

```
import string import csv import os.path import sys from evdev import InputDevice, categorize, ecodes, list_devices from
select import select class Reader: def __init__(self): path = os.path.dirname(os.path.realpath(__file__)) self.keys =
"X^1234567890XqwertyuiopXjklXyxcvbnmX if not os.path.isfile(path + '/deviceName.txt'): sys.exit('Please run config.py
first') else: with open(path + '/deviceName.txt','r') as f: deviceName = f.read() devices = [InputDevice(fn) for fn in
list_devices()] for device in devices: if device.name == deviceName: self.dev = device break try: self.dev except:
sys.exit('Could not find the device %s\n. Make sure is connected' % deviceName) def readCard(self): stri='' key = '' while
key != 'KEY_ENTER': r,w,x = select([self.dev], [], []) for event in self.dev.read(): if event.type==1 and
event.value==1: stri+=self.keys[ event.code ] #print( keys[ event.code ] ) key = ecodes.KEY[ event.code ] return stri[:-1]
import string import csv import os.path import sys from evdev import InputDevice, categorize, ecodes, list_devices from
select import select class Reader: def __init__(self): path = os.path.dirname(os.path.realpath(__file__)) self.keys =
"X^1234567890XqwertyuiopXasdfghiklXXXXXyxcvbnmX if not os.path.isfile(path + '/deviceName.txt'): sys.exit('Please run
config.py first') else: with open(path + '/deviceName.txt','r') as f: deviceName = f.read() devices = [InputDevice(fn) for
fn in list_devices()] for device in devices: if device.name == deviceName: self.dev = device break try: self.dev except:
sys.exit('Could not find the device %s\n. Make sure is connected' % deviceName) def readCard(self): stri='' key = '' while
key != 'KEY_ENTER': r,w,x = select([self.dev], [], []) for event in self.dev.read(): if event.type==1 and
event.value==1: stri+=self.keys[ event.code ] #print( keys[ event.code ] ) key = ecodes.KEY[ event.code ] return stri[:-1]
"X^1234567890XqwertyuiopXasdfghiklXXXXXyxcvbnmX if not os.path.isfile(path + '/deviceName.txt'): sys.exit('Please run
```

**INTERNET
SECURITY
DAYS 2018**



Kriminologische Perspektiven auf das Phänomen Cybercrime

Prof. Dr. Gina Wollinger • Arne Dreißigacker



Fachhochschule
für öffentliche Verwaltung
NRW

Köln



- Kriminalität: Situation in Deutschland
- Cybercrime: Lage und Entwicklung
- Ausblick: Forschungsprojekt

Kriminalität in Deutschland



8 Hannoverische Allgemeine Zeitung NIEDERSACHSEN & DER NORDEN Dienstag, 27. Februar 2018

Grüko statt Groko

David McAllister ist neuer Grüko-Vizepräsident

Berlin/Oldenburg. Als die Karibik in Berlin ihre neue Präsidentschaft vorstellt, fällt auch Niedersachsen ein. Die Grünen wählen David McAllister zum neuen Vizepräsidenten der Partei. Er wird die Grünen in Niedersachsen vertreten. McAllister ist seit 2013 Mitglied des Bundestages und seit 2017 Mitglied des Niedersächsischen Landtages. Er ist Mitglied der Bundestagsverwaltung für die Bereiche Wirtschaft und Energie. McAllister ist seit 2013 Mitglied des Bundestages und seit 2017 Mitglied des Niedersächsischen Landtages. Er ist Mitglied der Bundestagsverwaltung für die Bereiche Wirtschaft und Energie.

Mit Sicherheit

Weniger Einbrüche, weniger Diebstähle: Die Kriminalität in Niedersachsen sinkt – und immer mehr Fälle kann die Polizei aufklären. Nur bei Gewalt in Schulen zeigt die Kurve nach oben.

So hat sich die Zahl der Straftaten in Niedersachsen seit 1990 entwickelt

Jahr	Zahl der Straftaten
1990	6764
1991	6764
1992	6764
1993	6764
1994	6764
1995	6764
1996	6764
1997	6764
1998	6764
1999	6764
2000	6764
2001	6764
2002	8000
2003	7500
2004	7000
2005	6800
2006	6700
2007	6600
2008	6500
2009	6500
2010	6500
2011	6500
2012	6500
2013	6500
2014	6500
2015	6500
2016	6500
2017	6500

EINBRÜCHE

Menschen sichern ihre Wohnungen besser

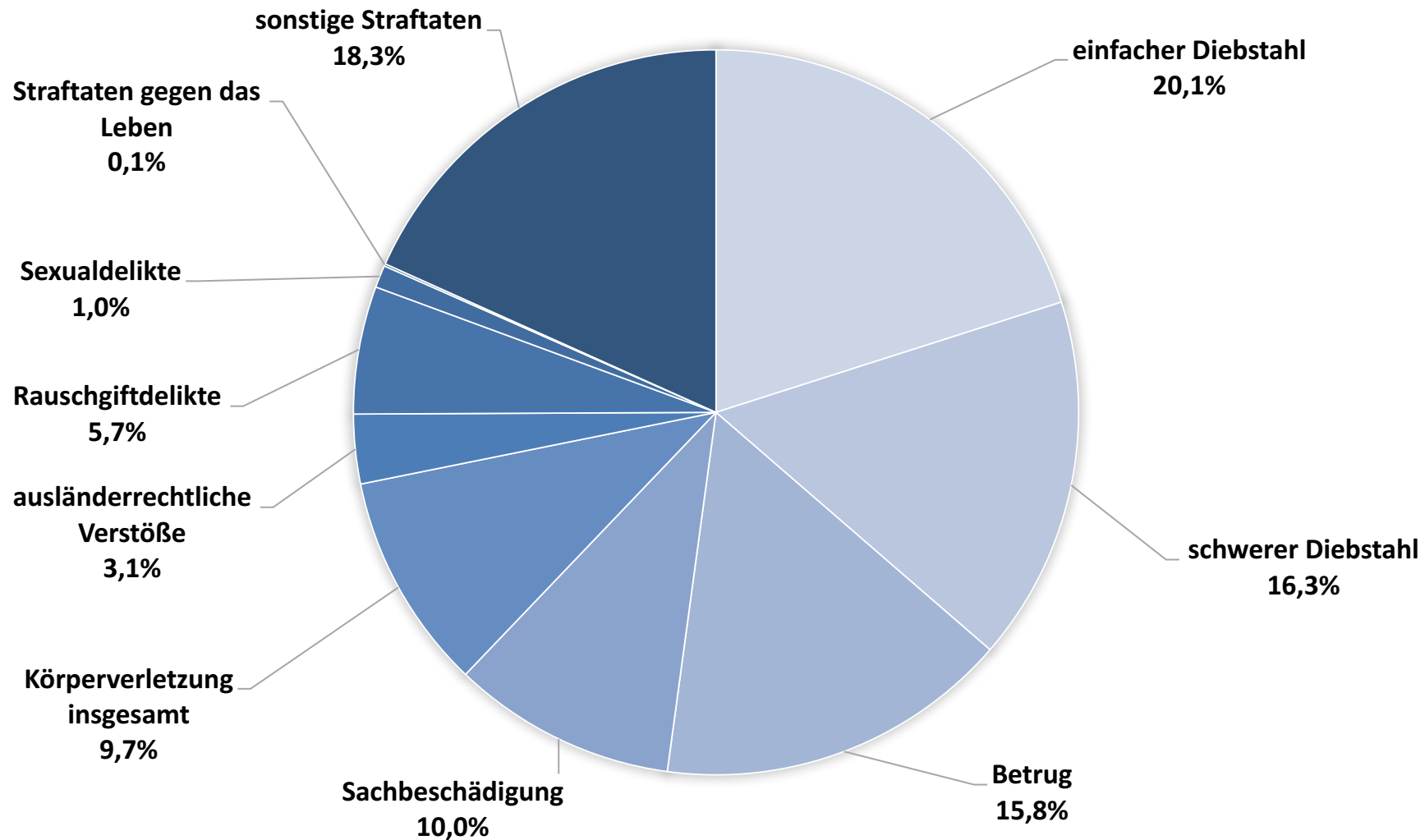
17 Prozent der im vergangenen Jahr bei Wohnun- gen eingedrungenen Täter sind Frauen. Die Polizei hat im vergangenen Jahr 13 585 Einbrüche aufgeklärt. Das ist ein Plus von 10 Prozent gegenüber dem Vorjahr. Die Polizei hat im vergangenen Jahr 13 585 Einbrüche aufgeklärt. Das ist ein Plus von 10 Prozent gegenüber dem Vorjahr.

SCHULGEWALT

Mehr Taten angezeigt

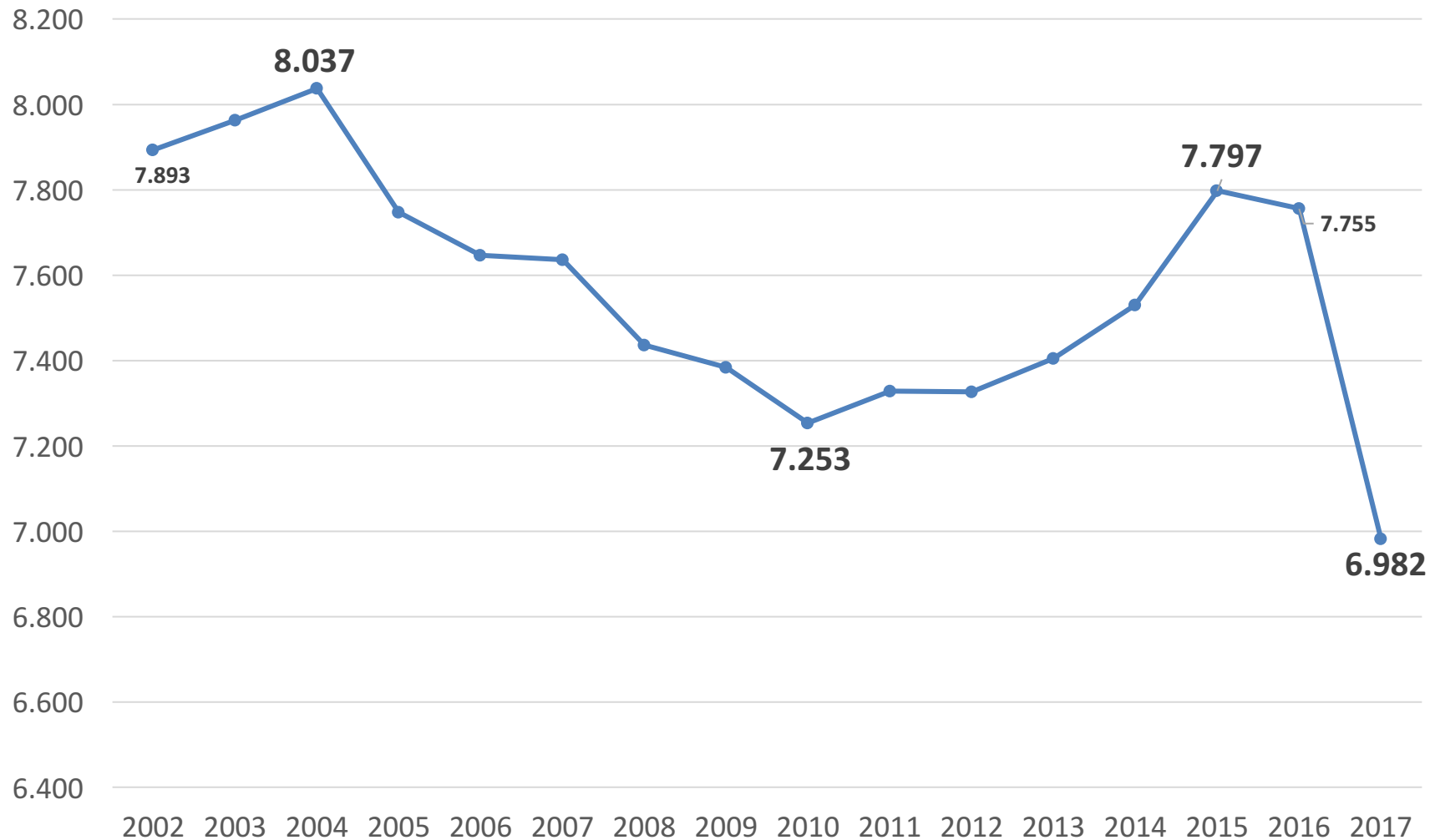
Gegen den Trend bei der Kriminalität von mehr gemeldeten Taten, die aber nicht aufgeklärt werden, zeigt die Statistik der Polizei im vergangenen Jahr. Anstieg ist dabei bei den Einbrüchen zu sehen. Die Polizei hat im vergangenen Jahr 13 585 Einbrüche aufgeklärt. Das ist ein Plus von 10 Prozent gegenüber dem Vorjahr.

Kriminalität in Deutschland



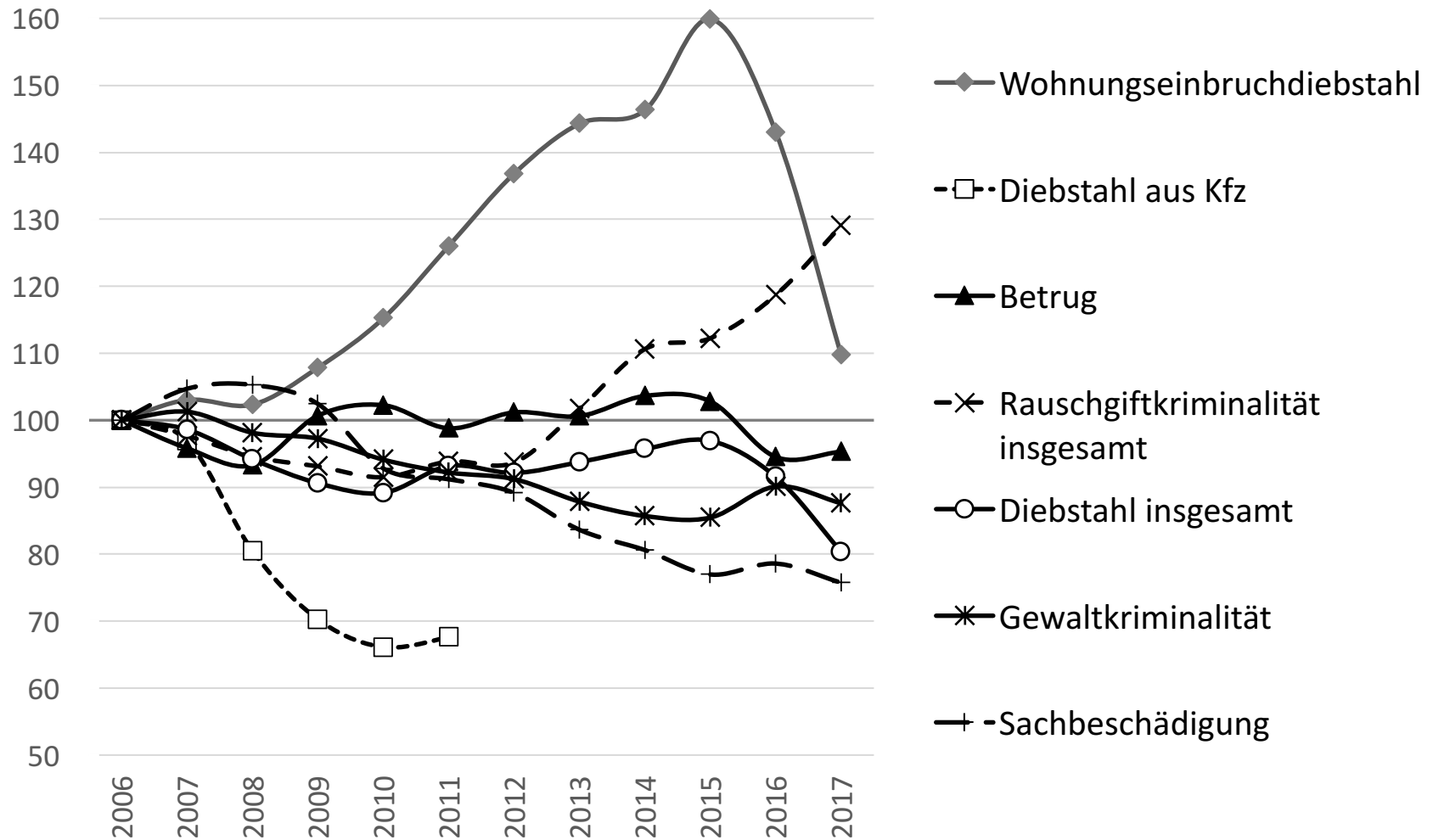
Häufigkeitsziffer Gesamtkriminalität; Quelle: PKS 2002-2017

Kriminalität in Deutschland



Häufigkeitsziffer Gesamtkriminalität; Quelle: PKS 2002-2017

Kriminalität in Deutschland

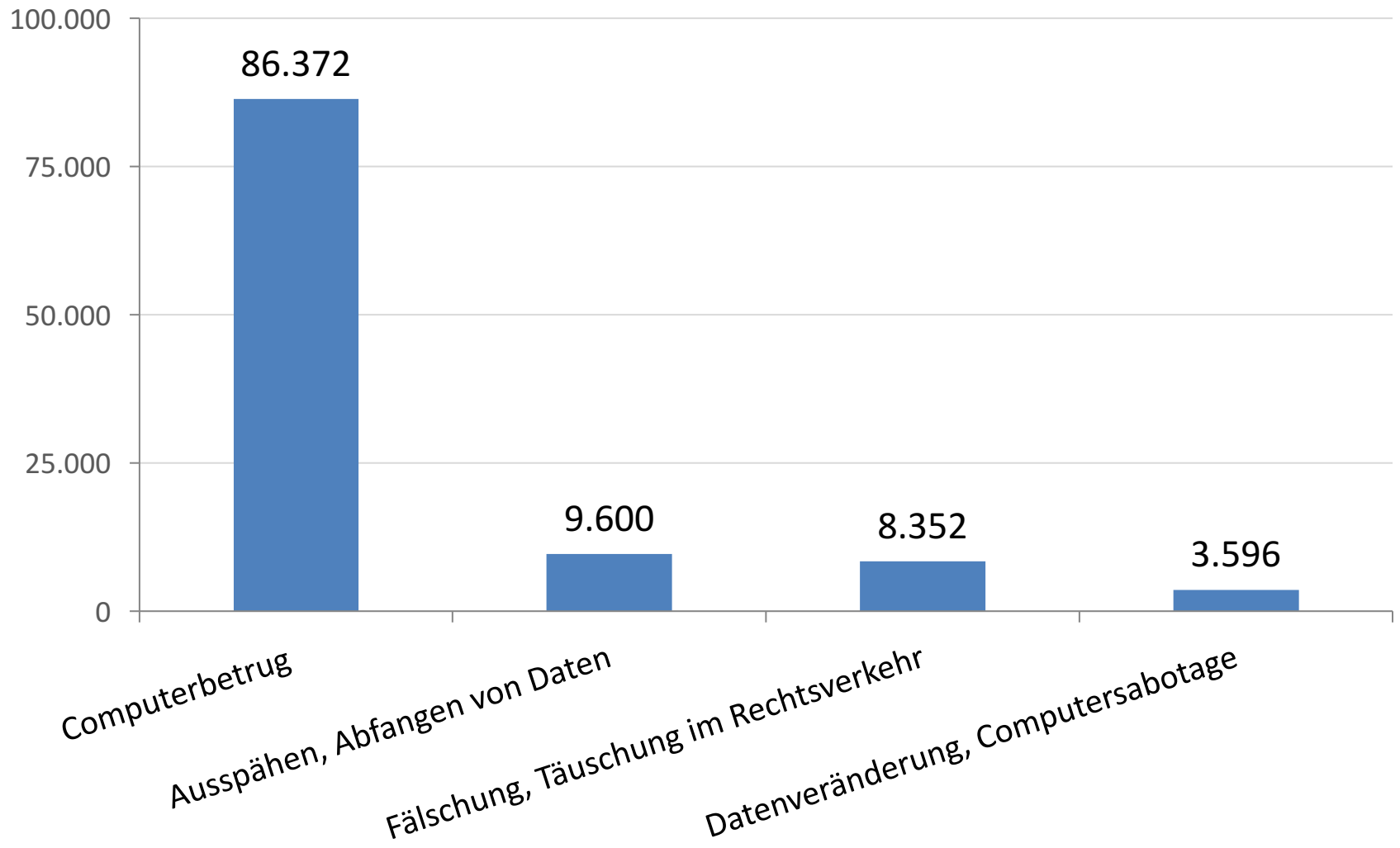


Häufigkeitsziffer nach Deliktsbereichen; 2006=100 Quelle: PKS 2006-2017

Aussagekraft der PKS

- Nur wenn Tatort in Deutschland
- 1 Tathandlung = 1 Fall (unabhängig von Anzahl der Opfer)
- Anzeigebereitschaft
 - Opferwerdung nicht bekannt
 - Keine Erwartung, dass eine Anzeige sich lohnt
 - Furcht vor Reputationsschaden
- Definition des Deliktbereichs Cybercrime

Deliktsbereich Cybercrime



Anzahl der Fälle „Cybercrime im engeren Sinn“; Quelle: PKS 2017

- Cybercrime im engeren Sinn
- Cybercrime im weiteren Sinn
 - Stichwort: Tatmittel Internet
 - PKS 2016: 253.290 Fälle
 - V.a. Betrugsdelikte (Waren- und Kreditkartenbetrug)

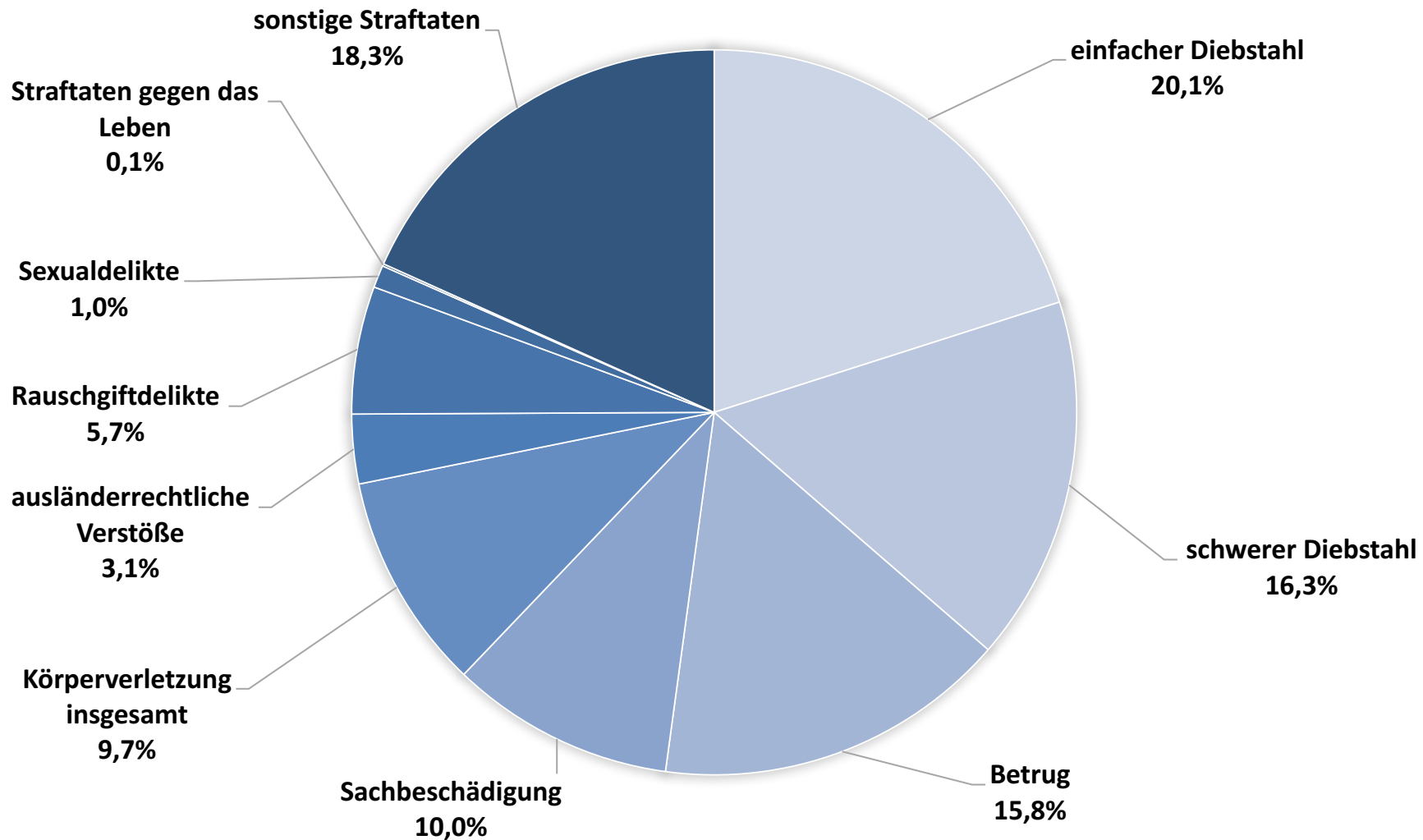
- Bitkom 2016: Innerhalb 2-Jahreszeitraum erlebten 69% der Industrieunternehmen Wirtschaftsspionage, Sabotage oder Datendiebstahl (ähnlich auch BSI 2017)
- WIK 2017: 53% der KMU hatten Probleme durch Viren, 14% erlebten einen Erpressungsversuch, 8% Datendiebstahl, nur 20% haben nichts erlebt

Einschätzung der Entwicklung im Deliktsbereich Cybercrime aufbauend auf drei Thesen:

Cybercrime-Delikte sind...

1. keine neuen Kriminalitätsphänomene
2. profitabel
3. einfach in der Ausführung

Cybercrime-Delikte sind keine neuen Kriminalitätsphänomene



Häufigkeitsziffer Gesamtkriminalität; Quelle: PKS 2002-2017

Cybercrime-Delikte sind profitabel



Willkommen im Tor Browser

Sie können jetzt anonym im Internet surfen.

[Tor-Netzwerkeinstellungen testen](#)

Sicheres Suchen mit DuckDuckGo.

Was nun?

Tor ist NICHT alles was benötigt wird, um anonym zu surfen! Sie müssen eventuell einige Gewohnheiten ändern, um sicherzustellen, dass Ihre Identität geschützt bleibt.

- [Tipps, um anonym zu bleiben](#)
»
- [Tor-Browser-Benutzerhandbuch](#) »

Sie kön

Es gibt vi
das Tor-N
stärker zu

- [Einen
betreit](#)
- [Ihre D](#)
- [Etwas](#)



Beispiel: Handel mit Daten

https://haveibeenpwned.com

The screenshot shows the homepage of the 'Have I Been Pwned' website. At the top, there is a navigation bar with links for Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main heading is a large white box containing the text '';--have i been pwned?'. Below this is a sub-heading: 'Check if you have an account that has been compromised in a data breach'. A search bar contains the URL 'www.cybercrime-forschung.de' and a 'pwned?' button. The result is 'Good news — no pwnage found!' with 'No breached accounts' below it. A section titled '3 Steps to better security' includes a 'Start using 1Password.com' button and three steps: Step 1 (Protect yourself using 1Password), Step 2 (Enable 2 factor authentication), and Step 3 (Subscribe to notifications). The footer has social media icons and a 'Donate' button.

Home Notify me Domain search Who's been pwned Passwords API About Donate

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

www.cybercrime-forschung.de pwned?

Good news — no pwnage found!
No breached accounts

3 Steps to better security [Start using 1Password.com](#)

Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.

Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.

Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

[Why 1Password?](#)

[Donate](#)

Cybercrime-Delikte sind einfach in der Ausführung

SaaS – Password cracking service

The screenshot shows a web interface for a password cracking service. The main heading is "Email Password Cracking made easy..!!". Below this, there is a paragraph of introductory text: "Fill in the below form to the best of your knowledge. Make sure that the email addresses are entered correctly. Once submitted, check your email for a confirmation mail. Add our email address(es) in your address book, to prevent our emails and the proofs landing in bulk folder. Once you verify the order by clicking on the confirmation link sent to you, we will process your order." The form contains several input fields: "Your Name", "Your Email Address", "Confirm your Email Address", "Your Country" (with radio buttons for "Most Urgent", "Urgent", and "Just do it whenever you can"), "Victim Name", "Victim Email Address", "Confirm Victim Email Address", "Victim Victim Country", "Victim Language", and "Optional Information" which includes "How you know us", "Your Yahoo! Chat ID", "Your MSN Chat ID", "Preferred Mode of Payment", and "Bonus offered (if any)". There is also a text area for "Any Instructions?". A "Submit your Order" button is located at the bottom of the form.

Nice introduction

Your victim details

"where did you heard about us?"

Source: Raj Shamni, cyber crime exposed

Kriminologische Einschätzung Cybercrime

- Deliktsverschiebung in digitalen Raum
- Mangel an Awareness
- Bedarf der „Nachrüstung“ der Sicherheitsbehörden

Forschungsprojekt „Cyberangriffe gegen Unternehmen“

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

Die Initiative „IT-Sicherheit in der Wirtschaft“ des Bundesministeriums für Wirtschaft und Energie will vor allem kleine und mittelständische Unternehmen beim sicheren Einsatz von IKT-Systemen unterstützen. Gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung soll eine Grundlage dafür geschaffen werden, um die Bewusstseinsbildung in der digitalen Wirtschaft beim Thema IT-Sicherheit im Mittelstand zu stärken. Unternehmen sollen durch konkrete Unterstützungsmaßnahmen dazu befähigt werden, ihre IT-Sicherheit zu verbessern. Weitere Informationen zur Initiative und ihren Angeboten sind unter www.it-sicherheit-in-der-wirtschaft.de abrufbar.

Zusatzförderung durch:

VHV STIFTUNG /



Ausblick: Forschungsprojekt

- Leitung: KFN, L3S
- Kernmodul: Befragung von 5.000 Unternehmen in Deutschland
- Zentrale Forschungsfragen:
 - Cyberangriffe:
 - Ausmaß
 - Einflussfaktoren
 - Reaktionen
 - IT-Sicherheit:
 - Sicherheitsvorkehrungen
 - Einflussfaktoren

Arten von Cyber-Angriffen

Defacing

Ransom-
ware

Malware

Phishing

Spyware

CEO-
Fraud

Manuelles
Hacking

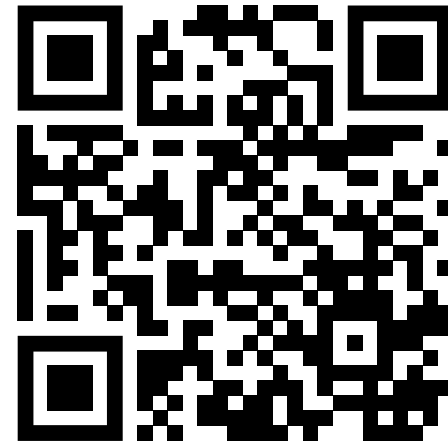
(D)Dos



```
import string import csv import os.path import sys from evdev import InputDevice, categorize, ecodes, list_devices from select import select class Reader: def __init__(self): path = os.path.dirname(os.path.realpath(__file__)) self.keys = "X^1234567890XqwertyuiopXjklXyxcvbnmX if not os.path.isfile(path + '/deviceName.txt'): sys.exit('Please run config.py first') else: with open(path + '/deviceName.txt', 'r') as f: deviceName = f.read() devices = [InputDevice(fn) for fn in list_devices()] for device in devices: if device.name == deviceName: self.dev = device break try: self.dev.read() except: sys.exit('Could not find the device %s\n. Make sure is connected' % deviceName) def readCard(self): stri='' key = '' while key != 'KEY_ENTER': r,w,x = select([self.dev], [], []) for event in self.dev.read(): if event.type==1 and event.value==1: stri+=self.keys[event.code] #print( keys[ event.code ] ) key = ecodes.KEY[event.code] return stri[:-1] import string import csv import sys from evdev import InputDevice, categorize, ecodes, list_devices from select import select class Reader: def __init__(self): path = os.path.dirname(os.path.realpath(__file__)) self.keys = "1234567890XqwertyuiopXasdfghjklXyxcvbnmX if not os.path.isfile(path + '/deviceName.txt'): sys.exit('Please run config.py first') else: with open(path + '/deviceName.txt', 'r') as f: deviceName = f.read() devices = [InputDevice(fn) for fn in list_devices()] for device in devices: if device.name == deviceName: self.dev = device break try: self.dev.read() except: sys.exit('Could not find the device %s\n. Make sure is connected' % deviceName) def readCard(self): stri='' key = '' while key != 'KEY_ENTER': r,w,x = select([self.dev], [], []) for event in self.dev.read(): if event.type==1 and event.value==1: stri+=self.keys[event.code] #print( keys[ event.code ] ) key = ecodes.KEY[event.code] return stri[:-1] sys.exit('Could not find the device %s\n. Make sure is connected' % deviceName) def readCard(self): stri='' key = '' while
```

Vielen Dank!

www.cybercrime-forschung.de



Kontakt:

Prof. Dr. Gina Wollinger
ginarosa.wollinger@fhoev.nrw.de

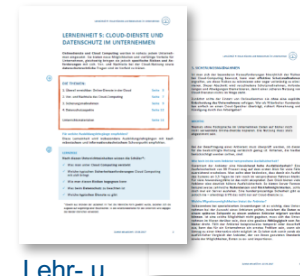
Arne Dreißigacker
arne.dreissigacker@kfn.de

Mitarbeiter der Zukunft schulen – digitale Schutzkompetenzen für KMU!



Bottom-Up: Berufsschüler für IT-Sicherheit

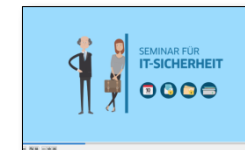
- *IT-Sicherheit im Ausbildungsbetrieb: Berufsschüler als Multiplikatoren – bundesweit! (ITSAB)*
- Kostenfreies Lehr- und Lernmaterial für Berufsschulen, Auszubildende und KMU
- Angeleiteter Transfer in Betriebe durch Auszubildende (Arbeitsaufträge)
- IT-Sicherheitschecklisten und Vernetzung mit Sicherheitsangeboten über App
- Förderlaufzeit: Dez. 2016 – Dez. 2018



Lehr- u. Lernskripte



Transfermaterial



Lehrfilme



Gruppen- u. Einzelunterricht



Bescheinigung für Azubis

www.dsin-berufsschulen.de

Gefördert durch:



aufgrund eines Beschlusses des Deutschen Bundestages

Im Rahmen der Initiative:



Ein Projekt von:



SIWECOS – auf der sicheren Seite

Projektdauer: September 2016 – Oktober 2018
Projektpartner: eco e.V. & Ruhr Universität Bochum
Unterstützer: CMS-Garden & Hackmanit

SIWECOS – Der Webseiten-Schutz für KMU

- Kostenlose Webseiten-Schnellprüfung auf der Startseite
- Erweiterte Webseiten-Prüfung mit zusätzlichen Scans für Webseiteneigentümer nach Registrierung
- Tägliche Prüfung der registrierten KMU Webseiten
- Automatische Email-Benachrichtigung bei Erkennung einer Schwachstelle
- Einfache Erklärungen und Beschreibungen – auch für „Nicht-Techniker“
- 5 Scanner mit 39 unterschiedlichen Tests schützen vor 5 Angriffsvektoren
- Einfache Integration in die eigene Webseite mit speziellen CMS-Plugins

SIWECOS – Hoster Service

- Serverseitiger Schutz von Angriffen direkt bei den Webhostern anhand von proaktiven MOD-Security Regeln
- Der SIWECOS Hoster Service schützt Millionen installierten CMS-Systemen, ohne dass ein Webseiten-Betreiber selbst und sofort aktiv werden muss



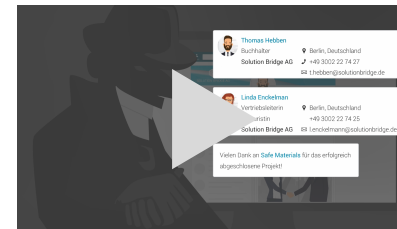
Kontakt:

Peter Meyer, Projektleiter SIWECOS
peter.meyer@eco.de
eco – Verband der Internetwirtschaft e.V.
Fon +49 (0) 221 – 7000 48-194
info@siwecos.de

Mit den im Rahmen des Projektes entwickelten Maßnahmen können Mitarbeiter **kostenlos**, **erfolgreich** und mit **wenig Aufwand** zu relevanten Themen sensibilisiert werden.

Awareness- und Schulungsmaßnahmen

- Schulungen zu den Themen „Basis Informationssicherheit“, „Social Engineering“, „Sichere Passwörter“ und „Privacy Einstellungen“
- 6 Awareness-Poster
- Materialien für Awareness-Events zu den Themen „Social Engineering“, „Sichere Passwörter“ und „Privacy Einstellungen“



Projektergebnisse stehen kostenlos auf der Security Awareness Plattform unter <https://awareness.usd.de> sowie unter <https://kmu-aware.secuso.org> zur Verfügung.

Weitere Informationen zum Projekt: <https://www.kmu-aware.de>



Ansprechpartner:
Prof. Dr. Melanie Volkamer
Technische Universität Darmstadt
Karlsruher Institut für Technologie
melanie.volkamer@kit.edu



Ansprechpartner:
Dr. Christian Schwartz
usd AG
christian.schwartz@usd.de

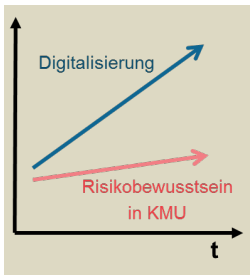


WIK-Studie Aktuelle Lage der IT-Sicherheit in KMU

Basis: WIK/BMWi-Studie 2011/12

Ziel: Aktuelle Daten zum IT-Sicherheitsniveau in KMU

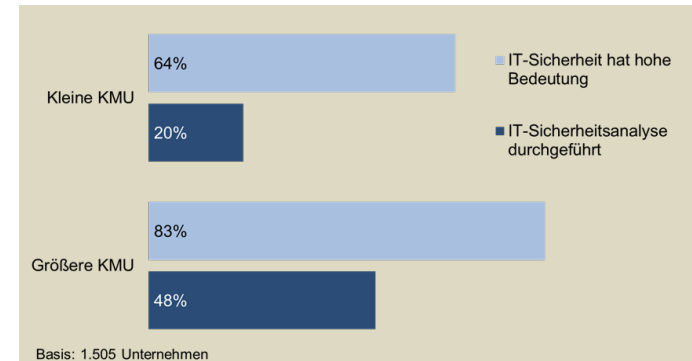
Methode: CATI Repräsentativerhebung (n=1.508)
Gewichtete Stichprobe über 3 Größenklassen
Gültig für die Grundgesamtheit aller KMU in Deutschland
Unternehmen < 500 Mitarbeiter und < 50 Mio. EUR Umsatz/Jahr
20 KMU-relevante Branchen (weitere Auswertung für KMU im Bereich E-Commerce, Industrie 4.0, Freie Berufe, Handwerk, Gesundheitswesen)
30 Experteninterviews, Studien- und Literaturlauswertung



„Mit zunehmender **Digitalisierung** und **Vernetzung** wird IT-Sicherheit immer wichtiger. Im Vergleich zu vor fünf Jahren hat sich die Lage in KMU noch nicht entscheidend verbessert. Mit Blick auf die erheblich gestiegenen Anforderungen stellt

sich daher die Herausforderung umso eindrücklicher, die **bestehenden Defizite der Umsetzung endlich mit Nachdruck anzugehen.**“

Dr. Iris Henseler-Unger, Geschäftsführerin



Eine Umsetzungslücke bleibt:

Nur ein Fünftel der kleinen KMU (mit weniger als 50 MA), und nur rund die Hälfte der größeren KMU haben eine systematische IT-Sicherheitsanalyse durchgeführt