IT-Sicherheit

Prof. Dr. Reiner Hüttl

Inhalt

- Motivation, Ziele
- Verschlüsselung
- Digitale Signaturen und PKI
- Applikationssicherheit
- Secure Software Engineering
- Authentifizierung, Autorisierung
- Sichere Kommunikation
- Datenschutz
- Regeln zur IT-Sicherheit

Organisation

- Prüfung: Mündliche Prüfung, 15 Minuten
- Die Folien sind kein vollständiges Skript!
  z.T. in deutsch z.T. in englisch
  z.T. subjektive Meinungen die diskutiert werden können / sollten
- Zur Prüfung sind notwendig
  - Teilnahme an Videokonferenzen, Chats
  - zusätzliche persönliche Mitschriften
  - Eigene Recherche (Bücher, Web, Videos)
  - Teilnahme an den Übungen
  - Ausführen der Online Aufgabe (Übungen, Tests, …)

Literatur

Hier kann man alles nachlesen was man in den Folien nicht verstanden hat oder zu knapp behandelt worden ist.

Zusätzlich gibt es in der Bibliothek noch weitere E-Books zum Vertiefen

- Claudia Eckert: IT-Sicherheit, De Gruyter Studium, 2018
- Jörg Schwenk: Sicherheit und Kryptographie im Internet, Vieweg, 2014 **(E-Book)**
- Klaus-Rainer Müller: IT-Sicherheit mit System, Vieweg, 2018 **(E-Book)**
- Wolfgang Ertl: Angewandte Kryptographie, Hanser Verlag, 2019 **(E-Book)**
- Matthias Rohr: Sicherheit von Webanwendungen in der Praxis, Springer Vieweg, 2018 **(E-Book)**
- Klaus Schmeh: Kryptografie, dpunkt.verlag, 2013
- Schäfer G., Roßberg M: Netzsicherheit, dpunkt.verlag, 2014
- Bruce Schneier: Applied cryptography, John Wiley & Sons, 2015 **(E-Book)**
- Bruce Schneier: Secret and Lies, John Willey & Sons, 2015 **(E-Book)**
- Inge Hanschke: Informationssicherheit & Datenschutz - einfach & effektiv, Hanser, 2019 **(E-Book)**
- Steffen Wendzel: IT-Sicherheit für TCP/IP- und IoT-Netzwerke, Springer Vieweg, 2018 **(E-Book)**

Webseiten

- http://www.bsi.de (Bundesamt für Sicherheit in der Informationstechnik)
- http://www.cert.org/ (US-Computer Readiness Team, analysieren und veröffentlichen vulnerabilities)
- http://www.teletrust.de/ (Verein zur Förderung der Vertrauenswürdigkeit in den IuK-Technologien)
- http://www.heise.de/security/ (Alerts, Artikel, Tools, Foren)
- http://www.kes.info/ (Zeitschrift für Informationssicherheit)
- http://www.nsa.gov/ (National Security Agency/Central Security Service in USA)
- http://www.rsa.com (Security Provider)

IT-Sicherheit

Kapitel 1: Motivation, Ziele

Prof. Dr. Reiner Hüttl, FH Rosenheim, © 2020, 15.03.2021

Der Shell-Schock: Bash-Sicherheitslücke (2014)

- Erlaubt Ausführen von Schadcode
- In Umgebungsvariablen lässt sich Code einfügen der beim S
  Shell ungeprüft ausgeführt wird
- Test mit folgender Anweisung
  `env x='() { :;}; echo vulnerable' bash -c ""`
  → Ausgabe `vulnerable`
- Programmierfehler: Fehlerhafter Parser bei Funktionsdefinition von Umgebungsvariabalen
- Wie kann man sich schützen?

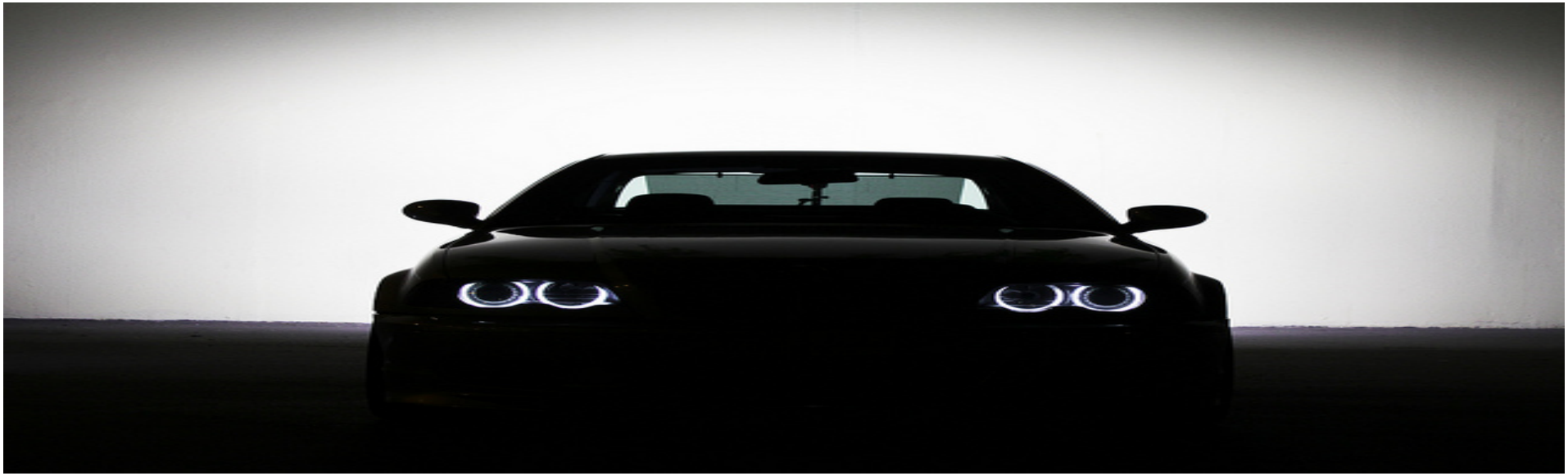
https://www.heise.de/security/meldung/ShellShock-Standard-Unix-Shell-Bash-erlaubt-das-Ausfuehren-von-Schadcode-2403305.html

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=2ahUKEwjm-ZbT0qzoAhViRBUIHcfpBiMQFjADegQIBhAB&url=https%3A%2F%2Fwww.owasp.org%2Fimages%2F1%2F1b%2FShellshock_-_Tudor_Enache.pdf&usg=AOvVaw1o9Chco8_W946RsItbrmsY

Sicherheitslücke bei BMW Connected Drive (2015)

- Use Case: Die Tür des Fahrzeugs kann über Remote App durch den Besitzer entriegelt werden

- **Misuse Case**: Ein Hacker kann mit einer tragbaren Mobilfunk-Basisstation Daten an das Fahrzeug senden um die Tür zu entriegeln



Schwachpunkte im Sicherheitskonzept ermöglichen den Hack

- Zum Zeitpunkt der Untersuchung hatte ConnectedDrive sechs Schwachpunkte, die seine Sicherheit kompromittierten:
  - BMW verwendet in allen Fahrzeugen dieselben symmetrischen Schlüssel.
  - Einige Dienste verzichten bei der Datenübertragung zum BMW-Backend auf eine Transportverschlüsselung.
  - Die Integrität der ConnectedDrive-Konfiguration wird nicht geschützt.
  - Die Combox verrät mit NGTP-Fehlermeldungen die VIN des Fahrzeugs.
  - Per SMS versendete Daten im NGTP-Format werden mit dem unsicheren DES-Verfahren verschlüsselt.
  - Die Combox hat keinen Schutz vor Replay-Angriffen.

- Quelle: http://www.heise.de/ct/ausgabe/2015-5-Sicherheitsluecken-bei-BMWs-ConnectedDrive-2536384.html

Es geht noch besser: Jeep Cherokee (2015)

- Durch eine Schwachstelle im Infotainment-System konnten Sicherheitsforscher die Kontrolle über einen Jeep übernehmen
  - Radio, Klima, …
  - Bremsen
  - Lenkrad
  - Rückwärtsgang
  - …
- Die Attacke geht über das Internet.

Video: http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Auch Staaten werden angegriffen: Bundestag-Hack (2015)

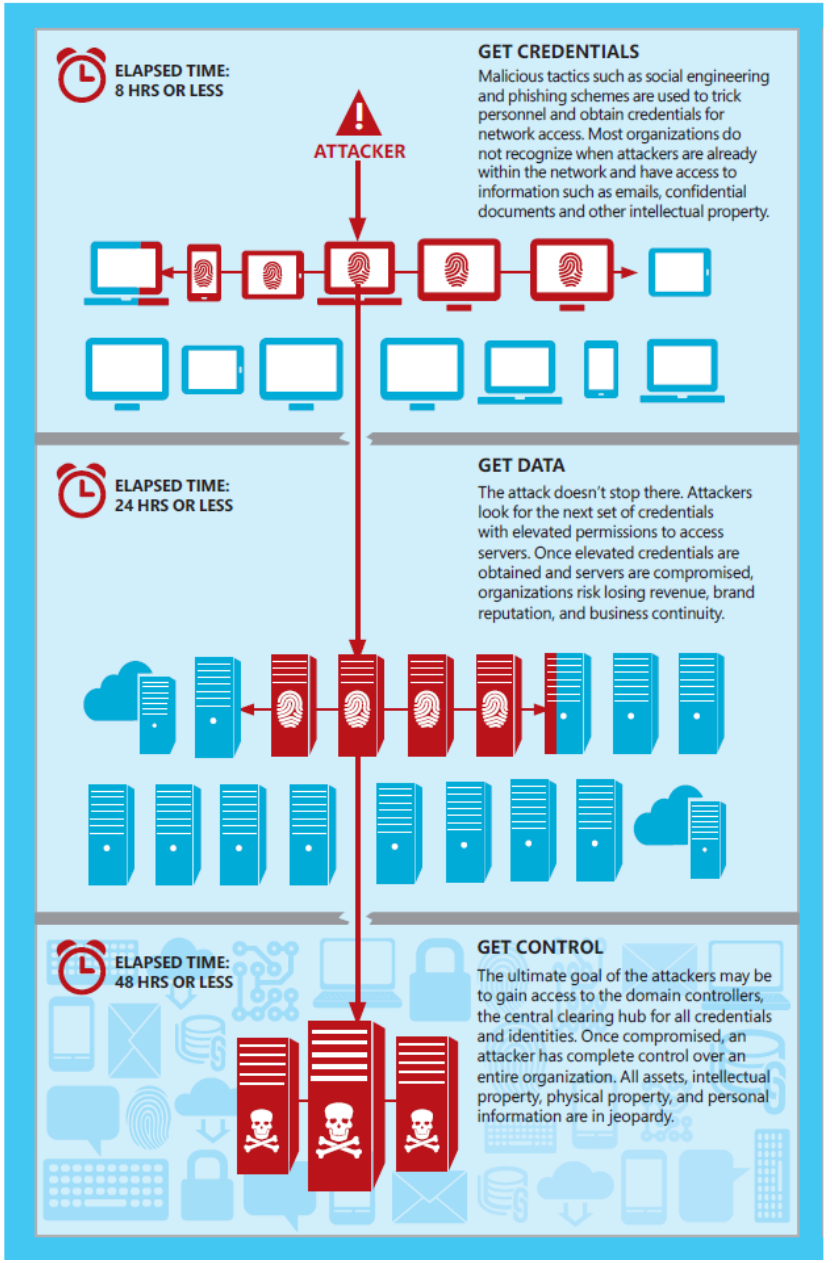
- Angriff auf Abgeordneten-Rechner mit Mail-Anhang oder **Drive-by-Download**
- Diebstahl von Credentials für Domänenadministratoren-Knoten mit Open-Source-Tool **mimikaz**

- **Pass-the-Hash (PtH) Attack**
  Angreifer versucht nicht Passwort aus Hash zu berechnen, sondern kann mit Hash selbst Zugang zu Systemen erhalten (meist über Schwachstellen in Single-Sign-On Systemen)
- Ausbreitung im internen Netz mit gängigen Methoden und öffentlich verfügbaren Tools

https://de.m.wikipedia.org/wiki/Datei:Bonn_Bundestag_Plenarsaal1.jpg

Anatomy of a PtH Attack

- Attack Activities
  - **Privilege escalation**
    attackers try to gain higher-level permissions on a system or network
  - **Lateral movement**
    attackers tries to enter and control remote systems on a network and subsequently gaining access to it
- Mitigations
  - Restrict and protect high privileged domain accounts
  - Restrict and protect local accounts with administrative privilleges
  - Restrict inbound traffic with firewalls

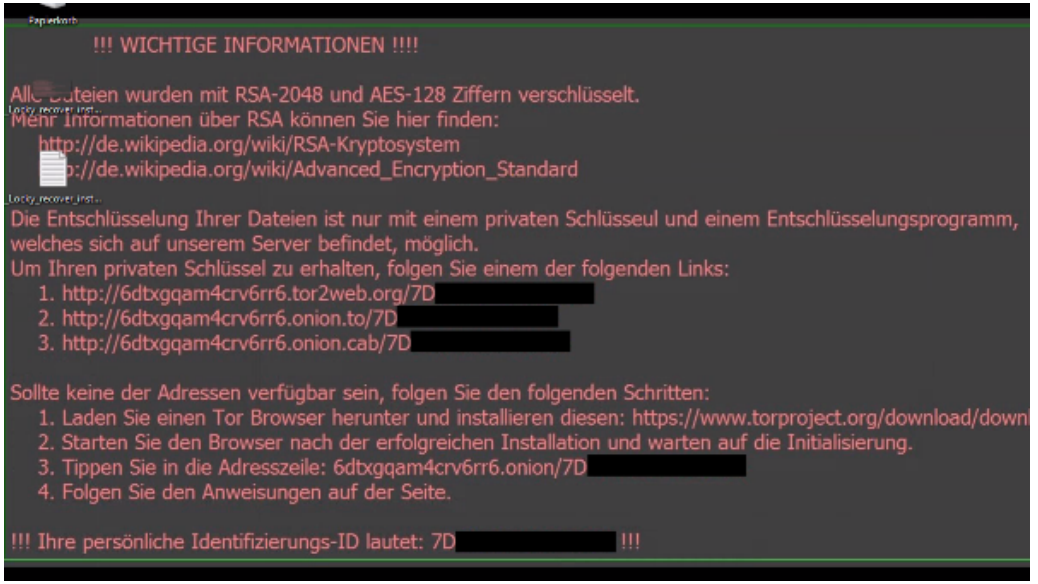


https://de.m.wikipedia.org/wiki/Datei:Bonn_Bundestag_Plenarsaal1.jpg

https://www.microsoft.com/en-us/download/details.aspx?id=36036

Das kann jeden treffen: Locky Ransomeware (2016)

- In einer E-Mail ist ein Anhang der ein Makro enthält
- Makro speichert eine Datei die Malware nachlädt
- Malware verschlüsselt Dateien auf Computer und zugängige Laufwerke
- Malware löscht auch alle Shadow Copies von Dateien
- Wie kann man sich schützen?



https://nakedsecurity.sophos.com/2016/02/17/locky-ransomware-what-you-need-to-know/

Auch die Hardware macht Probleme (2018)

- Ursache
  - Out-of-order execution in Prozessoren
  - Speculative execution
  - Eine Seitentabelle für User Prozesse und Kernel
- Angriffe
  - **Meltdown**
    - Zugriff auf Speicher (Cache) fremder Prozesse provoziert durch Exception
  - **Spectre**
    - Interpretierte Skriptsprachen wie JavaScript extrahieren Informationen aus dem Adressraum des Webbrowsers
- Wie kann man sich schützen?
  - Kernel-Page-Table-Isolation (KPTI)
  - Browser Patches
  - Problem: Performance der Prozessoren wird sinken

Weitere Details siehe:
https://www.heise.de/security/meldung/FAQ-zu-Meltdown-und-Spectre-Was-ist-passiert-bin-ich-betroffen-wie-kann-ich-mich-schuetzen-3938146.html

Computerviren und Malware

- **Computervirus**
  - Programmcode, der nur als Programmteil innerhalb eines Wirtsprogramms funktionsfähig ist
  - bei Ablauf des Wirtsprogramms kommt auch der Viruscode zur Ausführung und kann sich verbreiten und schädliche Wirkung entfalten
  - Varianten: Programm-, Datei-, Boot-, Makro-Viren

- **Wurm** („der Autonome“)
  - eigenständiges Programm, das Kopien von sich selbst erzeugt und zum Ablauf bringt.
  - treten meist in Netzwerken auf;
  - Fortpflanzung durch Kopieren und Verschicken des Duplikats an andere Systeme
  - Unterschied zu Computerviren: Würmer sind selbstständige Programme.

Malware

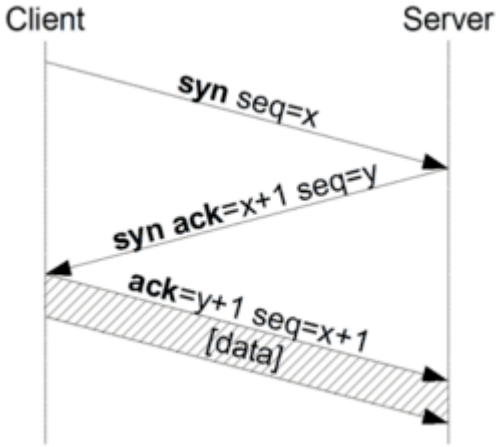
- **Trojanisches Pferd** („der Heimliche“)
  - eigenständiges Programm, das eine nicht dokumentierte Routine enthält, die eine unerwartete, meist destruktive Zusatzfunktion ausführt.
  - beliebtes Programm zum illegalen Sammeln von Passwörtern
  - Unterschied zu Computerviren und Würmern: Trojanisches Pferd zeigt keine Vermehrung oder Bewegung, sondern bleibt immer an der gleichen Stelle im gleichen System.
- **Spyware**: überwacht Aktivitäten des Computernutzers, sammelt sensible Daten und sendet sie an den Ersteller
- **Ransomware**: Verschlüsselt die Daten und fordert Lösegeld für die Freigabe
- **Adware**: Aggressive Werbesoftware, kann Sicherheit beeinträchtigen um Werbung zu schalten

Malware

- **Bots**: fernsteuerbare Schadsoftware, mehrere infizierte Computer bilden ein Botnet
- **Rootkit**: gewähren dem Angreifer Administrator Rechte und Remote-Zugriff auf das infizierte System
- **Keylogger**: zeichnet die Tastatureingaben der Benutzers auf uns sendet sie an den Angreifer
- **Exploit**: Schadsoftware, die Verwundbarkeiten ausnutzen. Sie dient dazu, Angriffe auf verwundbare Software durchzuführen.
- Quellen:
  - https://www.youtube.com/watch?time_continue=4&v=n8mbzU0X2nQ&feature=emb_logo
  - https://www.heise.de/tipps-tricks/Was-ist-Malware-4614964.html
  - Steffen Wendzel: IT-Sicherheit für TCP/IP- und IoT-Netzwerke, Springer Vieweg, 2018 (E-Book)

Denial of Service Attacken

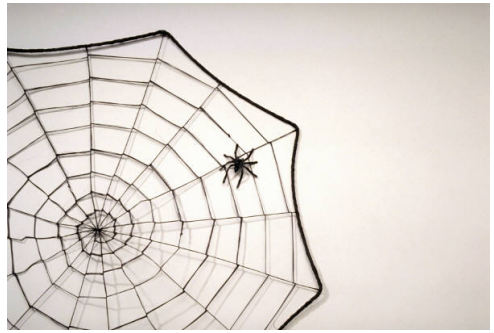
- Als **DoS**-Angriff bezeichnet man einen Angriff auf ein IT-System mit dem Ziel, einen oder mehrere seiner Dienste arbeitsunfähig zu machen. In der Regel geschieht dies durch Überlastung.
- DOS: Verfügbarkeit eines Rechners stören
- Beispiel: TCP SYN-Flooding



https://deacademic.com/dic.nsf/dewiki/1221679

- DDos Verteilte DOS-Angriffe: Angriff erfolgt koordiniert von einer größeren Anzahl anderer Systeme
  - Phase 1: Installation von Agenten auf ungeschützten Rechnern
  - Phase 2: Angriffsphase

Soziale Netzwerke



- Problem: freizügiges Bereitstellen von Informationen
- Identitätsdiebstahl (Evil-Twin)
  ermöglicht: Rufschädigung = Fälschen einer Identität mit zusammengetragenen persönlichen Daten zu einer Person
- Entlocken von geheimen Informationen
- Möglicher Weg für das Einspeisen von Schadcode
- Gefahr durch Angriffe auf die Webanwendung (CSRF, XSS usw.)

Sicherheit = Security + Safety

- **Security**: (Informationssicherheit): keine unautorisierte Informationsveränderung
  - Schutz vor beabsichtigten, zielgerichteten und böswilligen Angriffen
  - Erkennen und Abwehr von Angriffen
  - Minimierung der Verwundbarkeit von Werten und Ressourcen
  - Bsp: DDOS, Spam, Abhören, Datenmanipulation
- **Safety**: (Funktionssicherheit): System funktioniert
  - Schutz vor unbeabsichtigten Ereignissen (menschliches und technisches Versagen)
  - Erkennen und Abwehr von Störungen, die die korrekte Funktionalität und Betriebssicherheit beeinträchtigen
  - Spezifikation der gewünschten Funktionalität und Erkennen von Abweichungen vom gewünschten Verhalten
  - Bsp: Systemausfälle, Leitungsausfälle, Verschleiß, Bedienungsfehler
- Sichere Systeme erhält man durch eine Kombination der Aspekte Security und Safety

Grundwerte der IT-Sicherheit: Verfügbarkeit, Integrität, Vertraulichkeit

Sicherheitsziele

CIA = Confidentiality, Integrity, Availability

Verfügbarkeit (Availability)

Daten und Funktionen sind stets verfügbar, wenn sie benötigt werden und für diejenigen, die sie benötigen.

Integrität (Integrity)

Keine unbefugte Manipulation von Daten und Funktionen

Vertraulichkeit (Confidentiality)

Keiner erhält unerlaubten Zugriff auf Daten, Nachrichten und Funktionen.

Nicht-Abstreitbarkeit (Non Repudiation)

Jede durchgeführte Aktion ist nachweisbar genau so passiert

Authentizität (Authenticity)

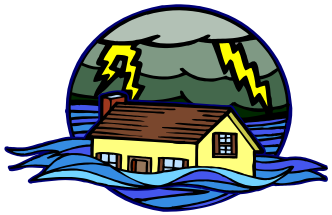
Echtheit von Daten, Zurechenbarkeit von Nachrichten

Details siehe z.B. https://www.kryptowissen.de/schutzziele.php

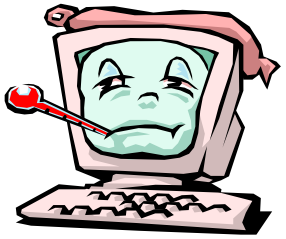
Weit verbreitete Fehleinschätzungen (siehe BSI)

- Bei uns ist noch nie etwas passiert
- Was soll bei uns zu holen sein, so geheim sind unsere Daten nicht
- Unser Netz ist sicher
- Unsere Mitarbeiter sind vertrauenswürdig

IT-Sicherheit ist …gefährdet durch



- **Höhere Gewalt**: Feuer, Wasser, Blitzschlag, Krankheit, ...
- **Organisatorische Mängel**: Fehlende oder unklare Regelungen, fehlende Konzepte, ...
- **Menschliche Fehlhandlungen**: "Die größte Sicherheitslücke sitzt oft vor der Tastatur"
- **Technisches Versagen**: Systemabsturz, Plattencrash, ...
- **Vorsätzliche Handlungen**: Hacker, Viren, Trojaner, ...



Wichtige Begriffe

- Eine **Schwachstelle (vulnerability)** ist ein sicherheitsrelevanter Fehler eines IT-Systems. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und ein System geschädigt wird. Durch eine Schwachstelle wird ein System anfällig für Bedrohungen.

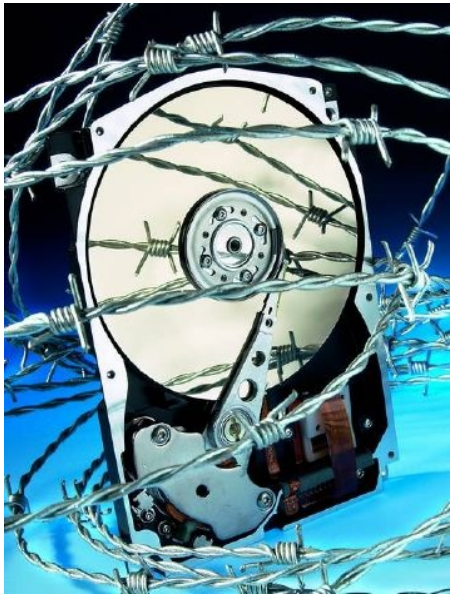
- **Bedrohungen (threat)** ist ein Umstand oder Ereignis, das eine oder mehrere Schwachstellen eines Systems ausnutzt, um ein oder mehrere Schutzziele zu gefährden.

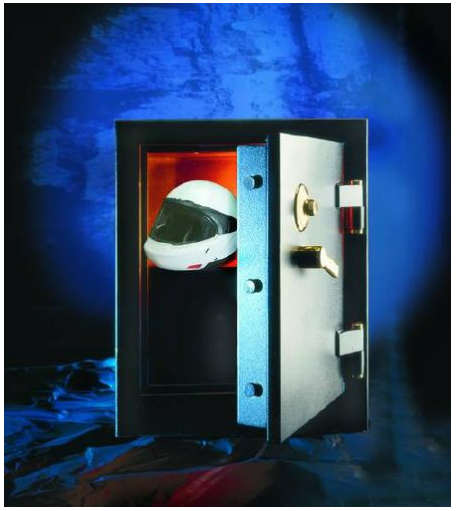
- Das **Risiko R (risk)** einer Bedrohung ist die Wahrscheinlichkeit E des Eintritts eines Schadensereignisses und die Höhe des potentiellen Schadens S, der daraus resultieren kann: $R=E \cdot S$

- Unter einem **Angriff (attack)** verstehen wir einen nicht autorisierten Zugriff auf ein Asset (schützenswertes Gut)

Mögliche Maßnahmen

- Passwort-Policy
- Virenschutz, Firewall
- Notfallplan
- Outsourcing-Regelung
- Datensicherungskonzept
- Zuständigkeiten festlegen
- Regeln für sichere SW-Entwicklung
- Schulung und Information der Beteiligten
- Kryptographie: Verschlüsselung, Signaturen
- usw.





(IX Thema 01 Security)

Schritte zur IT Sicherheit: ISMS (Informations Sicherheits Management System)

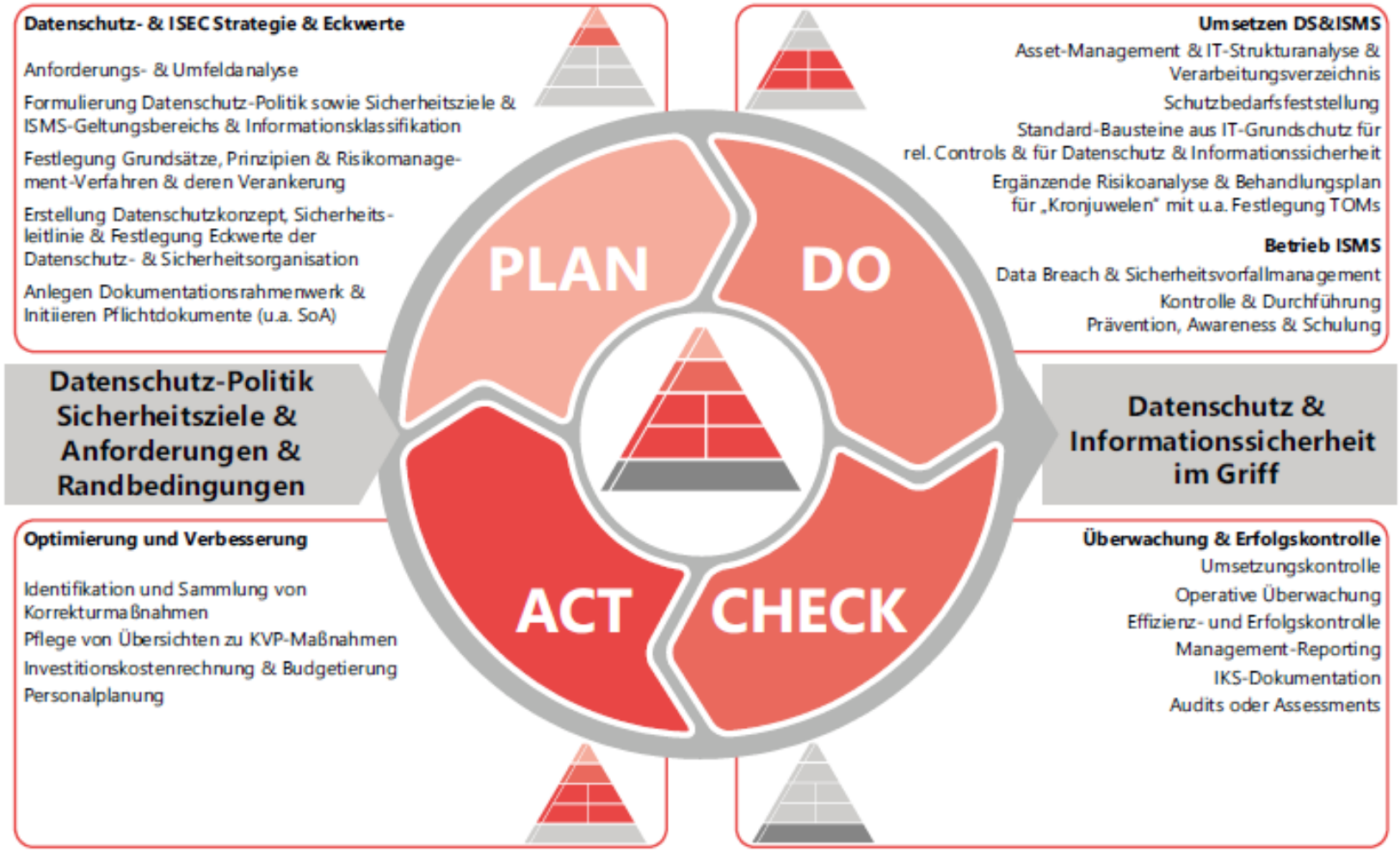
- Strategische **Sicherheitsziele** festlegen

  Verfügbarkeit **Integrität** **Vertraulichkeit**

- Sicherheitsleitlinie erstellen
- Aufgaben und Verantwortungen verteilen
- Kritische Applikationen und Daten identifizieren
- Risikobewertung
- Sicherheitsmaßnahmen umsetzen
- Informationspolitik und Schulung
- Regelmäßige Audits durchführen (z.B. BSI, TÜV-IT, ISO 27001)

Quelle: Inge Hanschke: Informationssicherheit & Datenschutz - einfach & effektiv, Hanser, 2019

PDCA-Zyklus eines ISMS



Quelle: Inge Hanschke: Informationssicherheit & Datenschutz - einfach & effektiv, Hanser, 2019

Was ist zu beachten?

- **Sicherheit ist ein kontinuierlicher Prozess !!!**
  - Alle Maßnahmen müssen regelmäßig überprüft werden
  - Neue Gefahren müssen erkannt werden
  - Neue Maßnahmen müssen bei Bedarf eingeführt werden
  - Alle sind von diesem Prozess betroffen und daran beteiligt
- **Die größte Schwachstelle ist der Mensch**
  - Unwissenheit
  - Unachtsamkeit
  - Bequemlichkeit
  - Zeit- und Termindruck