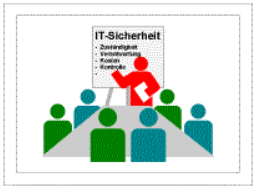


„Aktuelle IT-Bedrohungslage für die Wirtschaft

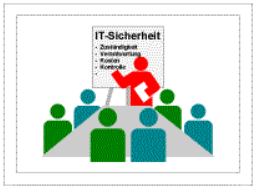
unter besonderer Berücksichtigung des BSI-IT-Grundschutzes und anderer standardisierter Methoden.

Rainmar Gnaehrich

Geschäftsführender Gesellschafter
der Fa. ObraSafe GmbH, St. Ingbert

Vorstandsmitglied (Landessprecher Saarland) der VSW
Vereinigung für die Sicherheit der Wirtschaft
Hessen, Rheinland Pfalz, Saarland

Vortragsgliederung



I. **Einleitung – Datenverlust und Datenmissbrauch.**

II. **Ausgangslage – IT-Sicherheit gerade für den Mittelstand (KMU).**

III. **Prävention - das IT-Sicherheitsniveau erhöhen, die Schadenrelevanz positiv verändern.**

IV. **BSI – Produkte und Tools – Was man weiß, was man wissen sollte! Anleitung und Unterstützung.**

V. **Microsoft - Sicherheitsinitiativen**

VI. **Nützliche Links und Literaturhinweise.**

VII. **10 Thesen zur IT – Sicherheit.**

VIII. **Erkenntnis für die erfolgreiche Informationsgesellschaft.**

IX. **Kontakt**

I. Einleitung – Datenverlust und Datenmissbrauch

Perspektive international.

Mit der Nutzung neuer Internet – Technologien steigen auch die Risiken. Die Statistik macht den dramatischen Anstieg der international gemeldeten Vorfälle deutlich.

Jahr	2000	2001	2002	2003
Vorfälle	21,756	52,658	82,094	137,529

Carnegie Mellon
Software Engineering Institute
CERT® Coordination Center

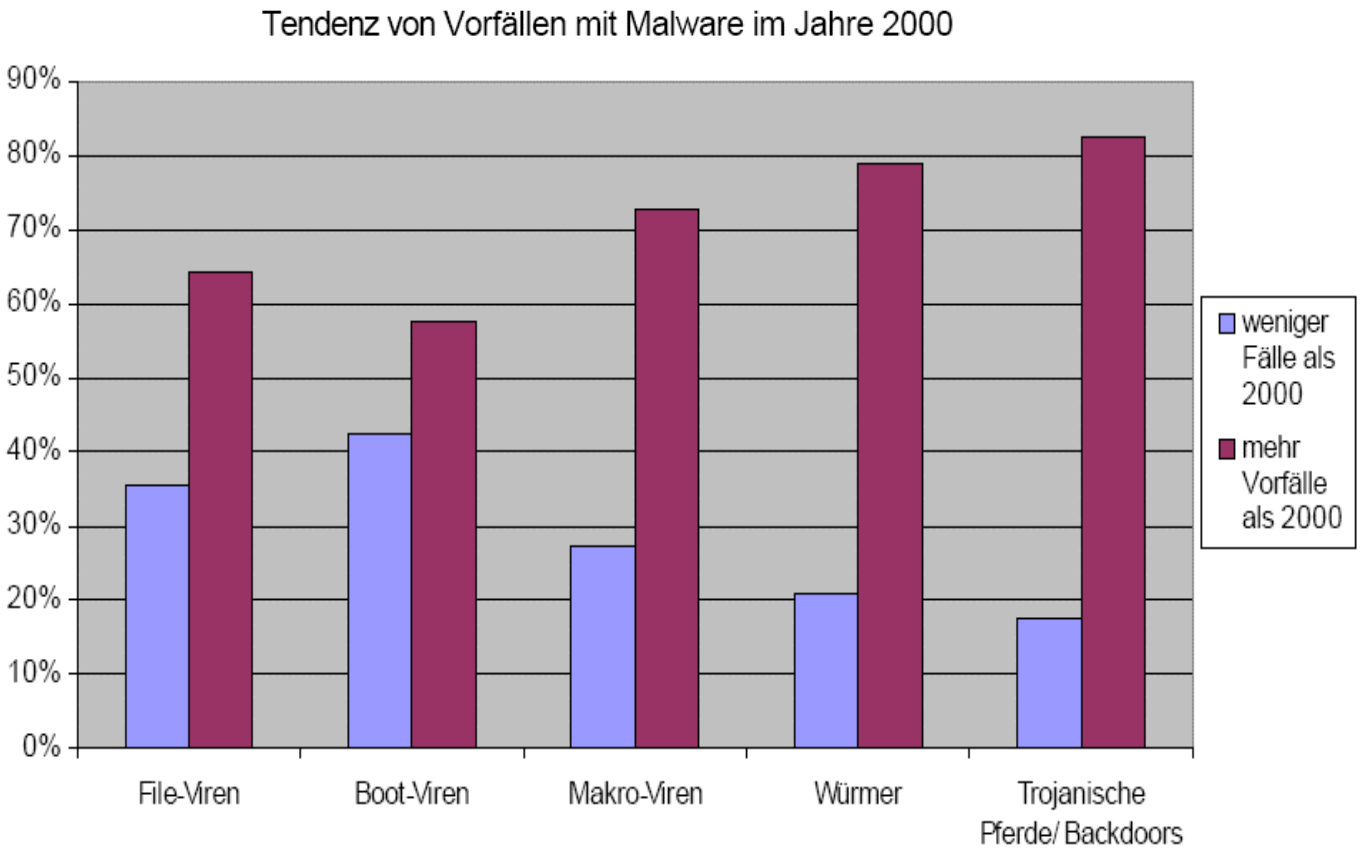
www.cert.org

Überlegungen zu
- Bedrohungen
- Schwachstellen
- Risiken und
- Verantwortlich-keiten.

Kompakte Sicherheits-konzepte zur Adaption an das eigene Umfeld.

I. Einleitung – Datenverlust und Datenmissbrauch

Aktuelle Risikosituation / KES Studie 2002



Chancen und Risiken neuer Technologien.

Das Internet als kritische Infrastruktur angesehen.

I. Einleitung – Datenverlust und Datenmissbrauch

Viren verursachen Milliardenschäden bei Mittelständlern.

Financial Times Deutschland berichtet am 24.03.04: Europäische Mittelständler verlieren jährlich 22 Milliarden Euro durch elektronische Schädlinge und unerwünschte E-Mail-Werbung. Jeder erfolgreich Angriff durch Viren schlägt im europäischen Durchschnitt mit etwa 5.000 Euro durch Arbeitsausfälle und Datenverluste zu Buche. Das ergab eine Umfrage des Antiviren-Software-Herstellers Network Associates.

Chancen und Risiken neuer Technologien.

Das Internet als kritische Infrastruktur angesehen.

I. Einleitung – Datenverlust und Datenmissbrauch

Bundeskriminalamt

Bundeslagebild
IuK-Kriminalität 2002

Stand 03.11.2003

Chancen und Risiken neuer Technologien.

Das Internet als kritische Infrastruktur angesehen.

BKA E-Mail: OA34@bka.bund.de

I. Einleitung – Datenverlust und Datenmissbrauch

COMPUTERWOCHE

Hacker greifen Supercomputer-Netze an
14.04.2004 um 15:31 Uhr

MÜNCHEN (COMPUTERWOCHE) - Mehrere US-amerikanische Forschungseinrichtungen, darunter die Stanford University, sind in den vergangenen Wochen von Hackern angegriffen geworden. Betroffen waren jeweils unter Linux oder Solaris betriebene Server in Hochgeschwindigkeitsnetzen, berichtet die zur Stanford University gehörende Organisation Information Technology Systems and Services. Mit Hilfe von gängigen Cracking-Tools hätten die Angreifer unter anderem Passwörter für den Netzzugang ausspioniert und seien in die internen Systeme eingedrungen. Dadurch seien etwa Server für die Entwicklung und Verteilung von Linux-Anwendungen beeinträchtigt worden. Details wollen die Sicherheitsexperten in Stanford derzeit nicht nennen. Die Vorfälle würden noch untersucht. (wh)

I. Einleitung – Datenverlust und Datenmissbrauch

- **Viele Menschen sind schlecht. Darum gibt es Viren, Würmer, jede Menge Spam und Wirtschaftsspionage. Es herrscht Krieg der Viren – Programmierer. Virus kontra Virus, der besonders perfiden Art. Ein Gros der Schutzsoftware tappt sogar im dunkeln. Lässt sich doch durch Verschlüsselungsmechanismen zuweilen kaum noch ein Muster erkennen. „NetSky“ – Internetwurm kontra „Beagles“ und „Mydooms“.**

- **Einige Experten glauben, dass der Bandenkrieg der Programmierer ein Ablenkungsmanöver für einen bevorstehenden Großangriff auf die weltweiten Netze sein könnte. Richard Clarke, amerikanischer Sicherheitsexperte und früherer Regierungsberater gehört dazu. Er befürchtet, dass wir vor einem gut koordinierten und groß angelegten Virenangriff mit weltweitem Schadenspotential stehen.**

- **Recherche und Analyse von Sicherheitsinformationen kosten meist viel Zeit – ein entscheidendes Problem für viele Unternehmen im Mittelstand.**

Die kritische Infrastruktur „Internet“.

Entlastung tut not – technisch, rechtlich, organisatorisch.

II. Ausgangslage –
IT-Sicherheit gerade für den Mittelstand (KMU)

Eine der wichtigsten Managementaufgaben im Unternehmen:

- **Schutz vor Angriffen und Störung von Geschäftsprozessen.**
- **Schutz des „verwundbaren Nervensystems“ bestehend aus einer Vernetzung von Rechnersystemen.**
- **Gewährleistung eines reibungslosen Geschäftsbetriebs durch ein „Nervensystem“, dass funktionsfähig, robust und sicher ist.**

Wir sind darauf angewiesen, dass Deutschland im „Electronic-Business“ ganz vorne in der Weltliga mitspielt.

PCs können sich nicht selbst verteidigen, sie brauchen Schutz.

IT-Sicherheit – ein wichtiges Instrument der Unternehmens-führung.

II. Ausgangslage –
IT-Sicherheit gerade für den Mittelstand (KMU)

Mittelstand vorbereitet?

Alltägliche Bedrohungsszenarien.

Oft keine eigenen IT-Experten.

Folge:

Auswirkungen werden in vielen Firmen

weder

„präventiv eingeschätzt“

noch

„einer systematischen Risikobewertung unterzogen“

Detaillierte Planung und Vorsorge, um notfalls Schadensauswirkungen zu minimieren,

„fehlen in der Regel“.

Begründete Sorglosigkeit.

II. Ausgangslage –
IT-Sicherheit gerade für den Mittelstand (KMU)

Mittelstand – gespalten.

Laut kürzlicher McAffee Security Studie teilt sich das Sicherheits-management europäischer Unternehmen in 2 Lager auf:

- **„Sofort agieren“**
- **„Abwarten und schauen“**

Gleichviel: Entlastung tut not.

Laut Ernst & Young – Umfrage unter 1.400 IT-Fachleuten hindern Zeit- und Kostengründe viele Unternehmen daran, sich um IT-Sicherheit zu kümmern.

II. Ausgangslage – Geschäftsleitung verantwortlich

„Abwarten und schauen“ ?

Äußerst problematisch durch neue persönliche Haftungsdimension im Bereich Risikovorsorge für:

- **Vorstände gem. §93, Abs. 2 Aktiengesetz.**
- **Geschäftsführer und Aufsichtsräte gem. §43 GmbH-Gesetz, §266 StGB.**

Weitere gesetzliche Vorgaben schreiben weitreichende Präventiv-maßnahmen vor:

- **Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), HGB, AktG.**
- **Richtlinien zur Kreditvergabe (Basel II).**
  Siehe auch www.bundesbank.de/bank/download/pdf/Overview_Deutsch.pdf

Achtung! Vorstehende Regeln gelten sowohl für Aktiengesellschaften als auch für GmbHs!

Gegen den Lauf der Dinge ankämpfen.

Übrigens: Wirtschaftsprüfer finden für Ihr Testat zur Sicherheitslage im Unternehmen unter www.idw.de

ihre Sicherheits-checkliste.

II. Ausgangslage –
IT-Sicherheit ist Chefsache in erster Linie

Und weiter zur Problematik „Abwarten und schauen“ :

- **Unterlassung kaum versicherbar.**
- **Delegation der Verantwortung nicht grundsätzlich an das IT – Management.**

Damit ist IT–Sicherheit – Chefsache und das abgewandelte St. Florians Gebet „Verschon‘ mein Haus, greif andere an“ gehört damit endgültig zur Business – Archäologie.

Unternehmenschefs ergreifen vielmehr pro aktiv Maßnahmen, bevor es zu Auswirkungen auf geschäftskritische Vorgänge kommt.

Zuwachs des Sehvermögens gefordert.

Das Ziel muss man früher kennen, als den Weg.

III. Prävention – das IT-Sicherheitsniveau erhöhen, die Schadenrelevanz positiv verändern.

Fachwissen, Warnhinweise und Informationsangebote:

Da bisher nicht ausreichend sichergestellt werden kann, dass die Informationstechnik das tut, was sie soll, und nichts tut, was sie nicht soll, kümmert sich das Bundesamt für Sicherheit in der Informationstechnik (BSI) als Bereichsbehörde des Bundesministerium des Innern mit mehr als 300 Mitarbeitern um Fragen der IT – Sicherheit.

BSI – Homepage: http://www.bsi.bund.de

IT Sicherheit setzt Wissen und Erfahrung voraus.

Die neutrale Fachbehörde: Hier ist gut sein.

III. Prävention – das IT-Sicherheitsniveau erhöhen, die Schadenrelevanz positiv verändern.

Bundesamt
für Sicherheit in der
Informationstechnik

Leitfaden IT-Sicherheit

IT-Grundschutz kompakt

http://www.bsi.bund.de/gshb/Leitfaden/index.htm

Ein kompakter Überblick über die wichtigsten organisatorischen, infrastrukturellen und technischen IT – Sicherheits-maßnahmen.

Der Leitfaden kann von den Internetseiten des BSI kostenlos heruntergeladen werden.

IV. BSI – Produkte und Tools
Was man weiß, was man wissen sollte!

Folgende Aufgaben und Dienstleistungen des BSI sollten Ihnen bekannt sein:

- **IT – Sicherheitshandbuch**
- **IT – Grundschutzhandbuch (Quasi Standard der IT Sicherheit)**
- **Schriften, Faltblätter zur IT – Sicherheit**
- **Leitfaden zur IT – Sicherheit (Der Überblick mit Checklisten)**
- **Web – Angebot des BSI (www.bsi.bund.de)**
- **Zertifizierung**
- **Kryptographische Grundlagenarbeit**
- **Beratung**
- **Virenhotline**
- **Viren – Newsletter**
- **Informationsdienst**
- **BSI – Kongress (alle zwei Jahre)**
- **Die Zeitschrift <Kes> in Zusammenarbeit mit dem Verlag SecuMedia als offizielles Organ des BSI.**

IT Sicherheit setzt Wissen und Erfahrung voraus.

V. Microsoft - Sicherheitsinitiativen

Microsoft-Sicherheitsinitiativen

1-tägiges kostenloses Training
für IT-Professionals

Kursagenda:

- **Grundlagen der IT-Sicherheit**
- **Sicherheit durch Patch-Management**
- **Server-Sicherheit**
- **Client-Sicherheit**

http://www.microsoft.com/germany/aktionen/securitytraining/itpro/

Achtung: In der Zeit von Mai bis Juli 2004 !

http://www.microsoft.com/technet/security/bulletin/notify.mspx

VI. Nützliche Links und Literaturhinweise

Task Force - Sicheres Internet
http://www.bsi.bund.de/taskforce/index.htm

Maßnahmenkatalog zum Schutz von verteilten Denial of Service-Angriffen im Internet
http://www.bsi.de/taskforce/ddos.htm

Maßnahmenkatalog zum Schutz vor Computer-Viren aus dem Internet
http://www.bsi.de/taskforce/viren.htm

ASW Arbeitsgemeinschaft für Sicherheit in der Wirtschaft
http://www.asw-online.de

VSW Vereinigung für die Sicherheit der Wirtschaft Hessen, Rheinland-Pfalz, Saarland
http://www.vsw-service.com

ObraSafe GmbH, Sicherheitssysteme
http://www.obrasafe.de

Gesellschaft für Datenschutz und Datensicherung e.V.
http://www.gdd.de

BITKOM Broschüre „Sicherheit für Systeme und Netze in Unternehmen“, 2. überarbeitete Auflage
http://www.bitkom.org

IT-Sicherheit im Überblick „Kompetenzzentrum für elektronischen Geschäftsverkehr (KEG) Saar“
http://www.keg-saar.de

Wer sich selbst kennt, kann sehr bald andere kennen lernen.

VII. 10 Thesen zum Schutz Unternehmenskritischer Infrastrukturen laut BSI

1. **Der Schutz Unternehmenskritischer Infrastrukturen ist wegen der weitreichenden Konsequenzen Managementaufgabe.**
2. **Herstellung und Verbesserung der Sicherheit erfordern systematisches Vorgehen.**
3. **Zusammenhänge und Abhängigkeiten sind zu erkennen und zu berücksichtigen.**
4. **Abhängigkeiten sind zu reduzieren; unabhängige, autarke Arbeitsmodule sind anzustreben.**
5. **Redundanzen für identifizierte kritische Systeme sind einzuplanen.**
6. **Notfallpläne und Krisenkonzepte sind zu erarbeiten und zu proben.**
7. **Der Faktor Mensch ist zu berücksichtigen (Bequemlichkeit, Gewohnheiten, Vorlieben).**
8. **Der Innentäter ist noch immer als größtes Risiko zu beachten.**
9. **Sicherheit kann nur durch Kombination aus IT-Sicherheit und materieller Sicherheit erreicht werden.**
10. **Maßnahmen zum Schutz Unternehmenskritischer Infrastrukturen erfordern die Bereitstellung von entsprechenden Ressourcen (Geld, Personal, Zeit) und auch die Durchsetzung und Kontrolle durch das Management.**

Mit der Zeit vollbringen.

VII. 10 Thesen zur IT-Sicherheit aus der Praxis

Mitarbeiter bei BMW in Dingolfing haben ihre Erfahrungen beim Aufbau der IT – Sicherheit in zehn kurzen Thesen zusammengefasst:

- **IT – Sicherheit ist machbar**
- **IT – Sicherheit ist bezahlbar**
- **IT – Sicherheit verlangt Transparenz von Risiken**
- **IT – Sicherheit geht alle an**
- **IT – Sicherheit muss integriert sein**
- **IT – Sicherheit ist ein permanenter Prozess**
- **IT – Sicherheit umfasst viele Disziplinen**
- **IT – Sicherheit ist vielschichtig**
- **IT – Sicherheit ist eine Dienstleistung**
- **IT – Sicherheit erfordert Professionalität**

VIII. Erkenntnis
für die erfolgreiche Informationsgesellschaft

„Zu wissen, wie man etwas macht, ist nicht schwer. Schwer ist nur, es zu machen.“
(Chinesisches Sprichwort)

IX. Kontakt - Gebäudesicherheit

SICHERHEITSSYSTEME

Die angemessene Absicherung von Räumen, Gebäuden, Informations- und technischer Infrastruktur – vorbeugend und abwehrend.

ObraSafe GmbH
Rainmar Gnaehrich
Annastr. 38
66386 St. Ingbert
Tel.: 06894 / 6013
Fax: 06894 / 80834
E-Mail: info@obrasafe.de
Internet: www.obrasafe.de

Full-Service: Integrierte Beratungs-leistung und Projekt-realisierung aus einer Hand.

IX. Kontakt - VSW

Weitere Information über die VSW Vereinigung für die Sicherheit der Wirtschaft Hessen, Rheinland Pfalz, Saarland erhalten Sie unter

www.vsw-service.com

Sowie bei

VSW Landessprecher Saarland
Rainmar Gnaehrich
Postfach 1745
66367 St. Ingbert

Telefon: 06894 / 6013
Fax: 06894 / 808 34

E-Mail: info@obrasafe.de

Netzwerk mit Nutzwert – gemeinnützig, unabhängig, neutral.