Datensicherung in der Praxis

Autor(en): **Rohrbach, G.**

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-904139

Datensicherung in der Praxis

G. Rohrbach

Informationen gehören zu den wichtigsten Vermögenswerten eines Unternehmens. In der Praxis konzentrieren sich die Datensicherungsvorkehrungen auf technische und organisatorische Massnahmen wie z. B. Verschlüsselung, Datenzugriffskontrolle, Vorgehen nach Sicherheitsnormen, klare Verantwortungsregelung sowie umfassende Kontrollen dieser Massnahmen. Im vorliegenden Artikel wird das Informationssicherungskonzept der IBM Schweiz skizziert.

Les informations font partie des ressources les plus précieuses d'une entreprise. En pratique, les dispositions à prendre sont principalement d'ordre technique et d'organisation, par exemple chiffrage, contrôle d'accès, procédures selon des normes de sécurité, stricte réglementation de la responsabilité ainsi que de sérieux contrôles de ces dispositions. Description de la conception d'IBM Suisse concernant cette sécurité.

Adresse des Autors

G. Rohrbach, IBM Schweiz, General-Guisan-Quai 26, 8022 Zürich.

1. Zielsetzung der Datensicherung

Die Datensicherung ist gewährleistet, wenn:

- die Sicherungsverantwortlichkeiten zugeteilt sind,
- betrieblich angepasste Sicherungsmassnahmen bestehen, welche Informationen und deren Verarbeitungseinrichtungen gegen Bedrohungen schützen,
- Kontrolleinrichtungen vorhanden sind, die das Funktionieren der Sicherungsmassnahmen überwachen.

2. Bedrohungen

Informationen und deren Verarbeitungseinrichtungen sind durch folgende Bedrohungen gefährdet:

- Manipulation an Daten und Programmen,
- Eindringen von betriebseigenen oder betriebsfremden Personen in EDV-Systeme mit dem Ziel, Informationen zu manipulieren, zu entwenden oder auszuspionieren,
- Verrat von vertraulichen Informationen,
- Sabotageaktionen an Rechenzentren, an deren Infrastruktureinrichtungen, an EDV-Geräten und an Informationen bzw. Informationsträgern,
- Diebstahl von EDV-Komponenten, -Programmen sowie -Informationen bzw. Informationsträgern,
- Diebstahl bzw. missbräuchliche Verwendung von EDV-Kapazität,
- Verstösse gegen Copyright-Bestimmungen im Softwarebereich,
- Zerstörung von EDV-Zentren, Informationen und Informationsarchiven durch zivile Katastrophen.

3. Sicherungsverantwortung

Grundsätzlich ist die Sicherungsverantwortung eine Linienverantwortung, die auf verschiedene Funktionen aufgeteilt ist (Fig. 1).

3.1 Der Eigentümer von Informationen (Owner)

Der Owner ist ein höherer Vorgesetzter, der in der Regel einer Organisationseinheit vorsteht. Er ist u.a. für folgende Massnahmen verantwortlich:

- Festlegung der Vertraulichkeitsklassifizierung für Informationen und Berichte,
- Bewilligung des Informationszugriffs,
- Festlegen der Kontrollmassnahmen für Informationen und EDV-Verfahren und Überwachen von deren Einhaltung,
- Bezeichnen der betriebsvitalen Informationen und Verfahren sowie Veranlassen von Notfalltests,
- Bekanntgebung von Sicherheitsvorschriften an die Benützer und das Rechenzentrum.

3.2 Das EDV-Zentrum (Supplier of Services)

Das EDV Zentrum verwaltet treuhänderisch die ihm übergebenen Informationen. Es ist für folgende Sicherheitsmassnahmen verantwortlich:

- Schutz des EDV-Zentrums und seiner Infrastruktureinrichtungen gemäss den vom Sicherheitsdienst erlassenen Normen,
- Schutz der Informationen entsprechend den von den Ownern bestimmten Vertraulichkeitsklassifizierungen,
- Erlass von sicherheitstechnischen Vorschriften zur Benützung von Datenstationen (z. B. Passwort-Regeln),
- Orientierung der Owner über den Stand der Informationszugriffsbewilligungen sowie über die erfolgten Zugriffe.

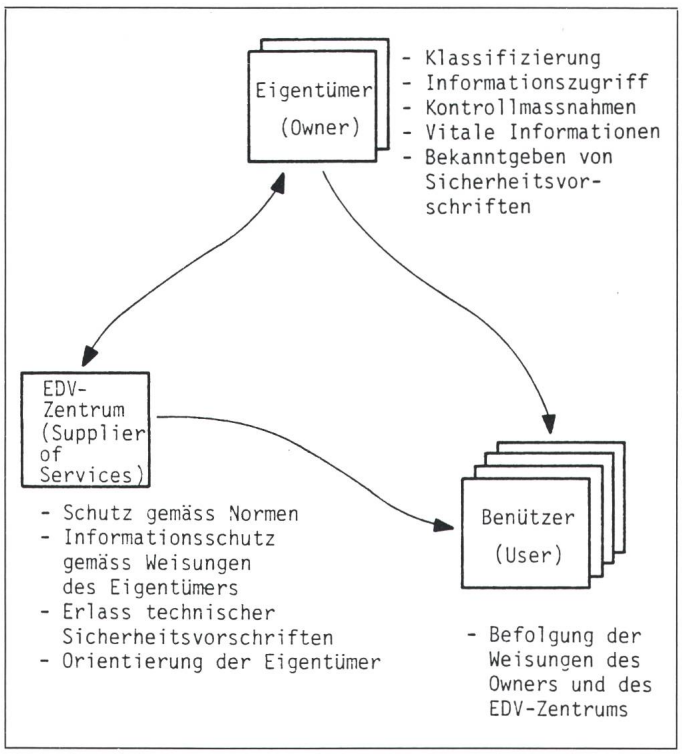


Fig. 1 Sicherungsverantwortung

3.3 Der Benützer (User)

Benützer sind alle Betriebsangehörigen, die EDV-Dienstleistungen zur Erfüllung ihrer Aufgaben benötigen. Sie sind für folgende Sicherheitsmassnahmen verantwortlich:
- Befolgung der vom Owner erlassenen Sicherheitsvorschriften,
- Einhaltung der vom Rechenzentrum erlassenen sicherheitstechnischen Vorschriften, z.B. zur Benutzung von Datenstationen.

3.4 Der Sicherheitsdienst

Der Sicherheitsdienst ist als Stabsabteilung zuständig für den Erlass von Sicherheitsnormen und deren Durchsetzung.

4. Technische Sicherungsmassnahmen

Folgende Massnahmen stehen im Mittelpunkt:

4.1 Objektsicherung

Diese umfasst physische Einrichtungen zur Sicherung des EDV-Zentrums und deren Infrastruktur, der Datenarchive und Datenstationen sowie Massnahmen zum Schutze der in diesem Bereich tätigen Mitarbeiter.

4.2 Zutrittskontrolle

Darunter fallen computergesteuerte Zutrittskontrollsysteme (Controlled Access Systems), welche u.a. sicherstellen, dass nur autorisierte Personen Zutritt zu definierten Sicherheitszonen erhalten.

4.3 Verschlüsselungseinrichtungen

Für die Übermittlung von Informationen ist der Einsatz von Verschlüsselungsgeräten ab einer festgelegten Vertraulichkeitsklassifizierung vorgeschrieben. Dies trifft auch für den Datenverkehr mit dem Ausland zu.

4.4 Datenzugriffskontrolle

Das IBM-Programmprodukt RACF (Resource Access Control Facility) stellt sicher, dass nur autorisierte Mitarbeiter Zugriff zu betrieblichen Informationen erhalten (Fig. 2). RACF differenziert nach Angaben der Owner zwischen Mitarbeitern, die Informationen lesen, und solchen, die Informationen verändern dürfen.

5. Organisatorische Sicherungsmassnahmen

Folgende Massnahmen, zu denen auch die im Abschnitt 3 beschriebene Sicherungsverantwortung gehört, sind wesentlich:

5.1 Normen

Sicherheitsnormen sind betriebsumfassend, einheitlich und umfassen u.a.:
- die Bezeichnung und Handhabung der Vertraulichkeitsklassifizierung,
- die Vorschriften für die Verschliessung von Pulten und Schränken nach Arbeitsschluss (Clean Desk),
- die Benutzeridentifizierung und Passwortgestaltung,
- die Zutrittskontrolle,
- die Handhabung «sensitiver» Anwendungs- und Systemprogramme,
- die Aufrechterhaltung des Betriebes in Notsituationen usw.

Die Sicherheitnormen sind von allen Mitarbeitern des Unternehmens zu befolgen. Die Ablehnung einer Sicherheitsnorm erfordert eine von der Geschäftsleitung genehmigte Risikoübernahme.

5.2 Organisation der Datensicherung

Für jede Organisationseinheit und jedes EDV-Zentrum ist ein von der Geschäftsleitung bestimmter, höherer Vorgesetzter in einer Nebenfunktion als Beauftragter für die Datensicherung zuständig. Er hat in der Linie, der er angehört, die Sicherheitsnormen durchzusetzen. Wo es erforderlich ist, wird er durch Fachspezialisten aus seinem Bereich unterstützt.

5.3 Schulung

Mitarbeiter mit Sicherungsverantwortung werden an internen Kursen

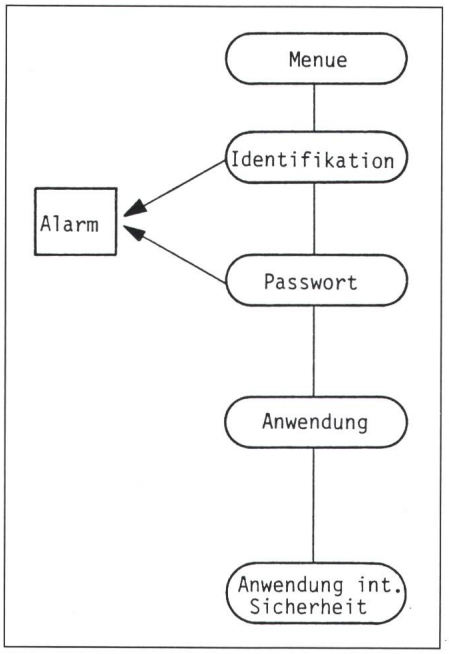


Fig. 2 Datenzugriffskontrolle RAFC

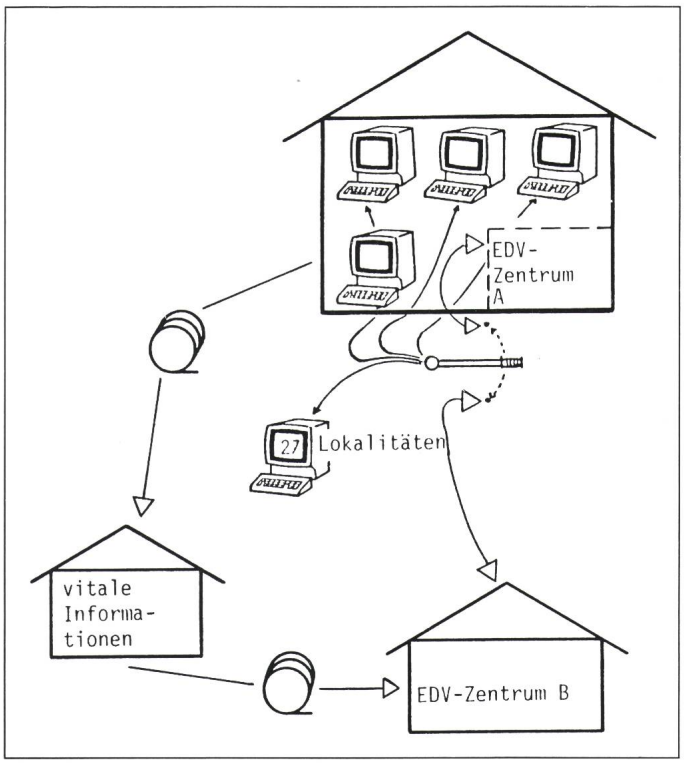
Das Passwort ist charakterisiert durch folgende Eigenschaften:
- 6 bis 8 Stellen
- mind. 2 Ziffern
- keine Wiederholung innert 24 Monaten
- nicht trivial
- Austausch nach spätestens 30 Tagen
- Änderung jederzeit möglich

geschult und jährlich weitergebildet. Alle Mitarbeiter der IBM Schweiz werden bei ihrem Eintritt über die Sicherheitsvorschriften informiert. Neuernannte Vorgesetzte erlernen bereits im ersten Managementseminar die Bedeutung der Sicherheits-Kontrollverantwortung. Mitarbeiter, die für den Aussendiensteinsatz vorgesehen sind, werden mit einem spezifischen Ausbildungsmodul auf besondere Sicherheitsvorschriften hingewiesen. Allen Mitarbeitern des Unternehmens werden durch periodische Aktionen die wichtigsten Sicherheitsbestimmungen in Erinnerung gerufen.

5.4 Zielvorgaben

Sicherheitsbeauftragte und Mitarbeiter mit besonderen Sicherheitsaufgaben erhalten persönliche Zielsetzungen. Die Qualität der Sicherheit im Unternehmen wird vierteljährlich gemessen und erlaubt einen konzernweiten Vergleich.

Fig. 3
Notfalltest bei IBM



6. Kontrollsystem

Erst ein wirkungsvolles Kontrollinstrumentarium kann den Nachweis erbringen, dass die angeordneten Sicherheitsmassnahmen wirkungsvoll sind und korrekt angewendet werden. Das IBM-Kontrollsystem ist mehrstufig ausgelegt:

6.1 Selbstbeurteilung (Self Assessment)

Jede Organisationseinheit, jeder Owner und jeder Benützer überprüft jährlich seinen Sicherheitsstatus anhand eines vom Sicherheitsdienst vorbereiteten Fragebogens. Abweichungen werden erfasst und der Unterzeichner des Fragebogens verpflichtet, innerhalb einer gesetzten Frist die Abweichung zu korrigieren.

6.2 Sicherheitsuntersuchungen durch Partnerfunktionen (Peer Review)

Alle zwei Jahre erfolgt in jedem Betriebsbereich eine Sicherheitsuntersuchung durch eine Partnerfunktion. Dieses vom Sicherheitsdienst kontrollierte Vorgehen kann wie folgt beurteilt werden:

- Der hohe Sicherheitsgrad ist erhalten geblieben,
- Mitarbeiter, die mit der Untersuchung betraut werden, lernen verschiedene Betriebsbereiche und Methoden der Sicherheitsgewährleistung kennen.
- Die Mitarbeiter werden durch die Untersuchungsvorbereitung, deren Durchführung sowie durch das Abfassen der entsprechenden Rapporte motiviert; ihre Kompetenz in Sicherheitsfragen nimmt zu.
- Betriebsbereiche, die auf diese Weise geprüft werden, zeigen eine grössere Bereitschaft, Verbesserungsempfehlungen zu akzeptieren.

6.3 Sicherheitsuntersuchungen durch den Sicherheitsdienst

Im Gegensatz zu den Peer Reviews werden die professionellen Untersuchungen durch Mitarbeiter des Sicherheitsdienstes durchgeführt. Die Untersuchungsergebnisse werden der Geschäftsleitung unterbreitet. Die Realisierung von Korrekturmassnahmen für aufgezeigte Schwachstellen ist zwingend.

6.4 Notfalltest

Jedes EDV-Zentrum prüft jährlich, ob eine Betriebsaufnahme der als vital bezeichneten Anwendungen innerhalb vorgegebener Zeiten möglich ist (Fig. 3). Dieser Test wird ausschliesslich mit ausgelagerten Daten und Programmen durchgeführt und findet im Ausweichsrechenzentrum, d.h. in einer anderen Lokalität, statt.

6.5 Penetrationstests

Unter Mitwirkung des Sicherheitsdienstes wird jedes EDV-Zentrum jährlich einem Penetrationstest unterzogen. Bei diesem Test versuchen Systemspezialisten, ob (unter Ausnutzung profunder Kenntnisse der Hard- und Software) in ein System eingedrungen werden kann und damit der Zugang zu vertraulichen Informationen möglich ist. Dieser Test deckt auf, wieweit die im EDV-Zentrum installierten Sicherheitsmassnahmen wirkungsvoll sind und nahtlos ineinandergreifen.

7. Schlussfolgerungen

Die Erfahrungen haben gelehrt, dass ein blosses Aneinanderfügen von Sicherheitsmassnahmen nicht zu einer umfassenden Sicherheit führt; ohne ein in der Unternehmensstruktur verankertes Sicherheitskonzept gibt es keine Informationssicherung.

Die zur Realisierung des Konzeptes erforderlichen technischen Mittel sind auf dem Markt erhältlich und haben sich bewährt. Zweckmässige organisatorische Sicherungsmassnahmen sind bekannt und erprobt. Damit liegt es an der Geschäftsleitung eines Unternehmens, die Datensicherung durchzusetzen und entsprechende Konzepte zu realisieren. Für IBM gehören die Geschäftsinformationen zu den wichtigsten Vermögenswerten, für deren optimalen Schutz sie zu sorgen bereit ist.