Information ist schützenswert : Computersicherheit : eine wichtige Komponente des Riskmanagements

Autor(en): **Stockar, Daniel von**

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): **82 (1991)**

Heft 17

PDF erstellt am: **22.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-903001

Information ist schützenswert

Computersicherheit – eine wichtige Komponente des Riskmanagements

Daniel von Stockar

Die Entwicklung der Industriegesellschaft zur Informationsgesellschaft wertet das Immaterialgut Information zum Produktionsfaktor auf. Damit wird Informationsschutz zur unternehmerischen Pflicht. Ganzheitliches Risikomanagement muss die Sicherheit des betrieblichen Informationssystems berücksichtigen. Da die verschiedenen Funktionen des Informationssystems zunehmend durch Computer abgedeckt werden, wird Computersicherheit immer wichtiger.

L'évolution de la société industrielle en société de l'information revalorise le produit immatériel information en facteur de production. La protection de l'information devient de la sorte un devoir de l'entreprise. Un management du risque global doit tenir compte de la sécurité du système d'information de l'entreprise. Les différentes fonctions du système d'information étant de plus en plus couvertes par des ordinateurs, la sécurité informatique revêt une importance accrue.

Adresse des Autors

Daniel M. von Stockar, dipl. Wirtschaftsinformatiker, lic. oec. publ.,
Leiter der Konzernfachstelle Informationsschutz,
Gebr. Sulzer AG, 8401 Winterthur

Bei zunehmender Abhängigkeit von zeitgerechter Information und der unaufhaltsamen Computerdurchdringung wird die Verfügbarkeit der Information und damit die Zuverlässigkeit des Informationssystems zum Lebensnerv einer Unternehmung. Das angemessene Risikomanagement des «vierten» Produktionsfaktors wird zur unternehmerischen Pflicht.

Wurde in ihrem Verantwortungsbereich schon einmal versucht, ein Informationsinventar aufzustellen? Haben sie daran gedacht, das es unter ihren Informationen am Arbeitsplatz auch solche von öffentlichem oder privatem Interesse gibt? Wie weit sind bereits Sicherheitsüberlegungen angestellt worden, zum Beispiel durch Beschränkung der Zugriffsberechtigung (Klassifizieren) oder durch Festhalten der Wichtigkeit für den Arbeitsablauf (Betriebsnotwendigkeit)? Stellen sie sich vor, solche Informationen gehen teilweise oder gesamthaft verloren oder geraten in falsche Hände...

Ursachen dafür gibt es viele. Brände, Wasserschäden und Fahrlässigkeit, aber auch Diebstahl und Computerkriminalität gehören zum Alltag, wie aus Schadenmeldungen bei Versicherungen zu schliessen ist. Obwohl oft geheimgehalten (z.B. aus Angst vor Imageverlust), liest man auch in der Tages- und Fachpresse vieles über Schäden aus mangelnder Informationssicherheit – zumeist aus aktuellem Anlass. Haben sie sich einmal Gedanken über die Schadenfolgen gemacht? Lassen sich diese bewerten?

Der vorliegende Artikel versteht sich als Einführung in den Informationsschutz. Nach einer Übersicht über Umfang, Ziel, Aufgaben und Methoden dieser Materie wird der Bereich Computersicherheit etwas genauer beleuchtet. Das letzte Kapitel soll mittels Richtlinien und Vorschlägen Hilfe zur Erstellung eines Informationsschutz-Konzepts anbieten.

Das betriebliche Informationssystem – Nervensystem der Unternehmung

Ein Informationssystem entsteht durch organisiertes Zusammenwirken von Information (Daten, Texte, Bilder usw.), Informationsverarbeitungsprozessen (Erfassung, Verwendung usw.) und Aktionsträgern (Menschen, Maschinen usw.) sowie durch festgelegte Interaktionsprotokolle. Konzeptionell lassen sich zwei Bereiche bilden: Die eigentliche Informationsverarbeitung und die Kommunikationskomponente. Bild 1 skizziert die weitere Unterteilung. Wichtig ist die konzeptionelle Trennung von Information und deren Verarbeitung. Die dadurch erreichbare Isolation der Informationsbestände ist die Voraussetzung für einen effektiven Schutz.

Ein Informationssystem ist grundsätzlich EDV-unabhängig. Allein die Tatsache, dass die wirtschaftlichen Wettbewerbsfaktoren Zeitvorsprung und Informationsvorsprung den zunehmenden Einsatz von Computern begünstigen, und daher betriebliche Abläufe vermehrt automatisiert werden, ist die Ursache für den zunehmenden EDV-Einsatz. Da alle Funktionsbereiche einer Unternehmung zunehmend vom Einsatz der Informationstechnologie betroffen sein werden, kommt dieser immer mehr die Aufgabe eines eigentlichen Nervensystems der Unternehmung zu. Aufgrund der sprunghaften Entwicklung und der raschen Generationenfolge beeinflusst die Informationstechnologie nicht nur stark die unternehmerische Wettbewerbsstrategie, sondern wird zum eigenständigen Wettbewerbsfaktor.

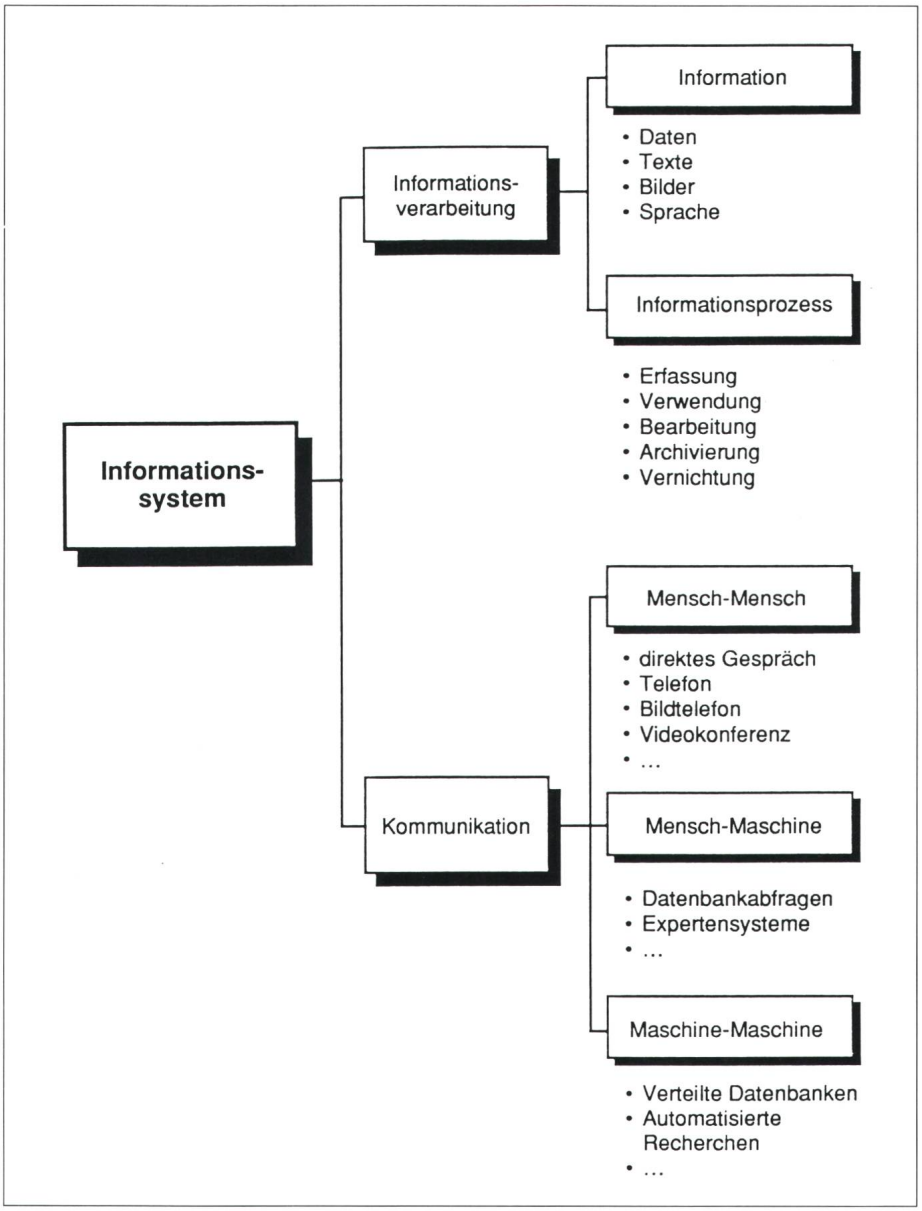


Bild 1 Komponenten des Informationssystems

Der viel zitierte qualitative Wandel unserer Industriegesellschaft in eine Informationsgesellschaft spiegelt sich in einer Neubewertung der Information als Produktionsfaktor wider. Für materielle Güter wurden über Jahrzehnte Kosten- und Investitionsrechnungsverfahren entwickelt, geprüft und verfeinert. Solche bewährte theoretische Grundlagen fehlen jedoch für das Immaterialgut Information. Allein das Defizit an gängigen Methoden rechtfertigt aber keinesfalls eine Unterschlagung der Information als Asset (wirtschaftliches Gut). Neu ist also weder die Information an sich, noch deren Verarbeitung, sondern die Notwendigkeit einer Differenzierung der Betrachtungsweise von Information im Bezug auf dessen immateriellen Wert. Dieses neue Wertverständnis wird seinen Niederschlag über kurz oder lang auch in betriebswirtschaftlichen Modellen und Methoden der Rechnungslegung und in Gesetzen finden.

Modernes Informationsmanagement

Historisch gesehen entstand diese Entwicklung mit dem Auftauchen des Information Resource Management (IRM) in den USA Anfang der 80er Jahre. Der Schwerpunkt der Überlegungen liegt bei den Interdependenzen zwischen der Unternehmensstrategie sowie den Informations- und Kommunikationstechniken. Die Erkenntnis, dass die Handhabung des Produktionsfaktors Information neben den bekannten EDV-technischen Fragestellungen auch organisations- und personalwirtschaftliche Auswirkungen hat, steht zurzeit im Zentrum der Diskussionen. Im Zuge dieser Entwicklungen bekommt die Frage nach dem Wert der Information bzw. dem Verlustrisiko zunehmendes Gewicht.

Informationssicherheit als Managementaufgabe

Sicherheit im Unternehmen stellt einen Zustand dar, in welchem bei möglichst geringer Beeinträchtigung durch Gefahren aller Art für eine erfolgreiche Zukunft gearbeitet werden kann. In bezug auf das Informationssystem bezweckt Sicherheit das vertrauliche (falls notwendig), richtige und zeitgerechte Verarbeiten und Zur-Verfügung-Stellen von Information.

Die erfolgreiche Implementation eines adäquaten Informationsschutzes steht und fällt mit der Motivation, der Mitarbeit und der Unterstützung durch die Unternehmensleitung. Auch ein noch so engagierter Sicherheitsbeauftragter muss in seinen Bemühungen scheitern, falls seine Entscheide nicht vom Topmanagement verabschiedet und getragen werden.

Die Aufgaben der Gestaltungsträger im Rahmen der Aufbauorganisation und die dazugehörige Kompetenzverteilung lassen sich wie folgt abgrenzen: Die Top-Management-Ebene pflegt einen aktiven Informationsaustausch mit dem Projektteam und manifestiert ihren Willen durch motivierte Mitarbeit bei der Erarbeitung der Sicherheitspolitik. Sie genehmigt die Politik, lebt ihr nach und wacht über deren Umsetzung im Betrieb. Auf der Bereichs-, Abteilungs- oder Divisionsebene wird die Risikoanalyse durchgeführt, sodann die Bewertung, Auswahl und Implementation der Schutzmassnahmen und die Kontrolle der Durchsetzung innerhalb der jeweiligen Verantwortungsbereiche. Auf der Mitarbeiterebene schliesslich kommt der Grundsatz zum Tragen, nach dem jeder einzelne im Betrieb seinen Beitrag zur Wahrung der Sicherheit zu leisten hat, dies in erster Linie durch eine korrekte Anwendung der Sicherheitsmassnahmen.

Auf dem Weg zum unternehmensweiten Informationsschutz können die folgenden Phasen identifiziert werden:

Phase 1: Der Bereich Informationssicherheit wird definiert

Ausgehend von einer generellen Sicherheitspolitik wird der Bereich Informationssicherheit definiert und zu einem integrierten Bestandteil der Unternehmenssicherheit erhoben. Die Informationsschutz-Politik schafft
- einheitliche und verbindliche Richtlinien und eine klare Regelung von Verantwortlichkeiten,
- Grundlagen für die interne Revision,
- die Möglichkeit, im Schadenfall allfällige rechtliche Schritte abzustützen.

Die Politik muss Aussagen machen über die Besitzverhältnisse und die Schutzwürdigkeit der im Betrieb anfallenden Daten. Das Unternehmen muss in der Politik ihr Interesse am Informationsschutz zum Ausdruck bringen.

Phase 2: Das Klassifikationssystem wird entwickelt und implementiert

Informationen müssen bezüglich der zwei Dimensionen betriebsnotwendig/nicht betriebsnotwendig und klassifiziert/nicht klassifiziert zugeordnet werden können. Da es unrealistisch ist, dass Manager und Mitarbeiter sämtliche Information bezüglich Betriebsnotwendigkeit und Klassifikation untersuchen, ist es notwendig, Richtlinien aufzustellen, welche die Sensitivität ganzer Informationsgruppen regelt, und festhält, wie diese Gruppen von Fall zu Fall zu handhaben sind. Das Umsetzen der Richtlinien für Klassifikation, Entklassifikation, Beschriftung, Ablage, Zugriff, Vernichtung und Vervielfältigung ist ex post ausserordentlich aufwendig und bereitet oft grosse Mühe. Der Informationssicherheits-Administrator ist demnach auch für die Wirtschaftlichkeit verantwortlich, das heisst für ein ausgeglichenes Verhältnis des Wertes der Information und des Aufwands für Aufbau und Administration des entsprechenden Schutzes.

Phase 3: Sicherheitsstandards werden entwickelt, festgeschrieben und implementiert

Die Sicherheitsstandards sind in schriftlicher Form zu erstellen und an alle Mitarbeiter zu adressieren. Ein Sicherheitshandbuch sollte die folgenden Themenkreise beinhalten bzw. abdecken:
- Festlegen einer einheitlichen Terminologie,
- Informationsschutzpolitik,
- Informationsbesitz- und Verantwortungsverhältnisse,
- Klassifikationssystem(e),
- Fachstellen, Funktionen, Pflichtenhefte,
- Sicherheitsabklärungen neuer und bestehender Mitarbeiter,
- Sicherheit im Verkehr mit dem zentralen Rechenzentrum,
- Sicherheit der Arbeitsplatzcomputer und lokalen Netze,
- Risikomanagement-Aspekte,
- Investitions-/Beschaffungspolitik,
- Richtlinien für die interne Revision.

Es ist eine Aufgabe des Informationsschutz-Administrators, dieses Handbuch auf dem aktuellen Stand zu halten.

Im Rahmen der Einführung und Überprüfung des Informationsschutzsystems spielt die Sensibilisierung aller Personen im Betrieb eine zentrale Rolle. Gezielte Orientierung und Motivation auf allen Stufen ist ein Schlüssel zum Erfolg. Die Erfahrung zeigt, dass mangelhafte Informationssicherheit ihre Ursache oft in fehlendem Verständnis oder sogar in Missinterpretationen und somit in ungenügender Ausbildung hat.

Risikomanagement

Sicherheitsverantwortung ist Risikoverantwortung. In einer Umwelt voller Risiken ist es unternehmerische Aufgabe, diese vorauszusehen und zu minimieren. Risiken entsprechen einer bezüglich Eintrittswahrscheinlichkeit und Schadenausmass bewerteten Gefahr. Sie lassen sich gliedern in *Aktionsrisiken* und *Bedingungsrisiken*. Aktionsrisiken oder auch Wagnisrisiken genannt, sind Risiken des normalen unternehmerischen Handelns und Entscheidens und haben einen tendenziell spekulativen Charakter. Einem erwarteten Gewinn steht die Möglichkeit eines Verlustes gegenüber. Sie sind grundsätzlich nicht versicherbar. Bei Bedingungsrisiken oder «reinen» Risiken handelt es sich um eine Gefährdung der Randbedingungen des normalen unternehmerischen Handelns und Entscheidens, also um unfallmässige Risiken; es sind Störungen durch plötzlich auftretende Ereignisse mit sofortiger Wirkung. Dabei können nur Schäden, also niemals Gewinne entstehen. Sie sind in der Regel versicherbar.

Als grobes Vorgehensraster für das Risikomanagement empfehlen sich wiederum drei Phasen:

Phase A: Risikoidentifikation

Erfolgt meist mittels Inspektionen vor Ort, durch Fragebogen sowie in Interviews mit den Gesamtverantwortlichen und verschiedenen Linieninstanzen. Die Fähigkeit zur zielgerichteten Kommunikation ist dabei von zentraler Wichtigkeit. Um die Komplexität der Situation zu erfassen, und vor allem um die Risiken gesamthaft zu identifizieren, empfiehlt sich ein Top-down-Ansatz. Dabei werden die folgenden Bereiche isoliert betrachtet:
- Perimeter (Gefahren aus der Umgebung),
- Peripherie (Objektschutz, Gebäudeschutz, Werkschutz)
- Konzentrationspunkte (Rechenzentrum, Netzeinspeisungen usw.),
- Systeme (Hardware und Software),
- Kommunikation,
- Personal.

Genaugenommen handelt es sich hierbei um die Identifikation von Gefahren, also um unbewertete Risiken. Auf dem derart entstandenen Gefahrenkatalog wird das Bedrohungsbild aufgebaut und die sogenannten Schutzzielsetzungen abgeleitet.

Das Bedrohungsbild vermittelt einen Überblick über die gesamte Bedrohung und lässt Bedrohungsschwerpunkte erkennen. Im Gegensatz zu den spekulativen Risiken werden in einem Bedrohungsbild ausschliesslich reine Risiken erfasst und beurteilt. Reine Risiken sind immer mit direkten und indirekten Schadenfolgen verbunden. Die Schutzzielsetzungen sind Rahmenbedingungen für die nachfolgenden Phasen. Sie bringen die Sicherheitsanforderungen einzelner Teilbereiche und/oder Aufgaben durch das Festlegen zum Beispiel einer maximalen Ausfallzeit zum Ausdruck.

Phase B: Risikobewertung

Das Risiko als bewertete Gefahr wird mit Hilfe von qualitativen oder quantitativen Methoden abgeleitet, im einfachsten Fall durch Verknüpfen des Schadenausmasses mit der Eintretenswahrscheinlichkeit. Weitergehende Methoden beziehen auch die Zeit und den internen Zinsfuss zur Abdiskontierung mit ein.

Die Bewertung der Gefahren ist ein komplexer Entscheidungsprozess und soll in enger Zusammenarbeit mit dem Management geschehen, denn sie bringt die wesentlichen Risiken zum Vorschein und ist deshalb von weitrei-

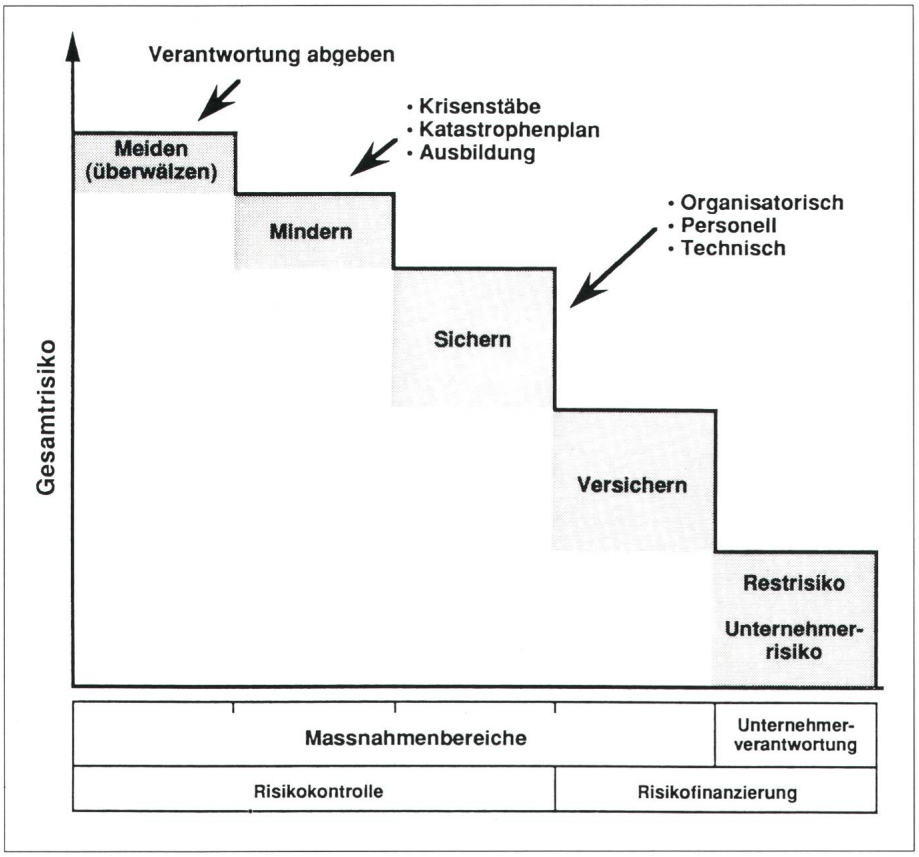


Bild 2 Sicherheitsdispositiv

chender Bedeutung. Es ist von Fall zu Fall zu entscheiden, ob die Investitionsrechnung, Portfoliotechniken, spieltheoretische Ansätze oder andere Bewertungsinstrumente zum Einsatz kommen.

Ein Risikokatalog sollte die folgenden drei Kategorien unterscheiden: Die Risikogruppe A bezieht sich auf die *subjektbezogenen* Gefahren (Fehlhandlungen). Darunter fallen die fahrlässigen Handlungen (mangelnde Sorgfalt, Irrtum, Unwissenheit usw.) und die vorsätzlichen Handlungen (Computerkriminalität usw.). Die Risikogruppe B steht für *objektbezogene* Gefahren (Fehlfunktionen). Unterschieden werden dabei Fehlfunktionen der Systeme selbst (Hardware, Software, Datenträger usw.) und Fehlfunktionen durch äussere Einflüsse (Stromausfall, Klima, Magnetismus usw.). Risiken aus *höherer Gewalt* (Wassereinbruch, Explosion usw.) werden der Risikogruppe C zugeordnet.

Phase C: Risikobewältigung

Das aus dem Risikokatalog ersichtliche Gesamtrisiko muss im Rahmen einer Bewältigungsstrategie mit betriebswirtschaftlich vertretbarem Aufwand und minimaler Beeinträchtigung von Abläufen sowie der daran beteiligten Personen auf ein tragbares Mass reduziert werden. Das in Bild 2 ersichtliche Sicherheitsdispositiv hat zentrale Bedeutung. Es basiert auf den Ergebnissen der vorherigen Phasen und stellt seinerseits die Management-Entscheidung dar, welche die Massnahmen zur Zielerreichung festlegt. Durch die Umsetzung des Sicherheitsdispositivs wird das erfasste Gesamtrisiko auf ein tolerierbares Restrisiko beschränkt; dieses muss bekannt und durch entsprechende Reserven abgedeckt sein. Die Risikokontrollmassnahmen (Meiden, Mindern, Sichern) einerseits haben die Reduktion von Schadenfrequenz, Schadenausmass und eine Erhöhung der Vorhersagbarkeit von Schadenereignissen zum Ziel. Das verbleibende Risiko wird andererseits durch Risikofinanzierung (Fremdfinanzierung: Versicherungen, Eigenfinanzierung: Unternehmerrisiko) abgedeckt. Für das unternehmerische Restrisiko soll das Motto gelten: «Don't risk more than you can afford to loose».

Jede Unternehmensleitung bedarf einer ganz gezielten Unterstützung im Bereich des Risikomanagements. Diese wird zum Beispiel von einer Fachstelle Informationsschutz angeboten. Die Dienstleistungen erstrecken sich von der Unterstützung bei der Formulierung der Sicherheitspolitik über die Durchführung von Analysen bis hin zur Beratung für eine zweckmässige Erfassung und Umlage der Kosten.

Der Risikomanager ermöglicht objektive Entscheide bezüglich der zu wählenden Anteile von Risikokontrolle und Risikofinanzierung. Zu diesem Zweck ist er ausgerüstet mit modernen – computergestützten – Hilfsmitteln (Datenbanken, Expertensysteme), welche Vorschläge unterbreiten, Vergleiche (z.B. innerhalb der Branche) ermöglichen und nicht zuletzt wertvolle Dienste im Sinne einer einheitlichen, vergleichbaren Dokumentation leisten. Risikomanagement dient letztlich einer besseren und planbaren Gesamtzielerreichung.

Computersicherheit

Wo Information in Form von Bits und Bytes mit wachsender Geschwindigkeit zwischen Arbeitsplätzen eines oder mehrerer Betriebe ausgetauscht wird, ist die Ordnungsmässigkeit der Informationsverarbeitung nicht mehr alleine durch den Schutz und die Überwachung des zentralen Rechenzentrums zu gewährleisten.

Bei Rechenzentren mit Hardware- und baulichen Investitionen von mehreren Millionen, lassen sich die 5...15% Aufwand für Sicherheitsspezialisten und -projekte (schweizerischer Durchschnitt) plausibel vertreten [1]. Demgegenüber scheint in Anbetracht der sinkenden Preise bei dezentralen Systemen (PCs, Workstations, Servers) eine angemessene Sicherheit an der Peripherie oft zu teuer. Häufig wird auch dem aus der wachsenden Komplexität des betrieblichen Informationssystems zunehmenden Sicherheitsbedürfnis nicht die nötige Beachtung zugemessen. Im Rahmen des Informationsschutzes drängt sich durch die zunehmende EDV-Durchdringung der Schwerpunkt Computersicherheit auf.

Der Begriff Computersicherheit umfasst Verfügbarkeit von Ressourcen, Robustheit gegen technische Störungen und Übertragungsfehler, Zuverlässigkeit aller Komponenten in verteilten Systemen, Schutz der Programme und Daten vor Verfälschung und Missbrauch durch unberechtigten Zugriff.

Computersicherheit beschränkt sich nicht auf die grossen Maschinen in Rechenzentren. Sie gilt unverändert auch für die arbeitsplatznahen Rechner bis hin zur Workstation und dem Personalcomputer. Gerade die oft ungenügende Sicherheit bei mittleren und kleinen Computern erfordert vielerorts noch einige Anstrengungen. Oft fehlen Kenntnisse der Eigentums-/Besitzsituation der Informationen und der daraus folgenden Verantwortlichkeit. Die zunehmende Vernetzung muss von isolierten zu ganzheitlichen Sicherheitsüberlegungen führen.

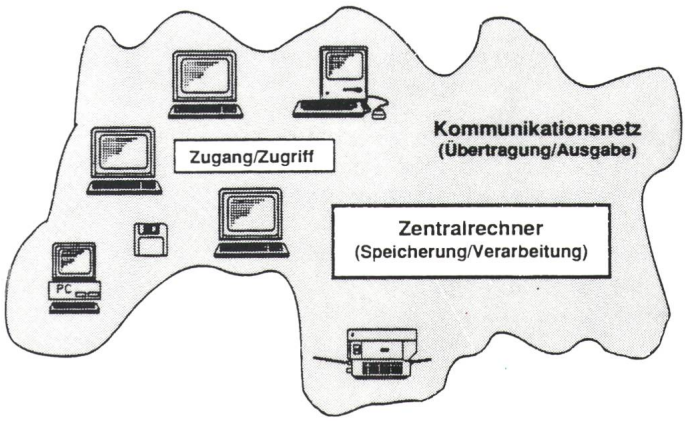
Computersicherheit soll nicht nur die Gefahren aus vorsätzlichen Handlungen und höherer Gewalt abdecken. Die weitaus häufigsten Schadenursachen sind fahrlässige Handlungen, also mangelnde Sensibilisierung und Disziplin [1]. Häufig werden die Kosten für Sicherheit im Verhältnis zu den Beschaffungskosten der Hardware betrachtet. Sicherheit scheint dann unwirtschaftlich. Richtigerweise muss die Sicherheit, auch der kleinsten peripheren Systeme, im Rahmen der Gesamtsicherheit betrachtet werden – keine Kette ist stärker als ihr schwächstes Glied.

Untersuchungen zeigen, dass der dezentral gespeicherte Informationswert denjenigen der entsprechenden Hardware meist um ein Vielfaches übersteigt. Mangelnde Sicherheit an der Peripherie kann selbst die aufwendigsten Schutzmassnahmen der zentralen EDV in Frage stellen.

Wie bereits angetönt, liegt der überwiegende Anteil von Schäden im Zusammenhang mit der EDV in der Unachtsamkeit. In diesem Lichte erscheint es angebracht, den Zugriff zu den Systemen prinzipiell einzuschränken, ganz unabhängig von der Klassifikation der installierten Programme und Daten. Jeder Systembenutzer muss zudem identifiziert werden. Nicht zuletzt die kurz vor dem Abschluss stehenden Verordnungen der EG, welche ganz gezielte Anforderungen zum Beispiel in bezug auf die Nachvollziehbarkeit von EDV oder den Datenschutz (im Wortlaut: «Protection of individuals in relation to the processing of personal data») stellen, lassen neue Bedürfnisse nach Computersicherheit erkennen [2]. Der Nachweis der Ordnungsmässigkeit der Datenverarbeitung ist nur aufgrund angemessener Sicherheitsstandards zu erbringen.

Das Objekt Informationssicherheit erlaubt eine Vielzahl von Betrachtungsperspektiven. Drei oft verwendete Strukturierungsansätze seien nachfolgend dargelegt:

Bild 3
Die drei sicherheitsrelevanten Systemkomponenten



1. Ansatz: Die Information an sich

Sie birgt zwei Risikoklassen: Abfluss und Verlust. Während durch Informationsabfluss Unberechtigte in den Besitz von möglicherweise klassifizierten Informationen kommen, beendet Informationsverlust die Verfügbarkeit von Information. Die prinzipiellen Gegenmassnahmen sind der Zugriffsschutz und/oder das Verschlüsseln der Daten gegen Abfluss (genauer: gegen die Einsichtnahme Unbefugter) und das Erstellen von Backups gegen Datenverlust.

2. Ansatz: Das Informationssystem

Bei der Betrachtung eines computergestützten Informationssystems sind gemäss Bild 3 die drei sicherheitsrelevanten Systemkomponenten Zugang/Zugriff, Speicherung/Verarbeitung und Übertragung/Ausgabe zu isolieren. Nur die Gesamtbetrachtung aller drei Komponenten führt zu einer ausgewogenen Sicherheit.

Zugangs- und Zugriffskontrolle

Dabei geht es unter anderem um die Identifikation von Personen (Access Control). Es gibt prinzipiell drei Methoden zur Identifikation:
- Haben (z.B. Schlüssel)
- Wissen (z.B. PIN, Passwort)
- Sein (biometrische Verfahren).

Durch Kombination dieser Methoden können höchste Identifikationsanforderungen realisiert werden.

Schutz von Daten und Programmen

Ist der Benutzer identifiziert, so stellt sich das Problem der Berechtigung (Authorization). Dabei sind zumindest drei mögliche Angriffe zu verhindern:
- unbefugtes Lesen
- unbefugte Veränderung
- unbefugte Verwendung (der Programme).

Dies erfolgt meist durch Software- und Hardware-Mechanismen in Kombination mit kryptografischen Verfahren (Verschlüsselung).

Schutz der übertragenen Daten

Eine sichere Übertragung wird implementiert durch Verschlüsselung (Encryption) und durch Methoden zur Authentizitätsabklärung (gegenseitige Identifikation). In diesem Bereich existieren bereits Standards.

Diese wurden von der International Standards Organization (ISO) entwikkelt. Als Bestandteil des Standards für die Kommunikationsarchitektur offener Systeme, des Open Systems Interconnect (OSI), bietet das Dokument [3] übersichtliche Hilfestellung zur Problemstrukturierung und führt zu modularen Lösungen. Dies wiederum ermöglicht flexible, anbieterunabhängige Sicherheitssysteme und damit den Schutz grosser Investitionen.

3. Ansatz: Die Information als Ressource

Er impliziert die folgenden Anforderungen bzw. Aspekte: Vertraulichkeit, Verfügbarkeit und Integrität. Wie bereits bemerkt, entscheidet die vertrauliche, zeitgerechte und korrekte Verfügbarkeit und Verarbeitung von Information über die Sicherheit und somit Güte eines Informationssystems.

Alle oben beschriebenen Ansätze bieten Hilfestellung zur Identifikation und Strukturierung von Risiken. Der Aspekt der Information als Ressource wird im folgenden Abschnitt weiterverfolgt.

Sicherheitskonzept

Abschliessend seien Anforderungen und Ansätze für ein Konzept dargelegt, welches die Umsetzung der Informationsschutz-Politik im Bereich der dezentralen EDV regeln soll. Das Konzept soll dem Informationsverantwortlichen bzw. seinem Chef ein Leitfaden zur Wahrnehmung der Sicherheitsverantwortung sein. Im weiteren soll damit die Grundlage für eine einheitliche Handhabung geschaffen werden. Dies ist Voraussetzung für einen ausgewogenen, wirtschaftlichen und prüfbaren betrieblichen Informationsschutz. Das Konzept soll helfen, den wesentlichen Bedrohungen entgegenzuwirken und ist Grundlage für ergänzende und weitergehende Vorschriften, Empfehlungen und Merkblätter.

Basis eines wirtschaftlichen Schutzes ist die Klassifikation nach einheitlichen Richtlinien, welche den Grad der Schutzbedürftigkeit der Daten angibt und aus welchem sich wiederum die zum Schutz notwendigen Massnahmen ableiten lassen. Wichtig ist auch die Bezeichnung der Träger der Sicherheitsverantwortung: Jeder Vorgesetzte ist für die Klassifikation der in seinem Bereich verarbeiteten Daten verantwortlich. Er kann einen Informationssicherheits-Beauftragten benennen. Es ist seine Aufgabe, geeignete Schutzmassnahmen zu ergreifen.

In Bild 4 sind die Sicherheitskriterien Vertraulichkeit, Verfügbarkeit und Integrität und die entsprechenden organisatorischen, personellen und technischen Massnahmen zusammengestellt. Es ist die Aufgabe des bezeichneten Beauftragten, in Absprache mit dem verantwortlichen Chef, geeignete Massnahmen zu ergreifen. Zur Unterstützung bei der Implementation der Sicherheitsmassnahmen sollte eine Fachstelle beigezogen werden können. Die Erkenntnis, dass die Sicherheitsproblematik bei dezentralen Systemen prinzipiell diesselbe ist wie bei grossen Rechenzentren, rechtfertigt das Bedürfnis nach Informationsschutz-Know-how. Die Flut von Sicherheitssystemen, zum Beispiel für PCs, ist nur mit grossem Zeitaufwand zu überblicken. Es ist eine Aufgabe der Fachstelle Informationsschutz, geeignete Systeme zu evaluieren, zu beraten, Installation und Konfiguration vorzunehmen und die (nicht zu unterschätzenden) Administrationsaufgaben zu instruieren.

	Organisatorische Massnahmen	Personelle Massnahmen	Technische Massnahmen
Vertraulichkeit	• Festhalten und Ueberprüfen der Klassifikation • Organisation des Zugriffsschutzes (User-ID und Berechtigungen) • Vier-Augen-Prinzip	• Sensibilisierung • Schulung • Bezeichnung der Träger der organisatorischen Massnahmen durch den Sicherheitsverantwortlichen • Verträge (Arbeitsvertrag, Geheimhaltungserklärung)	Schutz der Daten vor Einsichtnahme Unbefugter (je nach Klassifikation) durch: • Softwarelösungen • Hardwarelösungen • gemischte Lösungen • mit/ohne Datenverschlüsselung
Verfügbarkeit	• Verwaltung der Systeme und des Dateninventars • Fortführung der Sicherheitsanalyse • Organisation der Datensicherung • Standardisierung	• Sensibilisierung • Schulung • Standardisierung • Personalpolitik (z.B. Anreizsystem)	• Massnahmen zur Erhaltung der Daten • Sicherstellung des ordnungsgemässen Betriebes und der Wartung gemäss Herstellerangaben • Regelmässige Ueberprüfung der Software (z.B. auf Virenbefall) • Schutz vor Datenverlust durch regelmässige Sicherung • Schutz vor Datendiebstahl durch Datenverschlüsselung und Wegschliessen von Disketten und Backup
Integrität	• Klare Abläufe	• Festlegung von Berechtigungen und Verwaltung derselben • Geregelte Zuständigkeiten	• Korrekte, überprüfbare und festgeschriebene Abläufe und entsprechende Kontrollen

Bild 4 Massnahmensystematik für dezentrale Computersicherheit

Zusammenfassung

Das neue Wertverständnis bezüglich Information und deren Verarbeitung liegt einerseits in einer hohen Sensibilisierung der Öffentlichkeit im Rahmen der Speicherung und Verarbeitung personenbezogener Informationen, andererseits im legitimen Streben der Unternehmungen nach Wettbewerbsvorteilen durch Auskunftsbereitschaft und Rationalisierung.

Daraus ergeben sich neue Aufgaben für das Management. Die zunehmend systematische Nutzung der immateriellen Ressource Information birgt eine eigene Sicherheitsproblematik. Die verschiedenen Interessen von Informationsersteller, -eigentümer, -besitzer, Mitarbeiter, Konkurrenz, Gesetzgeber und der Öffentlichkeit können zu Problemen führen. Voraussetzung für die Lösung solcher Interessenskonflikte ist ein ordnungsgemässes, verlässliches, also sicheres betriebliches Informationssystem.

In der Umgebung der zentralen Rechenzentrumsdiensten wird über die Sicherheit in der Regel mit Sorgfalt gewacht. Schwachstellen sind die peripheren Systeme und Kommunikationseinrichtungen. Die Verantwortlichen müssen die Bedrohung erfassen und entsprechende Massnahmen veranlassen. Sensibilisierungsaktionen und zentrale Informations- bzw. Fachstellen sind erfolgversprechende Ansätze.

Literatur

[1] KES, Zeitschrift für Kommunikations- und EDV-Sicherheit, (1990)4 (September), Peter Hohl-Verlag, Ingelheim.
[2] EEC Council Decision 373 Articles 100a and 113.
[3] Security Architecture, OSI Reference Model Part 2, DIS7498-2, International Standards Organization, 1985.
[4] *Pfleeger Ch. P.:* Security in Computing, Prentice Hall, 1989.
[5] Datapro Reports on Information Security, International Edition, Mc Graw-Hill, 1991.

POLYPROF

.... ANSCHLIESSEN EINSCHALTEN

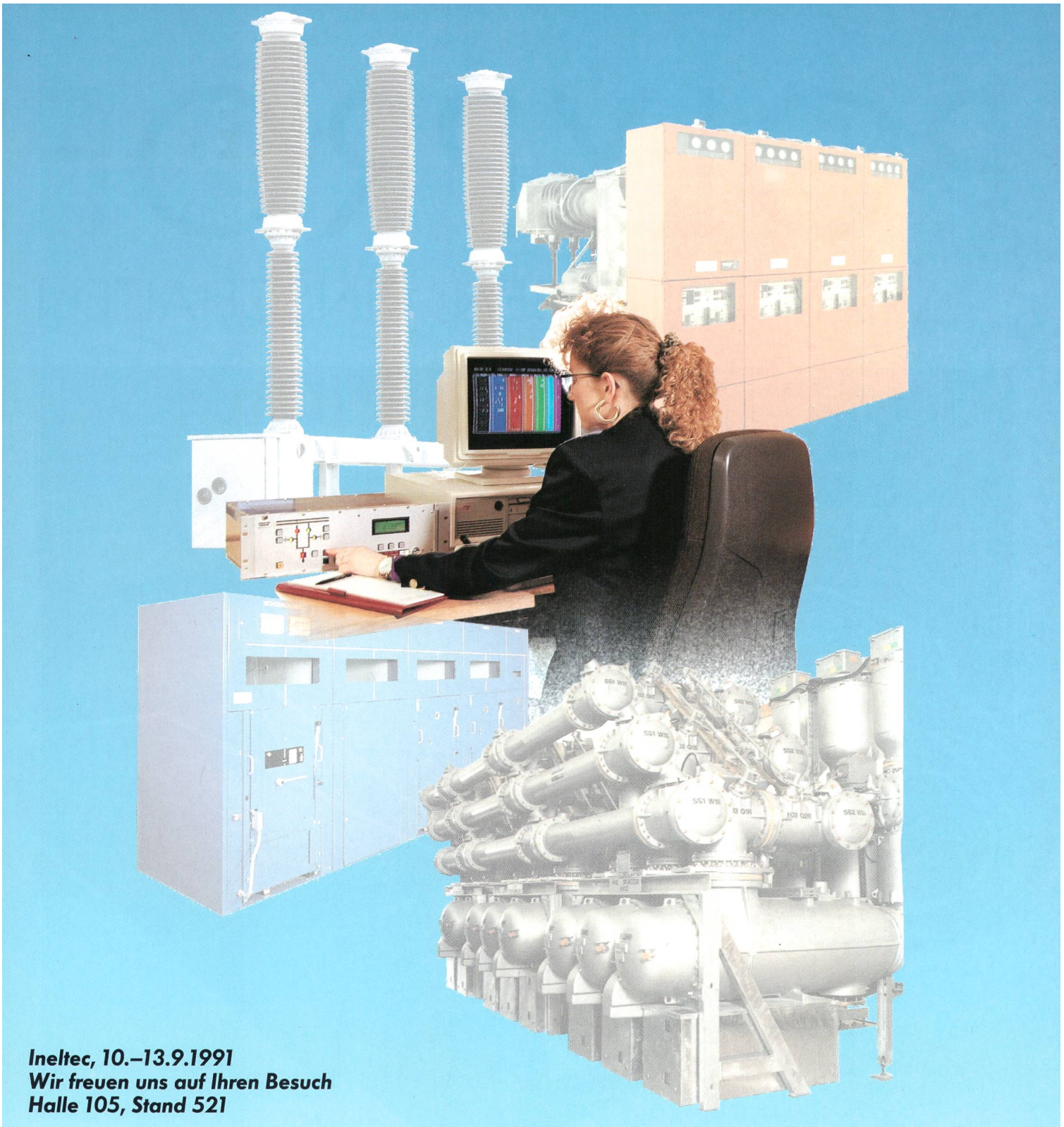
INELTEC 91
Halle 113, Stand 413

Die leuchtenunabhängigen Versorgungseinheiten POLYPROF für Halogen-Metall-Dampflampen sind keine sogenannten "Störefriede". Dank dem eleganten, ansprechenden Design kann der Beleuchtungsspezialist den elektrischen Teil von der Leuchte und deren thermischen Einflüssen trennen und somit auch kleine und kleinste Leuchten bauen.
Für weitere Auskunft fragen Sie uns.

H. Leuenberger AG, Fabrik elektrischer Apparate, Kaiserstuhlstrasse 44, CH - 8154 Oberglatt
Telefon 01 850 13 33, Telefax 01 850 59 85

Leuenberger

Ein Unternehmen der Lictor Holding AG



Ineltec, 10.–13.9.1991
Wir freuen uns auf Ihren Besuch
Halle 105, Stand 521

SERCOS – das neue Stations- und Feldleitsystem für Hoch- und Mittelspannungsanlagen

Wollen Sie in Ihrer Schaltanlage ein integriertes Leitsystem mit herstellerneutralen Kommunikations-Schnittstellen, ausgereiftem EMV-Konzept und optimalem Preis-/Leistungsverhältnis einsetzen?
Suchen Sie einen kompetenten Partner, bei dem Sekundär- und Primäranlage aus einer Hand kommen? Der alle Schnittstellenprobleme für Sie löst?

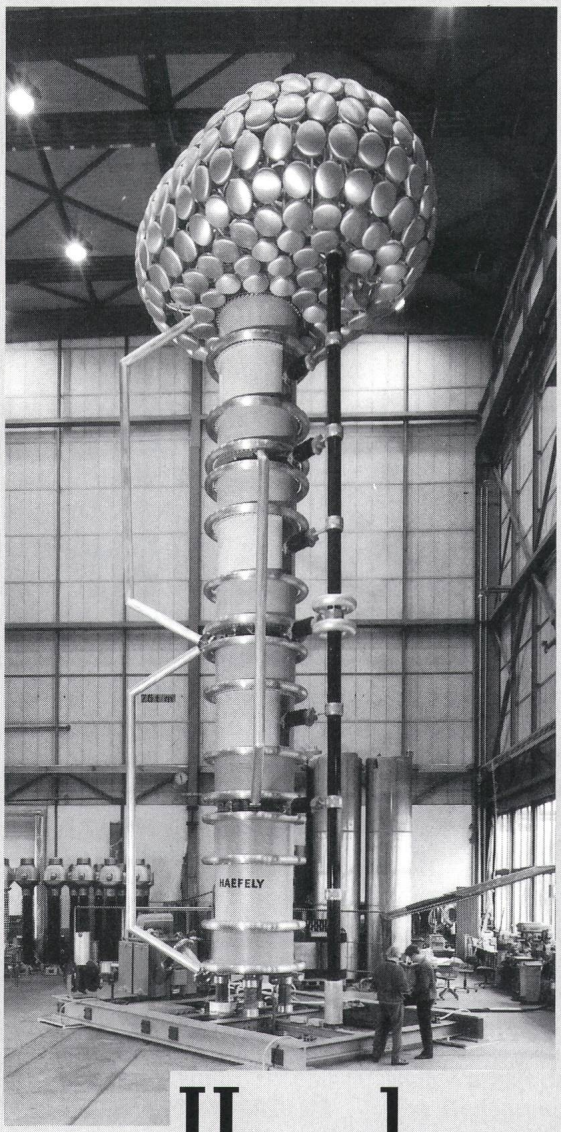
Dann heisst Ihre Lösung:
SERCOS (Sprecher Energie Control System) und

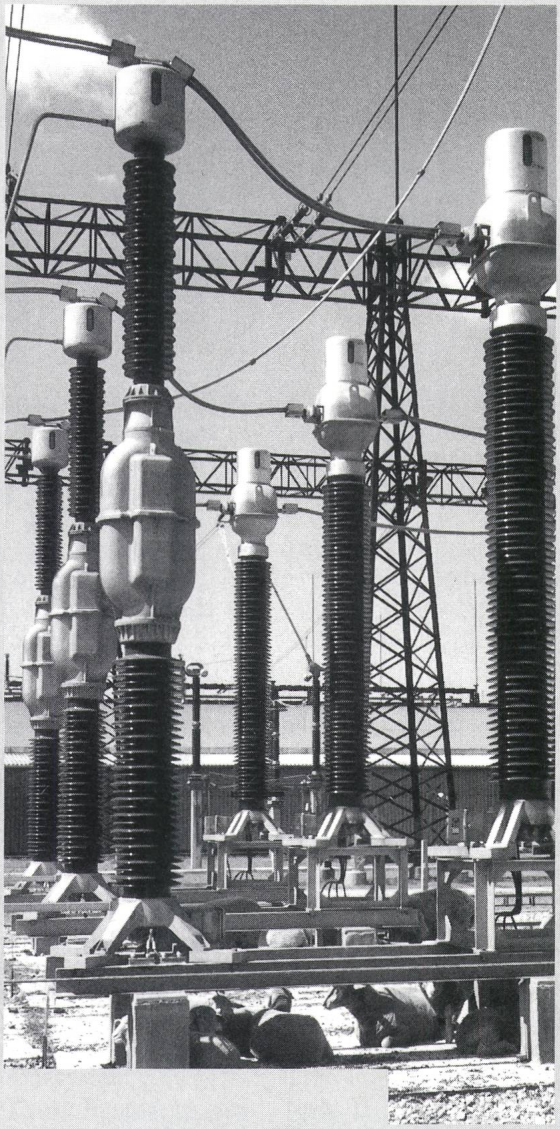
SPRECHER ENERGIE AG
Mittelspannungsanlagen
CH-5034 Suhr
Telefon: 064/33 77 33
Fax: 064/33 77 35

Alles aus einer Hand

SPRECHER ENERGIE

HAEFELY





Hochspannung

In zwei Bereichen der Hochspannungstechnik hat Haefely heute Kompetenz und weltweites Ansehen: Netzkomponenten und Prüfsysteme. Haefely-Netzkomponenten messen hohe und höchste Spannungen und Ströme in Hochspannungsnetzen der Elektrizitätsgesellschaften oder dienen der Informationsübertragung über Hochspannungs-Freileitungen (Messwandler 75-800 kV, TFH-Geräte, Reaktoren, Netzfilter, Durchführungen, Kondensatoren). Haefely-Prüfsysteme prüfen die elektrische Isolation von Hochspannungsapparaten und die elektromagnetische Verträglichkeit (EMV) von elektronischen Bauteilen, Geräten und Systemen.

Emil Haefely & Cie AG, Lehenmattstrasse 353, Postfach, CH-4028 Basel-Schweiz, Telefon +41.61. 31 55 111, Fax +41.61. 31 12 187
In Deutschland: Eichholzstrasse 65, Postfach 4301/ 44, 4600 Dortmund 41, Telefon 0231/ 40 24 95, Fax 0231/ 40 519

Besuchen Sie uns an der ineltec Basel Halle 102

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

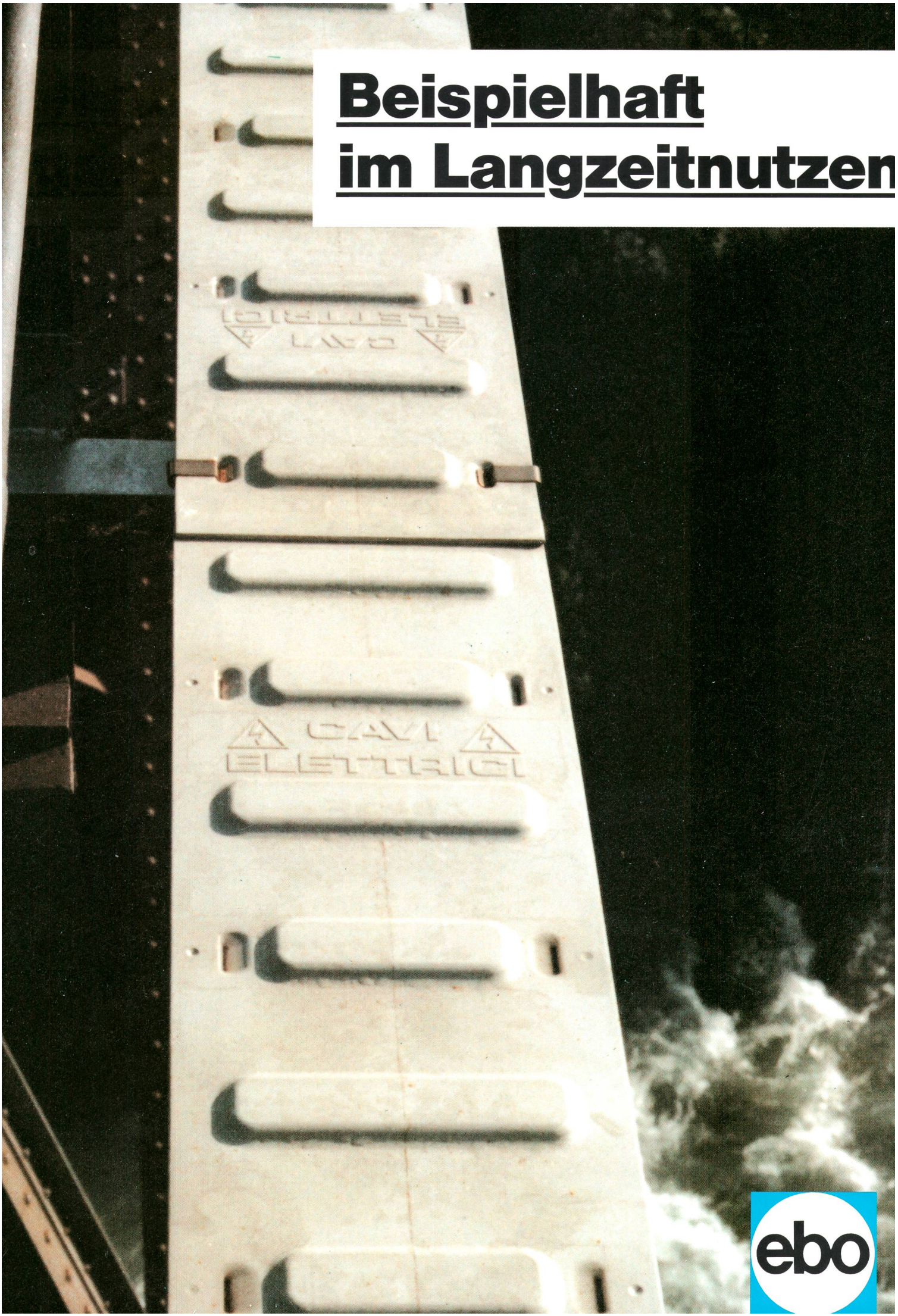
Wirksame Blitzschutzanlagen

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 817 431 – Telefax 01 / 55 14 26



Beispielhaft im Langzeitnutzen

ebo

GFK – für alle Fälle

Kabel- und Bodenkanäle aus glasfaserverstärktem Polyester-Kunststoff (GFK) bieten Sicherheit in Geschäfts- und Industriebauten, in Bahn- und Strassentunnels sowie in Freiluftanlagen. Das Material hat sich in Raumfahrt und anderen Hochtechnologiegebieten bewährt – und die daraus gefertigten Ebo-Kanäle sind international bekannt.

Keine Umgebung ist für Ebo-GFK-Kanäle zu extrem: Feucht- und Nassräume, Flughäfen, Strassen-, Bahn- und Kläranlagen, Chemie- und Lebensmittelbetriebe – aber auch Banken, Versicherungen, Sportstadien, öffentliche Gebäude, Parkgaragen usw.

Kabel- und Bodenkanäle widerstehen hohen mechanischen Belastungen. Verstärkungsrippen ergeben eine hohe Stabilität und einen geringen Gleitwiderstand beim Einziehen der Kabel.

Kabelkanäle mit besonderen Eigenschaften

Ebo-Kanäle korrodieren nicht. Sie sind beständig gegen Säuren, Laugen und die meisten Chemikalien. Das Material ist lebensmittelunbedenklich und ausserdem isolierend, schwerentflammbar, hitzebeständig, selbstverlöschend und halogenfrei. Im Brandfall bietet es den Kabeln einen längeren Schutz.

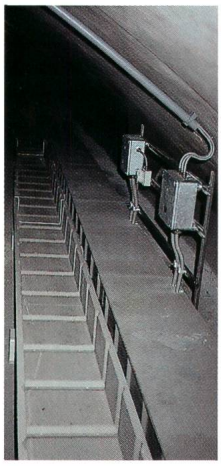
GFK unterliegt im Temperaturbereich von –80 bis +130 °C keinerlei Verformungen. Ein 8-mm-Zwischenraum in den Muffenverbindungen gleicht Längenänderungen aus. Die Kanäle sind dauerhaft beständig gegen intensive UV-Strahlung, Witterungseinflüsse, Abgase und Flugrost. Ebo-Kanäle sind alterungsbeständig weil sie nicht verspröden.

Auf Wunsch sind Stanzungen im Boden der Kabelkanäle erhältlich; sie dienen der Belüftung, lassen allfälliges Wasser abfliessen und nehmen die Ordnungs-Trennbolzen auf. Für eine schnelle, perfekte und wirtschaftliche Montage stehen Formteile für

Richtungsänderungen, Deckel, umfasser des Zubehör sowie ein patentiertes Befe gungssystem zur Verfügung.

Je nach Anwendung und Belastung wer Bodenkanäle mit Polyesterdeckel oder n Riffelblech abgedeckt. 12 Abmessungen mit einem grossen Zubehörsortiment, las keine Installationswünsche offen.

Das Preis-Leistungsverhältnis ist sehr attraktiv. Denn das geringe Gewicht der Kanäle, die schraubenlosen Verbindung durch das Muffensystem sowie die einfa Bearbeitung mit üblichen Handwerkzeug wie Stichsäge und Bohrer, verkürzen die Montagezeiten erheblich. Entgraten entfä



und es besteht weder für die Arbeitende noch für die Kabel eine Verletzungsgefal Der Langzeitnutzen ist der «Zusatzbonus

Der Vertrieb über den Elektro-Grosshand garantiert, dass Ebo-Produkte immer in Nähe zu finden sind.

Ebo AG
Zürichstrasse 103
CH-8134 Adliswil
Tel. 01/482 86 86
Fax 01/482 86 25