Wissenschaft.Niederösterreich
Am Puls der Zukunft.
FTI PROGRAMM
NIEDERÖSTERREICH

Diese Arbeit wird von der NÖ Forschungs- und Bildungsges.m.b.H. (NFB) im Rahmen des FTI Call Digitalisierung 2018 kofinanziert. Für den Inhalt dieser Publikation sind die Autor*innen verantwortlich.

Cybercrime – Die Diskrepanz zwischen Hell- und Dunkelfeld

DONAU UNIVERSITÄT KREMS

n[f+b]
NÖ Forschung & Bildung

KIRAS
Sicherheitsforschung

Über mich

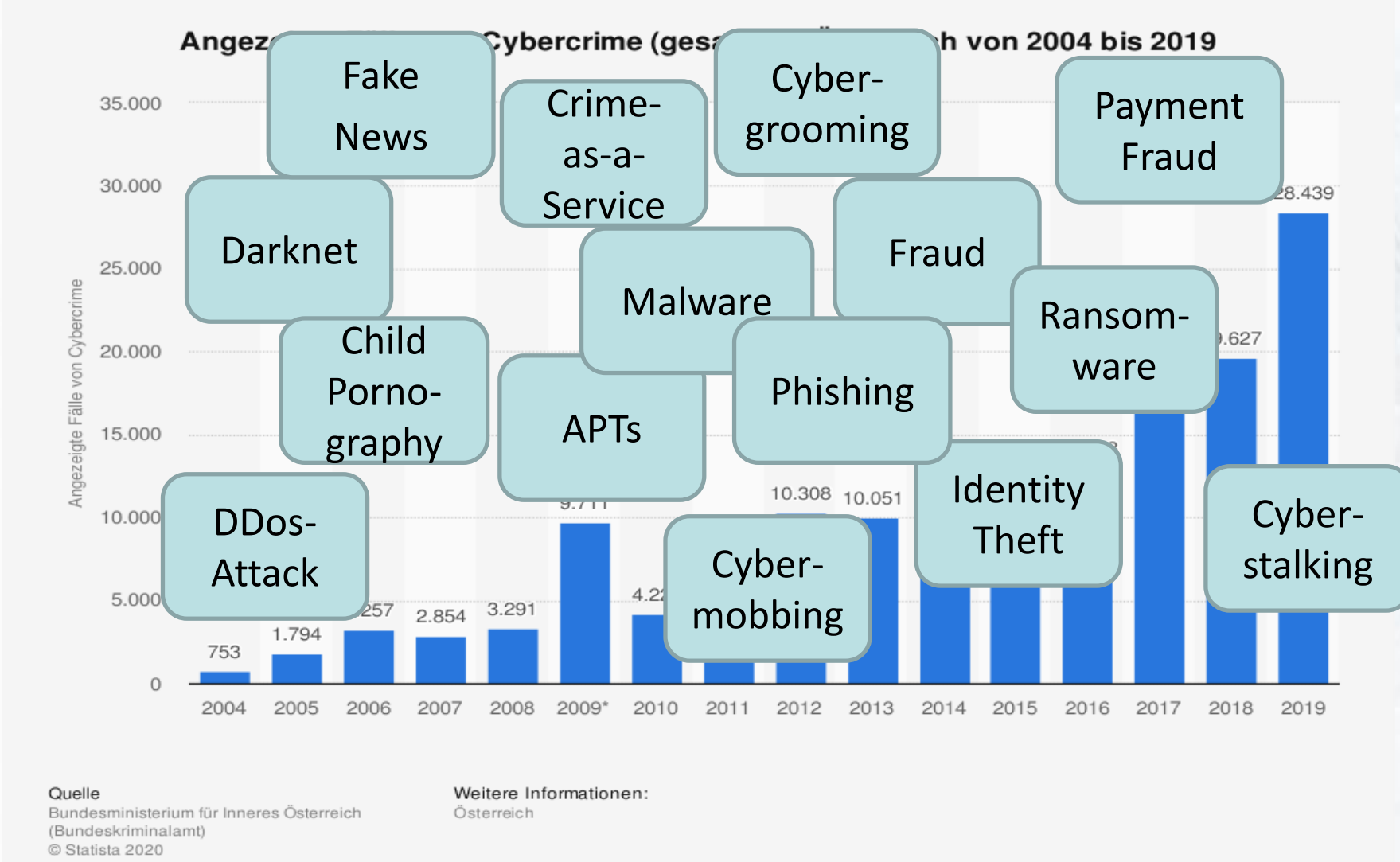
- Dr. an der Universität Wien.
  - Spezialisierung -> Cyberstalking
- Forschungsschwerpunkte: Recht- und Kriminalsoziologie mit dem Fokus auf Cybercrime und Menschenhandel, Misbehaviour in Internet, Sicherheitsforschung
- Reviewer Europäischen Kommission Sicherheitsforschung
- Seit 15 Jahren an der Donau-Universität Krems

Agenda

- Definition Cybercrime
- Ergebnisse einer Hellfeldstudie durchgeführt am Straflandesgericht in Wien
- Ergebnisse einer Dunkelfeldstudie über die Opferwerdung von Privatpersonen in Österreich
- Nicht-Ziel
  - IT-Forensik
  - Juristische Analysen
  - Technischen Möglichkeiten des Cyber-Angriffs
  - Maßnahmen der Cybersecurity

CYBERCRIME – EINE FRAGE DER DEFINITION

Registrierte Fälle in Österreich – Kriminalstatistik (PKS)



Was ist Cybercrime?

- Cybercrime-Delikte sind nicht nur Cyberattacken.
- Es hängt immer vom rechtlichen Rahmen jedes Landes ab.
- Es hängt von landespezifischen kulturellen Aspekten ab.
  - Beispiel: Hate-Crime
- Oft ist das Internet der Tatort. Das alleine ist jedoch kein Indiz für Cybercrime.
  - Beispiel: Sending an E-Mail

Zwei Arten von Cybercrime

- Core Cybercrime
  - Delikte, die nur online existieren.
  - “Attacken oder Angriffe” gegen Vertraulichkeit, Integrität, Verfügbarkeit von Netzwerken, Geräten, ...
  - Beispiel: Cyber vandalism, Virus, Malware, Ransomware etc.

- Cyber-enabled Crime
  - Delikte, die auch offline existieren.
  - Beispiel: Illegale Verwendung von Kreditkarten, Identitätsdiebsstahl,Betrug, Cyberstalking, Cybermobbing, Konsum von kinderpornographischen Inhalten.

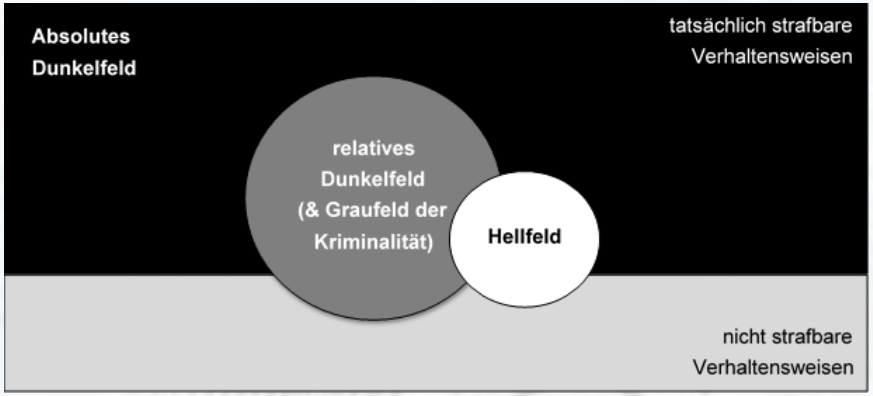
Rechtlicher Rahmen in Österreich laut StGB

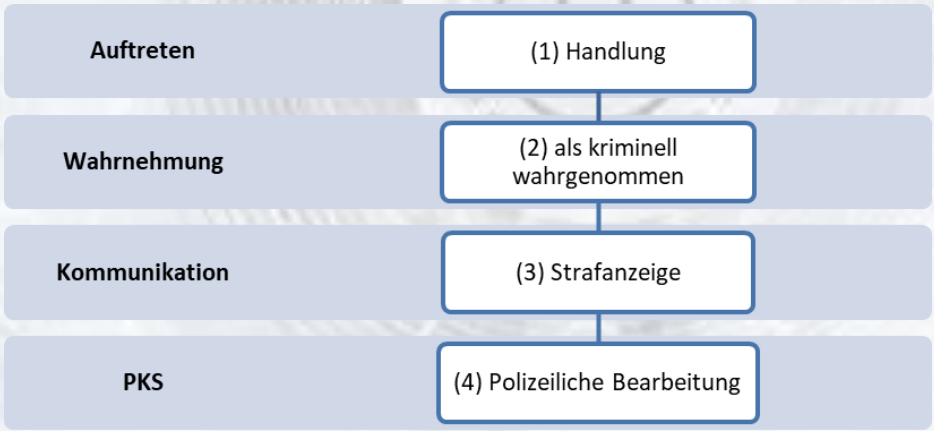
§ 126a	Datenbeschädigung
§ 148a	Betrügerischer Datenverarbeitungsmissbrauch
§ 118a	Widerrechtlicher Zugriff auf ein Computersystem
§ 119	Verletzung des Telekommunikationsgeheimnisses
§ 119a	Missbräuchliche Abfangen von Daten
§ 126b	Störung der Funktionsfähigkeit eines Computers
§ 126c	Missbrauch von Computerprogrammen oder Zugangsdaten
§ 225a	Datenfälschung
§ 207a	Kinderpornographie (Pornographische Darstellung Minderjähriger)
§ 208a	Anbahnung von Sexualkontakten zu Unmündigen (seit Jänner 2012)
§ 107c	Anti-Stalking-Paragraph (seit Jänner 2016)

HELLFELD VERSUS DUNKELFELD

Hellfeld versus Dunkelfeld

- Erklärung Hell- und Dunkelfeld
- Kunz / Singelnstein (2016) Kriminologie





Problematik – Dunkelfeld im Cybercrime

- Jede/-r, der eine/-n der das Internet nutzt kann Opfer werden.
- Es gibt kaum gültige Zahlen über Prävalenzen.
- Opferwerdung wird nicht gerne zugestanden.
  - Reputationsverlust, Scham, Unwissenheit
- Methodische Probleme beim Erheben des Dunkelfelds:
  - Erhebungsmethode: Zu wenig Privathaushalte werden befragt.
- Oft werden Online-Methoden herangezogen.
- Hier werden nur internet-affine Personen erfasst.
- Zu viele englische Fachbegriffe. -> sprachliches Problem
- Aktuell gibt es keine Quer- und Längschnittsbefragungen.
- Telefon, mündliche und schriftliche Befragungen sind zu zeit- und kostenintensiv.

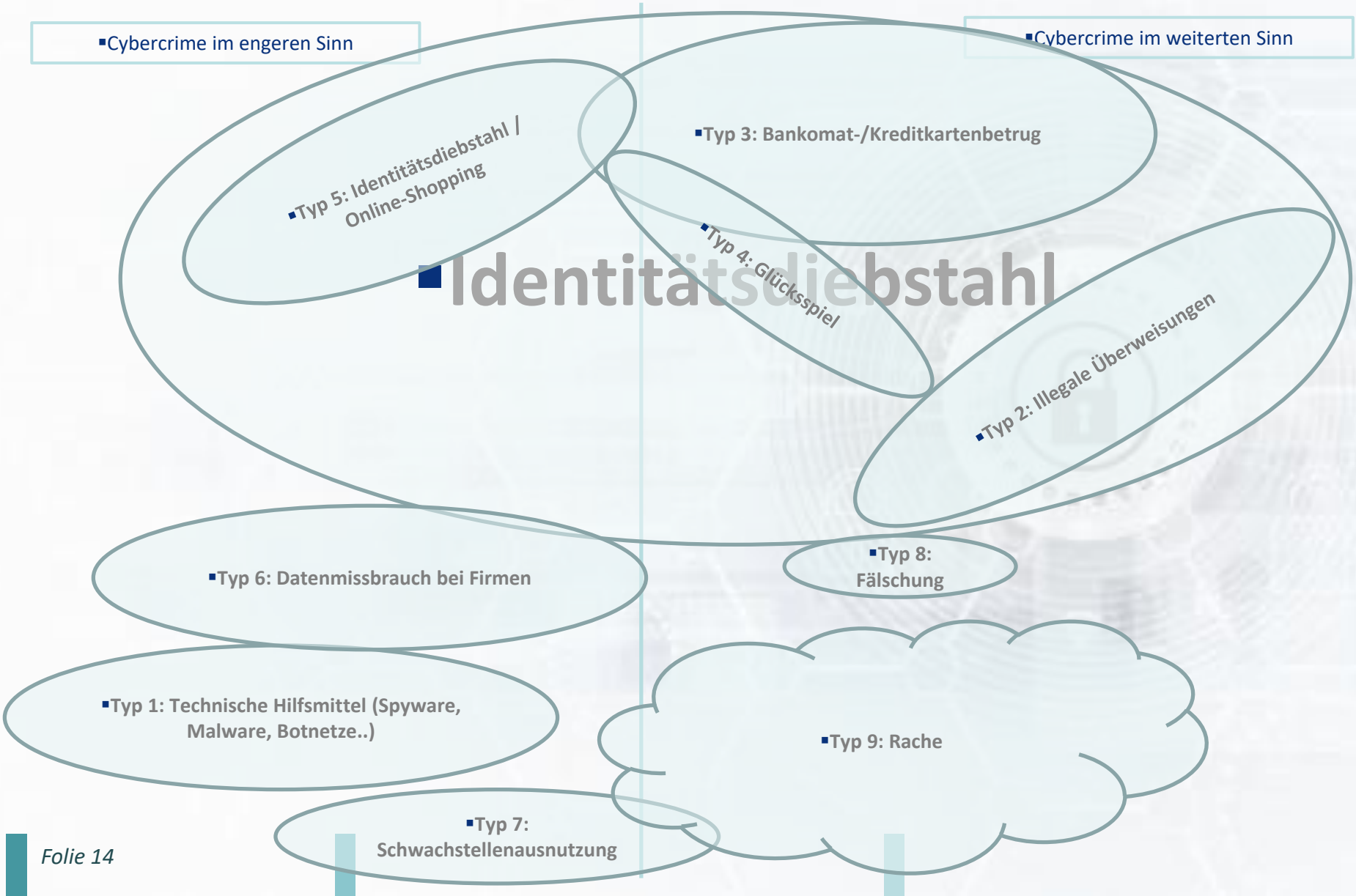
HELLFELD IN WIEN

Hellfeldstudie am Wiener Straflandesgericht 2006-2016 - Aktenanalyse

- N=5400 Akten
  - N=399 Hauptverhandlung bei Gericht

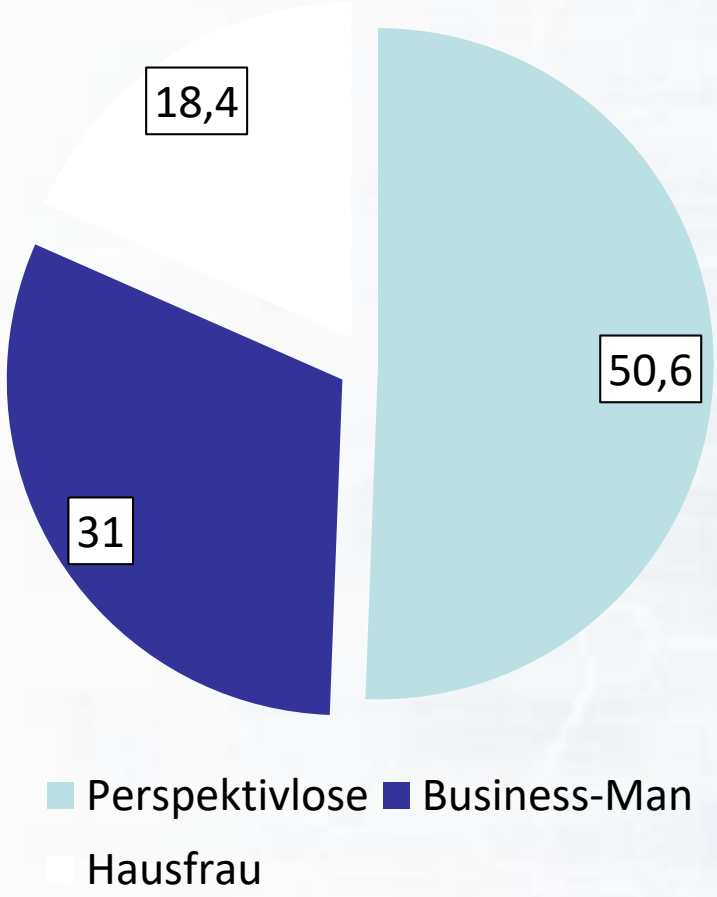
Das Projekt CERT-Komm I wurde von der FFG, unter der Programmlinie KIRAS gefördert.

Klassifizierung der Delikte



Wer sind die Täter/innen?

Täter des Hellfeldes



- *Werte in Prozentzahlen*

- Clusteranalyse
  - Geschlecht (100 %)
  - Beschäftigung (48 %)
  - Bildung (32 %)
  - Alter (4 %)
- Clusterqualität von 0,4 (Durchschnittlich)

Der Täter im Sinne des „Ideal-Typus“ in der Statistik

Männlich

Zirka 34 Jahre alt

Österreicher

Single

Sehr einfache Ausbildung

Nicht vorbestraft

Businessman

Mann

IT Background

Angestellt

Hohes Ausbildungslevel

Zirka 35 Jahre

Komplexe Attacken

31%

Hausfrau

Frau

Niedriges Ausbildungslevel

Kein IT- background

Geringe Komplexität

Zirka 32 Jahre alt

Arbeitslos

18,4 %

Perspektivlose

Männer

Niedriges Ausbildungslevel

Geringe Komplexität

Zirka 30 Jahre alt

Problematischer Background

Arbeitslos

Vorbestraft

„Süchtig“

50,6%

Opfer

- Private Individuen
  - 58 % aller Opfer
  - Einzelpersonen, Gruppen, Personen öffentliche Interesses
  - Schwachstelle: Unaufmerksamkeit und wenig ausreichende Sicherheitsmaßnahmen
  - Konsequenzen: psychischer Schaden, finanzieller Schaden, Informationsverlust

- Institutionen
  - 42 % aller Opfer
  - Firmen, Agenturen
  - Schwachstelle: öffentlich bekannte Sicherheitslücke, wenig ausreichende Sicherheitsmaßnahmen
  - Konsequenzen: Wiederherstellungskosten, Verlust von Informationen, finanzieller Schaden, Reputationsverlust

DUNKELFELD ÖSTERREICH

Privatpersonenbefragung

- In Zusammenarbeit mit dem Marktforschungsinstitut Integral
- Grundgesamtheit = alle Haushalte in Österrich
- In der Altersklasse 16-69 Jahre
- Stichprobe = n=1.007 repräsentativ
- Onlinebefragung
- Basis für die Befragung Delikte, die unter “Cybercrime” subsumiert werden und Betrugsdelikte

Das Projekt ARES wurde von der NÖ Bildungsgesellschaft gefördert.

Beschreibung der Stichprobe

Variable	n	Prozent	Mittelwert
Geschlecht	**1007**	**100**	**1,50**
männlich	503	50	
weiblich	504	50	
Alter	**1007**	**100**	**3,45**
14-24	89	8,8	
25-34	213	21,1	
35-44	179	17,8	
45-54	206	20,5	
55-69	320	31,8	

n = 1.007

Beschreibung der Stichprobe

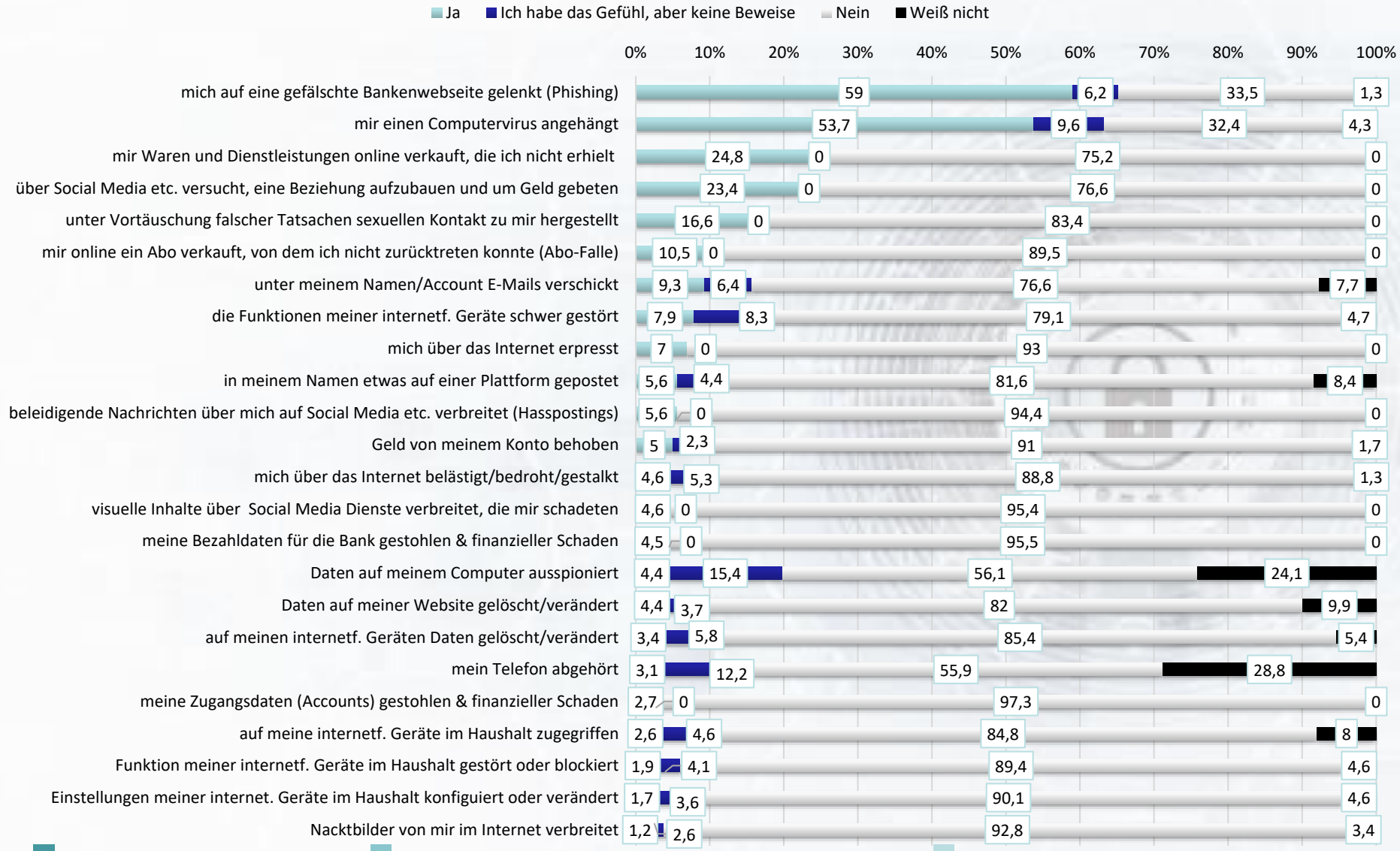
Variable	n	Prozent	Mittelwert
Bildung	**1007**	**100**	**3,46**
(Keine) Pflichtschule	44	4,4	
Lehre	326	32,4	
Mittlere (Fach-)Schule	225	22,3	
BHS-/HTL-Matura	139	13,8	
AHS-Matura	85	8,4	
Uni, FH, Akademie	188	18,7	
Haushaltsnetto-Einkommen	**977**	**100**	**5,54**
Unter € 1.000	52	5,3	
€ 1.000 - € 1.999	195	20	
€ 2.000 - € 2.999	244	25	
€ 3.000 - € 3.999	243	24,9	
€ 4.000 - € 4.999	142	14,5	
€ 5.000 und mehr	101	10,3	

n = 1.007

Opfer von Cybercrime - allgmein

- 84 % aller Österreicher waren schon einmal Opfer von Cybercrime
- Im statistischen Durchschnitt ist das Opfer 45 Jahre alt, hat Matura (Abitur) und ist angestellt.
- Männer werden signifikant öfter Opfer von Cybercrime als Frauen. Dies ist aber kein Ursache – Wirkungs – Zusammenhang. Es erklärt sich eher dadurch, dass Männer mehr internetfähige Geräte bedienen.

Wurden Sie schon einmal Opfer folgender Ereignisse? Jemand hat illegal...



WAS SOLLEN WIR TUN?

- Jeder kann Opfer von Cybercrime werden, unabhängig von Bildung, Geschlecht, sozialer Status…etc.
- Es gibt wenig allgemeine Schutzmaßnahmen, da die Delikte sehr unterschiedlich sind.
- Allgemein emfehlen wir folgende Maßnahmen:
  - Teilen Sie niemals Passworte
  - Führen Sie regelmäßige Softwareupdates durch
  - Verwenden Sie ein Antivirenprogramm
  - Teilen Sie keine intimen Fotos oder Videos
  - Zahlen Sie nie, wenn Sie dazu aufgefordert werden
  - Kontaktieren Sie die Polizei

Literatur

Allgemeine Grundlagen und Details zur Hellfeldstudie:

- Huber, Edith (2020) Cybercrime – Eine Einführung, Springer

Tipp:

IOCTA:

https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

DANKE!


DONAU UNIVERSITÄT
KREMS


n[f+b]
NÖ Forschung & Bildung


KIRAS
Sicherheitsforschung