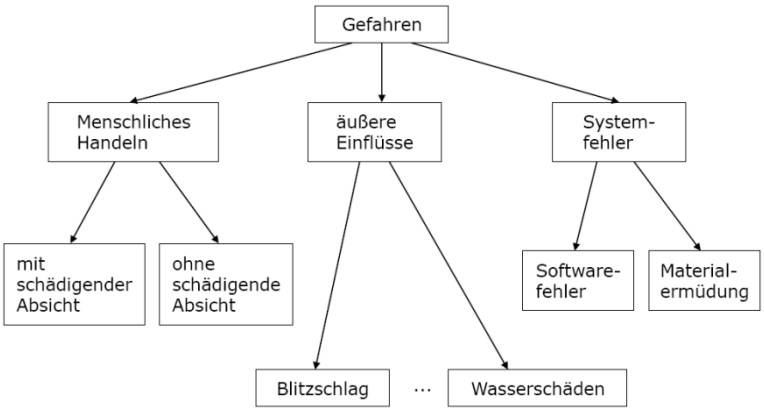
Teil 1: Sicherheit

1.1 Begriffsabgrenzung, Einführung, Gefahrenpotentiale

Sicherheit: Zustand des Geschütztseins vor Gefahr und Schaden

Gefahrenquellen



Computermissbrauch (Computerkriminalität)

- Sabotage
  - Zerstörung von HW oder SW
  - Verlust der Verfügbarkeit (denial of service)
  - → Vorteil, dass der Missbrauch dem Opfer bewusst ist
- Ausspähen von Daten (Verlust der Vertraulichkeit)
  - vor Ort durch browsing, auswerten, duplizieren
  - Systemzugang über Datenfernleitungen
  - passive Lauschangriffe (Abstrahlung, Lauschangriffe auf dem Übertragungsweg, Mitlesen)
  - Maskerade (Identität eines anderen)
  - Sammeln von „Abfall“ (Löschen bedeutet nicht immer löschen)
- Manipulation (Verlust der Integrität)
  - modifizieren, wiedereinspielen, einfügen, löschen
  - Systemveränderungen
  - aktive Angriffe
  - Leugnen der Kommunikation

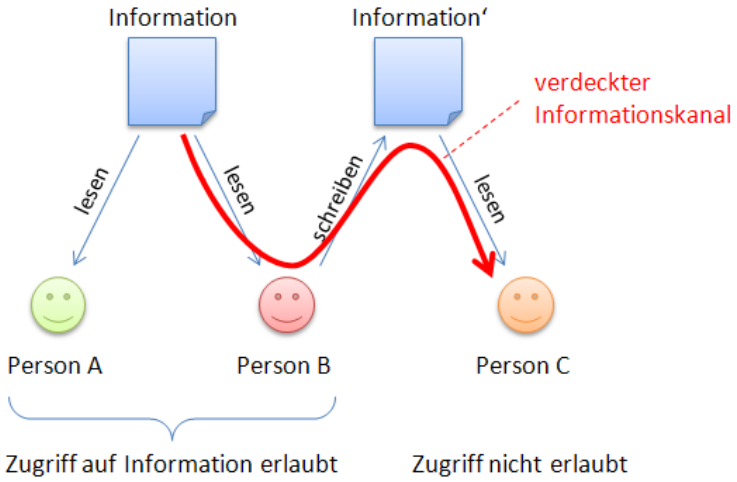
Klassifikation des Begriffs „Sicherheit“

- nach der Intention
  - Sicherheit gegen beabsichtigte Angriffe
  - Sicherheit gegen unbeabsichtigte Ereignisse
- nach der Art der Bedrohung
  - Verlust der Vertraulichkeit: unbefugter Informationsgewinn
  - Verlust der Integrität: unbefugte Modifikation von Daten oder HW
  - Verlust der Verfügbarkeit: unbefugte Beeinträchtigung der Funktionalität
  - Verlust der Originalität, Verlust der Authentizität
- nach der Art der bedrohten Ressource
  - Daten: Datenschutz, Datensicherheit, Datensicherung

  - Software: Softwareschutz (Piraterie), Sicherstellung der Integrität
  - Hardware: Verfügbarkeit, Schutz gegen Missbrauch
  - Anlagen: Gebäude, Klimaanlagen
- nach der Art der Vorkehrung
  - informationstechnische Maßnahmen
  - bauliche Maßnahmen
  - organisatorische /personelle Maßnahmen

Sicherheit

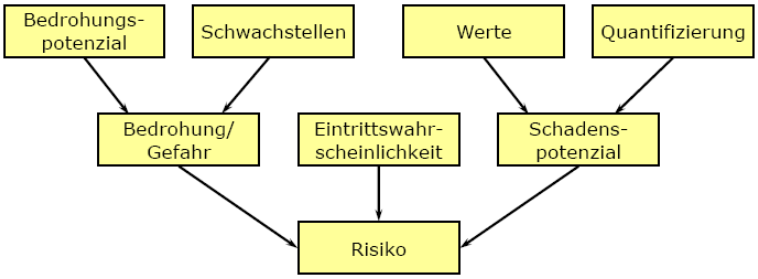
- Grundsicherheitsanforderungen (CIA)
  - Vertraulichkeit (confidentiality): Nur autorisierte Benutzer dürfen lesenden Zugriff auf das Sicherheitsobjekt erlangen.
  - Integrität (integrity): Das Sicherheitsobjekt darf nur von dazu berechtigten Subjekten in vorgegebener Weise verändert werden.
  - Verfügbarkeit (availability): Jedes dazu berechtigte Subjekt kann in vorgegebener Art und Weise und zu jedem vorgesehenen Zeitpunkt das Objekt benutzen.
- Weitere Sicherheitsanforderungen
  - Originalität: Das Objekt besitzt die vorgegebene Identität (Authentizität) und es handelt sich nicht um eine Kopie.
  - Authentizität: Das Objekt besitzt die Identität, das es vorgibt zu haben. Es darf sich um eine Kopie handeln.
  - Anonymität: Die wahre Identität des Objekts bleibt verborgen.
  - Pseudonymität: Anonymität, die jedoch von autorisierten Subjekten in vorgegebenen Situationen aufgehoben werden darf.
  - Nicht-Abstreitbarkeit: Subjekte können im Nachhinein keine Handlung abstreiten.
  - Mehrseitige Sicherheit: Einbeziehung der Schutzinteressen aller Beteiligten.
- Sicherheitsziele
  - Funktionssicherheit (safety): realisierte Ist-Funktionalität stimmt mit der spezifizierten Soll-Funktionalität überein (Ist-Funktionalität meist größer, die Differenz ist nicht unbedingt gewollt)
  - Informationssicherheit (security): System nimmt nur solche Systemzustände ein, die zu keiner unautorisierten Informationsveränderung oder -gewinnung führen
  - Datensicherheit (protection): System nimmt nur solche Systemzustände ein, die zu keinem unautorisierten Zugriff auf Systemressourcen, insbes. Daten, führen
  - Datenschutz (privacy): Fähigkeit einer natürlichen Person, die Weitergabe von Informationen, die sie persönlich betreffen, zu kontrollieren (informationelle Selbstbestimmung)
  - Verlässlichkeit (dependability): Funktionssicherheit und es wird gewährleistet, dass die spezifizierte Funktion zuverlässig (reliability) erbracht wird



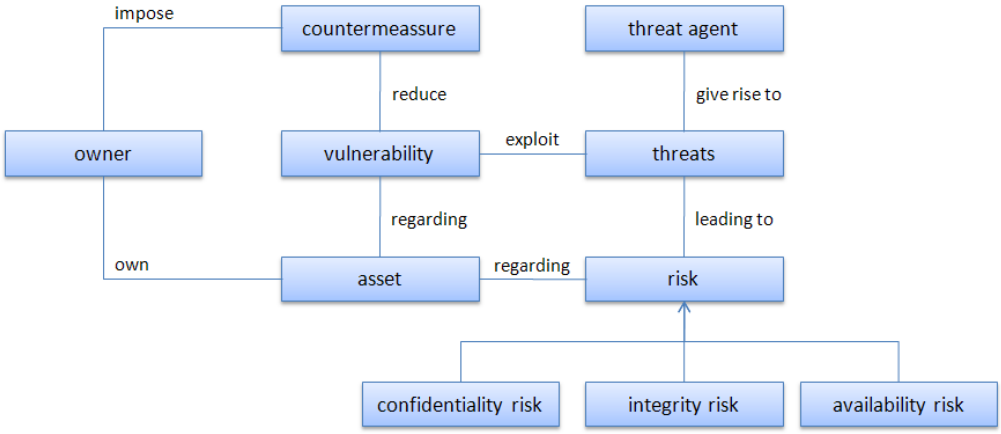
legitimer Informationskanal:
ist existent und darf benutzt werden

verdeckter Informationskanal
(Weitergabe von A oder B an C):
ist existent, darf aber nicht benutzt werden

Risiko: Unter dem Risiko einer Bedrohung verstehen wir die Wahrscheinlichkeit des Eintritts eines Schadensereignisses und die Höhe des potentiellen Schadens, der dadurch hervorgerufen werden kann.



Common Criteria Security Classes



Angriff: einen nicht autorisierten Zugriff(-sversuch) auf das System

- passiver Angriff: unautorisierte Informationsgewinnung, zielen auf den Verlust der Vertraulichkeit ab
- aktiver Angriff: unautorisierte Modifikation von Datenobjekten, richten sich somit gegen die Datenintegrität oder Verfügbarkeit des IT-Systems

1.2 Computeranomalien

Anomalie: System verhält sich abweichend von der zugrundeliegenden Systemspezifikation

Klassifikation

- 1. Art: Leistungen werden unvollständig oder fehlerhaft ausgeführt
  - HW-Fehler
  - SW-Fehler
- 2. Art: mutwillig herbeigeführte (veranlasste) Fehlfunktion
  - Zusatzfunktionen
  - Fehlfunktionen

Schadensfunktionen

- keine Aktion (kein Schadensteil vorhanden): Benutzung von Rechenzeit, Belegung von Speicherplatz
- Aktionen mit transienten Schäden (verschwinden nach der Aktion wieder aus dem Speicher): Spiel-, Spaß- und Demoviren
- Aktionen mit permanenten Schäden (Schaden tritt sofort ein)
- Aktionen mit bedingten permanenten Schäden (Schaden tritt nach Inkubationszeit ein)
  - Trojanisches Pferd in der LOGON Prozedur
  - Reduktion der Verarbeitungsgeschwindigkeit (Erzeugen von simulierten Fehlern und HW-Defekten)
- Logik- und Zeitbomben (Schaden tritt nur unter bestimmten logischen Bedingungen ein): Zusammenspiel von mehreren Viren

Arten von Computer-Anomalien

- Trojanische Pferde (Spoofing-Programme)
  - neben der Erfüllung einer gewünschten und sinnvollen Aufgabe wird eine nicht dokumentierte (unerwünschte) Zusatzfunktion ausgeführt
  - Bekämpfung: Programmauthentifikation (Programm authentisiert sich gegenüber dem Benutzer z.B. mit Hilfe einer kryptografischen Prüfsumme), Code-Inspektion, minimale Rechte
  - gehört zur Fehlerart 2, und nur bei einigen zur Fehlerart 1
- Wurm Programm
  - (über ein Netz) selbst-reproduzierende und eigenständige Programme
  - müssen explizit aufgerufen werden und nutzen Standardmöglichkeiten, die bei einer Vernetzung vorgesehen sind (z. B. remote job entry, interprocess communication, e-mail)
  - Bekämpfung: in jedem System, in dem der Benutzer das Recht besitzt, unkontrolliert Programme aufzurufen, kann er auch einen Wurm starten → Bereitstellung eines abgeschlossenen Spektrums an Programmen
- Viren
  - ein Virus ist ein Programm(-stück), dessen Ausführung bewirkt, dass es sich selbst als Ganzes oder modifizierte Version seiner selbst in ein anderes Programm kopiert
  - Ausbreitungsmechanismus: Erstinfektion folgt durch Programmtausch bzw. Programm-Sharing. Einmal im System, pflanzt sich der Virus im Schneeballverfahren fort, indem nach Aufruf des Wirtsprogramms der Infektionsteil ausgeführt wird.

- Vorbeugung gegen den Virenbefall
  - organisatorische Maßnahmen
    - SW-Beschaffung, SW Einsatz, Erstellung von Backup-Kopien
    - regelmäßige Kontrolle, Sensibilisierung der Anwender
  - Hilfe durch den SW-Hersteller
    - Mitliefern von Prüfsummen, Schreibschutz
    - Selbsttest von Programmen anhand intern gespeicherter kryptographischer Prüfsummen
    - Verwendung von Public Key-Verfahren
  - Einsatz von Virenwächtern, Virenkillern, Killer-Viren, …
  - für Spezialanwendungen
    - Unterbringung des BS auf einem HW-Baustein oder einer WORM (write once, read multiple)
    - Benutzung 2er bootfähiger Disks, Bootvorgang mittels HW-Schalter umschaltbar, gegenseitige Integritätsprüfungen möglich
  - gehört zur Fehlerart 2, und nur bei einigen zur Fehlerart 1
- Trapdoors
  - geheimer, in der Regel nicht autorisierter Zugang zu einem IT-System oder SW-Modul
- Wanze (Bug)
  - eine sich aufgrund eines (Programmier-)Fehlers ergebende Abweichung von der Spezifikation (des Programms) [kann auch in der Hardware liegen]
  - gehört zur Fehlerart 1

1.3 Grundlagen der Kryptologie

Begriffsabgrenzung

- Kryptographie (cryptography): die Wissenschaft von den Methoden, Daten so zu verändern, dass sie nur für autorisierte Personen verständlich sind
- Kryptoanalyse (cryptanalyses): die Wissenschaft von den Methoden zur Bewertung von kryptographischen Verfahren
- Kryptologie (cryptology): die Lehre von den „Geheimschriften“, stellt den Oberbegriff für Kryptographie und Kryptoanalyse dar
- Steganographie: die Lehre der Geheimhaltung der Information durch das Verbergen ihrer Existenz (z.B. Bilder als Informationsträger)

Chiffriersystem (cipher system)

- Das System besteht aus einem Verschlüsselungsalgorithmus (Chiffrieralgorithmus), der die Transformation der ursprünglichen Nachricht (Klartext, plaintext) in eine für Unbefugte nicht verständliche Nachricht (Ciphertext, Chiffrat) vornimmt.
- Diese Transformation (Chiffrierung, encryption) kann genau wie der umgekehrte Vorgang (Dechiffrierung, decryption) von einem Parameter (Chiffrierschlüssel, Dechiffrierschlüssel) gesteuert werden.
- für die Darstellung in Formeln werden im allgemeinen die Abkürzungen der englischen Begriffe verwendet:
  - E für Encryption
  - D für Decryption

  - P für Plaintext
  - C für Ciphertext
  - K für Key
- manche Chiffriersysteme unterscheiden zwischen Chiffrierschlüssel (KE) und Dechiffrierschlüssel (KD)
- Wird der Klartext P unter dem Schlüssel K chiffriert, so stellt sich das Resultat als $C = E_K(P)$ dar. Der Klartext ergibt sich aus der Dechiffrierung von C: $P = D_K(C)$.

Grundprinzipien klassischer Chiffriersysteme

- Transposition: die Zeichen des Klartextes werden nach einem vorgegebenen Schema vertauscht (Permutation des Klartextes), die Zeichen bleiben jedoch unverändert
- Substitution: hierbei werden Zeichen oder Zeichenketten durch andere ersetzt

Sicherheit der Chiffriermethoden

- Einfache Methoden wie Caesar- oder Vigenère-Chiffre können durch einfache Analysen und Aufdecken von Regelmäßigkeiten durch unberechtigte Personen gelöst werden.
- Bei der Substitution geben beibelassene Wortabstände Hinweise auf kurze Wörter, die relativ einfach zu finden sind. Des Weiteren können doppelte Buchstaben, häufige verwendete Buchstbaen sowie Vor- und Nachsilben Hinweise auf den Verschlüsselungsalgorithmus geben.
- Die Chiffriersysteme der heutigen Zeit beruhen auf schwer zu lösenden Problemen und garantieren praktische Sicherheit. Diese ist gegeben, wenn das Chiffriersystem
  - mit den verfügbaren Ressourcen
  - durch die bekannten Angriffe
  - mit vertretbarem Aufwand

  nicht gebrochen werden kann.

Single Key Systeme (Symmetrische Systeme)

- Zwei Personen teilen sich ein und denselben Schlüssel um eine Nachricht verschlüsseln und dann durch den Empfänger der Nachricht wieder entschlüsseln zu können. Wird der Schlüssel geheim gehalten, so kann niemand anderer die Nachricht lesen.
- Probleme
  - Wurde der Schlüssel aufgedeckt, können alle verfügbaren Nachrichten durch nicht autorisierte Personen entschlüsselt werden bzw. ungültige Nachrichten produziert werden.
  - Die Verteilung eines neuen Schlüssels muss unter maximalen Sicherheitsvorkehrungen geschehen (sicherer Kanal).
  - Jeder Teilnehmer kann sowohl ver- als auch entschlüsseln. Er könnte sich daher unter dem Namen seines Partners eine fingierte Nachricht schicken. Dieser hat keine Möglichkeit zu beweisen, dass die Nachricht nicht von ihm stammt. Umgekehrt kann ein Sender nicht beweisen, dass er eine Nachricht abgeschickt hat.
  - Da zwischen allen Personen, welche verschlüsselte Informationen austauschen wollen, eigene Schlüssel existieren müssen, wächst die Anzahl der Schlüssel rapide mit der Anzahl der Personen, welche Nachrichten austauschen.

Public Key Systeme (Asymmetrische Systeme)

- Jeder Benutzer hat einen Schlüssel (public key), der er der Öffentlichkeit zur Verfügung stellt und einen geheimen Schlüssel (private key).

- Der Benutzer kann mit seinem privaten Schlüssel Nachrichten entschlüsseln, welche von einem anderen mit dem public key verschlüsselt wurden. Wird der public key mit k_{pub} und der private key mit k_{priv} bezeichnet, dann gilt: $P = D(k_{priv}, E(k_{pub}, P))$. Damit werden für jeden Benutzer nur noch zwei Schlüssel benötigt.
- Verschickt Benutzer A eine Nachricht mit seinem privaten Schlüssel, so kann die Nachricht von anderen Benutzern mit seinem öffentlichen Schlüssel entschlüsselt werden: $P = D(k_{pub}, E(k_{priv}, P))$.

Die digitale Signatur

- digitale Signaturen sind das elektronische Analogon zur eigenhändigen Unterschrift
- verwirklicht durch kryptographische Verfahren (Hashfunktion und asymmetrische Verschlüsselungsverfahren) und organisatorische Maßnahmen (Zertifikate, Zertifizierungsstellen)

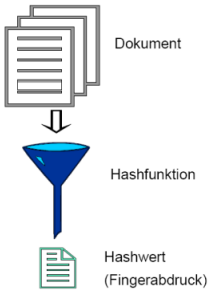
Funktionen der eigenhändigen Unterschrift

- Echtheitsfunktion: das unterzeichnete Dokument hat dem Aussteller vorgelegen und wurde von ihm anerkannt
- Identitätsfunktion: die Unterschrift macht durch ihre Personenabhängigkeit die Identität des Ausstellers deutlich
- Abschlussfunktion: bringt den Abschluss bzw. die Vollendung der Erklärung zum Ausdruck und hebt ihn vom bloßen Entwurf ab
- Warnfunktion: hat den Schutz des Unterzeichners vor Übereilung zum Inhalt und soll ihm die Relevanz des Unterschreiben bewusst machen
- Beweisfunktion: soll dem Träger der Beweislast in einem evtl. folgenden Streitfall die Beweisführung über das Vereinbarte erleichtern

Erfüllt die digitale Signatur diese Funkionen?

- Echtheitsfunktion: Ist erfüllt durch die Abhängigkeit der digitalen Signatur vom Text der Erklärung. Zusätzlich ist bei der digitalen Signatur die Integrität/Unversehrtheit der Daten gewährleistet, da unbefugte Manipulation bei der Übermittlung und Speicherung durch die Signaturprüfung sofort erkannt wird.
- Identitätsfunktion: Ist über ein Zertifikat der Zertifizierungsinstanz gewährleistet. Somit ist eine digitale Signatur personenabhängig.
- Abschlussfunktion: Wird insofern gewährleistet, als nur vorhandene Texte unterschrieben und unterschriebene Texte nicht unbemerkt verändert werden können. Es ist keine Blankounterschrift möglich.
- Warnfunktion: Wird durch die erforderlichen Handlungen im Zusammenhang mit dem Signieren erfüllt. Zu den Handlungen zählen das Bereitstellen einer Chipkarte, das Bestätigen der Funktionstasten sowie das Eingeben einer PIN.
- Beweisfunktion: Hängt von der Qualität und Sicherheit des der Signatur zugrundeliegenden Signaturverfahrens ab. Sind alle anderen vier aufgezählten Funktionen erfüllt, so erwirbt die Unterschrift eine Beweisfunktion.
  → die digitale Signatur ist in Deutschland mittlerweile der eigenhändigen Unterschrift gleichgestellt

Hashfunktionen



- eine Hashfunktion komprimiert einen beliebig langen Bitstring (Dokument mit Text, Bild etc.) auf eine feste Länge
  - Einweg
  - kollisionsresistent
  - Berechnung ist „leicht“
  - beliebig lange Nachricht

Asymmetrische Verschlüsselungsverfahren

- durch asymmetrische Verschlüsselungsverfahren lassen sich die folgenden Funktionen erfüllen:
  - Vertraulichkeit der Nachricht (optional bei digitaler Signatur)
    - A verschlüsselt Dokument mit öffentlichem Schlüssel von B
    - zum Entschlüsseln wird der private Schlüssel von B benötigt
    - nur B kann Dokument entschlüsseln
    - *Vertraulichkeit* durch Einzigartigkeit des privaten Schlüssels
  - Authentizität des Senders (zwingend bei digitaler Signatur)
    - A signiert Dokument mit seinem privaten Schlüssel
    - zum Entschlüsseln wird der öffentliche Schlüssel von A benötigt
    - jeder kann entschlüsseln, aber A ist der einzige, der signieren konnte
    - *Authentizität* durch Einzigartigkeit des privaten Schlüssels

Organisatorische Maßnahmen

- technische Maßnahmen reichen nicht aus, um Digitale Signaturen zu realisieren
- durch Hashwerte und asymmetrische Verfahren wird nur erkannt, mit welchem privaten Schlüssel unterzeichnet wurde
- wie werden Beziehungen zwischen einem Schlüsselpaar und einer Person hergestellt?
  → Lösung: Zertifikate

Zertifikate

- Zertifikat = „digitaler Ausweis“
- stellt den Zusammenhang zwischen dem öffentlichen Schlüssel und einer bestimmten natürlichen oder juristischen Person dar
- beinhaltet Angaben über
  - Name des Zertifikatinhabers
  - öffentlicher Schlüssel des Zertifikatinhabers
  - Authentifikationsalgorithmus des Zertifikatinhabers
  - Name der Zertifizierungsinstanz
  - Gültigkeitszeitraum …
- signiert mit dem privaten Schlüssel der Zertifizierungsstelle

Zertifizierungsstellen

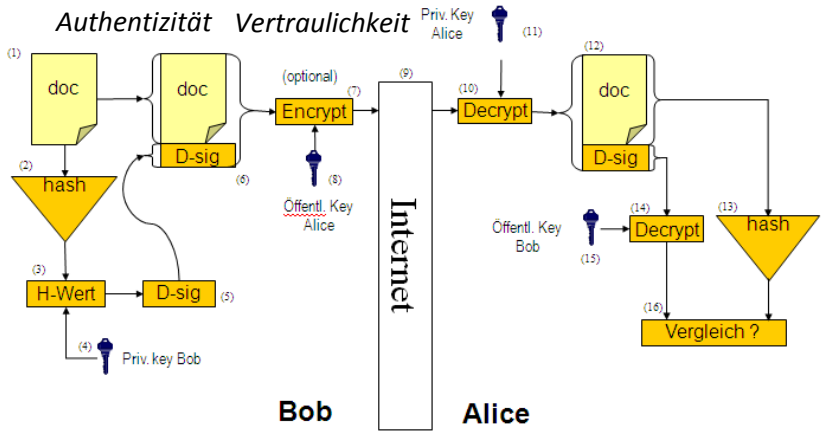
- Zertifizierungsstellen erteilen Zertifikate
- Synonyme: Vertrauenswürdige Stelle, Trust Center, CA (Certification Authority)
- Banken, Behörden oder Unternehmen

- zum Erhalt eines Zertifikates muss die Identität des Antragstellers nachgewiesen werden (z.B. mit Personalausweis)
- in einem Verzeichnis können geltende Zertifikate abgerufen werden
- Zertifikate können auch zurückgerufen werden
  - Ablauf der Gültigkeitsdauer
  - unsicher gewordener Authentifikationsalgorithmus
  - jemand Drittes hat Kenntnis vom geheimen Schlüssel

Digitale Signatur ohne Verlängerung der Nachricht

- gesamte Nachricht wird so transformiert, dass das Ergebnis die digitale Signatur darstellt
- in einem zweiten Schritt wird die Nachricht zur Gewährleistung der Geheimhaltung verschlüsselt
- Vorteile
  - Geheimhaltung der Nachricht ist gewährleistet
  - Vortäuschen einer falschen Identität wird durch zertifizierte Schlüssel verhindert
- Nachteile
  - Verifikation der digitalen Signatur muss immer stattfinden, um an die Nachricht zu gelangen
  - „Shadowing“ muss durchgeführt werden, da sonst Veränderungen der Daten während der Übertragung nicht erkannt werden könnten
  - für die Erzeugung der digitalen Signatur ist das vollständige Dokument zu transformieren, was zu einem beträchtlichen Aufwand führen kann

Digitale Signatur mit Appendix



Signieren	Versenden	Verifizieren
(1) Bob nimmt ein Dokument, (2) wendet an diesem eine Hashfunktion an (3) und erhält einen Hashwert. (4) Dieser wird mit dem privaten Schlüssel von Bob verschlüsselt (5) und Bob erhält die digitale Signatur, (6) welche er an das Dokument anhängt.	(6) Bob nimmt das signierte Dokument, (7) verschlüsselt es (optional) (8) mit dem öffentlichen Schlüssel von Alice (optional) (9) und schickt es über das Internet zu Alice. (10) Alice entschlüsselt das Dokument (optional) (11) mit ihrem privaten Schlüssel (optional) (12) und erhält das signierte Dokument.	(12) Alice nimmt das signierte Dokument, (13) bildet selbst einen Hashwert und (14) entschlüsselt die digitale Signatur (15) mit dem öffentlichen Schlüssel von Bob und erhält Bobs erstellten Hashwert. (16) Als letztes vergleicht sie beide Hashwerte miteinander.

Schlüsselmanagement

- sichere Erzeugung,
- Zertifizierung,
- Speicherung/Archivierung und
- Vernichtung von Schlüsseln

Zertifikat – Aufbau X.508 Standard

- Versionsnummer: beschreibt verwendetes Zertifikatsformat
- Seriennummer: eindeutiger Identifikator
- Signatur: verwendeter Algorithmus und Parameter
- Zertifikatsaussteller: ausstellende Instanz
- Gültigkeitsdauer: Zeitintervall
- Benutzername: eindeutiger Name des Benutzers
- Schlüsselinformationen: Schlüssel des Benutzers und Algorithmen
- eindeutiger Identifikator
- Erweiterungen

Aufgaben der Zertifizierungsstelle

- Schlüsselerzeugung innerhalb einer sicheren Umgebung des Trust Center
- Zertifikaterzeugung: Zertifikate werden mit dem privaten Schlüssel des Trust Center digital signiert
- geeignetes Trägermedium (z.B. Chipkarte): enthält Zertifikat des öffentlichen Schlüssels, öffentlichen Schlüssel des Trust Center, i.d.R. auch privaten Schlüssel des Teilnehmers
- ggf. Schlüsselaufbewahrung (Recovery) und Schlüsselrückgewinnung (Key Escrow)
- ggf. Zeitstempeldienst (bei Zertifikaten nach deutschem Signaturgesetz obligatorisch)

Schlüsselerzeugung

- Schlüssel müssen einzigartig bzw. eindeutig sein
- echte Zufallszahlen sehr schwierig zu erzeugen
- Pseudozufallszahlen berechnet aus einem Startwert (durch natürliche Zufallsereignisse) eine Zahl, deren Entstehung für einen Außenstehenden nicht nachvollziehbar ist

Schlüsselspeicherung

- Problem: Merken der verschiedenen Schlüssel
- Lösung: persönliche Sicherheitswerkzeuge, z.B. Chipkarten, USB-Token
- Zugriff durch Zugangssicherung gesichert, u.a. durch PIN, Biometrie
- ggf. kein direkter Zugriff auf Schlüssel, jedoch Anwendung des Schlüssels
- bei Schlüsselspeicherung im Computer keine Speicherung des Schlüssels im Klartext

Schlüsselvernichtung

- Chip: vollständige Zerstörung des Chips
- Archivierung auf Festplatte oder Hintergrundspeicher: vollständige Bereinigung des Speicherbereichs (Problem: virtueller Speicher)

1.4 Grundfunktionen vertrauenswürdiger Systeme

Grundlagen

- Ein IT-System stellt die Zusammenfassung von Objekten, Subjekten, möglichen Aktionen und Umfeldbedingungen dar.
  - Schutzwürdige Objekte: Informationen, Daten, Maschinen, Prozesse
  - Schutzwürdige Subjekte: Benutzer und die von ihnen initiierten Prozesse
  - Schutzwürdige Aktionen: Abstrakte Handlungen von Subjekten an Objekten
- Sicherheitspolitik: Menge von Regeln, die festlegen
  - gegen welche Bedrohungen das System geschützt werden soll?
  - wie das Systemmodell aussieht (Subjekte, Objekte, Aktionen, Umfeld)?
  - welche Grundsätze und Regeln in puncto Sicherheit in diesem Modell gelten?
  - welche Schutzwürdigkeit Objekte besitzen?
  - welches Restrisiko ein Betreiber akzeptieren kann?

Grundfunktionen

- Identifikation: Bestimmung der Identität eines Subjektes.
- Authentisierung: Nachweis einer angegebenen Identität order Gruppenzugehörigkeit eines Subjektes.
- Rechteverwaltung: Verwaltung der Rechtebeziehung zwischen Subjekten und Objekten.
- Rechteprüfung: Überprüfung ob ein bestimmtes Subjekt die Berechtigung hat, in der beabsichtigten Art auf das gewünschte Objekt zuzugreifen.
- Beweissicherung: Verstöße gegen die Sicherheitspolitik sollten zumindest nachträglich nachgewiesen werden können.

Authentisierung

- Die Authentisierung von Personen kann durch drei unterschiedliche Prinzipien erfolgen:
  - durch Wissen (z.B. Passwort)
  - durch Besitz (z.B. Pass, Ausweis)
  - durch persönliche Eigenschaften (z.B. biometrische Eigenschaften)

Authentifizierungstechniken

- Passwortverfahren
  - Passwörter sind in einem geschützten Bereich oder in verschlüsselter Form zu speichern
  - nach einer bestimmten Anzahl von Fehlversuchen ist eine vordefinierte Aktion zu setzen
  - zur Abwehr von Trojanischen Pferden sollte der zuletzt erfolgreiche bzw. fehlerhafte Versuch angezeigt werden
  - Vorteile: leichte Handhabung, leicht zu implementieren
  - Nachteile: schwer zu merken, Ausprobieren, Beobachten, Maskerade, Trojanische Pferde, Weitergabe erfolgt unbemerkt
- Challenge-Response-Verfahren
  - dem zu authentifizierenden Subjekt wird eine Frage bzw. eine Folge von Fragen (Herausforderung, challenge) gestellt, die es in vordefinierter Art und Weise beantworten (response) muss
  - Beispiel Authentifizierung mittels symmetrischer Verschlüsselung: Beide Kommunikationspartner verfügen über den gleichen, symmetrischen Chiffrieralgorithmus

und über einen gemeinsamen Schlüssel. Die prüfende Stelle B erzeugt eine Zufallszahl, die von der zu authentisierenden Stelle A verschlüsselt und wieder zurückgeschickt wird.
    - Vorteil: für jede Authentisierung wird jeweils ein R zufällig berechnet
- Zero-Knowledge-Verfahren
    - eine Person kann beweisen, dass sie ein Geheimnis kennt, ohne dieses Geheimnis (oder Teile davon) offenzulegen
- Public-Key-Verfahren
    - ein Benutzer weist seine Identität durch die Kenntnis seines geheimen Schlüssels nach
    - die Identifikation kann durch jeden anderen Teilnehmer mittels des öffentlichen Schlüssels von A erfolgen
- Besitzbasierende Verfahren
    - die Authentisierung durch Besitz findet vornehmlich im Bereich der physischen Zutrittskontrolle Anwendung
    - der Benutzer wird nicht als Person sondern als Mitglied einer Gruppe authentisiert
    - die Verfahren genügen keinen hohen Sicherheitsansprüchen, daher werden sie in der Praxis vornehmlich in Kombination mit wissensbasierten und/oder biometrischen Verfahren (Hybridverfahren) eingesetzt.
- Biometrische Verfahren
    - auch der Einsatz von Systemen zur Authentisierung auf Basis persönlicher Eigenschaften konzentriert sich auf den Bereich der physischen Zutrittskontrolle (hauptsächlich auf Hochsicherheitsanwendungen)
    - man unterscheidet zwischen Fehlern 1. Art (false acceptance) und 2. Art (false reject)

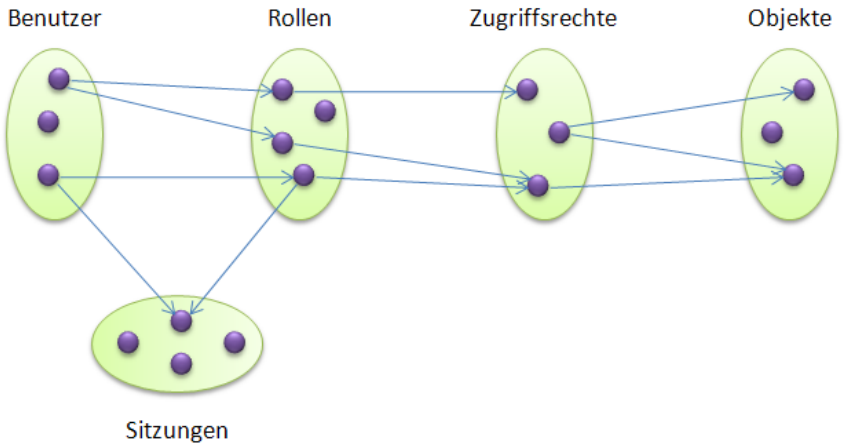
Rechteverwaltung, Rechteprüfung

- Im Anschluss an die Benutzeridentifikation und –authentisierung erfolgt die Zugriffskontrolle und Autorisierung. Dies setzt die Auswahl einer Sicherheitspolitik voraus.
- alle Modelle beinhalten
    - eine Menge von Objekten (passive Elemente)
    - eine Menge von Subjekten (aktive Elemente)
    - eine Menge von Regeln, die die Zugriffsrechte der gegebenen Subjekte auf die gegebenen Objekte definieren

Sicherheitspolitiken

- Diskrete Sicherheitspolitik (Discretionary Access Control, DAC)
    - für jedes Paar (Subjekt, Objekt) ist definiert, ob das Subjekt ein Zugriffsrecht auf das Objekt besitzt und welcher Art ein eventuelles Recht (Privileg) ist
    - die Speicherung erfolgt häufig in Form einer Zugriffskontrollmatrix
- Politik der Schutzklassen (Mandatory Access Control, MAC)
    - Objekte und Subjekte sind mit Sicherheitsstufen ausgestattet
    - ein Subjekt darf auf ein Objekt zugreifen, wenn die Freigabe des Subjektes die Klassifikation der referenzierten Objekte dominiert: $clear(S) \geq class(O)$
- Bell-LaPadula Sicherheitsparadigma
    - vereinigt die beiden zuvor genannten Modelle der Zuständigkeit und der Schutzklassen
    - Schreib-Regel: Schreiben darf ein Subjekt nur dann ein Objekt, wenn die Klassifikation des Objektes mindestens so hoch wie die Freigabe des Subjektes ist

  - die Schreibregel schützt vor unerlaubtem Informationsfluss: wer Zugang zu höher eingestufter Information hat, kann diese nicht in ein niedriger eingestuftes Objekt schreiben
  - BLP richtet sich hauptsächlich gegen den Verlust der *Vertraulichkeit*
- Biba Modell
  - ähnlich zum BLP-Modell, richtet sich jedoch gegen den Verlust der *Integrität*
  - statt Informationsfluss von oben nach unten zu verhindern, soll der Fluss von unten nach oben verhindert werden
- Clark-Wilson Modell
  - basiert auf dem Konzept der wohlgeformten Transaktionen und dem Prinzip der Aufgabentrennung
  - abhängig von der Aufgabe (Rolle) eines Benutzers innerhalb eines Unternehmens sind einem Benutzer Transaktionen zugeordnet
- Chinese Wall Policy
  - berücksichtigt auf welche Objekte ein Subjekt bereits Zugriff hat
  - ein Benutzer baut sich so sukzessive eine Mauer um die von ihm benötigten Datenobjekte auf
  - Beispiel: ein Mitarbeiter einer Beratungsfirme darf nicht zur gleichen Zeit zwei Firmen beraten, die Konkurrenten sind
- Role-Based-Access-Control (RBAC)
  - Berechtigung zur Nutzung geschützter Komponenten direkt an Rollen und damit an Aufgaben geknüpft. Die Aufgaben werden von Subjekten durchgeführt, so dass das Sicherheitsmodell festlegen muss, welche Subjekte welche Aufgaben durchführen.
  - Ein Subjekt darf nur in solchen Rollen aktiv sein, in denen er Mitglied ist.
  - Ein Subjekt nimmt nur Rechte wahr, die in einer Rolle, in der er aktiv ist, zugeordnet sind.
  - Dann muss gelten: Für alle Subjekte, die in einer Sitzung aktiv sind, gilt: es gibt es eine Rolle, die auch zur Sitzung gehört, und beides ist aktiv, und es gilt: es gibt ein Zugriffsrecht, das eine Verbindung zur Rolle hat



Zugriffskontrollmodell

- aufgrund von Zugriffsdaten werden Zugriffsrechte erteilt bzw. entschieden, ob eine Zugriffsanforderung zulässig ist oder nicht (Autorisierung)
- Verwaltung der Zugriffsdaten (Administration), wer darf die Daten lesen bzw. verändern?
  - Eigentümer-Paradigma
  - Administratoren-Paradigma

Beweissicherung (Auditing)

- Protokolle der Beweissicherung enthalten Informationen darüber, welche Subjekte zu welchem Zeitpunkt auf welche Art und Weise auf welche Objekte zugegriffen haben bzw. zuzugreifen versucht haben
  - Ergebnisprotokolle: enthalten Aufzeichnungen der betroffenen Daten vor und nach dem Angriff
  - Ereignisprotokolle: enthalten Aufzeichnungen der Aktionen, die auf Daten ausgeführt werden, sowie Parameter dieser Aktionen
- Art und Umfang der Protokollierung müssen vorab festgelegt werden
- durch Protokollierung können sich datenschutzrechtliche Probleme ergeben, die Protokollierung personenbezogener Daten bedarf der Zustimmung des Betriebsrates

1.5 Standardisierung, Evaluation, Ausblick

Möglichkeiten zur Evaluierung: ein Anwender, der ein sicheres IT-Produkt oder –System einsetzen will, hat folgende Möglichkeiten:

- er glaubt und vertraut den Beteuerungen und Versprechen der Hersteller (Vorsicht!)
- er prüft die Sicherheit der zur Auswahl stehenden IT-Produkte und –Systeme selbst (erhebliche Kosten, Fachwissen)
- Prüfung (Evaluation) und Bescheinigung (Zertifikation) von Sicherheitseigenschaften durch eine (oder mehrere) unabhängige Drittinstanz(en) → ausgestelltes Zertifikat stellt eine Beglaubigung von Sicherheitseigenschaften dar, wodurch auch ohne Preisgabe von vertraulichen Informationen Vertrauen beim Anwender geschaffen werden kann

Sicherheitskriterien

- zur Prüfung und Bescheinigung der Vertrauenswürdigkeit eines IT-Produkts werden entsprechende Sicherheitskriterien (security criteria) als objektive Bewertungsgrundlage benötigt, welche üblicherweise in Form von Kriterienkatalogen publiziert werden

Anmerkungen zu Evaluation und Zertifizierung

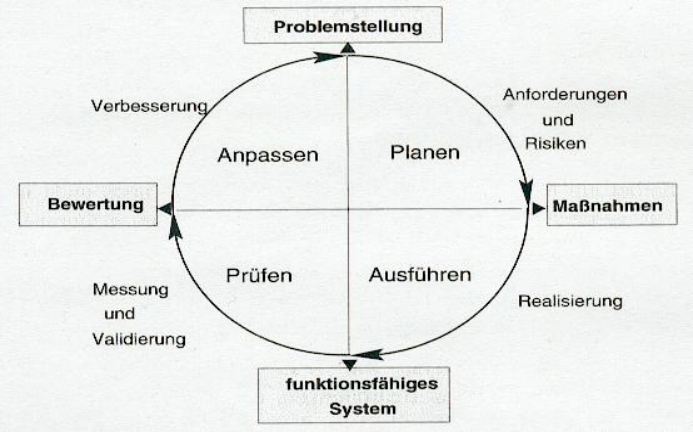
- geringe Zahl zertifizierter IT-Produkte
- bestehende Zertifizierungen zum Teil nicht erneuert
- Zeit- und Kostenaufwendungen
- Wie lange sollen Zertifikate gelten?
- durch den Kauf und den Einsatz von zertifizierten Produkten kann man sich Sicherheit nicht „kaufen“, notwendig ist eine Sicherheitspolitik und ein Sicherheitskonzept
- Kriterienkataloge beruhen zum Teil selbst noch auf umstrittenen Konzepten
- Umsetzung und Einhaltung einer Sicherheitsstrategie und eines entsprechenden –konzepts sind relativ unabhängig von Produkt- oder Systemzertifizierung
- kaum etwas kann gefährlicher und verhängnisvoller sein, als einem Systembetreiber ein subjektives Gefühl von Sicherheit zu vermitteln, das objektiv in keiner Art und Weise gegeben ist

1.6 Security Engineering

Ablauf

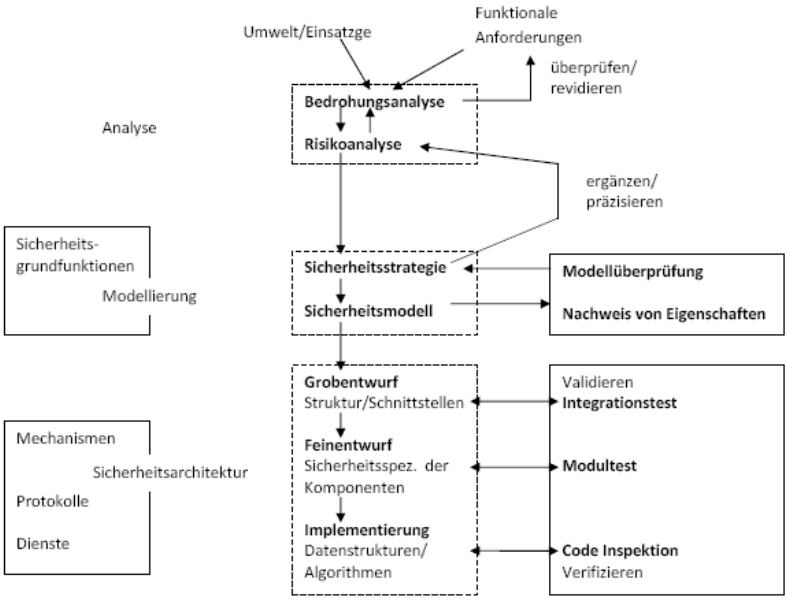
1) Strukturanalyse (Erfassung relevanter Systemeigenschaften)
2) Ermittlung des Schutzbedarfs (z.B. Vertraulichkeit, Integrität, Verfügbarkeit), orientiert sich an Schäden die auftreten können
3) Bedrohungsanalyse
4) Risikoanalyse
5) Sicherheitsstrategien, beschreiben die zu gewährleistenden Sicherheitseigenschaften
6) Sicherheitsarchitektur

Phasenstrukturiertes Vorgehen



- Planungsphase (1.-4.)
  - funktionale Anforderungen
  - Risiken und Bedrohungen ausgehend von der Umgebung
  - Sicherheitsanforderungen formulieren
  - Systemarchitektur entwerfen
- Ausführungsphase (5.-6.)
  - zur Realisierung der Architektur werden Maßnahmen, Dienste und Protokolle benötigt
- Prüfphase (Validation)
- Anpassungsphase
  - Prüfergebnisse → Anforderungen ergänzen, verfeinern, präzisieren → Bedrohungen bzw. deren Bewertungen anpassen oder kostengünstigere Verfahren
- dynamischer, iterierender Prozess der kontinuierlichen Überwachung der Einhaltung der Schutzziele, technologischer Wandel

Entwicklungsphasen



auch Rücksprünge von der Implementierung zur Analyse möglich

analog zum V-Modell

Allgemeine Konstruktionsprinzipien

- Erlaubnisprinzip: grundsätzlich ist verboten was nicht erlaubt ist
- Vollständigkeit: jeder Zugriff ist auf seine Zulässigkeit zu prüfen
- Need-to-know: Prinzip der minimalen Rechte
- Akzeptanz: Benutzerakzeptanz
- Offener Entwurf: no security through obscurity
- Sicherheitskern

Strukturanalyse

- zu erfassen sind:
  - funktionale Eigenschaften (Zuverlässigkeit, Leistungs-, Sicherheitsanforderungen)
  - Einsatzgebiet
  - Verwendungszweck
- Schritte
  1) Netztopologien (Komponenten und deren Vernetzung)
  2) für jede Komponente und jede Verbindung deren Charakteristika festhalten

Schutzbedarfsermittlung

- Zuordnung von Schutzkategorien mittels Schadensszenarien (was wäre wenn…)
- Schutzkategorien
  - niedrig bis mittel: Schadensauswirkungen sind begrenzt und überschaubar
  - hoch: können beträchtlich sein
  - sehr hoch: können existentiell bedrohliches, katastrophales Ausmaß annehmen
- Schadensszenarien
  - Szenario 1: Verstoß gegen Gesetze / Vorschriften / Verträge
  - Szenario 2: Beeinträchtigung der informationellen Selbstbestimmung
  - Szenario 3: Beeinträchtigung der persönlichen Unversehrtheit
  - Szenario 4: Beeinträchtigung der Aufgabenerfüllung
  - Szenario 5: negative Auswirkungen (z.B. Prestigeverlust)

- Szenario 6: finanzielle Auswirkungen

Zwischenfazit

- nachdem der Schutzbedarf ermittelt ist, Mus der Ist-Zustand der IT-Infrastruktur (der herrschende Sicherheitsstandard) bestimmt werden
- außerdem müssen die Defizite zwischen dem Ist- und dem Sollzustand, der dem Schutzbedarf Rechnung trägt, festgestellt werden
- mit einer Bedrohungs- und Risikoanalyse kann man ermitteln, wodurch Schäden potentiell entstehen und wie hoch das Risiko ist, das damit verbunden ist
- in diesem Schritt sind also Ursachen und Randbedingungen für das Eintreten von Schadensfällen zu hinterfragen

Bedrohungsanalyse

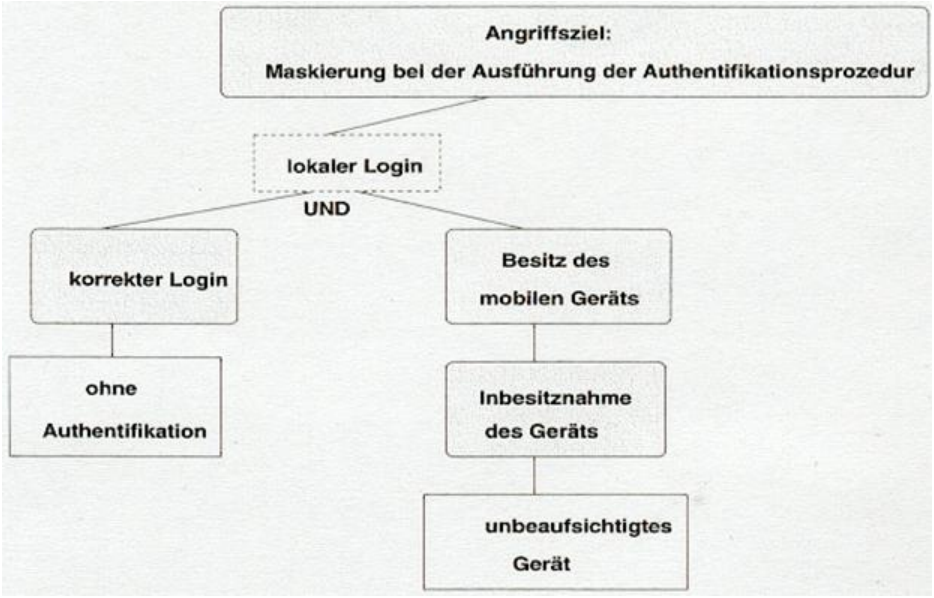
- potentiellen organisatorischen, technischen oder benutzerbedingten Ursachen für Bedrohungen, die Schäden hervorrufen können, sind systematisch zu ermitteln
- Analyseansätze: matrix- oder baumorientiert

Bedrohungsanalyse – Bedrohungsmatrix

Potentieller Auslöser / Gefährdungsbereiche	Programmierer	Interner Benutzer	Externer Benutzer	Mobiler Code
Externe Angriffe	u.a. Vandalismus	Beobachten der Passworteingabe	-	-
Interne Angriffe	Direkter Speicherzugriff	Logische Bomben	Passwort knacken	Viren
Verfügbarkeit	Speicher belegen	Prozesse erzeugen	Netzlast erzeugen	Monopolisieren der CPU

- weitere mögliche Gefährdungsbereiche: DoS, Abstreiten, Rechtemissbrauch
- weitere potentielle Auslöser von Bedrohungen: Dienste, Protokolle, Ausführungsumgebungen

Bedrohungsanalyse – Bedrohungsbaum (Angriffsbaum)



- Wurzel definiert ein mögliches Angriffsziel und damit eine mögliche Bedrohung des Systems
- nächste Ebene: Def. von Zwischenschritten, die zur Erreichung des Gesamtziels beitragen
- Verknüpfung durch UND- bzw. ODER-Knoten
- Blätter beschreiben jeweils einen einzelnen Angriffsschritt
- Pfade von Blättern zur Wurzel beschreiben unterschiedliche Wege zum Erreichen des globalen Angriffsziels an der Wurzel
- auch eine kompaktere, textuelle Darstellung möglich
- Bedrohungsbäume dienen dazu, auf systematische Weise sich die verschiedenen Wege zum Erreichen eines Angriffsziel klar zu machen und nicht nur naheliegende Bedrohungen zu betrachten

Risikoanalyse

- Bewertung der Bedrohungen
  - Wahrscheinlichkeiten für das Eintreten der verschiedenen Bedrohungen
    - geschätzter Aufwand für den Angreifer
    - Einschätzung des möglichen Nutzens für den Angreifer bei erfolgreichem Angriff
    - Einschätzung der möglichen Motive eines Angreifers
  - potentieller Schaden
- Risikobewertung abhängig vom zugrundeliegenden Angreifermodell
  - Angreifertyp (z.B. Skript Kidie, Hacker, Mitarbeiter, Wirtschaftsspion)
  - das zur Verfügung stehende Finanzbudget
  - Kenntnisse des Angreifers (nicht vorhandene – Insider Wissen)
  - Ziele des Angreifers (z.B. Neugier, reines Gewinnstreben, Rache)
- Penetrationstests
  - Simulation des Angriffsverhalten eines vorsätzlichen Innen- oder Außentäters → Ermittlung von Schwachstellen und potenziellen Schäden
  - Whitebox- oder Blackbox-Ansatz
  - Beispiele: Wörterbuchattacken, Aufzeichnen und Manipulieren des Netzverkehrs

Sicherheitsstrategie (security policy)

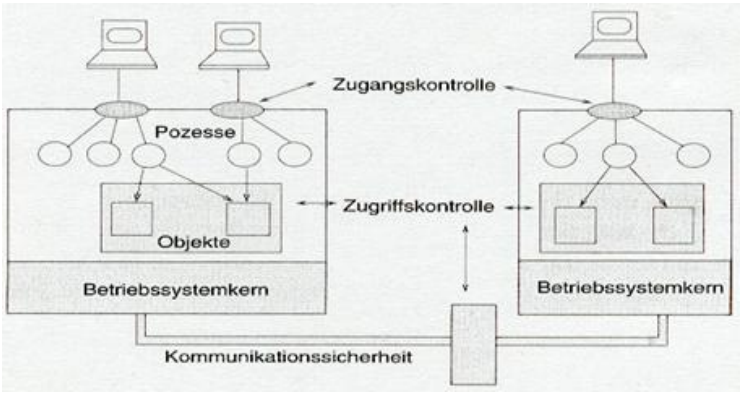
- Definition: Die Sicherheitsstrategie eines Systems oder einer organisatorischen Einheit legt die Menge von technischen und organisatorischen Regeln, Verhaltensrichtlinien, Verantwortungen und Rollen sowie Maßnahmen fest, um die angestrebten Schutzziele zu erreichen.
- Bedrohungs- und Risikoanalyse → Ist-Zustand, Schutzbedarf ist beschrieben im Soll-Zustand
- Maßnahmen sind abzuleiten und zu klassifizieren
- Sicherheitsstrategie muss von der obersten Managementebene verabschiedet, unterstützt und getragen werden → sicherheitsbewusste Unternehmenskultur
- besteht in der Regel aus Kombination von
  - systembestimmenden Anteilen (globale, unternehmensweit geltende Regeln)
  - benutzerbestimmenden Anteilen (erlaubt es Benutzern, die Rechtevergabe für Objekte, die sie erzeugt haben, individuell zu kontrollieren)

Sicherheitsmodell

- ausgehend von der Spezifikation der Sicherheitsanforderungen ist ein Sicherheitsmodell zu konstruieren, das die geforderten funktionalen und sicherheitsbezogenen Eigenschaften auf einem hohen Abstraktionsniveau modelliert
- formales Modell ermöglicht die Eigenschaften des Systems formal nachzuweisen

Sicherheitsarchitektur (Sicherheitsinfrastruktur)

- Definition: Bestandteil einer Gesamtsystem-Architektur, der die festgelegten Sicherheitseigenschaften durchsetzt und die für die Verwaltung der sicherheitsrelevanten Informationen und Konzepte erforderlichen Realisierungsmaßnahmen zur Verfügung stellt.



Validierung

- methodisch testen
  - Testziele, -pläne, -verfahren festlegen und dokumentieren
  - Vollständigkeit der Testszenarien und –abläufe bzgl. der relevanten Problembereiche ist zu begründen
  - Testergebnisse bewerten
  - Modul- und Integrationstest
  - auf Implementierungsebene: Code-Inspektion
- wenn möglich sicherheitsrelevante Funktionen verifizieren

Evaluation

- das implementierte System kann zusammen mit seiner Dokumentation und Einsatzumgebung einer Evaluierung durch Dritte gemäß einem nationalen oder internationalen Kriterienkatalog unterzogen werden
- dem System wird dadurch eine Sicherheitsklassifikation erteilt

Laufender Betrieb

- auch während des laufenden Betriebs ist zu prüfen, ob die verwendeten Sicherheitsmaßnahmen ausreichend sind
  - Monitoring (Beobachten des Systems, DoS)
  - Intrusion Detection Systeme (stellen Einbrüche fest)
  - neue Bedrohungen (dann wieder den gesamten Zyklus durchlaufen)

Teil 2: Datenschutz

Privacy

- drei verschiedene Sichtweisen
  - Privacy vs. öffentlich/allgemein: im Sinne von Fehlen, Getrenntsein, Entferntsein
  - Privacy als das Individuelle: Unabhängigkeit des Individuums, seiner Meinung & Handlungen
  - Privacy als intim/vertraulich: Privatsphäre, Vertrauen, Vertraulichkeit, Intimität
- Anspruch von Individuen, Gruppen oder Institutionen, zu entscheiden, wann, wie und in welchem Ausmaß Informationen über sie verarbeitet und an andere weitergegeben werden

Datenschutz

- Definition: Alle Maßnahmen, deren Ziel es ist, das Individuum (Betroffener) vor der missbräuchlichen (z.B. rechtswidrigen, zweckfremden) Verwendung (Speicherung, Verarbeitung, Weitergabe) der über seine Person gespeicherten Informationen (Daten) zu schützen.
- personenbezogene Daten: Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlich-juristischen Person
- Interessen beider Parteien müssen gegeneinander abgewägt werden; falls das Interesse des Unternehmens überwiegt, ist keine explizit Zustimmung des Betroffenen erforderlich
- untersagt ist die Verarbeitung der folgenden personenbezogenen Daten: rassische oder ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Daten über Gesundheit oder Sexualleben
- grundsätzlich gilt Datenvermeidung und Datensparsamkeit
- Einschränkungen
  - Notwendigkeit zur Vertragserfüllung mit Betroffenen
  - Erfüllung einer gesetzlichen Verpflichtung
  - Wahrnehmung lebenswichtiger Interessen des Betroffenen
  - Wahrnehmung einer Aufgabe im öffentlichne Interesse
- Unterauftragsverhältnisse (Auftraggeber ist verantwortlich)
- Richtlinien: Europäische Datenschutzrichtlinie (gibt Rahmenbedingungen vor), Bundesdatenschutzgesetz (BDSG) (konkretisiert Europ. Richtlinie)

Datenschutzbeauftragter

- Wann ist ein Datenschutzbeauftragter notwendig?

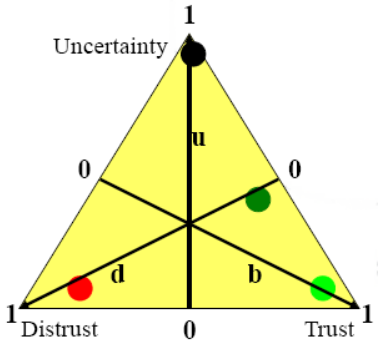
  - öffentliche oder nicht-öffentliche Stellen, die personenbezogene Daten automatisiert erheben, verarbeiten und nutzen oder dafür mindestens 20 Mitarbeiter beschäftigen
  - nicht-öffentliche Stellen haben spätestens innerhalb eines Monats nach Aufnahme ihrer Tätigkeit einen Datenschutzbeauftragen schriftlich zu bestellen
- Aufgabenstellung
  - wirkt auf die Einhaltung der Datenschutzgesetze und anderer Vorschriften hin
- Ausübungsform
  - hauptamtlich (nur bei gewissen Unternehmensgröße), nebenamtlich, extern
- organisatorische Eingliederung
  - gesetzlich festgelegt, dass er dem Vorstand oder der GF direkt unterstellt sein muss
  - Datenschutz ist eine Führungsaufgabe
- arbeitsrechtliche Stellung
  - ist auf seinem Gebiet weisungsfrei und darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden

Teil 3: Gastvortrag Trust Management

Vertrauen aufbauen

- durch Erfahrungsgewinn
  - Beobachten des Verhaltens des Gegenübers
  - Geschäfte mit dem Gegenüber tätigen
  - Testen des Gegenübers (durch kleine Fallen)
- durch Empfehlungen Dritter
  - jedoch: kann man dem Dritten vertrauen?

Vertrauensmodell Opinion Triangle



- 3 Intervalle [0,1]
- Triple b (belief, trust), d (disbelief, distrust), u (uncertainty)
- constraint: b + d + u = 1
- verschiedene Metriken von Josang/Knapskog und Beth/Borcherding/Klein entwickelt