HOCHSCHULE MITTWEIDA
University of Applied Sciences

Rechtsgrundlagen Cybercrime

Hacktivismus und Identität

Prof. Dr. Dirk Labudde

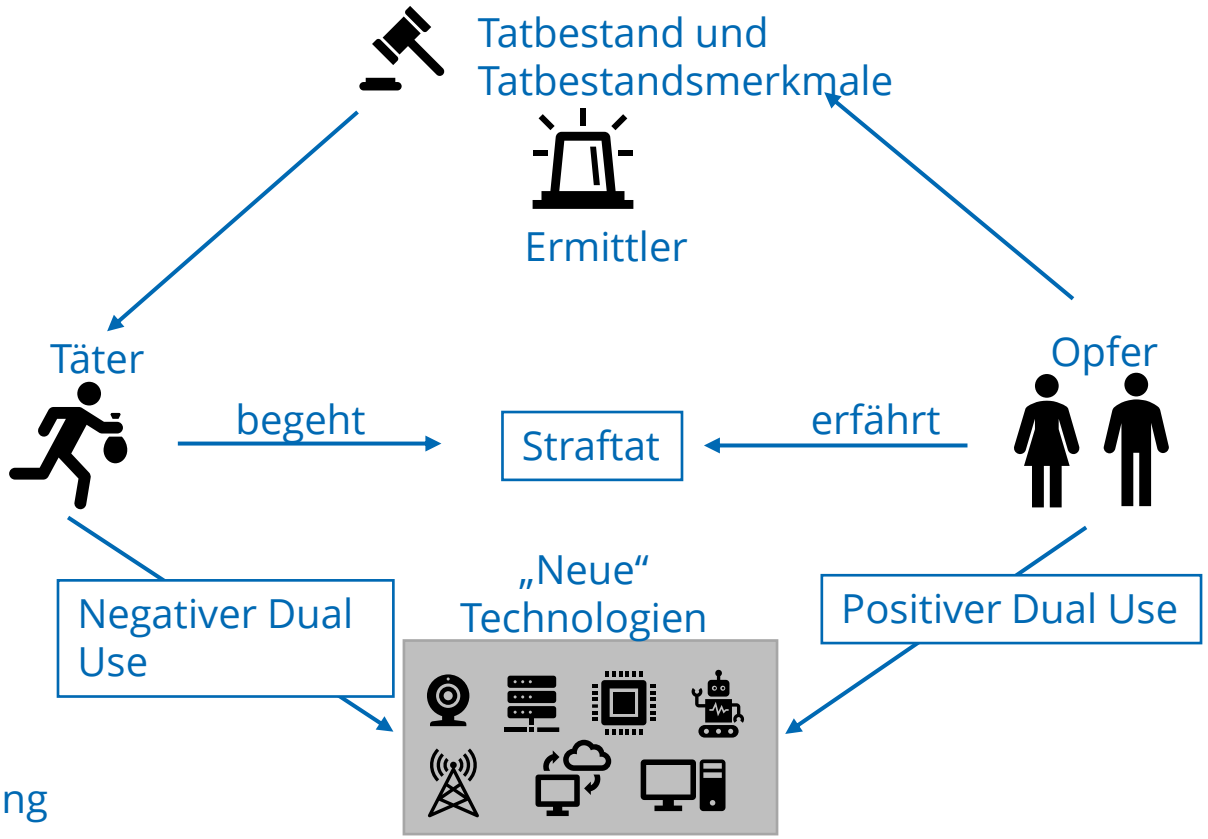
Bundeskriminalamt

Unser Alltag – Ein Leben in der Digitalen Welt – und deren Folgen

sexting

cyber boxxing

Cyber-Erpressung



Cybercrime

CYBERSTALKING

cybermobbing

cybergrooming

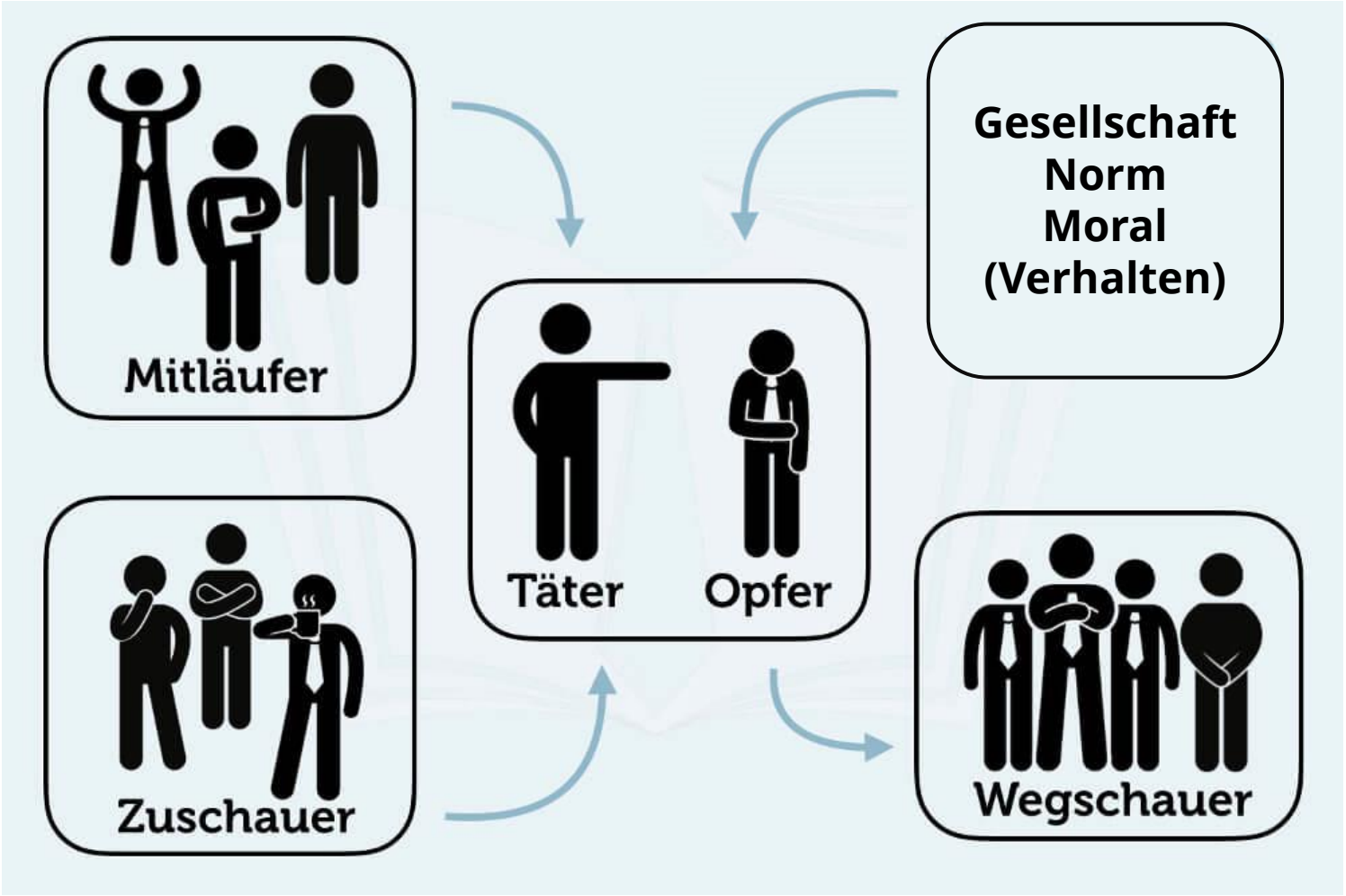
Wir haben es immer mit Menschen zutun!

Hacker, Black-Had, White-Had, Cyber-Terroristen

Strafverfolgungsbehörden, Interpol, CERT

CERT Bund **C**omputer **E**mergency **R**esponse **T**eam

Profiling


Mitläufer
Täter
Opfer
Gesellschaft
Norm
Moral
(Verhalten)
Zuschauer
Wegschauer

Den typischen Cyber-Kriminellen gibt es nicht

Mögliche Einteilung A:

- externe Hacker
- Eigene Mitarbeiter im Unternehmen
- Gruppen im Sinne der organisierten Kriminalität
- Cyber-Terroristen
- Staaten als Akteure von Cybercrime-Attacken

Mögliche Einteilung B:

- Cyber-Aktivisten (Hacktivisten)
- Cyber-Kriminelle
- Wirtschaftsspione im Cyber-Raum
- staatliche Nachrichtendienste im Cyber-Raum
- staatliche Akteure im Cyber-War (Militär)
- Cyber-Terroristen
- Skript Kiddies

Hacker

- Der Begriff Hacker hat eine Metamorphose in seiner Begrifflichkeit durchlebt. Waren am Anfang damit besondere Tüftler gemeint, so wird er heute im Zusammenhang mit Cyberverbrechen benutzt.
- 1960er Begriff Hacker für ein Team von Studenten (MIT)
  - Auseinanderbauen von Maschinen
  - Umkonstruktion der Maschinen
  - Ziel: haptischen Gefühl, Leistungssteigerung, Verständnis
- Computerexperten mit fortgeschrittenen Kenntnissen in Informationstechnologie
- Fähigkeit, Computersysteme zu analysieren, zu manipulieren und zu durchdringen

Hacker

White-Hat Hacker

- Ethik und Legalität im Vordergrund
- Verwendung von Hacking-Fähigkeiten für gute Zwecke wie Sicherheitstests und Schwachstellenanalysen
- Arbeitet oft in Sicherheitsunternehmen oder als Sicherheitsberater
- Enge Zusammenarbeit mit Unternehmen, Regierungsbehörden und Organisationen, um Schwachstellen zu identifizieren und zu beheben
- Entwickelt und verbessert Sicherheitsmaßnahmen und Schutzmechanismen
- Einhaltung ethischer Richtlinien und Gesetze

Black-Hat Hacker

- Ethik und Legalität weniger wichtig, primäres Ziel ist persönlicher Gewinn oder Schaden
- Nutzt Hacking-Fähigkeiten für kriminelle Aktivitäten wie Datendiebstahl, Betrug oder Sabotage
- Operiert oft im Verborgenen, um illegale Aktivitäten zu verschleiern
- Kann Teil von kriminellen Organisationen oder Hackergruppen sein
- Verletzt Gesetze und ethische Standards, um persönliche oder finanzielle Ziele zu erreichen
- Häufiges Ziel von Strafverfolgungsbehörden und Cybersecurity-Maßnahmen

Hacktivismus

Hacktivismus ist Aktivismus, der Techniken des Hackings verwendet, um politische oder soziale Ziele zu fördern. Hacktivisten setzen digitale Angriffe ein, um Missstände aufzuzeigen oder politische Botschaften zu verbreiten.

Arten von Hacktivisten

a. **Anonymous:** Diese Hackerbewegung ist aktuell in den Medien die bekannteste. Anonymous steht für ein freies Internet und einen freien Informationsfluss. Sie veröffentlicht Daten, die von vielen lieber verheimlicht werden. Mit ihren Methoden beeinflussen sie auch politische Bewegungen.
b. **Cyberoccupiers:** In dieser Bewegung findet man die wahren Aktivisten. Sie nutzen hauptsächlich das Internet und da vor allem soziale Netzwerke, um Beziehungen aufzubauen und Informationen und Propaganda zu streuen. Oft leisten Sie damit auch politischen Widerstand gegen Machthaber. Sie sehen ihre Arbeit als einen Beitrag zur Stärkung und Wahrung der Demokratie.
c. **Cyberwarriors:** Unter dieser Gruppierung versteht man in erster Linie Patrioten, die sich als ‚Cyber-Armee' zusammenschließen. Sie verunstalten Webseiten und kämpfen mit ‚Cyber-Waffen' gegen andere Gruppierungen, die nicht ihrer Meinung sind.

Anonymous

- Wenn sie sich ein Ziel gesetzt haben, können sie mit gezielten Cyber-Attacken Unternehmen tagelang blockieren und den Betrieb nachhaltig stören.
- Aktuell kann man die Bedrohung bzw. das Bedrohungspotenzial durch sie nur begrenzt bewerten, da es oft an einem genauen gemeinsamen Ziel fehlt.

- **Aber - Auffanglager für Skript-Kiddies und Personen, die unter dem Deckmantel der Anonymität, Anliegen der Gruppe unter der Zuhilfenahme von Cyber-Angriffen verwirklichen wollen.**
- Die Motive können unterschiedlichster Natur sein und bringen die gesellschaftlichen Anliegen einer Cyber-Generation zum Ausdruck!

Die Erstellung eines Täterprofils im Bereich Cybercrime

- Delikte
- Einzeltäter und Gruppentäter
- Motive
- Art der Angriffe
- Angriffsorte

Die Erstellung eines Täterprofils im Bereich Cybercrime

- Die Kriminologie, im Speziellen die Kriminalpsychologie, beschäftigt sich seit Jahrzehnten mit der Erstellung von Täterprofilen.
- Ursprung: Absicht, Gewaltverbrecher besser verstehen und auffinden zu können.

- Steht das Auffinden von Cyber-Kriminellen im Fokus, müssen unterschiedliche Facetten betrachtet werden.
- Frage:
  - Was versteht man konkret unter Cyber-Kriminalität
  - Wie unterscheiden sich die unterschiedlichen Angriffsarten, sodass ein Profil von Tätern erstellt werden kann?

Die Erstellung eines Täterprofils im Bereich Cybercrime

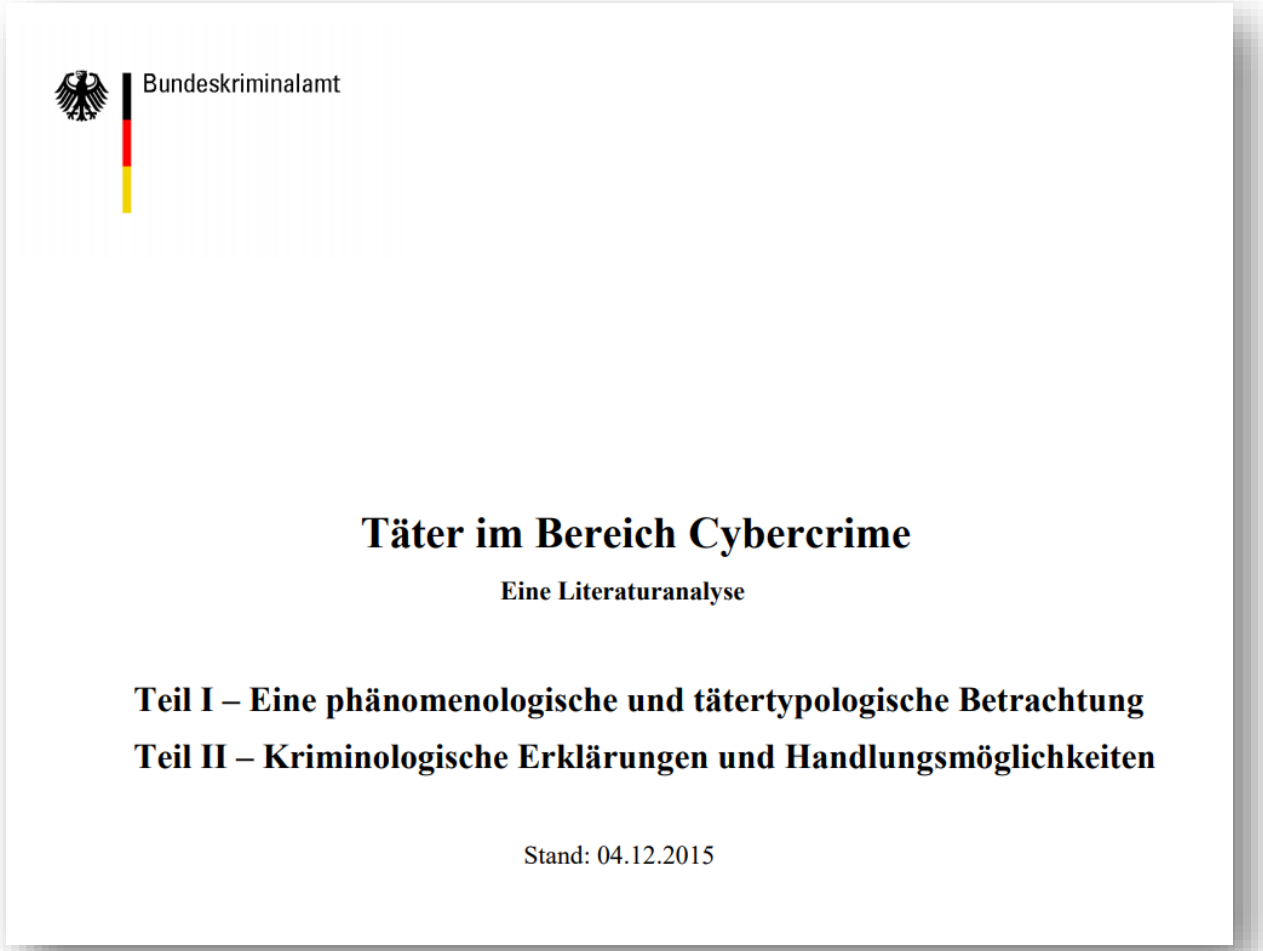
Ansätze

- Kirwan und Power (2013),
- Bässmann (2015)

Kirwan, G., und A. Power. 2011. *Cybercrime: The psychology of online offenders.* https://doi.org/10.1017/CBO9780511843846.
Kirwan, G., und A. Power. 2013. *Cybercrime: The psychology of online offenders*. Cambridge University Press. https://doi.org/10.1017/CBO9780511843846.

Bässmann, J. 2015. *Täter Im Bereich Cybercrime.* Wiesbaden. https://cdn.netzpolitik.org/wp-upload/BKA-Studie_Taeter-im-Bereich-Cybercrime_Eine-Literaturanalyse.pdf,

Die Erstellung eines Täterprofils im Bereich Cybercrime



Bundeskriminalamt

Täter im Bereich Cybercrime

Eine Literaturanalyse

Teil I – Eine phänomenologische und tätertypologische Betrachtung

Teil II – Kriminologische Erklärungen und Handlungsmöglichkeiten

Stand: 04.12.2015

Die Erstellung eines Täterprofils im Bereich Cybercrime

Das Profil ist immer individuell vom Delikt, Motiv und von der aktuellen Technologieentwicklung abhängig.

War noch vor einigen Jahren der typische Cyber-Kriminelle zwischen **30 und 40** Jahre alt, so stellen aktuell die **14- bis 30-Jährigen** den Großteil.

- mehr Männer als Frauen (Männer generell häufiger kriminell)
- Frauenanteil bis zu 24 %.
- Ausbildungsgrad der Täter – durchschnittlich
- Keine hochqualifizierte Ausbildung im IT Bereich

Die Erstellung eines Täterprofils im Bereich Cybercrime

Familiären Hintergrund der Täter

Cyber-Kriminellen - benachteiligt bzw. problembelastet
oder aus dysfunktionellen Familien (z. B. alleinerziehend,
Scheidung, Alkoholabhängigkeit, Adoptionen etc.)

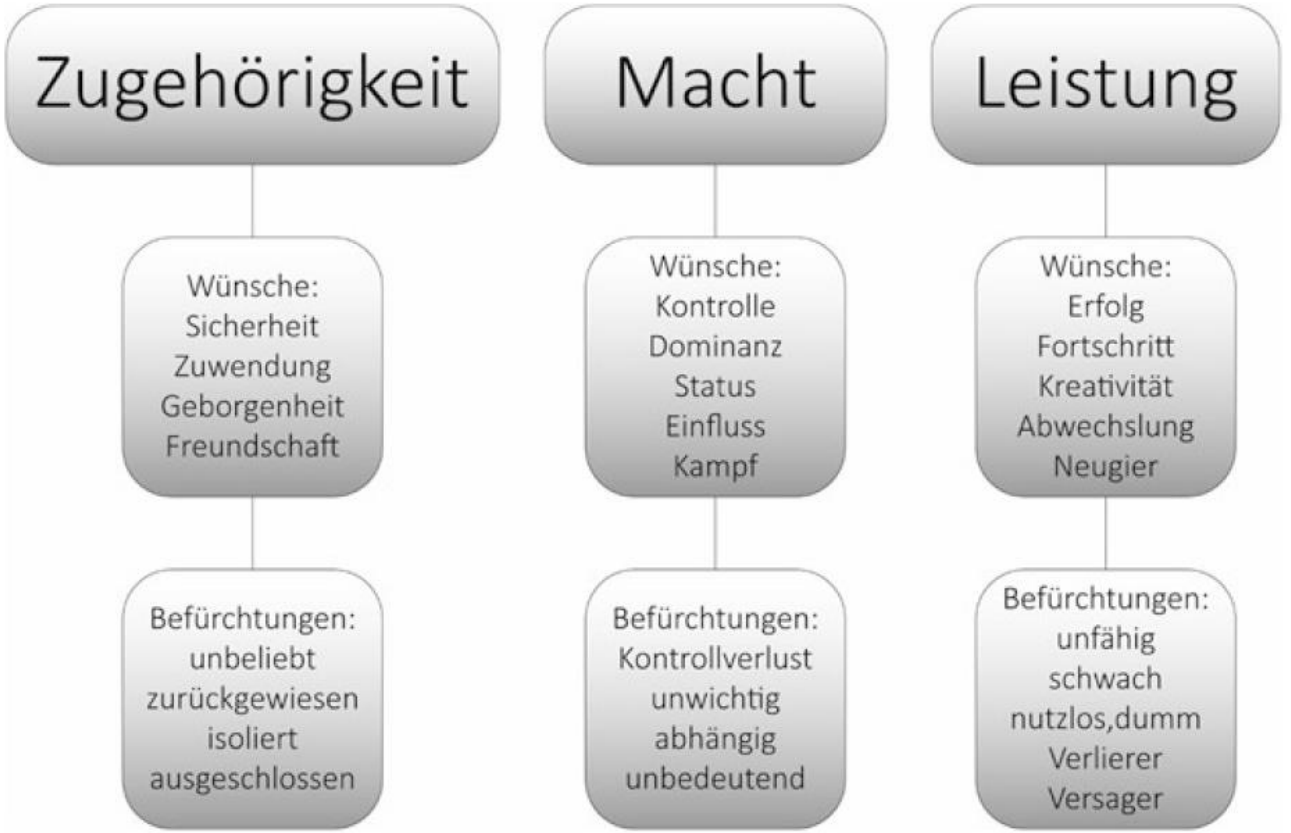
- finanziellen Mittelschicht verortet
- in einer eigenen Community z. B. Hackerforen gut integriert
- Selten Kommunikatoren
- Austausch findet ausschließlich in der Community statt
- keine Spezifizierung innerhalb der Cybercrime-Delikte

Die Erstellung eines Täterprofils im Bereich Cybercrime

Differenzierung der Täter nach folgender Typologie

Art der Differenzierung	Beschreibung	Beispiel
Delikt	In der Differenzierung nach Delikten geht es um eine strafrechtliche Unterscheidung. Man betrachtet den juristischen Sachverhalt.	Das Durchführen einen DDoS-Attacke, ist im Sinne des jeweilig zutreffenden Paragraphen des Strafgesetzbuches strafbar.
Formation	In welcher Gruppierung die Tater auftreten. Einzeltäter, Gruppentäter oder Staaten.	Russische und chinesische Betrüger schließen sich zusammen und stehlen online Geld von einer Bank in Australien.
Motiv	Mit welchem Motiv begründet der Täter die Tat. Motive sind extrinsischer (z. B. wirtschaftliche, terroristische) oder intrinsischer (z. B. persönlich, Rache) Natur.	Ein Mitarbeiter stiehlt unternehmensinterne Daten vom Laufwerk eines Vorgesetzten und spielt diese der Konkurrenz zu.
Art des Angriffs	Ungerichtete, gezielete und skalpellartige Angriffe	Ungerichteter Angriff: z. B. ein SPAM-E-Mail erhalten; Gezielter Angriff: z. B. einen Konkurrenten ausspionieren; Skalpellartiger Angnff: z. B. massive Schädigung einer IT-Infrastruktur.
Angriffsort	Klärt von wo aus der Angriff organisiert wird. Inland oder Ausland.	Österreichische User laden sich illegal Videos mit kinderpornografischen Inhalt auf ihren PC.

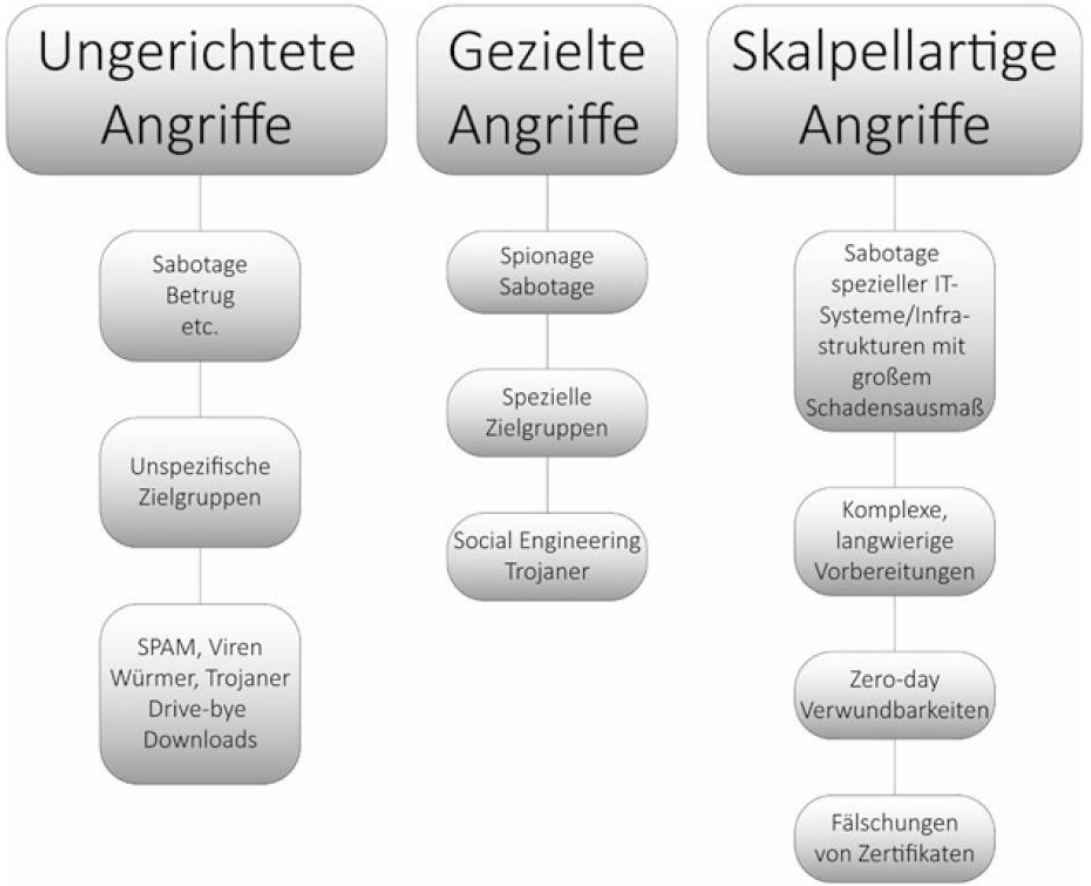
Die Erstellung eines Täterprofils im Bereich Cybercrime



Grundmotive des Menschen nach McClelland

Die Erstellung eines Täterprofils im Bereich Cybercrime

Art des Angriffs



Cybercrime im engeren Sinn

Die Erstellung eines Täterprofils im Bereich Cybercrime

Angriffsort woher kommen Angriffe

Inland oder aus dem Ausland

- die meisten Angriffe (Angriffe auf Unternehmensinfrastrukturen) stammen aus dem Ausland

Genaue Analysen über die Herkunftsländer der Opfer gibt es wenig. Gründe dafür gibt es viele.
Einer der wichtigsten Gründe ist, die Dunkelfeldziffer der Opfer sehr hoch ist.

Die Perspektive der Opfer

Ausgangslage

Der Schwerpunkt von Forschung und Entwicklung in diesem Bereich fokussiert auf den **Schutz kritischer Infrastrukturen** und Unternehmensinfrastrukturen. Es herrscht die Meinung vor, dass jeder Opfer von Cybercrime werden kann, sodass eine Differenzierung nicht nötig ist.

aber

je nach Art des Delikts sind auch die Opfer unterschiedlich

Die Perspektive der Opfer

Opfertypen:

- Staaten,
- Firmen
- Privatpersonen
- Betreiber kritischer Infrastrukturen (NIS-Richtlinie)

Richtlinie (EU) 2016/1148 des europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, Abl L 2016/194, 1.

Die Perspektive der Opfer

Opferzahlen
- Anzeigeverhalten
- Falschzuordnung von Straftaten

Hellfeld versus Dunkelfeld In der Kriminalität unterscheidet man zwischen Hellfeld- und Dunkelfeldziffer. Die Hellfeldziffer beschreibt jene Kenngröße an Kriminalitätsdelikten, die als Straftat der öffentlichen Hand bekannt sind. Die Dunkelfeldziffer hingegen beschreibt jene Zahl an Straftaten, die es gibt, die aber
nie zur Anzeige gebracht wurden.

Wichtig die Rolle von Regierungen und der Gesellschaft
NIS-RL

Zusammenfassung

In Bezug auf das Phänomen Cybercrime befinden wir uns in einer Multistakeholder-Landschaft
Man unterscheidet dabei:

- *Täter*
  Diese können als Einzelpersonen oder als Gruppe auftreten. Die Vorgehensweise der Täter kann darüber hinaus nach den Kategorien Deliktsart, Motivation (intrinsisch versus extrinsisch) und Angriffsort differenziert werden. Zusätzlich hat das deutsche BSI die technischen Arten des Cyber-Angriffs kategorisiert, so können Täter ungerichtet (also ohne ein bestimmtes Opfer im Fokus zu haben), zielgerichtet (auf ein konkretes Opfer ausgerichtet) oder skalpellartig (ein konkretes Opfer mit unterschiedlichen Methoden infiltrieren) vorgehen.
- *Opfer* kann im Cyberspace grundsätzlich jeder werden. Man unterscheidet dabei unter Privatpersonen, Unternehmen und kritische Infrastrukturen.
- *Weitere Akteure in der Cyberwelt* sind die Exekutive, Strafverfolgung, Betreiber, Government, CERTs, Anbieter von Softwarelösungen, Anbieter von IT-Security Produkten und viele mehr.

Cybercrime

Variante 1: Cybercrime im engeren Sinn (Core Cybercrime bzw. Cyberdependent Crime)
Unter diese Definition fallen alle Delikte, die es in keiner Variante offline gibt. Diese Kategorie von Cybercrime umfasst die Verletzung der Vertraulichkeit, Integrität und Verfügbarkeit von Netzwerken sowie von Geräten, Daten und Services in diesen Netzwerken. Dazu zählt Hacking, Cyber-Vandalismus, Verbreitung von Viren etc.

Cybercrime

Variante 2: Cybercrime im weiteren Sinn (Non-cyberspecific Cybercrime bzw. Cyberenabled Crime)
Delikte, die unter diese Kategorie fallen, können auch offline existieren. Dazu zählen Delikte, wie z. B. Kreditkartenmissbrauch, Informationsdiebstahl, Geldwäsche, Vergehen gegen das Urheberrecht, Cyberstalking sowie die Nutzung, Verbreitung und Zurverfügungstellung kinderpornografischer Inhalte usw (McGuire und Dowling 2013).

McGuire und Dowling 2013

Cybercrime

Variante 3: Verschleierung der Identität
Dies betrifft Täter, die sich einen Online-Avatar zulegen, und die diese Anonymität dazu verwenden, kriminell zu handeln, bzw. Täter, die sich gestohlener Identitäten oder Fake-Identities bedienen (Kirwan und Power 2013). Dazu zählen Delikte, wie z. B. die Verbreitung von nationalsozialistischem Gedankengut in den Sozialen Medien.

Kirwan und Power 2013 - https://doi.org/10.1017/CBO9780511843846

Cybercrime

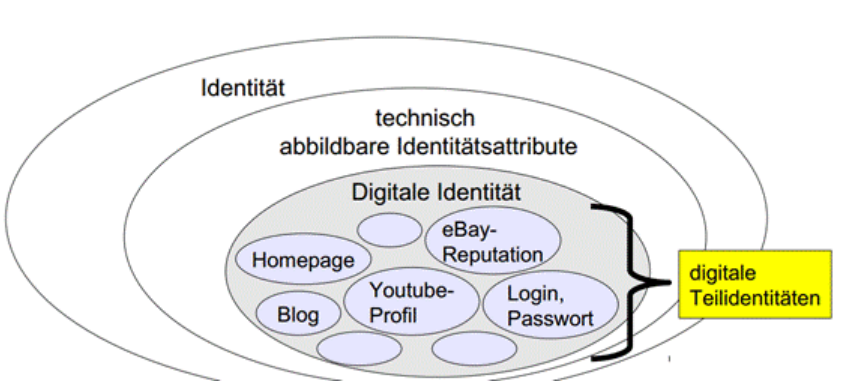
Avatar *„Ein Avatar (Substantiv, maskulin; der Avatar) ist eine künstliche Person oder eine Grafikfigur, die einem Internetbenutzer in der virtuellen Welt zugeordnet wird, beispielsweise in einem Computerspiel. Bei einem Instant Messenger, insbesondere beim alten AOL-Dienst, sprach man von einem Buddy Icon („Kumpel-Symbol“). […] Das Wort leitet sich aus dem Sanskrit ab. Dort bedeutet Avatāra „Abstieg“, was sich auf das Herabsteigen einer Gottheit in irdische Sphären bezieht. Der Begriff wird im Hinduismus hauptsächlich für die Inkarnationen Vishnus verwendet.*“ (Wikipedia)

Unsere Identität – unsere Daten

Identität ist ein lebenslanger Prozess und zeigt sich in Auftreten, Mimik, Gestik, Sprache und körperlichen Stärken und Schwächen und natürlich im inneren Bild / Selbstbild, Selbstgefühl und Glauben an sich, etc.

Teilabbildung im Netz

Unsere Identität(en)

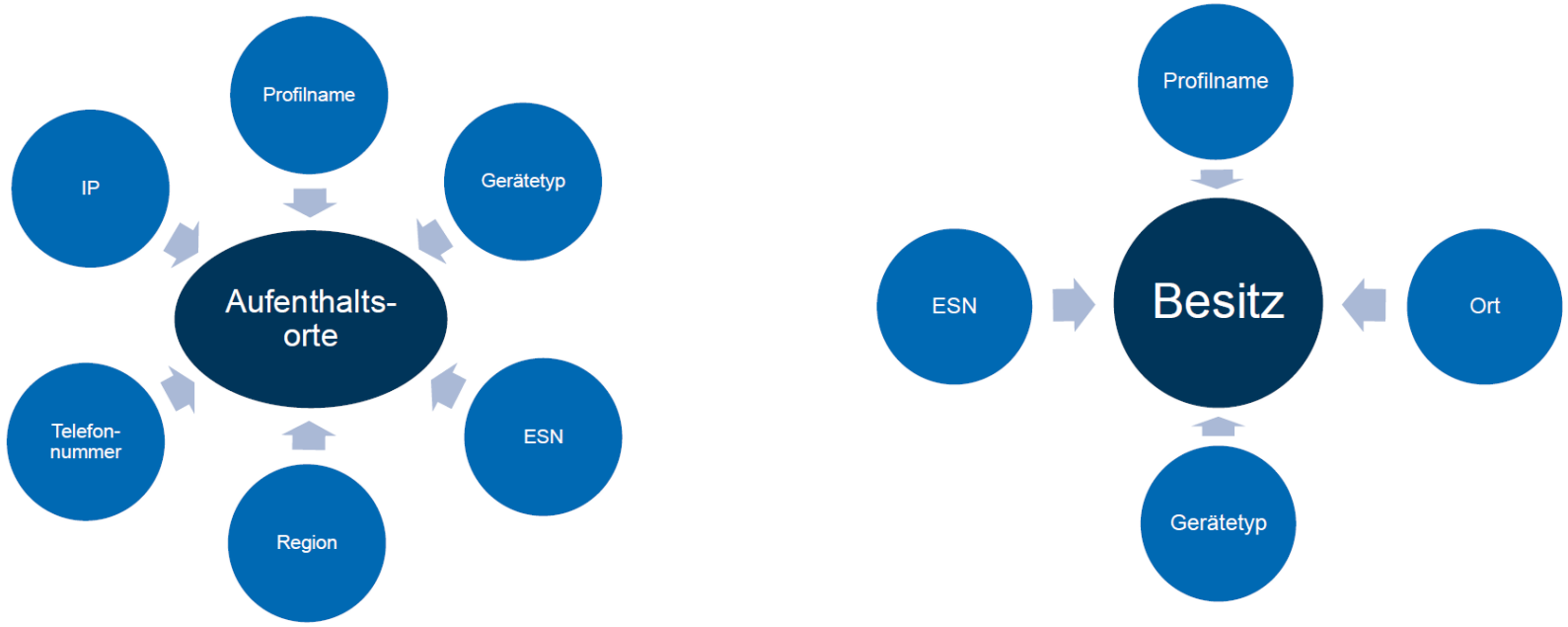


Digitale Teilidentitäten

Identitätsdiebstahl

- Die illegale Erfassung und Nutzung persönlicher Identifikationsdaten einer Person durch eine andere Partei
- Beinhaltet das Sammeln sensibler Informationen wie Namen, Geburtsdaten, Sozialversicherungsnummern, Kreditkarteninformationen usw.
- Kann durch verschiedene Methoden erfolgen, darunter Phishing, Malware, Social Engineering oder den Diebstahl physischer Dokumente
- Zweck ist oft finanzieller Betrug, Identitätsmissbrauch oder Zugriff auf vertrauliche Informationen
- Kann zu schwerwiegenden finanziellen Verlusten, rechtlichen Problemen und persönlichen Belastungen für das Opfer führen
- Erfordert oft umfangreiche Maßnahmen zur Wiederherstellung der Identität und zur Absicherung persönlicher Informationen

Profiling und Identität



esn: eindeutiges Zuordnungsmerkmal eines Gerätes

Unsere Studie

Daten – Information – Wissen

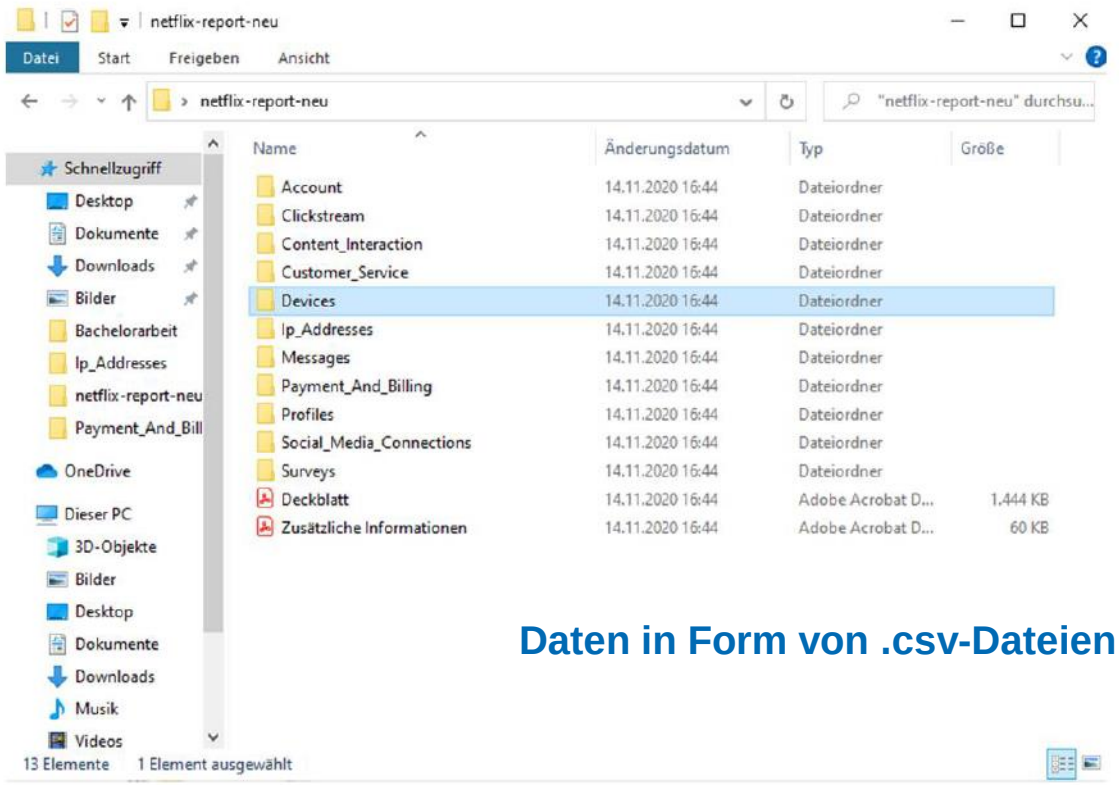
Stellen wir uns vor, jemand hat Ihren **Netflix – Account „erworben“.**

- **Kein Problem, habe meine Kreditkarte und Zugang geändert!**
- **Alles unter Kontrolle**

Er (der Jemand) besitzt jetzt deine Daten!

Zur Kontrolle fordern Sie ihre Daten von Netflix an!

300-seitige Studie zu Daten aus Netflix, Amazon, …



Daten in Form von .csv-Dateien und Textdokumenten

Nur Auszüge

- Allgemeine Informationen über den Kontoinhaber, z.B.
  - Name
  - E-Mail-Adresse
  - Telefonnummer
  - Verknüpfungen zu E-Mail, SMS, Whatsapp
  - …
- Abonnementüberblick

- IndicatedPreferences
  - Ausgewählte Serien und Filme bei erster Nutzung des Profils
- InteractiveTitles
  - Einzelheiten zu den getroffenen Auswahlen bei interaktiven Serien und Filmen
- MyList
  - Watchlist

- Informationen zu der Navigation durch die Netflix-Webseite
- Quelle (Browser, Fernseher, Android, IOS)
- Datum und Uhrzeit des Zugriffs
  - Nur die Informationen der letzten 5 Monate verfügbar

- PlaybackRelatedEvents
  - Einzelheiten zu der Wiedergabesitzung einer Serie oder eines Filmes
- Raitings
  - Abgegebene Serien- und Filmbewertungen
- SearchHistory
  - Suchverlauf und gewohnheitsbezogene Empfehlungen
- ViewingActivity
  - Angeschaute Serien und Filme

Nur Auszüge

- Angaben zu den Geräten, welche mit dem Konto verbunden sind

profileName	esn	deviceType	acctFirstPlaybackDate	acctLastPlaybackDate	acctFirstPlaybackDateF	acctLastPlaybac
	NFUWA-001-99	Netflix Windows App - (	2018-11-14 19:07:19.5	2020-11-13 18:38:52.6	2018-11-14 19:07:19.5	2020-11-13 18:
	NFCDFF-02-G1F	Firefox PC (Cadmium)	2020-01-09 18:59:18.9	2020-11-13 16:22:48.4	2020-01-09 18:59:53.9	2020-11-13 14:
	WWW-BROWSE	Netflix WWW-BROWSER UNSUPPORTED BROWSER				
	NFAPPL-02-IPHC	Apple iPhone 6s	2019-08-27 18:14:17.2	2020-11-12 17:43:12.3	2019-08-27 18:14:17.2	2020-11-12 17:
	NFCDFF-02-F9T(	Firefox PC (Cadmium)	2019-03-28 15:29:38.4	2020-11-09 22:47:40.4	2019-03-28 15:29:38.4	2020-11-09 21:

- Angaben zu den IP-Adressen der zum Streaming benutzten Geräte

	A	B	C	D	E	F	G
1	esn	country	localizedDeviceDescription	deviceDescription	ip	regionCodeDisplayName	ts
2	NFUWA-001-9944250F98445F488	DE	Netflix Windows App - Cadr	Netflix Windows App - Cadn	2003:d3	Bavaria	13.11.2020 18:22
3	NFUWA-001-9944250F98445F488	DE	Netflix Windows App - Cadr	Netflix Windows App - Cadn	79.212.4	Bavaria	13.11.2020 13:59
4	NFUWA-001-9944250F98445F488	DE	Netflix Windows App - Cadr	Netflix Windows App - Cadn	2003:d3	Bavaria	13.11.2020 15:48
5	NFCDFF-02-G1FXYX7FLEBMQ6EL	DE	Firefox PC (Cadmium)	Firefox PC (Cadmium)	141.55.1	Saxony	13.11.2020 10:53
6	NFAPPL-02-IPHONE8=1-6403786	DE	Apple iPhone 6s	Apple iPhone 6s	79.212.4	Bavaria	12.11.2020 17:43
7	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

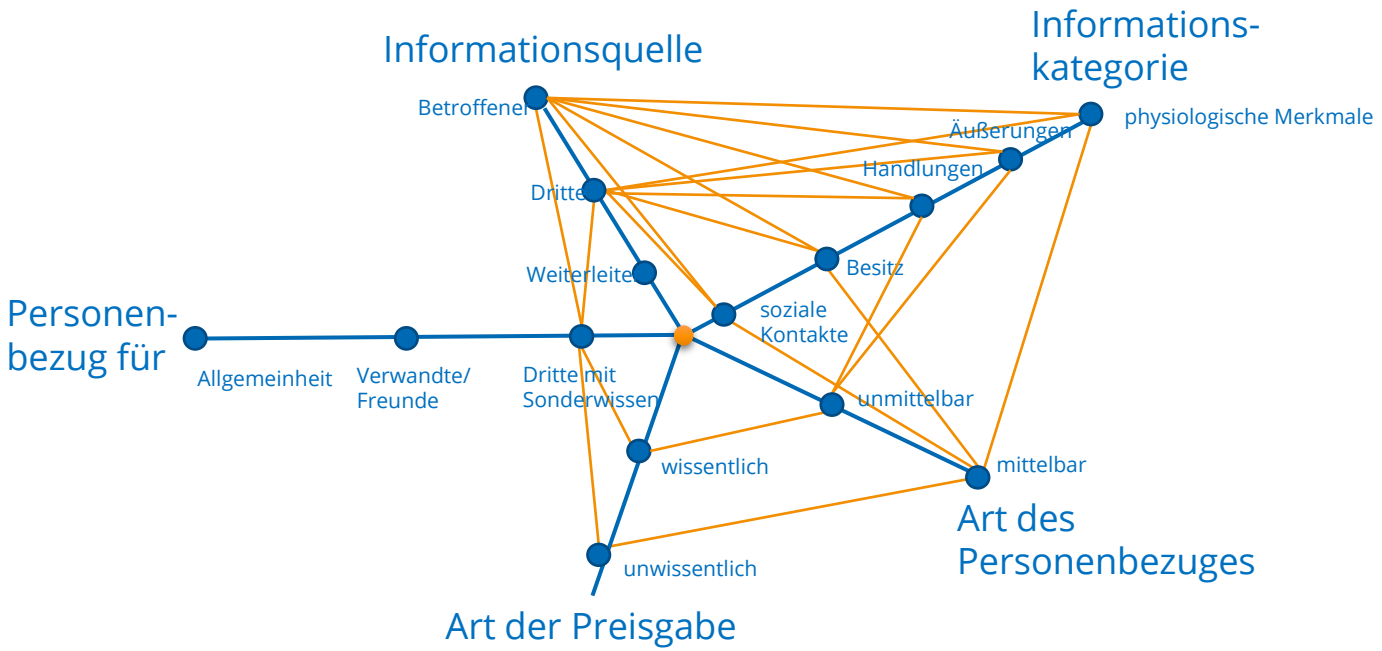
Social_Media_Connections

- Angaben zu sozialen Medien, welche mit dem Netflix-Konto verbunden sind (Facebook)

Surveys

- Informationen zu Netflix-Umfragen nach Abonnementkündigung

Dimensions-Diagramm Netflix



Personenprofil

- Alter
- Geschlecht
- Herkunft / Sprache
- Angewohnheiten

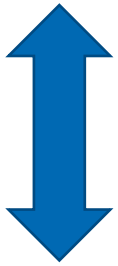
Sehverhalten

- Vorlieben (Serien / Filme, Genre)
- Arbeitsverhältnis
- Arbeitszeit und Freizeit

Identitätsdiebstahl und Onlinehandel

- Identitätsdiebstahl im Zusammenhang mit Internetbanking beinhaltet den Missbrauch gestohlener persönlicher Daten, um unbefugten Zugriff auf Bankkonten oder finanzielle Transaktionen durchzuführen.
- Angreifer können gestohlene Identitäten nutzen, um sich in die Online-Banking-Konten ihrer Opfer einzuloggen und Geld zu überweisen, Konten zu leeren oder betrügerische Transaktionen durchzuführen.

Durch die Marktdurchdringung einzelner Technologien
hat unser Leben eine neue Qualität erhalten. Ein ständiges Immer-erreichbar-Sein hat in den letzten Jahren unser Lebens-, Kommunikations- und Mediennutzungsverhalten maßgeblich verändert, sodass manche Kritiker bereits von einem gesellschaftlichen Wandel der Kommunikation sprechen.



Der Anstieg von und die Methodenvielfalt der Delikte von Cybercrime sind primär auf die Entwicklung im Telekommunikationssektor und die Digitalisierungsmaßnahmen zurückzuführen.

Identitätsdiebstahl und Onlinehandel

Unabhängig davon, dass diese Entwicklung negative Auswirkungen für den Einzelhandel hat, ist festzuhalten, dass mit diesem Trend immer mehr Menschen ihre **Zahlungsdaten, wie z. B. Kreditkarten- oder Bankkontonummern, Adressen und weitere persönliche Daten, im Netz preis** geben.

Dies bietet Personen, die sich des Internets aus kriminellen Gründen bedienen, neue Möglichkeiten und grundsätzlich einen Nährboden.

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