschutz-





rechtlichen Randbedingungen frühzeitig in alle Planungen einzubeziehen und bei der Realisierung zu beachten.

Innenwirkung
Es ist zu überlegen, auf welcher Ebene die Verantwortlichen mit Konsequenzen zu rechnen haben. Dies betrifft sowohl Konsequenzen, die sich unmittelbar aus der Verletzung von Gesetzen und Vorschriften ergeben (z.B. strafrechtlich, disziplinarisch) als auch Konsequenzen durch politischen/öffentlichen Druck, z.B. Rücktritt.

Interne Konsequenzen

Finanzielle Auswirkung
Hierunter fallen Sachschäden, zusätzlicher Aufwand (z.B. für Wiederherstellung) sowie Kosten durch Manipulationen, unberechtigte Kenntnisnahme oder Nichtverfügbarkeit. Damit werden über diesem Aspekt sowohl unmittelbare als auch mittelbare Kosten abgedeckt.

Schaden

Sensitivitätsgrad
Er bezieht sich auf die Sensitivität der IT-Anwendung (z.B. vertrauliche Algorithmen) und der Informationen (personenbezogene, VS- oder andere sensitive Daten, wie z.B. behördeninterne Informationen oder sensitive Informationen aus Unternehmen).

'sensitive' Bezugspunkte

Dauer der Verzichtbarkeit
Hier wird die Abhängigkeit der Aufgabenstellung von der IT-Anwendung und deren Informationen betrachtet, d.h. über welchen Zeitraum auf die Anwendung oder die Informationen verzichtet werden kann, ohne daß die Aufgabenerledigung nicht zu sehr verzögert wird. Die Aktenlage muß innerhalb dieses Zeitraums die manuelle Erledigung der Aufgabe ermöglichen.
Die Kriterien sind zu bewerten und für die einzelnen Anwendung auf diese Weise die Gefahren einzuschätzen. Hat man die Risiken erkundet und deren Wahrscheinlichkeit sowie ihre möglichen Auswirkungen bedacht, kommt man zu den Maßnahmen für die Realisierung des IT-Grundschutzes. Auch hier wieder nur einige Schlaglichter:

Notfalls: Manuell per Akte

Maßnahmen und ihre Auswirkungen

Einen Maßnahmenkatalog bieten diverse Arbeitshilfen an. Anhand deren kommen wir zum Beispiel zu folgenden Bereichen:

Organisation

Standards erforderlich

- Festlegung von Verantwordichkeiten und Regelungen für den IT-Einsatz. (Dies verlangt einheitliche Regelungen ohne große Abweichungen vom Standard.)
- Aufgabenverteilung, Funktionstrennung
- Betriebsmittelverwaltung, Datenträgerverwaltung
- Vergabe von Zutrittsberechtigungen
- abzuschließende Türen, Schlüsselverwaltung
- Beaufsichtigung oder Begleitung von Fremdpersonen
- Paßwortschutz, Regelung des Paßwortgebrauchs
- Vergabe von Zugriffsrechten

Personal

Auf Standard verpflichten

- Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Regelungen
- geregelte Einarbeitung neuer Mitarbeiter (Kann nur hinsichtlich des Hausstandards erfolgen.)
- Vertretungsregelungen
- Schulung vor Programmnutzung (Kann nur hinsichtlich des Hausstandards erfolgen.)
- Schulung zu IT-Sicherheitsmaßnahmen (Kann nur hinsichdich des Hausstandards erfolgen.)

Gebäude

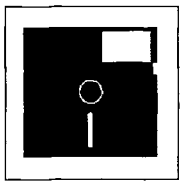
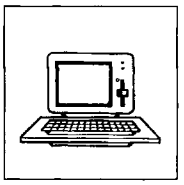
Gebäudeschutz

- unterbrechungsfreie Stromversorgung, Aufteilung der Stromkreise
- Lagepläne der Versorgungsleitungen

Verkabelung

Netzschutz

- Brandabschottung von Versorgungs-Trassen
- Entfernen oder Kurzschließen und Erden nicht benötigter Leitungen
- Dokumentation und Kennzeichnung der Verkabelung

DOS-PC

Regelung für Wartungs- und Reparaturarbeiten (Wäre erschwert bei Geräten, die nicht dem Standard entsprechen!)
Nutzungsverbot nicht freigegebener Software
Überprüfung des Softwarebestands
Herausgabe einer PC-Richtlinie (Kann nur hinsichtlich des Hausstandards erfolgen.)
Verschluß der Diskettenlaufwerksschächte
Bildschirmsperre
Regelmäßiger Einsatz eines Viren-Suchprogramms, Verhaltensregeln bei Auftreten eines Computervirus
Erstellen einer PC-Notfalldiskette (Kann nur hinsichtlich des Hausstandards erfolgen.)
regelmäßige Datensicherung (Kann nur erfolgen, wenn die Programme Daten auf den Servern sichern oder ein Remotezugriff freigegeben wäre.)

Maßnahmen im Netz

Servergestütztes PC-Netz

regelmäßiger Sicherheitscheck des Netzes
Protokollierung am Server
geeignete Aufbewahrung der Backup-Datenträger
Sicherungskopie der eingesetzten Software
sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
regelmäßige Datensicherung der Server-Festplatte

Zentrale Datensicherung

Bei alledem zeigt sich die große Bedeutung von Hausstandards. Abweichungen davon erschweren einen Großteils gerade der wichtigsten Maßnahmen. Es zeigen sich aber auch die oben schon angesprochenen Möglichkeiten eines besseren Sicherheitskonzeptes in vernetzten Systemen als bei alleinstehenden PCs. Erfolgt die Dateiablage generell auf zentralen Servern (Etagenservern), so werden zudem alle Dateien von der *zentralen* Datensicherung erfaßt und der Anwender braucht sich nicht selbst um die Sicherung seiner Daten zu kümmern.

Netzkontrolle

Die ständige Funktionskontrolle des Netzes kann vom Arbeitsplatz des Systembetreuers mit Hilfe einer Netzwerk-Management-Station erfolgen.
Der PC, auf dem neue Programme, Disketten etc. getestet werden, darf natürlich nicht in das Netzwerk eingebunden sein.

Remote-Zugriff

Wollte man die Einsichtsmöglichkeiten der Systemverwalter begrenzen, müßte ein Remotezugriff über das Netz auf Daten verhindert werden. Dies erschwert aber zentrale Fehlerbehebung und Update-Verwaltung. Letzterem würde ich jedoch größeres Gewicht beimessen, kann sich doch jeder Benutzer gegen Einsichtnahme in seine Dateien selbst schützen, indem er vertrauliche Daten nur verschlüsselt und/oder auf Diskette speichert.

Löschen ist nicht Vernichten

In Benutzerhinweisen ist übrigens deutlich darauf hinzuweisen, daß lediglich in den Papierkorb gelegte Dateien nicht gelöscht sind, sondern rekonstruiert werden können. Abhilfe bieten insoweit sogenannte Shredder, die das Wiederherstellen von gelöschten Dateien verhindern.

On-line-Verbindungen zu anderen Dienststellen

Online-Verbindungen

Grundsätzlich sollte man nicht für die Öffentlichkeit bestimmte Daten nicht über öffentliche Wählleitungen (Datex-P) – sondern nur über Standleitung – zugänglich machen.

Zugriffsrechte

Herzstück der Datensicherheit und des Datenschutzes

Die Systemsicherheit erlaubt keine uneingeschränkten Benutzerrechte. Hierzu ist eine Sicherheitssoftware einzusetzen. Dies ist bei einigen Behörden SafeGuard professional. Das Programm organisiert den Zugang – auch auf die Diskettenlaufwerke. Das halten Datenschutzbeauftragte für ausreichend[4].

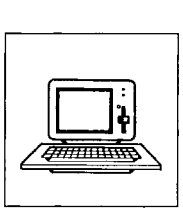
Mindestens 6 Schutzebenen

Die Schutzebenen sind im einzelnen:

- Erstzugang zum System, benutzerspezifisches Grundmenü, Festlegung von Daten- und Programmbereichen, lokale Festplattenzugriffe
- hard- und softwareseitiger Diskettenlaufwerkschutz
- Zugriffe auf Datenbereiche auf dem Server, die über das Netz zur Verfügung gestellt werden

---

[4] vgl. Rüßmann, Wie sind PCs und Personal Computing datenschutzrechtlich zu behandeln?, jur-pc 1993, 2351, 2356 vorletzter Absatz



- Zugriffe auf Programme und Verfahrensdaten unter dem Serverbetriebssystem
- Mailsystem (Zulassung zur Teilnahme am System der elektronischen Post)
- Zulassung zur Arbeit mit der Gerichtsverfahrens-Software überhaupt und Festlegung der Zugriffe auf Verfahrensdaten

Die Systembetreuung muß den Daten- und Systemzugriff durch die Anwender getrennt in diesen verschiedenen Ebenen, die jede für sich einen eigenen Zugriffsschutz bietet, regeln. Dies ermöglicht es dann, jedem Benutzer all das, was er für seine tägliche Arbeit benötigt, bereitzustellen, alles andere dagegen vor dem Zugriff durch ihn zu schützen. Ausschließlich die Mitarbeiter der Systembetreuung dürfen Zugriffsrechte vergeben können, neue Benutzer einrichten sowie die jeweiligen Änderungen bei Zuständigkeits- oder Funktionswechsel vornehmen. Beim Datenzugriff ist die Zugriffsart – je nach den spezifischen Anforderungen des Arbeitsplatzes – festzulegen (kein Zugriff, nur lesender Zugriff oder lesender und schreibender Zugriff). Bestimmte Datenbereiche sind nur einzelnen Benutzern oder genau spezifizierten Gruppen von Benutzern zur Verfügung zu stellen.

Systemzugang und Paßwort

Der Systemzugang darf nur den eingerichteten Benutzern möglich sein. Bei Inbetriebnahme eines PC-Arbeitsplatzes muß die Eingabe des Nutzernamens und des von diesem Nutzer vergebenen Paßwortes verlangt werden. Paßworte müssen eine Mindestlänge haben. Fünf Zeichen bieten sich hier als realistisch an. Es ist Zeichenmischung zu fordern, d.h. das Paßwort muß aus mindestens einem Buchstaben und mindestens einer Zahl bestehen. Das Paßwort darf nicht aus einfachen Buchstaben- oder Ziffernkombinationen oder aus leicht zu erratender Namen, z.B. dem Namen naher Angehöriger oder Monatsnamen, bestehen. Jeder Nutzer hat sein Paßwort vertraulich zu behandeln und es keinem Dritten mitzuteilen. Die schriftliche Aufzeichnung ist zu vermeiden.

Verdeckte Paßworteingabe

Die Paßworteingabe darf nur unbeobachtet erfolgen. Ist das Paßwort einem Unbefugten bekannt geworden oder besteht ein entsprechender Verdacht, ist unverzüglich ein neues Paßwort zu vergeben. Paßwörter sind vom System zu verschlüsseln.

Begrenzte Paßwort-Gültigkeit

Das Paßwort muß in einem festgelegten Turnus gegen ein neues gewechselt werden. Zeitliche Überziehungen muß das System anzeigen. Nach drei Fehlversuchen mit falschen Paßwörtern hat eine Rechnersperre zu erfolgen, die nur vom Systemverwalter aufgehoben werden kann. Jeder Benutzer muß sein Paßwort jederzeit ändern können. Eine Mindestgeltungsdauer muß aber dafür sorgen, daß niemand sein Paßwort so oft hintereinander ändert, bis er wieder das alte eingeben kann.

Die Systembetreuer dürfen vom Benutzer vergebene Paßwörter nicht rekonstruieren, sondern lediglich löschen können, so daß der Benutzer anschließend ein neues Paßwort vergeben muß.

Bei Abwesenheit von mehr als drei Tagen ist das Zugriffsrecht des Abwesenden zu sperren.

Verbot privater Software

BMJ-Handreichungen 4.4

In den Hinweisen zur Sicherheit beim Einsatz von APCs des Bundesamts für Sicherheit in der Informationstechnik[5] wird darauf hingewiesen, daß "der Einsatz privater Software ...[6] zu dienstlichen Zwecken nicht zulässig ist. Bestehende Ausnahmeregelungen sollen zum frühest möglichen Zeitpunkt aufgehoben werden". Für Bundesgerichte ist die Nutzung privater oder privat erstellter Software ebenso nach 4.4 der BMJ-Handreichungen grundsätzlich zu verbieten. Der einzelne Anwender/Benutzer hat gegenüber dem Gerichtspräsidenten (bei Richtern) bzw. der Verwaltung eine schriftliche Erklärung betreffend die Einhaltung von Datenschutz und Datensicherheit abzugeben. Sie hat u.a. zu enthalten:

- Ausschließlichkeit des Einsatzes der von der zentralen IT-Stelle freigegebenen Hard- und Software
- Einhaltung der vorgegebenen Datensicherheitsmaßnahmen
- Verbot, PCs zweckentfremdet einzusetzen und nicht lizenzierte Software (private Programme, Raubkopien, Daten usw.) einzusetzen

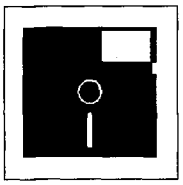
Diese strikte Handhabung hat auch gute Gründe.

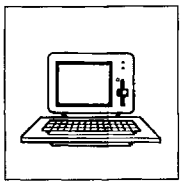
Die öffendiche Verwaltung ist auf das einwandfreie Funktionieren und die uneingeschränkte Verfügbarkeit ihrer informationstechnischen Systeme und der darin verarbeiteten Daten angewiesen. Auch im Hinblick auf die Außenwirkung ist dies zu gewährleisten.

---

5 früher ZSI, Hinweise Nr. 9021 Nr. 2.9

6 und sogar privater PCs, worauf in diesem Aufsatz aber nicht näher eingegangen werden soll





Die dazu erforderlichen Maßnahmen sind abhängig vom Umfeld, insbesondere von der Komplexität des Systems, in das PCs eingebunden sind. Sie haben sich in erster Linie am Schutzbedürfnis der Daten, von denen Kläger und Beschwerdeführer eine vertrauliche Behandlung in besonderem Maße erwarten dürften, sowie des Systems zu orientieren und erst in zweiter Linie an den Interessen der Anwender.

Kosten bei Virenbefall

Daneben stehen wirtschaftliche Überlegungen. Um einen virenbefallenen PC wieder in einen ordnungsgemäßen Zustand zu versetzten, ist ein Aufwand von ca. 1000 DM notwendig.

Höhere Kosten ohne Standards

Auch der Betreueraufwand steigt bei nicht dem Standard entsprechenden Anwendungen in extreme Höhe, will man einem Nutzer, der Probleme hat, nicht unter Verlust aller über den Standard hinaus geschaffenen Dinge, einfach die Standardversion neu aufspielen. Über den Standard hinausgehende Software darf die Systemverwaltung und -benutzung aber nur unwesentlich belasten. Dies ist bei vielfältigen und unterschiedlichen Wünschen nicht gegeben, da die Software jeweils zunächst allein und danach im Gesamtsystem getestet werden muß. Vor der Installation durch die Systemverantwortlichen ist eine Prüfung auf Viren sowie auf Systemkompatibilität durchzuführen. Einspielen, Fehlerbehebungen und häufig wiederkehrende Updates sind jeweils individuell durchzuführen.

Verlust von Garantiezusagen

Die wohl vertragsmäßig erforderliche Abstimmung mit einer für das Gesamtsystem verantwortlichen Firma kostet ebenfalls Zeit und Geld. Ohne diese Abstimmung aber würden Garantiezusagen ihren Wert verlieren und beim Auftreten von Fehlern würden kostenintensive Arbeiten außerhalb der Garantie und der regelmäßigen Wartung anfallen.

DOS und sein Treiberproblem

Zudem lassen die bei komplexen Systemen mit einem hohen Treiberbedarf auftretenden Speicherplatzprobleme im DOS-Bereich nicht zum Standard gehörende Software als zusätzliche Installation kaum zu.

Wirtschaftlichkeit nur bei umfassender Kompatibilität

Private Software bietet ferner in der Regel kein Zugriffskontrollsystem. Fehlerhafte Hard- und Software bedroht die Integrität der Programme und Daten sowie die Verfügbarkeit des Systems und der Daten. Über das Netz erstrecken sich die Bedrohungen auf Netzkomponenten (Etagenserver, Kommunikationsserver etc.) und auf andere PCs. Der Einsatz nicht zentral beschaffter Software birgt die Gefahr, daß es zu gefährlichen Veränderungen an Programmen und Daten durch Viren oder anderen Einwirkungen kommt. Außerdem besteht die Gefahr einer unzweckmäßigen und unrationellen Nutzung der PCs mangels Standard, mangels Schulung, mangels Wartung und Weiterentwicklung. Soweit Programme von Standardprodukten nicht unterstützt werden, wird außerdem deren Wirtschaftlichkeit beeinträchtigt. Nicht ganz billige objektorientierte Oberflächen sind überflüssig, wenn nicht WINDOWS-fähige Programme im sog. DOS-Fenster aufgerufen werden. Allein dafür ist eine graphische Oberfläche nicht zu vertreten. Zudem bietet das geöffnete DOS-Fenster unter WINDOWS dem Anwender die Möglichkeit, Sicherheitsvorkehrungen zu umgehen, etwa die Sperre der Betriebssystemebene.

Der Dienstherr darf nicht von 'Freaks' abhängig sein.

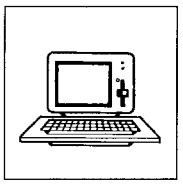
Das Verbot privater Software gilt aber auch, weil durch den dienstlichen Einsatz privater Software häufig Abhängigkeiten des Dienstherrn von einzelnen Mitarbeitern entstehen, indem konventionell vorgeschriebene Verfahrensabläufe durch einzelne Mitarbeiter abgeändert werden und nur noch über "Herrschaftswissen" steuerbar sind. Das ist für die generelle Verwaltungsstruktur (Organisationsgewalt des Dienstherrn) nicht hinnehmbar.

Isolierte PC's: Weder sinnvoll noch wirtschaftlich

Isolierte PCs lösen zwar ein paar Probleme (Gefährdungen im Netz) werfen aber dafür weitere Probleme auf. Selbst Prof. Dr. Dr. Berkemann nennt eine Vernetzung der PCs als eine Bedingung[7]. Gegen einen vermehrten Einsatz isolierter PCs am Richterarbeitsplatz spricht, daß Insellösungen eine zentrale Fehlerbehebung und Update-Verwaltung verhindern. Der vernetzte PC muß grundsätzlich Vorgabe und Ziel aller Planungen an Gerichten sein. Alle Richter sollen von ihren Arbeitsplätzen aus sowohl Verbindung zur Geschäftsstelle, zu anderen Richterarbeitsplätzen (Mail) als auch zu externen Host-Systemen (juris, externe Datenbanken) aufnehmen und CD-ROM-Laufwerke im Netz ansprechen sowie Telefax versenden und direkt empfangen können. Dies ist beim Stand-alone-PC in dieser Fülle schier unmöglich. Ohne die genannten Nutzungsmöglichkeiten im Netz wäre die Ausrüstung der Arbeitsplätze aber nicht mehr wirtschaftlich. Stand-alone-PCs ließen außerdem keine wirtschaftliche Nutzung der auf Kommunikation angelegten Informationstechnik in den Geschäftsstellen zu.

---

[7] Reflexionen zur EDV-gestützten und EDV-strukturierten Arbeitswelt als sekundäres Ziel und Teil richterlichen Handelns, jur-pc 1994, 2838 ff, 2843



Booten und Programmstart von Diskette unterbinden

Laufwerksverriegelung

Ohne die nachfolgend beschriebenen Schutzmaßnahmen stimmen für die Justiz zuständige Ministerien oftmals ausschließlich Geräten ohne Diskettenlaufwerke zu. Dies wäre aber den Anwendern nicht vermittelbar.

Grundsätzlich sollen die Diskettenlaufwerke daher hardwaremäßig geschützt werden. Auch im geöffneten Zustand muß das Booten des Rechners von einer Diskette unmöglich sein. Nach Beendigung der Arbeit muß wieder eine automatische Sperre erfolgen.

Da ausschließlich durch die Systemverwaltung zur Verfügung gestellte Programme verwendet werden dürfen, darf ein Programmstart von Diskette oder ein Kopieren von Programmen von Diskette auf Festspeichermedien (oder umgekehrt) nicht möglich sein. Dies stellt sicher, daß keine ungeprüften Programme eingespielt oder vorhandene kopiert werden können. Das Booten des Rechners von einer Diskette darf nicht möglich sein. Der Verschluß von bootfähigen Laufwerken verhindert so, daß die bei einem Systemstart von der Festplatte sich automatisch installierenden Sicherheitsmechanismen außer Kraft gesetzt werden. Der Zugriff auf die Betriebssystemebene ist somit – wie gewünscht – auf das Systembetreuungspersonal beschränkt.

Im Sicherheitsprogramm ist festzulegen, daß ausführbare Dateien (z.B. COM, EXE, BAT) von Diskettenlaufwerken nicht gestartet und derartige Dateien nicht kopiert werden können. Solche Maßnahmen, die dem dienstlichen PC leider Funktionen nehmen, die ein Anwender von seinem häuslichen Gerät her kennt, sind zwar schwierig zu vermitteln – aber notwendig, um den oben dargestellten Gefahren, wie insbesondere Nichtbeachtung von Sicherheitsmaßnahmen, Manipulation an Daten oder Software, unberechtigte Nutzung sowie Computerviren, zu begegnen.

Einzige Alternative: diskless PC's – unerträglich!

Alternative wäre allein der Verzicht auf Diskettenlaufwerke. Dies würde die Arbeit der Richter, die vom häuslichen Arbeitsplatz auf Disketten Arbeitsergebnisse mitbringen wollen, weitaus mehr tangieren, als die temporäre Sperre für Daten und totale Sperre für Programme.

Dateiverwaltung

Dateien und Verzeichnisse

Vom Nutzer erzeugte Dateien sollen unter Berücksichtigung der Zugriffsrechte auf dem Diskettenlaufwerk, der Festplatte und im Normalfall auf einem zentralen (virtuellen) Laufwerk gespeichert werden. Der Anwender darf nur Dateien und Verzeichnisse löschen können, die er selbst angelegt hat.

Virenschutz

Virenschutz muß gewährleistet sein und darf nicht übergangen werden.

Ziel muß ein speicherresidentes Virensuch- und Virenentfernungsprogramm an jedem PC sein, das ausreichende Update-Möglichkeiten bietet. Das Virenschutzprogramm hat sich bei Inbetriebnahme des PCs automatisch resident im Speicher zu aktivieren. So kann es sowohl Programme und Daten als auch die BOOT-Sektoren von Festplatte und Disketten permanent einer Virenkontrolle unterziehen. Ein virenbefallener PC muß vom Netz abgehängt oder gesperrt werden. Es genügt nicht, lokal am Arbeitsplatz zu melden, daß Viren entdeckt wurden, wenn sich diese Meldung einfach übergehen läßt. Eine zentrale Meldung beim Systemadministrator wäre aus meiner Sicht auch nicht bedenklich. Selbst die richterliche Unabhängigkeit geht nicht soweit, ungehindert virenverseuchte Disketten am Arbeitsplatz zu verwenden.

Dunkelschaltung

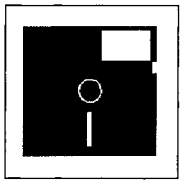
Dunkelschaltung mit Paßwort

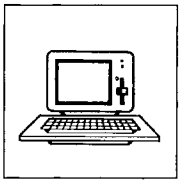
Auf den PCs muß die Möglichkeit bestehen, den Bildschirm dunkel zu schalten. Die Deaktivierung der Dunkelschaltung darf nur mit Paßwort-Eingabe möglich sein. Bei kurzfristigem Verlassen des Raums während der Arbeitszeit ist die Bildschirmdunkelschaltung zu aktivieren. Wird der Raum für längere Zeit verlassen (z.B. in der Mittagspause), hat die Abmeldung vom System zu erfolgen. Beim Verlassen des Dienstzimmers ist das Dienstzimmer zu verschließen.

Raumschutz

Räumliche Separierung zentraler Netzkomponenten

Zentraleinheiten des Netzwerks und sonstige Geräte zur Steuerung globaler Netzfunktionen sind in einem gesonderten Raum unterzubringen. Deren Türen können durch den Einbau eines Knaufs anstelle des Türgriffs an der Flurseite mit relativ geringem Aufwand gesichert werden. Das Betreten des Rechnerraumes darf nur den Systembetreuern sowie den mit der Wartung beauftragten Mitarbeitern einer Fremdfirma gestattet sein. Für Fenster bietet sich die Ausstattung mit schwer zerstörbarem Glas und einer Alarmanlage an. Von einer Vergitterung des





Fensters muß abgesehen werden, wenn damit ein Fluchtweg aus dem Raum versperrt wird. Zu fragen ist deshalb, ob Serverräume nicht grundsätzlich in höhere Etagen zu legen sind.

Datenträger-Behandlungsvorschriften

Datenträger

Datenträger sind vom jeweiligen Nutzer verschlossen und vor äußeren Einflüssen geschützt aufzubewahren. Beim Transport von Disketten außer Haus müssen verschließbare Diskettenboxen Verwendung finden. Disketten oder sonstige Datenträger sind, wenn sie nicht mehr gebraucht werden oder unbrauchbar sind, an die Systemverantwortlichen zurückzugeben, damit sie ordnungsgemäß wiederverwendet oder vernichtet werden können. Zurückgegebene Disketten sind so zu löschen, daß die Wiederherstellung der Daten nicht möglich ist. Unbrauchbare Datenträger sind physikalisch zu zerstören.

Tägliche Sicherung aller Bewegungsdateien

Datensicherung

Der Schutz vor Datenverlust erfordert die tägliche Sicherung aller Bewegungsdateien durch ihre Auslagerung auf einen externen Datenträger (Streamer). Soweit Daten zentral auf dem Server abgelegt werden, entfällt für den einzelnen Anwender damit das lästige Sichern auf Disketten. Der Sicherungslauf sollte während des Nachtbetriebs ohne Stillstand, automatisch und bedienerlos erfolgen. Turnusmäßige Vollsicherungen aller Daten sind außer Haus zu hinterlegen.

Sicherheitsschränke sind wärmeempfindlich.

Die Originaldisketten der Software, die Sicherungsbänder sowie die Originale der Lizenzverträge für die Software sind in einem feuergeschützten Safe auf erhöhten Regalböden aufzubewahren. Sein Standort muß klimatisiert sein, wenn der Safe einen chemischen Feuerschutz enthält. Der chemische Prozeß kann, wenn er einmal wegen zu hoher Raumtemperatur eingesetzt hat, nicht gestoppt werden und nur einmal ablaufen. Der Safe ist danach ebenso unbrauchbar, wie übrigens auch die auf seinem Boden gelagerte Dinge, da dort die Schutzflüssigkeit einwirken kann.

Zu fordern: Anwesenheit von Nutzer oder Systemverwalter

Reparaturen

Die Installation, Instandsetzung oder Instandhaltung von Geräten durch einen Angestellten der Wartungs- oder Lieferfirmen darf nur in Anwesenheit des Nutzers oder des Systemverwalters erfolgen. Ein Zugriff auf geschützte Daten ist dem Angestellten nur dann zu gestatten, wenn dies für eine Prüfung der Funktionstauglichkeit unabweisbar erforderlich ist. Kommt die Instandsetzung eines Geräts oder datenspeichernder Teile im Gericht nicht in Betracht, sind geschützte Daten zu löschen, sofern dies technisch möglich ist. In jedem Fall hat der Angestellte sich schriftlich zu verpflichten, geschützte Daten, von denen er während der Installation, Instandsetzung oder Instandhaltung Kenntnis erlangt, Dritten, insbesondere seinem Arbeitgeber und dessen übrigen Arbeitnehmern, nicht zu offenbaren.

Zu garantieren: Physikalisches Löschen der Daten.

Entsorgung

Sollen Geräte oder Datenträger, auf denen geschützte Daten gespeichert sind, vernichtet oder vorübergehend oder endgültig aus dem Gericht entfernt werden, sind, soweit technisch möglich, alle vorhandenen Daten nach Sicherung physikalisch zu löschen. Ist das ausnahmsweise nicht möglich, hat ihr Empfänger schriftlich zu versichern, die Datenträger unverzüglich ohne erneute Inbetriebnahme zu zerstören oder, soweit die Datenträger noch benutzbar sind, die auf ihnen gespeicherten Daten zur Wahrung des Datengeheimnisses sofort physikalisch zu löschen.

Schulung zur Datensicherheit

Schulung

Schulungen müssen auch Datenschutz und Datensicherheit umfassen, sollen alle theoretisch erarbeiteten Maßnahmen letztendlich auch greifen. Neben den bereits im Rahmen der Grundlagen-Schulung zu vermittelnden Kenntnissen des Datenschutzes und der Datensicherheit sind zusätzlich jeweils spezielle Kurse für alle Anwender erforderlich. Die Datenschutz-Schulung muß durch den Datenschutzbeauftragten des Hauses erfolgen.

Haushaltsmäßige Folgen mangelnder Sicherheit

Ohne Schutz keine Haushaltsmittel!

Die dargestellten Schutzmaßnahmen sind Folgen des gebotenen Datenschutzes und oftmals auch der berechtigten Forderungen des Personal- und Richterrates. Sie gleichzeitig am Richterarbeitsplatz außer Kraft zu setzen, entspräche kaum dem Sinn solcher Maßnahmen und hätte zur Folge, daß ein IT-Sicherheitskonzept, in dem solches niedergelegt wäre, nicht anerkannt würde. Ohne ein anerkanntes Sicherheitskonzept aber würden Haushaltsmittel nicht freigegeben. Auch dies ist zu bedenken, wenn man als Anwender gerade einmal wieder unter dem Joch der Sicherheitsmaßnahmen besonders leidet.