HOCHSCHULE MITTWEIDA
University of Applied Sciences

# Rechtsgrundlagen Cybercrime

## Herausforderungen

Prof. Dr. Dirk Labudde

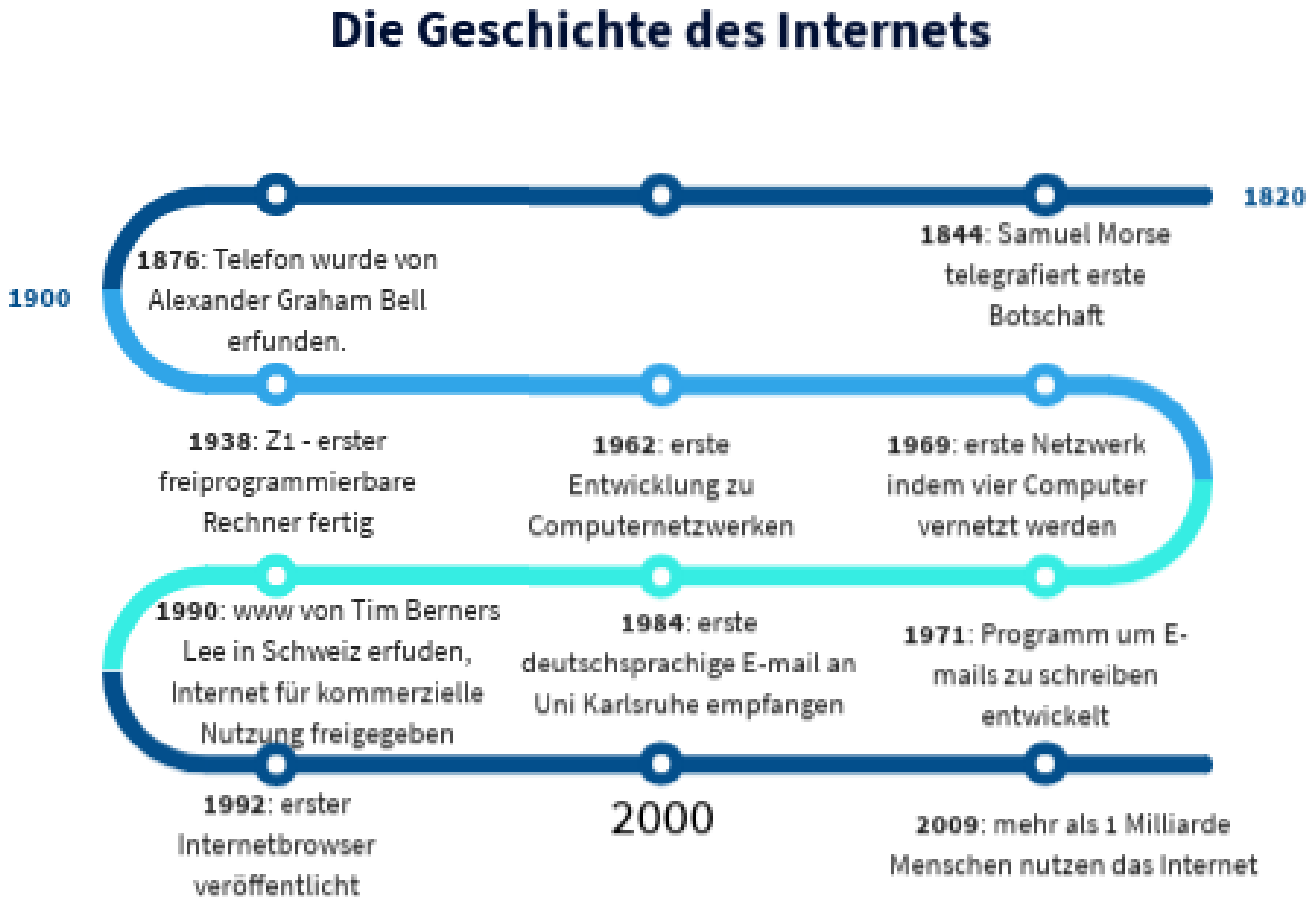
Bundeskriminalamt

# Herausforderungen im Zusammenhang mit Cybercrime

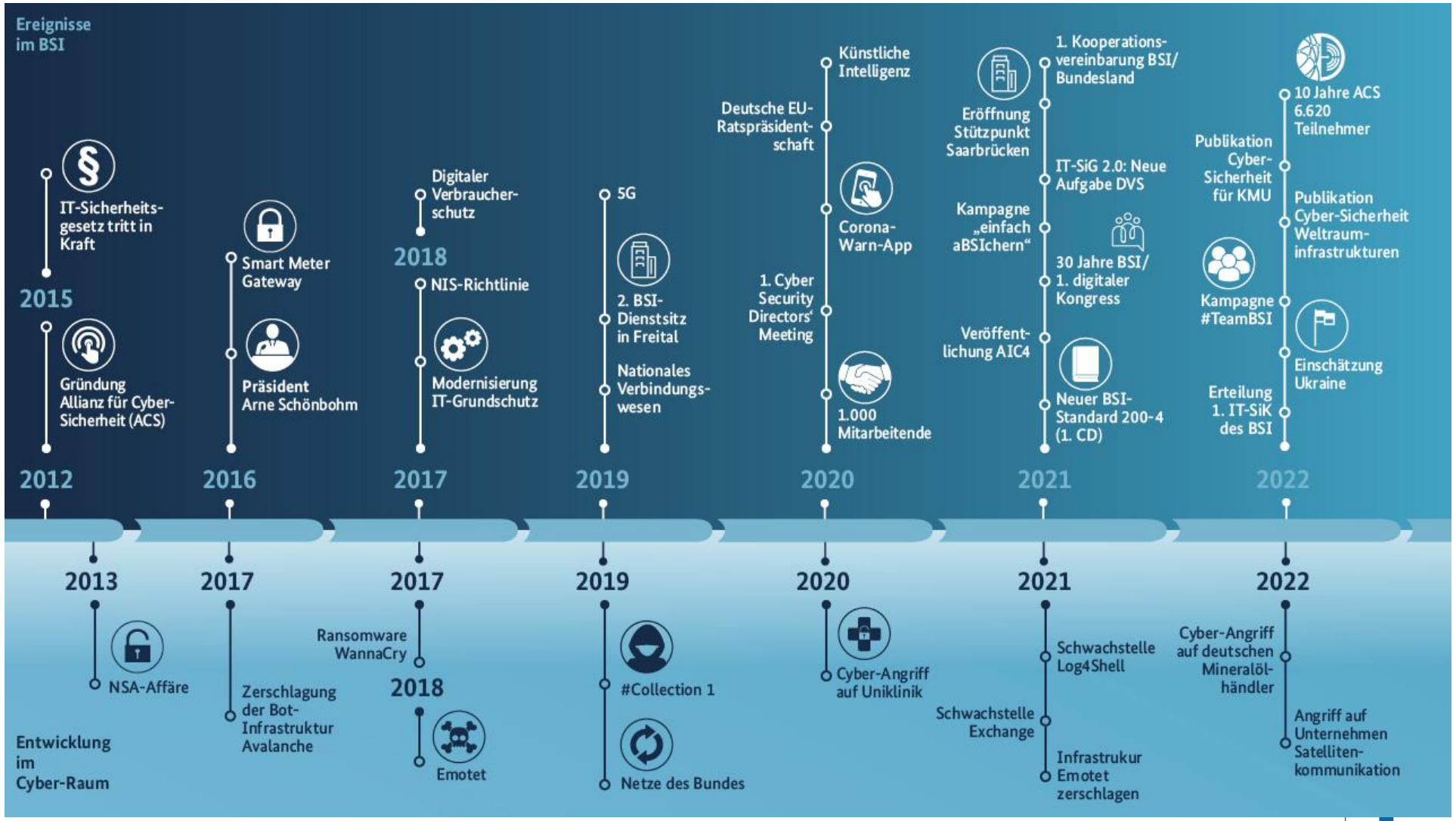
- schnelle technologische Entwicklung
- zeitintensive Gesetzgebungsprozesse
- Industrialisierung von Cybercrime
- Faktor Mensch

# Schnelle technologische Entwicklung

# Entwicklung damals



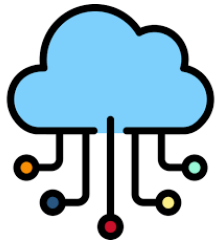
# Ereignisse im BSI



# „Neue“ Technologien für die breite Masse

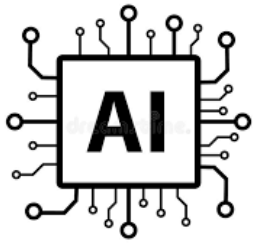
## Cloud-Computing

Die Verbreitung von Cloud-Computing-Technologien hat Unternehmen und Einzelpersonen ermöglicht, auf sichere und kostengünstige Weise auf eine Vielzahl von IT-Ressourcen zuzugreifen, ohne eigene physische Infrastruktur betreiben zu müssen. Dies hat die Flexibilität, Skalierbarkeit und Zusammenarbeit verbessert.



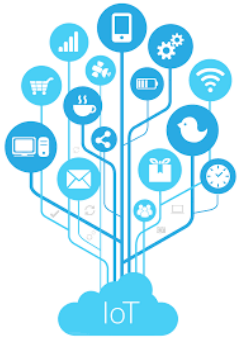
## Künstliche Intelligenz und maschinelles Lernen

Fortschritte in den Bereichen künstliche Intelligenz und maschinelles Lernen haben die Entwicklung intelligenter Systeme ermöglicht, die komplexe Aufgaben ausführen können, wie Bilderkennung, Sprachverarbeitung, automatisierte Entscheidungsfindung und persönliche Assistenten wie Siri und Alexa.




## Internet der Dinge (IoT)

Die Vernetzung von physischen Geräten und Objekten mit dem Internet hat zu einer neuen Ära des "intelligenten" Wohnens und Arbeitens geführt. Durch IoT können Geräte miteinander kommunizieren und Daten austauschen, um Effizienz zu steigern, Automatisierung zu ermöglichen und neue Dienste bereitzustellen.



# Die Hälfte aller Cyberangriffe haben ihren Ursprung in der Cloud

5. Dezember 2023

Die Hälfte aller Cyberangriffe haben ihren Ursprung in der Cloud und kosten Unternehmen im Schnitt 4,1 Millionen US-Dollar. Die Studie von Illumio unterstreicht zudem, dass Zero-Trust-Segmentierung für die Cloud-Sicherheit unverzichtbar ist. Ferner informiert die weltweite Studie „Cloud Security Index: Redefine Cloud Security with Zero Trust Segmentation“ über den aktuellen Stand der Cloud-Sicherheit, die Auswirkungen von Angriffen auf die Cloud und die Gründe für das Versagen herkömmlicher Cloud-Sicherheitstechnologien beim Schutz von Unternehmen in der Cloud.

Cloud-Anwendungen

# Hacker-Angriff auf Microsoft war gravierend

*Stand: 08.09.2023 12:03 Uhr*

**Im Juli hatten sich Hacker Zugang zu Outlook-E-Mail-Konten von 25 Organisationen verschafft. Nun gab Microsoft zu, dass sich die Hacker, die aus China kommen sollen, offenbar 2021 weitgehende Befugnisse in der Microsoft-Cloud verschafft hatten.**

## Die Hälfte aller Cyberangriffe haben ihren Ursprung in der Cloud

5. Dezember 2023



Die Hälfte aller Cyberangriffe haben ihren Ursprung in der Cloud und kosten Unternehmen im Schnitt 4,1 Millionen US-Dollar. Die Studie von Illumio unterstreicht zudem, dass Zero-Trust-Segmentierung für die Cloud-Sicherheit unverzichtbar ist. Ferner informiert die weltweite Studie „Cloud Security Index: Redefine Cloud Security with Zero Trust Segmentation" über den aktuellen Stand der Cloud-Sicherheit, die Auswirkungen von Angriffen auf die Cloud und die Gründe für das Versagen herkömmlicher Cloud-Sicherheitstechnologien beim Schutz von Unternehmen in der Cloud.

# Cloud-Security

**Why aren't traditional security tools enough? Organizations that use cloud-based services need more efficiency, visibility, and capabilities to reduce risks in their environment:**

**95%**
need better visibility into connectivity from third-party software.

**95%**
need better reaction times to cloud breaches.

**95%**
seek to reduce workloads / increase efficiency for security operations (SecOps) teams.

**Over 9 in 10**
are concerned that connectivity between their cloud services and on-premises environments increases the likelihood of a breach.

**46%**
don't have full visibility into the connectivity of their organization's cloud services, increasing the likelihood of unauthorized connections.

**Only 24%**
are highly confident they can stop attackers from lateral movement through their networks.

**What repercussions are organizations facing because of insufficient protection?**

- Nearly **half the data breaches** suffered over the past year **originated in the cloud**.
- The average organization **lost nearly $4.1 million** due to **cloud breaches** in the past year.

Cloud-Anwendungen

Hacker-Angrif

*Stand: 08.09.2023 12:03*

Im Juli hatten sich Hac
Organisationen versch
aus China kommen sollen, offenbar 2021 weitgehende Befugnisse in der Microsoft-Cloud verschafft hatten.

berangriffe haben ihren
oud

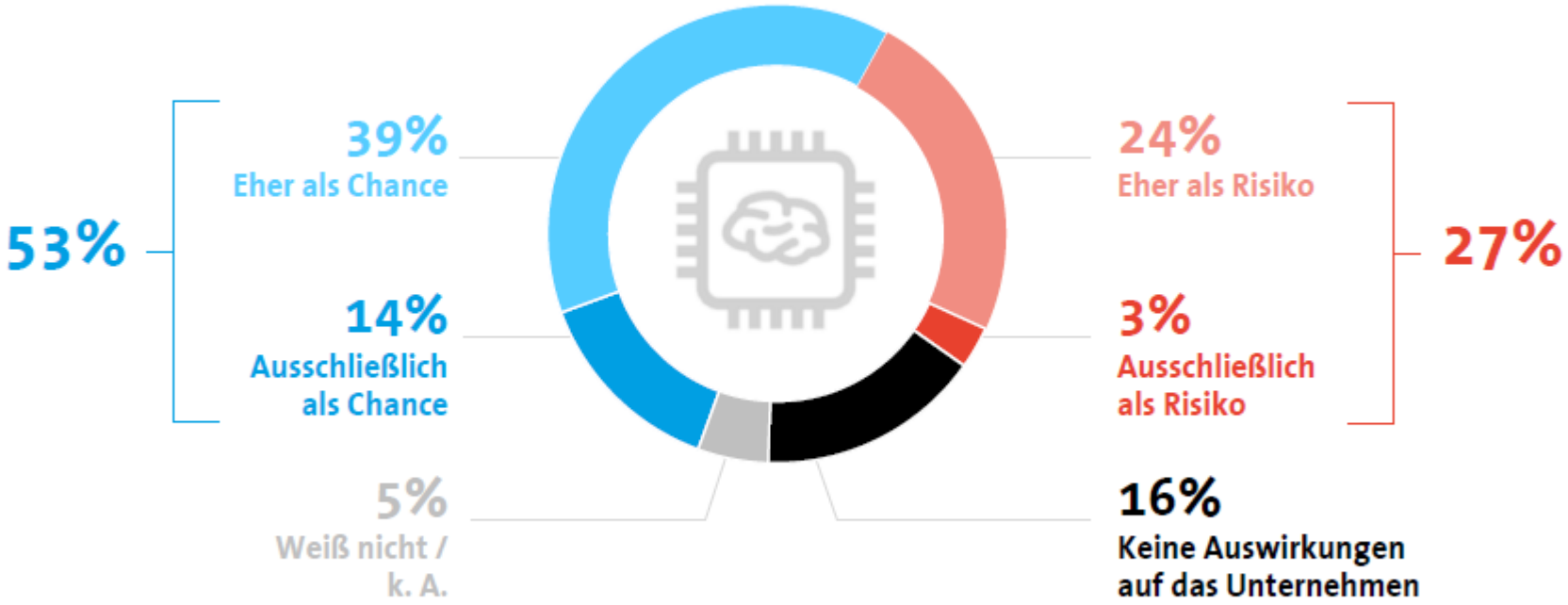


Die Hälfte aller Cyberangriffe haben ihren Ursprung in der Cloud und kosten Unternehmen im Schnitt 4,1 Millionen US-Dollar. Die Studie von Illumio unterstreicht zudem, dass Zero-Trust-Segmentierung für die Cloud-Sicherheit unverzichtbar ist. Ferner informiert die weltweite Studie „Cloud Security Index: Redefine Cloud Security with Zero Trust Segmentation" über den aktuellen Stand der Cloud-Sicherheit, die Auswirkungen von Angriffen auf die Cloud und die Gründe für das Versagen herkömmlicher Cloud-Sicherheitstechnologien beim Schutz von Unternehmen in der Cloud.

# Künstliche Intelligenz

## Mehrheit sieht Künstliche Intelligenz als Chance

Sehen sie Künstliche Intelligenz eher als Chance oder eher als Risiko für ihr Unternehmen?




11 Basis: Alle befragten Unternehmen (n=606) | Abweichungen zu 100 Prozent rundungsbedingt | Quelle: Bitkom Research

bitkom

# Künstliche Intelligenz

## Neuer Phishing-Betrug: KI-generierte Video-Anrufe

Die jüngste Betrugsmasche von Cyber-Kriminellen sei der CEO-Betrug, warnt die IT-Expertin - bekanntgeworden als "Hongkong-Bank-Betrug". Dabei handele es sich um eine neue Variante des "Phishing". Allerdings werde kein Link zu einer gefälschten Webseite verschickt, sondern KI simuliere Personen und Sprache in einem Videoanruf. "Man sieht realistische Videos." Vermeintliche Vorgesetzte würden darin Mitarbeiter auffordern, Geld zu überweisen.

Die Gefahr durch Cyber-Kriminalität sei kein neues Problem, ergänzt die Informatik-Professorin. "KI macht es einfach effektiver."

# Künstliche Intelligenz

Kriminalität in den Niederlanden

## Polizei warnt vor KI-generierter Kinderpornografie

**Den Haag** · Obwohl kinderpornografische Bilder, die mit künstlicher Intelligenz erstellt wurden, strafbar sind, nimmt ihre Zahl rasant zu. Jetzt hat die niederländische Polizei genau davor gewarnt und die KI-Hersteller zu Maßnahmen aufgefordert.

jenerierte Video-Anrufe

ne von Cyber-Kriminellen sei der CEO-Betrug, warnt die
orden als "Hongkong-Bank-Betrug". Dabei handele es sich um eine neue Variante des "Phishing". Allerdings werde kein Link zu einer gefälschten Webseite verschickt, sondern KI simuliere Personen und Sprache in einem Videoanruf. "Man sieht realistische Videos." Vermeintliche Vorgesetzte würden darin Mitarbeiter auffordern, Geld zu überweisen.

Die Gefahr durch Cyber-Kriminalität sei kein neues Problem, ergänzt die Informatik-Professorin. "KI macht es einfach effektiver."

# Künstliche Intelligenz

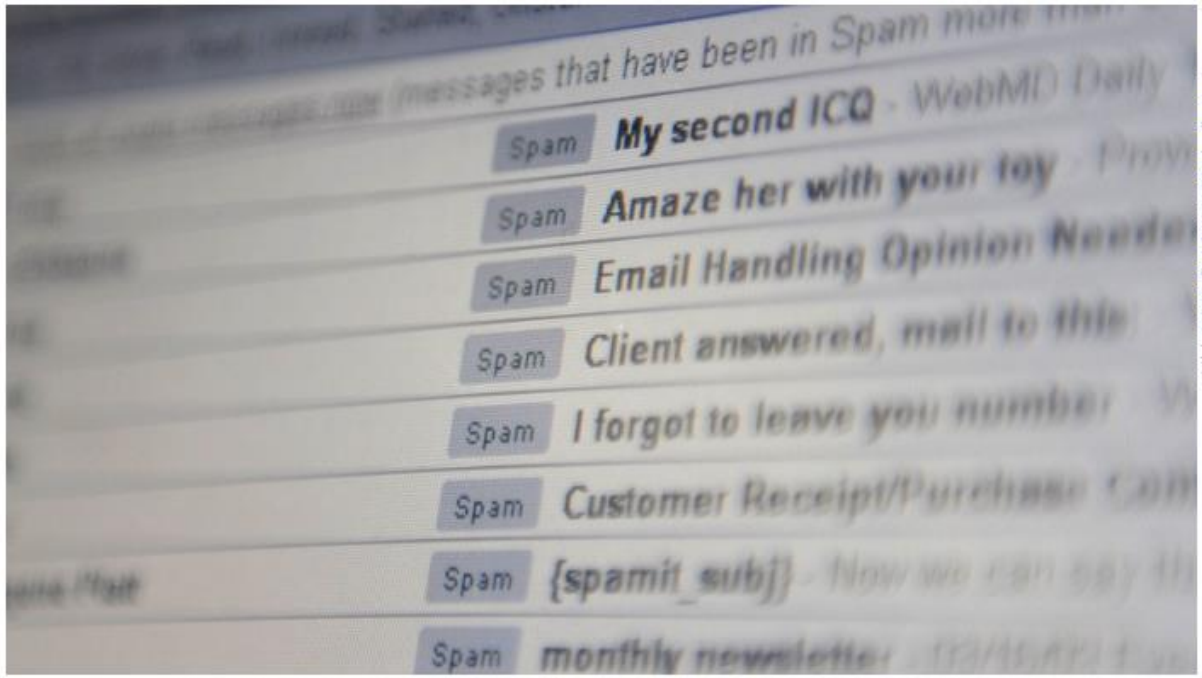
CHATBOT FÜR CYBERKRIMINELLE

## WormGPT generiert äußerst überzeugende Phishing-Mails

Der KI-Chatbot WormGPT unterstützt Cyberkriminelle dabei, überaus überzeugende und strategisch gerissene Phishing-Mails zu erstellen.

in Pocket speichern | merken

16. Juli 2023, 10:08 Uhr, Marc Stöckel




(Bild: MIKE CLARKE/AFP via Getty Images)

Mit WormGPT generierte Phishing-Mails könnten schon bald zahlreiche Postfächer überfluten.

Kriminalität in den Niederlanden

Polizei warnt vor KI-g
Kinderpornografie

Den Haag · Obwohl kinderpornografische Bil
Intelligenz erstellt wurden, strafbar sind, nim
Jetzt hat die niederländische Polizei genau d
KI-Hersteller zu Maßnahmen aufgefordert.

KI-generierte Video-Anrufe

masche von Cyber-Kriminellen sei der CEO-Betrug, warnt die
tgeworden als "Hongkong-Bank-Betrug". Dabei handele es
ariante des "Phishing". Allerdings werde kein Link zu einer
e verschickt, sondern KI simuliere Personen und Sprache in
Man sieht realistische Videos." Vermeintliche Vorgesetzte
beiter auffordern, Geld zu überweisen.

ber-Kriminalität sei kein neues Problem, ergänzt die
rin. "KI macht es einfach effektiver."

# Auch IoT bleibt nicht verschont

## Smart-TVs sind primäre Schwachstelle im Smart-Home

4. Juli 2023


Netgear hat gemeinsam mit Bitdefender die Sicherheitsrisiken untersucht, mit denen die heutigen Smart-Homes konfrontiert sind, und was in Zukunft auf vernetzte Heimumgebungen zukommt. Der" IoT Security Landscape Report 2023" basiert auf Bedrohungsdaten, die von 2,6 Millionen Smart-Homes auf der ganzen Welt, die durch Netgear Armor powered by Bitdefender geschützt sind, analysiert wurden. Rund 120 Millionen IoT-Geräte wurden untersucht, die mehr als 3,6 Milliarden Sicherheitsereignisse, Schwachstellen und Angriffsszenarien identifizierten und isolierten, um in der Konsequenz die Sicherheit zu verbessern und so das intelligente Zuhause zu einer sichereren Umgebung zu machen.

# Zeitintensive Gesetzgebungsprozesse

# NIS-Richtlinie

- NIS: Network and Information Security
- NIS Richtline 2016:
  - Nationale Strategien für die Cybersicherheit.
  - Schaffung einer Kooperationsgruppe für die strategische Zusammenarbeit und den Informationsaustausch zwischen den Mitgliedstaaten zu unterstützen.
  - Schaffung eines Netzwerks von Computer-Notfallteams (CSIRTsNetzwerk)
  - Einführung von Sicherheitsanforderungen und Meldepflichten
  - Nennung oder Schaffung nationaler Behörden, zentraler Anlaufstellen und CSIRTs.

# NIS-2-Richtlinie

NIS = Sicherheit von Netz- und Informationssystemen

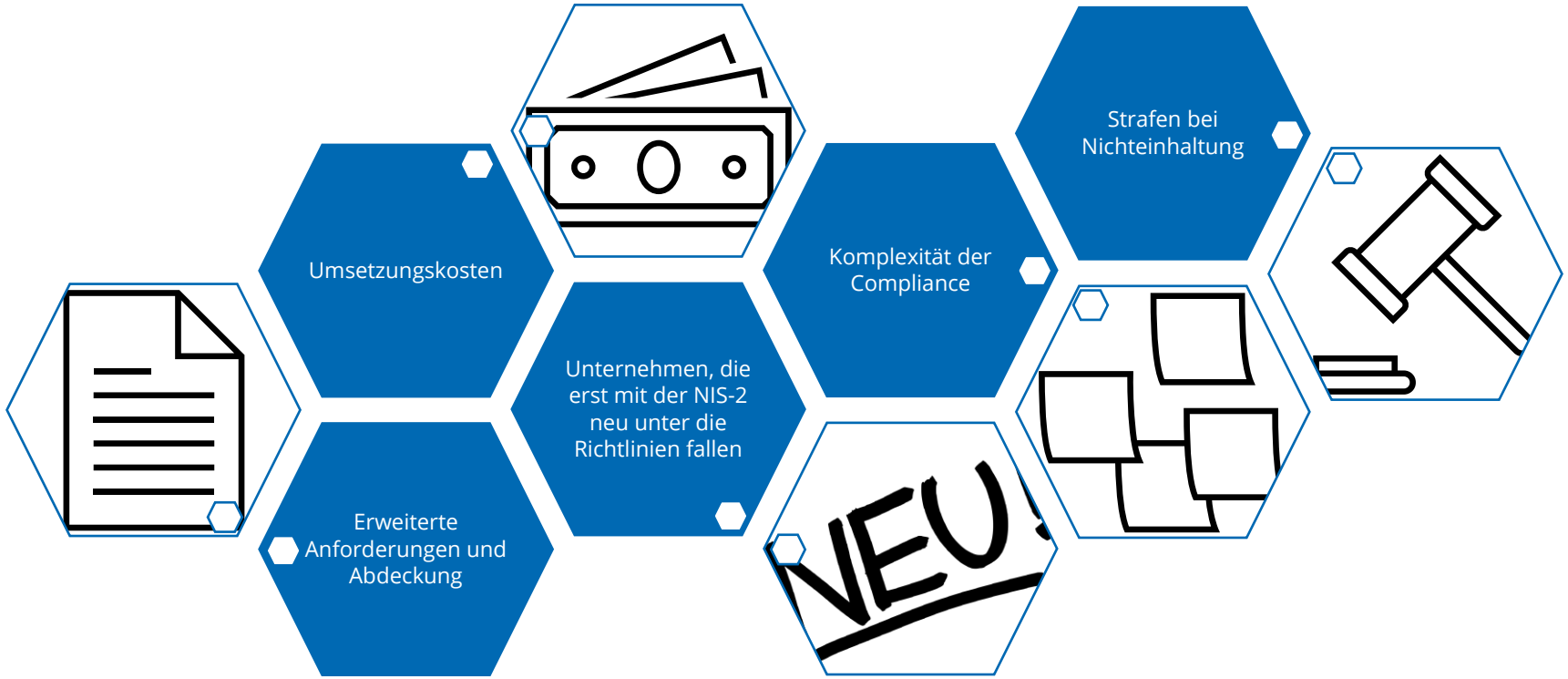

Fast 5,5 Jahre Umsetzungszeit

4 Jahre Umsetzungszeit

# NIS-2-Richtlinie

- NIS-2 muss bis Oktober 2024 umgesetzt werden
- What‘s new?
  - **Erweiterter Anwendungsbereich:** Die Richtlinie erstreckt sich auf eine breitere Palette von Unternehmen und Sektoren, einschließlich Digitaldienstleistern und kritischer Infrastrukturen.
  - **Stärkere Sicherheitsanforderungen:** Die Richtlinie legt strengere Anforderungen an die Sicherheit von Netzwerken und Informationssystemen fest, einschließlich Maßnahmen zur Erkennung von Angriffen (z. B. XDR) und zur Wiederherstellung von Geschäftstätigkeiten nach Cyberangriffen.
  - **Regelmäßige Überprüfungen:** Unternehmen müssen ihre Technologien und Prozesse regelmäßig von unabhängigen Auditoren überprüfen lassen, um sicherzustellen, dass sie den Anforderungen entsprechen.
  - **Erhöhte Meldepflicht:** Unternehmen sind verpflichtet, ernsthafte Sicherheitsvorfälle den nationalen Behörden zu melden.
  - **Strafen bei Nichteinhaltung:** Es werden Sanktionen für Unternehmen eingeführt, die gegen die Sicherheitsanforderungen verstoßen, um die Einhaltung der Richtlinie zu gewährleisten.

# NIS-2-Richtlinie – weitere Herausforderungen



# Industrialisierung von Cybercrime

# Industrialisierung von Cybercrime

- Die Professionalisierung der Cyberkriminalität erreicht 2024 ein neues Niveau der Profitabilität, teilweise durch die Verbreitung von Ransomware-as-a-Service (RaaS).
- Die Anzahl der Opfer von Ransomware-Angriffen hat sich im Vergleich zu 2022 verdoppelt, was zeigt, dass Ransomware immer noch eine der schädlichsten, kostspieligsten und häufigsten Angriffsmethoden im EMEA-Raum ist.
- Es gibt einen klaren Trend zu gezielten Angriffen auf den öffentlichen Sektor und kritische Infrastrukturen, insbesondere im Gesundheits-, Bildungs- und Regierungswesen, aufgrund mangelnder Sicherheitsressourcen in diesen Bereichen.
- Cyberkriminelle nutzen immer aggressivere Ransomware-Methoden, darunter Double-Extortion-Angriffe, bei denen sie sensible Daten verschlüsseln und mit ihrer Veröffentlichung drohen.

# Beispiel: Ransomware-as-a-Service

# Beispiel: Ransomware-as-a-Service

- RaaS ist ein Geschäftsmodell, bei dem Cyberkriminelle die Infrastruktur und die Werkzeuge zur Durchführung von Ransomware-Angriffen als Service anbieten.
- Es ermöglicht auch unerfahrenen oder weniger technisch versierten Kriminellen, Ransomware-Angriffe durchzuführen, da sie die benötigten Tools von einem Anbieter mieten oder kaufen können.


- Die RaaS-Plattformen bieten in der Regel eine benutzerfreundliche Oberfläche, technischen Support und oft auch Kundendienstleistungen für die Verhandlung mit Opfern.

# Beispiel: RaaS als Teamarbeit

Initial Access Broker:

- Sind Kriminelle oder Gruppen, die sich auf den Zugriff auf kompromittierte Systeme oder Netzwerke spezialisieren.
- Sie verkaufen diesen Zugriff an RaaS-Anbieter oder andere Kriminelle, die dann die Ransomware-Angriffe durchführen.

Ransomware Affiliate:

- Personen oder Gruppen, die Ransomware von RaaS-Anbietern mieten oder kaufen, um Angriffe durchzuführen.
- Sie erhalten oft einen Anteil der erpressten Gelder als Provision für ihre Beteiligung an erfolgreichen Angriffen.

# Beispiel: RaaS als Teamarbeit

Data Manager:

- Verantwortlich für die Sammlung und Verwaltung gestohlener Daten während eines Ransomware-Angriffs.
- Sie organisieren und kategorisieren die gestohlenen Daten und spielen oft eine Rolle bei der Verhandlung mit Opfern.

Ransomware Developer:

- Entwickelt und wartet die Ransomware-Software, die für Angriffe verwendet wird.
- Sie sind für die Aktualisierung und Anpassung der Ransomware an neue Sicherheitsmaßnahmen und Technologien verantwortlich.

# Beispiel: RaaS als Teamarbeit

Negotiator:

- Verhandelt im Namen der Angreifer mit den Opfern über das Lösegeld und versucht, die höchstmögliche Zahlung zu erzielen.

Chaser:

- Verfolgt und überwacht die Zahlungen von Opfern nach einem Ransomware-Angriff.
- Stellt sicher, dass die Opfer das Lösegeld bezahlen und unterstützt bei Problemen mit der Zahlungsabwicklung.

Accountant:

- Verwaltet die finanziellen Aspekte des RaaS-Geschäfts, einschließlich der Aufzeichnung von Einnahmen und Ausgaben sowie der Verteilung von Gewinnen an beteiligte Parteien.

# Faktor Mensch

# Faktor Mensch

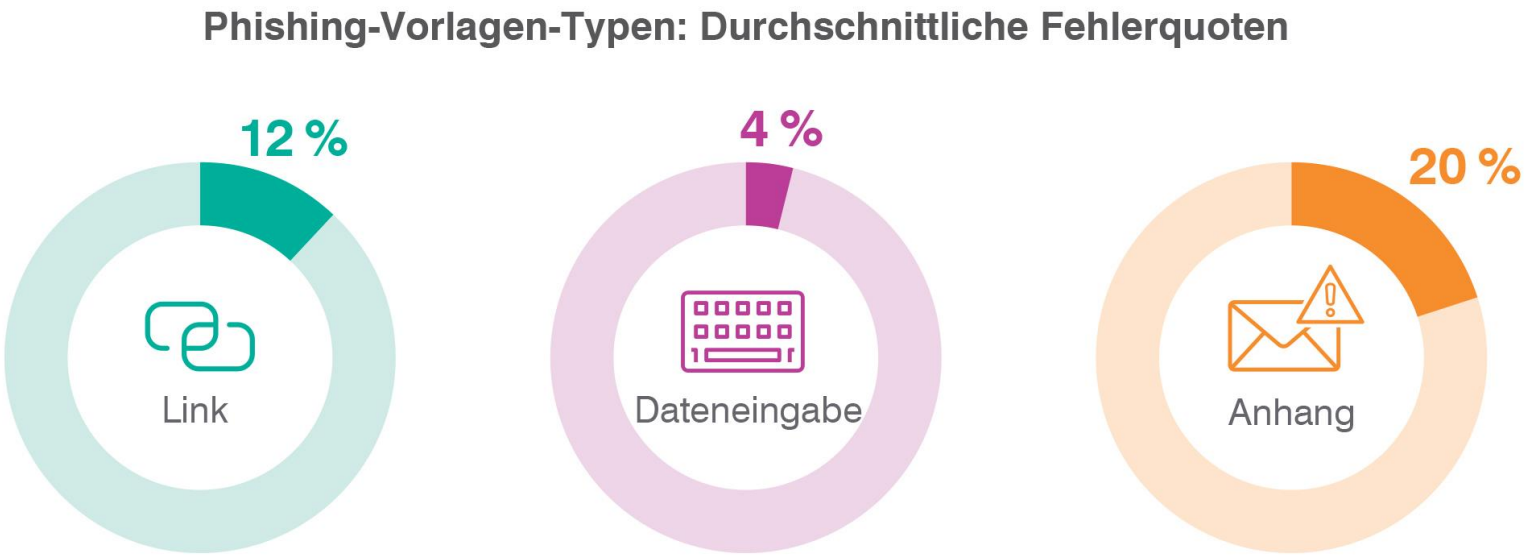
- Die Wirksamkeit unserer Sicherheitsmaßnahmen hängt stark von unserer Fähigkeit ab, den menschlichen Faktor zu berücksichtigen, da Cyberkriminelle zunehmend auf Social Engineering setzen, um ihre Erfolgschancen zu maximieren.
- Schätzungen zeigen, dass der Faktor Mensch in bis zu 74 Prozent aller Datenschutzverletzungen eine Rolle spielt, und dieser Anteil wird laut Prognosen weiter steigen.
- Die Professionalisierung der Cyberkriminalität und der Einsatz von Künstlicher Intelligenz ermöglichen es Cyberkriminellen, überzeugende und realitätsnahe Social-Engineering-Angriffe durchzuführen, was es schwieriger macht, zwischen echten und trügerischen Nachrichten zu unterscheiden.

# Frage!

*Denken Sie an die Cybercrimephänomene, die Sie kennengelernt haben.*

*Welche der Phänomene nutzen den Menschen als Schwachstelle?*

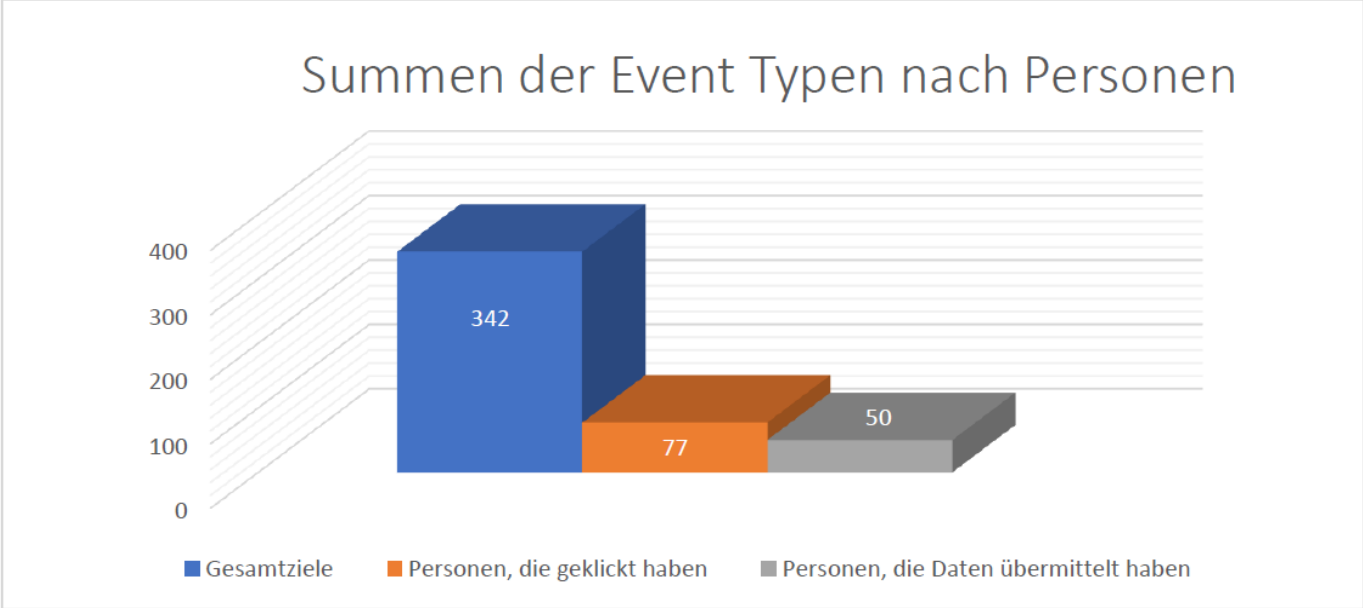
# Beispiel Phishing




Quelle: Umfrage von Proofpoint

# Phishing – eigenes Beispiel

- Phishing-Angriff auf ein Unternehmen mit 342 Empfängern
- 77 Personen klickten auf den Link in der E-Mail (23 %)
- 50 Personen übermittelten ihren Nutzernamen und Passwort (15 %)



# DER FAKTOR MENSCH 2017

Böswillige E-Mail-Angriffe nutzen Menschen aus – und nicht Code.

Dies sind die Techniken, mit denen Cyber-kriminelle im Jahr 2016 am häufigsten Benutzer zum Öffnen böswilliger E-Mails und Social-Media-Beiträge verleiteten.

## BEC-ANGRIFFE (BUSINESS EMAIL COMPROMISE) NEHMEN ZU

Das Volumen der BEC-Nachrichten stieg von 1% im Jahr 2015 auf **42% zum Ende 2016**.


## SOCIAL-MEDIA-KONTO-PHISHING WIRD IMMER BELIEBTER

Social-Media-Phishing nahm im Jahr 2016 **um 150%** zu.

## MALWARE-KATEGORIEN VARIIEREN IHRE VERBREITUNG VON TAG ZU TAG

Ransomware-Kampagnen werden bevorzugt von **Dienstag bis Donnerstag** durchgeführt.


**Donnerstag** durchgeführt.

## ZEIT IST GELD

**87% aller Klicks auf böswillige URLs** finden innerhalb der ersten 24 Stunden nach Eingang statt.

Fast 50% der Klicks erfolgen innerhalb einer Stunde.

25% aller Klicks erfolgen innerhalb von nur 10 Minuten.

## ANGRIFFSSPITZE IST UM DIE MITTAGSZEIT

**Klicks erreichen ihren Höchstwert 4 bis 5 Stunden** nach Arbeitsbeginn, also um die Mittagszeit.

## BETRÜGERISCHE MOBILGERÄTE-APPS LEGEN BENUTZER HEREIN

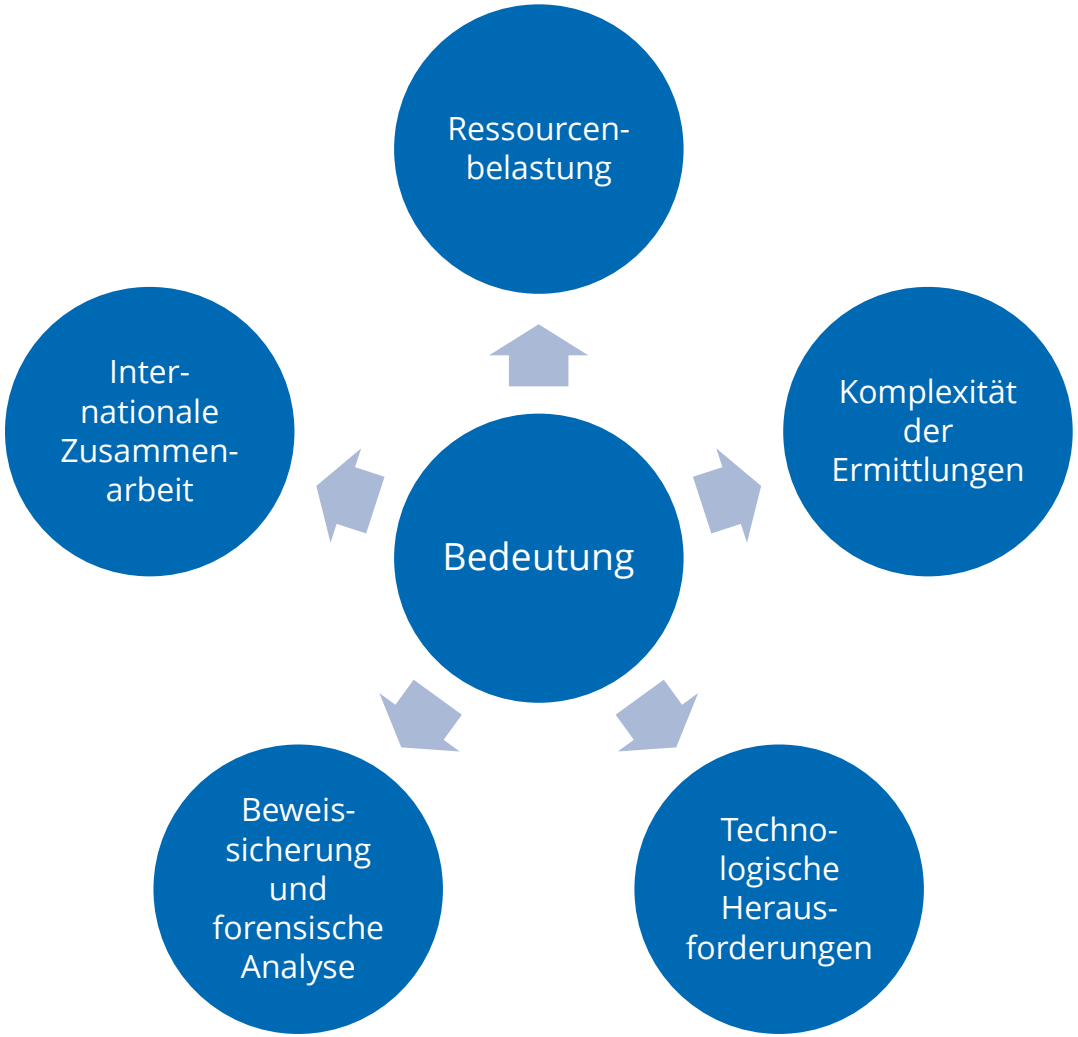
Böswillige Apps **missbrauchen Marken und nutzen irreführende Namen**, um Benutzer zum Download der Malware zu verleiten.

## MEHR MOBILTELEFONE BEDEUTEN MEHR RISIKEN

42% aller Klicks auf böswillige URLs erfolgen auf Mobilgeräten – **zweimal mehr als die 20% im Vorjahr**.

# Was bedeutet das für uns/euch?

# Bedeutung für Ermittlungsbehörden und Ermittler



# Bedeutung für Ermittlungsbehörden und Ermittler

Ressourcenbelastung:

- Mangel an ausgebildeten Fachkräften für Cyberkriminalitätsermittlungen
- Begrenzte finanzielle Mittel für die Beschaffung von Technologie und Ausrüstung
- Hohe Arbeitsbelastung aufgrund der Vielzahl von Cyberangriffen
- Notwendigkeit, ständig aktualisierte Technologie und Tools bereitzustellen

# Bedeutung für Ermittlungsbehörden und Ermittler

Komplexität der Ermittlungen:

- Notwendigkeit internationaler Zusammenarbeit bei grenzüberschreitenden Angriffen
- Schwierigkeit, komplexe technische Taktiken von Cyberkriminellen zu verstehen
- Herausforderungen bei der Überwachung und Verfolgung von anonymen Tätern im Internet
- Notwendigkeit, verschiedene Rechtsprechungen und Gesetze zu berücksichtigen

# Bedeutung für Ermittlungsbehörden und Ermittler

Technologische Herausforderungen:

- Schneller technologischer Fortschritt erfordert kontinuierliche Weiterbildung der Ermittler
- Mangel an Zugang zu spezialisierter Technologie und forensischen Tools
- Herausforderungen bei der Identifizierung und Verfolgung von verschlüsselten Kommunikationskanälen
- Schwierigkeiten bei der Bekämpfung von Angriffen mit Hilfe von KI und automatisierten Tools

# Bedeutung für Ermittlungsbehörden und Ermittler

Beweissicherung und forensische Analyse:

- Notwendigkeit, digitale Beweise sicher zu sammeln und zu speichern, um ihre Integrität zu gewährleisten
- Herausforderungen bei der forensischen Analyse großer Datenmengen und komplexer IT-Systeme
- Neue Sicherungs- und Analysemethoden
- Sicherstellung der Verwendbarkeit digitaler Beweise vor Gericht und Schutz vor Manipulation oder Fälschung
- Notwendigkeit, forensische Untersuchungen schnell und effizient durchzuführen, um die Ermittlungen nicht zu verzögern

# Bedeutung für Ermittlungsbehörden und Ermittler

Internationale Zusammenarbeit:

- Unterschiedliche Rechtssysteme und Gesetze in verschiedenen Ländern erschweren die Zusammenarbeit
- Sprach- und kulturelle Barrieren können die Kommunikation und den Informationsaustausch behindern
- Notwendigkeit, Vertrauen und Kooperationsmechanismen zwischen den Strafverfolgungsbehörden aufzubauen
- Herausforderungen bei der Koordinierung von Ermittlungen über verschiedene Zeitzonen und geografische Gebiete hinweg

# 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