
Informationssicherheit

Was ist Informationssicherheit?

Bruce Schneier

in Secrets & Lies

Digitale Sicherheit umfasst Computer

- komplex
- instabil
- fehlerbehaftet



Mathematik ist perfekt

- Realität ist subjektiv

Mathematik ist definiert

- Computer sind störrisch

Mathematik ist logisch

Menschen sind

- unberechenbar
- launenhaft
- schwer zu durchschauen

Was ist Sicherheit?



Was ist Sicherheit?

Sicherheit

lat. Sēcūrītās, sēcūrus „sorglos“, sēd „ohne“ und cūra „(Für-)Sorge“

Zustand

- frei von unvertretbaren Risiken der Beeinträchtigung
- gefahrenfrei

bezogen auf

- Menschen
- Objekte und Systeme
- Wertvorstellungen

Sicherheit ist ein Grundbedürfnis des Menschen

- Sicherheitsbedarf steigt
 - Globalisierung
 - Mobilität
 - Abhängigkeit von Technik



Was ist Sicherheit?

Relative Sicherheit

Relativer Zustand der Gefahrenfreiheit

- bestimmter Zeitraum
- bestimmte Umgebung
- bestimmte Bedingungen

Sicherheitsvorkehrungen können zu Fall gebracht werden

- Ereignisse, die sich nicht beeinflussen oder voraussehen lassen

Beeinträchtigungen können nicht ausgeschlossen werden

- nur hinreichend unwahrscheinlich gemacht werden



Modell: Kraftfahrzeugwesen

- trotz
 - zahlreicher Vorschriften
 - regelmäßiger Überprüfungen
- Führen von Kraftfahrzeugen erzeugt regelmäßig gefährliche Zustände
 - absichtlich
 - böswillig
 - unabsichtlich
 - fahrlässig

Was ist Sicherheit?

Komplexe Systemen

In komplexen Systemen ist es unmöglich, Risiken völlig auszuschließen

„Vertretbares Risiko“

- hängt von vielen Faktoren ab
- wird subjektiv und kulturell verschieden bewertet

Wahrscheinlichkeiten

- höhere Wahrscheinlichkeiten für Beeinträchtigungen mit steigendem Nutzen werden als vertretbar angesehen
- Aktien-Spekulation, Teilnahme am Straßenverkehr, ...

Sicherheitskonzepte

- Definierter Zustand von Sicherheit
- Definition von Maßnahmen

Erfolgreiche Sicherheitsmaßnahmen

- können Beeinträchtigungen (erwartete und unerwartete) abwehren oder hinreichend unwahrscheinlich machen

Was ist Sicherheit?

Begriffspräzisierung

Security and Safety

- Im Deutschen nicht unterschieden
- werden unter „Sicherheit“ zusammengefasst

Security

- Sicherheit eines Systems
- Angriffssicherheit
- Schutz des Objektes vor der Umgebung, Immunität

Safety

- Betriebssicherheit
- Schutz der Umgebung vor einem Objekt, Isolation
- Zuverlässigkeit eines Systems



Sicherheitskonzepte spezifizieren diese Anforderungen

Es ist z.B. unzureichend, an einer Fluchttür lediglich „Sicherheit“ zu fordern

- Safety-Anforderung
 - Gewährleistung eines gefahrlosen Flucht- und Rettungsweges
- Security-Anforderung
 - Vermeidung einer unberechtigten Nutzung der Tür im Normalbetrieb

Was ist Sicherheit?

Sicherheit und Freiheit

Größtmögliche Sicherheit

- große Zahl von Vorschriften und Einschränkungen
- die „aus Sicherheitsgründen“ erlassen werden

Individuelle Freiheit

Kritiker warnen

- in als unsicher empfundenen Zeiten
- steigt Bereitschaft, stärkere Überwachung hinzunehmen
- führt zur Schwächung von Bürger- und Grundrechten

Sicherheitsgründe

- vorgeschoben oder unverhältnismäßig
- Argumente für eine Beschränkung der Grundrechte
 - Moral, Sexualität, Jugendschutz, Kriminalität, und Terrorismus

Motiv einschränkender Vorschriften

- weniger im Schutz des Einzelnen
- sondern Staat oder Institutionen von Schadensersatzansprüchen freizuhalten



Was ist Sicherheit?

Technische und zwischenmenschliche Sicherheiten

Technische und zwischenmenschliche Sicherheiten

Vertrauen in Mechanismen

- Vertrauen in Gleichgültig- und Interesselosigkeit
 - Geldautomat behandelt alle Benutzer gleich, hat kein Interesse an ihnen

Vertrauen in Menschen

- dagegen in dem Glauben, individuell und loyal behandelt zu werden

Widerspruch führt in allen soziotechnischen Systemen zu Paradoxien

- soziale Sicherheit hat sich von einer vorwiegend zwischenmenschlichen zu einer mehrheitlich technischen gewandelt



Was ist Sicherheit?

Aspekte der Sicherheit

Individuelle Sicherheit

Sicherheit einer Person

- physisch
 - unmittelbare körperliche Unversehrtheit und Bedrohungsfreiheit
- wirtschaftlich
 - dauerhafte Gewährleistung der existentiellen Basis, welche die Zukunft der Person absichern

Sicherheit ist für Menschen

- Objektive Gefahren- oder Risikofreiheit
- Subjektive Empfindung der Geborgenheit
 - unabhängig davon, ob sie zutrifft
- Gefühl kann einzelne Personen oder ganze Bevölkerungsgruppen einnehmen

Was ist Sicherheit?

Aspekte der Sicherheit

Kollektive Sicherheit

- die Sicherheit einer Seite darf nicht zu Lasten einer anderen Seite gehen
- es werden gemeinsame Maßnahmen entwickelt
 - die die Sicherheit für beide Seiten verbessert (Multilaterale Sicherheit)
 - in dem sich beide Seiten verpflichten, ihre Konflikte friedlich zu lösen
 - einen unbeteiligten Dritten als Schiedsrichter einschalten

Begriff stammt aus der Außenpolitik

- kooperative Form der Konfliktlösung

Innere Sicherheit und Äußere Sicherheit

- Schutz, den eine Gemeinschaft aufbaut
- umfasst die Mitglieder, aber nicht Außenstehende

Rechtssicherheit

- Rahmenbedingungen, die der Gesetzgeber schafft
- Funktionieren eines des Rechtssystems garantieren

öffentliche Sicherheit

- Wahrung der Rechtsordnung
- Einrichtungen des Staates, der Rechtsgüter und der Grundrechte des Einzelnen

Was ist Sicherheit?

Wirtschaftliche Sicherheit

Materieller / finanziellen Mittel

- ist für die Existenz oder
- für geplanten Vorhaben
- im vorgesehenen Zeitraum gewährleistet

Dies kann sowohl

- das einzelne Individuum betreffen, als auch
- Kollektive (betriebswirtschaftliche Unternehmen oder ganze Staaten)

Versicherungen

- Absicherung unabweisbare Gefahren
- erhöht nicht objektiv die Sicherheit
 - aber das subjektive Sicherheitsgefühl
 - im Eintrittsfall eine Behebung oder Ausgleich des Schadens ermöglichen

Betriebswirtschaftliche Sicherheit

- technische, logistische und organisatorische Maßnahmen
- in Bezug auf Maschinen oder Anlagen im industriellen Bereich
- Ausfallsicherheit, Verlässlichkeit und Verfügbarkeit

Was ist Sicherheit?

Objektive vs. subjektive Sicherheit

Objektive Sicherheit

statistisch / wissenschaftlich nachweisbare Sicherheit

- beispielsweise in Bezug auf Unfalldaten

Subjektive Sicherheit

„gefühlte“ Sicherheit

- Insbesondere im ÖPNV gibt es hier Untersuchungen und Überlegungen die subjektive Sicherheit zu erhöhen
- „Lichtschutz-Faktor“

Was ist Sicherheit?

Technische Sicherheit, Betriebssicherheit

Technische Konstruktionen oder Objekte

Zustand der voraussichtlich störungsfreien und gefahrenfreien Funktion

- „Sicherheit“ ist abhängig von ihrer Definition
- welcher Grad von Unsicherheit akzeptiert wird

Zuverlässigkeit

- Tritt bei einer Störung keine Gefährdung auf, spricht man von Zuverlässigkeit
- Die Norm IEC 61508 definiert Sicherheit als „Freiheit von unvermeidbaren Risiken“
- „funktionalen Sicherheit“ als Teilaspekt der Gesamtsicherheit

Gesetzliche Vorschriften

- Vorrangig Gesundheits- und Umweltschutz

Was ist Sicherheit?

Technische Sicherheit, Betriebssicherheit

Technische Konstruktionen

Bauteilzuverlässigkeit

- Primäre Grundlage für die Betriebssicherheit
- Bauteile dürfen nicht durch Überbelastung oder Materialversagen Ihre Funktionsfähigkeit verlieren

Bedeutung der Software bei technischen Systemen

- Software für sicherheitskritische Systeme
- hoher Aufwand für die Sicherstellung der Fehlerarmut der Software
- strenge Maßstäbe an den Softwareentwicklungsprozess
- Für einige Bereiche gibt es einschlägige Normen Industrien (Eisenbahn: EN 50128)

Häufig stehen kostenaufwändige Sicherheitsmaßnahmen den wirtschaftlichen Belangen zum Kapitalgewinn entgegen

Was ist Sicherheit?

Sicherheitstechnik

Sicherheit in der Technik

- Problemen und Lösungen

Sicherheitsmaßnahmen für technische Anlagen

- Spezialfälle zur Gewährleistung der Sicherheit der beteiligten Menschen
- wirtschaftlich motiviert

Unmittelbare Sicherheit

Gefahrenentstehung wird verhindert

safe-life-Ansatz

- Versagen wird ausgeschlossen
- Klärung aller äußeren Einflüsse
- sicheres Bemessen
- weiterer Kontrolle wird
- beschränktes Versagen ermöglicht gefahrlose Außerbetriebnahme möglich

redundante Anordnung von Baugruppen

- Gesamtfunktion immer gewährleistet
- auch bei Teilausfällen

Mittelbare Sicherheit

zusätzliche Schutzeinrichtungen

weisen eine mögliche Gefährdung ab

- z.B. Verkleidungen bei Maschinen verhindern eine Gefahr durch bewegte Teile

Andere Schutzsysteme arbeiten mit Sensoren

Hinweisende Sicherheit

auf Gefahren hinweisen

- Gefahrenhinweise
- Gefahrensymbole
- Verkehrszeichen

schwächste und rechtlich geringste Form in jedem Fall notwendig



Was ist Sicherheit?

Sicherheitstechnik

Unbeabsichtigten Folgen von Sicherheitssysteme

können Sicherheitsgewinn zunichte machen

Prognosen vs. empirische Beobachtung

- Der auf Prognosen setzenden Sicherheitsforschung wird vorgeworfen, empirische Beobachtung der Systeme zu vernachlässigen

Verfahren der Sicherheitstechnik

- Auswirkungsanalyse
- Fehlerbaumanalyse
- PAAG-Verfahren
 - Prognose, Auffinden der Ursache, Abschätzen der Auswirkungen, Gegenmaßnahmen

Was ist Sicherheit?

Beispiel: Risiken von VPNs

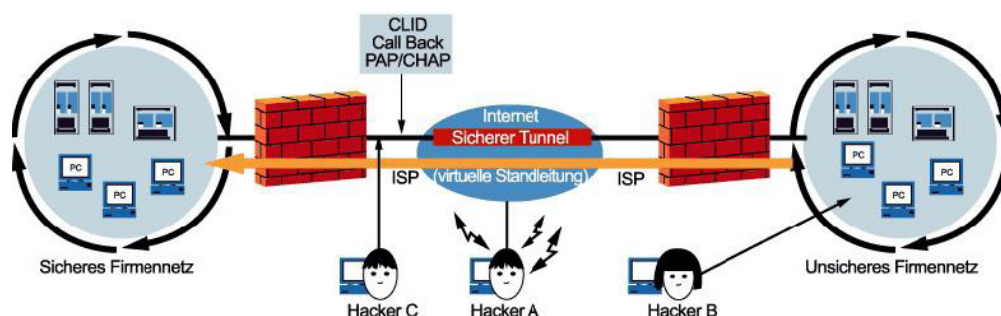
Risiken und Nebenwirkungen beim Einsatz von VPNs

- Nicht alle VPN-Systeme sind sicher gegen Man-in-the-Middle-Angriffe
- insbesondere in der Phase des Aushandels der Übertragungs- und Verschlüsselungsparameter

Implementierung von VPNs erfordert eine Menge Vorarbeiten

- Vielzahl und Komplexität der verfügbaren Protokolle

VPNs erfordert je nach Architektur erhebliche zusätzliche Ressourcen



Was ist Sicherheit?

Schutzeinrichtungen

Trennend

- Verkleidung, Verdeckung
- Sicherheitsdomänen, Firewall

Ortsbindend

- Zweihandbedienung
- Tipptaster
- Anketten

Abweisend

- Handabweiser, Fingerabweiser
- Zugangskontrolle, Raumverschluss

Detektierend

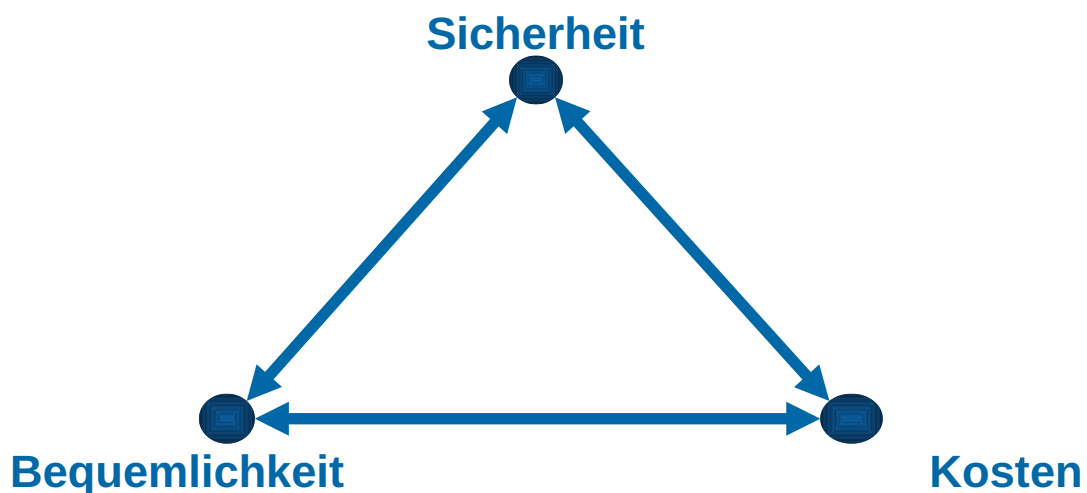
- Lichtschranke
- Pendelklappen
- Monitoring
- Intrusion Detektion



IT-Sicherheit im Spannungsfeld

Sicher - Bequem - Billig

„Suchen Sie sich zwei davon aus!“



Was ist Informationssicherheit?

IT-Sicherheit im Fokus

Warum ist Sicherheit überhaupt ein Thema?

Verteilte Informatiksysteme sind kritische Ressourcen

- Globalisierung der Kommunikationsbedürfnisse und -infrastruktur (Internet)

"grenzüberschreitenden" Kooperation

- Email, Informationssysteme, Desktop-Conferencing, Soziale Netzwerke

Offene Systeme

- Vielfältige Schnittstellen und Datenaustausch
- Erhöhung des Angriffs- und Schadenpotentials

Physische Sicherheit kann oft nicht gewährleistet werden

- Zugang zu Räumen und IT-Systemen

Wem vertraue ich, wem nicht?

- Vertrauen als wichtige Ressource, Ziel eines Sicherheitsdienstes

Warum Informationssicherheit?

- Das Streben nach Informationssicherheit resultiert aus einer risikoorientierten Herangehensweise
- Es soll Unternehmen vor Kapitalschäden jeglicher Art schützen

Klassische Beispiele sind:

- Image- und Vertrauensverlust
- Datenverlust
- Produktivitätsausfall
- Wirtschaftsspionage
- Verletzung von Marken- und Urheberrechten

Es liegt in der Natur der Sache, dass Unternehmer solchen Schäden durch entsprechende Maßnahmen vermeiden wollen.

IT-Sicherheit im Fokus

Warum ist Sicherheit überhaupt ein Thema?

Verteilte Informatiksysteme sind kritische Ressourcen

- Globalisierung der Kommunikationsbedürfnisse und -infrastruktur (Internet)

"grenzüberschreitenden" Kooperation

- Email, Informationssysteme, Desktop-Conferencing, Soziale Netzwerke

Offene Systeme

- Vielfältige Schnittstellen und Datenaustausch
- Erhöhung des Angriffs- und Schadenpotentials

Physische Sicherheit kann oft nicht gewährleistet werden

- Zugang zu Räumen und IT-Systemen

Wem vertraue ich, wem nicht?

- Vertrauen als wichtige Ressource, Ziel eines Sicherheitsdienstes

Was ist Informationssicherheit?

Datensicherung

Datensicherung

Normbegriff der Rechtsordnung: Summe aller

- technischen und
- organisatorischen Maßnahmen

zur Gewährleistung des Datenschutzes



Die Maßnahmen müssen in einem angemessenen Verhältnis zum angestrebten Schutzzweck stehen.

IT-Sicherheit im Fokus

Früher

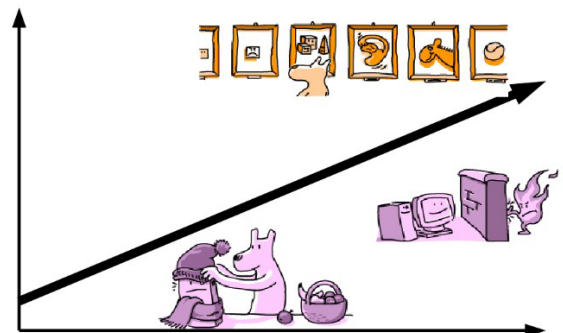
- öffentliche Netze: abgeschlossen, zentral verwaltet
- Internet: reines Forschungsnetz, kein lohnendes Angriffsziel, Benutzer vertrauen einander

Heute

- große IT-Landschaften
- Komplexität
- Dezentralisierung
- kommerzielle Nutzung des offenen, dezentralen, „anarchischen“ Internets

Folge

- Sicherheitsmechanismen werden zum unverzichtbaren Bestandteil moderner Kommunikationssysteme



- **Vernetzung**
- **Internet-Nutzung**
- **Komplexität der IT**
- **Schwachstellen**
- **Schadsoftware**
- **Risiko**
- **IT-Grundschutz**
 - Bedeutung
 - Umfang

Was ist Informationssicherheit?

Datensicherheit

Datensicherheit als technischer Begriff

- Planende,
- steuernde,
- verarbeitende und
- kontrollierende Maßnahmen

zur Gewährleistung der Sicherheitsziele

- Verfügbarkeit
- Vertraulichkeit
- Integrität

der informationstechnischen Infrastruktur

Was ist Informationssicherheit?

Datensicherheit

Datensicherung als antiquierter Begriff

- Kopieerstellung von Datenbeständen
- Ziel: Rekonstruktion bei Verlust
 - Verfügbarkeit
 - Integrität

Datensicherung zur Gewährleistung der

- Verfügbarkeit
- Integrität

der informationstechnischen Infrastruktur ist im weiteren Sinne auch Voraussetzung für die Erzielung einer Gesamtsicherheit, die

- alle Komponenten der IT-Infrastruktur erfasst, die
- für die betrieblichen Wertschöpfungsprozesse relevant sind

Interesse von Unternehmen

- Sicherstellung der kontinuierlichen Bedürfnisbefriedigung
- Gewinnmaximierung

Interesse des Einzelnen

- Schutz seiner (personenbezogenen) Daten vor Missbrauch



Was ist Informationssicherheit?

IT-Systeme

IT-Systeme bestehen aus

Objekten

Subjekten

Aktionen

Umfeldbedingungen



Was ist Informationssicherheit?

Objekte

Objekte eines IT-Systems sind alle aktiven und passiven Komponenten

- Hardware
- Software
- gespeicherten Daten

Im weiteren Sinne

- Gesamte informationstechnische Infrastruktur

schutzwürdige Objekte

- Einzelne Objekte (Server, Anwendungen, Verbindungen)
- Gruppen von Objekten
- Gesamter IT-Verbund

Für jedes Objekt muss geregelt sein

- welche Subjekte
- unter welchen Voraussetzungen
- Zugang und
- Zugriff erhalten

Was ist Informationssicherheit?

Subjekte

Subjekte eines IT-Systems sind

- Betreiber
- Anwender
- Benutzer

Zugang der Subjekte zu IT-Systemen und Zugriff auf einzelne Objekte erfordert

- Identifikation
- Authentifizierung

Subjekte können auch technische Kommunikationselemente sein

- selbststeuernde Aktionen
 - z.B. Verbindung zu fremden Systemen
- mit dem Ziel des Zugriffs auf fremde Objekte
 - aufbauen
 - nutzen
 - wieder abbauen

Was ist Informationssicherheit?

Anmeldung

Zugangsverfahren

Anmeldeverfahren von Subjekten zu IT-Systemen oder einzelnen Objekten

Im Zugangsverfahren wird die Berechtigung von

- natürlichen oder
- technischen Subjekten

durch

- technische oder
- logische Verfahren

zur Identifizierung / Authentifizierung überprüft



"I usually don't do this on the first date,
but here's my username and password."

Zugriff

Ausführung von

- lesenden,
- schreibenden oder
- steuernden Aktionen

auf definierte Objekte eines IT-Systems

Zugriffskontrolle erfolgt auf logischer Ebene

- nach ordnungsgemäßer Zugangskontrolle
- mittels Verfahren zur Identifizierung und / oder
- Authentifizierung von Zugriffsrechten.

Need-to-Know-Prinzip

Ein Subjekt darf nur auf ein Objekt zugreifen können, wenn dies in seiner Zuständigkeit liegt.



Was ist Informationssicherheit?

Aktionen

Aktionen

- passiv
- aktiv
- objektsteuernd
- objektnutzend

Differenzierung auf Softwareebene durch

- Systemsoftware
- Anwendungssoftware

Was ist Informationssicherheit?

Umfeld

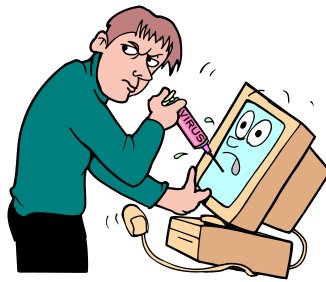
Konstrukte am Standort beschreiben das Umfeld

- räumlich
- versorgungstechnisch
- Klimatechnisch
- ...

Sekundäres Umfeld vernetzter Systeme

- Netztopologie
- Kommunikationsarchitektur

Bedrohung – Gefährdung - Schwachstelle - Risiko



Bedrohung

Bedrohung

Beeinträchtigung des angestrebten Zustandes der Informationssicherheit

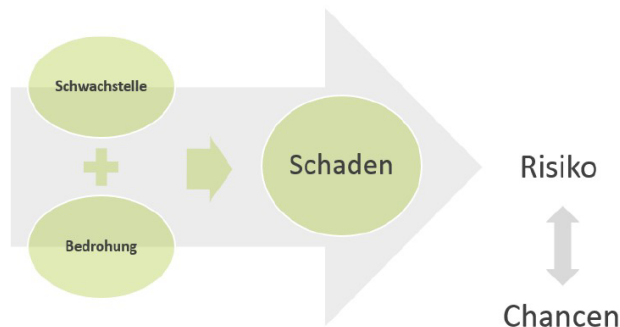
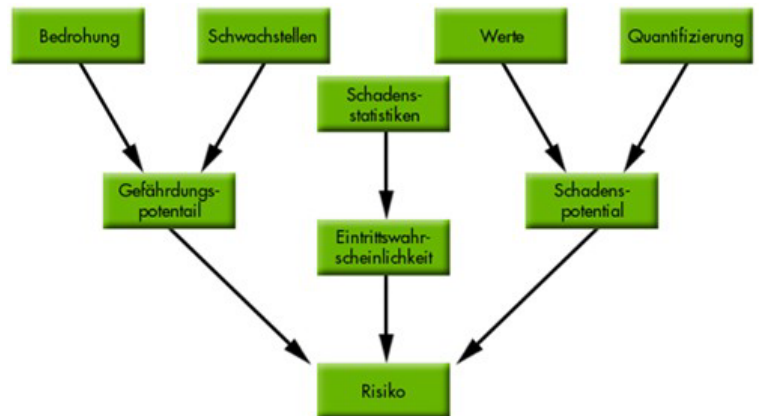
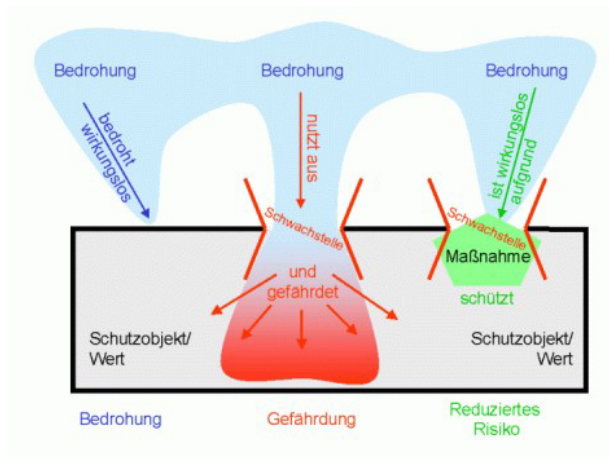
- ungesteuerte oder ungeplante
- gesteuerte oder geplante Aktion
- eines Subjektes oder Objektes

außerhalb der zweckbestimmten Nutzung des bedrohten Objektes

Klassifizierung von Bedrohungen

- Eintrittswahrscheinlichkeit
- Ort der Entstehung
- Aktionsebenen
- allgemein oder speziell

Bedrohung – Gefährdung – Schwachstelle – Risiko – Chance



Bedrohungen in der Praxis

Beispiele

- Irrtum und Nachlässigkeit
- Malware
- Internetdienste (WWW, E-Mail,...)
- Hacking und Cracking
- Wirtschaftsspionage
- Diebstahl von IT-Einrichtungen
- ...

Irrtum und Nachlässigkeit

Die meisten Datenverluste entstehen durch Irrtum oder Nachlässigkeit

- Ergebnisse einer Befragung von 300 Windows Netz- und Systemadministratoren

70% schätzen die Gefahr durch unbeabsichtigtes Löschen von wichtigen Daten höher ein als durch Virenbefall

- 90% davon erklären dies durch einfache Anwenderfehler

Risikofaktor Mensch

Nicht nur Technik kann die Sicherheit einschränken

- Menschliches Verhalten tritt als zusätzlicher Risikofaktor auf



Ein vermeintlich sicheres VPNs kann dazu führen

- dass sich die Benutzer in falscher Sicherheit wiegen
- auch sensitive Informationen übertragen
- die sie sonst lediglich sicheren Netzen anvertrauen würden
- Aufmerksamkeit potenzieller Angreifer konzentriert nach der Implementierung eine VPN wieder verstärkt auf die Firmennetzen selbst
 - Da der Übertragungskanal hohe oder unmögliche Hürden stellt

KES-Studie

Bedeutung der Gefahrenbereiche

	Bedeutung heute		Prognose		Schäden	
	Rang	Priorität	Rang	Priorität	Rang	ja, bei
Irrtum und Nachlässigkeit eigener Mitarbeiter	1	1,50	2	1,70	2	51%
Malware (Viren, Würmer, Troj. Pferde,...)	2	1,34	1	2,80	1	54%
unbefugte Kenntnisnahme, Informationsdiebstahl, Wirtschaftsspionage	3	0,60	4	1,14	8	9%
Software-Mängel/-Defekte	4	0,57	5	0,96	3	43%
Hacking (Vandalismus, Probing, Missbrauch,...)	5	0,48	3	1,26	5	9%
Hardware-Mängel/-Defekte	6	0,40	8	0,32	4	38%
unbeabsichtigte Fehler von Externen	7	0,30	9	0,26	7	15%
höhere Gewalt (Feuer, Wasser,...)	8	0,24	11	0,04	9	8%
Manipulation zum Zweck der Bereicherung	9	0,17	7	0,43	10	8%
Mängel der Dokumentation	10	0,15	10	0,20	6	17%
Sabotage (inkl. DoS)	11	0,12	6	0,55	11	8%
Sonstiges	12	0,03	12	0,00	12	3%

IT-Sicherheit ist notwendig...

Schadensbilanz

Anzahl der Sicherheitsvorfälle steigt

- 75 % aller Unternehmen
- im letzten Jahr Vorfälle
- mit geschäftsschädigenden Auswirkungen

Schadenshöhe eines Einzelschadens

- Maximum: hohe zweistellige Mio-Beträge
- Durchschnitt: 5-6-stellige Beträge

Art der Schäden

- größtes Einzelproblem: Schadsoftware
- überwiegend Grundwert Verfügbarkeit
- Zunehmend gezielte Angriffe

Rangfolge der Ursachen

- Mensch
- Technik
- Umwelt



Erkennen von Sicherheitslücken I





Bedrohungen

Bedrohungen zufälliger Art

- Stromausfall
- Benutzerfehler
- Administrationsfehler
- Planungsfehler
- Systemfehler
 - Software
 - Hardware
 - Übertragungsfehler

gezielte Bedrohungen

- „Hacker“
 - Die Kreativen
 - „script kiddies“
- kriminelle Einzeltäter
 - Elektr. Bankraub
 - Insider
- kriminelle Organisationen
- Behörden

Motivationen von Angreifern

- Kriminelle Bereicherung
- Wirtschaftsspionage
- Neugierde, Kick
- Selbstwertgefühl
- Protest
- Rache
- illegale Geschäften
- Geheimdienstliche Tätigkeit
 - Militärisch
 - Wirtschaftlich
- Verdeckte Ermittlung

Gefährdungen

Gliederung

Elementare Gefährdungen

- Naturkatastrophen
- Abhören
- ...

Höhere Gewalt

- Feuer
- Wasser
- Blitzschlag
- Krankheit
- ...

Organisatorische Mängel

- Fehlende oder unklare Regelungen
- fehlende Konzepte
- ...

Menschliche Fehlhandlungen

- "Die größte Sicherheitslücke sitzt oft vor der Tastatur"
- Irrtum
- Fahrlässigkeit
- ...

Technisches Versagen

- Systemabsturz
- Plattencrash
- ...

Vorsätzliche Handlungen

- Hacker
- Viren
- Trojaner
- ...

Bedrohungen

Abhören übertragener Daten

- Nachrichten
 - unverändert noch einmal senden
 - verändern und absenden

Maskerade

- Vorspiegeln einer fremden Identität
- Versenden von Nachrichten mit falscher Quelladresse

Unerlaubter Zugriff auf Systeme

- Zugangsrechte erweitern

Bewusst kritische Systemressourcen überbeanspruchen

- Überlastsituation herbeiführen
 - Denial of Service
- „Abschießen“ von Protokollinstanzen
 - durch illegale Pakete

Code mit speziellen Eigenschaften erzeugen

- Viren
 - Modifizieren Funktion eines „Wirtsprogramms“
- Würmer
 - Verwenden eine Sicherheitslücke und ein Transportmittel, um sich fortzupflanzen
- Trojanische Pferde
 - Fremder Code wird eingeschleust und von unbedarften Benutzern oder Programmen ausgeführt
- Speicher, CPU, Kommunikationskanäle, Datenstrukturen, ...



Angriffstechniken

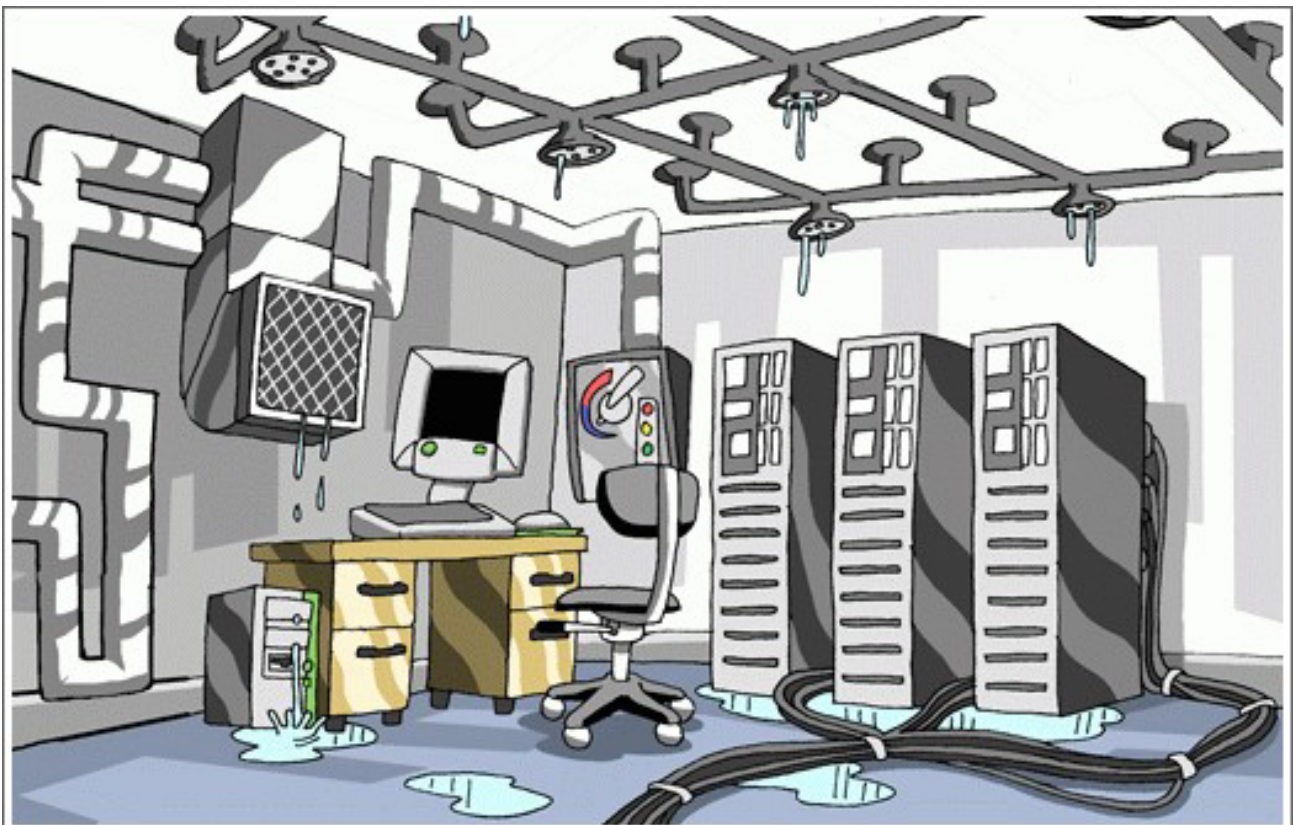
- Anzapfen
 - Leitungen oder Funkstrecken
- Zwischenschalten
 - man-in-the-middle attack
- Wiedereinspielen abgefangener Nachrichten
 - replay attack
 - z.B. von Login-Nachrichten zwecks unerlaubtem Zugriff
- gezieltes Verändern/Vertauschen
 - von Bit oder Bitfolgen
 - ohne die Nachricht selbst entschlüsseln zu können
- Brechen kryptographischer Algorithmen



Gegenmaßnahmen

- nur bewährte, als sicher geltende Algorithmen verwenden
- ausreichende Schlüssellänge
- Möglichkeiten zum Auswechseln von Algorithmen vorsehen

Sicherheit vor Wasserschäden?



Immer die gleichen Fragen

Welche Formen von Missbrauch wären möglich?

- wenn vertrauliche Informationen in die Hände Dritter gelangten?

Welche Konsequenzen hätte es?

- wenn wichtige Informationen verändert würden?
 - z. B. während einer Datenübertragung oder auf ihrem Server
 - Als Ursache kann nicht nur böse Absicht unbekannter Dritter, sondern auch technisches Versagen in Frage kommen.

Was würde geschehen?

- wenn wichtige Computer oder andere IT-Komponenten plötzlich ausfallen
- und einen längeren Zeitraum (Tage, Wochen, ...) nicht mehr nutzbar sind

Könnte die Arbeit fortgesetzt werden?

Wie hoch wäre der mögliche Schaden?

Nebeneffekte

Vorteile durchdachter IT-Sicherheitskonzepte

- neben dem Sicherheitsgewinn
- nach einiger Zeit weitere Vorteile

IT-Leiter beobachten häufig folgende "Nebeneffekte"

- Mitarbeiter sind zuverlässiger
- Arbeitsqualität steigt
- Wettbewerbsvorteile
- Wartungsarbeiten an IT-Systemen erfordern deutlich weniger Zeit
- Administratoren arbeiten effektiver

Einsatz mobiler Endgeräte

Viele unterschiedliche Geräte

- Fehlende Sicherheitsmechanismen

Diverse Betriebssysteme

- diverse Versionen
- mangelndes Patch-Management

Durchsetzbarkeit von Sicherheitsrichtlinien

Undefinierte Einsatzbedingungen

- räumlich
- Benutzer
- Netzwerk

Viele Schnittstellen

private/betriebliche Nutzung

- Mangelnde Trennung

Fehlende Regelungen

- Freiheitsgarde
- Administration

Hoher Aufwand zur Absicherung

Echelon

Systematische Beobachtung internationaler elektronischer Kommunikation

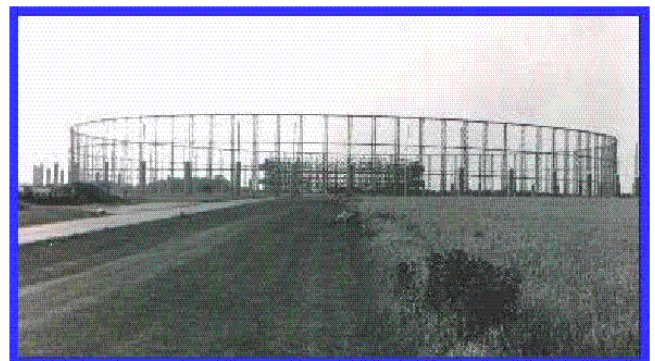
- HF Radio
- Mikrowellenkommunikation
- Unterseekabel
- Satellitenkommunikation

Analyse der aufgefangenen Signale

- Dekodierung nach Typ (Sprache, e-mail, Fax, Telex, etc.)
- Suche nach Schlüsselwörtern (Watch List)
- Sprechererkennung (Spracherkennung technisch noch schwierig)
- Verkehrsanalyse

Verwendungszwecke

- Militärisch, Strafverfolgung, Wirtschaftsspionage



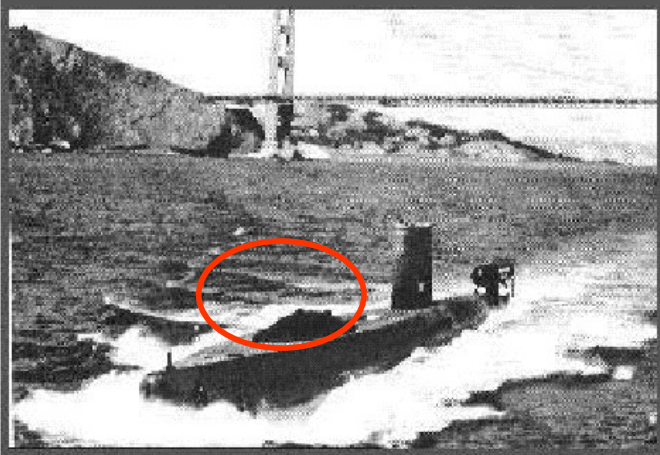
High frequency radio interception antenna (AN/FLR9)



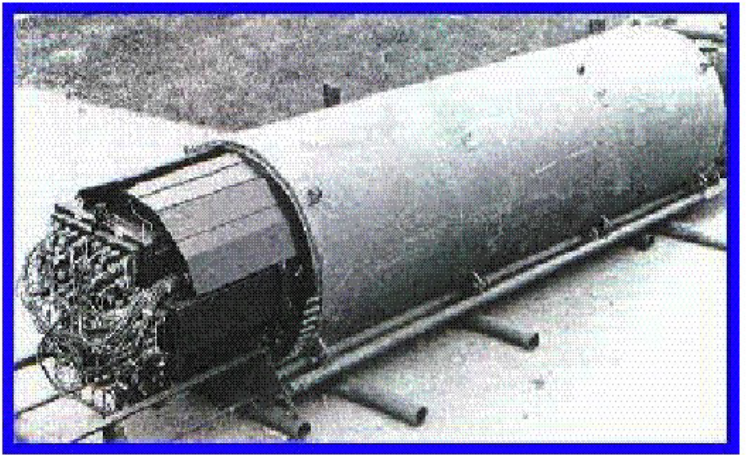
Satellite ground terminal at Etam, West Virginia, connecting Europe and the US via Intelsat IV



GCHQ constructed an identical "shadow" station in 1972 to intercept Intelsat messages for UKUSA



USS Halibut with disguised chamber for diving



Cable tapping pod laid by US submarine off Khamchatka

Sicherheits-Ziele



Informationen sind Werte

wertvoll für eine Organisation

- wie auch die übrigen Geschäftswerte

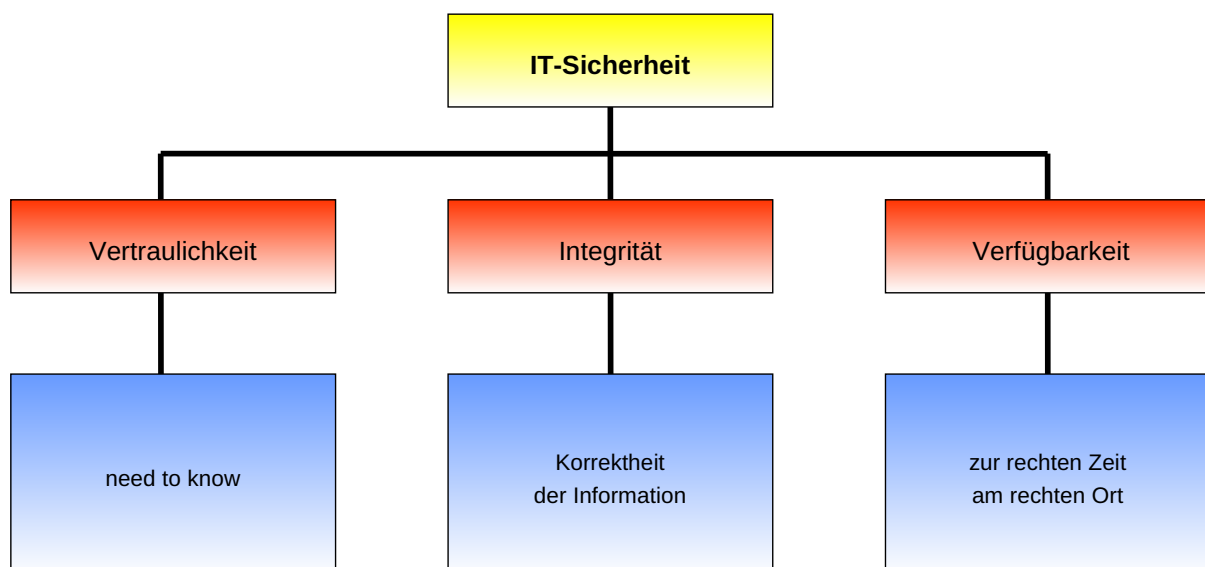
müssen in geeigneter Weise geschützt werden

Angemessen Schutz unabhängig von

- Erscheinungsform
- Art der Nutzung
- Speicherung

Sicherheits-Ziele

Grundwerte der Informationssicherheit



Grundwerte

Vertraulichkeit

Vertraulichkeit

Eigenschaft einer Nachricht

- nur für beschränkten Empfängerkreis vorgesehen
- Weitergabe und Veröffentlichung nicht erwünscht

Schutz der Vertraulichkeit

Rechtsnormen

technische Mittel

- gefördert oder erzwungen

Eines der drei wichtigsten Sachziele in der Informationssicherheit

„der Schutz vor unbefugter Preisgabe von Informationen“

Grundwerte

Vertraulichkeit

Verschlüsselung

unterstützt dieses Ziel

- Komplexere Ansätze sind unter der Bezeichnung Digitale Rechteverwaltung bekannt

Verdeckte Kanäle

- Auch wenn Maßnahmen zum Einsatz kommen, die die Vertraulichkeit gewährleisten oder zu ihr beitragen sollen (wie etwa Verschlüsselung), ist es möglich, dass ein sog. verdeckter Kanal entsteht.
- Verdeckter Kanal
 - nicht Policy-konformer Kommunikationskanal
 - der vertrauliche Daten an einen unberechtigten Empfänger übertragen kann
 - Seitenkanäle sind ein Teilgebiet der verdeckten Kanäle

Schutz der Objekte

vor unautorisiertem Zugriff

- von nicht berechtigten Subjekten
- Jeder Zugriff, der nicht durch eine klare Regelvorschrift ausdrücklich zugelassen ist, muss verweigert werden!

Schutz vor

der Zerstörung oder dem Diebstahl

Beeinträchtigungen der ordnungsgemäßen Aktionssteuerung und –ausführung

- Umfeld-,
- Software-,
- Hardware- oder
- Anwender-Versagen

Grundwerte

Verfügbarkeit

Ein System, das 24 Stunden am Tag, an 365 Jahrestagen (24 × 365) zur Verfügung steht (8760 Stunden)

- Systeme, die mit einer hohen Verfügbarkeit (99,99 % oder besser) laufen müssen, bezeichnet man als hochverfügbare Systeme.

Verfügbarkeit	Minimale erwartete Betriebszeit (Stunden)	Maximale erlaubte Ausfallzeit (Stunden)	Maximale erlaubte Ausfallzeit (Minuten)
99,00%	8672,4	87,6	5256
99,10%	8681,16	78,84	4730,4
99,20%	8689,92	70,08	4204,8
99,30%	8698,68	61,32	3679,2
99,40%	8707,44	52,56	3153,6
99,50%	8716,2	43,8	2628
99,60%	8724,96	35,04	2102,4
99,70%	8733,72	26,28	1576,8
99,80%	8742,48	17,52	1051,2
99,90%	8751,24	8,76	525,6
99,99%	8759,124	0,876	52,56
100,00%	8760	0	0

Grundwerte

Kennzahlen der Verfügbarkeit

Netto-Verfügbarkeit

- Multiplikation der Verfügbarkeit der Teilsysteme

maximale Dauer eines einzelnen Ausfalls

Ausfallzeit im Jahresdurchschnitt

- auch Verfügbarkeitsklasse

Zuverlässigkeit

- über einen gegebenen Zeitraum unter bestimmten Bedingungen korrekt zu arbeiten

Fehlersicherer Betrieb

- Robustheit gegen
 - Fehlbedienung
 - Sabotage
 - höhere Gewalt

System- und Datenintegrität

Wartbarkeit

- verallgemeinernd: Benutzbarkeit überhaupt

Reaktionszeit

- wie lange dauert es, bis das System eine spezielle Aktion ausgeführt hat

Mean Time to Repair

- MTTR, mittlere Dauer der Wiederherstellung nach einem Ausfall

Mean Time between Failure

- MTBF, mittlere Betriebszeit zwischen zwei auftretenden Fehlern ohne Reparaturzeit

Mean Time to Failure

- MTTF, siehe MTBF, wird jedoch bei Systemen/Komponenten verwendet die nicht repariert, sondern ausgetauscht werden

Grundwerte

Integrität

Integrität

lat. integritas „Unversehrtheit“, „Reinheit“, „Unbescholtenheit“

- eines der drei klassischen Ziele der Informationssicherheit

Keine einheitliche Definition des Begriffs

- „Verhinderung unautorisierter Modifikation von Information“
 - Evaluationskriterien für Informationssicherheit der frühen 1990er Jahre (ITSEC)
- „Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen“
 - Glossar des Bundesamtes für Sicherheit in der Informationstechnik

Schutz vor Beeinträchtigung von Funktionen technischer Komponenten

- der formalen oder materiellen Struktur von Daten durch
- Manipulationen mittels unzulässiger Aktionen

Authentizität und Integrität von

- Information
- Benutzer
- Hardware
- Software

Arten von Integrität

Korrektur Inhalt

- Sachverhalte der realen Welt werden korrekt abgebildet werden

Unmodifizierter Zustand

- Nachrichten werden unverändert zugestellt werden
- Programme und Prozesse laufen wie beabsichtigt ab

Erkennung von Modifikation

- unerwünschte Modifikationen (die nicht verhindert werden können) werden erkannt

Temporale Korrektheit

- zeitliche Bedingungen werden eingehalten
 - Reihenfolgen
 - maximale Verzögerungszeiten
 - Synchronität

Integrität (Daten) und Authentizität (Datenursprung)

- können nicht unabhängig betrachtet werden
 - ein modifizierter Inhalt mit bekanntem Absender ist ebenso nutzlos wie
 - ein unmodifizierter Inhalt mit gefälschtem Absender

Veränderung von Daten

- kann bei einer Datenübertragung nicht verhindert werden

Technische Maßnahmen zur Sicherstellung der Integrität

- fehlerhafte Daten erkennen
- ggf. eine erneute Datenübertragung durchführen

Möglichkeit der technischen Umsetzung

- Prüfsummen
- Schützen nicht vor absichtlicher Veränderung

Message Authentication Code

- können Übertragungsfehler und Manipulationen erkennen

Keine Schutz vor

- Totalverlust einer Nachricht
- ungewollter Duplikation
- veränderter Reihenfolge mehrerer Nachrichten
- Diese können durch Maßnahmen wie Quittierungsmeldungen oder Sequenznummern sichergestellt werden.

Verbindlichkeit

- Non-Repudiability
- Beweisbarkeit von Vorgängen gegenüber Dritten
- Nichtabstreitbarkeit der Datenherkunft
 - wichtig z.B. bei Verträgen

Schutz vor der Verfälschung der Identität von

- Absendern und
- Empfängern

Schutz von

- Transportsystemen und
- logischen Kommunikationsverbindungen

gegen Manipulation der Transaktionen

Weitere Forderungen

Authentizität (Authenticity)

- Gesicherte Datenherkunft

Überwachung

- des Zugriffs zu Ressourcen

Ordnungsgemäßes Funktionieren

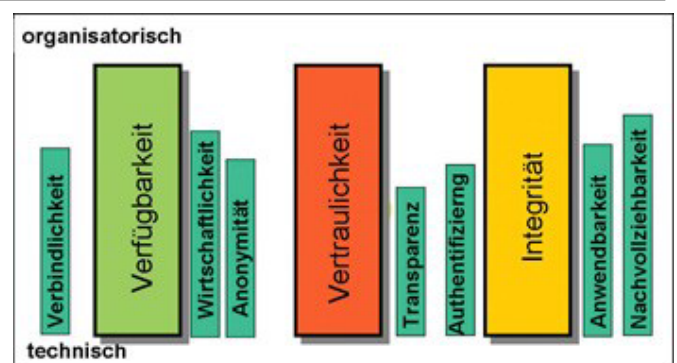
- eines IT-Systems

Revisionsfähigkeit

- Organisation des Verfahrens
- Nachvollziehbarkeit, wie und wann welche Daten in das IT-System gelangt sind

Transparenz

- das IT-Verfahren ist nachvollziehbar
 - für Sachkundige
 - in zumutbarer Zeit
 - mit zumutbarem Aufwand
- setzt eine aktuelle und angemessene Dokumentation voraus



Wann ist ein System sicher?

Informationssicherheit

Ausschluss-Definition

Informationssicherheit kann durch Ausschluss definiert werden

Danach gilt ein IT-System als sicher, wenn

- in der Realität
- keine Bedrohungen auftreten, die die
 - Sicherheit des Gesamtsystems oder
 - einzelner Objekte
- beeinträchtigen.

Die Ausschluss-Definition bietet keinen pragmatischen Ansatz.

- Sie hat nur theoretischen Charakter.

Induktive Definition

- vom Speziellen zum Allgemeinen

geht davon aus, dass unter den

- bekannten oder
- vermuteten Aktionen

Manipulationen möglich sind, die nach

- Art und
- Auswirkung

erfassbar sind.

Induktive Definition der Sicherheit

Ein System muss

- nach Abschluss der Installation oder
- zu einem anderen definierten Zeitpunkt

als sicher angenommen werden.

Ein System ist so lange als sicher anzusehen, wie

- kein Subjekt Aktionen ausführen kann, die die
 - Vertraulichkeit,
 - Verfügbarkeit,
 - Integrität und
 - Verbindlichkeit

der Objekte beeinträchtigen.

Informationssicherheit

pragmatischen Ansatz

Eine weitere Definition folgt dem pragmatischen Ansatz

Ein System ist dann sicher, wenn es geeignet ist, durch

- eigene oder
- additive Maßnahmen
- die zur Gewährleistung der Sicherheitsziele festgelegten Anforderungen in der Praxis

zum Abschluss der Installation oder zu einem Zeitpunkt zu erkennen.

Schadensfälle

als warnendes Beispiel

Schadensfälle als warnendes Beispiel

Szenario 1: "Kein Backup,,

- Server sichert Daten auf Bandlaufwerk
- Laufwerk jedoch unbemerkt bereits seit 5 Jahren defekt
- Nach einem Festplattencrash sind nun die Daten der letzten 5 Jahre verloren gegangen.

Maßnahmen

- regelmäßige Überprüfung der Backup-Bänder
- Rücksicherung prüfen und üben
- Lagerung von Sicherungsbändern außerhalb der eigenen Büroräume, beispielsweise in einem Bankschließfach

Schadensfälle als warnendes Beispiel

Szenario 2: "Befall durch Computer-Viren"

- Unternehmen hat Virens Scanner im Einsatz
- Update nur sporadisch
- E-Mail-Virus verbreitet sich im Netz, der Office Dokumente zerstört
- Um weitere Schäden zu vermeiden müssen der Mailserver und alle Arbeitsstationen vom Netz getrennt werden
- Durch zerstörte Daten, Verspätungen bei der Auftragsabwicklung und verlorene Arbeitszeit entsteht ein beträchtlicher Schaden
- Nach dem Update aller IT-Systeme taucht eine neue Variante des Virus auf – alles beginnt von vorn

Maßnahmen

- Update-Konzept für Sicherheits-Updates erstellen
- "IT-Inseln" innerhalb des Unternehmens nicht vergessen (z. B. Notebooks und Testrechner)

Schadensfälle als warnendes Beispiel

Szenario 3: "Ausfall des Administrators"

- Ein Administrator kümmert sich seit Jahren allein um die IT-Systeme im Unternehmen
- Ein Unfall macht ihn dienstunfähig
- Ausfälle und Probleme häufen sich
- Externe IT-Spezialisten können nicht helfen, da Passwörter nicht hinterlegt und die Systemarchitektur so gut wie nicht dokumentiert ist
- Bestimmte Individuallösungen sind den IT-Spezialisten nicht bekannt...

Maßnahmen

- System-Einstellungen und -Parameter ausführlich dokumentieren
- Passwörter sicher hinterlegen
- Notfallplan mit Anweisungen für die Verfahrensweise bei den wichtigsten Schadensfällen erstellen
- Vertretungsregeln einrichten

Schadensfälle als warnendes Beispiel

Szenario 4: "Hackerangriff aus dem Internet"

- Psychologe verwaltet Patientendaten auf einem Rechner mit Internetanschluss
- Daten wurden unbemerkt von einem Hacker entführt und anonym in einem Internet-Forum veröffentlicht
- Der Staatsanwalt erhebt Anklage, da mit vertraulichen Patientendaten fahrlässig umgegangen wurde.
- Der entstandene Schaden für die betroffenen Patienten ist enorm und kaum quantifizierbar.

Maßnahmen

- Internet-Zugänge sichern
- vertrauliche Daten verschlüsseln

Schadensfälle als warnendes Beispiel

Szenario 5: "Innentäter"

- Ehemaliger Mitarbeiter einer Lack und Farben herstellenden Firma wechselt die Firma in gleicher Branche
- Um in der neuen Firma eine besondere Kenntnis vorweisen zu können stiehlt er aus der nicht weiter verschlossenen Entwicklungsabteilung seiner alten Firma das Rezept für einen Speziallack
- Nicht nur der Dieb, sondern auch 2 Manager bekommen eine Vorstrafe
- Der Wettbewerbsvorteil der bestohlenen Firma ist nicht mehr vorhanden und die Umsatzeinbußen enorm

Maßnahmen

- Räume und Gebäude gegen unbefugten Zutritt sichern
- wichtige Daten verschlüsseln

Die häufigsten Versäumnisse

Aspekte der Sicherheit

Keine angemessenen Sicherheitskonzepte

- Planung
- Kontrolle
- Zuständigkeiten
- Funktionierender Sicherheitsprozess

Unzureichend konfigurierte Systeme

- Vorhandene Sicherheitsmechanismen werden nicht angewandt
- Zu starker Fokus auf Aufrechterhaltung des Betriebes
- Mangelnder Überblick über Sicherheitsrelevanz administrativer Tätigkeiten

Gravierende Sicherheitslücken in Software

- Kurze Entwicklungszeit von Software
- Features, Features, Features
 - Money, Money, Money

Automatisierte, grafische Hacking-Werkzeuge

- Relativ niedrige „Einstiegshürde“
- Dual use - Werkzeuge

Die häufigsten Versäumnisse (I)

Typischen Fehler und Versäumnisse

- geringe Abhängigkeiten von Unternehmensgröße und Branche

Unzureichende IT-Sicherheits-Strategie

- Sicherheit hat einen zu geringen Stellenwert
- Dauerhafte Prozesse zur Beibehaltung des Sicherheitsniveaus fehlen
- Sicherheitsvorgaben sind nicht dokumentiert
- Kontrollmechanismen und Aufklärung im Fall von Verstößen fehlen

Schlechte Konfiguration von IT-Systemen

- Die Rechtevergabe wird nicht restriktiv genug gehandhabt
- IT-Systeme sind schlecht konfiguriert

Unsichere Vernetzung und Internet-Anbindung

- Sensitive Systeme sind gegen offene Netze unzureichend abgeschottet

Die häufigsten Versäumnisse (II)

Nichtbeachtung von Sicherheitserfordernissen

- Sicherheitsmaßnahmen werden aus Bequemlichkeit vernachlässigt
- Anwender und Administratoren sind mangelhaft geschult

Schlechte Wartung von IT-Systemen

- Verfügbare Sicherheits-Updates werden nicht eingespielt

Sorgloser Umgang mit Passwörtern und Sicherheitsmechanismen

- Mit Passwörtern wird zu sorglos umgegangen
- Vorhandene Sicherheitsmechanismen werden nicht genutzt

Mangelhafter Schutz vor Einbrechern und Elementarschäden

- Räume und IT-Systeme werden nur ungenügend gegen Diebstahl oder Elementarschäden geschützt

Die wichtigsten Maßnahmen

Systematisches Herangehen an IT-Sicherheit

Angemessene Berücksichtigung von IT-Sicherheit

IT-Sicherheitsziele und Maßnahmen festlegen

Rahmenbedingungen

- Gesetze, Verträge, Kundenanforderungen, Konkurrenzsituation

Rolle der IT und IT-Sicherheit

- für das Unternehmen bzw. die Behörde

Werte die zu schützen sind

- Know-how, Betriebsgeheimnisse, personenbezogene Daten, IT-Systeme

Mögliche Schadensfälle

Regelungen

- Zu jedem vorhandenen Sicherheitsziel und jeder zugehörigen Maßnahme sollten geeignete Regelungen getroffen werden

Handlungsplan

- mit klaren Prioritäten der Sicherheitsziele und -maßnahmen sollte erstellt werden

Zuständigkeiten

- müssen festgelegt werden

Systematisches Herangehen an IT-Sicherheit

Angemessene Berücksichtigung von IT-Sicherheit

Richtlinien und Zuständigkeiten

- müssen bekannt gemacht werden

Umständliche Sicherheitsanforderungen

- sollten vermieden werden

Bei allen Projekten

- frühzeitig und ausreichend IT-Sicherheitsaspekte berücksichtigen

Alternative Lösungsansätze

- Bei mangelnden Ressourcen

Kontrolle und Aufrechterhaltung der IT-Sicherheit

- Die IT-Sicherheit sollte regelmäßig überprüft werden
- Vorhandene Arbeitsabläufe und Sicherheitsrichtlinien sollten regelmäßig hinsichtlich Zweckmäßigkeit und Effizienz überprüft werden

Langfristig sollte ein umfassendes Sicherheitsmanagement aufgebaut werden

- Alle bestehenden Sicherheitsrichtlinien sollten schriftlich in einem Sicherheitskonzept dokumentiert werden

Sicherheit von IT-Systemen

Vorhandene Schutzmechanismen

- anwenden

Virenschutzprogramme

- flächendeckend einsetzen

Datenzugriffsmöglichkeiten

- auf ein Mindestmaß beschränken

Allen Systembenutzern

- Rollen und Profile zuordnen

Administratorrechte

- auf erforderliches Maß einschränken

Programmprivilegien

- begrenzen

Standardeinstellungen

- geeignet anpassen

Handbücher und Dokumentationen

- frühzeitig lesen

Installations- und Systemdokumentationen

- ausführlich erstellen und regelmäßig aktualisieren

Zum Schutz von Netzen muss eine Firewall verwendet werden

- Eine sichere Firewall muss bestimmten Mindestanforderungen genügen
- Nach außen angebotene Daten sollten auf das erforderliche Mindestmaß beschränkt werden
- Nach außen angebotene Dienste und Programmfunktionalität sollten auf das erforderliche Mindestmaß beschränkt werden

Beim Umgang mit Web-Browsern

- ist besondere Vorsicht geboten, riskante Aktionen sollten unterbunden werden

Bei E-Mail-Anhängen

- ist besondere Vorsicht notwendig

Ein gesonderter Internet-PC zum Surfen

- ist eine kostengünstige Lösung für die meisten Sicherheitsprobleme bei der Internet-Nutzung

Faktor Mensch

Kenntnis und Beachtung von Sicherheitserfordernissen

Sicherheitsrichtlinien und -anforderungen

- müssen beachtet werden

Ordnung am Arbeitsplatz

- es dürfen keine sensiblen Informationen frei zugänglich sein

Wartungs- und Reparaturarbeiten

- besondere Vorsichtsmaßnahmen beachten

Mitarbeiter

- müssen regelmäßig geschult werden

Ehrliche Selbsteinschätzung

- Expertenrat einholen

Sicherheitsvorgaben

- müssen kontrolliert werden

Konsequenzen für Sicherheitsverstöße

- festlegen und veröffentlichen
- Sicherheitsverstöße tatsächlich sanktionieren



Sicherheits-Updates

- müssen regelmäßig eingespielt werden
- Aktionsplan zum Einspielen von Sicherheits-Updates erstellen

Sicherheitseigenschaften verwendeter Software

- regelmäßige ausführliche Recherche

Software-Änderungen sollten getestet werden

Unzureichende Software-Tests



News Hintergrund Erste Hilfe

Security > News > 7-Tage-News > 2014 > KW 9 > Bitcoin-Börse Mt.Gox ist insolvent

28.02.2014 12:05

« Vorige | Nächste »

Bitcoin-Börse Mt.Gox ist insolvent

vorlesen / MP3-Download

Die Anleger hatten viele Fragen, die Betreiber keine Antworten. Jetzt ist klar: Bei der ehemals größten Bitcoin-Börse gehen die Lichter aus.

Die ehemals größte Handelsplattform für die Krypto-Währung Bitcoin, [Mt.Gox](#), hat einen Insolvenzantrag gestellt. Mt.Gox habe Schulden von rund 6,5 Milliarden Yen (46,6 Millionen Euro), hieß es am Freitag auf einer Pressekonferenz in Tokio.

Einem kursierenden Dokument zufolge, bei dem es sich [um einen Krisenstrategie-Entwurf](#) der insolventen Bitcoin-Börse handeln soll, ist dem Unternehmen durch einen Fehler im selbst entwickelten Transaktionsystem ein Schaden in Höhe von 744.000 Bitcoins entstanden – umgerechnet rund 284 Millionen Euro.

Vor drei Wochen hatte Mt. Gox [einen Abhebungs-Stop verhängt](#). Seitdem war es den Nutzern nicht mehr möglich, Transaktionen über die Bitcoin-Börse durchzuführen. Spätestens mit der Insolvenzanmeldung dürfte für die ehemaligen Kunden von Mt. Gox die letzte Hoffnung schwinden, die die dort befindlichen Krypto-Münzen jemals wiederzusehen. (dpa) / (rei)

Bitcoin, die digitale Währung



Die virtuelle Währung Bitcoin auf dem Weg ins reale Leben: An speziellen Börsen kann man Bitcoins kaufen und verkaufen, diverse Online-Händler und Läden akzeptieren Bitcoins als Zahlungsmittel, erste Bitcoin-Geldautomaten werden aufgestellt. Dass die digitale Währung weder von Regierungen noch von Banken kontrolliert wird, macht für viele den besonderen Reiz aus. Allerdings leiden die Bitcoin-Börsen immer wieder unter Turbulenzen und Cyber-Attacken - ein Grund, neben der unterschiedlichen Haltung der nationalen und internationalen Währungshüter und Finanzinstitutionen, für häufige starke Bitcoin-Kursschwankungen.

Chaos bei British Airways

Ein Fehler beim Software-Update führte zum Systemabsturz

- Booking-System brach zusammen
- Bildschirme flackerten
- Flüge fielen aus
- Tickets mussten per Hand ausgestellt werden
- Weltweit mussten Fluggäste warten



Verwendung von Sicherheitsmechanismen

Umgang mit Passwörtern und Verschlüsselung

Sicherheitsmechanismen

- sorgfältig auswählen

Sichere Passwörter

- Sollten gut gewählt werden

Voreingestellte oder leere Passwörter

- sollten geändert werden

Arbeitsplatzrechner

- sollten bei Verlassen mit Bildschirmschoner und Kennwort gesperrt werden

Sensitive Daten und Systeme

- müssen geschützt werden



Schutz vor Katastrophen und Elementarschäden

Notfallchecklisten

- erstellen
- jedem Mitarbeiter bekannt geben

Backup

- Alle wichtigen Daten müssen gesichert werden
- regelmäßig

IT-Systeme angemessen schützen

- Feuer
- Überhitzung
- Wasserschäden
- Stromausfall

Zutrittsschutz

- zum Schutz vor Einbrechern müssen umgesetzt werden

Inventarisierung

- gesamter Bestand an Hard- und Software sollte in einer Inventarliste erfasst werden



	Integrität	Vertraulichkeit	Verbindlichkeit	Verfügbarkeit
Virenschutz	✓	✓	✗	✓
Passwort	✓	✓	✗	✓
Backup	✓	✓	✗	✓
Rechtmanagement	✓	✓	✗	✗
Firewall	✗	✓	✗	✓
Verschlüsselung	✓	✓	✗	✗
Signaturen	✓	✗	✗	✗
Intrusion Detection	✗	✗	✗	✓

Sicherheitsdienste

Überwiegend mit kryptographischen Mechanismen

Authentisierung

- Datenpakete (data origin authentication)
- Systeme/Benutzer (entity authentication)

Integritätssicherung (integrity protection)

- häufig kombiniert mit Daten-Authentisierung

Verschlüsselung (encryption)

Schlüsselaustausch (key exchange)

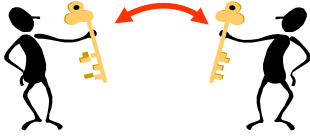


Ohne kryptographische Mechanismen

- Zugriffskontrolle (access control)
- Einbruchserkennung (intrusion detection)

(A)symmetrische Kryptographie

Symmetrische Kryptographie



Instanzen besitzen gemeinsamen geheimen Schlüssel.

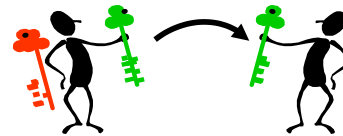
Vorteile

- geringer Rechenaufwand
- kurze Schlüssel

Nachteile

- Schlüsselaustausch schwierig
- keine Verbindlichkeit

Asymmetrische Kryptographie (Public-Key-Kryptographie)



Schlüsselpaar aus privatem und öffentlichem Schlüssel

Vorteile:

- öffentliche Schlüssel sind relativ leicht verteilbar
- Verbindlichkeit möglich

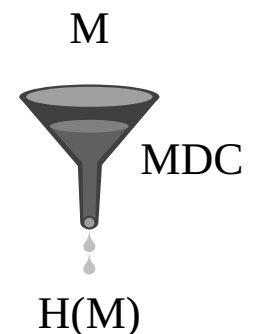
Nachteile:

- längere Schlüssel
- hoher Rechenaufwand

Authentisierung (1)

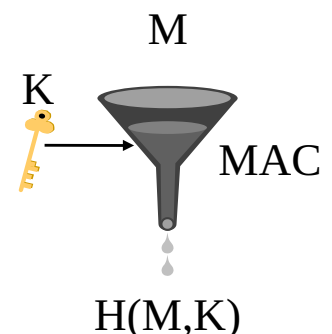
Kryptographische Hash-Funktion (Message Digest Code, MDC):

- Nachricht M (beliebig lang) $\rightarrow$ Hash-Wert $H(M)$ (min. 128 bit)
- Wichtig: „Einweg“-Eigenschaft: keine Kollisionen effizient erzeugbar
Beispiele: MD5, SHA-1, RIPEMD-160



Schlüsselabhängige Hash-Funktion (Message Authentication Code, MAC):

- Nachricht M , Schlüssel $K \rightarrow$ Hash-Wert $H(M,K)$
- kann aus MDC konstruiert werden: HMAC (RFC 2104), z.B. HMAC-MD5



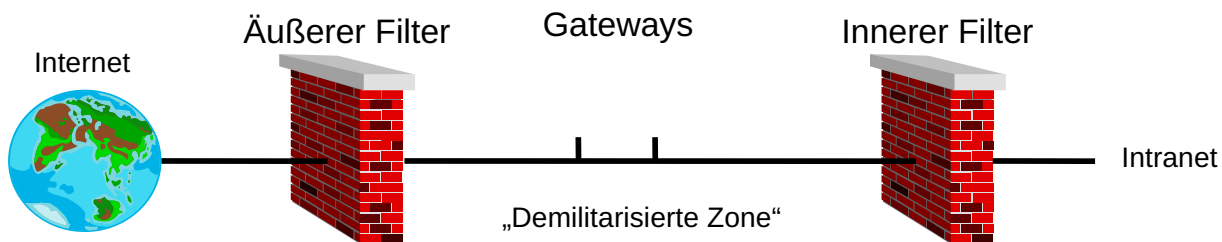
Firewalls

Auf Anwendungsebene: System von Zugriffsrechten

- Beispiele: Unix/NT-Dateirechte, SNMP-Objektrechte

Auf Netzwerk-/Transportebene: Firewalls

- Paketfilter filtern nach Quell/Zieladresse + Ports (TCP/UDP)
- am einfachsten: ingress/egress filtering (nach Topologie)
- Anwendungs-Gateways (Zugriffskontrolle, Protokollierung)
- oftmals private Adressen und Adressumsetzung (NAT)
- Probleme mit manchen Protokollen (z.B. FTP, H.323)



Secure Shell (SSH)

Aufgabe: sichere entfernte Rechnernutzung (remote login)

- rsh/rlogin haben keine Authentisierung
- telnet überträgt Passworte ungeschützt

Funktionsweise

- Austausch eines Sitzungsschlüssels (Diffie-Hellman)
- Austausch der Server-Authentisierung (digitale Signatur)
- symmetrische Verschlüsselung + MAC für alle Pakete
- Benutzer-Authentisierung (dig. Signatur oder Passwort)

Zusätzliche Funktionalität

- Verschlüsselte Dateiübertragung mit scp
- Verschlüsselte Tunnel für einzelne TCP-Ports
- automatische Einrichtung eines X11-Tunnels



Secure Socket Layer (SSL)

Aufgabe: Verschlüsselung/Datenintegrität für einzelne Sockets

- Haupteinsatzgebiet: verschlüsselte HTTP-Verbindungen

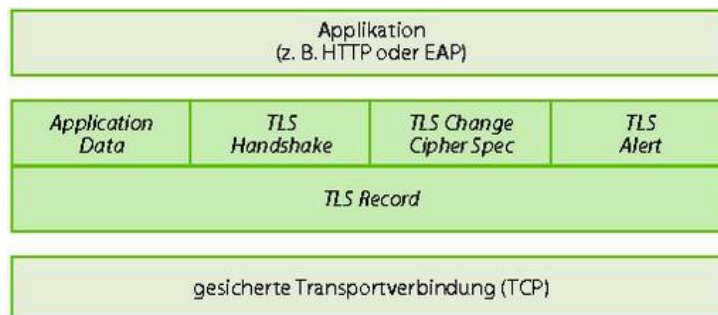
Funktionsweise:

- Austausch eines Sitzungsschlüssels (Diffie-Hellman)
- optional Server-/Benutzer-Authentisierung (dig. Signatur)
- danach: Verschlüsselung + MAC für alle Pakete



Versionen:

- von Netscape: SSL 1.0 bis SSL 3.0
- Transport Layer Security (RFC 2246) basierend auf SSL 3.0



IP Security (IPSec)

Aufgabe: sicheres Tunneln von IP-Paketen

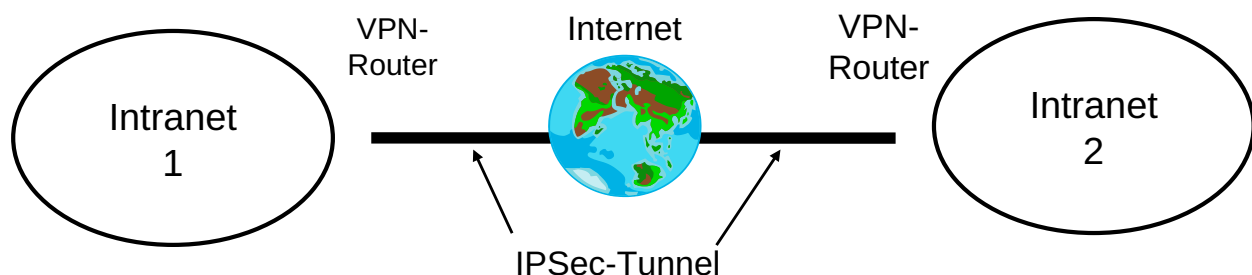
- Haupteinsatzgebiet: virtuelle private Netze (VPNs)

Funktionsweise:

- MAC und/oder symm. Verschlüsselung
- 2 Paketformate: AH (RFC 2402), ESP (RFC 2406)

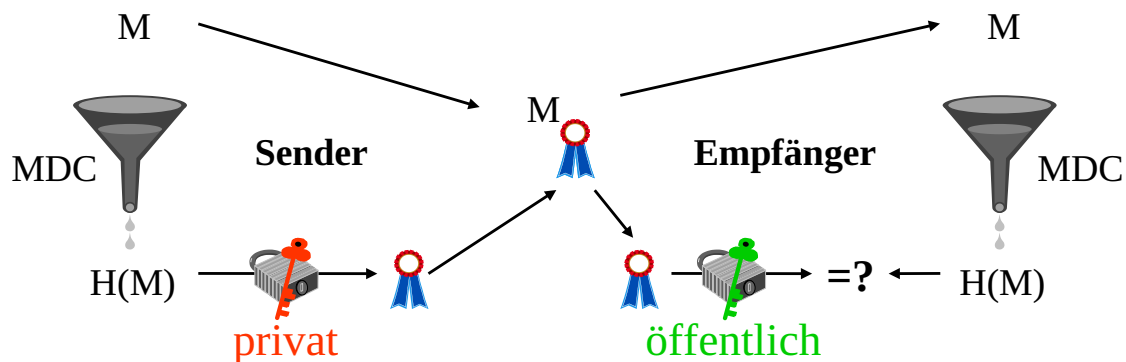
Produkte

- StrongSwan (www.strongswan.org)
- Windows (VPN-Funktionen)



Digitale Signatur

- Hash-Wert $H(M)$ wird mit privatem Schlüssel signiert
- Empfänger überprüft Signatur mit öffentlichem Schlüssel
- kann auch Verbindlichkeit garantieren
- wichtigste Algorithmen: RSA, AES
- min. Schlüssellänge: 1024 bit
(160 bit bei DSA-Variante mit elliptischen Kurven)



 [News](#) [Hintergrund](#) [Erste Hilfe](#)

[Security](#) > [News](#) > [7-Tage-News](#) > [2014](#) > [KW 20](#) > NSA-Skandal: Cisco beschwert sich über mar

15.05.2014 14:30 [« Vorige](#) | [Nächste »](#)

NSA-Skandal: Cisco beschwert sich über manipulierte Postsendungen

 [vorlesen](#) / [MP3-Download](#)

Der US-Netzausrüster empört sich darüber, dass die NSA Cisco-Postsendungen abfängt und die enthaltenen Geräte manipuliert. Das untergrabe das Vertrauen in die Industrie, schreibt der Konzern, der mit Umsatzrückgängen zu kämpfen hat.

Cisco hat der NSA vorgeworfen, mit ihrem Eingriff in den Postversand von Netzwerktechnik das Vertrauen in die IT-Industrie zu untergraben. [In einem Blogbeitrag](#) verlangt Mark Chandler, stellvertretender Vizepräsident des Unternehmens, man müsse die Möglichkeit haben, unbehelligt Internetinfrastruktur an die eigenen Kunden liefern zu können. Wenn man sich daran halte, bestimmte Ziele nicht zu beliefern, müsse sich die Regierung auch daran halten, legale Lieferungen nicht zu manipulieren. Cisco selbst arbeite jedenfalls mit keiner Regierung zusammen, um eigene Produkte zu schwächen.

Hintergrund für diese Kritik an der US-Regierung sind Dokumente des NSA-Whistleblowers Edward Snowden, die darlegen, wie die NSA Postsendungen abfängt, [um Cisco-Geräte mit Malware zu versehen](#). Die Dokumente hatte der Enthüllungsjournalist Glenn Greenwald in einem Buch öffentlich gemacht. Cisco schließt sich nun einem Aufruf von IBM an und ergänzt ihn um die Forderung, Postsendungen nicht anzutasten. Außerdem sollten den Herstellern Sicherheitslücken, die Regierungsbehörden bekannt sind, mitgeteilt werden. Daten, die US-Unternehmen auf Servern außerhalb der USA speicherten, sollten besser geschützt werden. Nur so könnte Vertrauen gewonnen werden.

Cisco hatte am Mittwoch bekanntgeben müssen, dass die Nachfrage nach eigenen Produkten schwach geblieben ist. Während der Umsatz im dritten Geschäftsquartal [um 6 Prozent zurückging](#), fiel der Gewinn sogar um satte 12 Prozent. ([mho](#))

