



Technische Hochschule
Ingolstadt
Fakultät Informatik

Vorlesung „Security Engineering in der IT“

Prof. Dr.-Ing. Hans-Joachim Hof

20.03.23



Technische Hochschule
Ingolstadt
Fakultät Informatik

Kapitel 1: Motivation und Ziele der Cybersicherheit

Prof. Dr.-Ing. Hans-Joachim Hof

20.03.23

Ziele dieser Veranstaltung



- **Studierende wissen, warum es Sinn macht, sich mit Security Engineering zu beschäftigen**
- **Studierende wissen, welcher Umfang Security Engineering hat**

- **Stellen Sie sich ein Studium ohne IT an der Hochschule vor – was wäre anders?**



Aktuelle Sicherheitsvorfälle

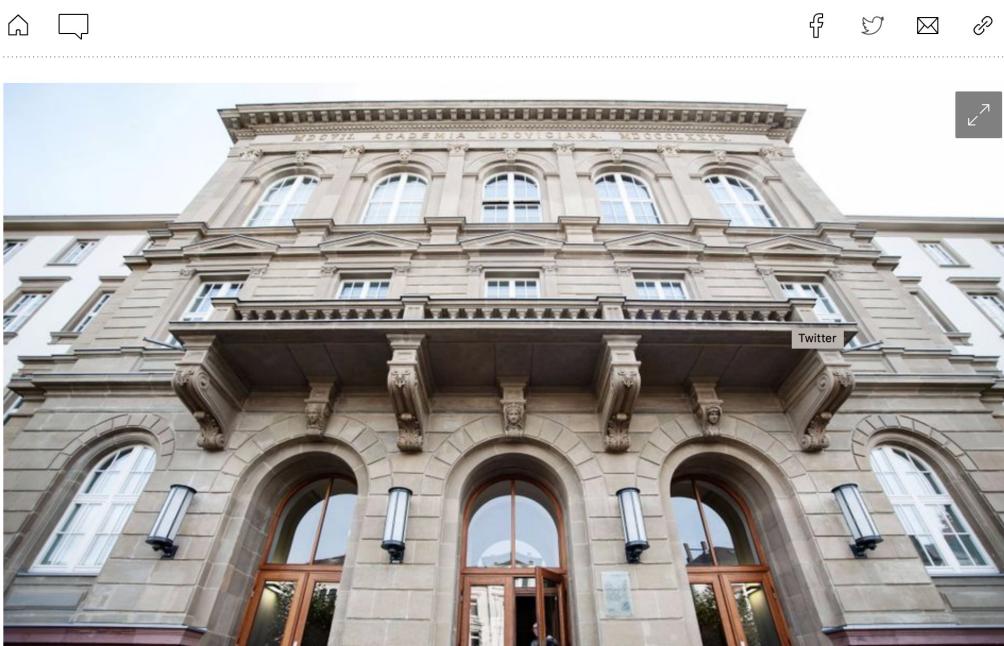
Uni Gießen gehackt (2020), Bergische Universität Wuppertal gehackt (2022)

Nach Cyberangriff

Wie die Uni Gießen auch offline funktioniert

Nach einem Hackerangriff schaltete die Justus-Liebig-Universität alle Systeme ab - wochenlang lief alles ohne Computer. Für die Studierenden hatte das auch Vorteile.

Ein Interview von **Silke Fokken**
10.01.2020, 12:33 Uhr

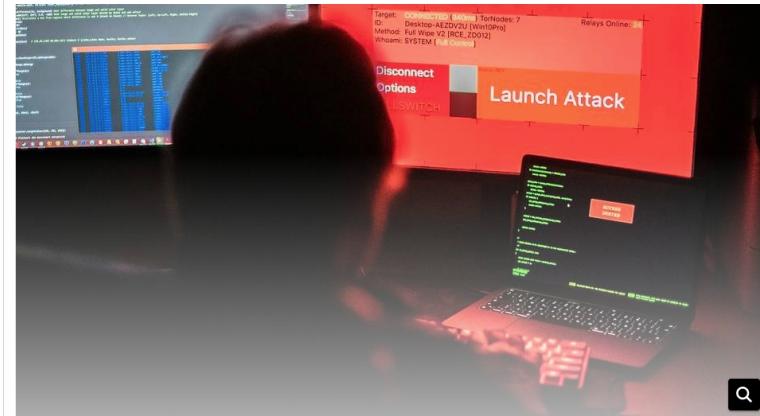


5 Weil Unbekannte die Uni Gießen mit einer Schadsoftware attackierten, nahm die Hochschule alle Systeme vom Netz. Schepp/ imago images

wz+ ZWISCHENFALL

Cyberattacke auf Uni Wuppertal: „Wir werden gerade sehr stark eingeschränkt beim Lernen“

28. Juli 2022 um 09:07 Uhr | Lesedauer: 2 Minuten



Liebe Beschäftigte, liebe Studierende,

die Bergische Universität ist von einem Hackerangriff betroffen und arbeitet derzeit mit Hochdruck an Lösungen.

Betroffen sind erhebliche Teile unserer IT-Infrastruktur, sodass eine Vielzahl von Systemen aktuell nicht oder nur eingeschränkt zur Verfügung steht. Dies betrifft leider auch unsere Kommunikationskanäle.

1g Cloud Applications und Security Engineering

Aktuelle Sicherheitsvorfälle

Gleiche Masche – versehentlich anderes Ziel – erstes Todesopfer durch IT-Angriff?

Uniklinik Düsseldorf
IT-Ausfall war erpresserischer Hacker-Angriff

17.09.2020 21:19 Uhr

Den IT-Ausfall an der Düsseldorfer Uni-Klinik haben Erpresser ausgelöst. Auch der Tod einer Frau, die infolge des Hackerangriffs zu spät behandelt wurde, beschäftigt die Ermittler.



Wie gefährlich Hackerangriffe werden können, zeigt sich in Düsseldorf. Dort legten Erpresser das Computersystem der Uni-Klinik lahm – wohlmöglich mit tödlichen Folgen.

1 min | 17.09.2020

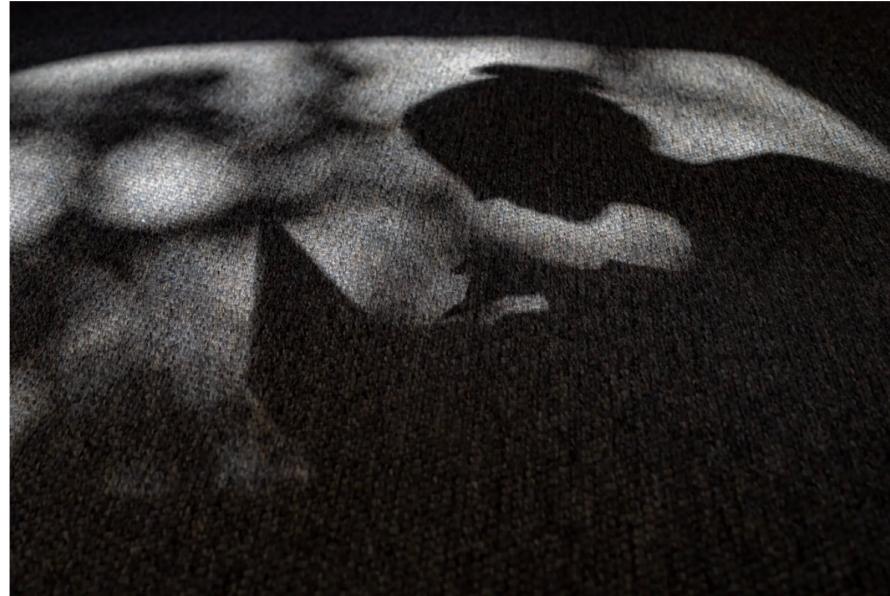
- Zwischen 11/2013 und 12/2016 64 Angriffe und Gegenangriffe auf die Ukraine [11], vermutlich weitreichende Einsatztests von Cyberwaffen
- Beispiele:
 - 05/2014: Geplante Desinformationskampagne, Webseite der Wahlkommission der Ukraine gehackt
 - 12/2015: Hacker legen Stromversorgung für 230.000 Menschen in der Region Iwano-Frankiwsk lahm
 - 12/2016: Hacker legen Stromversorgung im Norden von Kiew lahm
- Weiterer gravierender Angriff 06/2017: Notpetya Wurm wird in der Ukraine freigesetzt und richtet massiven Schaden an
- Seither: große Anstrengungen in der Ukraine, das Sicherheitsniveau zu erhöhen, Zusammenarbeit mit den USA
 - Ca 30 Unternehmen im Security-Bereich (vor dem Krieg)

OPINION

FARHAD MANJOO

The Ukrainian Cyberwar That Wasn't

March 11, 2022



Getty Images

Aktuelle Sicherheitsvorfälle

Vermutlich Sabotage: Bahnverkehr in Norddeutschland lahm gelegt (2022)

 tagesschau  Europa League

Startseite > Inland > Technische Störung: Bahn stellt Fernverkehr im Norden vorerst ein



Technische Störung

Bahn stellt Fernverkehr im Norden vorerst ein

Stand: 08.10.2022 09:31 Uhr

Ausgerechnet zum Start der Herbstferien im Norden werden unzählige Bahnreisende ausgebremst: Eine Störung des Zugfunks legt laut Bahn den gesamten Fernverkehr in Norddeutschland lahm. Wann der Verkehr wieder aufgenommen werden kann, ist unklar.

Eine technische Störung führt nach Angaben der Deutschen Bahn in Norddeutschland derzeit zum kompletten Stillstand im Fernverkehr. Betroffen seien alle ICE- sowie IC- und EC-Züge in Norddeutschland, teilte die Bahn mit. "Leider kommt es zu kurzfristigen Zug- und Haltausfällen", hieß es im Internetauftritt der Bahn. Die heftigen Probleme seien auf eine technische Störung des Zugfunks zurückzuführen.

Bahn-Expertin zu Anschlägen

"Derart professionelle Sabotage ist eine neue Dimension"

INTERVIEW Von Yannick von Eisenhart Rothe

Aktualisiert am 13.10.2022 - 10:38 Uhr
Lesedauer: 3 Min.

(Aussage von Professorin Birgit Milius, Professorin für Bahnbetrieb und Infrastruktur)

Lichtwellenleiter der Bahn



Bildquelle: <https://www.handelsblatt.com/politik/deutschland/one-fiber-start-up-will-glasfaserkabel-entlang-der-schienen-der-deutschen-bahn-verlegen/27184878.html>



Bildquelle: <https://www.zeit.de/mobilitaet/2020-04/glasfasernetz-deutschland-breitbandanschluesse-internet-schienennetz-deutsche-bahn>

Lichtwellenleiter der Bahn



Lichtwellenleiter der Bahn



GSM-R

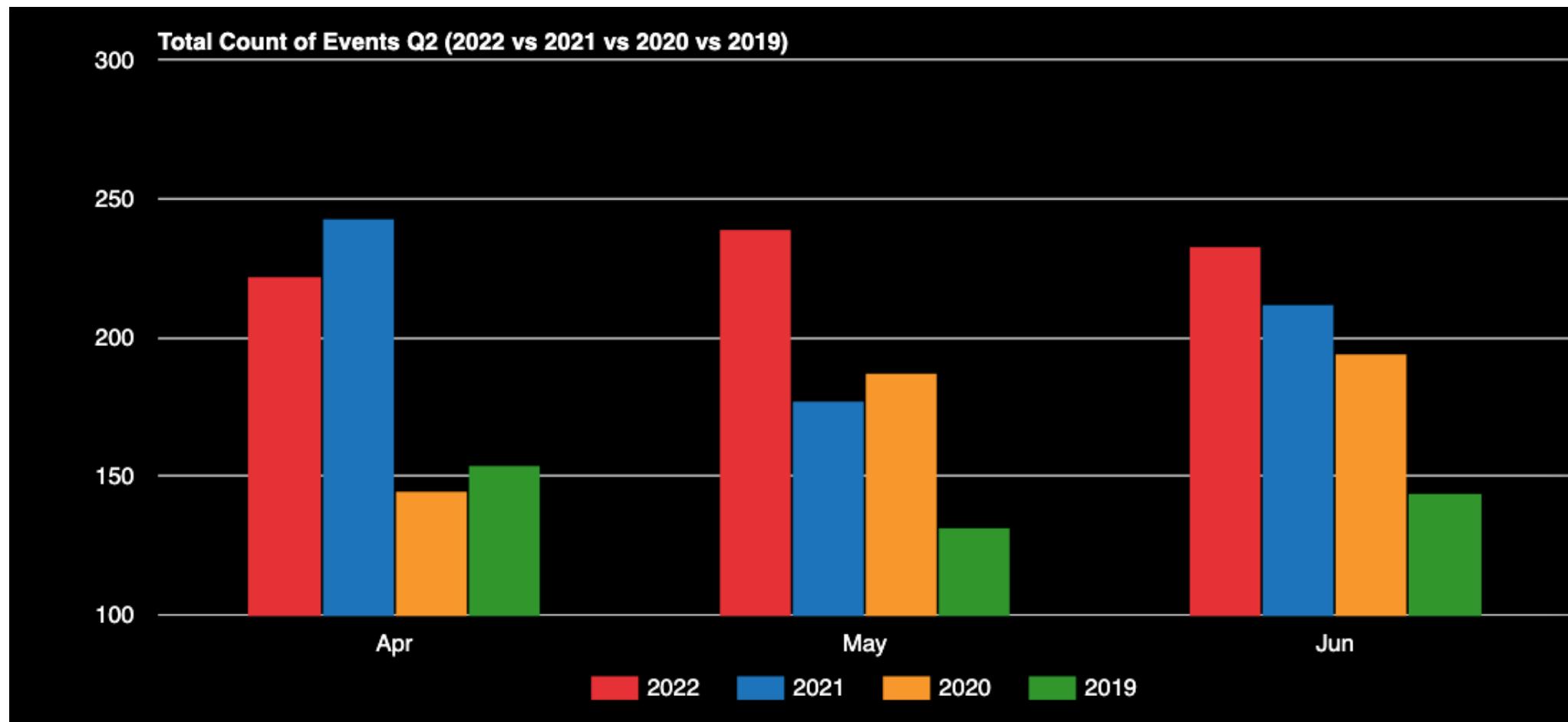


■ Diskutieren Sie bitte folgendes Szenario in Gruppen (30 Minuten):

„Sie wurden als Berater für die neue Bundesregierung bestellt. Schlagen Sie 10 Maßnahmen vor, um Deutschland vor Cyberangriffen zu schützen. Die Maßnahmen können technischer Natur sein oder organisatorischer Natur. Benennen Sie zu jeder Maßnahme Verantwortliche.“

- <https://www.hackmageddon.com/>
- **Sammlung und Auswertung öffentlich bekannt gewordener Hacking-Vorfälle durch eine Privatperson**
 - Frage: Was bedeutet das für die Aussagekraft?
 - Frage: Wie gehen Sie vor, um die Vertrauenswürdigkeit einer Quelle zu überprüfen?
- **Definition Bias: „Bias bezeichnet eine systematische Abweichung von der Wahrheit oder von dem, was objektiv betrachtet als fair oder angemessen betrachtet wird. Es handelt sich um einen Fehler oder eine Verzerrung, die in einer Studie, einer Analyse, einer Meinung oder einer Entscheidung auftreten kann.“**

Total Count of Events Q2 (2022, 2021, 2020, 2019)



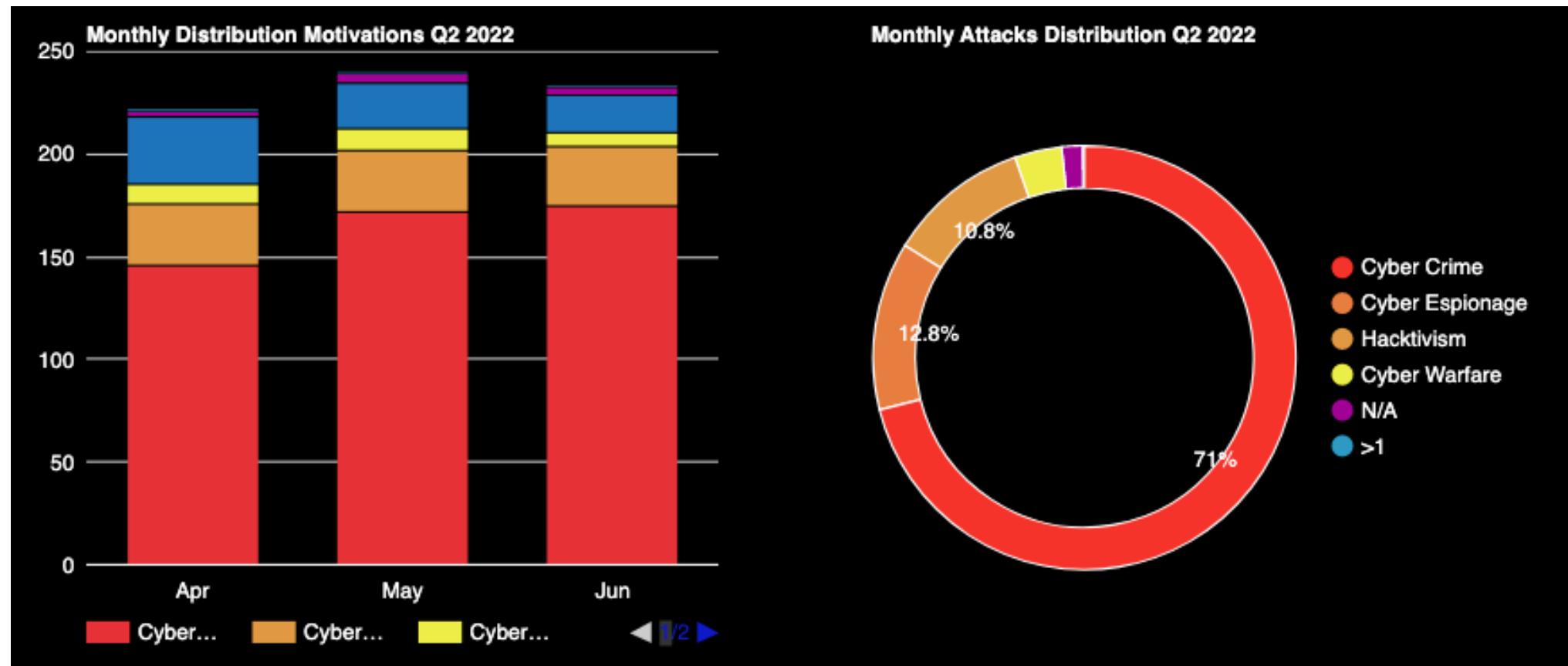
- **Cyber Crime:** „Cyber-Kriminalität (engl. cyber crime) bezeichnet alle Straftaten, die moderne Informationstechnik und elektronische Infrastrukturen (aus-) nutzen.“ (Quelle: BSI)
- **Cyber Warfare:** Cyber-Kriegsführung (engl. cyber warfare) bezeichnet grenzüberschreitende Cyber-Kriminalität, an der mindestens ein staatlicher Akteur beteiligt ist.
- **Cyber Terrorism:** Cyber-Kriminalität, die von einem Nachrichtendienst oder einer terroristischen Gruppe ausgeführt wird, um Regierungen oder staatliche Institutionen zu stören oder zu behindern, um politische oder ideologische Ziele zu erreichen
- **Cyber Espionage:** Cyber-Kriminalität mit dem Ziel, geheime oder vertrauliche Daten zu erlangen
- **Hacktivism:** Cyber-Kriminalität als Mittel des zivilen Ungehorsams um eine politische oder soziale Agenda zu bewerben.

- Finden Sie Beispiele zu den einzelnen Kategorien aus den letzten Jahren
- In welche Kategorie fällt der Angriff auf die Bahn?
- Unter welche Kategorie würde fiktive (!) Cyber-Kriminalität von „Letzte Generation“ fallen?

Statistiken zu Angriffen



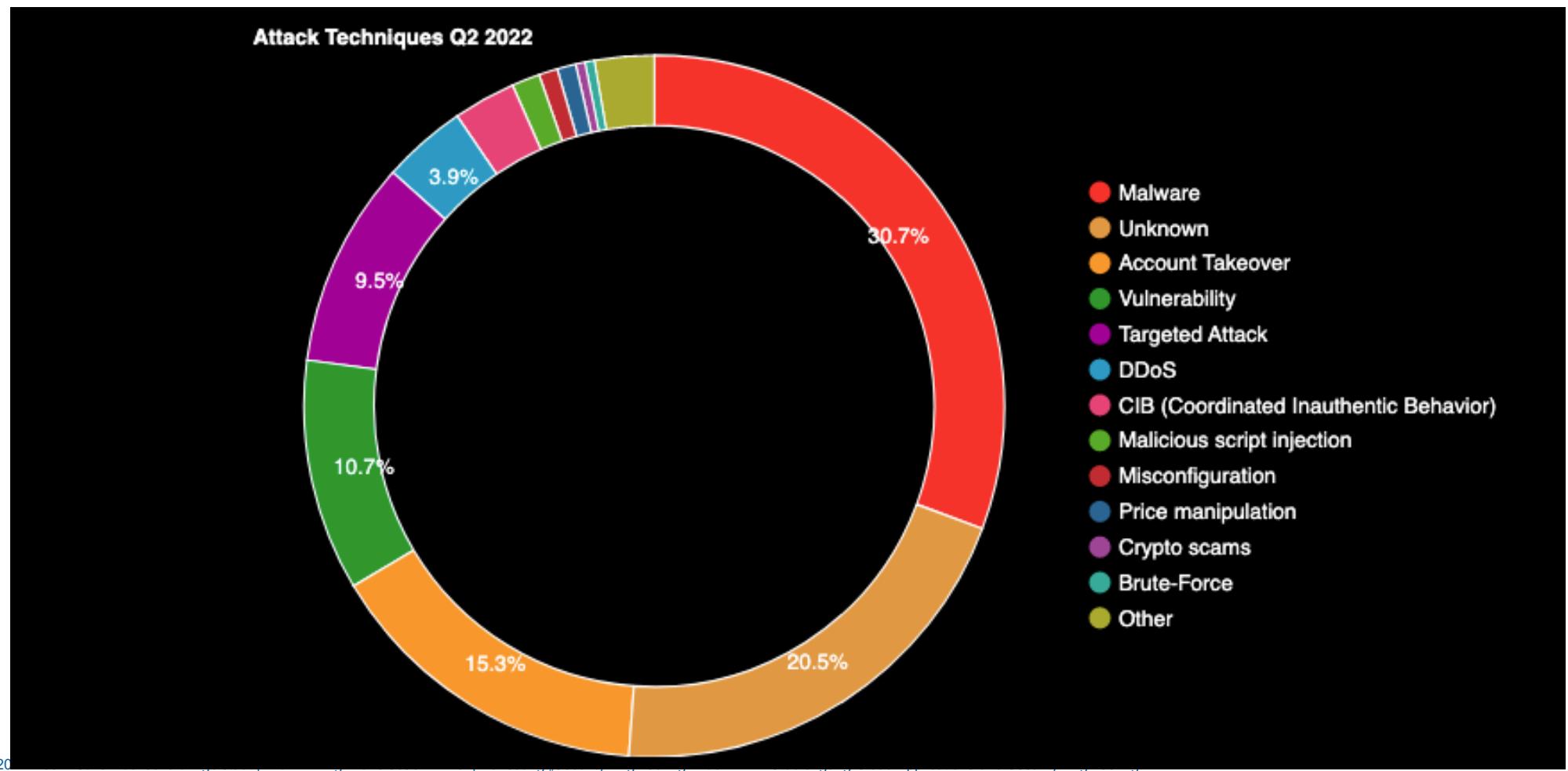
Motivation der Angriffe (Q2/2022)



- **Frage: Fällt Ihnen etwas bezüglich der Definitionen auf der vorigen Folie auf?**

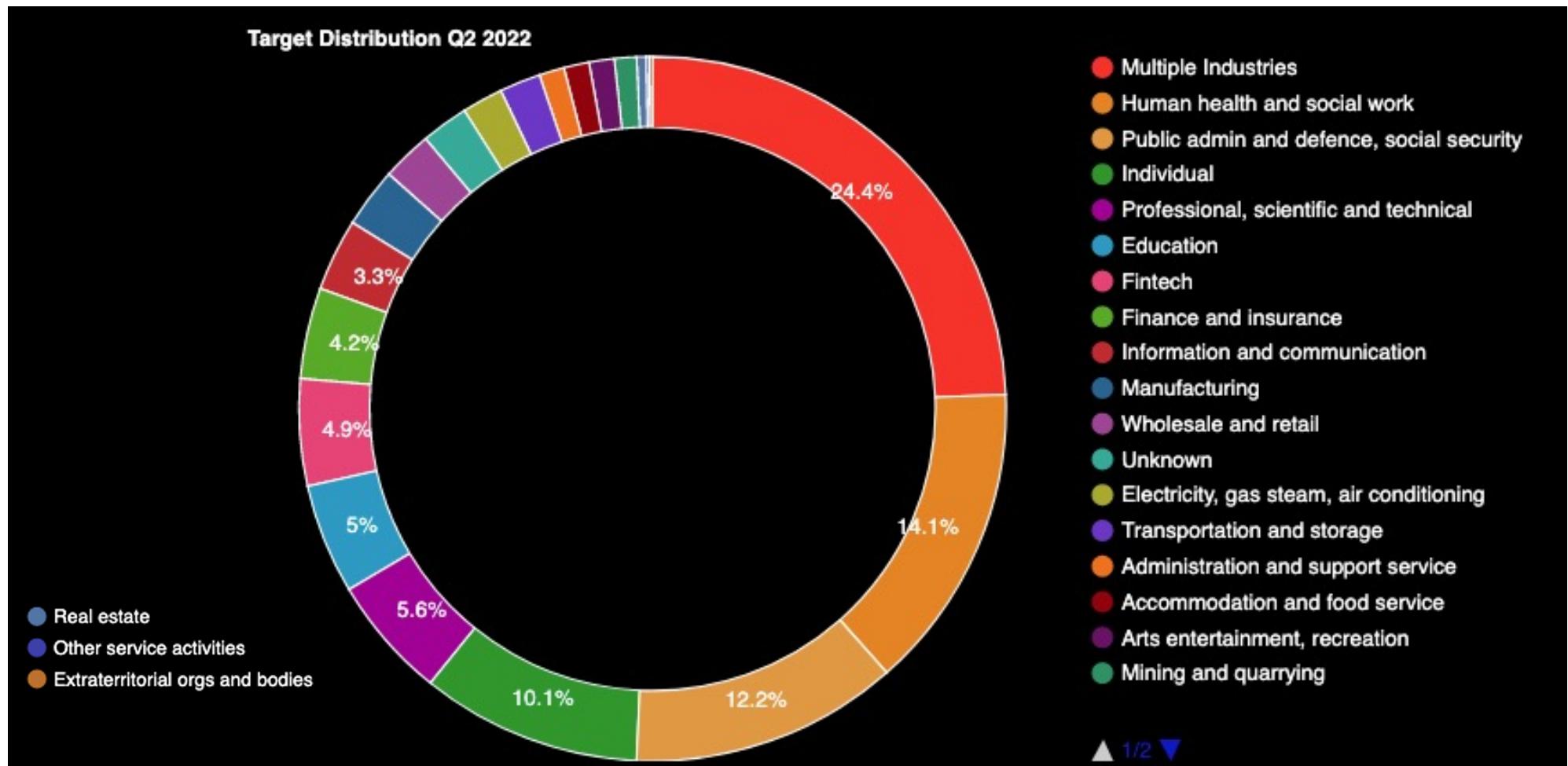
Statistiken zu Angriffen

Angriffsarten Q2/2022



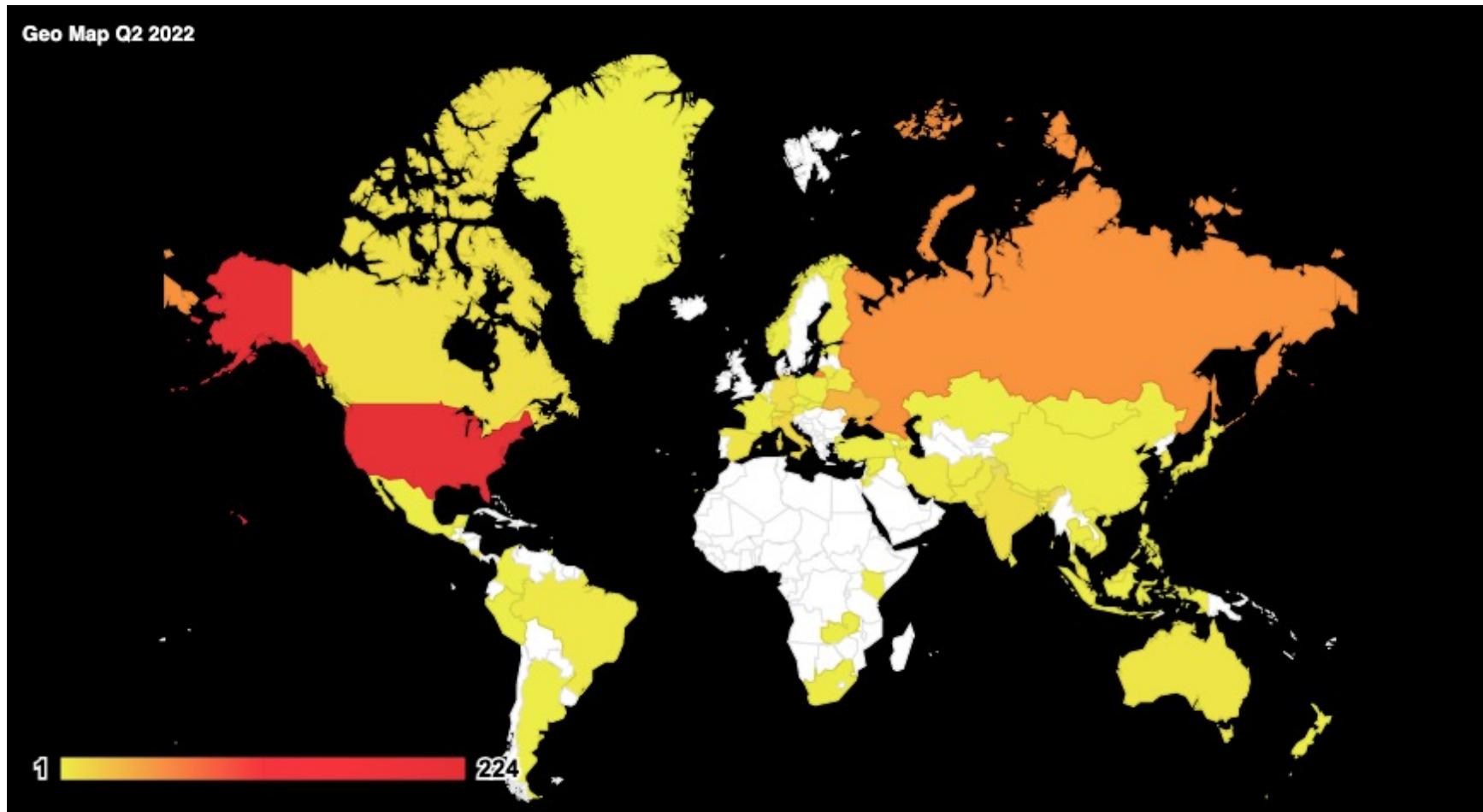
Statistiken zu Angriffen

Ziele von Angriffen (Q2/2022)



Statistiken zu Angriffen

Geomap Anzahl Angriffe Q2, 2022



Domänenspezifische Bedrohungen

Beispiel: Angriffe auf Fahrzeuge



- **Upstream, „2022 Global Automotive Cybersecurity Report“**

- **Aufgabe:**

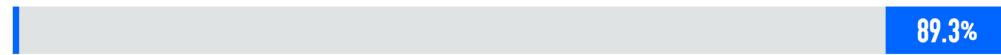
- Wie sind die Studienergebnisse entstanden?
- Welchen Bias könnte die Studie haben?
- Wie verifizieren Sie die Aussage des Reports?

2022 Global Automotive Cybersecurity Report

Verteilung Cyber Incidents 2020-2021



4.3.2 Threats to vehicles regarding their communication channels



4.3.6 Threats to vehicle data/code



4.3.7 Potential vulnerabilities that could be exploited if not sufficiently protected or hardened



4.3.5 Threats to vehicles regarding their external connectivity and connections



4.3.1 Threats regarding back-end servers related to vehicles in the field



4.3.3. Threats to vehicles regarding their update procedures



4.3.4 Threats to vehicles regarding unintended human actions facilitating a cyber attack



2022 Global Automotive Cybersecurity Report

Top Incidents in 2021



Top incidents in 2021:

JANUARY
A hacker exploited a vulnerability in a major European Tier-1 infotainment system that was deployed in an Asian OEM's vehicle. This was achieved by plugging in a USB device, then executing the exploitation to gain root shell access to the system.³⁶

FEBRUARY
An Asian OEM's American business arm experienced a ransomware attack by the DoppelPaymer gang, who demanded \$20 million in exchange for a decryptor and not leaking stolen data.³⁷

APRIL
A North American insurance agency with some 17 million vehicle policyholders, experienced a data breach that compromised drivers license ID numbers in early 2021.³⁸

MAY
Numerous vulnerabilities discovered in a European manufacturer's infotainment system, which could be exploited to take control of multiple in-cabin functions.⁴⁰

JUNE
Hackers exploited a feature in modern vehicles' ECUs, and managed for the first time to misuse it and remotely attack other ECUs. The hackers managed to attack and shutdown the powertrain ECU and power steering ECU in to vehicles.⁴²

AUGUST
A data breach hit two European OEMs, impacting more than 3.3 million customers and prospective buyers in North America.⁴¹

DECEMBER
The doors of a North American EV manufacturer's vehicle were hacked using a drone carrying a Wi-Fi dongle, exposing the vulnerabilities these vehicles have to wireless adjacent attacks.³⁹

JULY
Hacking the CAN bus of a European OEM's vehicle, a hacker was able to wirelessly transmit vehicle data to a third party device.⁴³

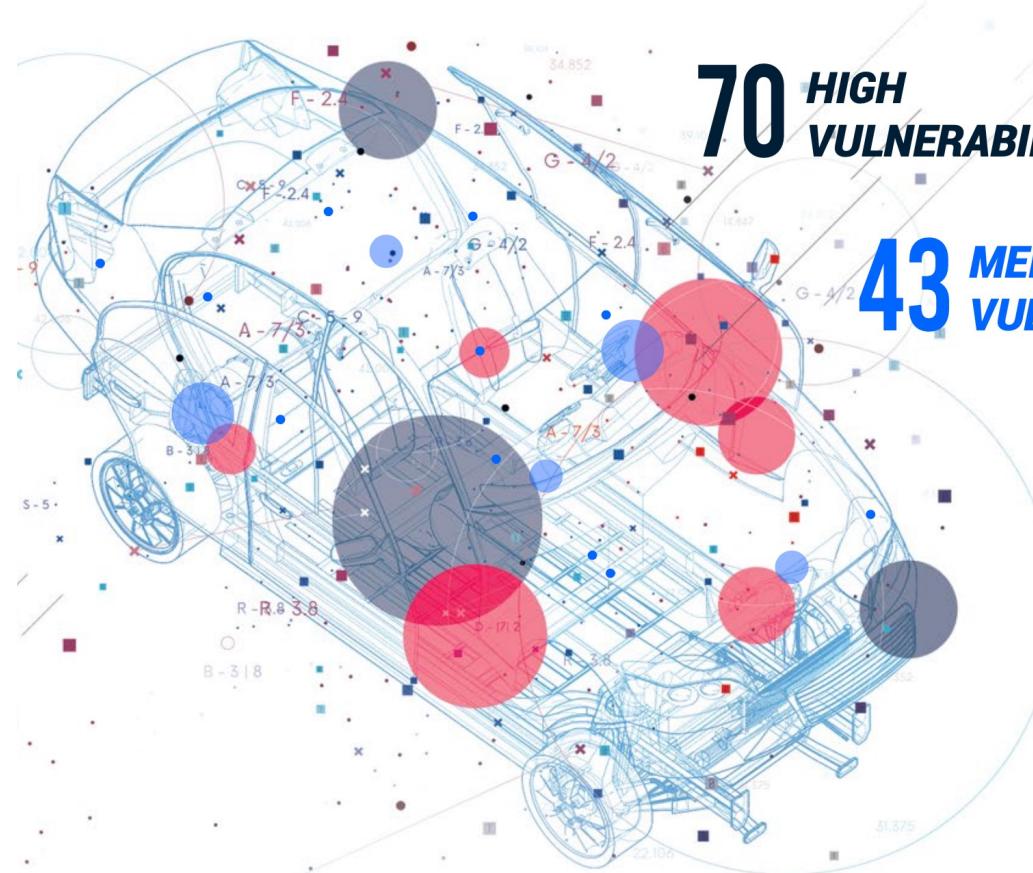
DECEMBER
Hackers exposed multiple vulnerabilities in the operating system used by major agriculture OEMs, allowing black-hat actors to remotely manipulate machinery, even taking them out of service.⁴⁵

DECEMBER
Researchers found vulnerabilities affecting devices or properties embedded in or used for connected cars, chargers, in-vehicle infotainment (IVI) systems, and digital remotes with car chargers were at risk, including vehicle-to-grid (V2G) systems in Europe.⁴⁶

26 CRITICAL VULNERABILITIES

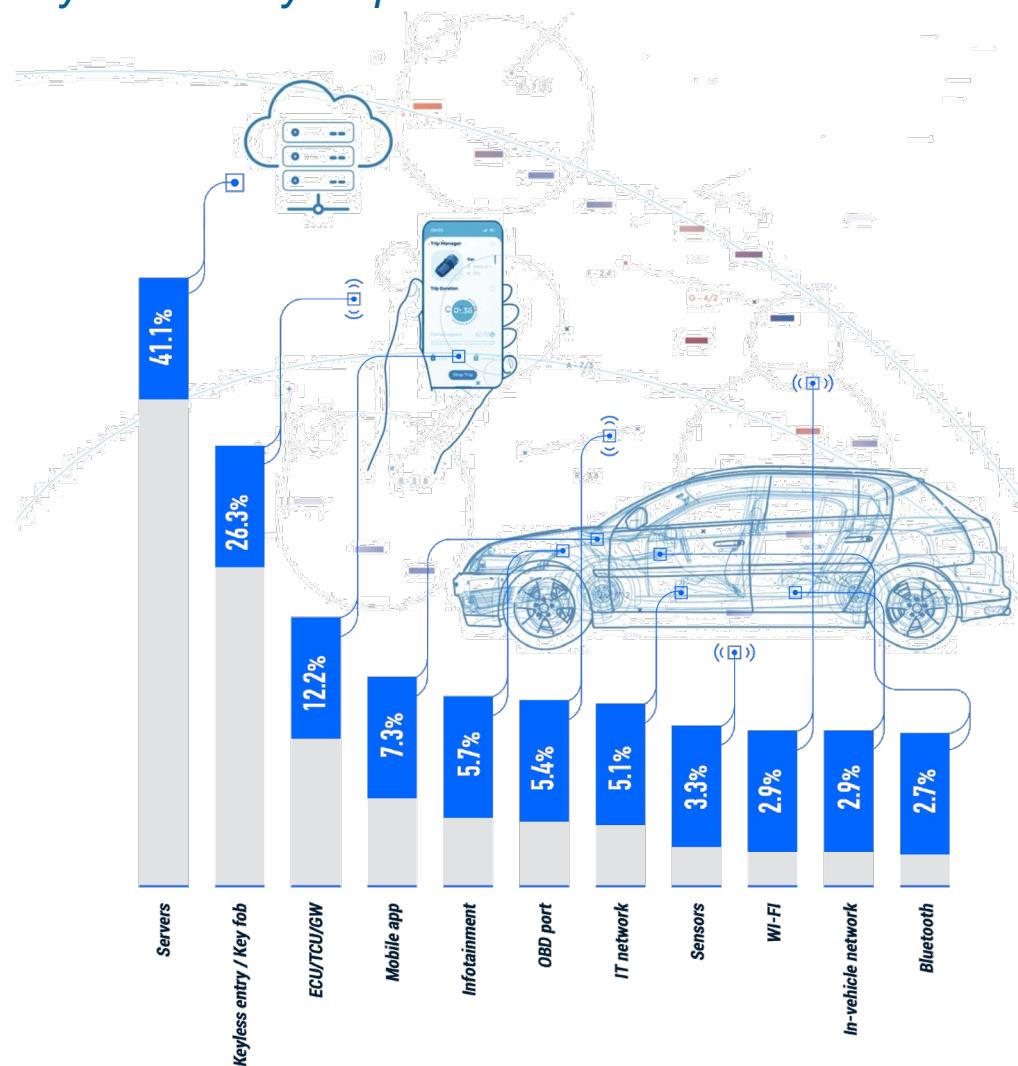
70 HIGH VULNERABILITIES

43 MEDIUM VULNERABILITIES



2022 Global Automotive Cybersecurity Report

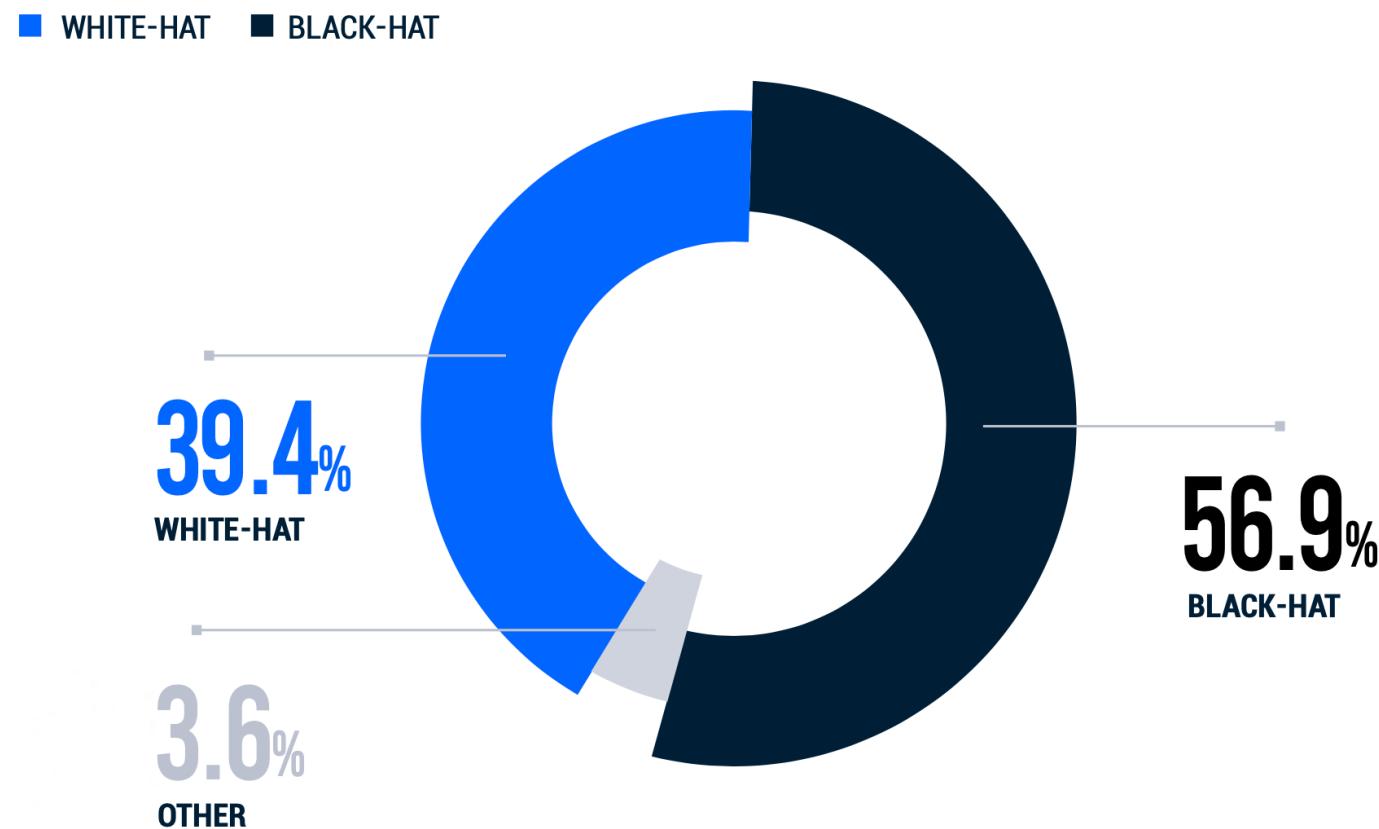
Angriffsvektoren 2010-2021



- **Definition Angriffsvektor: „Methode oder Technik, die ein Angreifer verwendet, um in ein System einzudringen oder zu kompromittieren“**

2022 Global Automotive Cybersecurity Report

Wer sind die Angreifer?





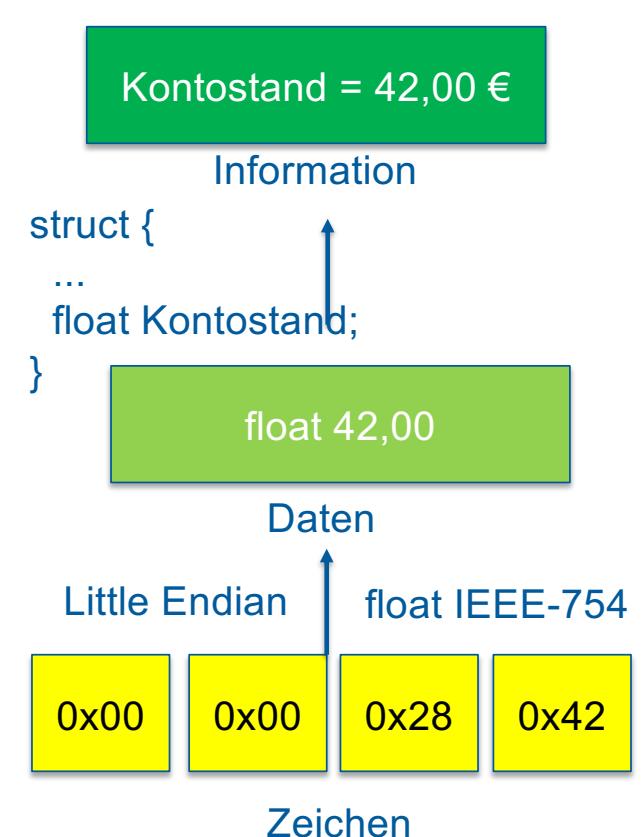
- **Definition White Hat Hacker:** „Konstruktiver Hacker, der sich bei seinen Tätigkeiten im legalen Rahmen bewegt.“
- **Definition Black Hat Hacker.** „Hacker mit destruktiven Zielen, meist mit krimineller Motivation“



- **Definition White Hat Hacker:** „Konstruktiver Hacker, der sich bei seinen Tätigkeiten im legalen Rahmen bewegt.“
- **Definition Black Hat Hacker.** „Hacker mit destruktiven Zielen, meist mit krimineller Motivation“

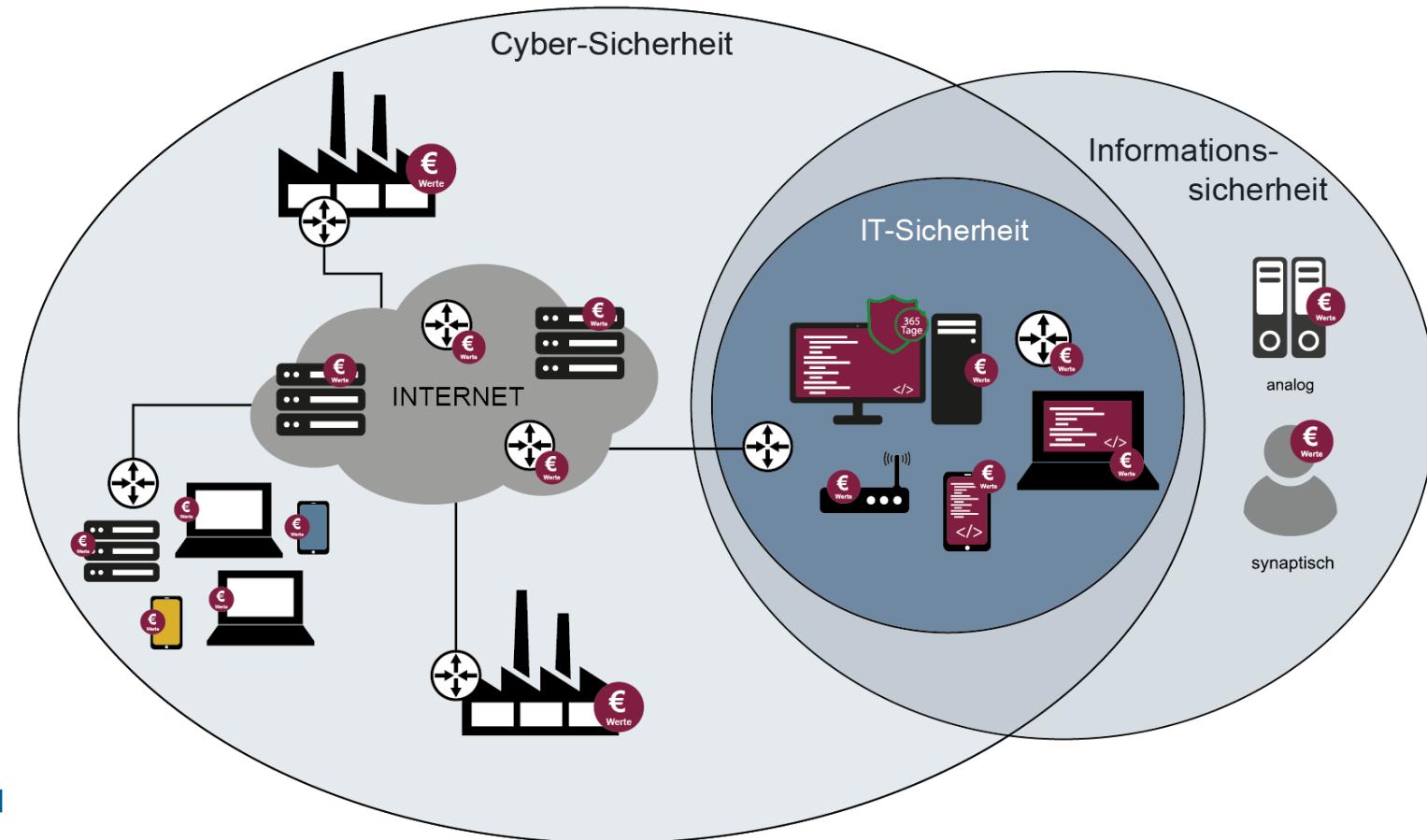
- **Definition IT-Sicherheit [1]:** „IT-Sicherheit ist der Bereich der Informatik, der sich mit dem Schutz von Systemen und Informationen in allen ihren Erscheinungsformen beschäftigt. Der Schutz umfasst insbesondere die Abwehr von mutwilligen, bösartigen Angriffen auf Systeme oder Informationen“
- **Definition System [12]:**
„Unter einem System wird ein Ausschnitt aus der realen oder gedanklichen Welt, bestehend aus Gegenständen [...] und darauf vorhandenen Strukturen [...] verstanden. Systemteile, die nicht weiter zerlegbar sind oder zerlegt werden sollen, werden als Systemelemente verstanden“.
- **Definition Softwaresystem [12]:**
„Ein Softwaresystem ist [...] ein System, dessen Systemkomponenten und Systemelemente aus Software bestehen“.

- **Informationstheorie ist ein Bereich der Mathematik/Informatik, der sich mit der Übertragung und Kodierung von Information in Daten beschäftigt.**
- **Definition Information: Information ist das Wissen, das ein Absender einem Empfänger über einen Kanal vermittelt.**
- **Über den Kanal werden Daten übertragen, die durch Zeichen kodiert sind. Einzelne Zeichen werden durch eine Syntax zu Daten angeordnet.**
- **Aus Daten wird durch eine Interpretationsvorschrift Information.**



- **Definition Cybersicherheit:** Cyber-Sicherheit [...] befasst sich mit allen Aspekten der IT-Sicherheit, wobei das Aktionsfeld auf den gesamten Cyberraum ausgeweitet wird“ [13].
- **Definition Cyberraum:** „Der Cyberraum umfasst sämtliche mit dem globalen Internet verbundene IT-Systeme und IT-Infrastrukturen sowie deren Kommunikation, Anwendungen, Prozesse mit Daten, Informationen, Wissen und Intelligenzen einschließlich der Akteure.“ (frei nach [13])
- **Definition Informationssicherheit:** „Informationssicherheit zielt auf den Schutz von Informationen in allen ihren Erscheinungsformen durch technische, personelle und organisatorische Maßnahmen“

Zusammenhang Cyber-Sicherheit, IT-Sicherheit und Informationssicherheit



Bildquelle: [13]

Wichtige Teilgebiete der Cybersicherheit

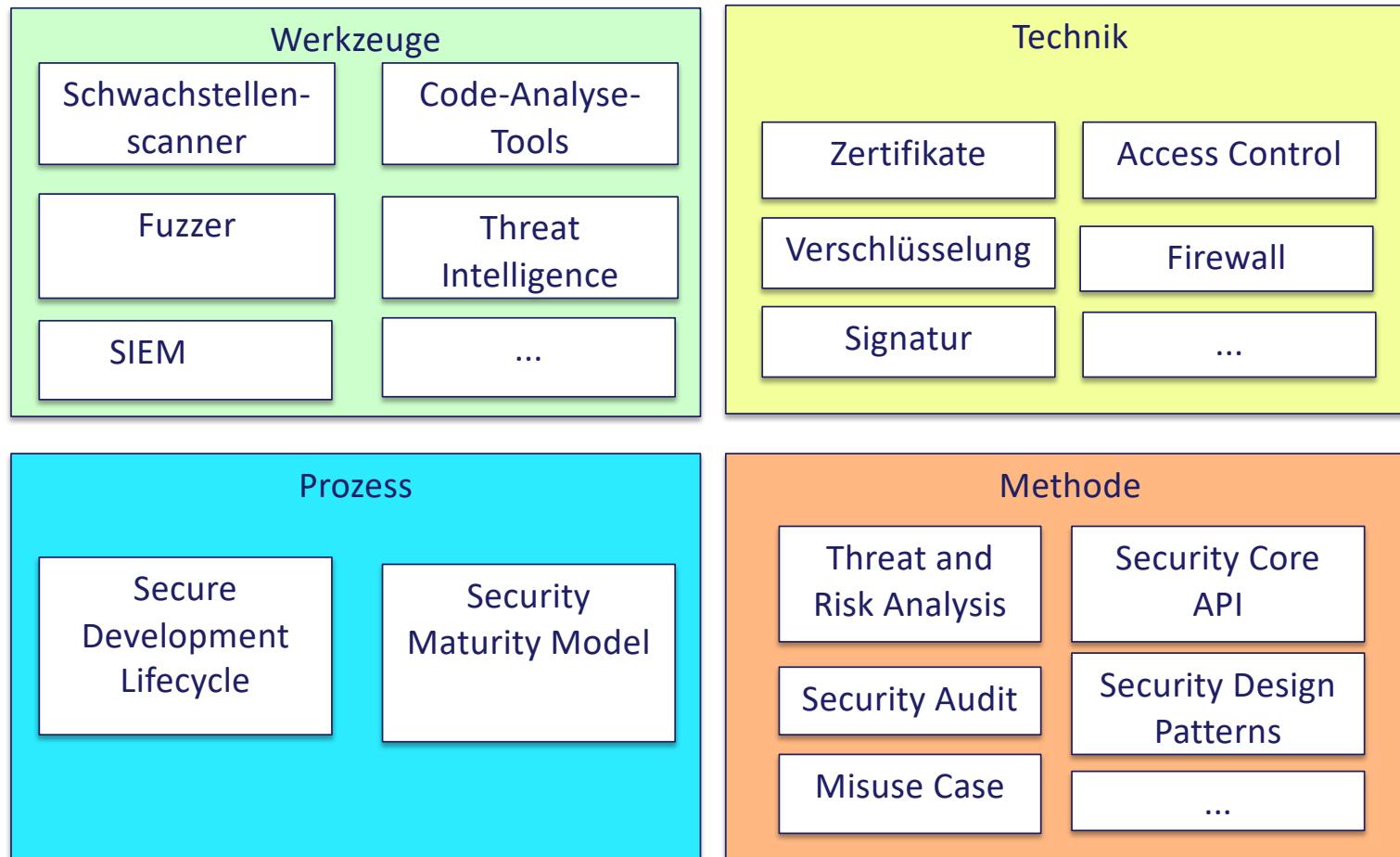


- Definition Security-Engineering: Security-Engineering ist der Bereich der IT-Sicherheit, der sich mit Techniken, Werkzeugen, Prozessen und Methoden für Entwurf, Implementierung und Test von Systemen und Anpassungen existierender Systeme an sich ändernde Umweltbedingungen beschäftigt mit dem Ziel, Systeme zu erzeugen, die auch unter Angriff zuverlässig funktionieren (nach [2]).

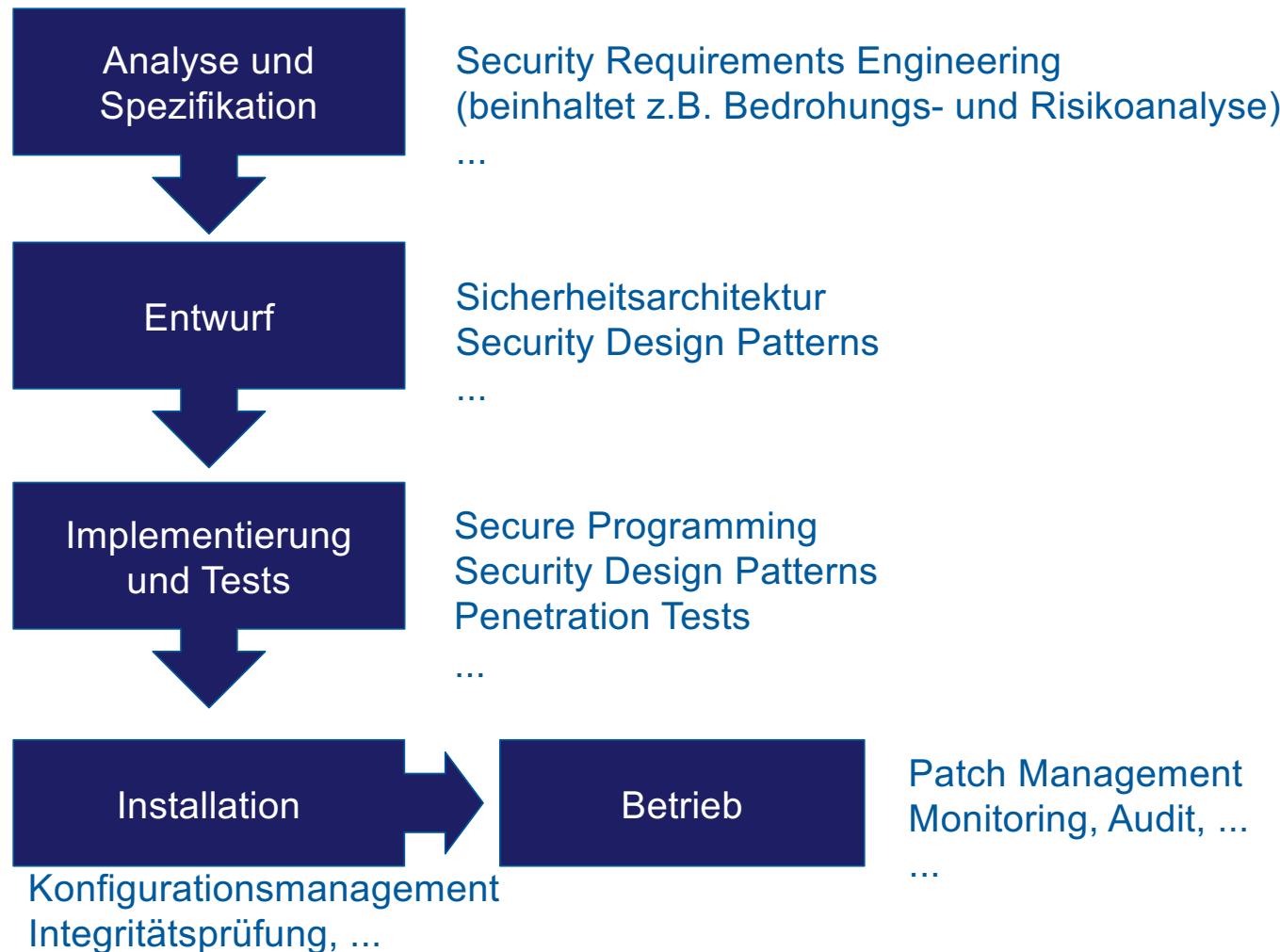
Welche Techniken, Werkzeuge, Prozessen und Methoden für

- Entwurf,
- Implementierung und
- Test von Systemen auf deren IT-Sicherheit
- Anpassung existierender Systeme an sich ändernde Umweltbedingungen zum Erhalt eines angemessenen Schutzniveaus

kennen Sie bereits?



Security Engineering im Softwarelebenszyklus



Referenzen



- [1] Marie-Theres Tinnefeld, Benedikt Buchner, Thomas Petri, Hans-Joachim Hof: „Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht“, 6. Auflage, Beck Verlag, ISBN 978-3110416725, 2017
- [2] Ross Anderson: „Security Engineering: A Guide to Building Dependable Distributed Systems“, 2. Auflage, Wiley Verlag, ISBN 978-0-470-06852-6, 2008
- [3] James Manyika, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, Dan Aharon: „The Internet of Things: Mapping the Value Beyond the Hype“, McKinsey&Company Report, 2015, online verfügbar: https://www.mckinsey.de/files/unlocking_the_potential_of_the_internet_of_things_full_report.pdf [letzter Abruf 24.02.2017]
- [4] Shell Deutschland, Prognos AG: „Shell PKW-Szenarien bis 2040 - Fakten, Trends und Perspektiven für Auto-Mobilität“, 2014, online verfügbar: https://www.prognos.com/uploads/tx_atwpubdb/140900_Prognos_Shell_Studie_Pkw-Szenarien2040.pdf [letzter Abruf 24.02.2017]
- [5] Robert „Hobbes“ Zakon: „Hobbes‘ Internet Timeline 24“, 2017, online verfügbar: <https://www.zakon.org/robert/internet/timeline/> [letzter Abruf 24.02.2017]
- [6] <https://www.businessinsider.de/karriere/gehaelter-in-der-it-wo-eine-ausbildung-mehr-geld-bringt-als-der-bachelor-a/>
- [7] <https://www.bitkom.org/Presse/Presseinformation/Markt-fuer-IT-Sicherheit-auf-Allzeithoch>
- [8] <https://www.computerwoche.de/a/fachkraetemangel-erhoeht-das-sicherheitsrisiko,3550024>
- [9] <https://www.computerwoche.de/a/wie-firmen-die-it-sicherheit-erhoehen,3548081>
- [10] http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf
- [11] Maria Baezner, "Cyber and Information warfare in the Ukrainian conflict", Technical Report, ETH Zurich, 2018. URL: [[https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/321570/20181003_MB_HS_RUS-UKRV2_rev.pdf]]
- [12] Helmut Balzert, „Lehrbuch der Softwaretechnik - Basiskonzepte und Requirements Engineering“, Spektrum Akademischer Verlag Heidelberg, ISBN 978-3-8274-1705-3, 3. Auflage, 2009
- [13] Norbert Pohlmann, Glossar Cybersicherheit, <https://norbert-pohlmann.com/glossar-cyber-sicherheit/cyber-sicherheit-2/> [letzter Abruf 01.03.2022]