Bundesrat **Drucksache 599/90**

28. 08. 90

In – Fz

Unterrichtung

durch den Bundesrechnungshof

Bericht des Bundesrechnungshofes gemäß § 99 BHO über die Sicherheit der Informationsverarbeitung in Rechenzentren der Bundesverwaltung

Der Präsident des
Bundesrechnungshofes
I 1 — 20 80 07

Frankfurt, den 28. August 1990

An den
Herrn Präsidenten des Bundesrates

Sehr geehrter Herr Präsident!

Hiermit leite ich dem Bundesrat einen Bericht des Bundesrechnungshofes gemäß § 99 der Bundeshaushaltsordnung über die Sicherheit der Informationsverarbeitung in Rechenzentren der Bundesverwaltung zu.

Den Bericht übersende ich auch der Präsidentin des Deutschen Bundestages und der Bundesregierung.

Mit vorzüglicher Hochachtung

Dr. Zavelberg

Druck: Bonner Universitäts-Buchdruckerei, 5300 Bonn
Alleinvertrieb: Verlag Dr. Hans Heger, Postfach 20 13 63, Herderstraße 56, 5300 Bonn 2, Telefon 02 28/36 35 51, Telefax 02 28/36 12 75
ISSN 0720-2946

Bundesrat Drucksache **599/90**

Bericht des Bundesrechnungshofes gemäß § 99 BHO über die Sicherheit der Informationsverarbeitung in Rechenzentren der Bundesverwaltung

Inhaltsverzeichnis

Vorbemerkung

Die Bundesverwaltung ist bei der Erfüllung ihrer vielgestaltigen Aufgaben in hohem Maße von einer sicheren Informationstechnik abhängig. Mit Hilfe der Datenverarbeitung wird beispielsweise jährlich ein Finanzvolumen in dreistelliger Milliardenhöhe verwaltet.

Der Sicherheit der Informationsverarbeitung, insbesondere in kassenwirksamen, sicherheitsempfindlichen und sonstigen sensiblen Bereichen, kommt eine herausragende Bedeutung zu. Die Datenverarbeitungsanlagen müssen technisch verfügbar und gegen Ausfall gesichert, die Vertraulichkeit der Daten sowie die Richtigkeit und Unversehrtheit der Daten und Programme müssen gewährleistet sein.

Um den möglichen Gefährdungen zu begegnen und eine ausreichende, zugleich aber wirtschaftlich vertretbare Sicherheit der Informationstechnik zu erreichen, müssen Sicherheitsmaßnahmen technischer, organisatorischer und personeller Art zusammenwirken.

Sicherheitsmaßnahmen kosten im allgemeinen Geld. Nicht ausreichende Sicherheitsmaßnahmen können aber zu Schäden führen, deren finanzielle und sonstige Auswirkungen den Sicherheitsaufwand bei weitem übersteigen. Als notwendiger Teil der Investitionsentscheidung sollten der Sicherheitsaspekt und die damit im Zusammenhang stehenden Ausgaben bereits bei der Planung berücksichtigt werden. Für eine sachgerechte Bewertung des mit Sicherheitsmaßnahmen verbundenen Aufwands und Nutzens ist die Erstellung von Risikoanalysen und Sicherheitskonzepten unabdingbar. Sie bilden die Voraussetzung für eine angemessene Sicherheit der Informationsverarbeitung.

Der Bundesrechnungshof und die in seinem Auftrag tätigen Vorprüfungsstellen haben bei ihren Prüfungen erhebliche Mängel in der Sicherheit der Informationstechnik festgestellt. Dabei hat sich ergeben, daß ein großer Teil der Mängel mit vergleichsweise geringem finanziellem Aufwand, beispielsweise durch regelmäßige Kontrolle der Wirksamkeit bereits bestehender Sicherheitsvorkehrungen, behoben werden kann.

Ein Fortbestand der Mängel kann zu erheblichen Nachteilen für den Bund führen. Die von der Bundesregierung bisher ergriffenen und geplanten Maßnahmen zur Verbesserung der Sicherheit reichen nicht aus. Vielmehr sollte durch intensive Beratung sowie Aus- und Fortbildung bei den mit Informationstechnik befaßten Stellen das notwendige Sicherheitsbewußtsein geweckt oder weiter verstärkt werden.

Deshalb hält es der Bundesrechnungshof für geboten, seine Feststellungen dem Deutschen Bundestag, dem Bundesrat und der Bundesregierung mitzuteilen.

Zusammenfassung

0.1 Sicherung der Verfahren

In Rechenzentren der Bundesverwaltung, in denen sensible kassenwirksame, personen- und auch sachmittelbezogene Daten verarbeitet werden, sind die Verfahren nicht hinreichend gegenüber Katastrophen oder möglicher Sabotage gesichert.

0.2 Risikoanalysen und Sicherheitskonzepte

Für die eingesetzten Verfahren wurden keine Risikoanalysen durchgeführt. Die daraus abzuleitenden umfassenden Sicherheitskonzepte fehlten. Die Katastrophenschutzpläne waren unvollständig.

0.3 Technische Verfügbarkeit

Die technische Verfügbarkeit der in den Rechenzentren eingesetzten Verfahren ist nicht immer in ausreichendem Maße gewährleistet.

0.4 Zugangskontrollen; Schutz der Programme und Daten

Bei Rechenzentren wiesen die Zugangskontrollen zu den einzelnen Sicherheitsbereichen Lücken auf. Gleiches galt für den Schutz der Programme und Daten gegen Manipulation, unberechtigte Kenntnisnahme und Datenverlust.

Abschnitt I

1 Allgemeine Feststellungen

1.1

Der Bundesrechnungshof hat im Rahmen einer Querschnittsprüfung — unter Beteiligung der Prüfergruppen Datenverarbeitung der Vorprüfungsstellen des Bundesministers für Verkehr und des Bundesministers der Verteidigung sowie des Prüfungsdienstes bei der Deutschen Bundesbahn — die Sicherheit der Informationsverarbeitung in Rechenzentren der Bundesverwaltung, der Deutschen Bundespost und der Deutschen Bundesbahn geprüft.

Über einen Teil der Prüfungsergebnisse bei Rechenzentren der Bundeswehr hat er bereits in den Bemerkungen 1989 berichtet (Drucksache 11/5383 Nr. 30). Die gleichen wie die dort geschilderten bedeutsamen Mängel (Nr. 30.1.1) hat er auch bei allen weiteren Prüfungen festgestellt:

- Es fehlen verfahrensbezogene Risikoanalysen, die Aufschluß darüber geben, welcher finanzielle, organisatorische und personelle Sicherheitsaufwand gegenüber möglichen Bedrohungen wirtschaftlich angemessen ist und welche Risiken als Restrisiken hingenommen werden können.
- Es fehlen umfassende Sicherheitskonzepte, die auf diesen Risikoanalysen aufbauen und in denen das lückenlose Zusammenspiel aller daraus abgeleiteten Sicherheitsteilmaßnahmen zu einer Gesamtsicherheit dargestellt wird.
- Die Regelungen für den Katastrophenfall sind unzureichend; Katastrophenschutz- und Wiederanlaufübungen wurden unterlassen.

In vielen Fällen war eine zu große Zahl von Mitarbeitern in Rechenzentren berechtigt, Programme und Daten zu lesen und zu verändern.

Der Schutz von Programmen und Daten vor unberechtigtem Zugriff zwecks Kenntnisnahme, Manipulation oder Zerstörung ist insgesamt unzureichend. Daraus ergibt sich insbesondere für personenbezogene, kassenwirksame und sonstige sensible Daten ein hohes Risiko gegenüber Manipulation, Verlust der Vertraulichkeit und Verlust der Verfügbarkeit.

1.2

Der Bundesrechnungshof und die anderen Prüfungsorgane haben den Bundesminister für Verkehr, den Bundesminister für Post und Telekommunikation, den Bundesminister der Verteidigung sowie den Vorstand der Deutschen Bundesbahn aufgefordert, die Mängel umgehend zu beseitigen. So sei dafür zu sorgen, daß die Bedarfsträger für die in den Rechenzentren eingesetzten Verfahren eine Risikoanalyse erstellen. Für die Rechenzentren müßten auf der Basis der Risikoanalysen umfassende Sicherheitskonzepte und Katastrophenschutzpläne erarbeitet werden. Übungen für den Notfall sollten durchgeführt werden. Die Zugriffsberechtigung auf Programme und Daten sei restriktiv zu erteilen. Die Notwendigkeit der Berechtigung des Zugriffs sei regelmäßig und zeitnah zu überprüfen. Je nach Bedeutung der Daten sei bei Versuchen unberechtigten Zugriffs der Sachverhalt umgehend aufzuklären.

1.3

Die geprüften Stellen haben die Mängel grundsätzlich anerkannt. Wegen des Fehlens von Personalkapazitäten und Arbeitshilfen seien sie aber außerstande, kurzfristig Risikoanalysen und Sicherheitskonzepte zu erstellen. Katastrophenschutzpläne würden erarbeitet oder auf den neuesten Stand gebracht. Übungen werde man nach Fertigstellung der Katastrophenschutzpläne durchführen. Eine Überarbeitung der Zugriffsrechte wurde angekündigt.

1.4

Der Bundesrechnungshof vermag nicht einzusehen, daß die Bundesminister und der Vorstand der Deutschen Bundesbahn mit dem Hinweis auf Personalmangel die dringend gebotene Verbesserung der Sicherheit in den Rechenzentren der Bundesverwaltung hinausgezögert haben. Risikoanalysen und Sicherheitskonzepte stellen die unverzichtbaren Grundlagen der Sicherheit dar. Die Bundesminister und der Vorstand sollten bemüht sein, die Prioritäten so zu setzen, daß diese Aufgaben im Rahmen der vorhandenen Stellen ordnungsgemäß erledigt werden können. Dazu gehört auch, durch entsprechende Auswahl und Förderung von Nachwuchskräften frühzeitig Vorsorge zu treffen, daß die vorhandenen Stellen mit qualifiziertem Personal besetzt sind. Seit der ersten Prüfungsmitteilung des Bundesrechnungshofes im Jahre 1988 zu diesen Themen ist der Stand der Sicherheit in den Rechenzentren der Bundesverwaltung noch nicht entscheidend verbessert worden.

Die Bundesminister sowie die Vorstände der Deutschen Bundesbahn und der Unternehmen der Deutschen Bundespost sollten nunmehr unverzüglich die erforderlichen Schritte unternehmen, um die aufgezeigten Mängel abzustellen und den Stand der Sicherheit der Informationsverarbeitung zu verbessern.

Abschnitt II

Über diese die Ressorts, die Deutsche Bundesbahn und die Deutsche Bundespost in gleichem Maße betreffenden Beanstandungen hinaus wurden in einzelnen Rechenzentren weitere gravierende Mängel festgestellt.

2 Bundesminister für Verkehr

2.1 Administrative Datenverarbeitung

In dem Rechenzentrum eines zum Geschäftsbereich des Bundesministers gehörenden Bundesamtes werden verschiedene Datenbanken geführt sowie Statistiken erstellt, die als Grundlage für verkehrs- und wirtschaftspolitische Entscheidungen dienen.

2.1.1 Technische Verfügbarkeit

2.1.1.1

Die technische Verfügbarkeit der Datenverarbeitungsanlage war in hohem Maße von der Leistungsfähigkeit der im Rechenzentrum installierten Klimaanlage abhängig. Diese war nicht in der Lage, bei ungünstigen Witterungsverhältnissen die für einen zuverlässigen Betrieb nötige Anlagenkühlung zu erreichen. Schon im Normalbetrieb lief die Anlage ständig unter Vollast. Ersatzanlagen und Reserven waren nicht vorhanden. Bei einer eingetretenen Störung der Klimaanlage mußte die Datenverarbeitungsanlage nach 30 Minuten wegen Überhitzung abgeschaltet werden. Die im Rechenzentrum zur Überwachung der Klimaanlage eingesetzte Anzeigetafel war nicht funktionsfähig.

2.1.1.2

Der Bundesrechnungshof hat darauf hingewiesen, daß die technische Verfügbarkeit des Rechners — und damit der Datenbanken — durch die störanfällige und unzureichende Klimatisierung in hohem Maße gefährdet ist. Weiterhin bestehe die Gefahr, daß beim Betrieb der Datenverarbeitungsanlage in erhöhter Umgebungstemperatur bleibende Schäden an der Hardware entstehen. Diese Gefahr werde noch vergrößert, weil die Anzeigetafel Übertemperaturen nicht rechtzeitig anzeige.

Der Bundesrechnungshof hat das Bundesamt aufgefordert, auf der Grundlage einer zu erstellenden Risikoanalyse die erforderliche Verfügbarkeit des Rechenzentrums sicherzustellen. So muß die Klimaanlage ausreichend dimensioniert und mit einer vorzugebenden Ausfallrate betrieben werden. Die Anzeigetafel sollte funktionsfähig sein.

2.1.1.3

Das Bundesamt hat die Beanstandungen anerkannt und mitgeteilt, es habe Sofortmaßnahmen zur Verbesserung der Klimasituation ergriffen. Um Maßnahmen zur Entlastung der Klimaanlage durchführen zu können, habe man für das Jahr 1991 Haushaltsmittel beantragt. Durch den für das Jahr 1992 vorgesehenen Umbau des Rechenzentrums würden sich weitere Verbesserungen ergeben.

2.1.1.4

Der Bundesrechnungshof gibt zu bedenken, daß die Maßnahmen zur Verbesserung der Klimatisierung des Rechenzentrums erst im Laufe des Jahres 1991 ausreichende Wirkung zeigen werden. Bis dahin ist die Verfügbarkeit des Rechners weiterhin gefährdet. Der Bundesminister sollte in der Übergangszeit für die wichtigsten Datenverarbeitungsanwendungen geeignete Maßnahmen treffen.

2.1.2 Datenerfassung

2.1.2.1

In dem Referat Datenerfassung des Bundesamtes sind von 154 Kräften täglich etwa 60 000 Belege zu bearbeiten. Eine organisatorische Regelung in Form einer allgemeinen Erfassungsanweisung fehlte. Die Zugänge zu den Erfassungsräumen blieben unverschlossen und unbewacht. Die Belege mit personenbezogenen Daten wurden in den Datenerfassungsräumen offen gelagert. Auch nach Dienstschluß blieben die Belege frei zugänglich. Die Erfassung personenbezogener Daten geschah ohne Vollzähligkeitskontrolle der eingehenden Belegstapel. Eine Prüfung der Richtigkeit der Erfassung (Prüferfassung) fand nur teilweise statt. Bei zu starkem Arbeitsanfall unterblieb sie häufig. Eindeutige Regelungen über die Durchführung der Prüferfassung bestanden nicht. Als Zugriffsschutz zu den Erfassungsdaten diente lediglich eine zwei- bis vierstellige, den anderen Benutzern bekannte Kennung. Ein Techniker des Hardware-Herstellers, dem systemweite Zugriffsberechtigung eingeräumt war und der Wartungsarbeiten ohne Aufsicht durchführte, besaß als einziger Kenntnisse von bestimmten Systemfunktionen.

2.1.2.2

Der Bundesrechnungshof hat beanstandet, daß eine zuverlässige und ordnungsgemäße Datenerfassung

nicht gewährleistet war, weil Erfassungsanweisungen fehlten. Die nicht konsequent durchgeführte Prüferfassung kann die Richtigkeit und Unversehrtheit (Integrität) der Datenbestände und Statistiken erheblich beeinträchtigen. Wegen der Unzulänglichkeit der Zugangs- und Zugriffskontrolle sei weder die Vertraulichkeit noch die Unversehrtheit der Daten in ausreichendem Maße gewährleistet.

Der Bundesrechnungshof hat gefordert, organisatorische Regelungen für die Datenerfassung einzuführen, die Zugangskontrolle zu den Erfassungsräumen zu verschärfen und die Räume außerhalb der Dienstzeit verschlossen zu halten. Zwar sei eine lückenlose Vollzähligkeitskontrolle bei den Erfassungsbelegen wirtschaftlich nicht vertretbar, doch sollte das Bundesamt auf andere geeignete Weise die Risiken bei der Belegbehandlung verringern.

2.1.2.3

Das Bundesamt hat die Beanstandungen anerkannt. Es habe Maßnahmen ergriffen, die Zugangs- und Zugriffskontrolle zu den Datenerfassungsräumen zu verbessern. Eine Überwachung des Beleglaufes sei eingeführt worden. Der Techniker des Hardware-Herstellers solle in Zukunft nur noch unter Aufsicht eines Mitarbeiters der Datenerfassung Wartungsarbeiten durchführen. Den systemweiten Zugriff auf alle Dateien und Programme benötige er aber zur Fehlerbehandlung; dies sei auch bei anderen Anwendern üblich.

2.1.2.4

Der Bundesrechnungshof verkennt nicht, daß die Erfassung solch großer Belegmengen Probleme bereitet. Er sieht aber weiterhin die Gefahr der Manipulation und des Verlustes an Vertraulichkeit, wenn Außenstehende so weitreichende Systemzugriffe besitzen. Der Bundesminister sollte zusätzliche, kurzfristig wirksame Maßnahmen mit dem Ziel treffen, die Erfassungsdaten zuverlässig abzusichern.

2.2 Technisch-wissenschaftliche Datenverarbeitung

In dem Rechenzentrum einer Bundesanstalt im Geschäftsbereich des Bundesministers werden Daten für die Gewinnung von planerischen und bautechnischen Grundlagen des Straßenbauwesens verarbeitet. Es unterstützt die Forschungsplanung und -koordinierung sowie Untersuchungen auf dem Gebiet der Unfallforschung. Es wirkt außerdem mit bei Analysen zur Gestaltung des Verkehrsgeschehens und des Straßenumfeldes. Das Rechenzentrum der Bundesanstalt ist gleichzeitig Rechenzentrum des Bundesministers. Es wird auch von anderen Stellen in Anspruch genommen.

2.2.1 Programmentwicklung und Produktion, Datenerfassung

2.2.1.1

Bei der Entwicklung und Pflege der Software sowie bei der Datenverarbeitungsproduktion wurde festgestellt:

- Die Entwicklung der Programme war von der Ausführung (Programmproduktion) nicht getrennt. Programmierer konnten Programme auch dann noch ändern, wenn sie schon in der Verarbeitung genutzt wurden.
- Entwickelte Programme wurden nicht vollständig getestet. Zum Test wurden vorhandene Datenbestände (Produktionsdaten) benutzt, die nicht alle Testfälle abdeckten.
- Die Abnahme von Programmen vor der Überführung in die Produktion war nicht ausreichend geregelt.
- In der Verarbeitung wurden Programme eingesetzt, die weder abgenommen noch freigegeben waren.
- Programme in der Produktion wurden weder zentral verwaltet, noch unterlag die jeweilige Programmversion einer Kontrolle (Versionskontrolle).

Weitere Feststellungen betrafen die Datenerfassung:

- Eine Arbeitsanweisung für die Datenerfassung lag nicht vor.
- Daten wurden im Online-Verfahren erfaßt und nach nur sehr begrenzten Plausibilitätsprüfungen direkt in die Produktionsdateien übertragen.
- Es bestand keine Berichtigungsmöglichkeit für falsch erfaßte Daten. Die erfaßten Daten wurden nicht protokolliert.

2.2.1.2

Der Bundesrechnunghof hält die festgestellten Mängel für schwerwiegend. Er hat darauf hingewiesen, daß die Trennung von Entwicklung und Produktion Grundvoraussetzung für die Richtigkeit und Unversehrtheit der Programme und Datenbestände ist. Durch die unvollständigen Tests mit Produktionsdaten ist es nicht möglich, eine ausreichende Qualität der Programme zu erreichen. Durch den Zugriff auf Produktionsdaten ist außerdem eine Manipulation an diesen nicht auszuschließen. Nur durch eine zentrale Verwaltung und Versionskontrolle der Produktionsprogramme kann sichergestellt werden, daß die Programme Funktionen ausführen, die vom Nutzer gewollt sind.

Die Richtigkeit und Unversehrtheit der Datenbestände und deren Vertraulichkeit sind wegen der unzureichenden Plausibilitätsprüfung und der fehlenden Erfassungsregelung nicht gewährleistet.

Der Bundesrechnungshof hat die Beseitigung dieser Mängel gefordert.

2.2.1.3

Die Bundesanstalt hat die Beanstandungen grundsätzlich anerkannt. Entwicklung und Produktion würden künftig durch die Vergabe unterschiedlicher personenbezogener Zugriffsberechtigungen (Nutzerkennungen) voneinander getrennt. Eine zentrale Verwaltung und eine Versionskontrolle der Produktionsprogramme könne man aber derzeit nicht einführen, da das hierfür erforderliche Personal nicht zur Verfügung stehe. Bei zukünftigen Programmabnahmen werde man auch Sicherheitsprüfungen durchführen. Die festgestellten Mängel bei der Datenerfassung seien nicht der Regelfall.

2.2.1.4

Der Bundesrechnungshof gibt zu bedenken, daß die Trennung von Entwicklung und Produktion nicht allein durch die Vergabe unterschiedlicher Nutzerkennungen erreicht wird. Der Bundesminister sollte weitere organisatorische und softwaretechnische Maßnahmen bei der Programmentwicklung und Datenerfassung ergreifen, um die Integrität und Vertraulichkeit der Daten und Programme zu gewährleisten. Im übrigen ist nicht entscheidend, ob die Mängel bei der Datenerfassung die Regel sind. Es kommt darauf an, möglichst alle Mängel zu vermeiden. Der Schutz der Produktion und der Datenbestände vor Manipulationen muß sichergestellt sein.

2.2.2 Programm- und Datensicherung

2.2.2.1

Bei der Bundesanstalt bestand kein einheitliches, abgestimmtes Sicherungsverfahren für die Nutzer- und für die Systemdateien. Eine Archivierungsanweisung existierte nicht. Datenträger wurden unkontrolliert aus dem Archiv gegeben. Eine regelmäßige Inventur der Magnetbänder fand nicht statt. Die letzte Inventur wurde im Jahre 1983 durchgeführt. Entgegen dem Prinzip der Funktionstrennung wurden Aufgaben der Archivverwaltung und der Maschinenbedienung (Operating) von ein und derselben Person wahrgenommen. Die Operatoren hatten eine systemweite Zugriffsberechtigung mit uneingeschränktem Zugriff auf alle Dateien.

2.2.2.2

Der Bundesrechnungshof hat beanstandet, daß aufgrund der uneinheitlichen, nicht abgestimmten Sicherung und der Mängel bei der Archivierung ein ausreichender Schutz vor Datenverlust und vor Diebstahl von Datenträgern nicht gewährleistet ist. Die fehlende Funktionentrennung und die systemweite Zugriffsberechtigung bergen die Gefahr der unberechtigten Kenntnisnahme und Manipulation von Daten und Programmen.

Er hat die Bundesanstalt aufgefordert,

- das Sicherungsverfahren abzustimmen und zu vereinheitlichen sowie eine Archivierungsanweisung zu erstellen,
- ein vollständiges Bestandsverzeichnis der Magnetbänder zu führen,
- regelmäßig Inventuren durchzuführen,
- Funktionentrennung zwischen Archivar und Operator einzuführen und die Zugriffsrechte zu beschränken.

2.2.2.3

Die Bundesanstalt hat entgegnet, sie halte ihre „umfangreichen" Sicherungsarbeiten gemäß einem Sicherungsplan für ausreichend. Ein Bestandsverzeichnis der Magnetbänder sei bereits vorhanden. Regelmäßige Inventuren der Datenträger im Archiv könnten nur mit zusätzlichem Personal durchgeführt werden. Die Trennung der Aufgaben von Archivar und Operator sei aus personellen Gründen nicht möglich. Es sei erforderlich, die Operatoren weiterhin mit systemweiter Zugriffsberechtigung auszustatten, damit sie ihre Arbeiten fristgerecht durchführen könnten.

2.2.2.4

Der Bundesrechnungshof kann sich den Ausführungen der Bundesanstalt nicht anschließen. Ein alle Datenträger umfassendes Bestandsverzeichnis fehlte. Zur Rekonstruktion der Daten und Programme im Katastrophenfall ist ein einheitliches, zwischen den Nutzern und dem Rechenzentrum abgestimmtes und alle Teilaspekte umfassendes Sicherungskonzept erforderlich. Dieses ist nicht vorhanden.

Ein Bedürfnis für die Vergabe der sicherheitsrelevanten systemweiten Zugriffsberechtigung an Operatoren ist nicht erkennbar. Diese Berechtigung sollte nur sehr restriktiv vergeben werden. Operatoren benötigen in einem Produktionsrechenzentrum zu ihrer Aufgabenerledigung keine Berechtigung zum Zugriff auf alle Daten und Programme.

2.3 Einschränkung der Zugriffsberechtigung

Der Bundesminister hat sich zu den Beanstandungen bei dem Bundesamt und der Bundesanstalt nicht geäußert. Er sollte dafür Sorge tragen, daß ein abgestimmtes Sicherungskonzept erstellt wird. Die Zugriffsberechtigungen in der Bundesanstalt sollten restriktiv, d. h. beschränkt auf das für die jeweilige Aufgabenerfüllung erforderliche Maß, vergeben werden.

3 Bundesminister der Verteidigung

3.1 Verarbeitung sensibler Daten

3.1.1

In einem Rechenzentrum der Bundeswehr werden sensible, zum Teil als Verschlußsache (VS) eingestufte Daten verarbeitet. Das Rechenzentrum liegt ungeschützt unmittelbar an einer öffentlichen Straße. An seiner Rückfront befinden sich öffentliche Parkplätze. Datenbestände, aus denen VS-Vertraulich eingestufte Listen erstellt werden, lagerten ohne besondere Schutzvorkehrungen im Datenträgerarchiv. Für die Verarbeitung wurde nicht abstrahlsichere und nicht zugelassene Hardware benutzt.

Der Bundesminister wurde bereits bei der Prüfung eines anderen Rechenzentrums im Jahre 1988 aufgefordert, ein Konzept für die Verarbeitung von VS-Daten für alle Rechenzentren der Bundeswehr zu erstellen. Ein solches Konzept liegt noch nicht vor.

3.1.2

Der Bundesrechnungshof hat bemängelt, daß wegen der organisatorisch und räumlich unzureichenden Sicherung der Datenbestände Mitarbeiter des Rechenzentrums unberechtigt Listen erstellen können, die für die Verteidigung bedeutsam sind. Durch den Gebrauch nicht abstrahlsicherer Geräte ist die Vertraulichkeit der Daten nicht gewährleistet. Der Bundesrechnungshof hat das Rechenzentrum aufgefordert zu prüfen, ob die Abstrahlung bei als Verschlußsache eingestuften Daten hinzunehmen oder ob zu deren Verarbeitung ein sichereres Rechenzentrum zu benutzen ist.

3.1.3

Der Bundesminister hat mitgeteilt, daß er Absicherungsmaßnahmen vorgesehen hat, die er für ausreichend hält. Zur Vorbereitung und Durchführung der Listenerstellung seien mehrere Personen erforderlich. Der Einsatz von abstrahlsicherer Hardware bei einer Verarbeitungsdauer der Liste im Minutenbereich sei unwirtschaftlich.

3.1.4

Die Kritik des Bundesrechnungshofes, daß der Bundesminister nicht alle gebotenen Maßnahmen zum Schutze der sensiblen Daten ergriffen habe, ist nicht ausgeräumt. Durch seine Lage ist das Rechenzentrum in verstärktem Maße der Gefahr von Abhörangriffen ausgesetzt. Dies kann die Auslagerung von sensiblen Verfahren erforderlich machen.

Der Bundesminister sollte nunmehr beginnen, das vom Bundesrechnungshof geforderte Konzept für die Verarbeitung von VS-Daten zu erstellen. Dabei sollten auch sensible, aber nicht als Verschlußsache eingestufte Daten berücksichtigt werden.

3.2 Mikroverfilmung

3.2.1

In dem Rechenzentrum werden Daten mikroverfilmt, die teilweise als Verschlußsache eingestuft sind. Die eingesetzte Verfilmungsanlage ist für die Verarbeitung solcher Daten nicht zugelassen. Maßnahmen zur Abschirmung von kompromittierender Abstrahlung waren nicht getroffen.

3.2.2

Der Bundesrechnungshof hat es als unvertretbar angesehen, VS-Daten mit Geräten zu verarbeiten, die dafür nicht zugelassen sind. Die Vertraulichkeit der dort verfilmten Daten ist nicht gewährleistet, da die Strahlungsintensität des Mikroverfilmungsgerätes besonders groß sein und mit einfachen handelsüblichen Geräten aufgefangen und dargestellt werden kann. Das Risiko der Computerspionage wird durch die Lage des Rechenzentrums vergrößert.

3.2.3

Der Bundesrechnungshof hat den Bundesminister aufgefordert, die Sicherheitslücke unverzüglich zu beseitigen. Dieser hat mitgeteilt, die Bundeswehr habe ein Schutzgerät installiert, das eine mögliche Auswertung der Abstrahlung verhindern soll. Er werde die Arbeitsweise des Schutzgerätes überprüfen lassen.

3.2.4

Der Bundesrechnungshof hat Zweifel, ob die vorgesehene Maßnahme die gewünschte Wirkung erbringen wird. Der Bundesminister sollte die Schutzwirkung des Gerätes unverzüglich untersuchen lassen.

4 Deutsche Bundesbahn

Die Deutsche Bundesbahn betreibt mehrere Rechenzentren, und zwar sowohl für operative Zwecke (wie Transportsteuerung, Fahrzeuginformations- und Vormeldesystem, Container-Vormeldeverfahren, Fahrkartenverkauf) als auch für administrative Aufgaben (z. B. Personaldatenverarbeitung, Lohn- und Bezüge-Abrechnung, Steuerung des Güterkraftverkehrs und der Materialwirtschaft).

4.1 Objektsicherheit

4.1.1

Die Objektsicherheit eines Rechenzentrums wies Lücken auf:

- Es liegt ungeschützt an einer stark befahrenen Straße.
- Fahrzeuge konnten unmittelbar an den Gebäudemauern abgestellt werden.

- Die Gebäuderückseite war lediglich mit niedrigen Garagenwänden abgesichert.
- Der Pförtner konnte nicht die gesamte Gebäuderückseite überwachen.

Der kontrollierte Zugang zu den Sicherheitsbereichen des Rechenzentrums war nicht gewährleistet:

- Die Mitarbeiter hatten Schließmechanismen der Türen zu den verschiedenen Sicherheitsbereichen außer Funktion gesetzt.
- Über einen tagsüber nicht gesicherten Personenaufzug waren die Maschinensäle der Datenverarbeitungsanlage auch für Unbefugte zugänglich.
- Magnetbandarchive in unmittelbarer Nähe von zwei Anlagen waren nicht als getrennte Sicherheitsbereiche eingerichtet.
- Zugangsberechtigungen zum Rechenzentrum waren in großer Zahl auch an nicht ständig im Gebäude beschäftigte Personen ausgegeben worden.

4.1.2

Der Bundesrechnungshof hat bemängelt, daß die Sicherung des Gebäudes — insbesondere unter Berücksichtigung seiner ungeschützten Lage — unzulänglich ist, was mögliche Sabotagehandlungen begünstigt.

Geräte und Datenträger seien vor Sabotage und Diebstahl nicht ausreichend geschützt, weil der Zugang zu dem Gebäude und den verschiedenen Sicherheitsbereichen nicht genügend kontrolliert wird. Die zu große Zahl von zutrittsberechtigten Personen vergrößere diese Gefahr. Insgesamt ergebe sich dadurch ein erhebliches Sicherheitsrisiko.

Der Bundesrechnungshof hat den Vorstand aufgefordert, die äußere Absicherung des Gebäudes zu verbessern sowie die baulichen und organisatorischen Mängel der Zugangskontrolle zu dem Gebäude zu beheben. Weiterhin sei erforderlich, die Anzahl der Zutrittsberechtigten auf die ständig im Rechenzentrum beschäftigten Mitarbeiter zu begrenzen und die schwerwiegenden Mängel beim Zugangskontrollsystem innerhalb des Gebäudes zu beseitigen.

4.1.3

Der Vorstand hat die Mängel anerkannt und mitgeteilt, er habe verschiedene Maßnahmen eingeleitet, um die äußere Sicherheit des Gebäudes zu verbessern. Getrennte Sicherheitsbereiche für die Magnetbandarchive könnten aber erst im Rahmen von Baumaßnahmen geschaffen werden.

4.1.4

Der Bundesrechnungshof hält es für geboten, daß schon jetzt — bis zum Abschluß der Baumaßnahmen — geeignete Vorkehrungen getroffen werden, um die Kontrollen des Zugangs zum Gebäude und den Schutz der Magnetbandarchive zu verbessern.

Der Vorstand sollte die eingeleiteten Maßnahmen mit Nachdruck durchführen und Sicherheitsaspekte auch während der Umbauphase mit höchster Priorität verfolgen.

4.2 Einsatz von Sicherheitssoftware

4.2.1

Einer großen Zahl von Mitarbeitern des Rechenzentrums war der uneingeschränkte Zugriff auf alle Daten und Programme der Produktionsrechner möglich. Insgesamt besaßen 31 Personen den „Generalschlüssel". Mehrere Nutzer arbeiteten unter einer gemeinsamen Nutzerkennung. Zugriffsversuche wurden nicht regelmäßig und zeitnah kontrolliert.

Bei der Einrichtung und Verwaltung der Sicherheitssoftware wurde festgestellt:

- Im System waren ungültige Nutzerkennungen gespeichert.
- Die Paßworte waren für einen Zeitraum von 60 Tagen gültig.
- Nicht alle Zugriffsberechtigungen wurden einheitlich von einer zentralen Stelle im Rechenzentrum verwaltet.
- Magnetbanddateien waren in das Zugriffsschutzsystem nicht einbezogen.

4.2.2

Der Bundesrechnungshof hat wegen der festgestellten Mängel die Sicherheit von Daten und Programmen vor unberechtigter Kenntnisnahme, Veränderung und Zerstörung als nicht mehr gewährleistet angesehen. Insbesondere die im Rechenzentrum verarbeiteten personenbezogenen, kassenwirksamen und sonstigen sensiblen Daten waren einem hohen Risiko des Verlustes der Vertraulichkeit und Unversehrtheit ausgesetzt.

4.2.3

Der Vorstand hat die Beanstandungen anerkannt und mitgeteilt, er habe die Zugriffsrechte eingeschränkt.

4.2.4

Die Neuregelung des Zugriffsschutzes bietet nach der Überzeugung des Bundesrechnungshofes noch immer keine ausreichende Sicherheit vor Manipulation. Die Zugriffsberechtigungen sind noch nicht weitgehend genug eingeschränkt; Zugriffsversuche werden nicht kontrolliert.

Der Vorstand sollte dafür Sorge tragen, daß insbesondere bei den Neuentwicklungen die Zugriffsberechtigungen noch restriktiver erteilt werden.

4.3 Schutz der Datenfernübertragung

4.3.1

Eines der geprüften Rechenzentren bildet den zentralen Knoten im bundesweiten Datenfernübertragungsnetz der Deutschen Bundesbahn. Alle Kabelzuführungen laufen in einem nicht abgesicherten, öffentlich zugänglichen Kabelschacht zusammen. Eine Zuführung an verschiedenen Stellen (Mehrwegesystem) zur Erhöhung der Verfügbarkeit des Datennetzes gibt es nicht.

4.3.2

Der Bundesrechnungshof sieht das Datenfernübertragungsnetz durch die fehlende Mehrfachauslegung der Zuleitungen und die ungesicherte Kabelführung als nicht ausreichend gegen Sabotageakte geschützt an.

Er hat den Vorstand aufgefordert, Vorkehrungen zu treffen, um die Verletzbarkeit der Datenfernübertragung zu beseitigen.

4.3.3

Der Vorstand hat die Feststellungen anerkannt und mitgeteilt, daß er zur Zeit Möglichkeiten einer Verbesserung der Sicherheitsvorkehrungen untersuche.

4.3.4

Die besondere Gefährdung des Datenfernübertragungsnetzes erfordert ein sofortiges Handeln. Der Vorstand sollte sicherstellen, daß die Mängel unverzüglich beseitigt werden.

5 Deutsche Bundespost

In einem Rechenzentrum der Deutschen Bundespost werden täglich rd. 300 000 Fernmelderechnungen erstellt, kuvertiert und versandt sowie weitere, zum Teil auch kassenwirksame Datenverarbeitungsverfahren durchgeführt.

5.1 Programme mit schädlichen Nebenwirkungen

5.1.1

In den Speicherbereich, der den Programmierern zur Veränderung von Produktionsprogrammen zugeteilt war, gelangten über die Datenfernübertragung unkontrolliert Nachrichten und Daten. Es war nicht auszuschließen, daß sich darunter auch ausführbare Programme mit schädlicher Nebenwirkung befanden, die Produktionsprogramme in nicht vorhersehbarer Weise verfälschen können.

5.1.2

Der Bundesrechnungshof hat bemängelt, daß manipulierte Programme im Bereich kassenwirksamer Verfahren zur Ausführung kommen könnten. Er hat darauf hingewiesen, daß durch die Art der derzeit praktizierten Programmabnahme Beeinträchtigungen der Richtigkeit und Unversehrtheit der Produktionsprogramme kaum erkannt werden könnten.

Der Bundesrechnungshof hat den Bundesminister aufgefordert, künftig sicherzustellen, daß Produktionsprogramme lediglich in Bereichen mit eingeschränkten Zugriffsberechtigungen gespeichert werden, in die also Daten und Programme nur kontrolliert gelangen können und die einer maschinellen Änderungskontrolle unterliegen (geschützte Bereiche).

5.1.3

Der Bundesminister hat mitgeteilt, daß er die bisher von ihm erlassenen Regelungen über den Schutz des Speicherbereichs der Programmierer für ausreichend halte. Das Einschleusen von Programmen mit schädlicher Nebenwirkung sei nicht durch das Einschränken von Berechtigungen, sondern nur durch eine mit hohem Aufwand verbundene manuelle Kontrolle aller durchgeführten Änderungen an den Programmen zu verhindern.

5.1.4

Der Bundesrechnungshof ist der Auffassung, daß trotz der vom Bundesminister bisher getroffenen Regelungen weiterhin die Möglichkeit einer schädlichen Programmänderung besteht. Solange durch Nachrichtenübermittlung Programme fremder Herkunft in dieselben Speicherbereiche gelangen können, in denen die Programmierer Produktionsprogramme speichern und bearbeiten, besteht die Gefahr der Beeinflussung durch diese Programme. Der Bundesrechnungshof bleibt deshalb bei seiner Auffassung, daß Produktionsprogramme nur in geschützten Bereichen gespeichert werden sollen. Die vom Bundesrechnungshof hierfür vorgeschlagene maschinelle Versionskontrolle ist mit vertretbarem Aufwand durchführbar und bietet darüber hinaus höheren Schutz als die vom Bundesminister angeführte manuelle Kontrolle.

5.2 Zugriffsschutz dezentraler Rechner

5.2.1

An den zentralen Rechner in diesem Rechenzentrum waren über Datenfernübertragung eigenständige Rechner angeschlossen, die auf Datenbestände und Programme des zentralen Rechners zugreifen konnten. Das eingesetzte Betriebssystem gewährleistete keinen Schutz gegen die Wiederholung unerlaubter Paßworteingabeversuche. So wurden zwar wiederholte Versuche protokolliert, die zugehörige Benut-

zerkennung wurde jedoch nach einer bestimmten Anzahl von Fehlversuchen nicht automatisch gesperrt. Die Protokolle über Paßworteingaben wurden nicht systematisch ausgewertet. Weiterhin hat der Bundesrechnungshof festgestellt, daß die Systembetreuer der dezentralen Rechner umfassende Zugriffsrechte bei der Verwaltung von sicherheitsrelevanten Programmfunktionen hatten. Eine Kontrolle ihrer Tätigkeit fehlte jedoch.

5.2.2

Der Bundesrechnungshof hat beanstandet, daß der mangelnde Schutz vor wiederholten unberechtigten Zugriffen sowie die unkontrollierte Ausübung umfassender Zugriffsrechte die Vertraulichkeit sowie die Richtigkeit und Unversehrtheit der auf den dezentralen Rechnern betriebenen Datenverarbeitungsanwendungen und der dort verwalteten Daten gefährden. Er hat dem Bundesminister vorgeschlagen, dafür zu sorgen, daß neben den protokollierten Zugriffsversuchen auf Programme und Dateien auch die Tätigkeit der Systembetreuer durch einen unabhängigen Kontrolleur geprüft wird.

5.2.3

Der Bundesminister hat mitgeteilt, daß die beschriebenen Mängel auf die bisher nicht vollständige Installation der vorgesehenen Sicherungsvorkehrungen zurückzuführen seien. Er hat zugesagt — wie vom Bundesrechnungshof empfohlen —, die Einrichtung einer Kontrolle zu untersuchen. Für die Prüfung und Verfolgung von Zugriffsverstößen würden Regelungen erarbeitet.

5.2.4

Der Bundesrechnungshof vertritt den Standpunkt, daß die zur Gewährleistung der Vertraulichkeit sowie der Richtigkeit und Unversehrtheit der Datenverarbeitungsanwendungen erforderlichen Maßnahmen mit mehr Nachdruck zu betreiben sind. Er wird die Wirksamkeit der getroffenen Maßnahmen zu gegebener Zeit prüfen.

5.3 Ausweichrechenzentrum

5.3.1

Die Katastrophenschutzplanung des Bundesministers sieht vor, daß das Drucken, Separieren, Kuvertieren und Versenden der täglich rd. 300 000 Fernmelderechnungen nach einem Totalausfall des Rechenzentrums von einem geplanten Rumpf-Rechenzentrum übernommen wird, in dem technische Einrichtungen für die Weiterverarbeitung der Arbeitsergebnisse bereitgehalten werden sollen. Bisher liegt nur die Planung zur Errichtung des Rumpf-Rechenzentrums mit der zugehörigen Infrastruktur vor.

5.3.2

Der Bundesrechnungshof hat beanstandet, daß es bei Totalausfall des Rechenzentrums nicht möglich ist, kurzfristig die Fertigung der Fernmelderechnungen in ein anderes Rechenzentrum zu übernehmen. Er hat dem Bundesminister empfohlen, über die bereits vorgelegte Planung zügig zu entscheiden.

5.3.3

Der Bundesminister hat mitgeteilt, in Kürze eine weitere Entscheidung über die Errichtung der Rumpf-Rechenzentren zu treffen. Das bisherige Konzept sei insbesondere hinsichtlich der Rechnerverlagerung und der erforderlichen Datenfernübertragungsleitungen zu überarbeiten. Die Oberpostdirektionen würden unabhängig davon aufgefordert, geeignete Räumlichkeiten auszuwählen und — soweit möglich — mit der erforderlichen Infrastruktur auszustatten.

5.3.4

Der Bundesminister und die Vorstände der Unternehmen der Deutschen Bundespost sollten über das vorliegende Konzept unverzüglich entscheiden.

Der Bericht ist vom Großen Senat des Bundesrechnungshofes beschlossen worden.

Frankfurt am Main, 28. August 1990

Bundesrechnungshof
Dr. Zavelberg

-1-B

Bundesrat Drucksache 599/90 (Beschluß)
09.11.90

Beschluß

des Bundesrates

zum

Bericht des Bundesrechnungshofes gemäß § 99 BHO über die Sicherheit der Informationsverarbeitung in Rechenzentren der Bundesverwaltung

Der Bundesrat hat in seiner 624. Sitzung am 9. November 1990 beschlossen, von dem Bericht Kenntnis zu nehmen.

Alleinvertrieb: Verlag Dr. Hans Heger, Postfach 20 08 21, 5300 Bonn 2
ISSN 0720-2946