Planung und Realisierung von Datenschutzeinrichtungen in einem öffentlichen Rechenzentrum

Autor(en): **Gribi, P.**

Objekttyp: **Article**

Zeitschrift: **Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association Suisse des Electriciens, de l'Association des Entreprises électriques suisses**

Band (Jahr): **77 (1986)**

Heft 1

PDF erstellt am: **06.08.2024**

Persistenter Link: https://doi.org/10.5169/seals-904140

Planung und Realisierung von Datenschutzeinrichtungen in einem öffentlichen Rechenzentrum

P. Gribi

Im Rechenzentrum BEDAG werden EDV-Dienstleistungen erbracht für die kantonale Verwaltung, die Universität, das Inselspital und die Hasler AG. Die Vielfältigkeit der Benützer in einem gemeinsamen Rechenzentrum und die Speicherung von personenbezogenen Daten bedingen ein hohes Mass an Betriebssicherheit, Datensicherheit und Datenschutz. Der Aufsatz beschreibt die technischen, baulichen und organisatorischen Massnahmen, welche ergriffen werden, um einen im Verhältnis zum betriebenen Aufwand optimalen Schutz zu erreichen.

Le Centre de calcul BEDAG procède au traitement électronique des informations pour l'administration cantonale, l'Université, l'Hôpital de l'Ile et la S.A. Hasler. La variété des utilisateurs d'un même centre de calcul et la mémorisation de données concernant des personnes exigent une grande sécurité de service. Description des dispositions techniques, de construction et d'organisation à prendre pour obtenir une protection optimale, par rapport aux frais d'exploitation.

Adresse des Autors

P. Gribi, dipl. Statistiker, Rechenzentrum BEDAG, 3012 Bern.

1. Einleitung

Die BEDAG, Bernische Datenverarbeitung AG, ist ein Rechenzentrum, dessen Aktionäre der Kanton Bern, das Inselspital und die Firma Hasler AG sind. Als Service-Center konzipiert, bietet sie ihren Kunden EDV-Leistungen zu möglichst günstigen Konditionen an. Im Jahre 1984 verteilten sich die Dienstleistungen folgendermassen auf die recht unterschiedlichen Benützer:

37% öffentliche Verwaltung des Kantons Bern
42% Universität
17% Inselspital
1% Hasler AG
3% Nichtaktionäre

Die niedrige Beteiligung der Hasler AG rührt daher, dass diese gegenwärtig mit einem eigenen Überangebot an Computerleistung konfrontiert ist. Die Dienstleistung der BEDAG erstreckt sich auf die produktive Durchführung von On-line-Systemen, Stapelverarbeitung, individueller Datenverarbeitung und die Zurverfügungstellung von Hilfsmitteln für die Anwendungsentwicklung. Die eigentliche Entwicklung von Anwendungspaketen wird durch die Aktionäre der Gesellschaft wahrgenommen. Bedingt durch die Vielfältigkeit der Benützer sind die Anforderungen und Erwartungen bezüglich Datenschutz sehr unterschiedlich. Es liegt in der Verantwortung des Zentrums, allen Benützern einen ausreichenden Schutz für ihre Daten zu gewährleisten.

2. Grundsätze

Sicherheit in einem Rechenzentrum muss umfassend geplant und realisiert werden, damit der erreichte Schutz den Erwartungen und dem Aufwand entsprechend ausfällt. Wesentliche Komponenten der Sicherheit sind die Betriebssicherheit, die Datensicherheit und der Datenschutz. Letzterer gewinnt zunehmend an Bedeutung. Datenschutz kann sowohl für personen- wie auch sachbezogene Daten Anwendung finden. Die in Vorbereitung befindliche Gesetzgebung beschränkt sich allerdings auf personenbezogene Daten. Alle drei Komponenten müssen ausgewogen berücksichtigt werden unter Einbezug nicht nur des Rechenzentrums, sondern auch der Archive, des Datentransportes, der Datenübermittlung und der Lokalitäten der teilhabenden Benützer.

Insbesondere in einem Rechenzentrum mit unterschiedlichen, nicht zusammengehörenden Benützern fällt es schwer, uniforme Datenschutzgrundsätze durchzusetzen. Grundlage für einen wirkungsvollen Datenschutz ist jedoch die Bereitschaft der Benützer, sich für ihre Daten verantwortlich zu fühlen, d.h. die Rechte und Pflichten als Eigentümer zu übernehmen. Gesetze, Verordnungen und Richtlinien mögen entsprechende Massnahmen wohl unterstützen, reichen aber nicht aus für einen wirkungsvollen Datenschutz. Der Aufwand für die getroffenen Massnahmen soll auch in einem vernünftigen Verhältnis zur erreichbaren Reduktion des Gefährdungsgrades der Daten liegen.

3. Gefahren für Daten

Der Nutzen eines Computereinsatzes nimmt zu, je grösser die Datenmengen sind, die gespeichert und verarbeitet werden müssen und je umfangreicher die Verarbeitung der Daten ist. Die Konzentration grosser Datensammlungen in einem Rechenzentrum lässt missbräuchliche Zugriffe lohnenswert erscheinen. Die Kombination verschiedener Daten kann zu zusätzlichen Informationen führen, deren Verwendung nicht mehr durch die Verwaltungstätigkeit erklärt werden kann oder den Absichten des Be-

sitzers der Daten (z.B. Forscher) widerspricht.

Als Gelegenheit für missbräuchliche Einsicht oder Entwendung muss der Austausch von Daten zwischen dem Benützer und dem Rechenzentrum in Betracht gezogen werden. Eine weitere Gelegenheit zur Entwendung ergibt sich aus der Speicherung der Daten auf leicht transportierbaren Medien, wie z.B. Magnetbändern. Glücklicherweise ist aber die Interpretation, insbesondere von numerischen Daten, ohne begleitende Dokumentation schwierig. Diese wird sinnvollerweise von den eigentlichen Daten getrennt aufbewahrt. Gefahren für die Daten lauern nicht nur im Computer des Rechenzentrums, sondern auch in den Datenarchiven, auf den Transportwegen der Datenträger, bei der Übermittlung der Daten über das Fernmeldenetz und beim Benützer. Vergleichbare Gefahren bestehen allerdings auch bei konventionellen Karteien.

Die zu untersuchenden Gefahren können in drei Kategorien unterteilt werden.

1. *Unberechtigter Zutritt* in den geschützten Bereich des Rechenzentrums, in das Archiv oder in die Lokalitäten des Benützers: Dadurch können Datenträger behändigt, Listen eingesehen und Manipulationen an Daten über Terminals vorgenommen werden.
2. *Entwenden von Daten:* Abhängig von den getroffenen Massnahmen gegen den Zutritt wird die Versuchung zur Entwendung von Datenträgern und Listen grösser oder kleiner sein. Insbesondere die Entwicklungen im Sektor der Personal Computer bringen die Datenträger in immer handlichere Form und verstärken damit das Entwendungsrisiko.
3. *Unberechtigter Zugriff* auf Daten, die im Computer gespeichert sind: Als Hilfsmittel kommen Terminals (bei regulären Benutzern) oder Personal-Computer, die widerrechtlich auf das Datenübermittlungsnetz des Computers geschaltet werden (Hacking), in Frage. Diese Gefahr beinhaltet besondere Risiken, weil dadurch gespeicherte Daten nicht nur eingesehen, sondern auch abgeändert werden können.

4. Datenschutzeinrichtungen

Die oben beschriebenen Gefahren müssen mit umfassenden, aber ausgewogenen Massnahmen reduziert werden. Eine vollständige Elimination der Risiken ist meistens wirtschaftlich nicht tragbar, kann aber kompensiert werden durch ein gut ausgebautes Kontrollsystem, das erlaubt, den Missbrauch von Daten möglichst rasch festzustellen. Die BEDAG hat sich entschieden, einen umfassenden Zugriffsschutz zu realisieren, der nur sehr selektiv gelockert wird. Insbesondere von Studentenseite stösst dieses Konzept allerdings auf Widerstand, weil es für jeden Benützer einige Umtriebe bedeutet.

Durch die zentrale Speicherung der Daten wird die Durchführung von wirkungsvollen Massnahmen und deren Überwachung wesentlich erleichtert. Permanente Zugriffskontrollen, erzwungene Benützeridentifikation, Zutrittskontrollen und die Verhinderung von Umgehungsmöglichkeiten mittels technischer und organisatorischer Massnahmen stellen sicher, dass die Daten nicht in fremde Hände gelangen. Gegen jede der beschriebenen drei Gefahrenarten gilt es *bauliche, organisatorische* und *technische* Massnahmen zu ergreifen.

4.1 Massnahmen gegen unberechtigten Zutritt

Bauliche Massnahmen, wie Sicherheitszonen, Schleusen, Überwachung und verschliessbare Büros, schränken das Risiko bereits wesentlich ein. Technische Hilfsmittel, wie Badges mit Code, Saldierung der Ein- und Austritte sowie individuelle, funktionsbezogene Zutrittsberechtigung zu den verschiedenen Sicherheitszonen, verstärken die obigen Massnahmen.

Allerdings ist ein optimaler Erfolg nur erreichbar bei gleichzeitiger Motivation der Mitarbeiter (Rechenzentrum und Benützer), die getroffenen Massnahmen nicht als Schikanen zu betrachten, sondern als flankierende, notwendige Massnahmen zum Schutz der von ihnen betreuten Daten. Firmengrundsätze zum Umgang mit Daten und deren Unterstützung und Befolgung auf allen Stufen des Kaders, werden beim gesamten Personal die Bereitschaft für einen verantwortungsbewussten Datenschutz wesentlich heben.

4.2 Massnahmen gegen Entwendung

Zur Entwendung bieten sich insbesondere leicht transportierbare Datenträger, wie Magnetbandspulen, Magnetbandkassetten, Disketten und Listen an. Wirkungsvolle Massnahmen zur Verminderung des Risikos für schützenswerte Daten umfassen deshalb:

- die Überwachung aller Transporte von Datenträgern,
- Eingangs-, Ausgangs- und Bestandeskontrolle von Datenträgern,
- die Aufbewahrung unter Verschluss (das Reinigungspersonal braucht Zutritt auch zu geschützten Räumen),
- die Abgabe von Datenträgern nur an autorisierte Personen,
- die getrennte Aufbewahrung der Daten und des Datenverzeichnisses. Codierte Daten auf einem Datenträger sind ohne entsprechendes Inhaltsverzeichnis sehr schwierig und sicher nur teilweise zu entziffern.

Mittels technischer Hilfsmittel können die Daten zusätzlich verschlüsselt werden. Eine elektronische Kennzeichnung der Datenträger und deren Erkennung beim Durchgang durch die Schleuse wird mit zunehmender Verkleinerung der transportablen Datenträger immer erstrebenswerter.

4.3 Massnahmen gegen unberechtigten Zugriff

Der unberechtigte Zugriff auf Daten in Listen kann durch Massnahmen gegen unberechtigten Zutritt und Entwendung minimiert werden. Der unberechtigte Zugriff auf Daten im Computer erfolgt über Ein-/Ausgabegeräte des Computers. Diese umfassen heute insbesondere alle mit dem Computer verbundenen Terminals und Personal Computer. Bei erfolgreichem Aufruf des entsprechenden Programmes können Daten nicht nur abgerufen, sondern auch verändert werden. Dies gilt es wirkungsvoll zu verhindern durch die Realisation eines umfassenden Zugriffssteuerungskonzepts.

Globale Zugriffsberechtigungen sind grundsätzlich zu verhindern. Richtlinien zur Einstufung und Behandlung von vertraulichen Daten und entsprechende Motivation der Mitarbeiter sind Voraussetzung, dass technische Massnahmen, wie

- eine auf die Betriebssoftware des Computers abgestimmte Zugriffssteuerungssoftware,
- Verschlüsselung schützenswerter Daten,
- Einsatz von Mietleitungen für Datenübermittlung,
- abschliessbare Personal Computer, inkl. der in ihnen enthaltenen Datenträger

zum Erfolg führen.

Durch den Einsatz von Zugriffssteuerungssoftware kann der Benützer gezwungen werden, sich mittels Namen und Passwort zu identifizieren. Versuche mit falscher Identifikation können registriert und ausgewertet werden. Ausgewählte Arbeiten können auf bestimmte Terminals in geschützten Arbeitsbereichen beschränkt werden. Insbesondere dürfen Datenänderungen nur durch autorisierte Personen vorgenommen werden.

Diese Massnahmen sind jedoch nur wirkungsvoll, wenn der Benützer seine Verantwortung gegenüber seinen Daten wahrnimmt und seine Identifikation weder bewusst noch fahrlässig weitergibt. Der Zwang zum regelmässigen Ändern des Passwortes soll auch hier zusätzliche Sicherheit verschaffen. Diese Massnahmen, der Einsatz von Mietleitungen für Datenübertragung und die Verschlüsselung von Daten, bieten einen wirksamen Schutz auch gegen wiederholtes Hacking.

5. Schlussbemerkungen

Im Kanton Bern bieten die kantonale Verordnung über den Datenschutz vom September 1977 und die entsprechenden im Rechenzentrum BEDAG getroffenen organisatorischen, baulichen und technischen Sicherungsmassnahmen ein wirksames Instrumentarium für einen zeitgemässen Datenschutz. Das kommende Datenschutzgesetz wird dieses Instrumentarium noch verfeinern. Der Schutz von Daten im Grosscomputer ist besser als in manchen manuellen Karteien und auch besser als in Kleincomputern, die normalerweise mit weniger Schutzmassnahmen ausgerüstet sind. Das Rechenzentrum BEDAG hat bereits vor 1977 Massnahmen zum Datenschutz implementiert. Alle Massnahmen zum Schutz der Daten im Rechenzentrum werden periodisch überprüft und die Sicherheit mit neuen technischen Hilfsmitteln laufend verbessert.

Die periodischen Überprüfungen durch die Revisionsstellen müssen auch die Datenschutzmassnahmen kontrollieren. Neben allen baulichen, organisatorischen und technischen Massnahmen kommt dem Benützer als Eigentümer der Daten massgebende Bedeutung zu. Das schwächste all dieser Elemente bestimmt die Stärke der Datenschutzmassnahmen insgesamt.