



Hochschule für  
Wirtschaft und Recht Berlin  
Berlin School of Economics and Law

**Tele-  
kommunikations-  
systeme**

# IT-Sicherheit

**Gerrit.Kalkbrenner@hwr-berlin.de**



# IT-Sicherheit: Zentrales Thema in der IT

- Dazu fast tägliche Schlagzeilen in den Medien
  - Daten-Diebstahl
  - Spionage
  - Sabotage
- Probleme
  - Ausgespähte Daten sind geldwert
  - Daten werden per Funk übertragen und sind damit öffentlich



# Warum ist IT-Sicherheit so schwierig?

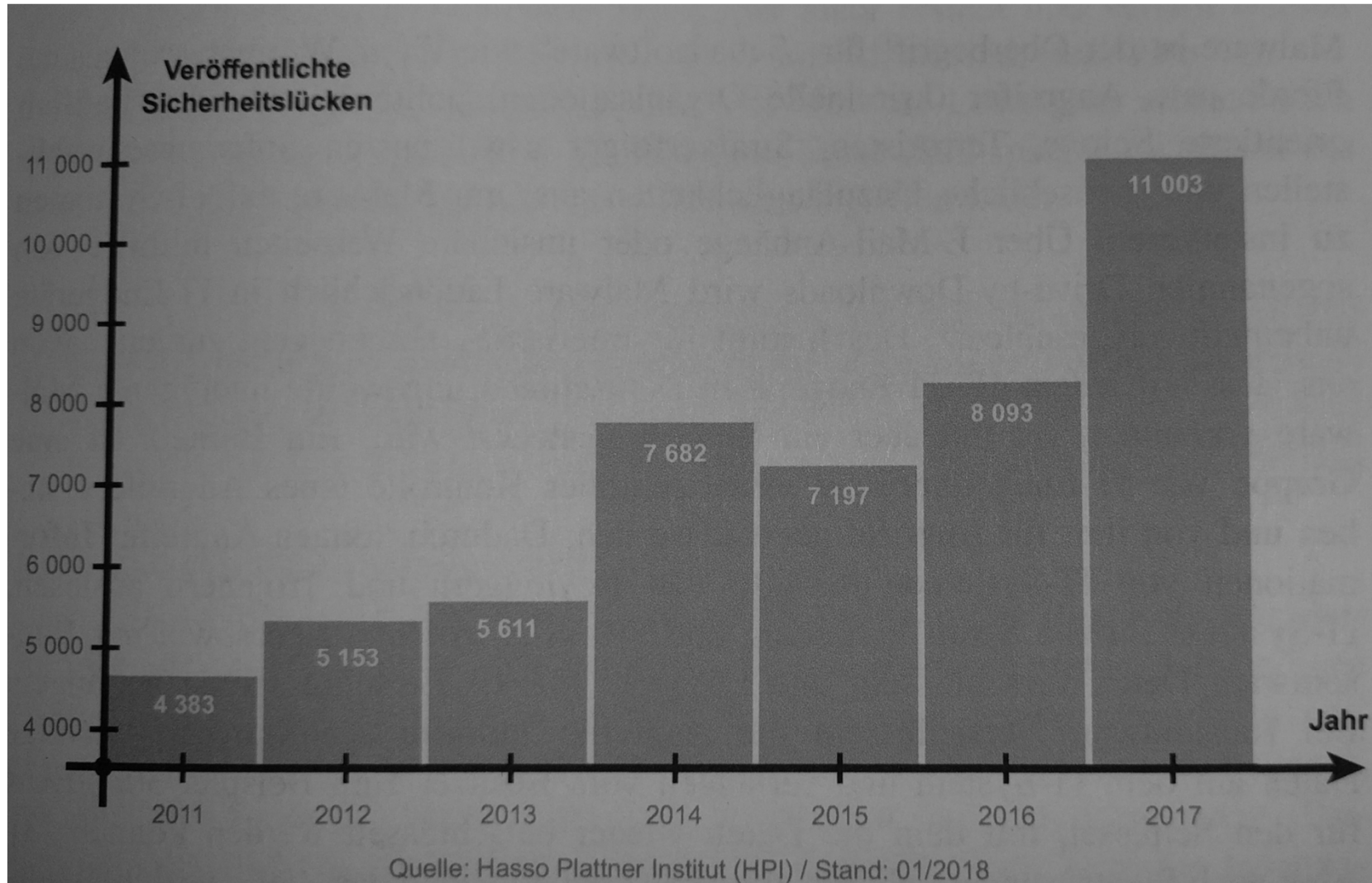


## Warum ist IT-Sicherheit so schwierig?

- IT-Sicherheit muss vollständig sein!
- Das schwächste Glied in einer Kette ist entscheidend!



# Problem: fehlerhafte Software



**Abb. 1.1** Schwachstellen in Software



# Angreifer und ihre Motivation



## Die 3 Ziele der Datensicherheit

1. Geheim, Vertraulich
2. Unversehrtheit
3. Verbindlichkeit, Nichtabstreitbarkeit
4. Verfügbarkeit



# Überblick

- Lehr- und Lernverfahren zur Vorlesung
- Netzwerke: Überblick und Anforderungen
- Vom Signal zum Datenstrom
- Systematisierung, Schichten im Referenzmodell
- Schichtweise von Physik bis Anwendung
- Protokolle, Topologie, Komponenten, Standards





# Telekommunikation

- Rauchzeichen
- Signalfahnen
- Lichtzeichen
  
- Das viktorianische Internet:  
-> Telegraphie





# Probleme mit Telegraphie

- Abhörbarkeit
  - Auf den Verbindungswegen
  - In den Vermittlungs-Stationen
- Beteiligte Personen wurden "verbeamtet"
- Kabel wurden regelmäßig geprüft
- Widerstandsmessung der Endgeräte
- Projekt Polykom: Verteiltes Regieren Berlin/Bonn
  - Evakuierte Röhren mit Glasfasern



## **Heute ist Telekommunikation viel komplexer. Wozu benötigt?**

- Kommunikation: zwischen Personen
- Kommunikation: zwischen Systemen
- Kommunikation: Person- System
- Übermittlung von Informationen
- Der Wert der Information entfaltet sich erst, wenn sie kommuniziert wird.

# Arten der Telekommunikation

Entwickelt nach Bedarf und verfügbarer Technik

- Boten, Sichtzeichen, Rauchzeichen
- Telegraphie
- Telefon, Fax
- Rundfunk, Fernsehen
- Betriebsfunk (Seefunk, Flugfunk)
- Satellitenkommunikation
- Computernetzwerke

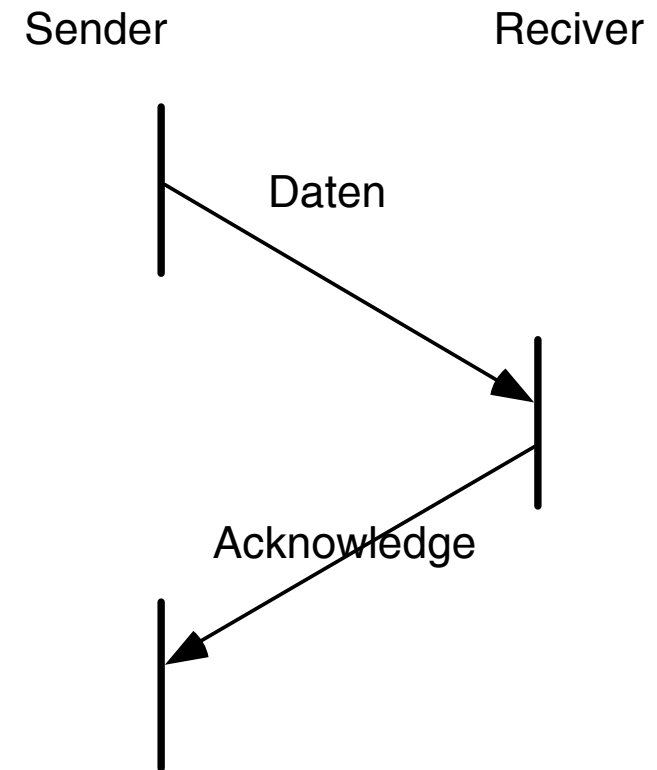


# Definierte Absprachen über Kommunikations-Semantik

- Einsatz festgelegter Protokolle

Sie legen fest:

- Syntax und Semantik der Kommandos
- Reaktionsmuster





# Standards

- ISO OSI: 7 Schichtenmodell
- ITU Standards (ehemals CCITT)
- Internet
  - RFCs
  - Draft
  - Internet Standard



## Systematisierung, Schichten im Referenzmodell

7	Application	Philosophieren
6	Presentation	Sprache
5	Session	
4	Transport	Übermittlung
3	Network	
2	Data Link	Abschnitt-Sicherung
1	Physical	



# Arten von Netzwerken

Entfernung	Plazierung	Beispiel
0,1 m	Main-Board	Datenfluss-Rechn.
1 m	System (Very Local)	Multi-Computer VLAN
1 m	Körper (Personal, Body)	PAN, BAN
10 m	Raum	LAN
100 m	Gebäude	
1 km	Campus	
10 km	Stadt	MAN
100 km	Land	WAN
1.000 km	Kontinent	
10.000 km	Welt	Internet, GAN





## Motivationen für Angriffe

- Spaß an der Technik
- Neugierde
- Herausforderung
- Anerkennung
  
- Zerstörungswut
- Geld
- Nationale Sicherheit



## Gruppen von Angreifern

- Hacker
- Unternehmens-Cracker
- IT-Spione
- IT-Terroristen
- Professionelle Kriminelle/Berufskriminelle
- Vandalen
- Behörden



## Themen dieser Veranstaltung

- Sichtweisen auf Cyber-Sicherheit
- Kryptographie
- Hardware- und Sicherheitsmodule
- Digitale Signaturen, Zertifikate
- Identifikation und Authentifikation
- Trusted Computing
- Cyber-Sicherheit Frühwarnung
- Firewall-Systeme



## Themen dieser Veranstaltung 2

- IP-Sec Verschlüsselung
- Transport Layer Security (TLS)  
Secure Socket Layer (SSL)
- DDoS Angriffe
- Email-Sicherheit
- Blockchain
- KI und Cyber-Sicherheit
- Social Web Sicherheit
- Wirtschaftlichkeit



# Teilnahmebedingungen

- Klausur (80%)
- Hausaufgaben (10%)
  - Z.B. sich einen Public-Private Schlüssen generieren
- Kurzvortrag (10%)
  - Bericht über einen Sicherheitsvorfall
  - am besten aus dem persönlichen Umfeld
  - Schilderung: was ist passiert, Einschätzung der Situation, was kann getan werden, um zukünftige Fälle zu vermeiden



## Literatur

- David Wong: Kryptografie in der Praxis, dpunkt
- Norbert Pohlmann: Cyber-Sicherheit, Springer
- Claudia Eckert: IT-Sicherheit, De Gruyter
- c't: regelmäßige Berichte zu IT-Sicherheit
- c't Security
- c't DSGVO