IT-Sicherheit und Datenschutz

Kursüberblick - Geplante Themen

- Zugriffskontrolle (ZK) – Betriebssystem-ZK, obligatorische ZK, diskretionäre ZK, rollenbasierte ZK, attributbasierte ZK, Nicht-Interferenzen, Integritätsschutz, Firewall-Policiesprachen, ZK in Datenbanken, ZK in mobilen Systemen, ZK im Web
- Verwendung von Krypto zur Datensicherheit – Implementierung von Krypto korrekt, Authentifizierungsprotokolle, Homomorphe Verschlüsselung, sichere Mehrparteienberechnung – Verwendung von SGX und Hardware-Sicherheitsarchitekturen
- Datenschutz – Datenschutzrichtlinien, Datenanonymisierung (k-Anonymität, t-Nähe, l-Diversität), differentielle Privatsphäre: Konzepte und Algorithmen, differentielle Privatsphäre in der lokalen Umgebung, Mitgliedschaftsprivatsphäre

Beziehung zu anderen Sicherheitskursen

- Erfordert grundlegende Kenntnisse aus
  - Informationssicherheit
  - Kryptografie

- Geringe Überlappung mit
  - Software-Sicherheit
  - Netzwerksicherheit
  - Sozioökonomische und rechtliche Aspekte der Sicherheit
  - Sicherheitsanalytik

Kurs Logistik

- Zeit: Mo – Do 8:30 – 16:15
  Fr 8:30 – 12:00

- Dozent: Costis Aivalis
  costis.aivalis@gmail.com,
  Teams: aivalisco

- Webseite: https://aivalis.eu

Lesematerialien

- Kein erforderliches Lehrbuch, Lesematerial wird auf der Kurswebseite angekündigt/verteilt.
- Lesematerial für diese Vorlesung: – Teil 1A von Saltzer und Schroeder: "Der Schutz von Informationen in Computersystemen".
- Prüfung: Quiz am Freitag

Einige Datenlecks

- Equifax 2017
- Anthem 2015
- Target 2014
- Yahoo 2014
- Adobe 2013
- Dropbox 2012

Equifax 2017 (1/2)

Das Datenleck bei Equifax im Jahr 2017 war einer der größten Sicherheitsvorfalls in der Geschichte und betraf Millionen von Menschen weltweit. Equifax ist eine der drei großen US-amerika-nischen Auskunfteien, die sensible finanzielle Informationen von Verbrauchern sammeln und verwalten. Das Datenleck wurde im September 2017 öffentlich bekannt gegeben und hatte schwer-wiegende Auswirkungen auf Millionen von Verbrauchern.

Die Hacker hatten über einen Zeitraum von mehreren Monaten Zugriff auf die Systeme von Equifax und erlangten dabei Zugriff auf eine Fülle sensibler persönlicher Informationen, darunter Namen, Sozialversicherungsnummern, Geburtsdaten, Adressen und teilweise auch Kreditkarteninformationen von rund 147 Millionen Menschen. Dies machte das Datenleck zu einem der größten und schwerwiegendsten in der Geschichte der Datenverletzungen.

Equifax 2017 (2/2)

Das Unternehmen wurde stark kritisiert, weil es bekannt wurde, dass Equifax bereits Monate vor der öffentlichen Bekanntgabe des Vorfalls von der Sicherheitsverletzung wusste, aber nicht angemessen darauf reagierte. Zudem wurden Schwachstellen in der Sicherheitsarchitektur des Unternehmens und in seinen internen Prozessen aufgedeckt.

Die Auswirkungen des Equifax-Datenlecks waren weitreichend und führten zu einer erhöhten Sensibilisierung für Datenschutz- und Sicherheitsfragen. Es löste auch eine Debatte über die Verant-wortlichkeit von Unternehmen für den Schutz sensibler Verbraucherdaten aus und führte zu Forderungen nach strengeren Regulierungen und höheren Sicherheitsstandards für Unternehmen, die personenbezogene Daten verarbeiten.

Anthem 2015 (1/2)

Das Datenleck bei Anthem im Jahr 2015 war einer der größten Datenschutzverletzungen im Gesundheitswesen und betraf Millionen von Versicherten. Anthem Inc. ist eine der größten Kranken-versicherungs-gesellschaften in den USA und verwaltet sensible per-sönliche Gesundheits-informationen von Millionen von Menschen.

Im Februar 2015 gab Anthem bekannt, dass es Opfer eines massiven Cyberangriffs geworden war. Unbekannte Angreifer hatten Zugriff auf die Systeme des Unternehmens erhalten und dabei umfangreiche Mengen an persönlichen Daten erbeutet. Zu den gestohlenen Informationen gehörten Namen, Geburtsdaten, Sozialversicherungsnummern, Adres-sen, Mitgliedschaftsdaten sowie einige medizinische Informationen von bis zu 80 Millionen Versicherten und Mitarbeiter.

Anthem 2015 (2/2)

Das Datenleck wurde als äußerst besorgniserregend angesehen, da die gestohlenen Informationen äußerst sensibel waren und eine Vielzahl von persönlichen Daten umfassten, die für Identitätsdiebstahl und andere betrügerische Aktivitäten genutzt werden können.

Anthem reagierte auf den Vorfall, indem es die betroffenen Personen über das Datenleck informierte und kostenlose Kreditüberwachungsdienste sowie Identitätsschutzmaßnahmen anbot. Das Unternehmen arbeitete auch mit Strafverfolgungsbehörden und Sicherheitsexperten zusammen, um den Vorfall zu untersuchen und die Sicherheitsmaßnahmen zu verbessern.

Das Anthem-Datenleck führte zu einer verstärkten Sensibilisierung für die Sicherheit von Gesundheitsdaten und zu Forderungen nach strengeren Sicherheitsmaßnahmen im Gesundheitswesen, um die Vertraulichkeit und Integrität sensibler medizinischer Informationen zu gewährleisten.

Target 2014 (1/3)

Das Datenleck bei Target im Jahr 2014 war einer der größten und bemerkenswertesten Sicherheitsvorfälle im Einzelhandel. Target ist eine große US-amerikanische Einzelhandelskette, die von Millionen von Kunden besucht wird und eine Vielzahl von Produkten verkauft.

Im Dezember 2013 und Januar 2014 wurden die Systeme von Target Opfer eines Cyberangriffs. Unbekannte Hacker hatten Malware in das Point-of-Sale-System von Target eingeschleust, das dazu dient, Zahlungsinformationen von Kunden zu verarbeiten. Die Malware erfasste die Daten von Kredit- und Debitkarten von Kunden, die beim Einkauf in den Geschäften von Target verwendet wurden.

Target 2014 (2/3)

Das Ausmaß des Datenlecks war beträchtlich. Über 40 Millionen Kredit- und Debitkarteninformationen wurden gestohlen, und persönliche Daten von bis zu 70 Millionen Kunden, darunter Namen, Adressen, Telefonnummern und E-Mail-Adressen, waren ebenfalls betroffen.

Die Auswirkungen des Target-Datenlecks waren weitreichend. Kunden verloren das Vertrauen in die Sicherheit ihrer Zahlungsinformationen und des Einkaufserlebnisses bei Target. Das Unternehmen erlitt erhebliche finanzielle Verluste, darunter Kosten für die Untersuchung des Vorfalls, Entschädigungen für betroffene Kunden und Schadensersatzforderungen.

Target 2014 (3/3)

Das Target-Datenleck führte zu einer verstärkten Sensibilisierung für die Sicherheit von Zahlungsinformationen und dem Schutz personenbezogener Daten im Einzelhandel. Es verdeutlichte auch die Notwendigkeit für Unternehmen, proaktiv Sicherheits-maßnahmen zu ergreifen, um sich vor Cyberangriffen zu schützen und die Privatsphäre ihrer Kunden zu wahren.

Yahoo 2004 (1/3)

Das Datenleck bei Yahoo im Jahr 2014 war eine der größten und schwerwiegendsten Sicherheitsverletzungen in der Geschichte des Internets. Yahoo war zu dieser Zeit einer der größten Internet-dienstleister und bot eine Vielzahl von Diensten an, darunter E-Mail, Nachrichten, Finanzen und vieles mehr.

Im September 2016 gab Yahoo bekannt, dass es Opfer eines massiven Datenlecks geworden war, das bereits zwei Jahre zuvor, im Jahr 2014, stattgefunden hatte. Die Angreifer hatten sich Zugang zu den Systemen von Yahoo verschafft und gestohlene Daten von mindestens 500 Millionen Nutzerkonten erbeutet. Diese Daten umfassten Namen, E-Mail-Adressen, Telefonnummern, Geburtsdaten, verschlüsselte Pass-wörter und in einigen Fällen auch Sicherheitsfragen und -antworten.

Yahoo 2004 (2/3)

Das Ausmaß des Yahoo-Datenlecks war enorm und führte zu weitreichenden Konsequenzen. Es war eines der größten Datenlecks, das jemals bekannt wurde, und betraf eine riesige Anzahl von Nutzern weltweit. Die gestohlenen Daten konnten für Identitätsdiebstahl, Phishing-Angriffe und andere betrügerische Aktivitäten genutzt werden.

Das Datenleck hatte auch erhebliche Auswirkungen auf die Reputation von Yahoo. Das Unternehmen geriet in die Kritik, weil es nicht rechtzeitig über den Vorfall informierte und Schwächen in seinen Sicherheitssystemen aufzeigte. Die Offenlegung des Vorfalls führte zu einer Untersuchung durch Behörden und zu rechtlichen Konsequenzen für das Unternehmen.

Yahoo 2004 (3/3)

Das Yahoo-Datenleck verdeutlichte die Bedeutung von robusten Sicherheitsmaßnahmen und einer proaktiven Herangehensweise an den Schutz sensibler Benutzerdaten. Es unterstrich auch die Notwendigkeit für Unternehmen, transparent über Sicherheits-vorfälle zu informieren und angemessene Maßnahmen zum Schutz der Privatsphäre ihrer Nutzer zu ergreifen.

Adobe 2013

Das Adobe-Datenleck im Jahr 2013 war eines der größten Sicherheits-vorfälle in der Geschichte des Unternehmens. Dabei wurden ver-trauliche Informationen von Millionen von Adobe-Benutzern kompromittiert. Die gestohlenen Daten umfassten persönliche Benutzerdaten wie Namen, Passwörter, E-Mail-Adressen, Kredit-kartendaten und verschlüsselte Passwörter.

Dies führte zu erheblichen Bedenken hinsichtlich der Privatsphäre und Sicherheit der betroffenen Benutzer. Adobe gab bekannt, dass Hacker Zugriff auf ihre internen Netzwerke erlangt hatten und die Daten von bis zu 38 Millionen Kunden gestohlen wurden. Die Auswirkungen dieses Vorfalls waren weit-reichend und führten zu einer verstärkten Sensibilisierung für die Notwendigkeit besserer Sicherheitsmaßnahmen bei großen Unter-nehmen.

Dropbox 2012

Das Dropbox-Datenleck ereignete sich im Jahr 2012 und führte zur Kompromittierung von Benutzerdaten. Bei diesem Vorfall wurden die Anmeldeinformationen von rund 68 Millionen Dropbox-Konten gestohlen. Die gestohlenen Daten enthielten E-Mail-Adressen und mit gehashten Pass-wörtern, was bedeutet, dass sie in einer verschlüsselten Form gespeichert waren.

Dennoch bestand das Risiko, dass Angreifer versuchen könnten, die Passwörter zu entschlüsseln oder auf andere Weise auf die Konten zu-zugreifen. Dropbox reagierte schnell auf den Vorfall, setzte betroffene Benutzer zurück und forderte sie auf, ihre Pass-wörter zu ändern. Das Unternehmen informierte die betroffenen Benutzer über den Vorfall und ergriff Maßnahmen, um die Sicherheit seiner Plattform zu verbessern und zukünftige Datenschutzverletzungen zu verhindern. Das Dropbox-Datenleck unterstreicht die Bedeutung von robusten Sicherheitsmaßnahmen und die Notwendigkeit, die persönlichen Daten der Benutzer angemessen zu schützen.

Einige Datenschutzvorfälle (Privacy)

- Sony CD-Spyware
- Samsung Smart-TV-Schnüffelei
- Und viele mehr

Sony CD-Spyware (1/2)

Das Sony CD-Spyware-Skandal ereignete sich im Jahr 2005, als es entdeckt wurde, dass Sony BMG Musik-CDs eine Art von DRM-Software (Digital Rights Management) enthielten, die als "Extended Copy Protection" (XCP) bekannt ist. Diese Software wurde auf CDs installiert, um die illegale Vervielfältigung von Musik zu verhindern, aber sie ging weit darüber hinaus und griff in die Systeme von Benutzern ein, ohne deren Zustimmung oder Wissen.

Die XCP-Software wurde als Rootkit implementiert, was bedeutet, dass sie sich tief in das Betriebssystem des Computers einbettete und bestimmte Dateien und Prozesse verbarg, um sich vor Entdeckung zu schützen. Viele Benutzer waren sich nicht bewusst, dass ihre Computer mit dieser Software infiziert waren, da sie im Hintergrund lief und sich selbst vor den meisten Sicherheitsprogrammen verbarg.

Sony CD-Spyware (2/2)

Der Skandal brach aus, als Sicherheitsexperten herausfanden, dass die XCP-Software nicht nur als DRM fungierte, sondern auch die Sicherheitslücken des Systems ausnutzte, um sich vor Entfernung zu schützen und persönliche Daten der Benutzer an Sony zurückzusenden. Darüber hinaus entdeckten einige Experten, dass die Software die Stabilität und Sicherheit der Systeme beeinträchtigen konnte, auf denen sie installiert war.

Die Entdeckung führte zu weitreichender Kritik von Verbrauchern, Datenschutzaktivisten und der technischen Gemeinschaft. Sony BMG wurde beschuldigt, die Privatsphäre der Benutzer zu verletzen, illegale Softwarepraktiken anzuwenden und Sicherheitsrisiken zu schaffen. Das Unternehmen zog schließlich die betroffenen CDs zurück, veröffentlichte Entfernungsprogramme für die XCP-Software und stimmte einer Entschädigungsregelung für betroffene Benutzer zu. Der Vorfall unterstreicht die Bedeutung von Transparenz, ethischen Geschäftspraktiken und dem Schutz der Privatsphäre der Benutzer in der digitalen Welt.

Samsung Smart-TV-Schnüffelei (1/2)

Die Samsung Smart-TV-Schnüffelei bezieht sich auf einen Vorfall im Jahr 2015, als bekannt wurde, dass Samsung Smart-TVs dazu in der Lage waren, Gespräche im Raum aufzuzeichnen und möglicherweise sensible Informationen an Dritte zu senden. Diese Funktion war Teil einer Sprach-erkennungssoftware, die es Benutzern ermöglichte, mit ihrem Fernseher zu interagieren, indem sie Sprachbefehle verwendeten, um den Fernseher zu steuern oder auf bestimmte Funktionen zuzugreifen.

Es wurde entdeckt, dass die Smart-TVs von Samsung kontinuierlich Audio aufzeichneten, auch wenn die Benutzer nicht aktiv mit dem Fernseher interagierten. Diese aufgezeichneten Audiodaten wurden dann über das Internet an Drittanbieterunternehmen gesendet, die für die Spracherkennung und -verarbeitung zuständig waren. Das Problem lag darin, dass die Benutzer nicht ausreichend darüber informiert wurden, dass ihre Gespräche möglicherweise aufgezeichnet und an externe Server gesendet wurden.

Samsung Smart-TV-Schnüffelei (2/2)

Die Offenlegung dieser Praxis löste erhebliche Bedenken hinsichtlich der Privatsphäre und Sicherheit von Verbrauchern aus. Die Vorstellung, dass ein Fernseher im Wohnzimmer Gespräche mithört und potenziell sensible Informationen aufzeichnet, wurde von vielen als Eingriff in die Privatsphäre empfunden. Darüber hinaus war die Sorge groß, dass die aufgezeichneten Daten in die falschen Hände geraten könnten oder für unethische Zwecke missbraucht werden könnten.

Nach Bekanntwerden des Vorfalls reagierte Samsung, indem das Unternehmen betonte, dass die Spracherkennungsfunktion optional sei und dass Benutzer die Möglichkeit hätten, sie jederzeit zu deaktivieren. Außerdem versprach das Unternehmen, seine Datenschutzrichtlinien zu überarbeiten und transparenter über die Funktionsweise seiner Smart-TVs zu informieren. Der Vorfall unterstreicht die zunehmende Notwendigkeit, die Datenschutzpraktiken und die Transparenz von Unternehmen zu überwachen, insbesondere im Zusammenhang mit vernetzten Geräten und dem Internet der Dinge (IoT).

AOL-Datenfreigabe [NYTimes 2006]

• Im August 2006 veröffentlichte AOL-Suchschlüsselwörter von 650.000 Benutzern über einen Zeitraum von 3 Monaten.

- Benutzer-IDs wurden durch Zufallszahlen ersetzt.
- 3 Tage später wurde die Daten aus öffentlichem Zugriff zurückgezogen.

AOL-Datenfreigabe

AOL searcher # 4417749
"landscapers in Lilburn, GA" *queries on last name "Arnold"* *"homes sold in shadow lake subdivision Gwinnett County, GA"* *"num fingers"* *"60 single men"* *"dog that urinates on everything"*

NYT

Thelman Arnold, a 62 year old widow who lives in Liburn GA, has three dogs, frequently searches her friends' medical ailments.

Eine Neuidentifizierung tritt auf!

NYTimes: [A Face Is Exposed for AOL Searcher No. 4417749]

AOL-Datenfreigabe

- Benutzer 927:

  Laut Consumerist ist "Benutzer 927" ein Thriller über Cyber-Stalking, Suchmaschinen und die Art und Weise, wie Informationen in unserer vernetzten Welt beschafft, manipuliert und veröffentlicht werden.

  Das klingt passend, wenn man bedenkt, dass die realen Suchanfragen von Benutzer 927 von "Die Schöne und das Biest Disney-Porno" über "Holocaust-Vergewaltigung" bis hin zu "Oh, das mag ich, Baby. Ich ziehe meinen Umhang und meinen Zaubererhut an." reichten.

  https://www.businessinsider.com/aol-user-927s-entire-sordid-search-log

AOL-Datenfreigabe

- Das Minimovie “I Love Alaska” von Lernert Engelberts und Sander Plug enthüllt die traurige Such-Geschichte von user #711391…

Minimovies in Youtube: I Love Alaska

https://youtu.be/c-SOCGdPyNU?si=s2LiuApE-wr-KyCc

Michael Zimmer Director of the Center for Data, Ethics, and Society at Marquette University.

Was ist Informationssicherheit (Computersicherheit)?

Sicherheit = Aufrechterhaltung wünschenswerter Eigenschaften unter intelligenten Gegnern

Das Präzisieren des Obigen erfordert das Präzisieren der folgenden beiden Punkte:

- Wünschenswerte Eigenschaften
  - Verstehen, welche Eigenschaften benötigt werden.
- Intelligente Gegner
  - Muss Gegner verstehen/modellieren
  - Denken Sie immer an Gegner.

Sicherheitsziele/-Eigenschaften (C, I, A)*

- **Vertraulichkeit** (Geheimhaltung, Datenschutz)
  – Nur diejenigen, die dazu autorisiert sind, dürfen es wissen.
- **Integrität** (auch Echtheit in der Kommunikation)
  – Nur von autorisierten Parteien und auf erlaubte Weise verändert
  – Tun Sie Dinge, die erwartet werden.
- **Verfügbarkeit**
  – Diejenigen, die autorisiert sind, Zugriff zu erhalten, können Zugriff erhalten.

*(C, I, A) Confidentiality, Integrity, Availability

Was ist Datenschutz?

Es ist kompliziert! Datenschutz ist in erster Linie ein soziales und rechtliches Konzept.

Einige Konzepte aus dem Buch "***Understanding Privacy***" von Daniel J. Solove:

1. Das Recht, in **Ruhe** gelassen zu werden
2. Begrenzter **Zugang** zur eigenen Person
3. Geheimhaltung – die **Verheimlichung** bestimmter Angelegenheiten vor anderen;
4. Kontrolle über die **Nutzung von Informationen** über sich selbst durch andere
5. Personhood (**Personsein**) – der Schutz der eigenen Persönlichkeit, Individualität und Würde;
6. Intimität – **Kontrolle** über oder begrenzter Zugang zu eigenen intimen Beziehungen oder Aspekten des Lebens.

Sicherheit ist sekundär

- Welche Schutz-/Sicherheitsmechanismen hat man in der physischen Welt?
- Warum entsteht der Bedarf an Sicherheitsmechanismen?
- Sicherheit ist sekundär zu den Interaktionen, die Sicherheit notwendig machen.

> Robert H. Morris: Die drei goldenen Regeln zur Gewährleistung der Computersicherheit sind: (1) Besitze keinen Computer; (2) Schalte ihn nie ein; und (3) Benutze ihn nicht.

Informationssicherheit ist interessant

- Die interessantesten/herausforderndsten Bedrohungen für die Sicherheit werden durch menschliche Gegner dargestellt
  – Sicherheit ist schwieriger als Zuverlässigkeit
- Informationssicherheit ist ein selbsttragendes Gebiet
  – Kann sowohl aus Angriffsperspektive als auch aus Verteidigungsperspektive funktionieren
- Sicherheit handelt von Nutzen/Kosten-Abwägung
  – Oft ist die Abwägungsanalyse jedoch nicht explizit
- Sicherheit ist nicht ausschließlich technologisch
  – Menschen sind oft das schwächste Glied

Informationssicherheit ist herausfordernd

- Verteidigung ist fast immer schwieriger als Angriff.
- In welcher Weise ist Informationssicherheit schwieriger als physische Sicherheit?
  - Gegner können aus jeder Richtung kommen
  - Computer ermöglichen eine groß angelegte Automatisierung
  - Gegner können schwer zu identifizieren sein
  - Gegner können schwer zu bestrafen sein
  - Potenzielle Auszahlung kann viel höher sein
- In welcher Weise ist Informationssicherheit einfacher als physische Sicherheit?

Was ist Zugriffskontrolle?

- Zitat aus "Security Engineering" von Ross Anderson

– Ihre Funktion besteht darin zu steuern, welche Prinzipien (Personen, Prozesse, Maschinen, ...) Zugriff auf welche Ressourcen im System haben --- welche Dateien sie lesen können, welche Programme sie ausführen können und wie sie Daten mit anderen Prinzipien teilen usw.

Zugriffskontrolle ist allgegenwärtig

- **Anwendung**
  - Geschäftsanwendungen
- **Middleware**
  - Datenbankmanagementsysteme
- **Betriebssystem**
  - Kontrolle des Zugriffs auf Dateien, Ports
- **Hardware**
  - Speicherschutz, Privilegienlevel

Zugriffskontrolle ist wichtig

- Zitat aus "Security Engineering"
  – Zugriffskontrolle ist das traditionelle Schwergewicht der Computersicherheit. Hier treffen sich Sicherheitstechnik und Informatik.
- Das TCSEC* bewertet die Sicherheit von Computersystemen basierend auf Zugriffskontrollfunktionen + Gewährleistung.

* Das Trusted Computer System Evaluation Criteria (1983-1999), besser bekannt als ***Orange Book***, war die erste Haupt-Computer-Sicherheitsbewertungs Methodologie.

Zugriffskontrolle ist interessant

- Hat (relativ) gut entwickelte Theorien
  - Über 30 Jahre Geschichte
  - Einige (ziemlich komplexe) Theorien sind anscheinend für andere Bereiche nicht nützlich
- Viele interessante und tiefgreifende Ergebnisse
- Viele Missverständnisse und Debatten
- Ein großer Prozentsatz der veröffentlichten Arbeiten enthält ernsthafte Fehler
  - Korollar: Seien Sie skeptisch, glauben Sie nicht zu sehr, was andere gesagt haben, versuchen Sie, sich Ihre eigenen Meinungen zu bilden

Prinzipien der Sicherheit/Zugriffskontrolle (Saltzer und Schroeder 75)

1. Ökonomie des Mechanismus
   - Halten Sie das Design so einfach und klein wie möglich.
2. Fail-Safe-Standards
   - Standard ist kein Zugriff

Prinzipien der Sicherheit/Zugriffskontrolle

3. Vollständige Mediation
   – Jeder Zugriff muss überprüft werden.
4. Offenes Design
   – Die Sicherheit hängt nicht von der Geheimhaltung des Mechanismus ab.

Prinzipien der Sicherheit/Zugriffskontrolle

5. Trennung von Privilegien
   – Ein System, das zwei Schlüssel erfordert, ist robuster als eines, das nur einen Schlüssel erfordert.
6. Minimales Privileg
   – Jedes Programm und jeder Benutzer sollte mit den minimalen erforderlichen Privilegien arbeiten.

Prinzipien der Sicherheit/Zugriffskontrolle

7. Minimaler gemeinsamer Mechanismus
   – "Minimieren Sie die Menge des Mechanismus, der mehr als einem Benutzer gemeinsam ist und von allen Benutzern abhängt."
8. Psychologische Akzeptanz
   – "Die menschliche Schnittstelle sollte für die Benutzerfreundlichkeit ausgelegt sein."
   – Das mentale Bild des Benutzers seiner Schutzziele sollte mit dem Mechanismus übereinstimmen.

Eine unvollständige Geschichte der Zugriffskontrollforschung

Frühere Jahre: Zeit-Sharing-Betriebssysteme

- Referenzmonitor (1972)
- Zugriffsmatrix (1971)
- Diskretionäre Zugriffskontrolle
  – Trojanisches Pferd kann Informationen preisgeben

Vertraulichkeit

- Bell-LaPadula-Modell (No read up, No write down)
- Nicht-Interferenz (1982)
- Nichtableitbarkeit (1986)
- Verdeckter Kanal
- Beweisen von Informationsflusseigenschaften von Systemen und Programmen

Integrität

- Biba-Modell
- Clark-Wilson
- Chinesische Mauer

Datenbankzugriffskontrolle

- Ansatz von System R: gewähren/entziehen, Ansicht (grant/revoke, view)
- Ansatz von Ingres (Anfragenumformulierung)
- Mehrstufige Datenbanken
- Objekt-/relationale Datenbanken
- Reale Systeme
  - SQL gewähren/entziehen, Ansicht, gespeicherte Prozeduren, feingranulare Zugriffskontrolle
- Privatsphärenzentriert

Rollenbasierte Zugriffskontrolle

- Zuerst im Datenbankkontext
- Dann ein generischer Zugriffssteuerungsansatz
- Einschränkungen
- Administration
- Erweiterungen

Zugriffskontrolle in verteilten Systemen

- ABLP-Logik
- Vertrauensmanagement
  - PolicyMaker, KeyNote, QCM/SD3, Delegationslogik, Binder, RT
- Automatisierte Vertrauensverhandlung

Andere Bereiche

- Workflow-Systeme
- Firewall
- Mobile Systeme

Lesematerialien zum Thema

- Saltzer und Schroeder. Der Schutz von Informationen in Computersystemen

The Protection of Information in Computer Systems