HOCHSCHULE SCHMALKALDEN
UNIVERSITY OF APPLIED SCIENCES

Datensicherheit

Herausforderungen der IT-Technologien und des zunehmenden "cyber crime“ aus interdisziplinärer Sicht

Prof. Dr. iur. Wojciech Lisiewicz

Wintersemester 2024 / 2025

im Netz: http://wdb.fh-sm.de/DatenSicherheitVorlesung

Einige Fragen zum Einstieg

Überlegen Sie:

- Welche Erfahrungen haben Sie bisher mit EDV gemacht? Computer? Tablet? Mobiltelefon? Braucht man diese Geräte im **beruflichen** Alltag?
- Ist die Sicherheit von Daten wichtig? Für Sie? Für andere?
- Wann sind die Daten in einem Unternehmen (einer sonstigen Organisation / Institution) sicher?
- Sind die Daten auf den von Ihnen benutzten Geräten sicher? Was sorgt für die Sicherheit dieser Daten?

Warum sollten wir über Datensicherheit sprechen?

Rekordschäden: Cyberkriminalität kostet deutsche Wirtschaft 100 Milliarden im Jahr

kaprikfoto - Fotolia.com

https://www.e-recht24.de/news/strafrecht/11729-cybercrime-schaden-deutsche-wirtschaft.html

HOCHSCHULE SCHMALKALDEN
UNIVERSITY OF APPLIED SCIENCES

Warum sollten wir über Datensicherheit sprechen?

(kleines Update 2021)

Rekordschäden: Cyberangriffe kosten deutsche Wirtschaft pro Jahr über 200 Milliarden Euro

karelnoppe - Fotolia.com

Anke Evers

Veröffentlicht: 10. August 2021

teilen 9 | mitteilen | tweet | teilen

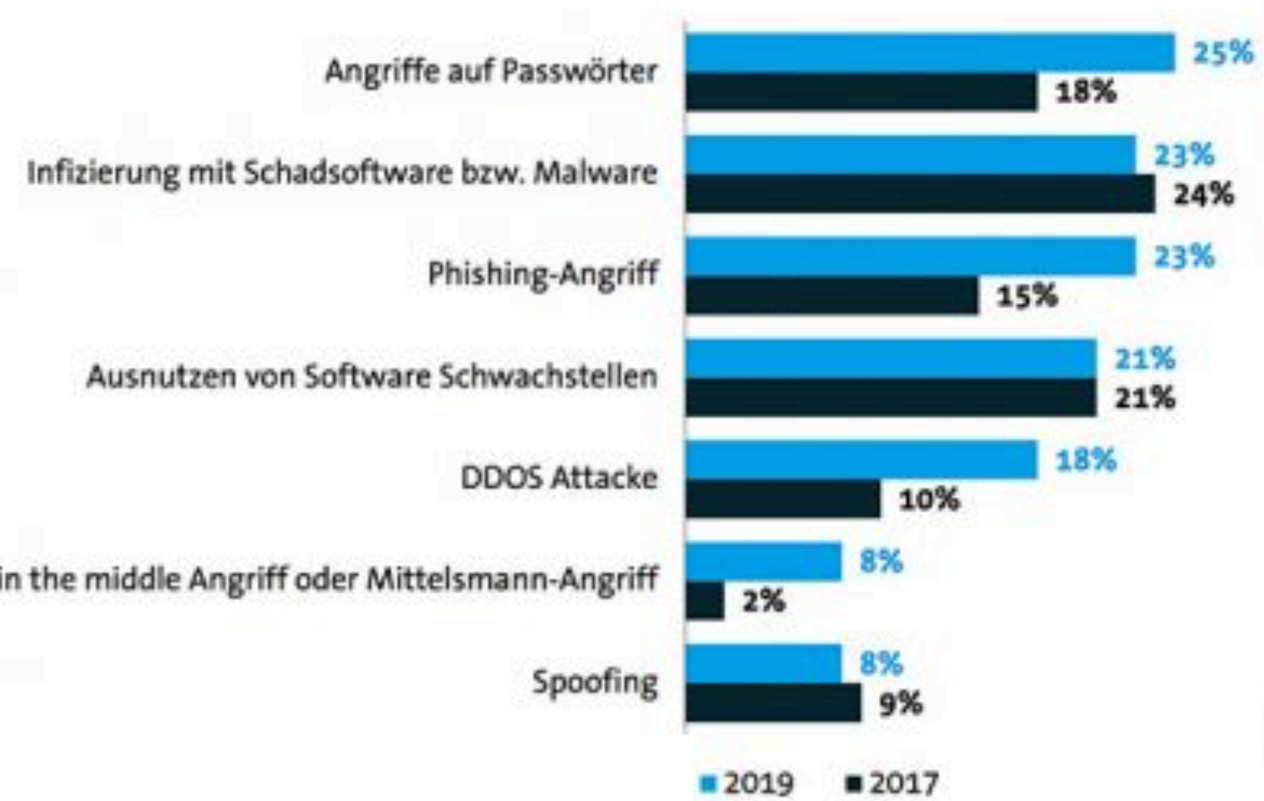
(1 Bewertung, 5,00 von 5)

https://www.e-recht24.de/news/datenschutz/12804-rekordschaeden-cyberangriffe-deutsche-wirtschaftt.html

Warum sollten wir über Datensicherheit sprechen?

Digitale Angriffe haben bei 7 von 10 Unternehmen Schäden erzeugt

Welche der folgenden Arten von digitalen Angriffen haben innerhalb der letzten zwei Jahre in Ihrem Unternehmen einen Schaden verursacht?



Digitale Angriffe haben bei

70%

der Unternehmen einen Schaden verursacht – 2017 waren es erst 43%.

Basis: Alle befragten Unternehmen (2019: n=1.070; 2017: n=1.069); Mehrfachnennungen in Prozent

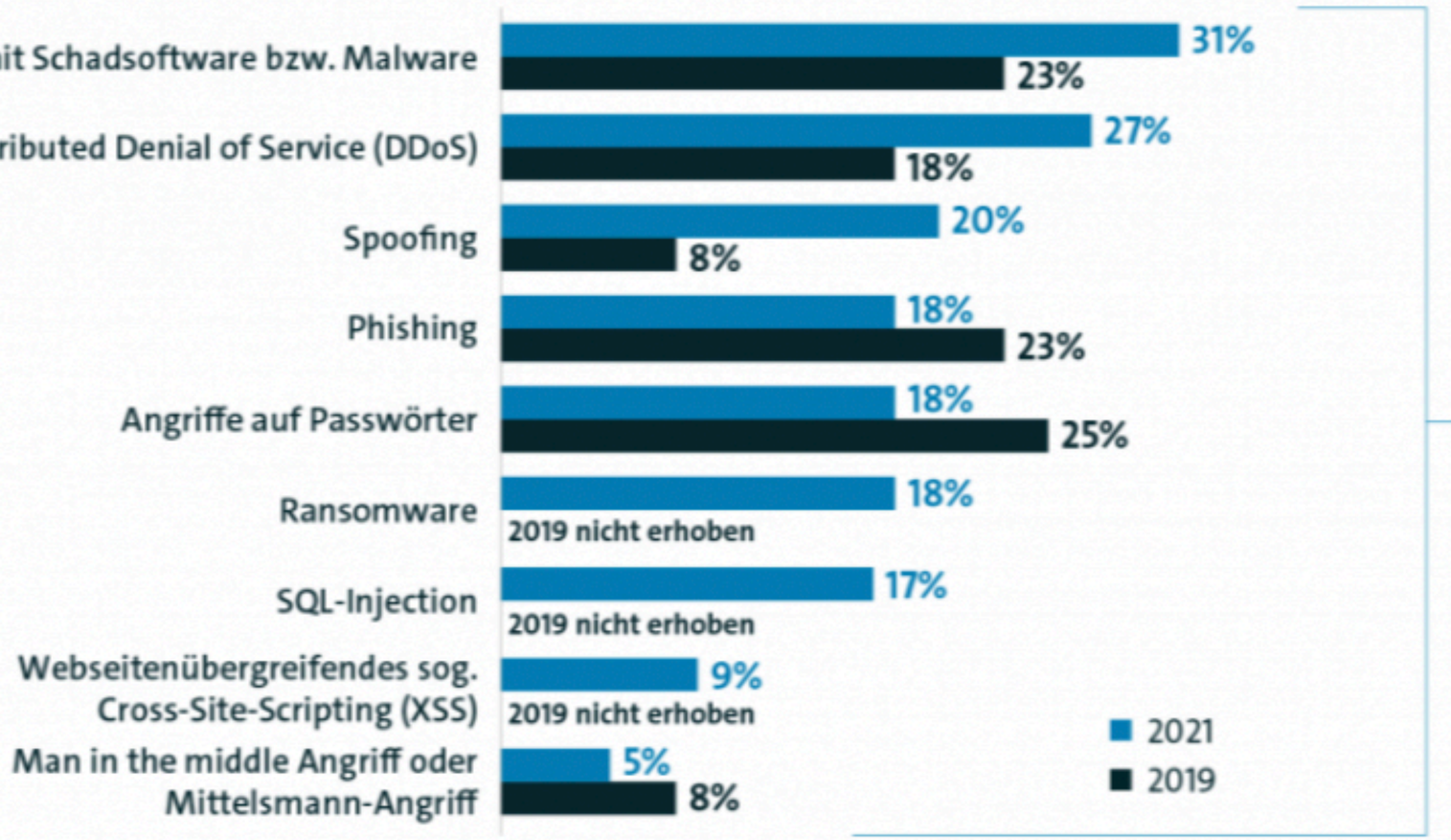
bitkom

https://www.zdnet.de/88372729/bitkom-100-milliarden-euro-schaden-pro-jahr-durch-cyberangriffe/

Warum sollten wir über Datensicherheit sprechen?

Cyberangriffe betreffen nahezu 9 von 10 Unternehmen

Welche der folgenden Arten von Cyberangriffen haben innerhalb der letzten 12 Monaten in Ihrem Unternehmen einen Schaden verursacht?



Cyberangriffe haben bei

86%

der Unternehmen einen Schaden verursacht – **2019** waren es erst **70%**.

Basis: Alle befragten Unternehmen (2021: n=1.067; 2019: n=1.070); Mehrfachnennungen in Prozent, 2017 und 2019: innerhalb der letzten zwei Jahre
Quelle: Bitkom Research 2021

bitkom

https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr

Warum sollten wir über Datensicherheit sprechen?

(kleines Update 2024)

- **8 von 10 Unternehmen von Datendiebstahl, Spionage oder Sabotage betroffen**
- **Rekordschaden von rund 267 Milliarden Euro**
- **China wird immer mehr zum Standort Nr. 1 für Angreifer**
- **Cyberangriffe: Zwei Drittel der Unternehmen fühlen sich in ihrer Existenz bedroht**

Berlin, 28. August 2024 - Deutsche Unternehmen rücken verstärkt in den Fokus von Angreifern aus dem In- und Ausland. In den vergangenen zwölf Monaten waren 81 Prozent aller Unternehmen vom Diebstahl von Daten und IT-Geräten sowie von digitaler und

https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2024

A.1. Einstieg: einige Beispiele (1)

Kammergericht Berlin, 2019/2020

- im Nachhinein als „APT 28“ bezeichnete Hackergruppe ist mit einem „emotet“-Angriff auf das Kammergericht erfolgreich
- die „Infektion“ kompromittiert die gesamte IT-Infrastruktur des Gerichts und macht die Arbeit ab Oktober 2019 unmöglich
- bis weit in das Jahr 2020 Arbeit mit Papier und Fax
- es war u. a. möglich, Daten zu verdeckten Ermittlern, Opfern von Verbrechen, Zeugen etc. abzugreifen

dabei war „emotet“ (im Gegensatz zu manchen Berichten in der Presse) nicht auf irgendetwas spezialisiert; es war nur ein Werkzeug, Datenklau oder ihre Verschlüsselung (und dann Erpressung) erst zu ermöglichen…

A.1. Einstieg: einige Beispiele (2)

Bundestag, 2015

- Trojaner wird auf den Rechnern im Netzwerk des BT installiert
- über weitere Angriffsstufen wurde Zugriff auf mehrere Arbeitsgeräte erlangt und auch auf administrative Funktionen im Netzwerk
- die Geräte waren praktisch durch Angreifer komplett fernsteuerbar - es war Zugriff sowohl auf alle Daten, wie auch auf Funktionen des kompletten Netzwerks möglich
- insgesamt flossen ca. 16 GB an Daten ab

beim Angriff spielte auch eine Fake-Seite der UN eine Rolle, auf die eine (ebenfalls „fake“) E-Mail leitete, die alle Mitarbeiter erhielten

A.1. Einstieg: einige Beispiele (3)

Düsseldorfer Klinik, 2020

- ein Ransomware-Angriff verschlüsselt Daten in einer Düsseldorfer Klinik und legt Datenverarbeitung lahm
- die Behandlung von Patienten ist nicht möglich
- auch Notfälle müssen in andere Krankenhäuser umgeleitet werden
- eine schwer erkrankte Frau kann nicht vor Ort notbehandelt werden - die deutlich verlängerte Fahrt in eine entlegene Klinik führt zu ihrem Tod

mittlerweile ist die IT nicht nur eine Frage von effizientem Arbeiten, sondern Bestandteil von lebenserhaltenden Systemen !!!

A.1. Einstieg: einige Beispiele (4)

Südwestfalen IT, 2023

- ein Ransomware-Angriff verschlüsselt Daten beim Dienstleister für 72 Kommunalverwaltungen, inkl. Stadt Siegen
- monatelang können Behörden keine Aufgaben wahrnehmen (Geburtsurkunde, Fahrzeugzulassung, Führerschein - nichts mehr möglich)
- erst im Sommer 2024 sind die Systeme wieder im Betrieb
- Zugriff auf Systeme der SIT über Lücke in Cisco-VPN

die besondere Reichweite des Daten-GAU-s in diesem Falle wirft die Frage auf, wer bezahlt dies nun? diese bleibt vorerst unbeantwortet! dabei lag hier klares Versagen des zuständigen IT-Dienstleisters vor!

A.2. Was und warum wird hier behandelt?

unsere Ziele

Überblick über die IT	▸ die sicherheitsrelevanten Aspekte der IT verstehen ▸ sinnvolle und problematische Lösungen unterscheiden können
IT-Fachmann verstehen	▸ blendet er gerade oder ist es plausibel? ▸ sind es seine Lieblings-Spielsachen oder gut konzipierte Lösung?
Weichenstellungen setzen	▸ welche Hard- und Software kann die Sicherheit jahrelang prägen? ▸ wie arbeite ich sicherheitstechnisch nachhaltig?
insbesondere: Bewusstsein schaffen	▸ was sind die Risiken und Gefahren? ▸ was sind die notwendigen Maßnahmen?

auch wenn Sie hier keine Hacker und Programmierer werden können - sie sollten vor dem Problem nicht kapitulieren!

A.3. Prüfung - Inhalt und Form

Die Prüfung des Gesamtmoduls besteht aus zwei Teilen:
- Datenschutz = Teil 1
- Datensicherheit = Teil 2

Prüfungsform in Teil 2

- Klausur
- Ein Szenario mit Darstellung der IT-Architektur in einem Unternehmen / einer Organisation steht im Zentrum.
- Zum Szenario sind Fragen zu Problemen / möglichen Maßnahmen zu beantworten.

Themen im Einzelnen

- Was sind die (im Szenario geschilderten) Probleme / Risiken / Gefahren?
- Wie kann diesen Problemen begegnet werden (Werkzeuge, Techniken, Maßnahmen)?

HOCHSCHULE SCHMALKALDEN
UNIVERSITY OF APPLIED SCIENCES

Lernmaterial

Skripte

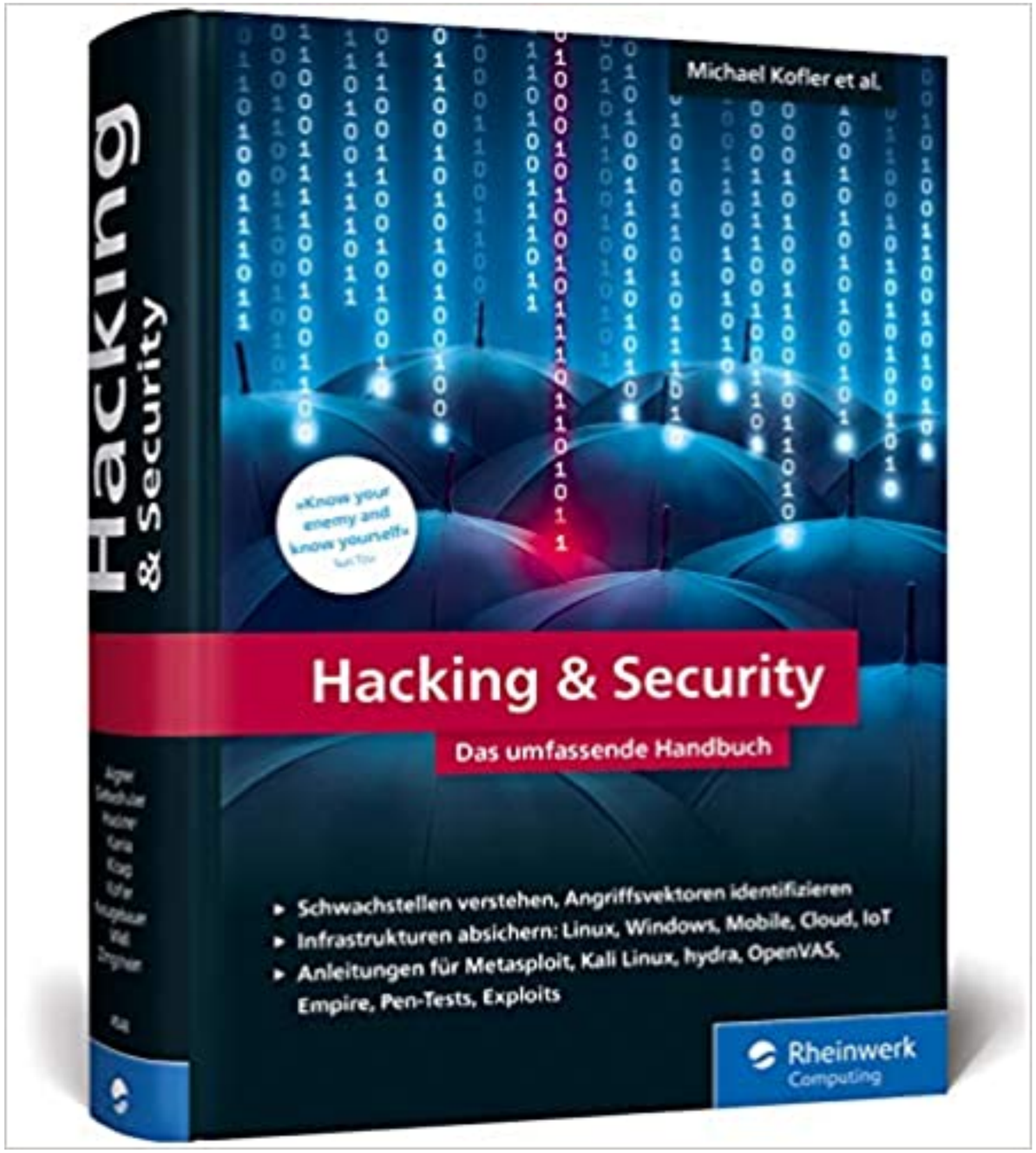
- http://wdb.fh-sm.de/DatenSicherheitVorlesung

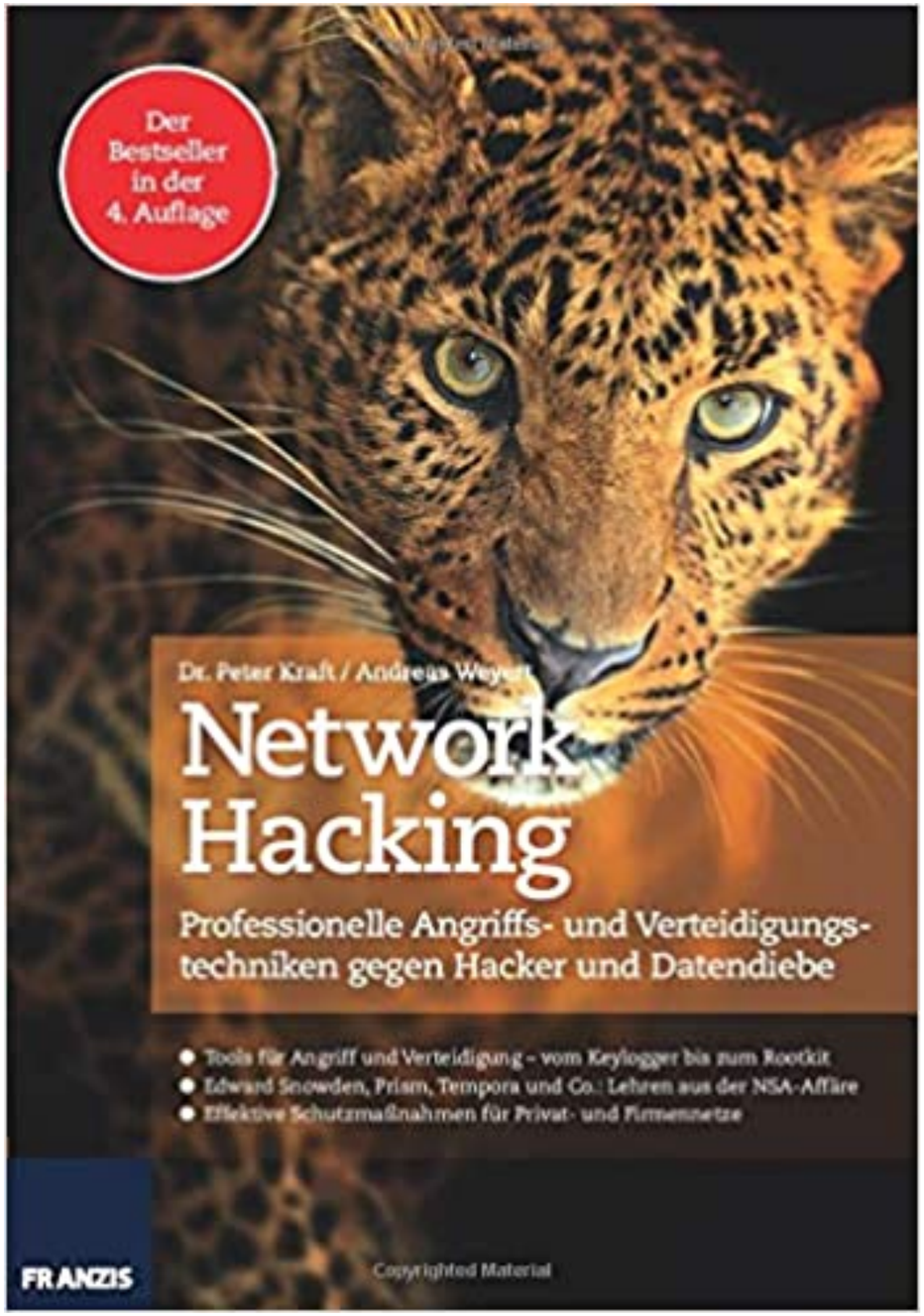
Bücher

- **Eckert, IT-Sicherheit, DeGruyter (eBook)**
- Kersten / Klett, Der IT Security Manager (eBook)
- Hellmann, IT-Sicherheit, DeGruyter
- Kipker, Cybersecurity - Rechtshandbuch, C. H. Beck

wegen Nachfragen:

Literaturempfehlungen für Neugierige





B. Bestandsaufnahme

Wo stehen wir?

- immer größere Abhängigkeit von der EDV
- eingesetzte Technik immer komplexer, auch wegen der „Featuritis“
- *die Technologie soll immer benutzerfreundlicher werden und ist es angeblich auch (?)*
- hoher Zeit- und Kostendruck => „agil statt stabil“
- immer stärkere Vernetzung von Systemen
- Datenlecks, GAUs, Angriffe, gravierende Ausfälle und sonstige „Desaster“ nehmen stark zu
- Fachkräftemangel, Cyberkriminelle immer besser, hybride Kriegsführung

Datensicherheit
Prof. W. Lisiewicz
E-Mail: w.lisiewicz@hs-sm.de

B. Bestandsaufnahme - was ist das eigentliche Problem?

Frankfurter Allgemeine
Wirtschaft

ERP-SOFTWARE

„Das ist schlimmer als Brexit, Trump und Handelskrieg“

VON SUSANNE PREUSS, STUTTGART - AKTUALISIERT AM 10.07.2019 - 17:51

B. Bestandsaufnahme

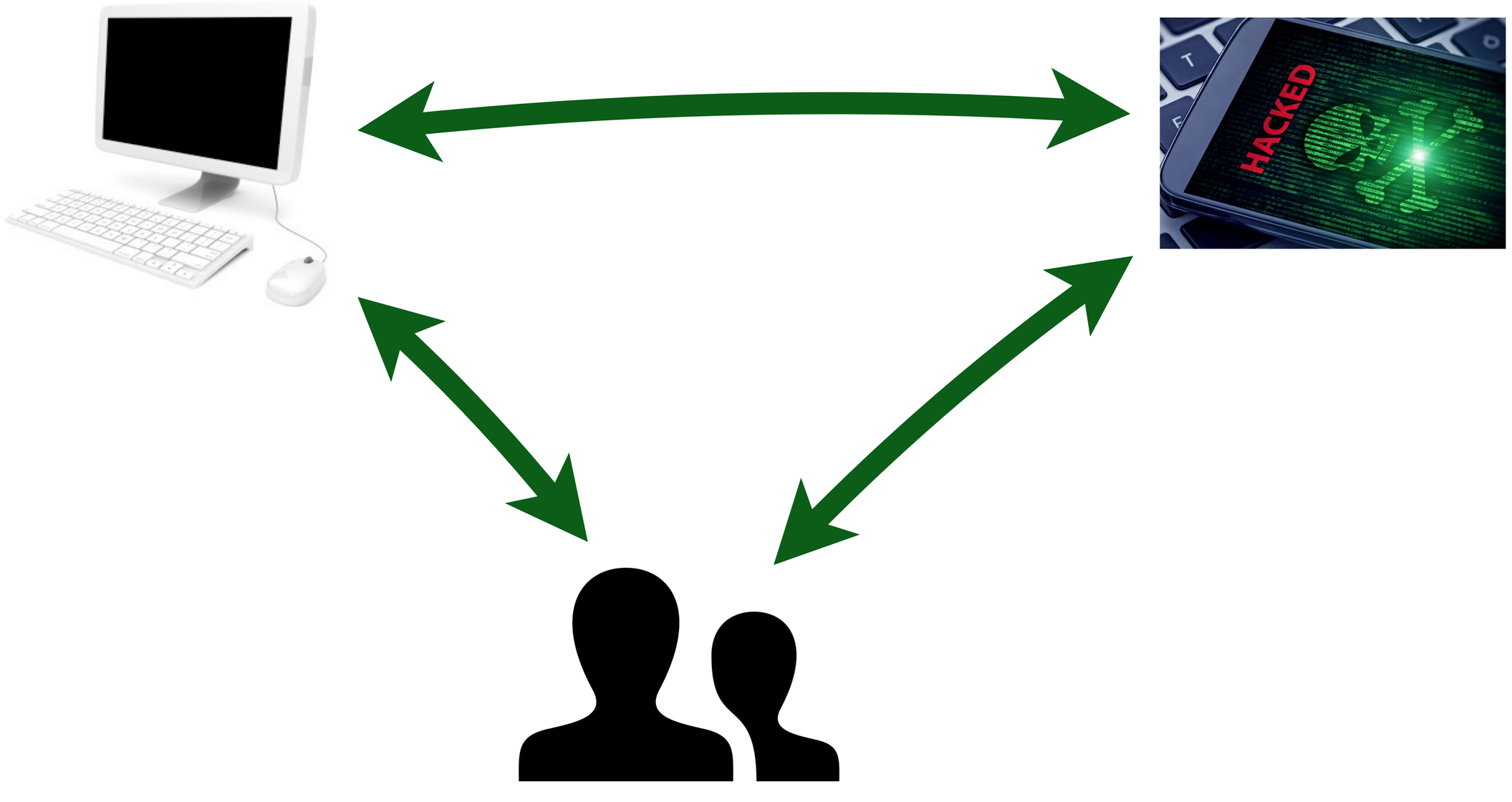
Fragen zum Nachdenken:

- warum hat moderne Software immer mehr Funktionen?
- warum wird der Eindruck erweckt, alles ist immer leichter?
- warum herrscht der Eindruck von Unsicherheit?
- warum erscheint es den Betroffenen, ihre Probleme werden nicht gelöst, gar ignoriert und dennoch ständig neue Produkte auf den Markt geworfen?

meine persönliche Beobachtung: Geschäftsmodell geht vor Kundenbedarf, Lizenz- oder Abo-Gebühr vor Problemlösung…

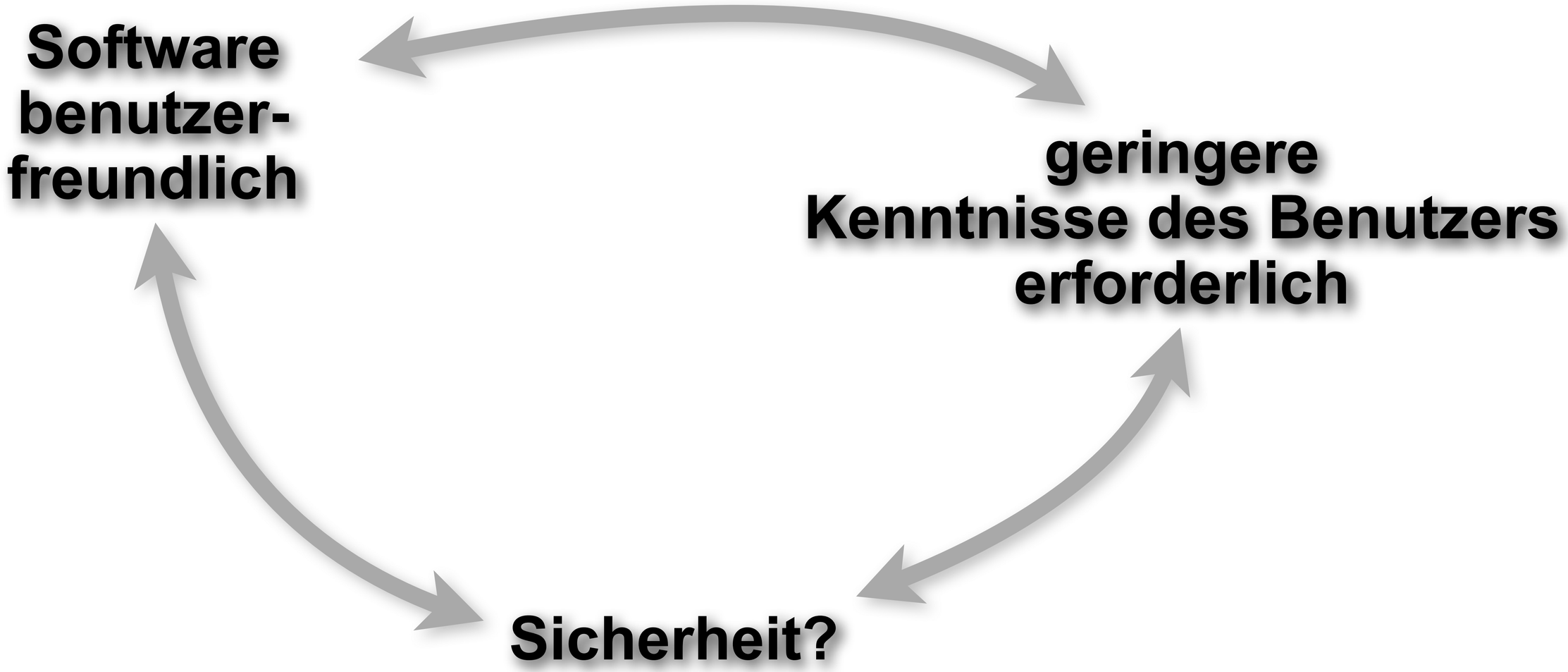
C.1. Mensch als Sicherheitsfaktor

IKT vs. Datensicherheit vs. Mensch



C.2. Spezielles Problem: Benutzerfreundlichkeit

Benutzerfreundlichkeit vs. Datensicherheit



C.2. Spezielles Problem: Benutzerfreundlichkeit

Folgen

Software benutzer-freundlich

geringere Kenntnisse des Benutzers erforderlich (?)

Sicherheit leidet!!!

C.2. Komplexität vs. Benutzerfreundlichkeit

ein sich (selbst) verstärkender Trend