Pressemitteilung 18. September 2003

IT-Sicherheit: Höchste Management-Verantwortung tut not

MÜNCHNER KREIS diskutiert Möglichkeiten wirksamer Schutzmaßnahmen

Eine hundertprozentige Abdeckung sämtlicher Sicherheitsrisiken bei elektronischen Informationssystemen kann nicht das Ziel sein, aber man kann dafür sorgen, dass ihre vitalsten Elemente weitgehend geschützt werden. Das ist ein Fazit aus der Fachkonferenz mit dem Thema

„Sicherheit und Schutz in der Informationsgesellschaft“

die der MÜNCHNER KREIS am 18. September 2003 in München veranstaltete. Als provozierenden Untertitel wählten die Veranstalter zwei Fragen: „Leisten wir uns die Sicherheit, die wir brauchen, und brauchen wir die Sicherheit, die wir uns leisten?“.

Der Konferenzverlauf zeigte, dass die erste Frage in vielen Fällen mit „Nein“ beantwortet werden muss und die Antwort auf die zweite Frage kein uneingeschränktes „Ja“ ergeben kann. Für die Sicherheit unserer Informationssysteme muß durchweg mehr getan werden. Die zunehmende interne und externe Vernetzung der Systeme sowie das Streben nach einer IT-basierten Optimierung der Geschäftsprozesse macht Infrastrukturen und Abläufe extrem verwundbar, wie es Prof. Dr. Heinz Thielmann (Fraunhofer Institut SIT Darmstadt, mitverantwortlich für die Tagungsleitung) ausdrückte. Die Bedrohungen und tatsächlichen Angriffe verschiedener Art haben zugenommen. Berichte über Viren und Würmer, die weltweit ganze Systeme lahmlegen und Dateien vernichten, liefern Schlagzeilen in den Medien, ebenso verunsichern die Meldungen über Hacker und Saboteure, die in sensible Computersysteme eindringen, die Öffentlichkeit. Hinzu kommen Nachrichten über elektronische Spionage durch Wettbewerber oder auch Nachrichtendienste fremder Länder.

Von diesen Bedrohungen sind nicht nur große Unternehmen betroffen. Die rund 3,5 Millionen kleineren und mittleren Unternehmen (KMU) sind davon keineswegs ausgenommen. IT-Sicherheit ist auch hier, wie Antonius Sommer (TÜV-IT) hervorhob, für den

Bestand und Erhalt dieser größten Unternehmensgruppe unverzichtbar. Die volkswirtschaftliche Bedeutung stabiler KMUs im Bereich der Industrie wird deutlich, wenn man bedenkt, dass sie ein gutes Viertel sämtlicher gewerblichen Arbeitnehmer beschäftigen und zu einem Drittel an der gesamten Bruttowertschöpfung beteiligt sind.

Welche finanziellen Schäden in jüngster Zeit durch Angriffe auf IT-Systeme entstanden sind, beleuchten einige Erhebungen aus den USA: So veranschlagt die kalifornische Marktforschungsfirma Computer Economics Inc., Carlsbad, für das Jahr 2002 die weltweiten Virusschäden auf 11,1 Mrd. $, was dem Zwanzigfachen gegenüber 1995 entsprechen soll. Für 2003 werden sogar bis zu 13 Mrd. $ erwartet. Auf Grund einer regelmäßigen Umfrage bei US-Firmen für die „CSI/FBI Computer Crime and Security Survey“ meldeten 251 Unternehmen für die Ausgabe 2003 eine Summe von insgesamt 201,8 Mio. $ für Schäden, die durch Angriffe verschiedener Art an ihren IT-Systemen entstanden waren.

Um solche Schäden zu vermeiden, sehen sich Unternehmen wie auch Institutionen der öffentlichen Verwaltung vielfältigen Aufgaben gegenüber. Das beginnt bei der Bewusstmachung des Gefahrenumfelds. Defizite weist hier vor allem das Topmanagement auf. Die jüngste Umfrage der internationalen Wirtschaftsprüfungs- und Beratungsfirma Ernst & Young („Global Information Security Survey“) bei Unternehmen aus 66 Ländern, davon 656 aus Europa, ergab, dass mehr als die Hälfte der Geschäftsleitungen den Stand der IT-Sicherheit in ihren Unternehmen nicht kennt. In 52 % aller befragten Firmen wird die Unternehmensspitze maximal einmal jährlich, zum Teil sogar nie, über das Thema IT-Sicherheit informiert.

Das ist umso beachtenswerter als in Deutschland Vorstände, Gechäftsführer und Aufsichtsräte für Sicherheitsmängel rechtlich durchaus zur Verantwortung gezogen werden können. Eine vielfältige Beschreibung der Haftungsbreite und ihrer Konsequenzen lieferte Rolf von Rössing (Ernst & Young). Nach seinen Beobachtungen werden IT-Risiken in den Führungsetagen oft sachlich überhaupt nicht verstanden. Die deutsche Rechtsprechung zur Haftung für Sicherheitsmängel, so von Rössing, ist gegenwärtig noch sehr unterschiedlich ausgeprägt und schafft durch mangelnde Vorhersagbarkeit zusätzliche Unsicherheiten. Führungskräfte sollten sich jedoch darüber im Klaren sein, dass Information das Kernstück unternehmerischer Tätigkeit ist und die Sicherheit der Infor-

mation auf der infrastrukturellen Ebene beginnt und bei der personellen Sicherheit endet.

IT-Manager klagen häufig über Budgetbeschränkungen (in der Ernst & Young Studie klagen hierüber 56 Prozent aller Unternehmen), die sie daran hindern, die notwendigen Sicherheitsmaßnahmen zu ergreifen. Sie verweisen auf die Schwierigkeiten, die Rentabilität ihrer Investitionen (Return-on-Investment - ROI) nachzuweisen. Wege dazu zeigte auf der Konferenz Prof. Dr. Jörg Sauerbrey (Siemens) auf: Speziell entwickelte ROSI-Kalkulatoren (Return-on-Security-Investment) ermöglichen Aussagen zum Amortisierungszeitpunkt einer Investition.

In den Griff bekommen lassen sich die Sicherheitsprobleme eines Unternehmens nur durch eine umfassende Sicherheitspolitik, deren Kern ein Sicherheits-Rahmenkonzept („Security Framework“) bildet. Das beginnt mit einem unternehmensweiten Prozess des Bewusstmachens, der alle Ebenen einschließt. In großen Unternehmen, so Prof. Thielmann, sind bereits entsprechende Kampagnen („Security Awareness“) angelaufen. Seine Forderung: In jedem Unternehmen muss ein „Total Security Management“ (TSM) eingerichtet werden. - Oftmals wird in der Öffentlichkeit übersehen, dass ein sehr großer Teil der Sicherheitsverletzungen von „Innentätern“, d.h. illoyalen (oder auch ehemaligen) Mitarbeitern begangen wird. Dieser Prozentsatz wird nach Angaben von Thielmann, der sich dabei auf zahlreiche Studien beruft, auf bis zu 70 – 80 % geschätzt.

Am Anfang jeder konkreten Umsetzung muss die Risikoanalyse stehen, über der nach Ansicht von Markus Pfyffer (IBM) die Frage stehen sollte „Wieviel Risiko kann und will ich tragen?“. Die Gesamtpalette der Risiken ist zu erfassen und zu bewerten. Dem hat sich die Schwachstellenanalyse anzuschließen. Sodann sind Prioritäten zu setzen, d.h. man konzentriert sich auf das Notwendige und das Realistische. Auf diesem Wege gelangt man zu den Grundlagen eines unternehmensweiten Sicherheitskonzepts.

In einem Fallbeispiel führte Pfyffer auch einen Katalog häufiger Verstöße gegen Sicherheitsprinzipien auf. Dabei nannte er u.a.:

- Keine Möglichkeit zur Erkennung von Angriffen auf Netzwerk und Systeme
- Aufzeichnungen von Firewalls werden nicht regelmäßig ausgewertet
- Das Problembewusstsein der IT-Mitarbeiter ist uneinheitlich ausgebildet

- Dienste und Betriebssysteme sind nicht mit den neuesten Ergänzungen (Patches, Hotfixes) versehen.
- Unsicherer Betrieb von drahtlosen LAN-Lösungen (Wireless-LAN)
- Auf allen Anwendungsservern wird ein gleiches Herkunfts-Passwort („root password“) verwendet.

Die Beschreibung der Risikofelder und Gefährdungsszenarien nahm auf der Fachkonferenz beträchtlichen Raum ein (s. auch Kasten im Anhang). Eine spektakuläre Präsentation zum Hackerproblem lieferte Sebastian Schreiber (SySS GmbH) in der Funktion als „Live-Hacker“. Ihm ging es darum zu demonstrieren, wie Hacker vorgehen und welche Möglichkeiten sie haben, in fremde IT-Systeme einzudringen. Zu seinen Thesen gehören Aussagen wie „Die Risiken des Internets werden völlig unterschätzt“ und „Heute kann selbst ein Laie in IT-Netze eindringen“. Sein Blick in die Zukunft wird vom Hase-Igel-Effekt überschattet: „Und hat man sein Betriebssystem endlich so gut im Griff, dass man glaubt, sicher zu sein - dann wird es wohl in den nächsten Tagen obsolet und durch ein neues ersetzt.“

Auf IT-Infrastrukturprobleme, die aus der Liberalisierung der Strommärkte erwuchsen, wies Reinhard W. Hutter (IABG) hin. Da der börsennotierte Stromhandel nur funktioniert, wenn der Strom des Anbieters durch die Netze anderer Anbieter geleitet werden kann, ist dazu eine IT-Steuerung der Stromnetze erforderlich. Die Energieversorgung ist dadurch von der Funktionssicherheit der IT-Systeme abhängig. Hutter hält die Gefährdungen, die aus diesem Verbundsystem erwachsen, für sehr hoch: Reguläre Ausfälle im Normalbetrieb können unter ungünstigen Umständen kaskadenartig weitere Systeme in Mitleidenschaft ziehen - von gezielten Angriffen an irgendeinem Ort des Verbundsystems ganz abgesehen. Seine Folgerung: Der Schutz auch solcher Infrastrukturen muß eine lebenswichtige Aufgabe staatlicher Vorsorge- und Ordnungspolitik sein.

Dass bei allem berechtigten Sicherheitsstreben der Schutz des Individuums nicht auf der Strecke bleiben darf, darauf verwies Frau Prof. Dr. Marie-Theres Tinnefeld (FH München). Die Eingriffsbefugnisse und Vorratssammlungen von Informationen durch öffentliche, besonders aber auch durch private Stellen beeinträchtigen nach ihrer Ansicht nicht nur die individuellen und kommunikativen Entfaltungsmöglichkeiten, sondern gefährden auch die wirtschaftliche Entfaltung, weil sie Ansatzpunkte für eine erfolgrei-

che Wirtschaftsspionage liefern. Die Referentin fordert ein an Grundrechten und der Verhältnismäßigkeit orientiertes Konzept, in dessen Rahmen Wirkungen und Nebenwirkungen von Sicherheitsmaßnahmen ständig überprüft werden.

An Hand einiger Fallbeispiele wurde den Konferenzteilnehmern gezeigt, dass es durchaus sichtbare Erfolge in der praktischen Umsetzung von Sicherheitskonzepten gibt: Nach Auffassung von Marcus Belke (2^B Advice GmbH) ist sichere Kommunikation immer dann möglich, wenn die Prinzipien von Integrität, Authentizität und Geheimhaltung eingehalten werden. Die Integrität und die Authentizität lassen sich durch elektronische Signaturen sichern. Geheimhaltung erreicht man durch Verschlüsselungsverfahren. So wurde z.B. in den 217 deutschen Botschaften, Vertretungen und Repräsentanzen das von Secunet und dem BSI (Bundesamt für Sicherheit in der Informationstechnik) gemeinsam entwickelte System SINA installiert, das lt. Belke zu den erfolgreichsten Projekten der Kommunikationsabsicherung zählt. Das System nutzt zwar das öffentliche Internet, schützt aber die Kommunikation mit dem Auswärtigen Amt vor jedwedem Lauschangriff.

Wie man Datensicherheit im stark gefährdeten Wireless-LAN (WLAN) erreichen kann, schilderte Thomas Koelzer (Secartis AG). Das chipkartenbasierte EAP-SIM-Verfahren (Enhanced Authentication Protocol + SIM-Karte) ist ein neues Authentifizierungsverfahren. Es ermöglicht beim Gebrauch von Handys sowohl die eindeutige Identifizierung des Nutzers als auch eine sichere und einfache Abrechnung der Nutzungszeit.

Welche Maßnahmen auf dem virtuellen Marktplatz eBay ergriffen wurden, um einen sicheren Handelsablauf zu gewährleisten, berichtete Geschäftsführer Jörg Rheinboldt (eBay GmbH). Neben der technischen Systemsicherheit entwickelte eBay ein Bündel von Verfahren, die den Nutzern Sicherheit im Umgang mit den Marktpartnern vermitteln sollen. Dazu gehören die Verifizierung der Anmeldeinformationen, das Bewertungsforum, in dem sich Käufer und Verkäufer nach erfolgter Transaktion gegenseitig bewerten, und sog. Treuhanddienste zur sicheren Abwicklung des Kaufvertrages. Entscheidend, so Rheinboldt, ist allerdings die eigenverantwortliche Mitwirkung der Marktteilnehmer.

Das kommende breitbandige Internet 2.0, das durch Medienkonvergenz, Interaktivität und durch neue Technologien eine Fülle neuer Angebote erwarten läßt, stellt die Diensteanbieter vor neue Herausforderungen in puncto Sicherheit. Andreas Kindt (T-Online) sieht sein Unternehmen dabei im Spannungsfeld zwischen dem Streben nach Sicherheit und Benutzerfreundlichkeit. Dabei gilt es, mit Hilfe des modernen Sicherheits-Instrumentariums (Authentifizierungs-/Autorisierungsverfahren, Verschlüsselungen, Digital Rights Management, Antivirussysteme, Firewalls etc.) verschiedene Aspekte zu berücksichtigen: Einerseits die Sicherheitsbelange der Endkunden, andererseits die Interessen der Anbieter von Inhalten (Content = Videos, Musik, Spiele) sowie von Partnern im elektronischen Geschäftsverkehr (z.B. Electronic Banking).

Für Tagungsleiter Prof. Dr.-Ing. Jörg Eberspächer (TU München; Vorstandsmitglied des MÜNCHNER KREISES) sind diese Beispiele ein hoffnungsvolles Indiz, dass IT-Sicherheit nicht nur machbar, sondern auch bezahlbar ist. Voraussetzung sei allerdings, dass der Problemkreis umfassend und professionell angepackt wird, und zwar im Bewusstsein, dass Sicherheit ein permanenter Prozess ist, der höchste Verantwortung seitens des Managements verlangt.

*

Der MÜNCHNER KREIS ist eine seit 1974 bestehende gemeinnützige, übernationale Vereinigung für Kommunikationsforschung, die es sich zum Ziel gesetzt hat, neue Entwicklungen in der Kommunikationstechnik transparent zu machen. Er fördert die Entwicklung, Erprobung und Einführung neuer Kommunikationssysteme durch sachliche Untersuchung und kritische Diskussion. Dazu veranstaltet er Mitgliederkonferenzen, Fachkonferenzen und Kongresse. Die Arbeitsergebnisse werden publiziert.
Die Arbeit des MÜNCHNER KREISES ist nicht fachlich spezialisiert, sondern interdisziplinär. Im MÜNCHNER KREIS wirken Personen und Institutionen der Wirtschaft, der Medien, der Politik und der Wissenschaft zusammen.

Anhang

Die Hauptrisiken der IT-Sicherheit

- Externe Gefährdungen
  - Krimineller Art: Viren/Würmer, Hacker, Terroranschläge, Spionage
  - Organisatorischer Art: Unternehmensübergreifende Systeme, Fusionen, Entflechtungen
- Interne Gefährdungen
  - Mangelhafte Technikwartung
  - Organisationsmängel (personell, Kompetenzabgrenzungen, Inkonsistenz von Unternehmensprozessen und IT-Prozessen)
  - Illoyale Mitarbeiter
  - Unwissende Mitarbeiter

Sicherheitsrisiken im Internet

Eine Auswahl von Charts aus dem Vortrag

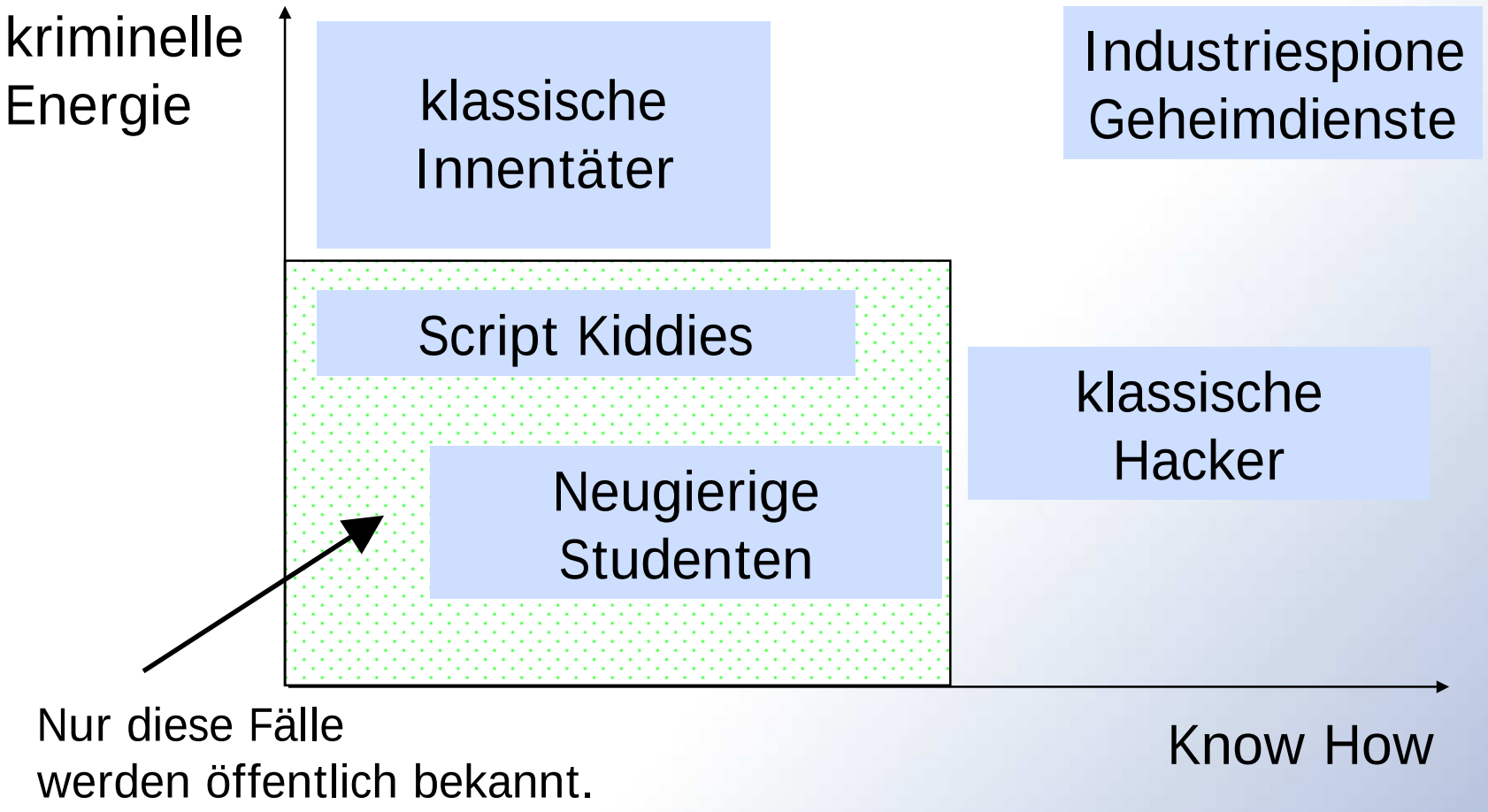
„Live Hacking: So brechen Hacker in Ihre Netze ein“

von Sebastian Schreiber, SySS GmbH

Drei Thesen zur Internetsicherheit

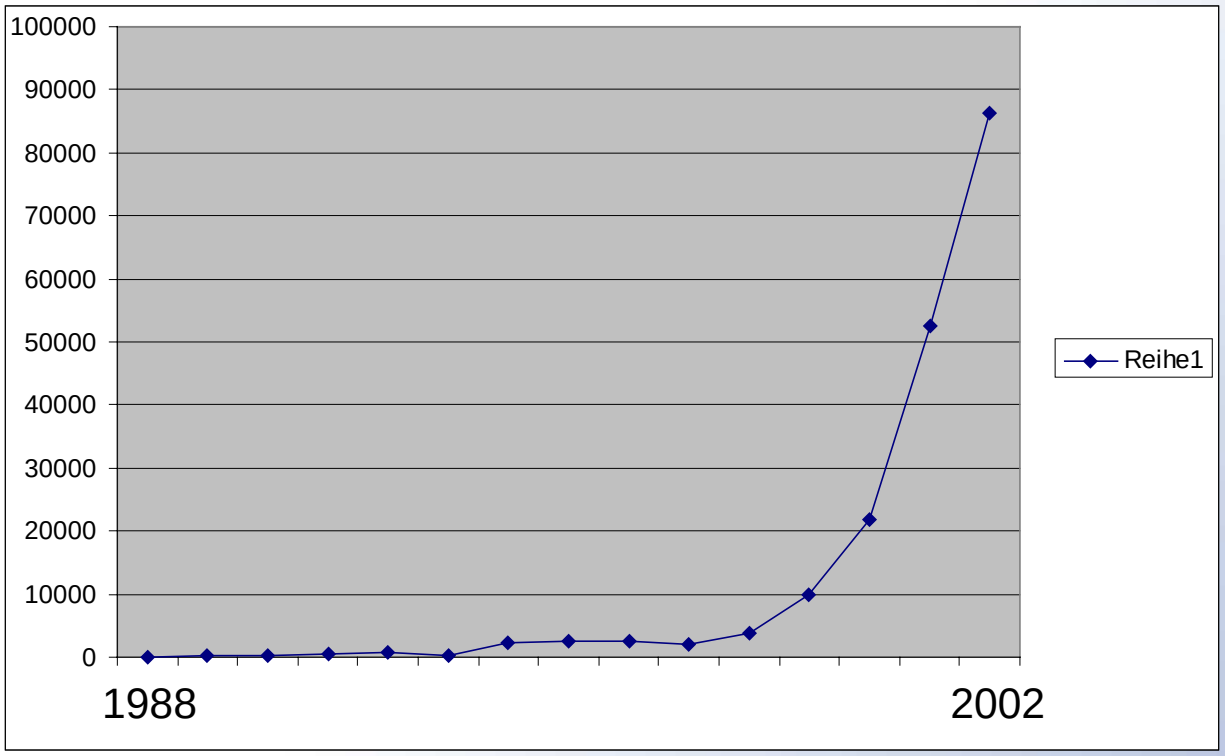
- Hackertools liegen zum Download bereit: Heute kann selbst ein Laie in IT-Netze eindringen.
- Nur die Attacken von Kindern und Vandalen werden überhaupt entdeckt.
- Die Risiken des Internets werden völlig unterschätzt; die Netze sind weitgehend ungeschützt. Dies wird sich in Zukunft nicht ändern!

Täterprofile



Incident Statistik von Cert.org

Jahr	Incidents
1988	6
1989	132
1990	252
1991	406
1992	773
1993	134
1994	2340
1995	2412
1996	2573
1997	2134
1998	3734
1999	9859
2000	21756
2001	52658
2002	86272



... Folgerung aus der Polizeistatistik ...

Frage: Wie hoch ist die Dunkelziffer?

- In der Regel zeigen Unternehmen Straftaten nicht an.

- In der Regel entdecken Unternehmen gar nicht, dass sie Opfer von Hackerattacken werden.

Kriminalstatistik	2000	2001	Steigerungsrate 2000/2001
Sabotage	268	920	343%
Ausspähung	538	1463	272%
Computerbetrug	17310	59670	345%
Prozentsatz der Ausspähungen, die vom Opfer entdeckt werden	3,00%	4,00%	
Prozentsatz der entdeckten Fälle, die zur Anzeige gebracht werden.	10,00%	8,00%	
Hochrechung: Reale Fälle pro Jahr	**179333**	**457188**	

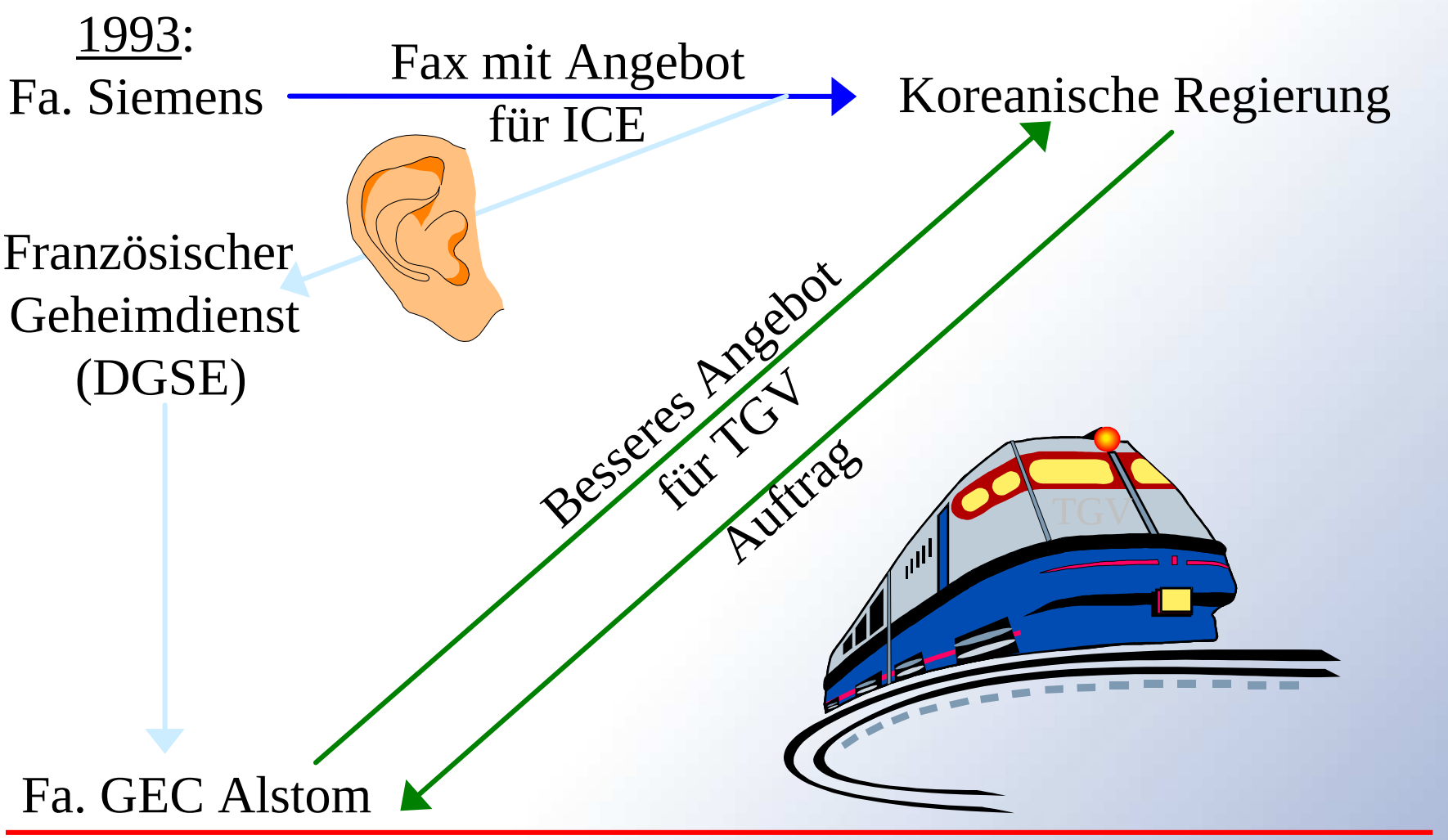
Rechtliche Hintergründe

- §202A StGB (Ausspähung von Daten)

  "...die gegen unberechtigten Zugang besonders gesichert sind,..."

- Schlussfolgerung:
  - Lediglich Datendiebstahl/Sabotage ist verboten - reine Einbrüche nicht.
  - Ausspähung von *ungesicherten* Daten ist nicht strafbar.
- Konkrete Gesetzeslücken:
  - Netbios-Ausspähungen
  - Lotus-Domino-Angriffe
  - WLAN-Angriffe („War-Driving")

Fallbeispiel: Computerspionage



Wird das Internet in Zukunft sicherer?

„Ja!“	„Nein!“
Sicherungssoftware wird immer besser;	… aber die Hackertools auch.
Budget für Security in Firmen steigt	… langsamer als die Anzahl und Komplexität der Systeme.
IT-Security findet Beachtung	… insbesondere bei jugendlichen Hackern.
Neue Sicherheitsstandards	… setzen sich nicht durch.