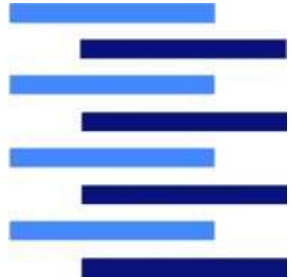
IT-Sicherheit



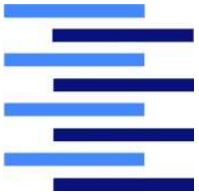
Prof. Dr.-Ing. Martin Hübner

https://users.informatik.haw-hamburg.de/~huebner

Ziele der Veranstaltung "IT-Sicherheit"

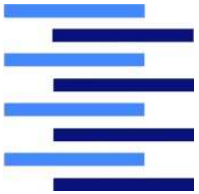
- Methoden zur Konstruktion von sicheren verteilten Systemen praktisch anwenden können
- Sicherheitsmodelle und Sicherheitseigenschaften von IT-Systemen verstehen und zum sicheren Betrieb von Anwendungen einsetzen können
- Angriffstechniken (z.B. in Netzwerken) sowie den gezielten Einsatz von Abwehrmaßnahmen beurteilen können

Gliederung der Vorlesung (1)



1. Einführung – Grundlegende Begriffe
    1. IT-Sicherheit - Worum geht es hier eigentlich?
    2. Security Engineering
2. Bedrohungen und Angriffe
    1. Rechtslage
    2. Angreifer
    3. Typische Angriffstechniken
    4. Malware
    5. Die gefährlichsten Programmierfehler
3. Grundlagen der Kryptographie
    1. Einführung
    2. Einfache Symmetrische Verfahren
    3. Moderne symmetrische Verfahren
    4. Asymmetrische Verfahren („Public Key“)
    5. Digitale Signaturen und kryptografische Hashfunktionen

Gliederung der Vorlesung (2)



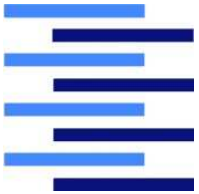
4. Public Key Infrastrukturen (PKI)

1. Vertrauensmodelle
2. Zertifikate
3. PKI-Organisation
4. PKI-Anwendungen

5. Authentifikation und Autorisation

1. Benutzerauthentifikation (Zugangskontrolle)
2. Authentifikation in verteilten Systemen
3. Modelle für die Zugriffskontrolle (Autorisation)
4. Zugriffskontrolle in UNIX
5. Zugriffskontrolle in Windows

Gliederung der Vorlesung (3)



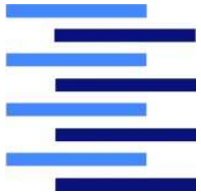
6. Sicherheitsmaßnahmen in Netzen

1. S/MIME
2. TLS
3. IPsec und VPN
4. WLAN: WEP und IEEE 802.11i

Literaturempfehlungen

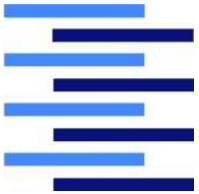
- [CE] Claudia Eckert: **IT-Sicherheit**, 9. Auflage, Oldenbourg Verlag, 2014
  Umfassende Darstellung aller Bereiche!
- [KS] Klaus Schmeh: **Kryptografie: Verfahren, Protokolle, Infrastrukturen**, 6. Auflage, dpunkt-Verlag, 2016 - *Didaktisch sehr gute Beschreibung kryptographischer Verfahren und ihrer Anwendung (PKI)*
- [PP] Christof Paar, Jan Pelzl: **Kryptografie verständlich**, 1. Auflage, Springer Vieweg Verlag, 2016
  Beschreibt alle kryptographischen Grundlagen – liegt als eBook im Pub-Verzeichnis!
- [KPS] Charlie Kaufman, Radia Perlman, Mike Speciner: **Network Security**, Prentice Hall, 2002 - *Deckt alle wesentlichen Aspekte der Vorlesung bzgl. Kryptographie, Authentifikation und Netzwerksicherheitsprotokollen ab, sehr gut lesbar*
- [MSK] Stuart McClure, Joel Scambray, George Kurtz: **Hacking Exposed: Network Security Secrets & Solutions**, 7. Auflage, McGraw-Hill Professional, 2012
  Umfassende Beschreibung von Hacker-Angriffstechniken und Abwehrmaßnahmen
- [MZ] Michal Zalewski: **Tangled Web - Der Security-Leitfaden für Webentwickler**, dpunkt-Verlag, 2013 - *Guter Überblick über Schwachstellen und Sicherheitsmaßnahmen in Webapplikationen*
- [BS] Bruce Schneier: **Angewandte Kryptographie**, Addison-Wesley, 1996
  Ein Klassiker: Ausführliche Beschreibung von kryptographischen Algorithmen inkl. Implementierungsbeispielen und C-Sourcecode

Weiterführende Web-Sites (kleine Auswahl!)

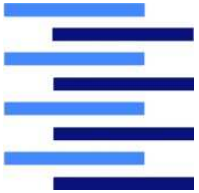


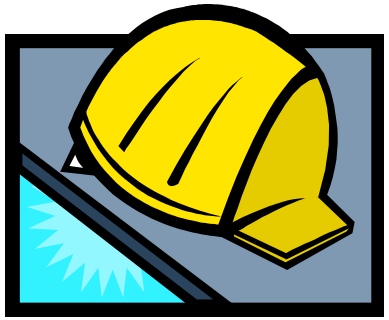
- Bundesamt für Sicherheit in der Informationstechnik
  www.bsi.de
- IT-Sicherheitsportal mit aktuellen Infos
  www.heise.de/security
- Microsoft Sicherheit
  www.microsoft.com/technet/security
- LINUX – Sicherheit
  www.linuxsecurity.com
- Kali-Linux: Debian-basierte Linux-Distribution mit vielen integrierten Tools für Penetrationstests und Sicherheitschecks
  www.kali.org
- EU-Datenschutzgrundverordnung / neues Bundesdatenschutzgesetz (gültig ab Mai 2018)
  dsgvo-gesetz.de

Kapitel 1
Einführung – Grundlegende Begriffe

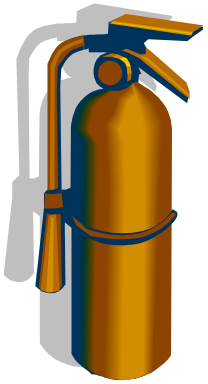


1. IT-Sicherheit - Worum geht es hier eigentlich?
2. Security Engineering

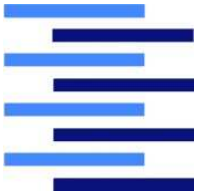




Was ist „IT – Sicherheit“?



Was ist „IT – Sicherheit“?

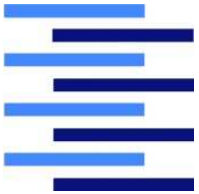


IT-Sicherheit:

Schutz von IT-Systemen

vor passiven oder aktiven Angriffen

IT-Systeme



„Ein IT-System ist ein dynamisches technisches System mit der Fähigkeit zur Speicherung und Verarbeitung von **Informationen**.“ [CE]

- „Offenes“ IT-System: vernetzt und physisch verteilt
- IT-Systeme sind Bestandteile größerer soziotechnischer Systeme!

➔ Rahmenbedingungen beachten, z.B.

- ➔ Benutzerverhalten und –akzeptanz
- ➔ gesetzliche und organisatorische Regelungen
- ➔ kommerzielle Bedingungen (Kosten!)

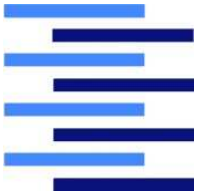
Schutzgüter: Was soll geschützt werden?

- **Informationen** und **Datenobjekte** sind die wesentlichen schützenswerten Güter eines IT-Systems!
- Datenobjekte *(Bitfolgen)* repräsentieren Informationen *(z.B. Kreditkartennummern)*
- Schutz der Informationen erreichbar durch Schutz der Datenobjekte!

➔ In welchen verschiedenen Datenobjekten sind die schützenswerten Informationen gespeichert?

- ➔ *Dateien (evtl. temporär!)?*
- ➔ *Hauptspeicher (Kopie eines Variablenwertes? Parameter auf dem Stack?)*
- ➔ *Cache?*
- ➔ *…*

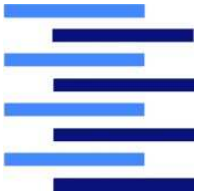
Wovor sollen die Güter geschützt werden?
→ Schutzziele



- Informationsvertraulichkeit *("Confidentiality")*
  - Schutz der Informationen vor unautorisierter Einsichtnahme (Geheimhaltung!)
- Datenintegrität *("Integrity")*
  - Schutz der Datenobjekte vor unautorisierter Veränderung (Verhindern von Modifikation oder Löschung!)
- Systemverfügbarkeit *("Availability")*
  - Schutz des IT-Systems vor (beabsichtigter) Störung (Verhindern von Abstürzen oder Performanceverlusten!)

Abkürzung: "CIA"

Hilfs-Schutzziele

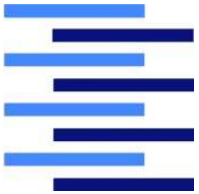


- Authentizität *("Authenticity")*
  - Bestätigung der Echtheit eines Subjekts/Objekts
    → Schutz vor Täuschung
    Überprüfung anhand einer eindeutigen Identität:
    Authentifikation *("Authentication")*
- Verbindlichkeit *("Non Repudiation")*
  - Beweisbarkeit der Durchführung einer Aktion
    → Schutz vor Falschbehauptungen
    Ein Subjekt kann im Nachhinein nicht abstreiten, die Aktion durchgeführt zu haben

Subjekte und Zugriffe

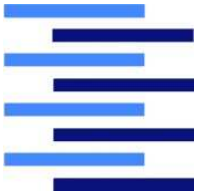
- Subjekte
  - Benutzer eines IT-Systems und alle Komponenten, die im Auftrag von Benutzern im System aktiv Veränderungen vornehmen können
  - *Beispiele: Prozesse, Prozeduren, Schaltkreise*
- Zugriff
  - Informationsfluss zwischen einem Subjekt und einem Datenobjekt
- Zugriffsrechte
  - Legen fest, in welcher Weise ein Subjekt auf ein Datenobjekt zugreifen darf
    (Autorisation ➔ Zugriffskontrolle)

Schwachstellen und Bedrohungen



- Schwachstelle eines Systems *("Vulnerability")*
  - Eine Möglichkeit, mit der die Sicherheitsdienste eines Systems umgangen, getäuscht oder unautorisiert modifiziert werden können
- Bedrohung *("Threat")*
  - Eine Bedrohung (Gefährdung) ist die mögliche Ausnutzung einer Schwachstelle, um einen Verlust der Datenintegrität, der Informationsvertraulichkeit oder der Verfügbarkeit zu erreichen
- Exploit
  - Ein Verfahren oder Werkzeug, um eine Schwachstelle eines Systems unberechtigt auszunutzen

Angriffe

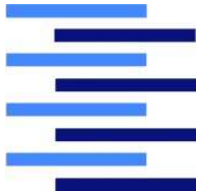


- Angriff
  - Ein nicht autorisierter Zugriff bzw. Zugriffsversuch auf ein IT-System, oft durch Ausnutzen einer Schwachstelle mit Hilfe eines Exploits

- Passiver Angriff
  - Zugriff auf vertrauliche Informationen
    (→ Verlust der Vertraulichkeit)

- Aktiver Angriff
  - Modifikation von Datenobjekten oder Systemressourcen
    (→ Verlust der Datenintegrität / Systemverfügbarkeit)

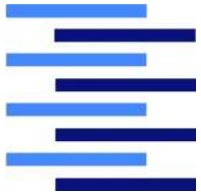
Mögliche Definitionen: Sicherheit



nach [CE]

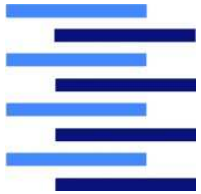
- Funktionssicherheit („Safety“)
  - Übereinstimmung der realen Ist-Funktionalität eines Systems mit der spezifizierten Soll-Funktionalität
  - *Korrektheit und Zuverlässigkeit des Systems → Schutz vor Systemfehlern*
- Informationssicherheit („Security“)
  - Eigenschaft eines funktionssicheren Systems, nur solche Zustände anzunehmen, die zu keiner unautorisierten Informationsveränderung oder -gewinnung führen
  - *Schutz der Informationen vor Angriffen*
- Datensicherheit („Protection“)
  - Eigenschaft eines funktionssicheren Systems, nur solche Zustände anzunehmen, die zu keinem unautorisierten Zugriff auf Daten oder andere Systemressourcen oder zum Verlust von Daten führen.
  - *Schutz der Datenobjekte vor Angriffen, Systemfehlern, Dummheit des Administrators, ... (u.a. durch Datensicherungsmaßnahmen)*

Mögliche Definitionen: Sicherheit (II)



- Datenschutz („Privacy“)
  - Schutz der Vertraulichkeit von personenbezogenen Daten bzw. Fähigkeit einer natürlichen Person, die Weitergabe seiner persönlichen Daten zu kontrollieren
  - Festlegung des Begriffs und von Verarbeitungsvorschriften für personenbezogene Daten *(inkl. Datensicherheit!)* erfolgt durch die EU-Datenschutz-Grundverordnung *(ab 25. Mai 2018),* das Bundesdatenschutzgesetz *(BDSG)* sowie Bundesländer-Datenschutzgesetze
  - Die Verarbeitung personenbezogener Daten ist zulässig, wenn
    - die/der Betroffene eingewilligt hat oder
    - ein gesetzlicher Erlaubnistatbestand vorliegt
  - Über die Einhaltung der Datenschutzgesetze wachen Bundes-/ Landes- und betriebliche Datenschutzbeauftragte → *leisten aber auch Beratung*
  - *Weitere Infos unter www.datenschutz.de*

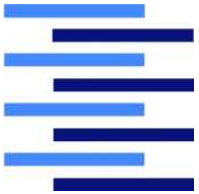
Mögliche Definitionen: Sicherheit (III)



- Cyber-Sicherheit
  - Schutz der Gesellschaft vor Angriffen, die sich durch Einsatz von IT-Systemen und aus Abhängigkeiten von Informationen für Menschen, Firmen, Infrastruktureinrichtungen etc. ergeben

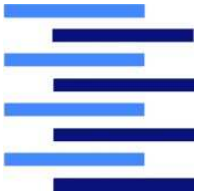
- **IT-Sicherheit**
  - Schutz von IT-Systemen vor passiven oder aktiven Angriffen
    → *Informationssicherheit (Security)* *+ Datensicherheit (Protection)*

Kapitel 1
Einführung – Grundlegende Begriffe



1. IT-Sicherheit - Worum geht es hier eigentlich?
2. Security Engineering

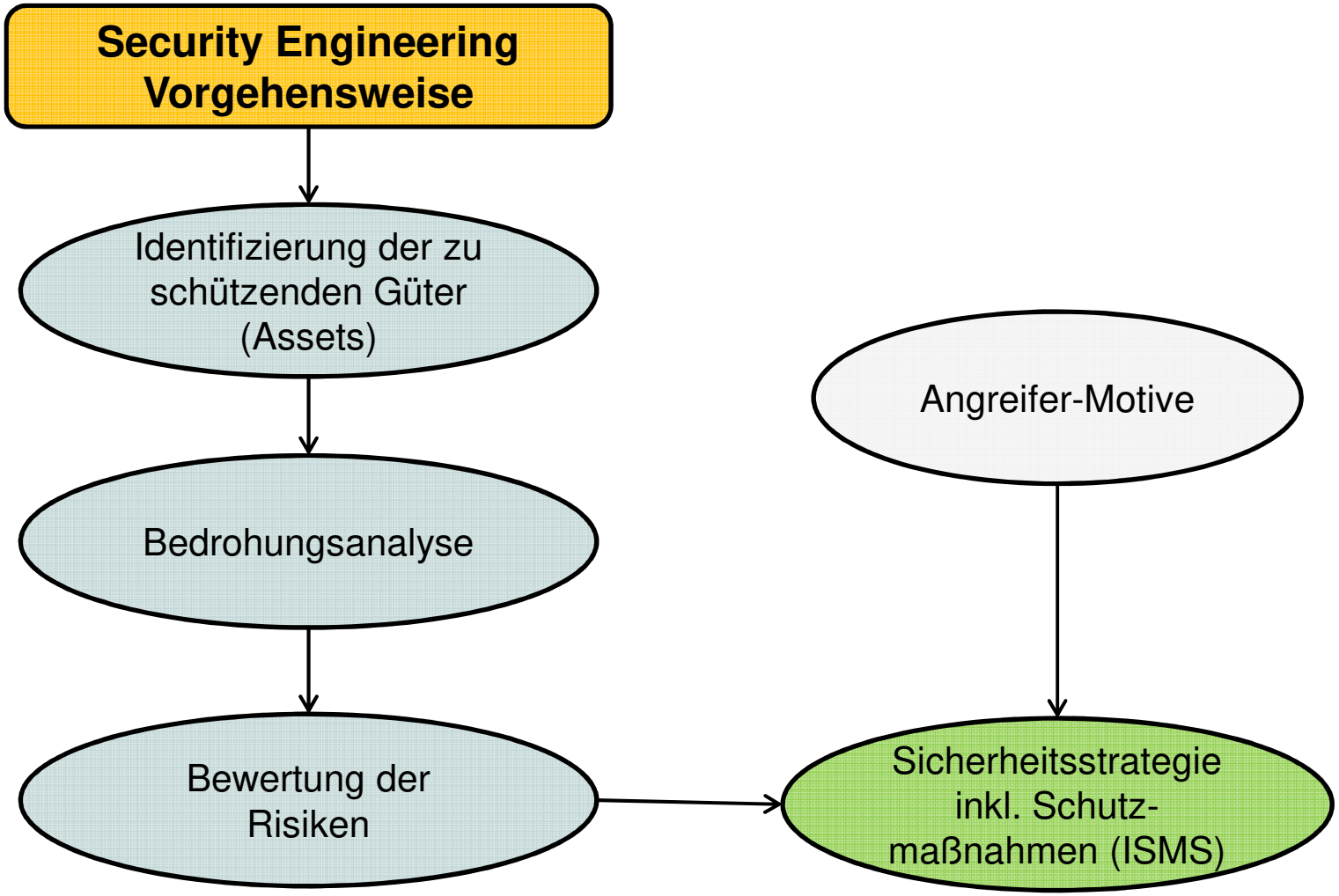
Vorbemerkung



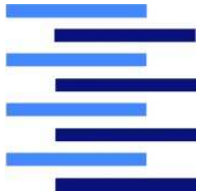
- Sicherheit wird nur erreicht, wenn **alle** Komponenten und Einflussfaktoren eines Systems berücksichtigt werden!
  - Technik
  - Organisation
  - Personal

➔ Eine systematische Vorgehensweise ist notwendig bei der Konstruktion / dem Betrieb von **sicheren** IT-Systemen

„Security Engineering“ – Vorgehensweise



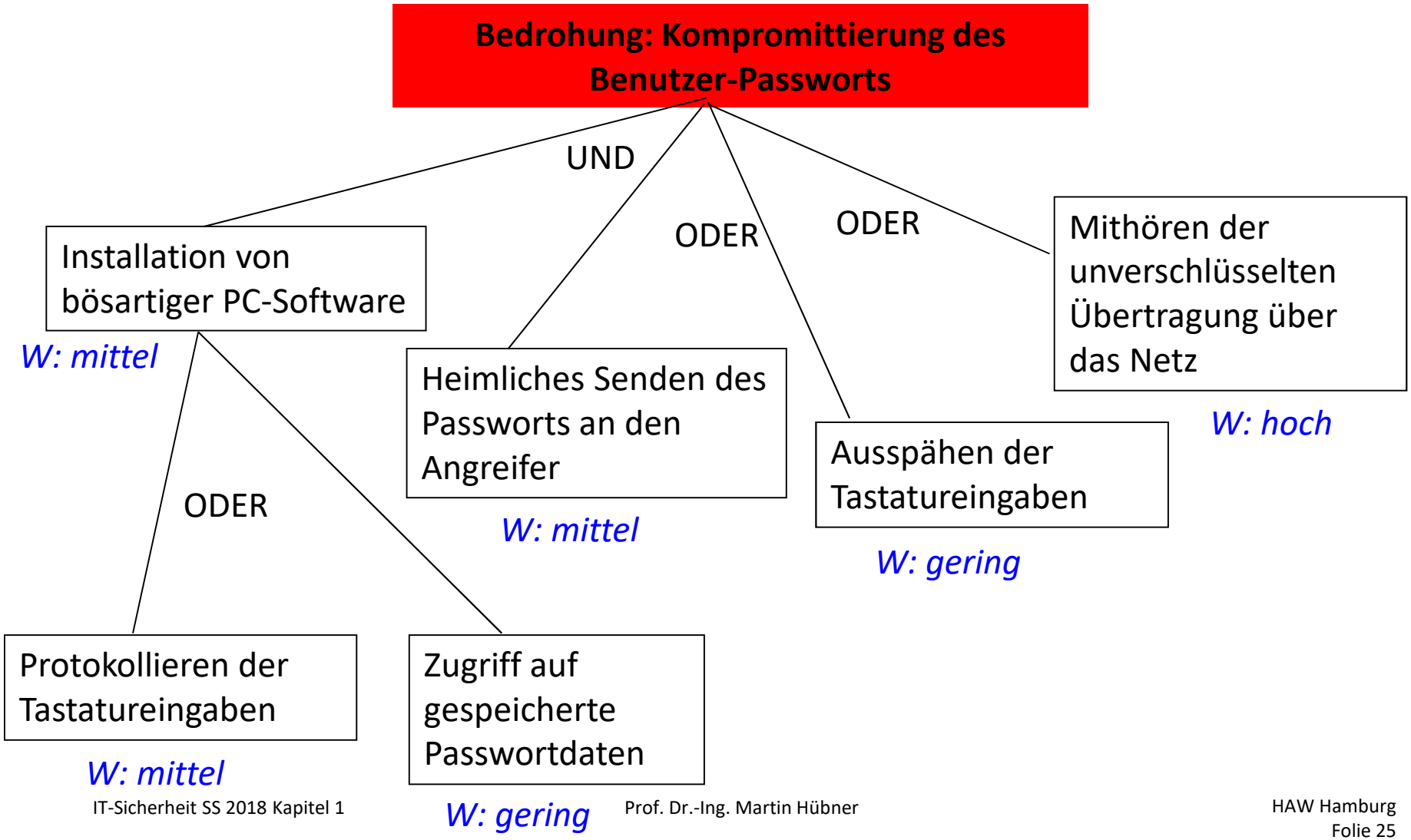
„Security Engineering“ – Vorgehensweise



- Identifikation der zu schützenden Güter („Assets“) (inkl. IT-Strukturanalyse)
  - **Was** soll geschützt werden (IT-Systeme, Anwendungen, Daten, Firmen-Reputation, ...)?
  - Wie hoch ist der **Wert** der zu schützenden Güter?
- Bedrohungs- und Risikoanalyse
  - Welche Bedrohungen (Gefährdungen) gibt es?
  - Wie hoch ist die jeweilige Eintrittswahrscheinlichkeit?
  - Wie hoch ist der jeweilige Schaden?
  - ➔ **Risiko einer Bedrohung = Eintrittswahrscheinlichkeit * Schadenshöhe**
- Erarbeiten einer Sicherheitsstrategie
  - Auswahl, Priorisierung und Realisierung von geeigneten Schutzmaßnahmen zur Reduktion des (Rest-)Risikos
  - Definition von Prozessen und Verantwortlichkeiten

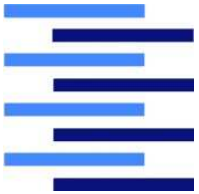
Techniken der Bedrohungs- und Risikoanalyse

Beispiel: Bedrohungsbaum mit Risikobewertung für eine Online-Anwendung mit Authentifikation über PC



Techniken der Bedrohungs- und Risikoanalyse

Ermittlung des Gesamt-Risikos eines Bedrohungsbaums



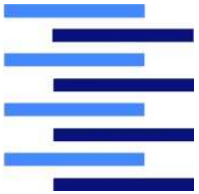
- Für die Bedrohung die Schadenshöhe ermitteln („Schutzbedarfsfeststellung“)
  Im Beispiel: Schaden ist **hoch** (z.B. Online-Banking)
- Ermittlung der Eintrittswahrscheinlichkeit:
  Aggregation der Einzelwahrscheinlichkeiten anhand der UND/ODER-Beziehungen:
  - UND: geringste Einzelwahrscheinlichkeit annehmen
  - ODER: höchste Einzelwahrscheinlichkeit annehmen

  Im Beispiel: Eintrittswahrscheinlichkeit der Bedrohung ist **hoch**

➔ Gesamt-Risiko = Eintrittswahrscheinlichkeit * Schaden: **hoch**

➔ **Wenn Risiko nicht akzeptabel:**
Maßnahmen zur Risiko-Reduktion treffen!

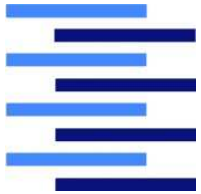
Techniken der Bedrohungs- und Risikoanalyse



STRIDE-Bedrohungsanalyse

- **STRIDE**-Bedrohungsanalyse ist des Teil des **Security Development Lifecycle der Firma Microsoft**
- Unterscheidung folgender Bedrohungsklassen:
  - **S**poofing Identity (Fälschung der Identität)
  - **T**ampering with Data (Verfälschung von Informationen)
  - **R**epudiation (Abstreitbarkeit möglich)
  - **I**nformation Disclosure (Weitergabe von vertraulichen Informationen)
  - **D**enial of Service (Systemverfügbarkeit)
  - **E**levation of Privilege (Unerlaubte Erhöhung von Rechten)
- Für jede zu schützende Systemkomponente potentielle Bedrohungen ermitteln
  - Fragen stellen, z.B.: „*Kann ein Angreifer einen Spoofing-Angriff durchführen?*“
  - Wenn eine Frage mit „Ja“ beantwortet wurde, den Angriff zur Liste der potentiellen Bedrohungen für diese Komponente hinzufügen

Techniken der Bedrohungs- und Risikoanalyse



DREAD-Risikobewertung

- **DREAD**-Risikobewertung ist des Teil des **Security Development Lifecycle der Firma Microsoft**
- Unterscheidung folgender Kriterien zur Bewertung einer potentiellen Bedrohung:
  - **D**amage Potential (Welcher Schaden kann angerichtet werden?)
  - **R**eproducibility (Wie leicht ist der Angriff reproduzierbar?)
  - **E**xploitability (Wieviel Fachkenntnis benötigt der Angriff?)
  - **A**ffected Users (Wieviele Benutzer sind betroffen?)
  - **D**iscoverability (Wie schnell kann die Schwachstelle bemerkt werden?)
- Für jede potentielle Bedrohung wird für jedes dieser 5 Kriterien eine Bewertung ermittelt anhand der Skala *gering* (1), *mittel* (2) oder *hoch* (3)
- Risiko einer Bedrohung = Summe aller Einzelbewertungen
  (hoch: 12-15, mittel: 8-11, gering: 5-7)
- *Quelle STRIDE/DREAD: http://msdn.microsoft.com/de-de/library/cc405496.aspx*
- *Beispiel: https://msdn.microsoft.com/de-de/library/cc431335.aspx*

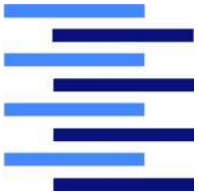
Problem: Scheinsicherheit

- Risiken werden oft nicht transparent
- Ungeeignete Maßnahmen führen zu leicht überwindbarer Sicherheit.
- Effektivität von Maßnahmen ist nicht immer per se ersichtlich.
- Maßnahmen erzeugen Kosten, reduzieren aber nur scheinbar das Risiko.
- Nutzer fühlen sich „sicher“, sind es aber faktisch nicht.

→ In der IT ist **Scheinsicherheit** manchmal schwierig zu erkennen!

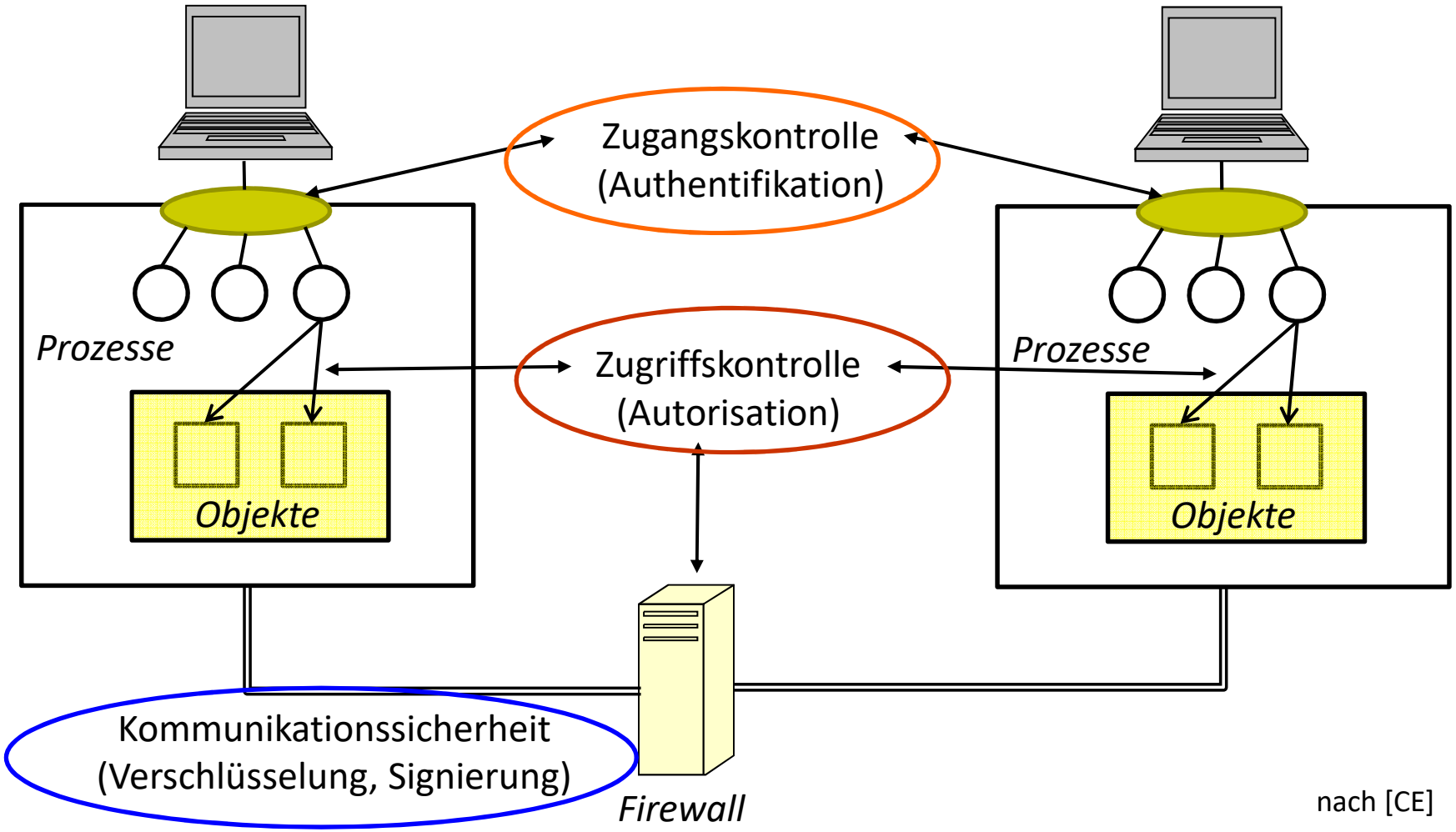
Weitere Beispiele

Sicherheitsstrategie



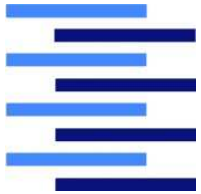
- „Die **Sicherheitsstrategie** eines IT-Systems oder einer organisatorischen Einheit definiert alle technischen und organisatorischen Regeln, Verhaltensrichtlinien, Verantwortlichkeiten und Rollen sowie alle **Maßnahmen**, um die angestrebten Schutzziele zu erreichen.“ [CE]
- ***Beispiele**: Systemverhalten (Speicherbereinigung, Beweissicherung, Rechteprüfung,…), Zugriffsrechte, Administrationsrollen, Benutzerverhalten (Passwortrichtlinien), Einsatz von spezieller Software (z.B. Virenscanner, Firewalls, Verschlüsselung), Absicherung von Räumen, Datensicherungsmaßnahmen, …*
- Zur systematischen Definition einer Sicherheitsstrategie ist eine **Sicherheitsarchitektur** hilfreich!

Komponenten einer Sicherheitsarchitektur und Schutzmaßnahmen



nach [CE]

Wichtige Schutzmaßnahmen

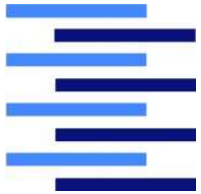


- Zugangskontrolle
  - Authentifikation von Subjekten
  - *„Ist X wirklich derjenige, für den er sich ausgibt?“*
- Zugriffskontrolle
  - Autorisation von Subjekten für den Zugriff auf bestimmte Objekte
  - *„Darf X auf Objekt Y zugreifen?“*
  - Spezialform: Firewall-Einsatz
    - Filtern von Netzzugriffen
    - *„Welche Anfragen / Verbindungswünsche lasse ich in das interne Netz hinein bzw. heraus?“*
- Verschlüsselung / Signierung
  - Anwendung kryptografischer Methoden
  - *„Wie kann X Informationen in der Form speichern, dass nur Y (autorisiert) darauf zugreifen kann?“*
  - *Wie kann ich Daten gegen Manipulation während der Übertragung schützen?*

Information Security Management System (ISMS)

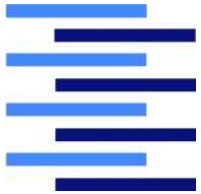
- Ein **Information Security Management System** (**ISMS)** ist eine Aufstellung von Verfahren und Regeln innerhalb eines Unternehmens, welche dazu dienen, die Schutzmaßnahmen zur Informationssicherheit dauerhaft zu definieren, umzusetzen, zu überprüfen und fortlaufend zu verbessern
- Erweiterung einer Sicherheitsstrategie um organisatorische Prozesse für Schutzmaßnahmen:
  - Plan → Definieren
  - Do → Umsetzen & Durchführen
  - Check → Überwachen & Überprüfen
  - Act → Instandhalten & Verbessern

Hilfreiche Standards und Richtlinien (1)



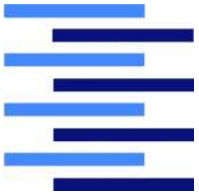
- **ISO 2700x**
  - 27000: ISMS – Overview and vocabulary
  - 27001: ISMS – Requirements
  - 27002: Code of practice for IS management
  - 27003: ISMS implementation guidance
  - 27004: IS management measurements
  - 27005: IS risk management
- **COBIT** (Control Objectives for Information and related Technology)
  - Veröffentlicht durch ISACA (Information Systems Audit and Control Association): www.isaca.org
  - Bezeichnet als „Best practice for management of IT-based business processes“
  - Erstellt für das Management, Auditoren, IT-Sicherheitsmanager
  - Integriert 41 (!) nationale und internationale Standards

Hilfreiche Standards und Richtlinien (2)



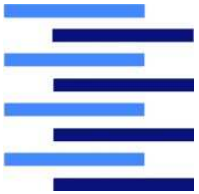
- **ITIL** („IT Infrastructure Library“)
  - Allgemeines Geschäftsprozessmodell für den Betrieb von IT-Infrastrukturen, insbesondere IT Service Management
  - Entwickelt im Auftrag der britische Regierung
  - SLAs („Service Level Agreements“) müssen auch Sicherheitsanforderungen beschreiben
  - Sicherheitsvorfälle werden genauso behandelt wie andere Betriebsstörungen („Incidents“)
- **ISO 15408** (“Common Criteria” for Information Technology Security Evaluation)
  - Framework zur Definition und Überprüfung von Sicherheitsanforderungen auf technischer Ebene

Hilfreiche Standards und Richtlinien (3)



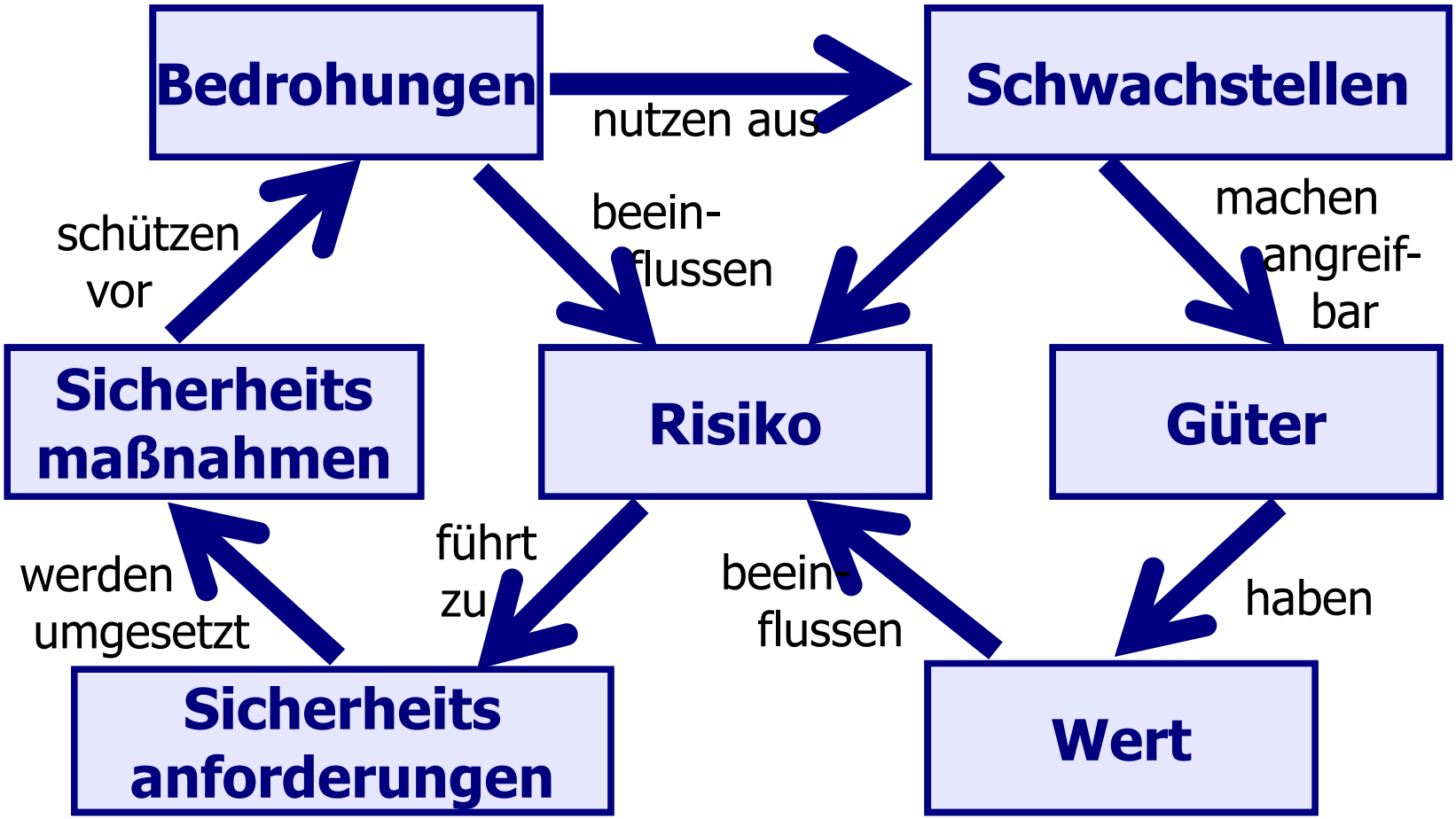
- **BSI** („Bundesamt für Sicherheit in der Informationstechnik“)
  - BSI-Standard 200-1:
    Managementsysteme für Informationssicherheit
    Kompatibel zu ISO 27001/27002
  - BSI-Standard 200-2:
    IT-Grundschutz-Methodik
    Basis ist das „IT-Grundschutzkompendium“ des BSI
    (→ liegt als pdf-Datei im pub)
  - BSI-Standard 200-3:
    Risikomanagement

IT-Grundschutzkompendium des BSI

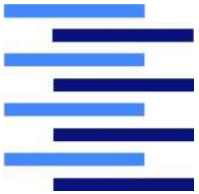


- Aufbau:
  - Gefährdungskataloge (Bedrohungen)
    - Elementare Gefährdungen, höhere Gewalt
    - Organisatorische Mängel und menschliche Fehlhandlungen, vorsätzliche Handlungen
    - Technisches Versagen
  - (Schutz-)Maßnahmenkataloge in Form von Bausteinen
    - Infrastruktur, Notfallvorsorge
    - Organisation und Personal
    - Hardware, Software, Kommunikation
- Anwendung:
  - Prüfung existierender IT-Systeme
  - Hilfe bei der Entwicklung einer Sicherheitsstrategie

Zusammenfassung



Ende des 1. Kapitels:
Was haben wir geschafft?



Einführung – Grundlegende Begriffe

1. IT-Sicherheit - Worum geht es hier eigentlich?
2. Security Engineering