HOCHSCHULE MITTWEIDA
University of Applied Sciences

Rechtsgrundlagen Cybercrime

Zusammenfassung und Ausblick

Prof. Dr. Dirk Labudde

Bundeskriminalamt

Cybercrime

Cybercrime

Cybercrime umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne) oder die mittels dieser Informationstechnik begangen werden (Cybercrime im weiteren Sinne).

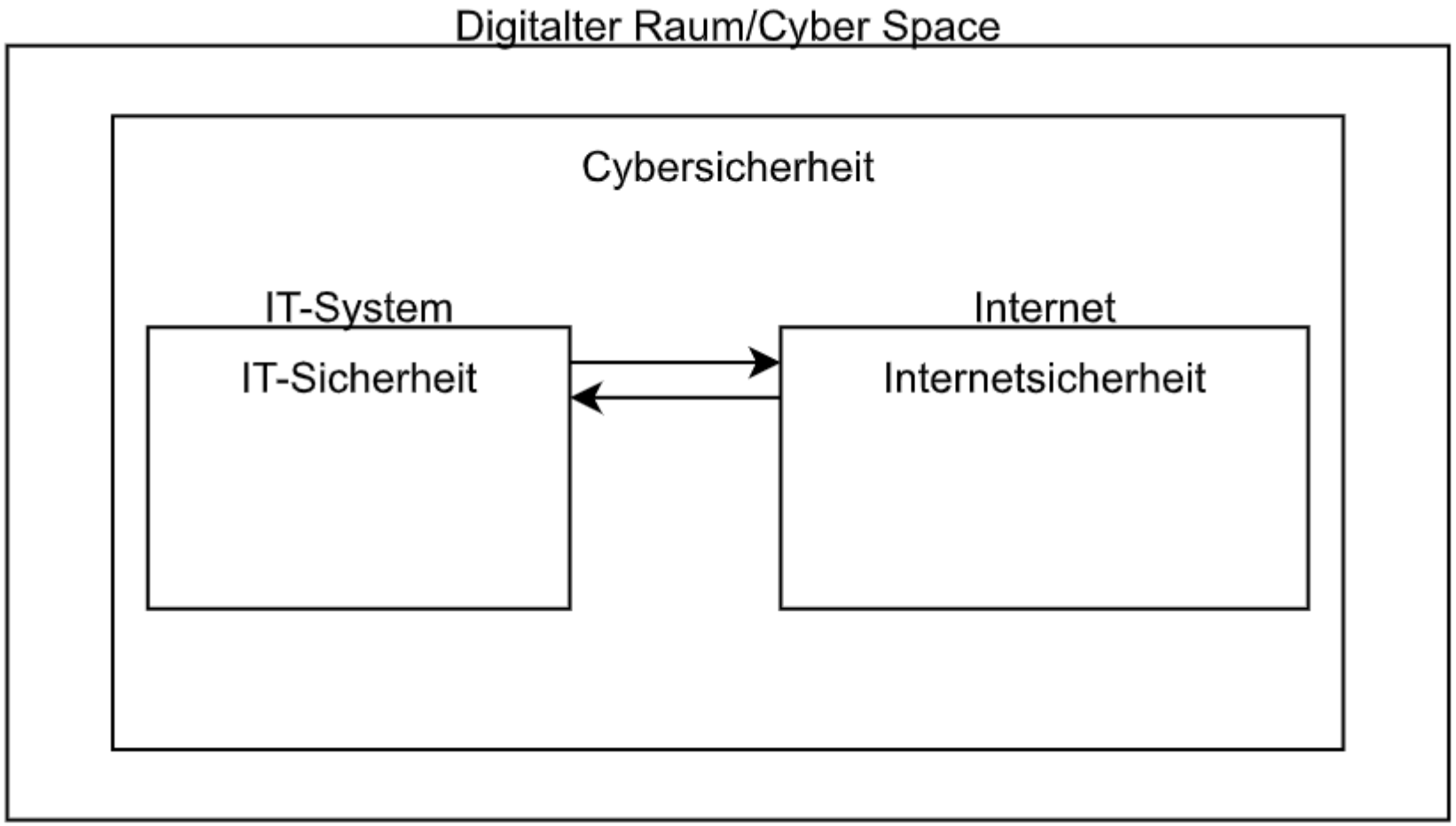
Cybercrime im engeren Sinne (CCieS)

- Delikte, bei denen in den Tatbestandsmerkmalen der jeweiligen Norm (Straftat oder auch Ordnungswidrigkeit) Elemente der elektronischen Datenverarbeitung genannt sind
- Z.B. der Computerbetrug (§ 263a StGB), das Ausspähen und Abfangen von Daten (§§ 202a, 202b, 202c StGB), die Datenveränderung sowie die Datensabotage (§§ 303a und 303b StGB
- Weitere Gesetze:
  - Urheberrechtsgesetz (UrhG),
  - Bundesdatenschutzgesetz (BDSG),
  - Telekommunikationsgesetz (TKG)

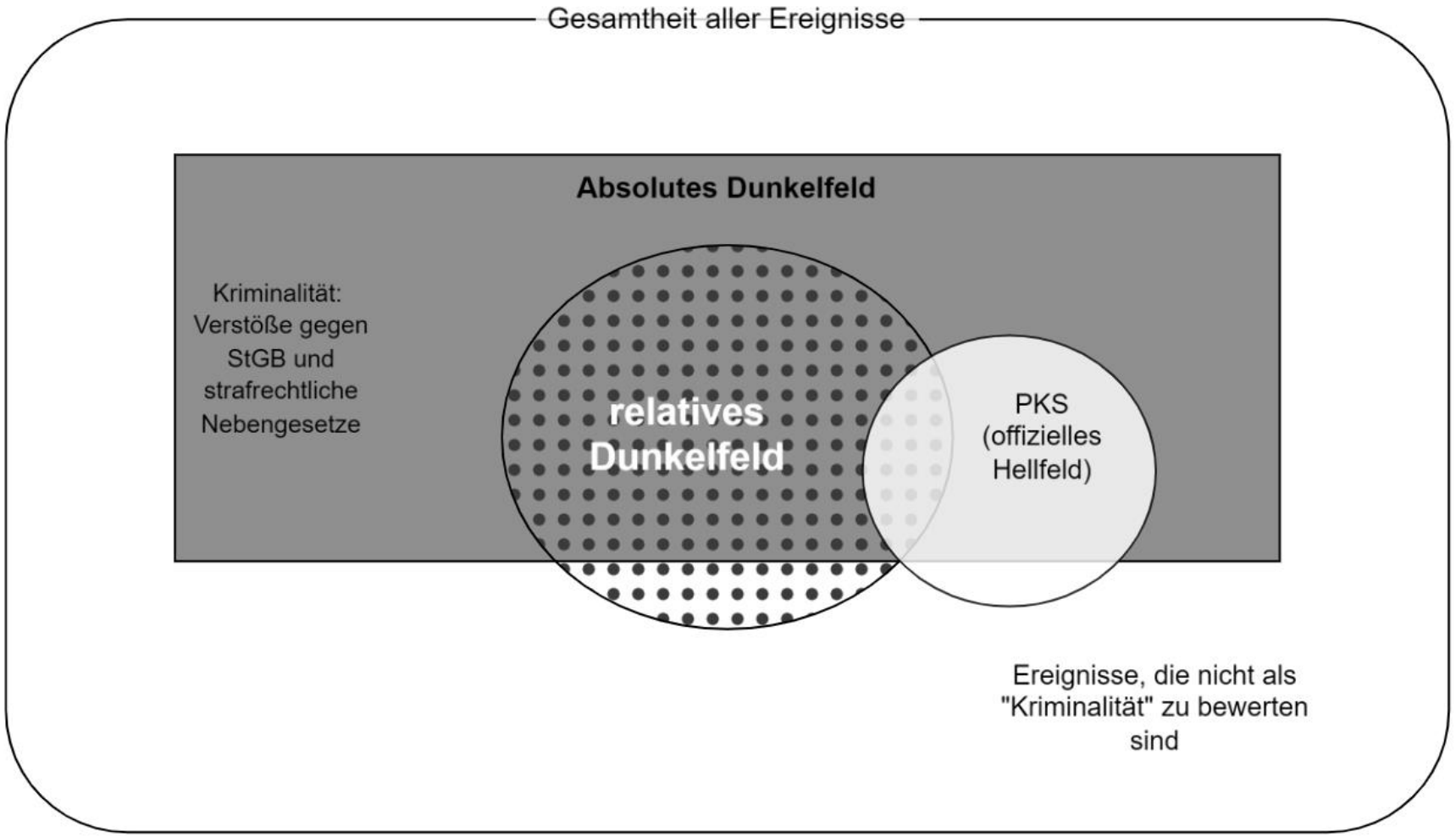
Cybercrime im weiteren Sinne (CCiwS)

- Straftaten, für deren Durchführung ein elektronisches Datenverarbeitungssystem unter Einbezug von Informations- und Kommunikationstechnik genutzt wird
- Beispiele:
  - Warenkreditbetrug,
  - Propagandastraftaten aus extremistischen Kreisen,
  - Gewaltverherrlichung,
  - das Verbreiten von Kinderpornografie
  - Beleidigungstatbestände.

Cyber Space



Hellfeld vs. Dunkelfeld



Hellfeld vs. Dunkelfeld

- Hellfeld: Summe aller Straftaten (Kriminalität), die den Strafverfolgungsbehörden bekannt ist, also offiziell registrierte Straftaten
- Absolutes Dunkelfeld: Summe aller Straftaten (Kriminalität), die den Strafverfolgungsbehörden nicht bekannt ist
- Relatives Dunkelfeld: schließt offiziell nicht erfasste, aber durch Befragungen bekannte Straftaten mit ein

Strafrechtsnormen

Strafrechtsnormen (CCieS)

- § 263a StGB – Computerbetrug
- §§§ 269, 270 StGB – Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung
- § 202a StGB – Ausspähen von Daten
- § 202b StGB – Abfangen von Daten
- § 202c StGB – Vorbereiten des Ausspähens und Abfangen von Daten
- § 202d StGB – Datenhehlerei
- § 303a StGB – Datenveränderung
- § 303b StGB – Computersabotage
- Softwarepiraterie: Herstellen, Überlassen, Verbreiten oder Verschaffen von sog. „Hacker-Werkzeugen“, die illegalen Zwecken dienen (§ 202c StGB)

Phänomene

Cybercrime hat viele Gesichter

Phänomene

Ausblick

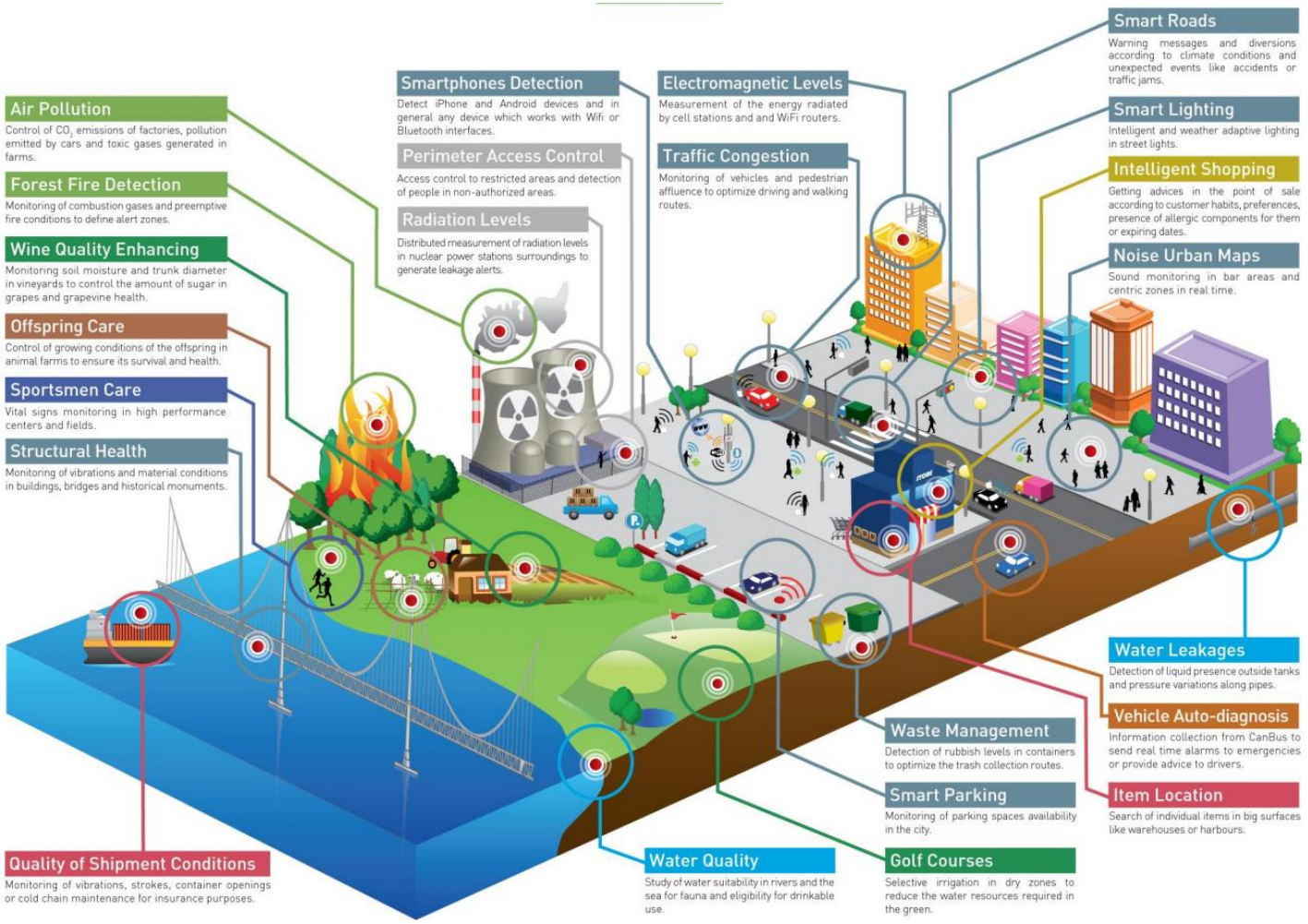
IoT und KI

Trends zeigen die Ausweitung der Technologie in Richtung Internet der Dinge (IoT) und Smart Home.
Alles soll zukünftig vernetzt sein, angefangen vom TV-Gerät bis hin zum Auto und der Kaffeemaschine.

Künstliche Intelligenz und IoT

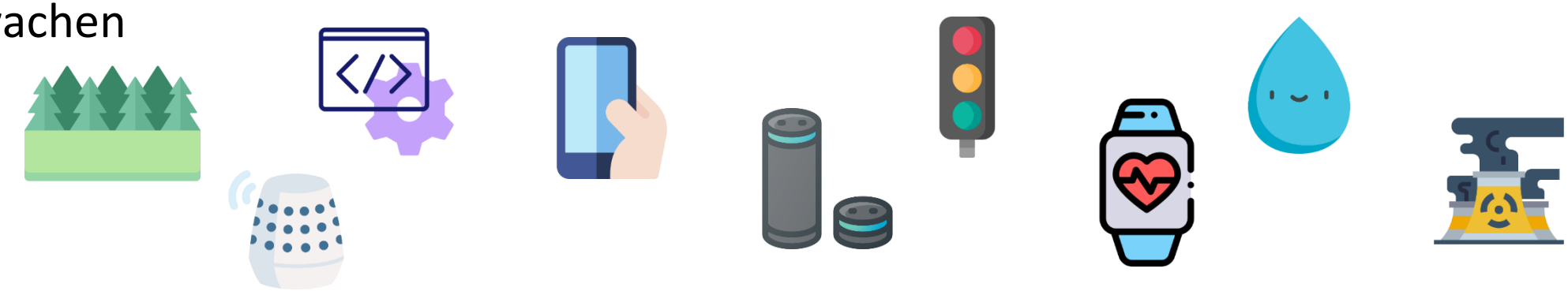
KI bietet die Chance, die Daten, die im IoT-Umfeld anfallen, besser als jemals zuvor zu analysieren.
So lassen sich entsprechend IoT-Lösungen besser in ein vorgegebenes Umfeld integrieren. Dies kann durch eine intelligente Echt-Zeit-Analyse bewerkstelligt werden und liefert neue anwendbare Muster.
Es lässt sich also der Grundsatz ableiten:
In Zukunft muss noch mehr das IoT zusammen mit KI gedacht werden.

Künstliche Intelligenz und IoT



IoT - Anwendungsfelder

- **Air Pollution**: Luft-/Umweltverschmutzungsgrad überwachen. Sensoren ermitteln die CO2-Emissionen in Industrieanlagen und an Verkehrswegen
- **Smartphone Detection:** Per WiFi oder Bluetooth lässt sich ein Smartphone in der Nähe erkennen. MAC-Adr., Hersteller und RSSI sind abfragbar. Wie lange hat sich „das Smartphone“ in einem bestimmten Bereich aufgehalten?
- **Structural Health**: Vibrationen und Materialzustand von Brücken, Gebäuden und Denkmälern permanent erfassen und auswerten
- **Sportsmen Care**: Vitalsignale von Sportlern draußen und im Fitnesscenter überwachen



Anwendungen von Public IoT

Öffentliche Sicherheit

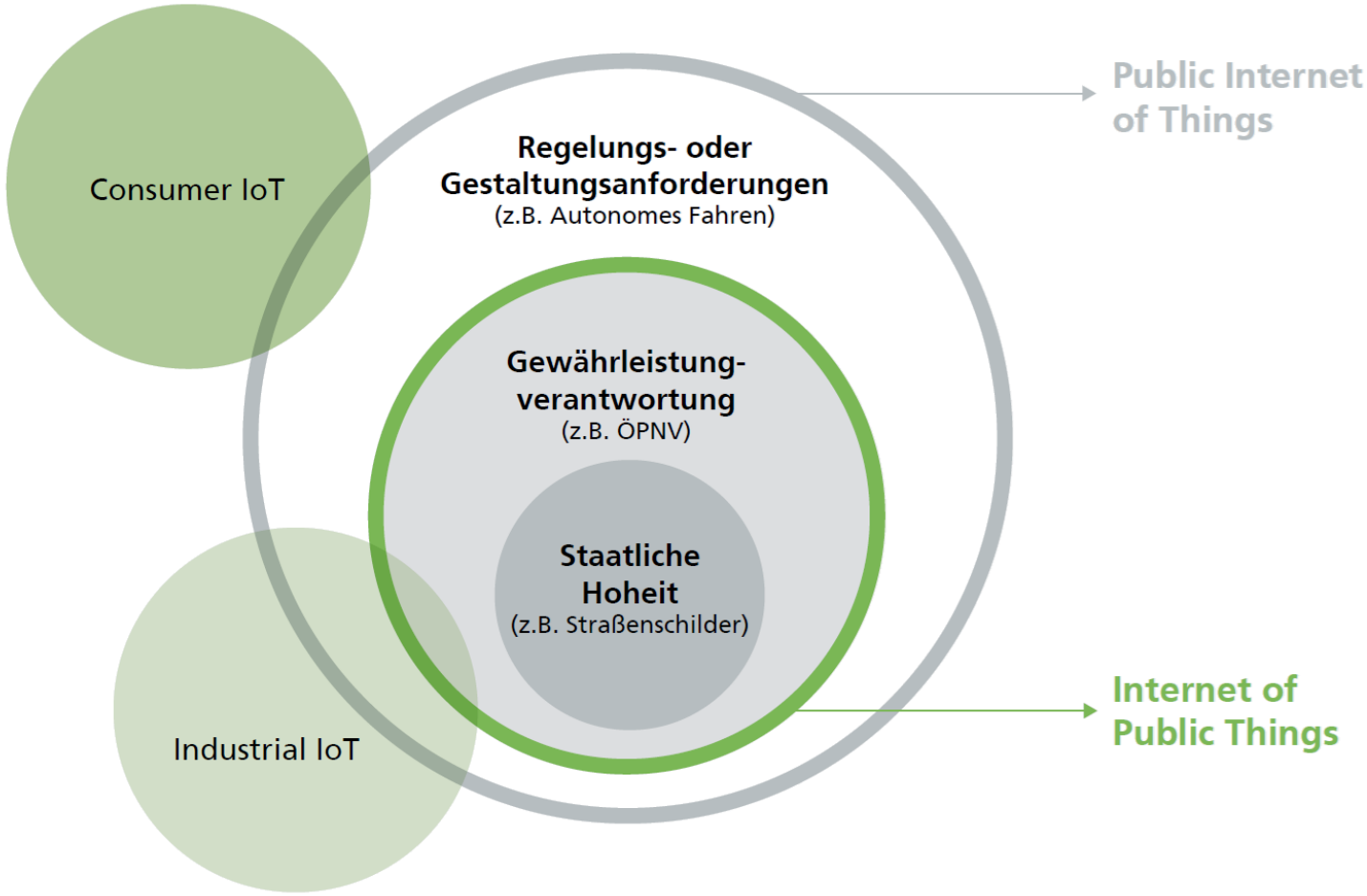
Verkehr

Energie

Umwelt und Bauen

Gesundheitswesen

Anwendungen von Public IoT



Was heißt „Internet der Dinge“ (idD) / „Internet of Things“ (IoT)?

Beispiele, wie der Mensch zur Quelle und Senke von Daten wird:

- Wearables erfassen mittels Sensoren Bewegungsabläufe, Körpertemperatur, Pulse, und weitere Vitalwerte
- Google und Novartis entwickeln eine smarte Kontaktlinse mit Chip und Antenne, welche den Glukosegehalt messen kann und die Werte an ein Smartphone sendet
- Proteus Digital Health hat ein System entwickelt, mit dem die Medikamenteneinnahme per Sensor aus dem Magen überwacht werden kann.

KI und IoT

- Datenproduktion
- Datenanalyse
- Simultane Analyse

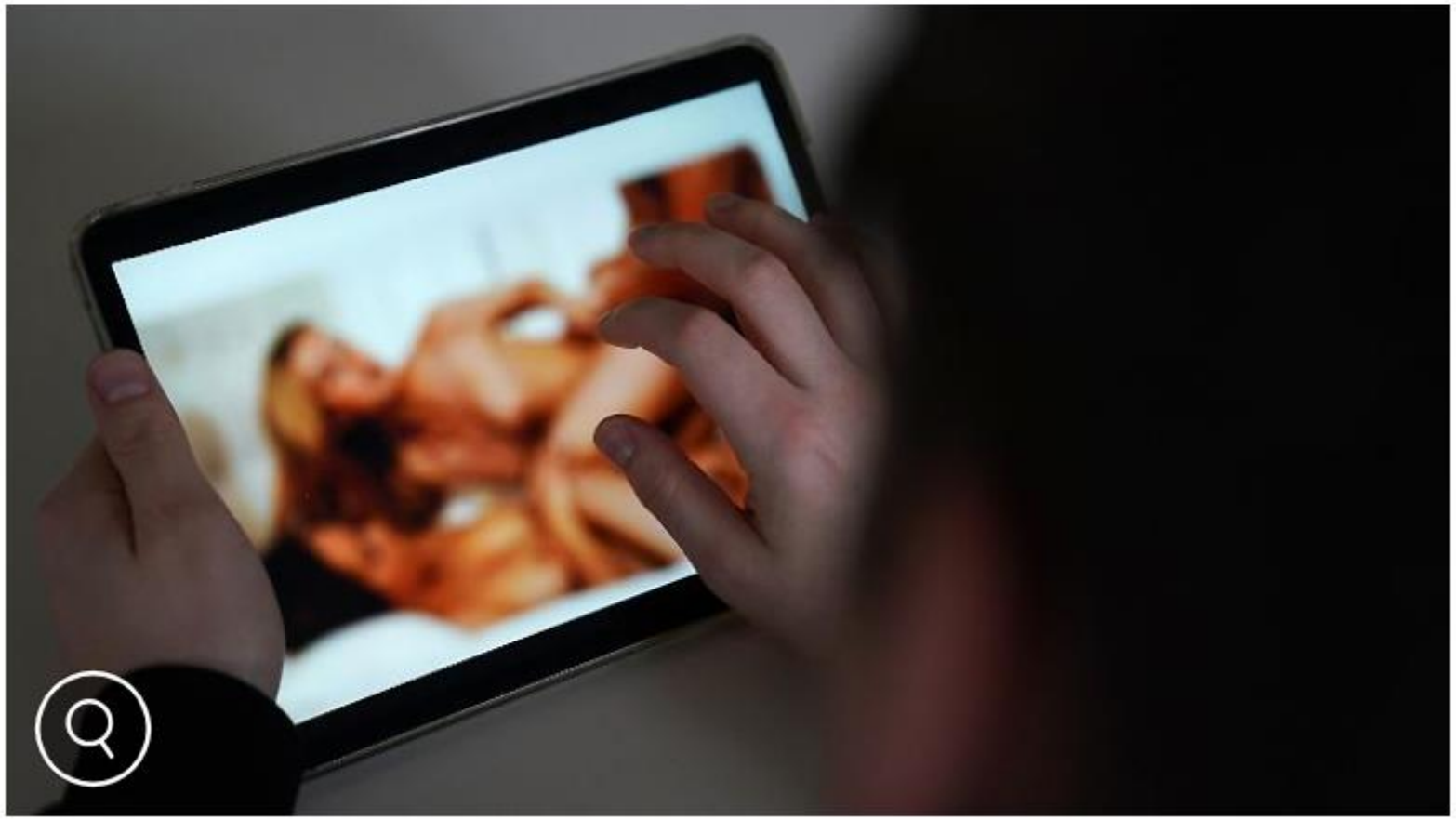
KI beeinflusst Cybercrime

Bei KI-Recherchen

Moderatorin entdeckt "Deepfake"-Pornos von sich

17.04.2024, 10:51 Uhr

Artikel anhören

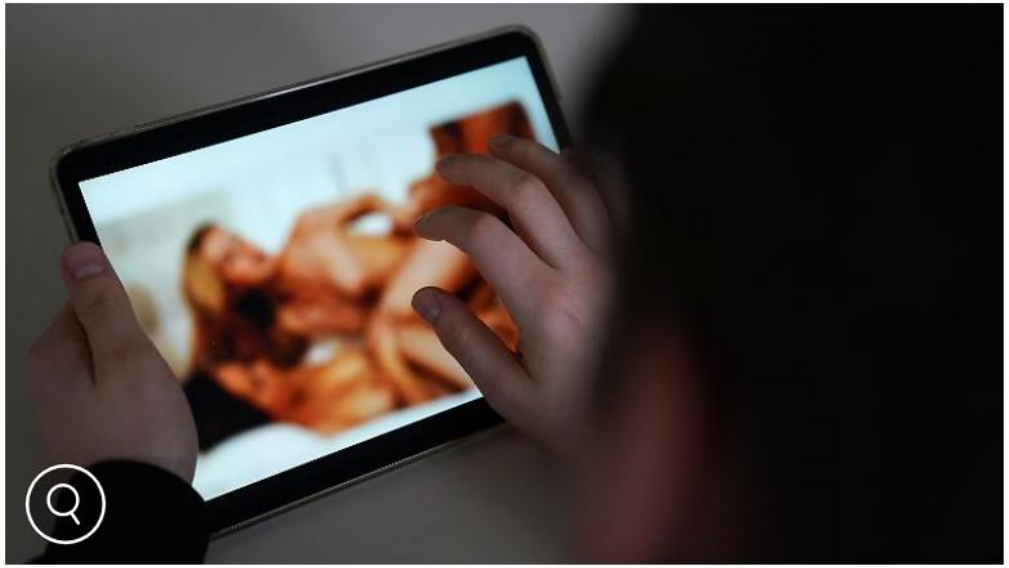


Bei KI-Recherchen

Moderatorin entdeckt "Deepfake"-Pornos von sich

17.04.2024, 10:51 Uhr

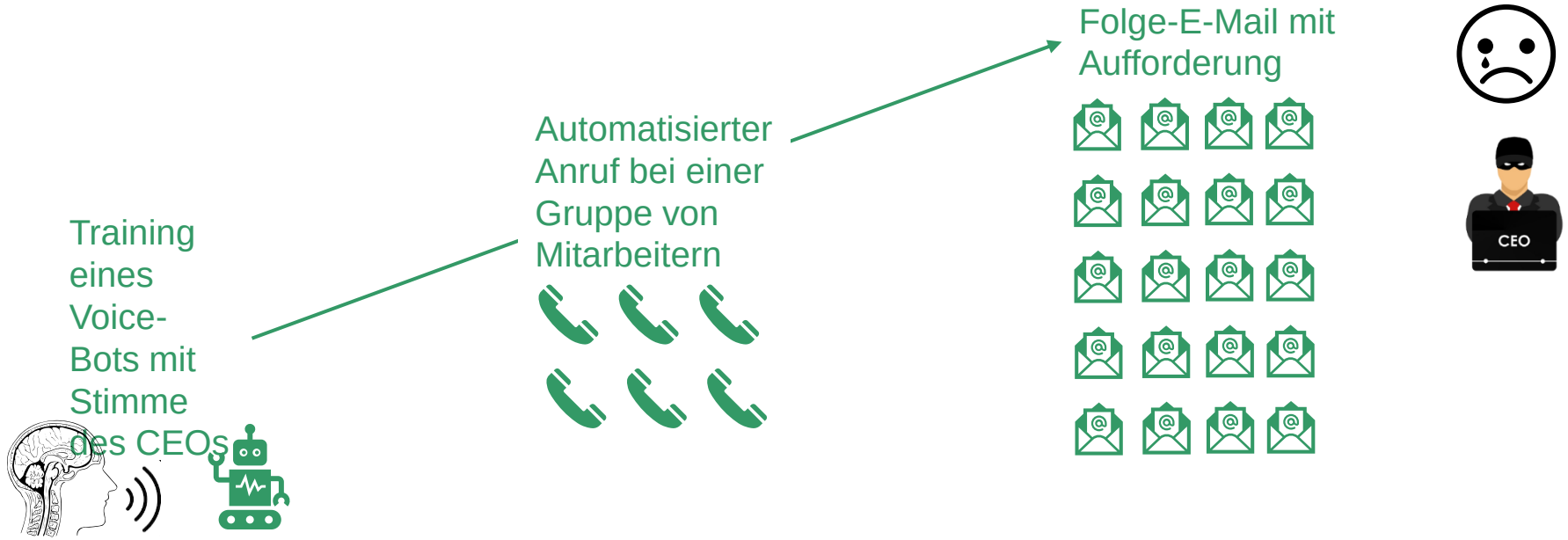
Artikel anhören



Während Meta [generelle] Vorfälle untersucht, will die britische Regierung Nägel mit Köpfen machen und die Generierung von sexualisierten Deepfakes unter Strafe stellen, auch wenn die Inhalte nicht mit anderen geteilt werden sollen. [Quelle: heise]

Next Generation Phishing

Zusätzliche Informationen über die Firma und deren Mitarbeiter



Kriminelle Anwendungen - Täuschungen

Fake-basiert

Betrugsmasche: Mit Chef-Stimme Transaktion erzwungen – Neuer Fall bei „Aktenzeichen XY“

Fake Payments: In diesen Fällen wird eine falsche Rechnung vorab für Waren / Dienstleistungen gestellt, die durchaus einer üblichen Rechnung entsprechen können. Die richtigen Ansprechpartner im Ziel-Unternehmen werden häufig mittels Social Engineering ermittelt.

Payment Diversion (auch „Mandate-Fraud“): Dabei geben sich die Betrüger als Geschäftspartner oder als Lieferanten aus und teilen mit, dass sich die bisherige Bankverbindung geändert hat. Das Opfer (Mitarbeiter Buchhaltung / Rechnungswesen / Finanzen) erhält i. d. R. eine E-Mail mit der Mitteilung über die geänderte Bankverbindung.

Scheckbetrug durch „Überzahlschecks“: Dabei meldet sich der Betrüger als vermeintlicher Käufer aus dem Ausland und es kommt zum Geschäftsabschluss. Der Betrüger überweist das Geld jedoch nicht, sondern schickt einen Auslandsscheck mit der Post, der über eine höhere Summe ausgestellt ist, als die Ware kostet. Das Opfer soll den „zu viel“ bezahlten Betrag zurücküberweisen. Nach Überweisung bzw. Zahlung via Western Union wird der Auslandsscheck mit dem Vermerk „gefälscht“ oder „mangels Deckung“ nicht eingelöst

Spear-Phishing

Zusätzliche Informationen über Mitarbeiter/Usergruppen

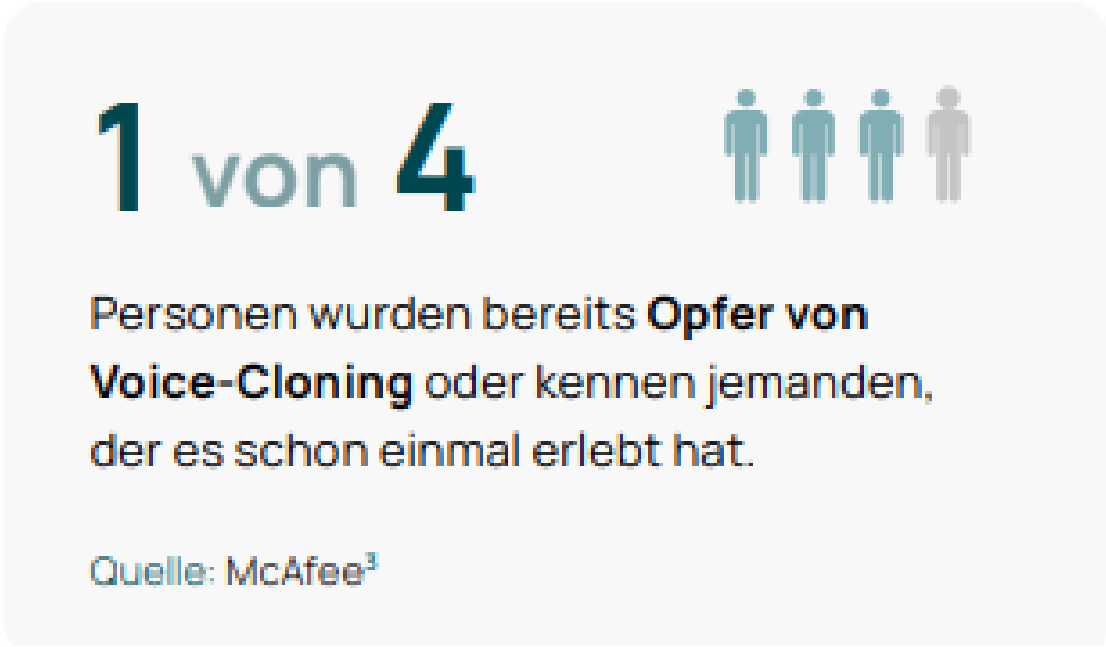
Bei Spear-Phishing handelt es sich um eine Betrugsmasche per elektronischer Kommunikation, die auf bestimmte Personen, Organisationen oder Unternehmen abzielt.

„Personalisierte“ E-Mail mit einer Aufforderung zum Handel!

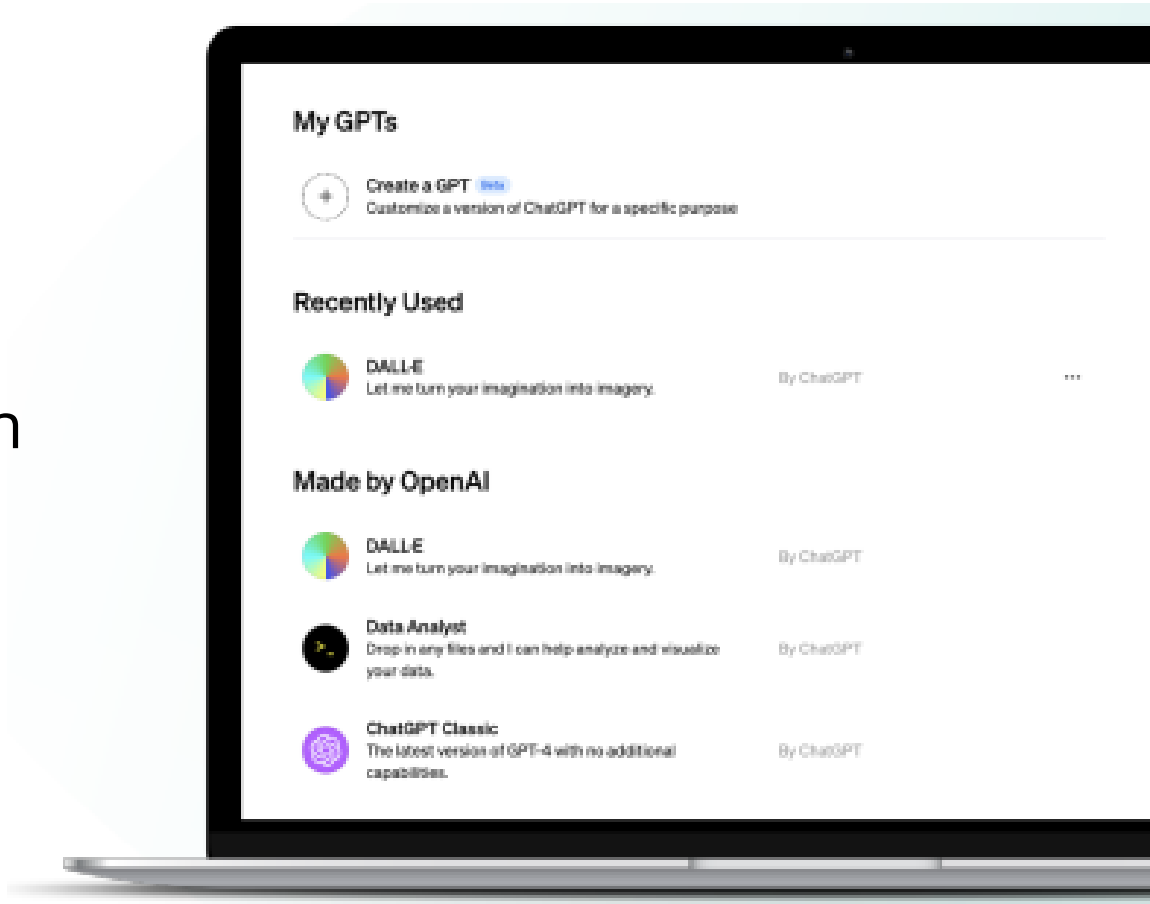
Aktivität/Link

Kriminelle Anwendungen - Täuschungen

Schon seit geraumer Zeit setzen Cyberkriminelle beide Technologien für ihre betrügerischen Zwecke ein. In jüngster Zeit häufen sich die Fälle jedoch aufgrund der schnellen Verbreitung von Tools, mit denen sich überzeugende Deepfake-Videos erstellen lassen, die nun vor allem bei Fehlinformations-Kampagnen und zur sozialen Manipulation genutzt werden



Personalisierte GPTs können zwar für viele Personen ein wertvoller Helfer sein, der sie bei täglichen Aufgaben unterstützt. Wir können jedoch davon ausgehen, dass 2024 auch Cyberkriminelle sich diese Möglichkeit zunutze machen und ihre ganz persönlichen HackingAssistenten erschaffen10 und sie dazu trainieren, extrem überzeugende Smishing-Nachrichten, SpearPhishing-Mails oder polymorphe Malware zu verfassen. [Quelle: HYAS 2023]



Cyberkriminelle fokussieren sich vermehrt auch auf neue Technologien. Dies konnte bereits beispielsweise im Bereich Cloud Computing und Künstliche Intelligenz beobachtet werden.

Ein ähnliches Schicksal ist für andere neue Technologien wie Quantencomputing zu erwarten. Dabei gehen Cyberkriminelle nach einer potenziell gefährlichen Methode vor:

„Harvest now, decrypt later“ (HNDL).

Das heißt, sie fokussieren sich zunächst auf das Sammeln verschlüsselter Daten in der Hoffnung, dass sie durch den Fortschritt im Quantencomputing in Zukunft in der Lage sein werden, die gesammelten Daten zu entschlüsseln.

Dieses Szenario könnte zu Datenschutzverstößen, Diebstählen geistigen Eigentums und Freilegung nationaler Sicherheitsstrategien von nie dagewesenem Ausmaß führen. [Quelle: SoSafe – Trends 2024]

Cybercrime ist eine sich schnell verändernde Disziplin. Alle Akteure werden und müssen sich auf zukünftige technische Mittel und Herausforderungen vorbereiten.

Vielen Dank

Prof. Dr. rer. nat. Dirk Labudde

Hochschule Mittweida | University of Applied Sciences
Technikumplatz 17 | 09648 Mittweida
Fakultät Computer- und Biowissenschaften | Fraunhofer Lernlabor

T +49 (0) 3727 58-1469
F +49 (0) 3727 58-21469

labudde@hs-mittweida.de

Haus 8 | Richard Stücklen-Bau | Raum 8-105
Am Schwanenteich 6b | 09648 Mittweida

HOCHSCHULE MITTWEIDA
University of Applied Sciences

hs-mittweida.de