Computerkriminalität und -sicherheit

Autor(en): **Schäffer, K.-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): **83 (1992)**

Heft 4

PDF erstellt am: **05.08.2024**

Persistenter Link: https://doi.org/10.5169/seals-902798

Computerkriminalität und -sicherheit

K.-P. Schäffer

Von Jahr zu Jahr nimmt die Zahl der in Betrieb stehenden EDV-Anlagen überproportional zu. 40–50% aller Beschäftigten in der Schweiz dürfen in irgendeiner Art und Weise ihre Arbeit mit Hilfe der EDV bewältigen. Die vielfältigen Anwendungsmöglichkeiten der EDV und deren Wichtigkeit für das Funktionieren unserer Wirtschaft und Verwaltung bedeuten, dass Missbräuche mit Computern einen viel höheren Stellenwert im Gesamtkomplex «Kriminalität» einnehmen als Missbräuche mit andern Arten von Technologien.

Le nombre des installations de traitement des données augmente d'une année à l'autre de manière exagérée. 40 à 50% des employés suisses accomplissent leur travail à l'aide de l'informatique. Les nombreuses possibilités d'utilisation de l'informatique et leur importance pour le bon fonctionnement de notre économie et de notre administration signifient que, dans l'ensemble que représente la «criminalité», des emplois abusifs d'ordinateurs sont bien plus graves que ceux d'autres technologies.

Kurzfassung eines Referates anlässlich der Clusis-Tagung vom November 1991 über die Unipede-Umfrage «Sicherheit in Rechenzentren».

Adresse des Autors
Dr. *Klaus-Peter Schäffer*, Elektra Baselland Liestal EBL, Mühlemattstrasse 6, 4140 Liestal.

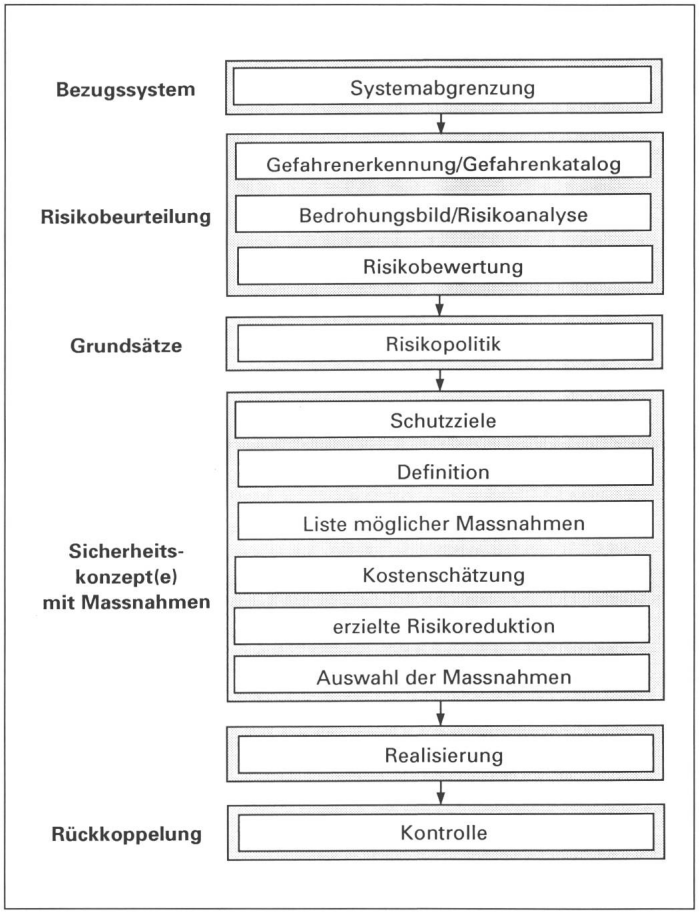
Problemkreise des Datenmissbrauchs

Bei den Missbräuchen von Computern geht es primär um zwei Problemkreise:

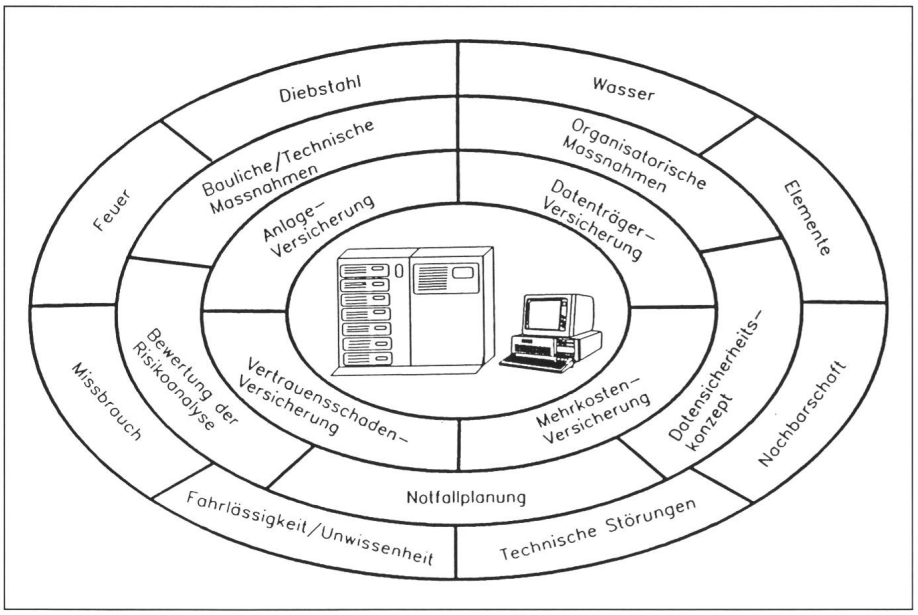
- Datenschutz bedeutet Bedrohung der Privatsphäre natürlicher und juristischer Personen durch die elektronische Sammlung und Speicherung von Daten. Auf den Datenschutz wird hier nicht näher eingetreten.
- Datensicherheit oder Computerkriminalität umfasst die Probleme der Sicherung von Daten vor vorsätzlichen Zerstörungen, Veränderungen oder anderen Zugriffen.

Die häufigsten Erscheinungsformen der Computerkriminalität lassen sich grundsätzlich in fünf Gruppen einteilen: Manipulation, Zeitdiebstahl, Computerspionage, Hardwarediebstahl und Computersabotage (Viren, Hacker). Sie vereinigen den grössten Teil aller Fälle auf sich.

Zum Schutz gegen die Computerkriminalität muss für jede Unternehmung mit EDV-Anlagen ein entsprechendes Sicherheitskonzept erarbeitet werden, das sich mit den baulichen, technischen



Mögliches Vorgehen zur Aufstellung und Realisierung eines Sicherheitskonzeptes



Bei einem Sicherheitskonzept zu beachtende Faktoren

und organisatorischen Massnahmen befasst. Dazu gehören die Risikoanalyse, die Sicherheitsgrundsätze, die Sicherheitsmassnahmen sowie die periodische Überprüfung und Anpassung des Konzeptes.

Die Auswahl der zu treffenden Sicherheitsmassnahmen erfolgt nach dem Grundsatz: Möglichst viel Sicherheit zu einem möglichst niedrigen Preis. Es handelt sich somit um ein Optimierungsproblem von Kosten/Sicherheit. Dazu gilt es zu prüfen, welche Risiken und Schwachstellen auf jeden Fall abgedeckt werden müssen. Der zu erwartende Schaden muss also den Kosten der Sicherheitsmassnahmen gegenübergestellt werden.

Die Erfahrung zeigt, dass die Datensicherung primär nicht kritisch ist. Im Vordergrund steht vielmehr die Gefahr des unerlaubten Informationsabflusses durch Dritte oder durch unberechtigte Mitarbeiter. Im weiteren besteht die Gefahr unerlaubter Veränderung oder des Zerstörens von Daten, sei es vorsätzlich oder fahrlässig, durch berechtigte und unberechtigte Mitarbeiter sowie durch Dritte.

Wichtig ist, dass die Zweckmässigkeit der getroffenen Sicherheitsmassnahmen periodisch überprüft und nötigenfalls angepasst werden, können doch sämtliche Massnahmen nie einen hundertprozentigen Schutz gewährleisten.

Sicherheit in Rechenzentren

Der Studienausschuss für Informatik der Unipede (Internationale Union der Erzeuger und Verteiler elektrischer Energie) hat 1990 angeregt, eine internationale Umfrage über den Stand der Sicherheit in Rechenzentren durchzuführen.

Sinn dieser Umfrage war es, einen generellen Überblick über die Sicherheitsstandards der Rechenzentren (RZ) der der Unipede angeschlossenen sowie anderer Unternehmungen und Branchen zu erhalten. Im weiteren sollte durch den sehr umfassenden Fragebogen auch ein Bewusstseinsprozess in Gang gesetzt werden, welche Aspekte bei einem Rechenzentrum sicherheitsrelevant sind, das heisst der Umfragebogen konnte von den angesprochenen EDV-Chefs bzw. Rechenzentrum-Leitern als Checkliste zur Beurteilung ihres Sicherheitsstandards verwendet werden.

Um die Motivation zu einer seriösen Beantwortung der Fragebogen zu erreichen, wurde bewusst auf Prüf- und Fangfragen verzichtet. Dadurch ist zwar eine Überprüfung der Reliabilität nicht möglich, doch sollte durch den hohen Motivationsgrad die entsprechende Zuverlässigkeit erreicht worden sein.

Einige Unternehmen haben «aus Sicherheitsgründen» auf die Rücksendung des Fragebogens verzichtet. Von den 45 ausgewerteten Fragebogen kamen die meisten von Elektrizitätswerken bzw. Elektrizitätsverteilunternehmen. Nur etwa 10% der Fragebogen stammten aus andern Branchen.

Von den Ländern her beteiligten sich in der Reihenfolge der Anzahl der Rücksendungen vor allem die Schweiz, Grossbritannien, Spanien, Italien und vereinzelt Belgien, Dänemark, Deutschland, Finnland, Frankreich und Griechenland.

Aus der Auswertung der Fragebogen geht deutlich hervor, dass den Sicherheitsbelangen des engeren EDV-Bereichs – wie Datensicherung, Funktionstüchtigkeit der Hardware und der Software, Schutz der Daten – hohe Beachtung geschenkt wurde.

Auch die Sicherheitsmotivation und die Überprüfung der Mitarbeiter wird mehrheitlich sorgfältig durchgeführt. Eine Ausnahme bildet das temporäre Personal und stellt damit eine Schwachstelle dar.

Hingegen wurde den infrastruktur- und bautechnischen Aspekten nicht der notwendige Stellenwert zugeordnet. Speziell im Bereich des Brandschutzes sind bei verschiedenen Anlagen grössere Mängel vorhanden. Der Einbau einer Brandmeldeanlage ermöglicht nur die sofortige Alarmierung, bringt aber keinen Schutz gegen bereits ausgebrochenes Feuer und den dabei entstehenden korrosiven Rauch.

Die Beurteilung der Klimageräte stellt diese oft als sicherheitstechnisch kritisch heraus. Auch der Standortfrage wurde generell zu wenig Beachtung geschenkt.

Für den Notfall sind nur die Hälfte der Rechenzentren gewappnet. Zudem existieren bei mehr als der Hälfte keine entsprechenden Back-up-Konzepte. Das Fehlen dieser Notfallplanung liegt sicher zum grossen Teil daran, dass ungenügende Versicherungsbedarfsanalysen, speziell für den Bereich Betriebsunterbruch, durchgeführt wurden.

Allgemein kann gesagt werden, dass bei der Versicherungsbedarfsanalyse das Betriebsunterbruchs-Risiko mit Abstand das grösste Risiko darstellt. Erst wenn dieser Tatbestand bewusst wird, entsteht die Motivation zur Durchführung der Notfallplanung und zur Betriebsunterbruchversicherung, die bei den analysierten Betrieben mangelhaft ist. Die Schweiz bildet hier eher eine positive Ausnahme.

Das Resultat dieser Umfrage lässt den Schluss zu, dass die Sicherheitsplanung der Rechenzentren schwergewichtig allein von der Informatik nahestehenden Personen (Informatiker, Mathematiker, Physiker usw.), und nicht einem Team, bestehend aus Baufachverständigen, Ingenieuren, allgemeinen Sicherheitsexperten, Versicherungsexperten und Informatikern, ausgeführt wurde.

Bei der Erstellung von integralen Sicherheitskonzepten für Rechenzentren ist die fachübergreifende Teamarbeit mit einem vernetzten, gesamtheitlichen Denken eine wesentliche Voraussetzung für ein optimales Gelingen.

Schweizerischer Elektrotechnischer Verein
Association Suisse des Electriciens
Associazione Svizzera degli Elettrotecnici
Swiss Electrotechnical Association

Wirksame Blitzschutzanlagen

Blitzschutzanlagen sind nicht billig. Sie können sogar teuer zu stehen kommen, wenn unsachgemäss geplant und ausgeführt, denn nachträgliche Änderungen sind immer mit hohen Kosten verbunden. Zudem besteht die Gefahr, dass derartige Anlagen im Ernstfall ihren Zweck nicht erfüllen.

Wir kennen die Probleme des Blitzschutzes und die optimalen Lösungen hiefür.

Wir stehen Privaten, Ingenieurunternehmen und kantonalen Instanzen zur Verfügung für Planung, Beratung, Kontrollen, Branduntersuchungen und Instruktionskurse.

Auskunft: Schweizerischer Elektrotechnischer Verein, Starkstrominspektorat
Seefeldstrasse 301, Postfach, 8034 Zürich
Telefon 01 / 384 91 11 – Telex 817431 – Telefax 01 / 55 14 26