

Zeitschrift: Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association suisse des électriciens, de l'Association des entreprises électriques suisses

Herausgeber: Schweizerischer Elektrotechnischer Verein ; Verband Schweizerischer Elektrizitätsunternehmen

Band: 83 (1992)

Heft: 4

Artikel: Computerkriminalität und -sicherheit

Autor: Schäffer, K.-P.

DOI: <https://doi.org/10.5169/seals-902798>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

Download PDF: 12.12.2025

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

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 Uniped-Umfrage «Sicherheit in Rechenzentren».

Adresse des Autors

Dr. Klaus-Peter Schäffer, Elektra Baselland
Liestal EBL, Mühlemattstrasse 6, 4140 Liestal.

Problemkreise des Datenmissbrauchs

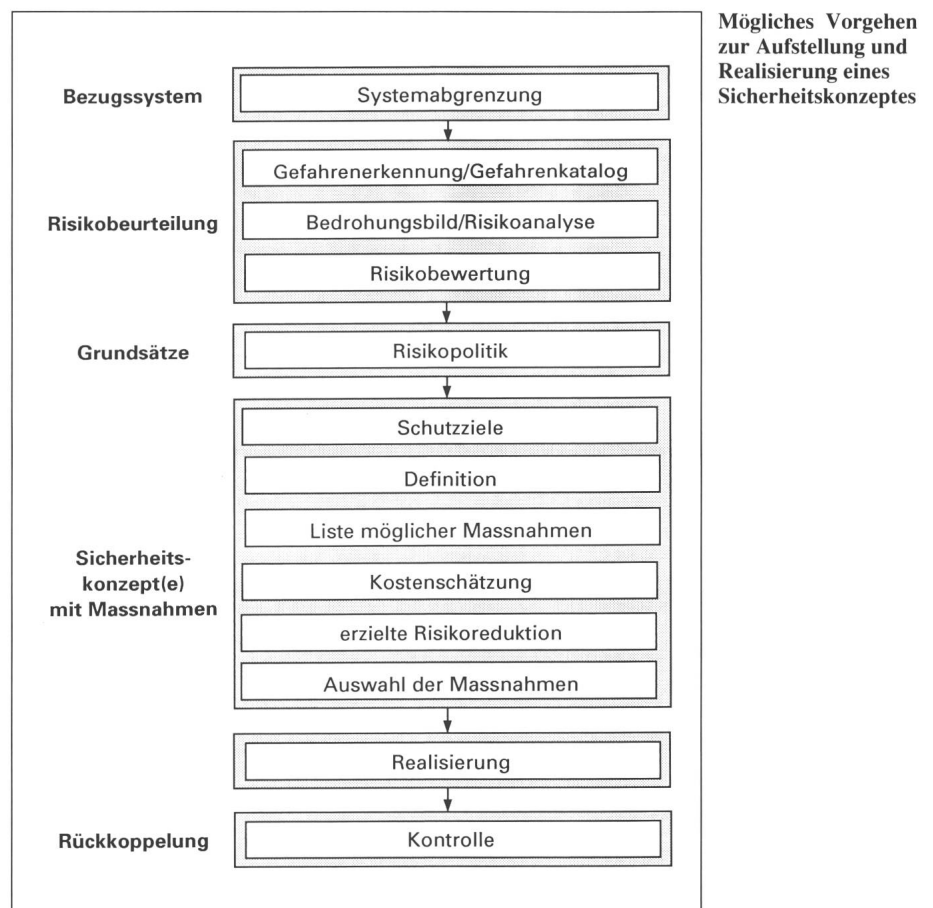
Bei den Missbräuchen von Computern geht es primär um zwei Problemkreise:

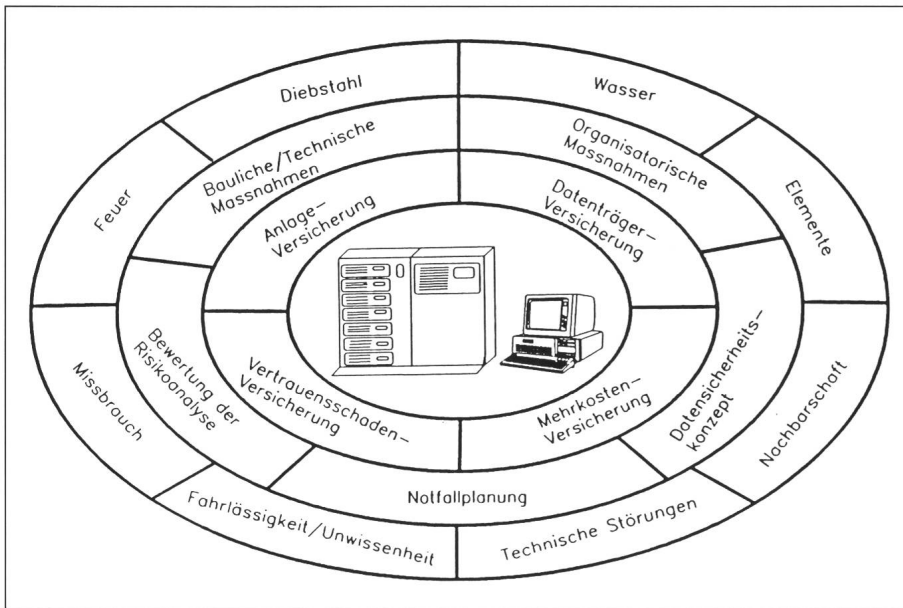
- Datenschutz bedeutet Bedrohung der Privatsphäre natürlicher und juristischer Personen durch die elektronische Sammlung und Speicherung von Daten. Auf den Datenschutz wird hier nicht näher eingetreten.
- Datensicherheit oder Computerkriminalität umfasst die Probleme der Sicherung von Daten vor vorsätz-

lichen 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





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 inter-

nationale 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 schwerge- wichtig 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.

Siegfried Peyer AG
peyerenergie



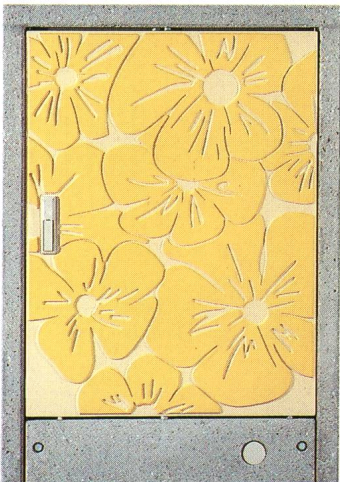
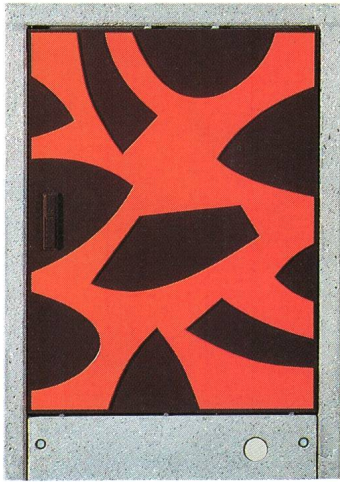
Kunst am Bau

Ortsnetz-Verteilkabinen von **peyer** als neue Gestaltungselemente für die heute veränderten, differenzierten Anforderungen an Design und Umweltintegration.

Zusätzlich zur bewährten Kabinen-Linie aus Verbundwerkstoff bringt **peyer** Betonkabinen mit neuartigem Oberflächen-Design.

Für Elektrizitätswerke und Planer eine Möglichkeit, neue, fröhliche Akzente in den öffentlichen Raum zu setzen.

peyerenergie
CH-8832 Wollerau
Telefon 01/784 46 46
Telex 875570
Fax 01/784 34 15



RUTSCHMANN

Transformatorstation Typ T 87



- Architektonisch sehr attraktiv, nur 1,5 m über Terrain
- Grösste Dauerhaftigkeit dank Beton und Chromstahl
- Bis vier Hochspannungsfelder 24 kV
- Grosse Niederspannungsverteilung
- Transformator 630 kVA
- Natürliche Kühlung
- Ideal in Fällen, bei denen eine Innenraumbenutzung ausser Betracht fällt.

Qualität und Preis überzeugen.

Verlangen Sie nähere Unterlagen bei

RUTSCHMANN

Rutschmann AG
8627 Grüningen, Tel. 01/935 21 56
Fax 01/935 21 76

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 hierfür.

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

Auskunft: Schweizerischer Elektrotechnischer Verein, Starkstrominspektorat
Seefeldstrasse 301, Postfach, 8034 Zürich
Telefon 01/384 91 11 – Telex 817 431 – Telefax 01/55 14 26