Universität Zürich[UZH]

Institut für Informatik

IT-Sicherheit: Bedrohungen

Vorlesung: Wirtschaftsinformatik 1, Frühjahrssemester 2020

Lerneinheit 8

Prof. Dr. Lorenz Hilty

hilty@ifi.uzh.ch

Gliederung

1. **Schutzziele der IT-Sicherheit**
2. Arten von Bedrohungen
3. Schadsoftware und Angriffsarten
4. Risiken für „Industrie 4.0“ und Internet of Things

Klassische Schutzziele

- **Verfügbarkeit (availability):**
  Die Informationen, die ein IT-System zur Verfügung stellt, sind für Berechtigte jederzeit zugänglich.
- **Vertraulichkeit (confidentiality):**
  Der Nachrichteninhalt sowie die Identität des Senders, Empfängers und das Stattfinden der Kommunikation an sich sind nur Personen bekannt, die dazu berechtigt sind. Entsprechendes gilt für gespeicherte Daten.
- **Integrität (integrity):**
  Der Inhalt einer Nachricht bzw. gespeicherte Daten sind vollständig und unverändert.

Entsprechend umfasst **IT-Sicherheit** die Summe der Massnahmen, die die Verfügbarkeit von IT-Systemen gewährleisten und den unberechtigten Zugriff sowie die unberechtigte Veränderung von Daten verhindern.

Zusätzliche Schutzziele

- **Zurechenbarkeit (accountability):**
  Wenn eine Kommuninkation stattgefunden hat, ist dies unbestreitbar und die Identitäten von Sender und Empfänger sind gegenüber berechtigten Dritten beweisbar, ebenso die Inhalte der Kommunikation.
- **Konsistenz unter Empfängern (consistency among recipients):**
  Mehrere Empfänger erhalten gleichzeitig die gleichen Inhalte oder können anderenfalls erkennen, dass das nicht der Fall ist.
- **Fairness (fairness):**
  Die Verfügbarkeit für alle berechtigten Nutzer eines IT-System ist gleich, sie können die gleichen Dienste nutzen oder anderenfalls erkennen, dass dies nicht der Fall ist.

Anforderungen an die IT-Sicherheit, die sich aus den verschiedenen Schutzzielen ableiten, können zu Zielkonflikten führen.

Mehrseitige (multilaterale) Sicherheit

- Beim Aufbau einer Kommunikationsverbindung wird das erforderliche Mass an Sicherheit zwischen den Beteiligten (automatisch) ausgehandelt
- Dabei werden die Schutzinteressen aller Beteiligten betrachtet, wobei sogenannte Schutzkonflikte ausgetragen werden, z.B. Konflikte zwischen Anonymitäts- und Zurechenbarkeitsansprüchen.

Gliederung

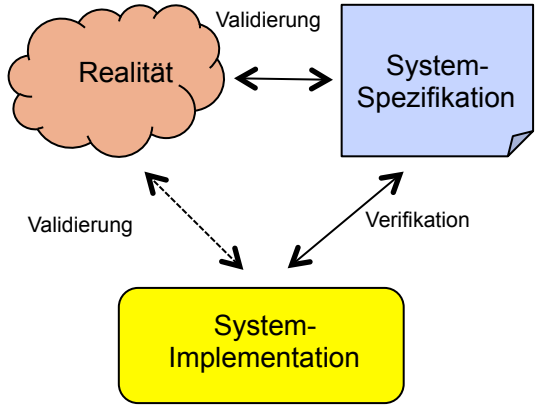
1. Schutzziele der IT-Sicherheit
2. **Arten von Bedrohungen**
3. Schadsoftware und Angriffsarten
4. Risiken für „Industrie 4.0“ und Internet of Things

Bedrohungen in Netzwerken

- **Internetkommunikation:**
  Verteilung von Schadsoftware (siehe Abschnitt 4) über das Internet, z.B. über E-Mails und Webserver; Denial-of-Service (DoS)-Angriffe; Abhören nicht ausreichend gesicherter Kommunikation
- **Kommunikation über drahtlose Netzwerke:**
  WLAN-Zugangspunkte (access points), sind durch Service Set Identifiers (SSIDs) identifiziert; diese kann ein „Evil Twin“ imitieren, so dass alle Kommunikation des Endgeräts zu ihm umgeleitet wird.

Bedrohungen durch Qualitätsprobleme

- **Programmfehler:**
  Grosse Softwaresysteme enthalten immer Fehler, weil ihre Komplexität nicht mehr zu beherrschen ist (E. Dijkstra: „unmastered complexity“).
- **Validierung:**
  Wurde ein System implementiert, das den richtigen Zweck erfüllt? (Beziehung System–Realität)
- **Verifikation:**
  Wurde das System richtig implementiert? (Beziehung Spezifikation–Implementation)



Die Möglichkeiten der Validierung und der Verifikation sind begrenzt, weil Systeme oft nicht vollständig spezifiziert werden können. Auch wenn eine vollständige Spezifikation vorliegt, sind die Möglichkeiten der Verifikation aufgrund der formalen Komplexität des Beweisverfahrens beschränkt.

Bedrohungen durch Qualitätsprobleme

- **Mangelnde Datenqualität:**
  Fehler in Daten (z.B. ein hoher Anteil an veralteten Adressen) können auch bei korrekten Programmen zu falschen Ergebnissen führen (GIGO-Prinzip: garbage in – garbage out)

- **Wartungsalbtraum:**
  Ein System zu ändern, das sich im Einsatz befindet, ist besonders aufwändig und führt in der Regel zu stark steigender Komplexität mit besonders hohen Sicherheitsrisiken. Viele Wartungsprobleme resultieren aus **Fehlern, die zu spät erkannt wurden:** Während die Behebung in der Analyse- oder Entwurfsphase noch leicht und sicher machbar gewesen wäre, kann der Aufwand später um einen Faktor 10-100 ansteigen und hohe Risiken nach sich ziehen.

Mehr zu Bedrohungen der IT-Sicherheit siehe:

Laudon/Laudon/Schoder 2016, **Abschnitt 15.1.2+3, S. 967-975.**

Gehört zum Prüfungsstoff!

Gliederung

1. Schutzziele der IT-Sicherheit
2. Arten von Bedrohungen
3. **Schadsoftware und Angriffsarten**
4. Risiken für „Industrie 4.0“ und Internet of Things

Schadsoftware (Malware, Malicious Software)

Nach Art der Ausbreitung:

- **Computervirus:**
  Programm, das sich selbst in andere ausführbare Programme (Wirtsprogramme) hineinkopiert und sich dadurch verbreitet.
- **Computerwurm:**
  Programm, das eigenständig ausführbar ist und sich über Netzwerke aktiv verbreitet. Ein Wurm braucht kein Wirtsprogramm.
- **Trojanisches Pferd („Trojaner“):**
  Ein Programm, das sich durch nützliche Funktionen tarnt und deshalb vom Benutzer installiert wird, aber mit Schadfunktionen kombiniert ist.
- **Rootkit:**
  Modifikation des Betriebssystems, die sich selbst verschleiert und Schadfunktionen ausführt.

Schadsoftware (Malware, Malicious Software)

Nach Schadfunktion:

- **Backdoor:**
  Schadfunktion eines Programms, die es einem Angreifer ermöglicht, Authentifizierungverfahren zu umgehen.

- **Spyware:**
  Schadfunktion eines Programms, die das Verhalten des Benutzers beobachtet und dem Angreifer meldet („phoning home“)

  - Adware: beobachtet Surfverhalten, um Werbung gezielt einzublenden
  - Keylogger: zeichnet jeden Tastendruck auf, um z.B. Passwörter oder Kreditkatennummern auszuspionieren
  - von staatlichen Stellen eingesetzte Spyware ist auch als „Govware“, „Policeware“ oder „Bundestrojaner“ bekannt

Historisch wichtige Beispiele für Viren und Würmer

Tabelle 15.6

Beispiele für bekannte Computerviren und Würmer

Name	Typ	Entdeckt	Beschreibung
Melissa	Wurm	März 1999	Ein Word-Makro, das sich automatisch an die ersten 50 Personen im Microsoft-Outlook-Adressbuch verschickt. Angeblich wurden zwischen 15% und 29% aller Geschäfts-PCs durch Melissa infiziert.
ILoveYou	Wurm	3. Mai 2000	ILoveYou ist in der Programmiersprache VBScript geschrieben. Das Skript löscht Dateien mit speziellen Dateiendungen (z. B. .jpg oder .css) und erstellt gleichnamige Kopien mit der Endung .vbs.
Code Red	Wurm	13. Juli 2001	Ein Wurm, der Microsoft-IIS-Webserver-Software ohne Patch angreift. Er greift nicht den PC eines Endbenutzers an, aber alle Internetbenutzer können die Auswirkungen dieses Wurms bemerken, wenn beispielsweise angeforderte Webseiten aufgrund der Aktionen des Wurms verzögert oder überhaupt nicht angezeigt werden. Computer Economics schätzte den Schaden auf 2,62 Mrd. USD.
Nimda	Wurm	September 2001	Verbreitung als E-Mail-Anhang oder durch Downloads infizierter Seiten. Der Rumpf der Nachricht scheint leer zu sein, enthält aber Code, der den Virus ausführt, sobald der Benutzer die Nachricht ansieht. Nimda kann verschiedene Weitergabemethoden verwenden und hat damit eine sehr hohe Infektionsrate. Computer Economics schätzte den Schaden auf 590 Mio. USD.
SQL Slammer	Wurm	24. Januar 2003	Ein Wurm, der im Speicher nicht gepatchter Microsoft-SQL-Server-Datenbanksoftware lebt und das Netzwerk verlangsamt. Von diesem Wurm angegriffene Systeme erlauben es einem entfernten Angreifer, beliebigen Code als Systembenutzer auszuführen.
Sobig.F	Wurm	18. August 2003	Sobig.F verteilte sich wie viele andere Würmer als Anhang einer E-Mail und deaktivierte sich selbst bereits am 10. September 2003. Es wird angenommen, dass mehr als eine Million Computer von dem Wurm betroffen waren.

MyDoom.A	Wurm	26. Januar 2004	Der Wurm verteilte sich als E-Mail-Anhang und führte zeitweise zu einer etwa 10%igen Verlangsamung des globalen Internetverkehrs. MyDoom.A stellte seine automatische Verbreitung am 12. Februar 2004 programmgesteuert ein.
Sasser.ftp	Wurm	Mai 2004	Sasser hat über das Internet zufällige IP-Adressen angegriffen, was dazu führte, dass Computer mehrfach abstürzten. Der Wurm betraf mehrere Millionen Computer weltweit (u.a. British Airways Check-in, Krankenhäuser in Hong Kong, Postämter in Taiwan oder die australische Westpac Bank). Zur Ergreifung des Sasser-Programmierers wurden von Microsoft 250.000 USD ausgeschrieben. Der Entwickler wurde am 8. Juli 2005 zu einer Jugendstrafe verurteilt.
Storm Worm	Wurm/ Trojaner	17. Januar 2007	Storm Worm verteilt sich als E-Mail mit einer Betreffzeile, die sich auf eine aktuelle Unwetterkatastrophe bezieht. Am 22. Januar 2007 war der Storm Worm bereits für 8% aller Computerinfektionen weltweit verantwortlich. Die durch den Storm Worm infizierten Rechner bilden das Storm-Botnetz. Im April 2008 wurde dieses Botnetz von Wissenschaftlern der Universität Mannheim genauer analysiert und man zählte je nach Tageszeit zwischen 5.000 und 40.000 aktive infizierte Rechner (Storm-Bots).
Agobot	Wurm	2007	Eine Familie von Würmern, die hochmodular aufgebaut und größtenteils in C++ geschrieben ist. Aufgrund der hohen Modularität war der Funktionsumfang beim Erscheinen wegweisend.

Mehr zu Schadsoftware siehe:

Laudon/Laudon/Schoder 2016, **Abschnitt 15.1.4, S. 976-981.**

Gehört zum Prüfungsstoff!

Angriffsarten (1/2)

- **Spoofing:**
  Vortäuschen einer falschen Identität des Kommunikationspartners gegenüber dem Angriffsziel, insbesondere
  - Frame-Spoofing: Fälschung von IP-Paketen
  - E-Mail-Spoofing: falsche Absender-Adresse
  - Link-Spoofing, Website-Spoofing: Verschleierung der tatsächlichen Website, auf die ein Link führt
- **Phishing:**
  Der Versuch, einem Benutzer sensitive Daten (z.B. Passwörter) zu entlocken, indem die Kommunikation mit einem einem scheinbar vertrauenswürdigen Gegenüber vorgetäuscht wird; hier kommen u.a. verschiedene Spoofing-Techniken zum Einsatz.

Angriffsarten (2/2)

- **Social Engineering:**
  Das Beeinflussen von Menschen mit dem Ziel, sie zur Preisgabe vertraulicher Informationen (z.B. von Passwörtern) zu bewegen.

- **Missbrauch von Sniffern:**
  Sniffer sind Netzwerkanalysewerkzeuge, die den Datenverkehr überwachen und von Administratoren eingesetzt werden. Durch Missbrauch von Sniffern können Angreifer vertrauliche Informationen abfangen, wenn diese nicht ausreichend verschlüsselt sind.

- **Denial-of-Service-Angriff (DoS-Angriff):**
  Die Dienste eines IT-Systems, insbesondere eines Servers, werden durch Überlastung gestört.

  - **Distributed-Denial-of-Service-Angriff (DDoS-Angriff):**
    DoS-Angriff durch eine grosse Zahl von angreifenden Systemen, inbesondere **Botnetze**, die durch Verbreitung von Schadsoftware geschaffen werden.

Gliederung

1. Schutzziele der IT-Sicherheit
2. Arten von Bedrohungen
3. Schadsoftware und Angriffsarten
4. **Risiken für „Industrie 4.0“ und Internet of Things**

Industrie 4.0

- Steuerung von Produktionsabläufen **durch cyber-physische Systeme**, d.h. Systeme mit enger Verzahnung zwischen physischen Komponenten und (eingebetteten) IT-Komponenten
- Die resultierende Konnektivität von Produktionsanlagen und Werkstücken schafft Milliarden zusätzlicher potenzieller Angriffspunkte
- Motive für Angriffe auf Industrie-4.0-Systeme sind Industriespionage und Sabotage.
- Schon vor „Industrie 4.0“ sind Angriffe durch Schadsoftware auf Produktionsanlage bekanntgeworden, Beispiele:
  - Beschädigung eine Hochofens, der nicht mehr heruntergefahren werden konnte
  - Explosion einer mit Sensoren ausgestatteten Pipeline in der Türkei
  - Beschädigung von Uranzentrifugen in Iran (durch den Wurm Stuxnet)

Internet of Things (IoT)

- Alltagsgegenstände werden durch eingebettete IT „smart“ und kommunizieren über das Internet.
- Man rechnet mit weltweit 50 Milliarden „smart things“.
- Der nicht von Menschen, sondern Maschinen ausgelöste Datenverkehr **(Machine-to-Machine Traffic, M2M)** wird das Internet dominieren.
- Die Möglichkeiten für Sniffing, die Verbreitung von Backdoors durch Viren und Würmer, den Betrieb von Botnetzen und die Verursachung physischer Schäden durch Cyberangriffe werden sich entsprechend vervielfachen.

Laudon/Laudon/Schoder
Wirtschaftsinformatik
3., vollständig überarbeitete Auflage

Grundlage für diese LE:
Abschnitt 15.1