DPT

Deutscher Präventionstag –
der Jahreskongress seit 1995

*Cybercrime gegen Privatnutzer*innen: Ausmaß und Prävention. Erste Ergebnisse einer Befragung von Privatnutzer*innen in Niedersachsen*

Anna Isenhardt
Philipp Müller
Gina Rosa Wollinger

Aus: Claudia Heinzelmann and Erich Marks (Hrsg.):
Prävention orientiert! ... planen ... schulen … austauschen ...
Ausgewählte Beiträge des 26. Deutschen Präventionstages
Forum Verlag Godesberg GmbH 2023

978.3.96410.030.6 (Printausgabe)
978.3.96410.031.3 (eBook)

Anna Isenhardt, Philipp Müller, Gina Rosa Wollinger

Cybercrime gegen Privatnutzer*innen: Ausmaß und Prävention

Erste Ergebnisse einer Befragung von Privatnutzer*innen in Niedersachsen

1. Einleitung und Begriffsbestimmung

Die Nutzung des Internets ist ein fester Bestandteil im Leben vieler Menschen. So nutzten im ersten Quartal des Jahres 2020 rund 90,0 % der Personen ab zehn Jahren das Internet. Ihr Anteil nahm seit 2010 stetig zu (Statistisches Bundesamt, 2020). Im Internet stehen den Nutzer*innen eine Vielfalt von Verwendungsmöglichkeiten zur Verfügung. Es kann zur Kommunikation oder zur Unterhaltung genutzt werden, aber auch zum Einkaufen oder um Videospiele zu spielen. Mit zunehmender Nutzung steigen jedoch auch die Möglichkeiten, Opfer von Straftaten zu werden.

Welche Delikte und Verhaltensweisen konkret unter dem Begriff Cybercrime zusammengefasst werden, ist nicht eindeutig festgelegt. Eine allgemeine Definition wurde von Huber (2019) erstellt, der zufolge man unter Cybercrime „alle Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik (IKT) oder gegen diese begangen werden" (ebd., S. 12) versteht. Das Bundeskriminalamt (BKA) unterscheidet zudem zwischen Cybercrime im engeren und Cybercrime im weiteren Sinn (siehe BKA 2017, S. 4ff). Cybercrime im engeren Sinn umfasst alle Delikte, die einen direkten Angriff auf IT-Strukturen darstellen. Beispiele sind Malware (Schadsoftware wie bspw. Viren, Würmer, Trojanische Pferde), Ransomware (Verschlüsselungssoftware, auch Erpressungssoftware genannt) oder die Ausspähung und das Abfangen von Daten. Cybercrime im weiteren Sinn meint hingegen Delikte, bei denen das Internet das Tatmittel und nicht das Tatziel ist. Diese Art von Delikten haben eine Offline-Entsprechung. Beispiele für diese Gruppe von Delikten sind insbesondere online stattfindender Warenkreditbetrug, aber auch Verhaltensweisen, die einen Aspekt von Cybermobbing oder Cyberstalking darstellen können.

Hellfelddaten weisen auf eine steigende Verbreitung von Cybercrimedelikten hin. So wurde laut der im Bundeslagebild des Bundeskriminalamts veröffentlichten Daten für Cybercrime im engeren Sinn eine Zunahme von 7,9 % vom Jahr 2019 auf das Jahr 2020 verzeichnet, für Cybercrime im weiteren Sinn betrug der Anstieg 8,7 % (BKA 2020, S. 38). Die in der Polizeilichen Kriminalstatistik registrierten Fälle stellen jedoch immer nur die Spitze des sprichwörtlichen Eisberges dar, wobei insbesondere bei Cyber-crimedelikten ein besonders großes Dunkelfeld vermutet wird. Gründe dafür sind, vor allem im Bereich Cybercrime im engeren Sinn, dass ein großer Teil der Straftaten aufgrund technischer Sicherungsmaßnahmen im Versuchsstadium abgewehrt werden oder Betroffene ihre Opferwerdung nicht bemerken, wenn beispielsweise ein Identitätsdiebstahl stattgefunden hat oder die technischen Geräte von Nutzern für die Begehung von Cybercrime missbraucht werden (z.B. als Teil eines Botnetzes zur Ausführung von DDoS-Angriffen; siehe BKA 2020 S. 9). Auch werden Straftaten aus dem Bereich Cybercrime eher selten angezeigt, insbesondere, wenn kein finanzieller Schaden entstanden ist oder ein eingetretener Schaden anders reguliert wurde, z.B. durch eine*n Plattformanbieter*in wie Ebay (ebd. sowie Dreißigacker 2016). Dunkelfeldstudien zur Betroffenheit von Privatnutzer*innen liegen bezogen auf Deutschland u.a. als Teil von Repräsentativbefragungen zu unterschiedlichen Kriminalitätsbereichen vor. So ergab bspw. eine Befragung des Landeskriminalamts Schleswig-Holstein, an der insgesamt 13.070 Einwohner*innen Schleswig-Holsteins ab 16 Jahren teilnahmen, dass insgesamt 16.7 % derjenigen Befragten, die das Internet privat nutzen, angaben, im Jahr 2014 Opfer von computerbezogener Kriminalität (Datenverlust durch Viren, Missbrauch persönlicher Daten, Phishing, Betrug im Internet) geworden zu sein (Dreißigacker 2016, S. 23f). Eine weitere Dunkelfeldbefragung, die auch ein Sondermodul zum Thema Cybercrime enthielt und bei der ebenfalls Personen ab 16 Jahren befragt wurden, wurde vom Landeskriminalamt Niedersachsen durchgeführt. Von den 16.137 Personen, die angaben, das Internet zu nutzen, wurde etwa ein Viertel bereits Opfer von computerbezogener Kriminalität (im engeren sowie im weiteren Sinn), wobei der größte Anteil einen Datenverlust durch Viren erlitt (rund 11,0 %; Pfeiffer et al. 2020, S. 26 f). Bundesweite Daten liefert z.B. der Deutsche Viktimisierungssurvey 2017. Befragt wurden 31.192 Personen ab 16 Jahren. Den Ergebnissen zufolge gaben 4,5 % der Befragten an, in den zwölf Monaten vor der Befragung durch Schadsoftware geschädigt worden zu sein, 0,8 % durch

Phishing[1] und 0,5 % durch Pharming[2] (Birkel et al., 2019, S. 18). Eine etwas früher, ebenfalls bundesweit durchgeführte Umfrage des Digitalverbands Bitkom (2016), in dessen Auftrag eine Befragung von 1.017 Internetnutzer*innen stattfand, kommt zu dem Ergebnis, dass in Deutschland rund 47,0 % der Internetnutzer*innen im vorausgegangenen Jahr Opfer von Cybercrime geworden sind, wobei Cybercrime im engeren Sinn mit ausspionierten Daten, Betrugsdelikten, Cybermobbing und sexueller Belästigung zusammengefasst wurde. Aus den Ergebnissen des Digitalbarometers 2019, bei dem 2.000 Personen zwischen 16 und 69 Jahren befragt wurden (Bundesamt für Sicherheit in der Informationstechnik & Polizeiliche Kriminalprävention der Länder und des Bundes 2019, S. 4), geht hervor, dass rund 24,0 % der Befragten bereits Opfer von Straftaten im Internet geworden ist. Besonders verbreitet waren Betrug beim Onlineshopping (rund 36,0 %), Phishing (rund 28,0 %) sowie Angriffe mit Schadsoftware wie Viren oder Trojanern (rund 26,0 %). Im Jahr 2020 zeigte sich ein ähnliches Bild (Bundesamt für Sicherheit in der Informationstechnik & Polizeiliche Kriminalprävention der Länder und des Bundes 2020, S. 3). Befragt wurden erneut 2.000 Personen, wobei im Vergleich zu 2019 Internetnutzer*innen zwischen 14 und 69 Jahren befragt wurden. Rund 25,0 % waren bereits Opfer von Kriminalität im Internet, davon jede*r vierte in den letzten zwölf Monaten vor der Befragung. Das verbreitetste Delikt war wiederum der Online-Betrug.

Von 2019 bis 2021 widmete sich das Kriminologische Forschungsinstitut Niedersachsen e.V. in einem vom Förderprogramm Pro*Niedersachsen geförderten Projekt vertieft dem Thema Cybercrime gegen Privatnutzer*innen und adressiert über die Beschreibung der Verbreitung von Cybercrime hinaus verschiedene weitere Forschungsfragen. Der Fokus liegt dabei auf Niedersachsen. Ziel des Projektes ist zunächst die Untersuchung der Verbreitung von Cybercrime im engeren und im weiteren Sinn. Zentral ist neben Viktimisierungserfahrungen auch die Frage nach den Täterschaften. Untersucht werden sollen außerdem Risikofaktoren für die Opferwerdung durch Cybercrime, psychische Folgen von Cybercrime und die Reaktionen von betroffenen Personen, insbesondere im Zusammenhang mit der Anzeigebereitschaft und der Erfahrung mit den Strafermittlungsbehörden. Ein weiterer Schwerpunkt liegt auf den Täter*innen-Opfer-Beziehungen. Das Projekt besteht aus zwei Modulen: Erstens, eine Befragung von 10.000 Einwohner*innen ab 16 Jahre in

1 „Pishing" bezeichnet die Beschaffung persönlicher Daten wie bspw. Passwörter oder Kreditkartennummern mit Hilfe gefälschter E-Mails.

2 „Pharming" bedeutet die Beschaffung persönlicher Daten wie bspw. Passwörter oder Kreditkartennummern durch das Umleiten auf gefälschte Internetseiten.

Niedersachsen und zweitens, 20 qualitative Interviews mit Opfern von Cybercrimedelikten, um insbesondere Reaktionen auf Opferwerdungen noch vertiefter zu beleuchten.

Im vorliegenden Beitrag werden erste Ergebnisse der niedersachsenweiten Befragung von Privatnutzer*innen präsentiert. Dabei wird zunächst dargestellt, wie das Internet von den Befragten genutzt wird und wie häufig die Befragten Opfer durch beide Formen von Cybercrime (Cybercrime im engeren und Cybercrime im weiteren Sinn) geworden sind. Anschließend werden Unterschiede zwischen der Häufigkeit der Opferwerdung nach Alter, Geschlecht, Schulabschluss und Gemeindegröße untersucht sowie das Anzeigeverhalten näher betrachtet, wobei ein besonderer Fokus auf den Gründen für eine Nichtanzeige liegt.

2. Methodisches Vorgehen

Die Datenbasis für die Analysen bildet eine repräsentative Dunkelfeldbefragung von 10.000 Einwohner*innen ab 16 Jahren in Niedersachsen, die im Jahr 2020 vom Kriminologischen Forschungsinstitut Niedersachsen e.V. durchgeführt wurde. Für die Befragung wurde ein zweistufiges Zufallsstichproben-Verfahren angewandt. Dazu wurde das Land Niedersachsen zunächst in die vier Regionen Braunschweig, Hannover, Weser-Ems und Lüneburg eingeteilt und in diesen insgesamt 73 Gemeinden zufällig ausgewählt. Innerhalb dieser Gemeinden wurde in einem zweiten Schritt durch die zuständigen Einwohnermeldeämter wiederum eine zufällige Auswahl von Einwohner*innen ab 16 Jahren getroffen. Diese zufällig ausgewählten Befragungsteilnehmer*innen wurden anschließend angeschrieben und ihnen ein 16-seitiger Fragebogen zugesandt. Nach ca. zwei Wochen erhielten die Befragten ein Erinnerungs- bzw. Dankesschreiben. Zusätzlich wurde ein monetärer Anreiz in Form eines 5-Euro-Scheines eingesetzt, der an den Fragebogen geheftet war. Dem Anschreiben lag ein frankierter Rückumschlag bei. Die Befragungsteilnehmer*innen hatten ferner die Möglichkeit, den Fragebogen online auszufüllen. Von den 10.000 zufällig ausgewählten Adressen waren 364 ungültig (verzogen, verstorben usw.). Auswertbare Fragebögen lagen letztendlich von 4.102 Personen vor.

2. 1 Beschreibung der Stichprobe

Die Daten wurden nach Alter, Geschlecht und Gemeindegröße gewichtet, so dass alle im Nachfolgenden dargestellten Ergebnisse auf gewichteten Daten basieren. 51,7 % der 4.102 Befragten sind weiblich, 48,2 % männlich und 0,1 % haben divers bei der Frage nach dem Geschlecht angegeben. Das Durchschnittsalter beträgt 50,2 Jahre, das Alter der Befragten reicht von 16 bis 98 Jahren. Der Großteil der befragten Personen lebt in einer Gemeinde mit 5.000 bis 19.999 Einwohner*innen (30,7 %) sowie 20.000 bis 49.999 Einwohner*innen (22,4 %). 13,9 % der Befragten lebt in einer Gemeinde mit 100.000 bis 499.999 Einwohner*innen, 11,9 % in einer Gemeinde mit 2.000 bis 4.999 Einwohner*innen, 8,0 % in einer Gemeinde unter 2.000 Einwohner*innen sowie 7,7 % in einer Gemeinde mit 50.000 bis 99.999 Einwohner*innen und 5,4 % der befragten Personen in einer Gemeinde ab 500.000 Einwohner*innen. 31,5 % der Befragten haben einen Realschul- oder gleichwertigen Abschluss, 30,2 % Abitur bzw. allgemeine oder fachgebundene Hochschulreife, 20,2 % einen Hauptschul- oder gleichwertigen Abschluss. 11,9 % der Befragten verfügen über Fachhochschulreife, 3,1 % sind Schüler*innen. 1,4 % der Befragten haben keinen Schulabschluss, 1,7 % einen sonstigen Abschluss.

2. 2 Operationalisierung von Cybercrime

Um Cybercrime-Viktimisierung zu erfassen, wurde hinsichtlich Cybercrime im engeren Sinn und Cybercrime im weiteren Sinn unterschieden. Für Cybercrime im engeren Sinn wurden fünf Formen von Opfererfahrungen erhoben. In Anlehnung an die Studie von Pfeiffer et al. (2020) wurden die Befragungsteilnehmer*innen gefragt, ob sie Datenverlust bzw. Datenbeschädigung durch Malware erfahren haben oder ob ihr Onlinebanking angegriffen wurde. In Anlehnung an das Digitalbarometer 2019, einer Bürgerbefragung zur Cyber-Sicherheit (Bundesamt für Sicherheit in der Informationstechnik & Polizeiliche Kriminalprävention der Länder und des Bundes 2019), wurde erhoben, ob bei jemandem vertrauliche Daten wie Passwörter, Zugangsdaten oder Kreditkartennummern durch gefälschte E-Mails oder Internetseiten ausspioniert sowie ob der Zugang zum Computer oder mobilen Geräten durch Schadsoftware gesperrt und die Person aufgefordert wurde, Geld zu bezahlen, damit sie wieder auf alles zugreifen kann (sog. Ransomwareangriff). Zusätzlich wurde in Anlehnung an den Eurobarometer (European Commission, Brussels 2018) gefragt, ob ein Konto in den Sozialen Medien oder das E-Mailkonto gehackt wurde.

Zur Messung von Cybercrime im weiteren Sinn wurden die im Folgenden aufgeführten Aspekte erfasst. Dabei handelt es sich nicht immer um strafbare Handlungen im eigentlichen Sinn. In Anlehnung an Sitzer et al. (2012; siehe auch Bergmann et al. 2019) wurden die Befragungsteilnehmer*innen gefragt, ob sie jemand im Internet verspottet, beleidigt, beschimpft oder bedroht hat, jemand über sie Gerüchte verbreitet oder schlecht geredet hat, von ihnen private Nachrichten, vertrauliche Informationen oder Fotos ins Internet gestellt wurden, um sie bloßzustellen oder ob sie online aus einer Gruppe ausgeschlossen wurden (zusammengefasst können diese Items genutzt werden, um Cyberbullying abzubilden). Sexuelle Belästigung bzw. sexuelles Cyberbullying wurde ebenfalls in Anlehnung an Sitzer et al. (2012) erfasst. Dazu wurde gefragt, ob den Befragten ungewollt online sexuelle Fotos oder Videos zugeschickt oder ob sie ungewollt online zu sexuellen Handlungen aufgefordert wurden. Außerdem wurde erfasst, ob jemand schon mal einen Shitstorm erlebt hat. Das Item, mit dem dies gemessen wurde, ist angelehnt an Bergmann et al. (2016). Analog zu einer Studie von Reyns (2010) zum Thema Cyberstalking wurde erfasst, ob die Befragten von jemandem mehr als einmal kontaktiert wurden, nachdem sie gebeten hatten, damit aufzuhören sowie ob ihnen gegenüber mehrmals ungewollte sexuelle Annäherungsversuche unternommen wurden. Weiterhin wurden die Befragungsteilnehmer*innen gefragt, ob sie beim Kauf oder Verkauf von Waren oder Dienstleistungen betrogen wurden (vgl. Pfeiffer et al. 2020) sowie ob jemand ihre persönlichen Daten gestohlen und sich als sie ausgegeben hat (Identitätsdiebstahl; vgl. European Commission, Brussels 2018). Im Rahmen der Viktimisierung durch Cybercrime im weiteren Sinn wurde außerdem Hate Speech erhoben. In Anlehnung an Wachs und Wright (2018) wurde erfasst, ob die Befragungsteilnehmer*innen online wegen ihres Geschlechts, nationalen Herkunft, Hautfarbe, Religionszugehörigkeit oder sexuellen Orientierung viktimisiert wurden. Für die nachfolgende Analyse wurde Hate Speech allerdings nicht berücksichtigt.

Für alle zuvor aufgeführten Cybercrime-Erfahrungen wurden Lebenszeit-Prävalenzen erfasst, d.h. ob die Befragungsteilnehmer*innen die jeweilige Verhaltensweise mindestens einmal in ihrem Leben erfahren haben. Weiterhin wurden Jahresprävalenzen bestimmt, d.h. die Häufigkeit der Opferwerdung im Jahr vor dem Befragungszeitraum.

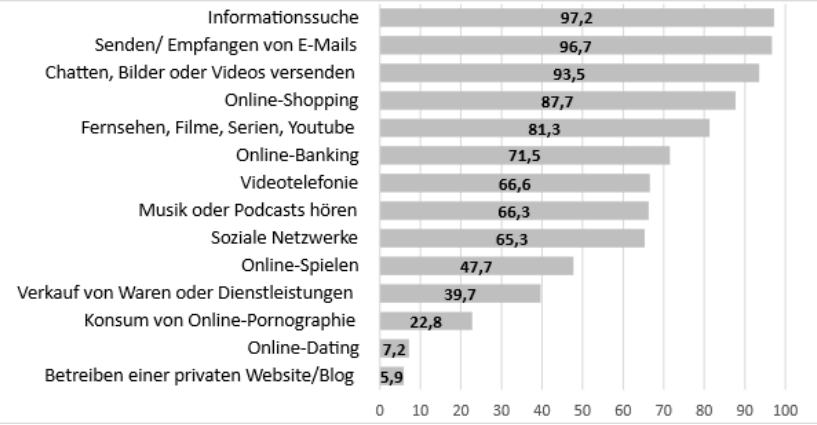
3. Ergebnisse

Die Befragungsteilnehmer*innen wurden zunächst gefragt, ob sie das Internet privat nutzen. 88,3 % der Befragten (n=3.623) bejahten dies. Die nachfolgend präsentierten Ergebnisse der Analyse beziehen sich auf die 3.623 Personen, die das Internet privat nutzen.

3. 1 Nutzungsverhalten

Die Befragungsteilnehmer*innen wurden weiter gefragt, wozu sie das Internet nutzen. In Anlehnung an eine Befragung des Statistischen Bundesamts (2021) wurden die Befragten gebeten einzuschätzen, für welche privaten Zwecke und wie häufig sie das Internet innerhalb eines typischen Monats vor der Corona-Krise genutzt haben (siehe Abbildung 1). Der Großteil der Befragten nutzt das Internet zur Informationssuche (97,2 %), zum Senden bzw. Empfangen von E-Mails (96,7 %) sowie zum Chatten, Bilder oder Videos Versenden (93,5 %). Weiterhin nutzen 87,7 % der Befragten das Internet für Onlineshopping, 81,3 % zum Anschauen von Filmen, Serien, Youtube oder Fernsehen und 71,5 % betreiben Online-Banking. Etwa zwei Drittel der Befragten nutzen Videotelefonie (66,6 %) sowie Soziale Netzwerke (65,3 %). Für Online-Dating nutzen nur 7,2 % der befragten Personen das Internet (siehe Abbildung 1 für weitere Nutzungsarten).

Abbildung 1: Internetnutzung innerhalb eines typischen Monats vor der Corona-Krise (gewichtete Daten, Anteile mind. 1-2 mal pro Monat bis täglich)



3. 2 Verbreitung von Cybercrime im engeren und im weiteren Sinn

Tabelle 1 zeigt die Lebenszeit- sowie Jahresprävalenzen für Cybercrime-Viktimisierungen für die beiden Cybercrime-Formen. Für Cybercrime im engeren Sinn wurde ein Gesamtindex gebildet, der die fünf zuvor dargestellten Verhaltensweisen und Einzeldelikte umfasst. Für Cybercrime im weiteren Sinn wurde dies analog dazu mit den weiteren elf Verhaltensweisen durchgeführt. 29,7 % der Befragten wurden in ihrem Leben mindestens einmal durch eine Verhaltensweise von Cybercrime im engeren Sinn viktimisiert. 13,9 % der Befragten erlebten dies mindestens einmal in den zwölf Monaten vor der Befragung. Cybercrime im weiteren Sinn ist im Vergleich zu Cybercrime im engeren Sinne etwas verbreiteter. Hier wurden 37,3 % der befragten Personen in ihrem Leben mindestens einmal viktimisiert, 24,5 % mindestens einmal in den zwölf Monaten vor dem Befragungszeitraum. Demnach ist in den zwölf Monaten vor der Befragung ungefähr jede*r vierte Befragte in irgendeiner Form durch Cybercrime im weiteren Sinn viktimisiert worden, durch Cybercrime im engeren Sinn nur knapp jede*r siebte Befragte.

Tabelle 1: Lebenszeit- und Jahresprävalenzen der Cybercrime-Viktimisierungen (gewichtete Daten, Anteile mind. einmal erlebt)

	Lebenszeitprävalenz	Jahresprävalenz
Cybercrime im engeren Sinn	29,7 % (Hk 1039; n=3495)	13,9 % (Hk 459; n=3293)
Cybercrime im weiteren Sinn	37,3 % (Hk 1309; n=3510)	24,5 % (Hk 798; n=3255)

Wenn die Jahresprävalenzen für die einzelnen Deliktformen von Cybercrime im engeren Sinn betrachtet werden, zeigt sich, dass 5,4 % der Befragten angaben, einen Datenverlust durch Viren, Trojaner oder Würmer erfahren zu haben. Das Konto in sozialen Medien bzw. das E-Mailkonto wurde bei 6,5 % der Befragten in den zwölf Monaten vor der Befragung gehackt. 4,9 % gaben an, dass bei ihnen vertrauliche Daten wie Passwörter, Zugangsdaten oder Kreditkartennummern durch gefälschte E-Mails oder Internetseiten ausspioniert wurden (Phishing). Einen Ransomwareangriff haben 2,4 % der befragten Personen im Jahr vor der Befragung erlebt. Bei nur 1,1% der Befragten wurde in den zwölf Monaten vor der Befragung das Online-Banking angegriffen.

Analog dazu wurden auch die Jahresprävalenzen für die einzelnen Verhaltensweisen von Cybercrime im weiteren Sinn betrachtet. Online verspottet, beleidigt, beschimpft oder bedroht wurden 6,4 % der Befragten

im Jahr vor der Befragung. 3,0 % gaben an, dass über sie im Internet Gerüchte verbreitet oder schlecht geredet wurde. Von 0,8 % wurden private Nachrichten, vertrauliche Informationen, Fotos oder Videos ins Internet gestellt bzw. versendet, um sie bloßzustellen. Online aus einer Gruppe ausgeschlossen wurden 3,3 % der Befragten und 7,2 % gaben an, dass sie mehr als einmal online kontaktiert wurden, nachdem sie die Person aufgefordert haben, damit aufzuhören. Einen Shitstorm erlebten 1,6 % in den zwölf Monaten vor der Befragung. 2,0 % der Befragten wurden durch Identitätsdiebstahl viktimisiert. Mehrmalige ungewollte sexuelle Annäherungsversuche erlebten 7,1 % der Befragten, ungewollt sexuelle Fotos oder Videos zugeschickt bekamen 7,9 % und 2,3 % gaben an, dass sie ungewollt zu sexuellen Handlungen über das Internet aufgefordert wurden. Am häufigsten wurde Kredit- bzw. Warenbetrug genannt. 8,4 % der Befragten gaben an, dass sie in den zwölf Monaten vor der Befragung mindestens einmal beim Kauf oder Verkauf von Waren oder Dienstleistungen im Internet betrogen worden waren.

3. 3 Unterschiede nach Geschlecht, Alter, Schulabschluss und Gemeindegröße

Der folgende Abschnitt beschäftigt sich mit Unterschieden in der Häufigkeit der Viktimisierung nach verschiedenen soziodemografischen Variablen, namentlich nach Geschlecht, Alter, Schulabschluss und Gemeindegröße. Geprüft wurde mit Hilfe von Chi-Quadrat-Tests, jeweils getrennt für Cybercrime im engeren und Cybercrime im weiteren Sinn, ob signifikante Unterschiede nach den genannten Variablen bestehen. Angesetzt wurde dabei ein Signifikanzniveau von 5 %. Untersucht wurden sowohl Unterschiede für die Lebenszeit- und Jahresprävalenzen insgesamt (Zusammenfassung einzelner Delikte und Verhaltensweisen in (1) Cybercrime im engeren Sinn und (2) Cybercrime im weiteren Sinn) als auch für die Jahresprävalenzen der in Abschnitt 5.2 aufgeführten einzelnen Delikte und Verhaltensweisen. In Tabelle 2 ist dargestellt, für welche soziodemografischen Variablen signifikante Unterschiede gefunden wurden (Lebenszeit- sowie Jahresprävalenzen insgesamt und/oder einzelne Delikte/Verhaltensweisen), wobei ein Häkchen das Vorhandensein mindestens eines signifikanten Unterschieds symbolisiert, während ein Kreuz symbolisiert, dass keine signifikanten Unterschiede vorlagen. Angesprochen werden im Folgenden nur diejenigen Delikte und Verhaltensweisen, für die signifikante Unterschiede gefunden wurden.

Tabelle 2: Darstellung signifikanter Unterschiede

	Cybercrime im engeren Sinn	**Cybercrime im weiteren Sinn**
Geschlecht	☒	☑
Alter	☑	☑
Schulabschluss	☑	☑
Gemeindegröße	☒	☒

Zunächst einmal lässt sich festhalten, dass für Cybercrime im weiteren Sinn mehr signifikante Unterschiede nach den betrachteten Variablen gefunden wurden als für Cybercrime im engeren Sinn. Für Cybercrime im engeren Sinn bestanden keine signifikanten Unterschiede nach Geschlecht und Gemeindegröße, sowohl im Allgemeinen als auch in Bezug auf die Einzeldelikte. Beim Vergleich nach Altersgruppen wurde deutlich, dass jüngere Befragte eher stärker betroffen waren. Dieser Befund traf sowohl auf die Lebenszeit- sowie Jahresprävalenzen insgesamt als auch auf das Hacking von E-Mail-Accounts oder Konten bei Sozialen Medien sowie das Ausspionieren vertraulicher Daten wie Passwörter, Zugangsdaten oder Kreditkartennummern durch gefälschte E-Mails oder Internetseiten zu. Auch bezüglich des Schulabschlusses zeigten sich signifikante Unterschiede, jedoch nur bezüglich der Lebenszeitprävalenz und es konnte kein eindeutiger Trend beobachtet werden.

In Bezug auf Cybercrime im weiteren Sinn zeigten sich zunächst signifikante Unterschiede nach dem Geschlecht der Befragten. Bei Betrachtung der Lebenszeit- und Jahresprävalenz insgesamt und damit für die Zusammenfassung der als Cybercrime im weiteren Sinn definierten Delikte und Verhaltensweisen, wird deutlich, dass Männer im Vergleich zu Frauen etwas häufiger Opfer geworden sind. Betrachtet man jedoch die Einzeldelikte, zeigt sich ein etwas differenzierteres Bild. Von Beleidigungen und Bedrohungen waren Männer häufiger betroffen. Online kontaktiert bzw. versucht zu kontaktieren, nachdem sie darum gebeten haben, aufzuhören, wurden etwas mehr Frauen. Frauen berichteten auch häufiger über Opferwerdungen durch die von uns erfassten Handlungen aus dem Spektrum der sexuellen Belästigung bzw. des sexuellen Cyberbullyings (sexuelle Fotos/Videos geschickt, zu sexuellen Handlungen aufgefordert). Von Betrug beim Kauf/Verkauf von Waren waren Männer häufiger

betroffen. Bezüglich des Alters fanden sich ebenfalls Unterschiede. Jüngere waren häufiger betroffen und die Anteile an Personen, die nie eine der Verhaltensweisen aus dem Bereich Cybercrime im weiteren Sinn erlebt haben, wird mit zunehmendem Alter größer. Es zeigten sich signifikante Unterschiede bei allen Einzeldelikten, wobei immer jüngere im Vergleich zu älteren häufiger Opferwerdungen angaben. In Bezug auf den Schulabschluss war für die Lebenszeit- und Jahresprävalenzen im Allgemeinen kein eindeutiger Trend zu erkennen, bei den einzelnen Delikten und Verhaltensweisen hingegen schon. Von vielen der abgefragten Handlungen waren häufiger Personen betroffen, die angaben, noch zur Schule zu gehen. Dies trifft auf die folgenden Delikte und Verhaltensweisen zu: Beleidigung, Beschimpfung, Bedrohung, online aus einer Gruppe ausgeschlossen werden, Kontaktaufnahme, obwohl darum gebeten wurde, aufzuhören, sexuelle Annäherungsversuche, sexuelle Fotos/Videos geschickt sowie zu sexuellen Handlungen aufgefordert worden zu sein. Für die Gemeindegröße fanden sich, wie für Cybercrime im engeren Sinn, keine signifikanten Unterschiede zwischen den Befragten.

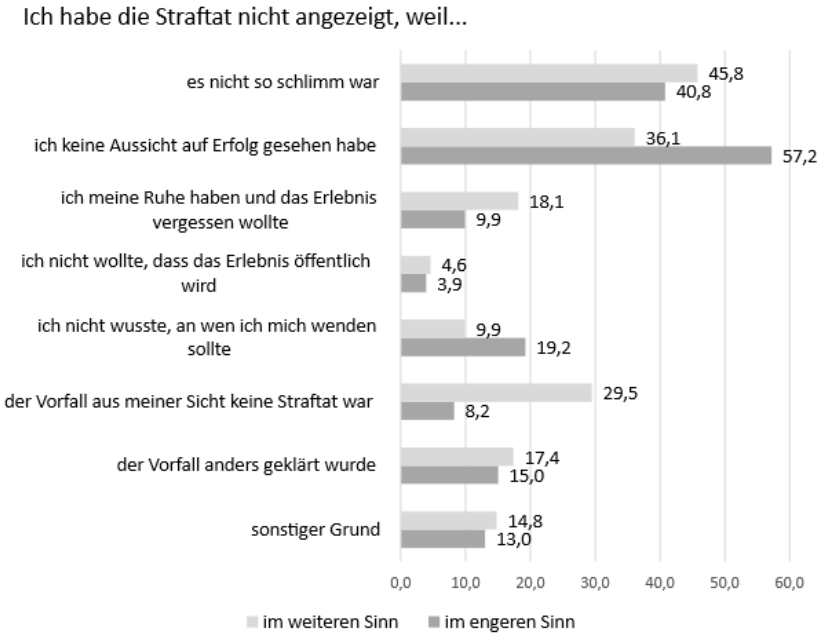
3. 4 Anzeigeverhalten

Weiterhin wurden die Befragungsteilnehmer*innen in Anlehnung an die Studie von Pfeiffer et al. (2020) gebeten, den letzten Vorfall anzugeben, den sie erlebt haben. Anschließend wurden sie u.a. gefragt, ob sie diesen angezeigt haben. Sie wurden außerdem gebeten, Gründe für die Nichtanzeige zu nennen. 1.284 Befragungsteilnehmer*innen haben einen letzten Vorfall angegeben. Bezüglich der Unterschiede der beiden Cybercrime-Formen lässt sich festhalten, dass im Fall von Cybercrime im engeren Sinn der letzte Vorfall von 9,4 % (N=392) der Befragten, die ein entsprechendes Delikt erlebt haben, angezeigt wurde. Für Cybercrime im weiteren Sinn wurde der letzte Vorfall hingegen von 16,2 % (N=857) der Befragten angezeigt.

Abbildung 2 zeigt die Gründe für eine Nichtanzeige des zuletzt erlebten Vorfalls für diejenigen Befragten, die angegeben haben, dass sie den Vorfall nicht angezeigt haben. Die Erfassung erfolgte ebenfalls in Anlehnung an Pfeiffer et al. (2020). Als häufigster Grund für eine Nichtanzeige wurde genannt, dass der letzte Vorfall als nicht so schlimm empfunden wurde. Für Cybercrime im engeren Sinn als zuletzt erlebten Vorfall haben dies 40,8 % der Befragten angegeben, für Cybercrime im weiteren Sinn 45,8 %. Keine Aussicht auf Erfolg wurde für Cybercrime im engeren Sinn von mehr als der Hälfte der Befragten angegeben (57,2 %), für Cybercrime im weiteren Sinn hingegen von 36,1 %. Dass jemand nicht wusste, an

wen man sich wenden sollte, wurde von 19,2 % (im engeren Sinn) bzw. 9,9 % (im weiteren Sinn) angeführt. Die Ansicht, dass es sich bei dem zuletzt erlebten Vorfall um keine Straftat handelte, wurde hingegen für Cybercrime im weiteren Sinn häufiger als Grund für eine Nichtanzeige genannt. Dies haben 29,5 % der Befragten angegeben, für einen Vorfall von Cybercrime im engeren Sinn hingegen lediglich 8,2 %. Ähnlich verhält es sich bei dem Grund, dass der*die Befragte seine Ruhe haben und das Erlebnis vergessen wollte.

Abbildung 2: Gründe für Nichtanzeige bezüglich des zuletzt erlebten Vorfalls in % (gewichtete Daten, Mehrfachantworten möglich, die Angaben beziehen sich nur auf die Befragten, die angegeben haben, dass sie den Vorfall nicht angezeigt haben)

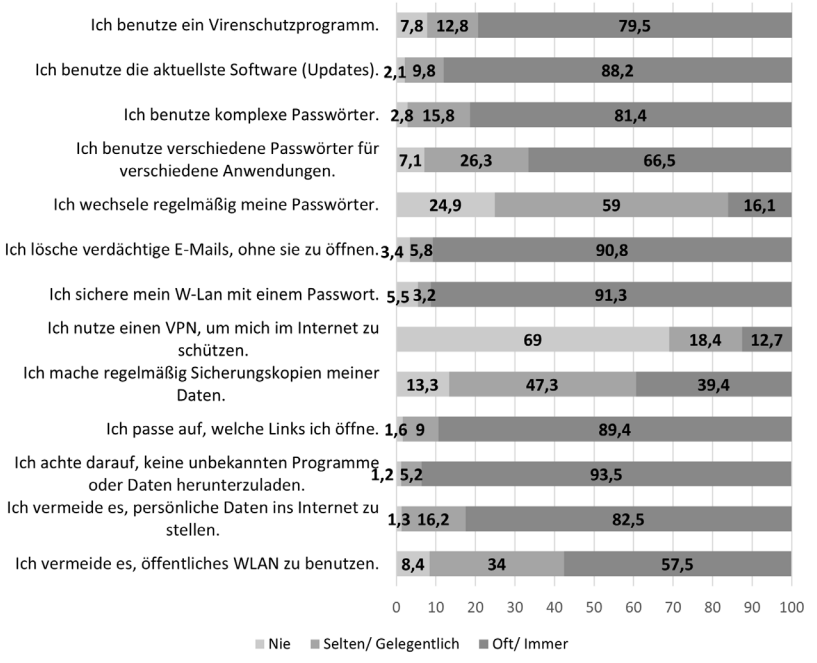


3. 5 Schutz- und Vermeideverhalten

Zusätzlich wurden die Befragungsteilnehmer*innen auch hinsichtlich ihres Schutz- bzw. Vermeideverhaltens bei der Internetnutzung befragt (siehe Abbildung 3). Wiederum in Anlehnung an die Studie von Pfeiffer et al. (2020) wurden sie gebeten, auf einer fünfstufigen Skala zu beantworten, welche Maßnahmen sie wie oft ergreifen, um sich im Internet vor

Kriminalität und Datenverlust zu schützen. 79,5 % der Befragten gaben an, dass sie oft bis immer ein Virenschutzprogramm nutzen. 12,8 % benutzen dies nur selten bis gelegentlich, 7,8 % nie. Komplexe Passwörter nutzen 81,4 % der Befragten oft bis immer, 15,8 % selten bis gelegentlich und 2,8 % nie. Dass sie ihr WLAN mit einem Passwort sichern, gaben 91,3 % der Befragungsteilnehmer*innen an, 3,2 % machen dies nur selten bzw. gelegentlich. Auffällig ist jedoch, dass 5,5 % der Befragten angaben, dass sie ihr WLAN nie mit einem Passwort sichern. Regelmäßige Sicherungskopien ihrer Daten machen nur 39,4 % der Befragten oft bis immer. 47,3 % machen dies nur selten bzw. gelegentlich und 13,3 % nie. Dass sie darauf achten, keine unbekannten Programme oder Daten herunterzuladen, gaben mit 93,5 % die meisten der Befragungsteilnehmer*innen an. Lediglich 5,2 % gaben an, dass sie dies nur selten bzw. gelegentlich tun, 1,2 % der Befragten nie. Der Großteil der Befragten achtet ebenso darauf, welche Links sie öffnen. 89,4 % machen dies oft bis immer, 9,0 % noch selten bis gelegentlich und 1,6 % nie.

Abbildung 3: Schutz- und Vermeideverhalten in % (gewichtete Daten)



4. Zusammenfassung und erste Ableitungen für die Prävention

Basierend auf einer Befragung von 10.000 Einwohner*innen Niedersachsens wurden im vorliegenden Beitrag Ergebnisse zur Verbreitung von Cybercrime zu Lasten von Privatnutzer*innen dargestellt. Berücksichtigt wurde sowohl Cybercrime im engeren als auch im weiteren Sinn. Unter Cybercrime im engeren Sinn werden Delikte zusammengefasst, bei denen IT-Strukturen das Tatziel sind (z.B. Angriffe durch Schadprogramme oder Ransomware), während bei Cybercrime im weiteren Sinn IT-Strukturen das Tatmittel sind (z.B. Warenkreditbetrug, Cyberbullying).

88,3 % der Befragten (n=3.623) haben angegeben, dass sie das Internet zu privaten Zwecken nutzen. Gefragt danach, wofür sie das Internet nutzen, wurde am häufigsten die Informationssuche, das Senden und Empfangen von E-Mails, Chatten sowie der Versand von Bildern oder Videos, Onlineshopping und Fernsehen und/oder Filme, Serien und Youtube schauen genannt. Von denjenigen Befragten, die das Internet privat nutzen, wurde in den zwölf Monaten vor der Befragung ungefähr jede*r vierte Befragte Opfer von irgendeiner Form von Cybercrime im weiteren Sinn sowie knapp jede*r siebte Befragte von Cybercrime im engeren Sinn. Auch bezüglich der Lebenszeitprävalenzen zeigen sich ähnliche Unterschiede; Viktimisierungen durch Cybercrime im weiteren Sinn kamen im Vergleich häufiger vor als durch Cybercrime im engeren Sinn. Die Anteile Betroffener insgesamt ähneln denen anderer Befragungen, wobei die Ergebnisse aufgrund unterschiedlicher Operationalisierungen nicht für alle Delikte direkt vergleichbar sind (Dreißigacker 2016; Bundesamt für Sicherheit in der Informationstechnik & Polizeiliche Kriminalprävention der Länder und des Bundes 2019; 2020; Pfeiffer et al. 2020). Bei Betrachtung der unter dem Oberbegriff Cybercrime im engeren Sinn zusammengefassten Delikte kamen Viktimisierungen durch das Hacking von E-Mailkonten und Konten in Sozialen Medien, Datenverluste oder Datenbeschädigungen durch Viren und das Ausspionieren von vertraulichen Daten am häufigsten vor. Bei Cybercrime im weiteren Sinn war es der Betrug beim Kauf oder Verkauf von Waren, das ungewollte Zusenden von Fotos oder Videos mit sexuellen Inhalten, die mehrmalige ungewollte Kontaktaufnahme, obwohl man darum gebeten hatte, dies zu unterlassen sowie mehrmalige ungewollte sexuelle Annäherungsversuche.

Es fanden sich einige signifikante Unterschiede zwischen den Befragten nach ihrem soziodemografischen Hintergrund. Besonders deutlich wurden die Unterschiede in Bezug auf Alter, Geschlecht und Schulabschluss

sowie in Bezug auf Delikte und Verhaltensweisen, die in den Bereich Cybercrime im weiteren Sinn fallen. So waren Männer insgesamt zwar häufiger von Cybercrime im weiteren Sinn betroffen, diese Betroffenheit bezog sich jedoch insbesondere auf den Betrug beim Kauf oder Verkauf von Waren sowie Beleidigung, Beschimpfung oder Bedrohung. Frauen wurden hingegen signifikant häufiger Opfer von sexueller Belästigung und sonstiger Belästigung. Sowohl von Cybercrime im engeren als auch im weiteren Sinn waren Jüngere häufiger betroffen als Ältere und die Anteile Nicht-Betroffener wurden mit zunehmendem Lebensalter größer. Zudem zeigte sich, dass von vielen Delikten und Verhaltensweisen aus dem Bereich Cybercrime im weiteren Sinn Schüler*innen häufiger Opfer wurden.

Bezogen auf den zuletzt erlebten Vorfall wurde auch nach dem Anzeigeverhalten gefragt und dabei zeigte sich, dass die gemachten Erfahrungen häufig nicht angezeigt wurden und bei Viktimisierungen durch Cybercrime im engeren Sinn seltener eine Anzeige erfolgte als bei Cybercrime im weiteren Sinn. Als Gründe für die Nichtanzeige wurde beispielsweise angegeben, dass der Vorfall nicht so schlimm gewesen sei, aber auch, dass die Befragten keine Aussicht auf Erfolg gesehen haben. Dies wurde für Cybercrime im engeren Sinn immerhin von jedem*jeder zweiten Befragten als Grund genannt. Auch äußerten einige Befragte, dass sie nicht gewusst hätten, an wen sie sich wenden sollten und zwar häufiger, wenn als letzter Vorfall ein Delikt aus dem Bereich Cybercrime im engeren Sinn angegeben wurde. Immerhin jeweils rund ein Siebtel (Cybercrime im engeren und im weiteren Sinn) gaben zudem an, dass der Vorfall anders geklärt wurde. Ähnliche Gründe für das Unterlassen einer Strafanzeige im Kontext von Cybercrime gaben auch Unternehmen als Opfer in einer deutschlandweit repräsentativen Umfrage an (Dreißigacker et al. 2020).

Zudem stellen nicht oder unzureichend geschützte IT-Strukturen ein Einfallstor für Cybercrimedelikte dar (BKA, 2020, S. 38). Die Ergebnisse der Befragung zeigen, dass sich eine überwiegende Mehrheit im Internet schützt und riskantes Verhalten und riskante Situationen vermeidet. Es haben jedoch auch immerhin noch 5,5 % angegeben, dass sie ihr WLAN nicht mit einem Passwort schützen, 13,3 % machen keine regelmäßigen Updates, 7,8 % nutzen kein Virenschutzprogramm, 7,1 % benutzen keine verschiedenen Passwörter für verschiedene Anwendungen und rund ein Viertel der Befragten wechseln ihre Passwörter nicht.

Auf der Grundlage der beschriebenen Ergebnisse lassen sich einige erste Ableitungen für die Prävention vornehmen. Zunächst einmal zeigen die Befunde, dass die Befragten je nach soziodemografischem Hintergrund unterschiedlich stark und auch von unterschiedlichen Delikten betroffen

sind. Dies spricht für den Ausbau und die Etablierung von Präventionsmaßnahmen, die für bestimmte Delikte gezielt bestimmte Bevölkerungsgruppen ansprechen (siehe für die Etablierung von altersspezifischen Maßnahmen auch Bundesamt für Sicherheit in der Informationstechnik und Polizeiliche Kriminalprävention der Länder und des Bundes 2019). Die vergleichsweise hohe Betroffenheit von Schüler*innen, insbesondere von Verhaltensweisen und Delikten aus dem Bereich Cybercrime im weiteren Sinn, spricht zudem dafür, die Vermittlung von Medienkompetenz in den Schulen weiter auszubauen. Zudem hat sich gezeigt, dass Cybercrimedelikte eher selten angezeigt werden. Die Anzeige bei den Strafverfolgungsbehörden ist jedoch wichtig, um einerseits die Aufklärung der Tat zu ermöglichen, aber andererseits auch, um das Ausmaß des Phänomens für Gesellschaft und Politik sichtbar zu machen. Dies bildet eine relevante Grundlage im Zusammenhang mit der Verteilung von Ressourcen und Personal. Um die Anzeigebereitschaft zu erhöhen, bedarf es einerseits Aufklärung dahingehend, bei welchen Phänomenen es sich um Straftaten handelt, warum eine Anzeige wichtig ist und wie man diese erstattet. Der letztgenannte Punkt, dass teilweise auch Unwissenheit darüber, an wen man sich in Bezug auf Viktimisierungen durch Cybercrime bei der Polizei wenden kann zu einem Ausbleiben der Strafanzeige führt, erwies sich auch in der bereits zuvor genannten Unternehmensbefragung von Dreißigacker et al. (2020) als relevant. Auch könnte darauf hingewiesen werden, dass parallel durch andere Erledigungsformen (wie bspw. Erstattungen durch Versicherungen oder Plattformen) eine Anzeige des Vorfalles erwünscht ist. Eine dritte Maßnahme könnte die weitere Sensibilisierung für die Bedeutung präventiven Verhaltens jedes*r Internetnutzers*in sein. Zwar zeigen die Ergebnisse, dass die meisten Befragten Schutzmaßnahmen anwenden, dies trifft jedoch nicht auf alle zu. Auch relativ einfach umzusetzende Maßnahmen wie beispielsweise die Installation eines Anti-Viren-Schutzprogramms werden nicht von allen ergriffen.

5. Literatur

Bergmann, M. C., Beckmann, L., Krieg, Y., Schepker, K., Baier, D. & Mößle, T. (2016). Cyberbullying, Cyberstalking und Cybergrooming – Gefahren der Nutzung neuer Medien: Eine Befragung an Katholischen Schulen in Nordrhein-Westfalen (unveröffentlichter KFN-Forschungsbericht). Hannover: KFN.

Bergmann, M.C., Kliem, S., Krieg, Y. & Beckmann, L. (2019). Jugendliche in Niedersachsen. Ergebnisse des Niedersachsensurveys 2017 (KFN-Forschungsberichte No. 144). Hannover: KFN.

Birkel, C., Church, D., Hummelsheim-Doss, D., Leitgöb-Guzy, N. & Oberwittler, D. (2019). Der Deutsche Viktimisierungssurvey 2017 - Erste Ergebnisse V1.1. Wiesbaden: BKA.

Bitkom (2016). Jeder zweite Internetnutzer Opfer von Cybercrime. Abrufbar unter: https://www.bitkom.org/Presse/Presseinformation/Jeder-zweite-Internetnutzer-Opfer-von-Cybercrime.html. (zuletzt geprüft am 14.07.2021).

BKA (Hrsg.) (2020). Cybercrime. Bundeslagebild 2020. Wiesbaden: BKA. Abrufbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2020.html;jsessinid=CE3C3AB78C7815E712BDF5B2C729AA7F. live2301?nn=28110. (zuletzt geprüft am 14.07.2021).

BKA (Hrsg.) (2017) Cybercrime. Bundeslagebild 2016. Wiesbaden: BKA. Abrufbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2016.html?nn=28110 (zuletzt geprüft am 14.07.2021).

Bundesamt für Sicherheit in der Informationstechnik (BSI) und Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) (Hrsg.) (2019). Digitalbarometer: Bürgerbefragung zur Cyber-Sicherheit. Bonn: BSI.

Bundesamt für Sicherheit in der Informationstechnik (BSI) und Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) (Hrsg.) (2020). Digitalbarometer: Bürgerbefragung zur Cyber-Sicherheit. Bonn: BSI.

Dreißigacker, A. (2016). Befragung zu Sicherheit und Kriminalität. Kernbefunde der Dunkelfeldstudie 2015 des Landeskriminalamtes Schleswig-Holstein. (KFN-Forschungsberichte No. 129). Hannover: KFN.

Dreißigacker, A., von Skarczinski, B. & Wollinger, G. R. (2020). Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer

repräsentativen Unternehmensbefragung 2018/2019. (KFN-Forschungsbericht No. 152). Hannover: KFN.

European Commission, Brussels (2018): Eurobarometer 82.2 (2014). TNS opinion [producer]. GESIS Data Archive, Cologne. ZA5931 Data file Version 3.0.0, https://doi.org/10.4232/1.12999.

Huber, E. (2019). Cybercrime. Wiesbaden: Springer.

Pfeiffer, H., Groß, E. & Schwarz, A. (2020): Befragung zu Sicherheit und Kriminalität in Niedersachsen 2015. Ergebnisse zum Schwerpunktfragenkomplex Computerbezogene Kriminalität. Landeskriminalamt Niedersachsen. Abgerufen am 08.07.2021 auf https://www.lka.polizei-nds.de/forschung/dunkelfeldstudie/dunkelfeldstudie--vierte-befragung-von-40000-menschen-steht-unmittelbar-bevor-115379.html.

Reyns, B. W. (2010). Being Pursued Online: Extent and Nature of Cyberstalking Victimization from a Lifestyle/Routine Activities Perspective. Dissertation: University of Cincinnati.

Sitzer, P., Marth, J., Kocik, C. & Müller, K. (2012). Ergebnisbericht der Online-Studie „Cyberbullying bei Schülerinnen und Schülern". Bielefeld.

Statistisches Bundesamt (2020). Computer- und Internetnutzung im ersten Quartal des jeweiligen Jahres von Personen ab 10 Jahren. Abrufbar unter: https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Einkommen-Konsum-Lebensbedingungen/IT-Nutzung/Tabellen/zeitvergleich-computernutzungikt.html (zuletzt geprüft am 08.07.2021).

Statistisches Bundesamt (2021): Erhebung über die private Nutzung von Informations- und Kommunikationstechnologien. IKT 2020. Abrufbar unter: https://www.destatis.de/DE/Methoden/Qualitaet/Qualitaetsberichte/Einkommen-Konsum-Lebensbedingungen/ikt-private-haushalte-2020.pdf (zuletzt geprüft am 08.07.2021).

Wachs, S. &Wright, M. F. (2018). Associations between Bystanders and Perpetrators of Online Hate: The Moderating Role of Toxic Online Disinhibition. International Journal of Environmental Research and Public Health, 15 (9), 2030.

Inhalt