KIRAS Sicherheitsforschung

Das Projekt wird innerhalb des Sicherheitsforschungs-Förderprogramms KIRAS durch das Bundesministerium für Verkehr, Innovation und Technologie gefördert.

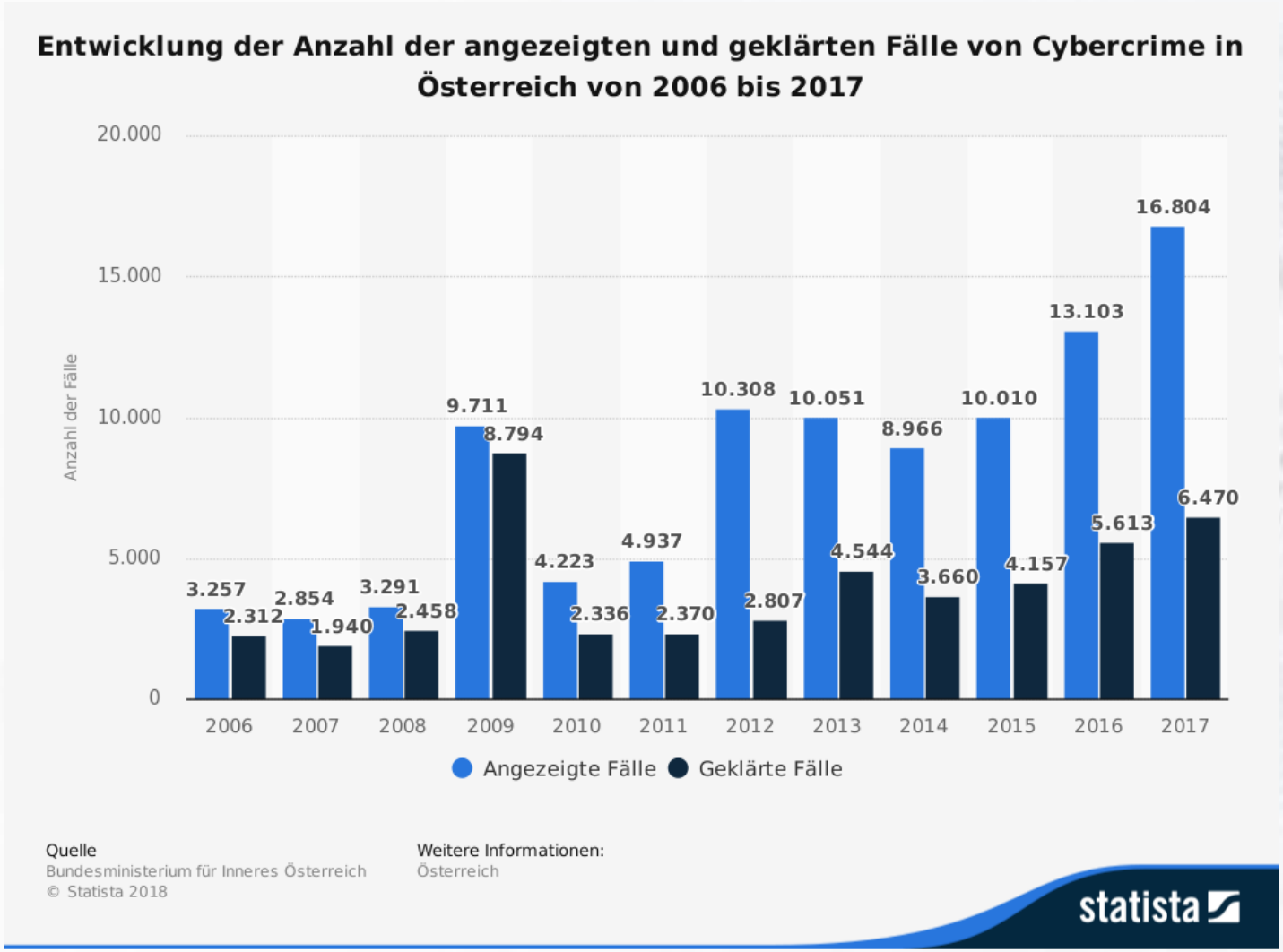
WITHOUT A TRACE – Die ungeklärten Cybercrime-Fälle des Straflandesgerichts Wien von 2006-2016

Dr. Edith Huber, Bettina Pospisil MA

Donau-Universität Krems

BUNDESKANZLERAMT ÖSTERREICH · SBA Research · universität wien · DONAU UNIVERSITÄT KREMS · research institute · IKARUS security software

Cybercrime-Statistik in Österreich



KIRAS
Sicherheitsforschung

FORSCHUNGSDESIGN

BUNDESKANZLERAMT ÖSTERREICH
SBA Research
universität wien
DONAU UNIVERSITÄT KREMS
research institute
IKARUS security software

Forschungsfragen

(1) Welcher Modus Operandi zeigt sich bei den ungeklärten Fällen?

(2) Welche Muster verfolgen die TäterInnen von Cybercrime-Delikten?

(3) Inwieweit unterscheiden sich die geklärten Cybercrime-Fälle von den ungeklärten Fällen?

Cybercrime-Delikte nach dem Strafgesetzbuch

§118a	• Widerrechtlicher Zugriff auf ein Computersystem
§119	• Verletzung des Telekommunikationsgeheimnisses
§119a	• Missbräuchliches Abfangen von Daten
§123	• Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses
§124	• Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses zugunsten des Auslandes
§126a	• Datenbeschädigung
§126b	• Störung der Funktionsfähigkeit eines Computersystems
§126c	• Missbrauch von Computerprogrammen
§148a	• Betrügerischer Datenverarbeitungsmissbrauch
§225a	• Datenfälschung

Aktenanalyse der Fälle von 2006 - 2016

N=5.408 Fälle

N=399 Verurteilungen

N=5.009 ungeklärte Fälle

Abzug von Identitätsdiebstahl, ungültige Fälle, etc. N=2.289

N=2.720 ungeklärte Fälle

n=20 %

KIRAS
Sicherheitsforschung

DER MODUS OPERANDI

BUNDESKANZLERAMT ÖSTERREICH
SBA Research
universität wien
DONAU UNIVERSITÄT KREMS
research institute
IKARUS security software

Cybercrime im engeren Sinn

Cybercrime im weiteren Sinn

KIRAS
Sicherheitsforschung

WELCHE TATHERGANGSMUSTER LASSEN SICH ERKENNEN?

BUNDESKANZLERAMT ÖSTERREICH
SBA Research
universität wien
DONAU UNIVERSITÄT KREMS
research institute
IKARUS security software

Der „idealtypische“ Täter ist…

männlich

rund 34 Jahre alt

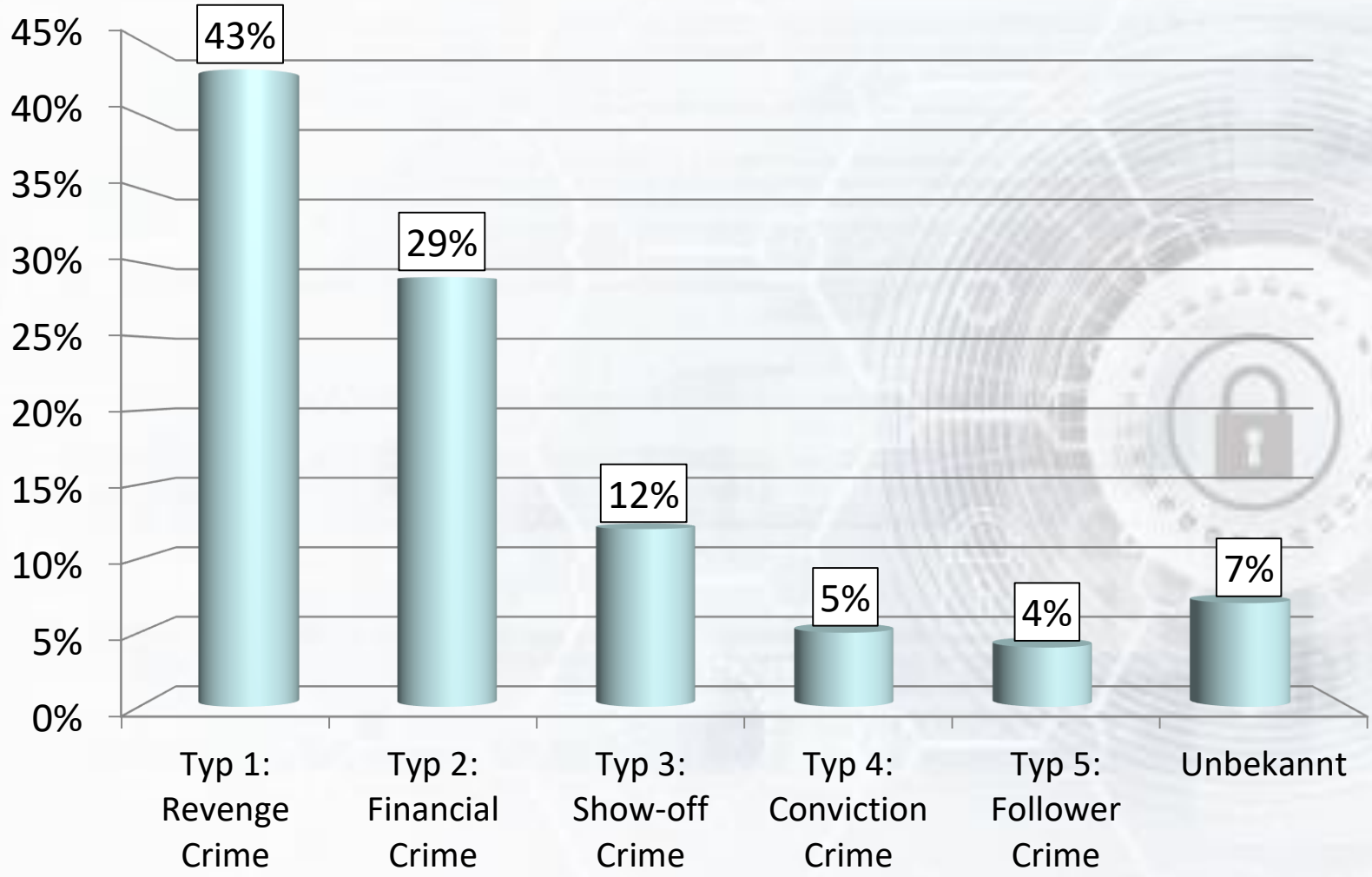
österreichischer Staatsbürger

ledig

durchschnittlich gebildet

nicht vorbestraft

Tathergangsmuster nach Motivation



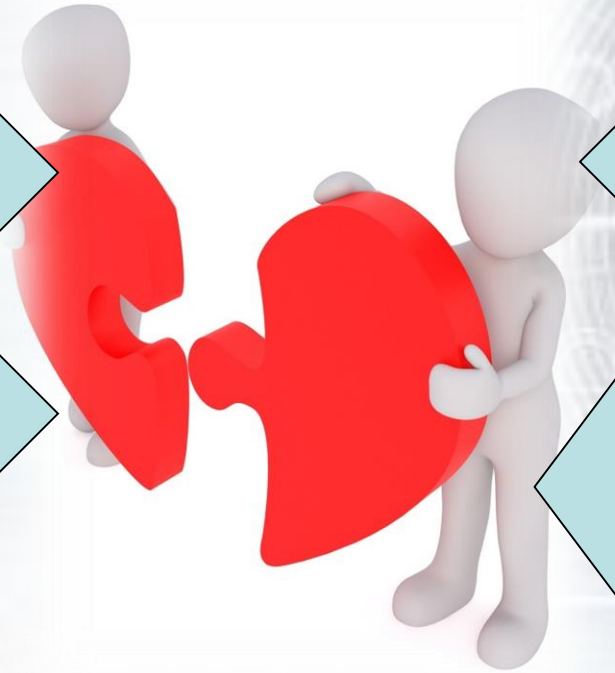
Revenge Crime

43%

EinzeltäterIn

kein technisches Know-How

einfaches Vorgehen



Beziehung zum Opfer

Opfer ist eine Privatperson

Beispiele: Datenmissbrauch über Social Media Plattformen

Financial Crime

29%

TäterIn agiert in der Gruppe

Einsatz technischer Hilfsmittel

einfaches Vorgehen

keine Beziehung zum Opfer

Opfer ist eine Privatperson oder Firma

Beispiele: Phishing, Social Engineering, Crime as a service, ...

Show-off Crime

13%

TäterIn agiert in der Gruppe

TäterIn ist jünger

eher komplexes Vorgehen

Tool-basierte Angriffsformen

keine Beziehung zum Opfer

Opfer ist eine Behörde oder Firma

Beispiele: Datenmissbrauch, Veröffentlichung privater und hochsensibler Daten, …

Conviction Crime

5%

Ziel ist die Verbreitung von Idealen

keine Beziehung zum Opfer

Einsatz technischer Hilfsmittel

Schaden: Reputationsverlust

TäterIn agiert in der Gruppe

Beispiele: Verbreitung extremistischer und verbotener Inhalte über Websites, …

Follower Crime

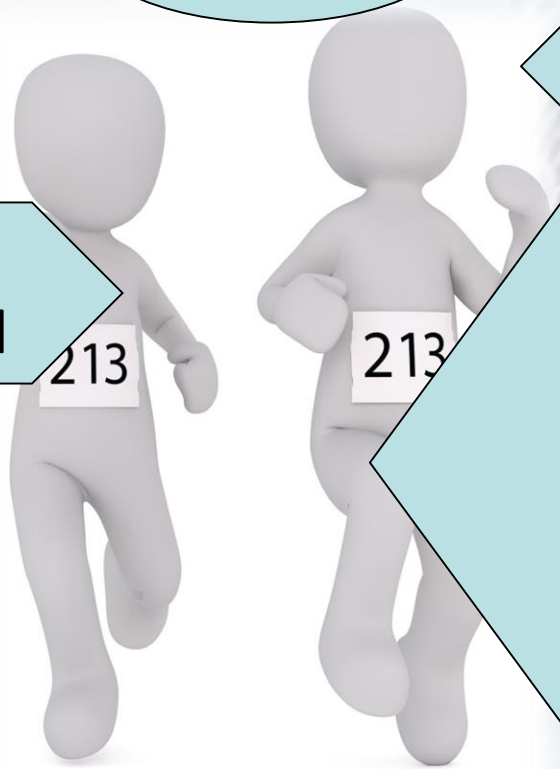
4%

Es gibt einen Tat-ermöglicher

keine Beziehung zum Opfer

kein Einsatz technischer Hilfsmittel

einfaches Vorgehen



Beispiel: Informationen werden aus fehlendem Bewusstsein genutzt bzw. ausprobiert

KIRAS
Sicherheitsforschung

GEMEINSAMKEITEN UND UNTERSCHIEDE DER GEKLÄRTEN UND UNGEKLÄRTEN FÄLLE

BUNDESKANZLERAMT ÖSTERREICH
SBA Research
universität wien
DONAU UNIVERSITÄT KREMS
research institute
IKARUS security software

Vergleich der Aktenanalysen

- Fälle mit Verurteilung
  - TäterIn ist größtenteils bekannt
  - Sehr simples Vorgehen
  - Verlagerung traditioneller Kriminalität in den Cyberspace

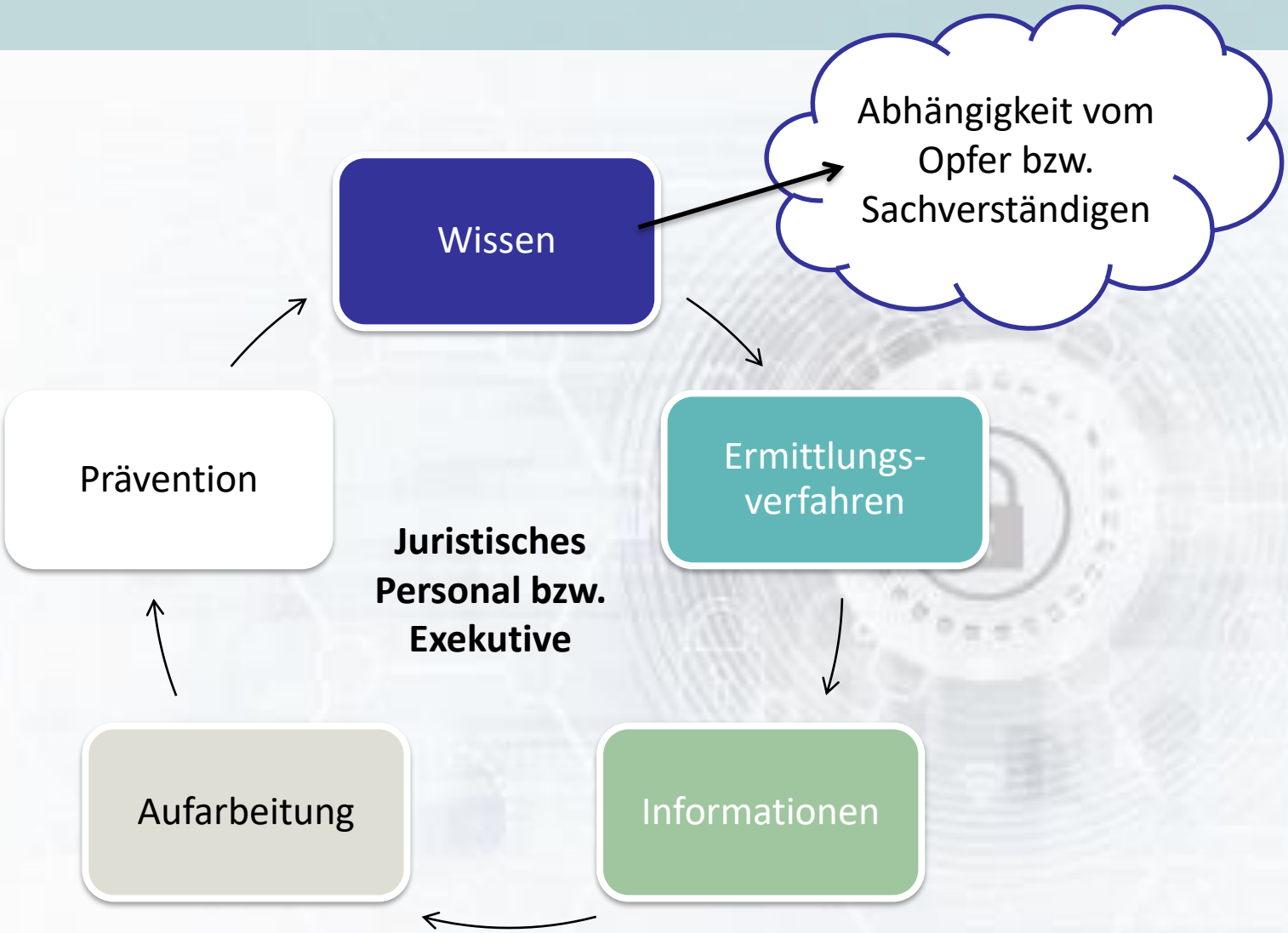
- Ungelöste Fälle
  - TäterIn ist größtenteils unbekannt
  - Größere Anzahl komplexerer Delikte
  - Aber auch: Revenge Crime
  - Technische Angriffe: Crime as a Service, kriminelle Finanzgeschäfte, Phishing, …
  - Gründe für die Nichtaufklärung:
    - Fehlende Gründe zur weiteren Verfolgung
    - Fehlende Anhaltspunkte
    - Fehlende Beweise

KIRAS
Sicherheitsforschung

SCHLUSSFOLGERUNGEN

BUNDESKANZLERAMT ÖSTERREICH
SBA Research
universität wien
DONAU UNIVERSITÄT KREMS
research institute
IKARUS security software

(1) Notwendigkeit des Wissensausbaus



(2) Notwendigkeit des effizienten Einsatzes

- Die beschränkte Verfügbarkeit hochqualifizierter ExpertInnen verlangt nach…
  - …dem weiteren Aufbau von ExpertInnen
  - …dem effizienten Einsatz bestehender Kompetenzen
- Zukünftig sollte aus Effizienzgründen unterschieden werden, in Fälle…
  - …mit technologisch anspruchsvollem Vorgehen (Cybercrime im engeren Sinn)
  - …in welchen die IKT als Tatmittel zur Begehung traditioneller Vergehen eingesetzt wurde (Cybercrime im weiteren Sinn)

KIRAS Sicherheitsforschung

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Edith Huber

E-Mail: edith.huber@donau-uni.ac.at

https://www.linkedin.com/in/dr-edith-huber-ab185930/

Bettina Pospisil, MA

E-Mail: bettina.pospisil@donau-uni.ac.at

BUNDESKANZLERAMT ÖSTERREICH SBA Research universität wien DONAU UNIVERSITÄT KREMS research institute IKARUS security software