# ESSE Einführung in Security – VO 01: Einführung in IT-Sicherheit

Christian Schanes, Florian Fankhauser, Franz Mairhofer

# Agenda

Brainstorming IT-Sicherheit

Security Nachrichten

Herausforderungen in der IT-Sicherheit

Definitionen

Sicherheitsziele

Schutzbedarf

Angriffe

Mehrere Phasen eines Angriffs

Lösungen

Literaturempfehlungen, Links

*Wie sind Sie bisher mit IT-Sicherheit konkret in Berührung gekommen?*

*Was verstehen Sie unter IT-Sicherheit?*

# IT-Sicherheit

# Security – Auswahl aus 1 Woche Nachrichten auf https://www.heise.de/newsticker/ – 1/6

- 28.09.2023
  - Liechtenstein: Kritik an IT-Sicherheit beim E-Gesundheitsdossier zurückgewiesen
  - Balkonkraftwerke: Bedrohliche Sicherheitslücken bei Hoymiles
  - Zehn Sicherheitslücken in Chrome geschlossen, eine wird bereits ausgenutzt
  - Unzählige Anwendungen betroffen: Chaos bei WebP-Lücke
  - Balkonkraftwerke: Hoymiles-Sicherheitslücke teilweise geschlossen
  - ING, Deutsche Bank und Co. wegen MOVEit-Lücke bei Majorel doch stärker betroffen
  - Verbraucherschützer: Betreiber von Zyklus-Apps schludern beim Datenschutz

# Security – Auswahl aus 1 Woche Nachrichten auf https://www.heise.de/newsticker/ – 2/6

- 29.09.2023
  - Jetzt patchen! Angreifer haben Netzwerkgeräte von Cisco im Visier
  - 60.000 geklaute Regierungsmails: Erste Zahlen nach Microsofts Cloud-Key-Debakel
  - Balkonkraftwerke: Hoymiles schließt Sicherheitslücken
- 30.09.2023
  - Kritische Lücke im Mailserver Exim
  - Cybercrime: Erpressergang greift Hotelkette MotelOne an
  - Chatkontrolle: Europol will ungefilterten Zugriff auf Daten von WhatsApp & Co.

# Security – Auswahl aus 1 Woche Nachrichten auf https://www.heise.de/newsticker/ – 3/6

- 01.10.2023
  - E-Voting: Bedrohung durch Cyberattacken und Vorwürfe der Wahlmanipulation
- 02.10.2023
  - Fritzbox-Sicherheitsleck analysiert: Risiko sogar bei deaktiviertem Fernzugriff
  - Gmail: E-Mail-Verschlüsselung jetzt auch in der App
  - Jetzt patchen! Exploit für kritische Sharepoint-Lücke veröffentlicht
  - BSI-Umfrage: Kritische Infrastrukturen haben Nachholbedarf bei IT-Sicherheit

# Security – Auswahl aus 1 Woche Nachrichten auf https://www.heise.de/newsticker/ – 4/6

- 03.10.2023
  - Drei Fragen und Antworten: Der beste Schutz für das Active Directory
  - Exim-Lücke: Erste Patches laufen ein
  - Windows stufte Tor Browser fälschlicherweise als Malware ein
  - Jetzt patchen! Ransomware schlüpft durch kritische TeamCity-Lücke
  - Erste Angriffe gesichtet: Angreifer können über Lücken in WS_FTP Daten löschen

# Security – Auswahl aus 1 Woche Nachrichten auf https://www.heise.de/newsticker/ – 5/6

- 04.10.2023
  - Webbrowser: Update für Google Chrome schließt Lücke mit hohem Risiko
  - Patchday: Attacken auf Android 11, 12 und 13 beobachtet
  - Rechteausweitung durch Pufferüberlauf in glibc
  - Weniger Spam und Phishing: Gmail bekommt neue Standards
- 05.10.2023
  - Jetzt patchen! Confluence Data Center: Angreifer machen sich zu Admins
  - Noch sicherer: TypeScript 5.3 importiert Attribute
  - Wieder Exploit-Update für iOS und iPadOS – das wohl auch Hitzeproblem fixt

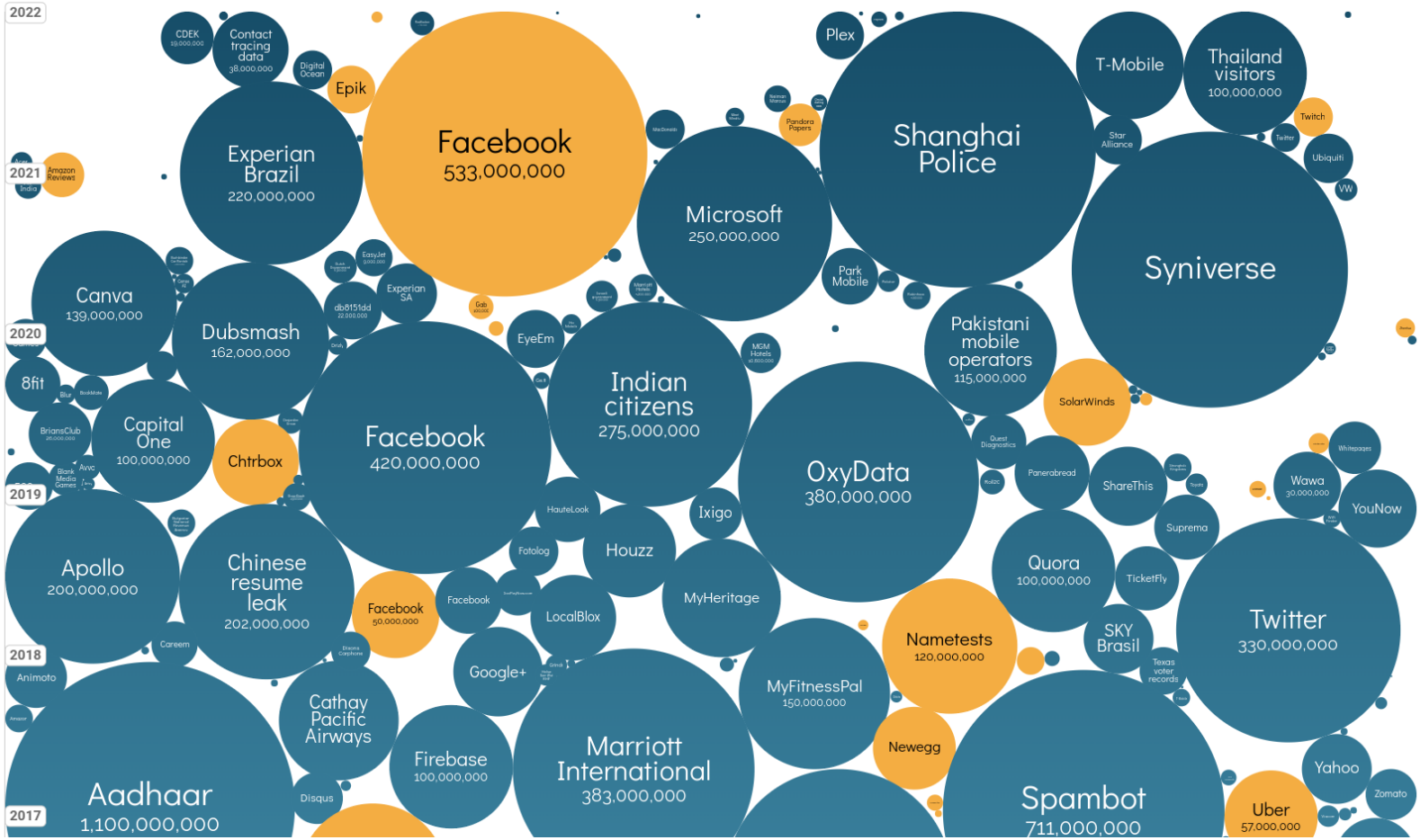
# Security – Auswahl aus 1 Woche Nachrichten auf https://www.heise.de/newsticker/ – 6/6

- 05.10.2023 (ff)
  - Phishing-Warnung: Angebliche Mails vom Europäischen Amt für Betrugsbekämpfung
  - KI-Tool: Kritische Sicherheitslücken in TorchServe
  - Root- und DoS-Attacken auf Cisco-Produkte möglich
  - Malware-Schutz: Watchguard EPDR und AD360 schließen Sicherheitslücken
  - MotelOne-Hack: Daten veröffentlicht, Datenschützer und Gäste in Sorge

# Weitere Security-Nachrichten

- Narkosegerät gehackt: Beatmungsfunktion gestoppt
- Österreichische Forscher entdecken TLS-Schwachstelle
- Moderne Yachten sind nicht ausreichend vor Hackern geschützt
- Börse Kucoin gehackt: Kryptogeld und Tokens im Millionenwert gestohlen
- Studie: Angreifer wollen ins Homeoffice – millionenfach über RDP-Verbindungen
- Ransomware gangs are complaining that other crooks are stealing their ransoms
- Brückenbau: LAN-Kabel als Antenne überwindet Air-Gaps
- Twitch-Leak: Einnahmen aller Streamer und Quellcodes veröffentlicht
- Hacker in Italien spionierten tausende Haushalte mit Webcams aus
- Regierung verschärft Strafen für Cybercrime-Delikte

# Viele, auch große, Unternehmen sind von Angriffen betroffen




(Vergleiche `https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/`)

# IT-Sicherheit/Computer-Sicherheit/Netzwerk-Sicherheit

- ...also Angriffe und Bedrohungen, wie sie nicht nur in der IT stattfinden!
- Unterschiede
  - Automatisierung
  - Angriff kann entfernt stattfinden
  - Verbreitung von Angriffstechniken
  - (Vermeintliche) Anonymität
  - Komplexität

# Herausforderungen in der IT-Sicherheit – 1/3

- Sicherheit ist nicht wichtig, [den Leuten] ist wichtig, dass es funktioniert!
- Das IT-Sicherheits-Team sagt immer *Nein!*
- Sicherheit ist ein Prozess (Bruce Schneier)
- Sicherheit oft schwer greifbar, unverständlich

- Programmierung meist Fokus der Lehre
- Programmieren ist einfach – das kann jeder/jede!
- Softwareentwicklungsprozess
- Projektumfeld – Termindruck, Funktionalität
- Test von Software auf spezifizierte Funktionalität
- Security vs. Usability, Security und Usability

# Herausforderungen in der IT-Sicherheit – 2/3

- Jede Software potenziell betroffen
  - Betriebssysteme (Windows, Linux, MacOS, Android,...)
  - Applikationen und Programmiersprachen (Office, Web-Browser, Java,...)
- Komplexität der Software/Projekte
- Zusammenspiel vieler Komponenten
- Systeme wachsen („never touch a running system“)
- Mitarbeiter:innen – Know-How/Spezialisierung
- Fülle an News, Sicherheitslücken,...
- Zeitaufwand teilweise hoch

# Herausforderungen in der IT-Sicherheit – 3/3

- Vernetzung (z.B. Internet)
- Mobilität (Notebook, Handy,...)
- Kabellose Übertragung: WLAN, Bluetooth, RFID,...

- Kreativität der Angreifer:innen (Trojaner, Phishing, Domainnamen,...)
- Ransomware
- Zero-Day-Angriffe
- Bug Bounties
- Weakest Link

# Weakest Link. . .

Over the Hedge, 2006-04-23

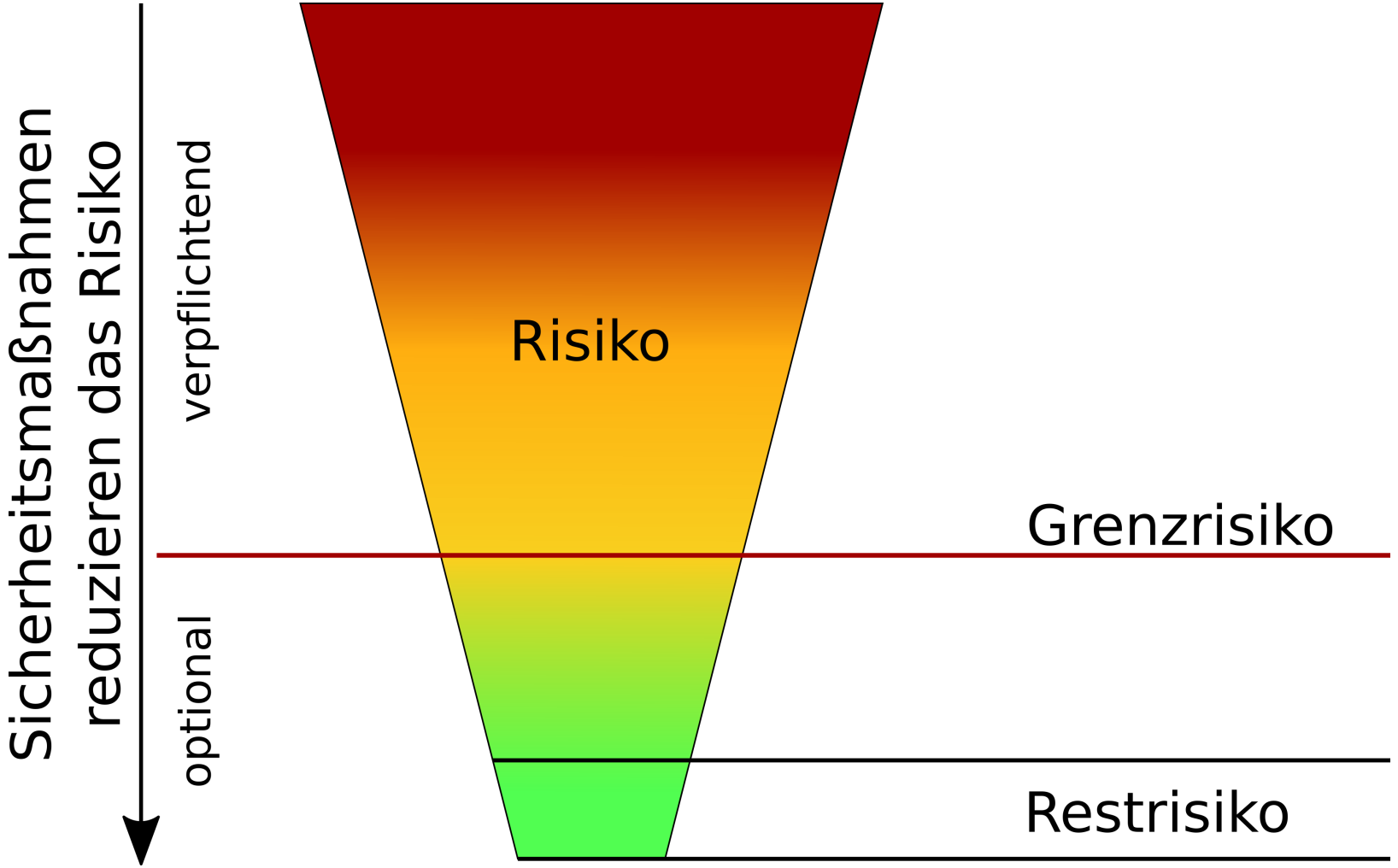
# Software Depenencies

https://xkcd.com/2347/

# Definition Sicherheit/Risiko

- Definition nach DIN VDE 31000
  - „Sicherheit ist eine Sachlage, bei der das [Rest-]Risiko nicht größer als das Grenzrisiko ist.“
  - „Das Grenzrisiko ist das größte noch vertretbare Risiko eines bestimmten technischen Vorganges oder Zustandes.“
  - „Eine absolute Sicherheit ohne jegliches Risiko gibt es weder in der Technik noch in der Natur.“
- Risiko = Schaden $*$ Eintrittswahrscheinlichkeit

# Risiko, Grenzrisiko, Restrisiko und Sicherheitsmaßnahmen



# Sicherheitsziele/Schutzziele

- Betrachtung unterschiedlicher Sicherheitsziele, i.A. v.a.
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
  - → „*CIA Triad*“ (Confidentiality, Integrity, Availability)
- Weitere Sicherheitsziele sind z.B.
  - Authentizität
  - Nichtabstreitbarkeit

(Vergleiche BSI: IT-Grundschutz-Kataloge)

# Schutzbedarf

Kategorien können z.B. sein:

- normal
- hoch
- sehr hoch

- gering
- mittel
- hoch
- sehr hoch

# Weitere Definitionen

**Bedrohung/Threat** Potenzielle Verletzung der IT-Sicherheit

**Angriff/Attack** Aktion, die eine Bedrohung wahr werden lässt

**Angreifer:in/Attacker** Subjekt, das einen Angriff durchführt

**Schwachstelle/Vulnerability** Sicherheitsfehler im System, welchen man für Angriff ausnutzen kann

**Exploit** Software, die eine Schwachstelle ausnützt

(Vergleiche M. Bishop: Introduction to Computer Security)

# Angriffe auf Systeme

Wenn jemand in ein System (Hardware, Software, Policies, Organisation,. . . ) einbricht,

nutzt dieser Angreifer/diese Angreiferin Fehler in Prozessen, Technik oder Management (oder einer Kombination davon) aus,

um unberechtigt auf Daten zuzugreifen oder Aktionen auszulösen.

(Vergleiche M. Bishop: Introduction to Computer Security)

# Kategorisierung von Angriffen und Beispiele

- Unberechtigter Zugriff auf Daten
  - Sniffing
  - Man in the Middle (MitM)
- Täuschung/Akzeptanz von falschen Daten
  - Spoofing
  - MitM
- Unterbrechung der Funktionalität
  - Denial of Service (DoS), Distributed Denial of Service (DDoS)
- Widerrechtliche Verwendung
  - Command Injection

(Vergleiche auch RFC 2828)

# Mehrere Phasen eines Angriffs

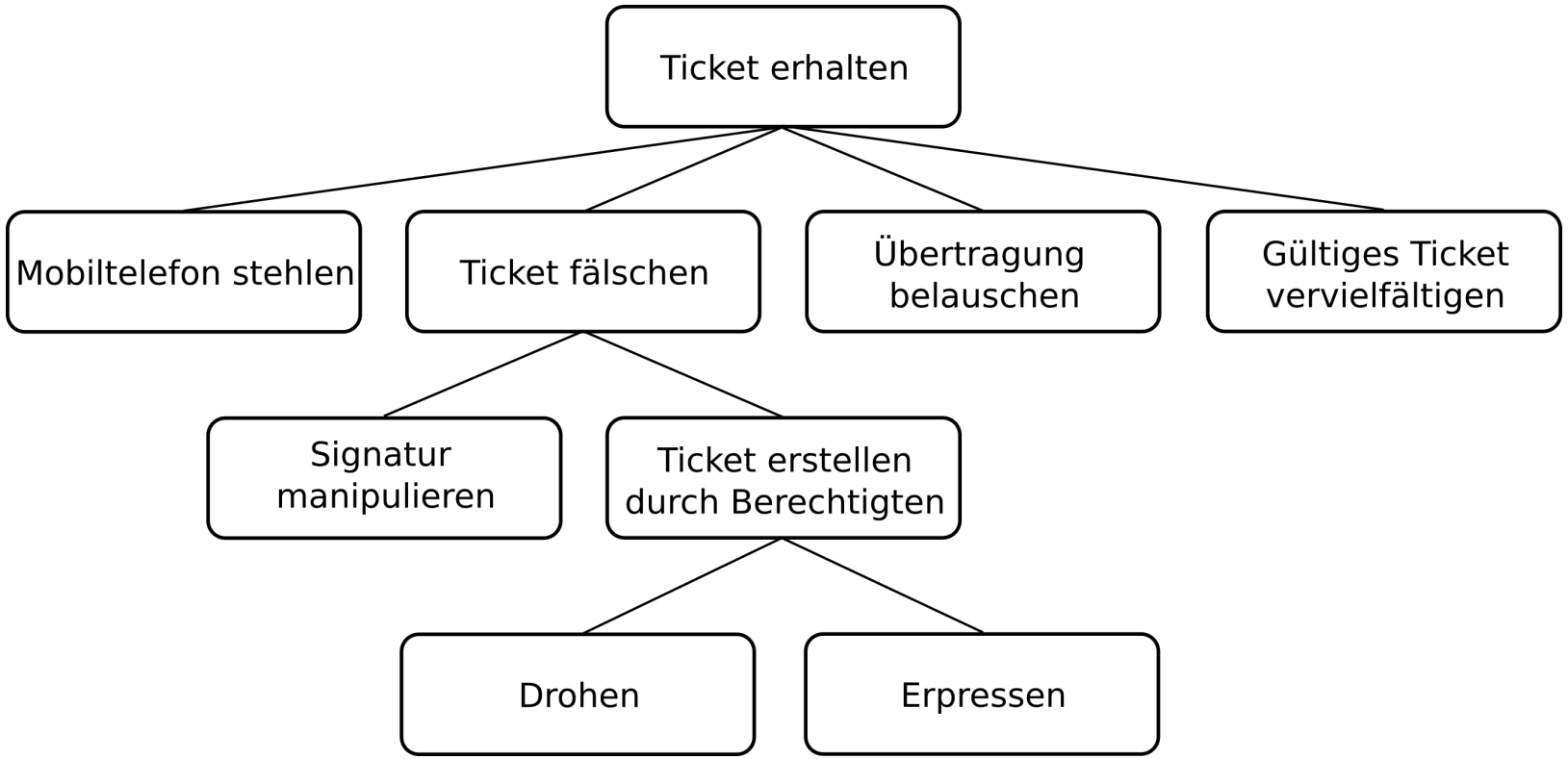
- Sammeln von Daten über das Angriffsziel
  - z.B. Verwendete Systeme, User-Kennungen,...
- Ausnutzen von gefundenen Sicherheitsproblemen (Zugriff, Ausweiten der Rechte)
  - z.B. SQL-Injection auf eine Datenbank
- Aufrechterhaltung des Zugriffs
  - z.B. Anlegen eines eigenen Benutzer-Accounts
- Verwischen von Spuren
  - z.B. Löschen von Logfiles

(Vergleiche E. Skoudis, T. Liston: Counter Hack Reloaded)

# Risiko- und Bedrohungsanalyse

- Gruppierung von Bedrohungen (z.B. nach)
  - Zielobjekt
  - Urheber:in
  - Motivation/Absicht
  - Wahrscheinlichkeit des Auftretens
  - Auswirkungen/Kosten
- Auflistung der Bedrohungen
- Risikoanalyse/Risikobewertung
- Sicherheitsmaßnahmen
- Restrisikoabschätzung

# Beispiel eines Angriffsbaums



# Bedrohungspotenzial von Angreifer:innen

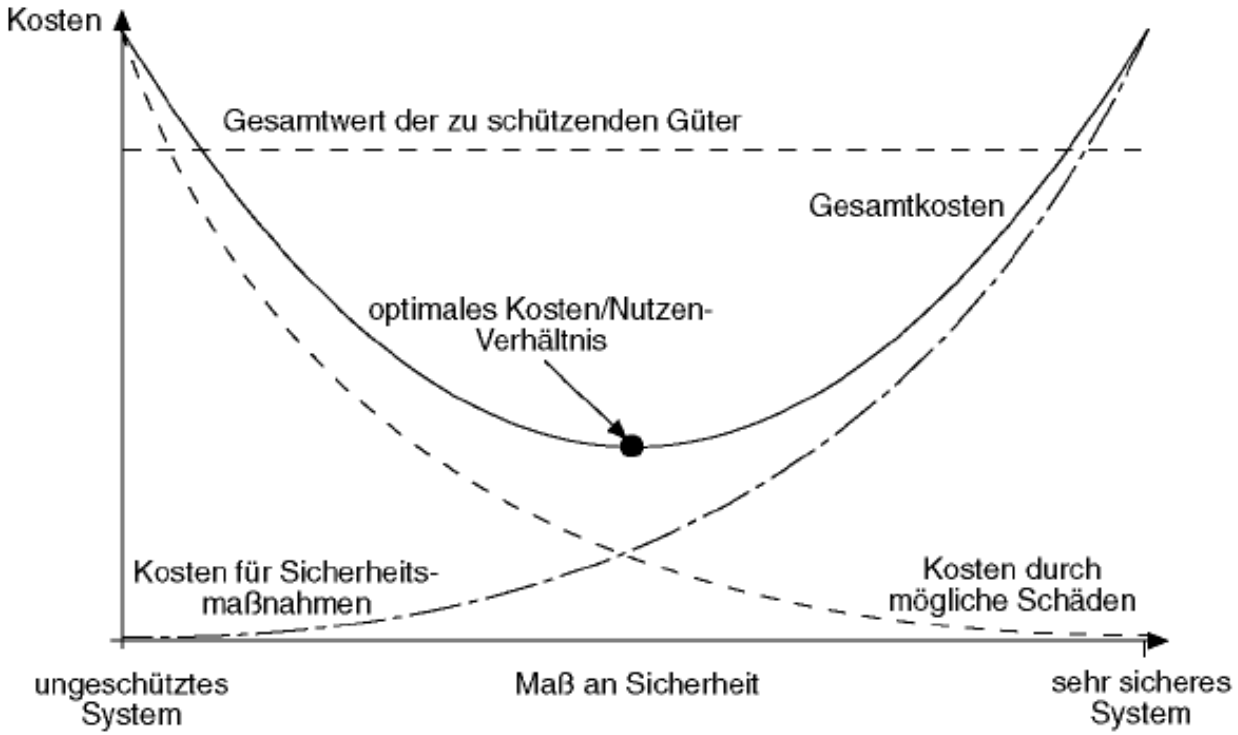
- Abhängig von mehreren Faktoren
  - Skill Level/Know-How
    (Script Kiddies, „*Hacker*“, White/Black Hat, Cracker,
    Mitarbeiter:innen,. . . )
  - Budget
  - Zeit
  - . . .

# Kostenfaktor IT-Sicherheit

- Oftmals nur Investitionen in Sicherheit für das Management sichtbar
- Ergebnisse dieser Investitionen bei guter Arbeit jedoch oft unsichtbar („*es passiert ja eh nix*“)

- ROI – Return of Investment
- Aufwand/Nutzen schwierig zu messen
- Erinnerung: Definition von Risiko
- Erfahrungswerte für
  - Kosten bei erfolgreichen Angriffen
  - Auftrittswahrscheinlichkeit von Angriffen
- SLAs (Service Level Agreements)
- Gesetze

# Kosten-/Nutzenanalyse




(Vergleiche M. Raepple: Sicherheitskonzepte für das Internet)

# Lösungen/Lösungsansätze

- Security und Architektur, Designprinzipien
  - Security von Beginn an berücksichtigen, bereits beim Design
  - Genau definierte Aufgaben und Schnittstellen
  - Verwendung von Standards
  - Sicherstellung von Support bei 3rd-Party-Produkten/Libraries
  - Testen auf Sicherheit
  - Security-Best-Practices berücksichtigen
- Lösungsansätze
  - Technische Lösungen
  - Organisatorische Lösungen
- *Mehr in den nächsten Vorlesungen/Übungen... :)*

# Auswahl der richtigen Sicherheitsmaßnahmen

(Vergleiche `https://www.gocomics.com/calvinandhobbes/1986/01/13`)

# Literaturempfehlungen, Links 1/4


- Ed Skoudis und Tom Liston. *Counter Hack Reloaded. A Step-by-Step Guide to Computer Attacks and Effective Defenses*. Pearson Education, Inc., 2. Auflage, 2006. ISBN 0-13-148104-5
- Jerome H. Saltzer und Michael D. Schroeder. The protection of information in computer systems. In *Proceedings of the IEEE*, Band 63, Seiten 1278–1308, 1975
- Bundesamt für Sicherheit in der Informationstechnik. IT-Grundschutz-Standards, 2020. `https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html`
- Matt Bishop. *Introduction to Computer Security*. Pearson Education, Inc, 2003. ISBN 0-321-24744-2

# Literaturempfehlungen, Links 2/4


- Thomas Walshe und Andrew Simpson. An Empirical Study of Bug Bounty Programs. In *2020 IEEE 2nd International Workshop on Intelligent Bug Fixing (IBF)*, Seiten 35–44, Februar 2020. doi: 10.1109/IBF50092.2020.9034828
- Bundesamt für Sicherheit in der Informationstechnik. Die Lage der IT-Sicherheit in Deutschland 2019, 2019. `https://www.bsi.bund.de/Lageberichte`
- BSI. Grundschutz, 2013. `https://www.bsi.bund.de/grundschutz.html`

# Literaturempfehlungen, Links 3/4

- Bundesamt für Sicherheit in der Informationstechnik. Leitfaden zur Basis-Absicherung nach IT-Grundschutz, 2017. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-2-IT-Grundschutz-Methodik/Leitfaden-Basis-Absicherung/leitfaden-basis-absicherung_node.html
- Common Weakness Enumeration (CWE): https://cwe.mitre.org/data/index.html
- The Jargon File: http://catb.org/jargon/

# Literaturempfehlungen, Links 4/4


- Full Disclosure. Full Disclosure Mailing List. https://nmap.org/mailman/listinfo/fulldisclosure
- Information is Beautiful Ransomware Attacks: https://informationisbeautiful.net/visualizations/ransomware-attacks/
- Bundesministerium für Inneres, Bundeskriminalamt. Cybercrime Report 2022. Technischer Bericht, 2023. https://bundeskriminalamt.at/306/files/Cybecrime_2022_V20230517_webBF.pdf

# Zusammenfassung

- Sicherheitsprobleme treten auf!
- Das Wissen um Motivation und Bedrohungspotenzial von Angreifer:innen hilft bei der Absicherung
- Bedrohungen und Angriffe in der IT ähnlich Bedrohungen und Angriffen abseits der IT
- Angriffe werden in Phasen unterteilt
- Es gibt viele unterschiedliche Herausforderungen in der IT-Security
- Security ist vielschichtig, Technische/Organisatorische Lösungen
- Sicherheitsziele, Schutzbedarf
- Kosten/Nutzen, Risiko

# Vielen Dank!

https://establishing-security.at/