Identitätsdiebstahl und -missbrauch im Internet

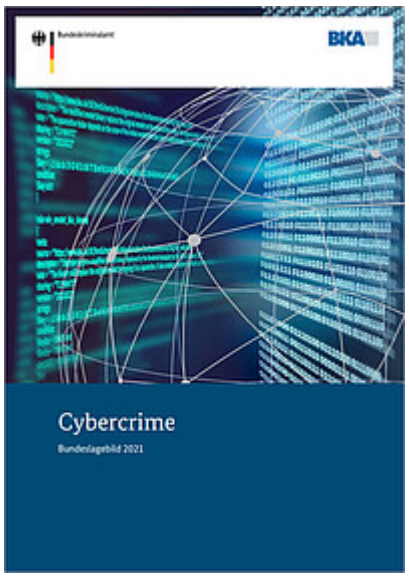
Aktuelle Entwicklungen und Herausforderungen

Von LKD a.D. Ralph Berthel, Frankenberg/Sa.[1]

Betrügen, also das Vorspiegeln falscher oder das Entstellen bzw. Unterdrücken wahrer Tatsachen mit dem Ziel, einen Irrtum zu erregen oder aufrechtzuerhalten, um sich rechtswidrig Vermögensvorteile zu verschaffen, zählt neben dem Diebstahl fraglos zu den ältesten Delikten, die die Kriminalgeschichte kennt. Zu den aktuellen Begehungsweisen beider Tatbestände gehören auch der Diebstahl und die betrügerische Nutzung von Daten, die die Identität einer Person charakterisieren. Identität (Abstraktum, also ein etwas nicht Gegenständliches bezeichnendes Hauptwort, zu lateinisch dem – svw. „derselbe“) soll hier als die Gesamtheit der Eigenschaften, die kennzeichnend für ein Individuum sind, Verwendung finden.[2] Handeln nach „Treu und Glauben“, also redliches, anständiges und verlässliches Agieren von Menschen wie auch Institutionen stellt sowohl im realen als auch im digitalen Alltag eine maßgebliche Voraussetzung für ein funktionsfähiges Gemeinwesen im Allgemeinen und für erfolgreiche Interaktionen im Rechtsverkehr im Besonderen dar.
Mit der Verlagerung großer Teile menschlicher Interaktionen in den digitalen Raum erlangen einerseits die Sicherheit von digitalen Identitäten und anderseits der rechtswidrige Zugriff auf diese sowie deren missbräuchliche Nutzung eine zunehmende Bedeutung. Für Täter stellen sie Tatgelegenheiten, für potentielle Opfer Bedrohungen und für Sicherheitsakteure eine der aktuellsten und größten Herausforderungen bei der Verbrechensbekämpfung und -prävention dar.[3]

1 Identität, Diebstahl und Missbrauch von Identitätsdaten im Internet – einige Begriffe

Klassische, analoge Identitätsprüfungsverfahren beruhen auf einem Dokument mit hoher Fälschungssicherheit, das von einer vertrauenswürdigen Instanz, wie im Falle des Personalausweises durch die zuständige Personalausweisbehörde, herausgegeben wird.
Die eineindeutige Identifikation handelnder Personen oder Institutionen stellt eine hochaktuelle Herausforderung für alle Akteure im digitalen Raum dar. Immer mehr Lebensbereiche werden digitalisiert. Damit sind auch immer mehr Daten und Informationen[4] über Personen, Institutionen und Prozesse im Netz verfügbar. Beispiele für die Identifizierung im Netz finden sich etwa beim Online-Banking oder jüngst bei digitalen Impfzertifikaten. Zuverlässige digitale Identitäten sind Garanten für Absender und Empfänger zugleich, dass sie die sind, die sie vorgeben, zu sein. Das trifft sowohl für Menschen als auch Maschinen zu.
In einer Vielzahl von Fallgestaltungen bilden Identifizierungen die Voraussetzung für Zugriffsrechte, Transaktionsmöglichkeiten oder Verwaltungsbefugnisse von Daten und Informationen. Eine Vielzahl derartiger Fallkonstellationen bieten auch Ansätze für Missbrauch und mithin kriminalistisch relevantes Handeln.



In diesem Aufsatz bezieht sich der Autor auf das Bundeslagebild Cybercrime 2020. Das Lagebild für das Jahr 2021 lag zum Zeitpunkt des Redaktionsschlusses noch nicht vor, ist aber mittlerweile erschienen und über die Homepage des Bundeskriminalamtes abrufbar.

Aus der Perspektive der Informationssicherheit kennzeichnet das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Begriff **„Identität“** wie folgt:
„Unter einer Identität wird im Kontext der Informationssicherheit die Menge von Merkmalen verstanden, die die Echtheit einer Person oder Sache nachweist. Die Identität einer Person oder Sache kann sowohl durch ein einziges Merkmal oder aber durch die Kombination diverser Merkmale bestimmt werden. Im Internet wird auf die Identität einer Person meist aus Identifikations- und Authentisierungsdaten geschlossen wie zum Beispiel aus der Kombination von Benutzername und Passwort.“[5] Dabei ist der Begriff „digitale Identität“ nicht scharf konturiert. „Im Prinzip erzeugen wir mit jeder Registrierung bei einem Online-Dienst eine neue digitale Identität.“[6] Digitale Identitäten beziehen sich dabei sowohl auf digitale Identitätsnachweise von natürlichen als auch juristischen Personen.
Als **Identitätsdiebstahl** kennzeichnet das BSI die „rechtswidrige Aneignung solcher Daten“. Wird zudem die Identität nach dem Diebstahl unautorisiert für eigene oder fremde Zwecke verwendet, wird dies als **Identitätsmissbrauch** bezeichnet.[7] Aus viktimologischer Sicht können sich kriminalistisch relevante Zugriffe auf bzw. missbräuchliche Nutzungen von digitalen Identitäten also sowohl auf Privatpersonen als auch Institutionen bzw. Unternehmen als Opfer beziehen.
Im Zusammenhang mit der kriminalistischen Betrachtung von Identitätsdiebstahl- und -missbrauch ist gelegentlich von **kompromittierten Accounts** die Rede.[8] Dabei handelt es sich um „ein System oder einen Datensatz, die als kompromittiert betrachtet werden können, wenn der Eigentümer des Systems, einer Datenbank oder eines Datensatzes keine Kontrolle mehr über die korrekte Funktionsweise und deren Sicherheit hat.“[9] Beim **Social Engineering** (eigentlich „angewandte Sozialwissenschaft bzw. „soziale Manipulation“, also soziale Beeinflussung, um bestimmte Reaktionen hervorzurufen) werden menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt, insbesondere durch Täuschung über die Identität und die Absicht des Täters. So geben sich Täter z.B. als Techniker oder als Mitarbeiter eines Unternehmens wie etwa PayPal, Facebook oder eines Telekommunikationsunternehmens aus, um Opfer zur Preisgabe von Anmelde- oder Kontoinformationen oder zum Besuch von präparierten Webseiten zu verleiten.[10]
In den Fällen, in denen Hacker vorgeben, jemand zu sein, der einer Person oder einem Netzwerk bekannt ist, um auf vertrauliche Informationen zugreifen zu können, wird von **Spoofing** gesprochen. Das BSI charakterisiert diese Begehungsweise als "Täuschungsversuche zur Verschleierung der eigenen Identität und zum Fälschen übertragener Daten. Das Ziel dieser Handlungen besteht darin, die Integrität und Authentizität der Informationsverarbeitung zu untergraben".[11] Zu ergänzen ist diese Definition um die Zielsetzung, Benutzer zu Handlungen zu bewegen, die dem Hacker zugutekommen, etwa indem er auf vertrauliche Daten zugreifen kann und/oder dem Benutzer Schaden zufügen. Eine typische Begehungsweise ist das **Mail-Spoofing**, bei dem die Täter darauf abzielen, dass persönliche Daten preisgegeben oder Finanztransaktionen durchgeführt werden. Die E-Mails, mit denen diese Angriffe gestartet werden, stammen scheinbar von vertrauenswürdigen Absendern wie Kunden, Kollegen oder Vorgesetzten. Darüber hinaus enthalten Spoof-E-Mails manchmal Anhänge, die beim Öffnen Malware wie etwa Trojaner oder Viren installieren. Eine weitere Begehungsweise stellt das **IP-Spoofing** dar. „Während sich Betrüger beim Mail-Spoofing auf einzelne Benutzer konzentrieren, ist IP-Spoofing in erster Linie auf Netzwerke ausgerichtet. Beim IP-Spoofing versucht ein Angreifer, durch das Senden von Nachrichten von einer gefälschten oder „gespooften“ IP-Adresse unbefugten

Zugang zu einem System zu erlangen.“[12]
„Spoofing im großen Stil wird als **Phishing** bezeichnet. Bei einem Phishing-Angriff legen Cyberkriminelle zahllose „Köder“ in Form gefälschter E-Mails, die an das E-Mail-Layout bekannter Unternehmen wie Amazon, DHL, eBay oder Postbank erinnern. … Sobald der Empfänger auf einen Link klickt, aktiviert er dadurch eine von vielen potenziellen Gefahren. … Cyberkriminelle können im Rahmen einer Phishing-Attacke ganz unterschiedliche Tools einsetzen. Ransomware ist ein direkter Angriff auf das Gerät des Empfängers. Keylogger und viele Trojaner dagegen stellen eher eine schleichende Gefahr dar: Sie überwachen die Aktionen des Nutzers und greifen Informationen zur Identität des Opfers ab, etwa persönliche oder finanzielle Daten, die für zukünftige Betrügereien verwendet werden können.“[13] Mit Phishing-Mails verfolgen Täter das Ziel, gutgläubige Nutzer dazu zu bewegen, auf einen „verseuchten“ Link zu klicken.
Beim sog. **Pharming** werden Opfer hingegen auf eine völlig falsche Website umgeleitet. Pharmer nutzen üblicherweise Schwachstellen in der DNS-Serversoftware aus. DNS-Server (Domain Name Service) lösen Internetnamen in numerische IP-Adressen auf. Cyberkriminelle leiten ihre Opfer auf gefälschte Websites um. Diese sind den Originalen täuschend ähnlich sind. Die Opfer ahnen oft nicht einmal etwas von der Manipulation. Gegenüber dem Phishing hängt der Erfolg der Täuschungshandlung hier nicht davon ab, dass das Opfer auf einen falschen Link hereinfällt und ihn anklickt.[14]

2 Zur Lage und zum Gefahrenpotenzial – ausgewählte Erkenntnisse

Während die in der Polizeilichen Kriminalstatistik (PKS) für 2020 erfassten Fallzahlen insgesamt eine rückläufige Tendenz gegenüber dem Vorjahr aufweisen (5.310.621 in 2020 gegenüber 5.436.401 im Jahr 2019; das entspricht einem Rückgang um 2,3%), weisen die Cybercrimedelikte eine deutliche Steigerung auf. Für 2020 wurden rund 108.000 Delikte der Cybercrime im engeren Sinne (CCieS)[15] registriert, was eine Steigerung von +^{7},9% im Vergleich zu den 2019 erfassten Fällen bedeutet.
Während im gesamtgesellschaftlichen Maßstab davon auszugehen ist, dass sich zunehmend mehr Lebensbereiche in den digitalen Raum verlagern oder zumindest auch in diesem stattfinden, ist das Wissen um deliktisches Handeln im Cyberraum eher schlecht ausgeprägt. Das BKA geht im Bereich Cybercrime von einem „überdurchschnittlich“ großen Dunkelfeld aus. Das führt das BKA u.a. auf folgende Deliktsspezifika zurück:
Die Opfer erkennen ihre Betroffenheit nicht (z.B. bei Diebstahl ihrer Identität bei einem Online-Shop). Die von ihnen eingesetzten technischen Geräte werden unbemerkt zur Begehung von Cybercrime-Straftaten missbraucht (z.B. bei Nutzung infizierter PCs oder Router als Teil eines Botnetzes zur Ausführung von DDoS-Angriffen).
Straftaten werden durch die Betroffenen oftmals nicht angezeigt, insbesondere dann, wenn noch kein finanzieller Schaden entstanden ist (z.B. bloßer Virenfund auf dem PC) oder der eingetretene Schaden von Dritten (z.B. Versicherung) reguliert wird. Geschädigte, insbesondere Wirtschaftsunternehmen, zeigen erkannte Straftaten nicht an, um u.a. die Reputation als „sicherer und zuverlässiger Partner“ im Kundenkreis nicht zu verlieren.[16]Es erscheint nachvollziehbar, dass der mit ca. 2% in der PKS abgebildete Anteil der CCieS an der Gesamtkriminalität nur einen Bruchteil dessen darstellen dürfte, was an kriminalistisch relevantem Handeln im Cyberraum tatsächlich stattfindet.

Im Bundeslagebild Cybercrime für 2020 werden digitale Identitäten als „beliebte Handelsware“ bezeichnet.[17] Unter Verweis auf „HaveIBeenPwnd“[18] bzw. das Hasso-Plattner-Institut werden dort rund 10 Mrd. bzw. 12 Mrd. identifizierte kompromittierte Accounts angeführt. Letztgenanntes Institut rechnet mit 1.635.908 geleakten Accounts pro Tag. Jeder gestohlene Datensatz könne wiederum als Ausgangspunkt für weitere kriminelle Handlungen genutzt werden, so das BKA.
Als klassisch für das rechtswidrige Erlangen digitaler Identitäten werden im Lagebild Spam-Mail-Kampagnen und professionelle Phishing-Mails mit maliziösen, also bösartigen, Office-Anhängen genannt. Der Spamversand erfolge über zuvor kompromittierte oder aber kommerziell angemietete Serverkapazitäten sowie über von Angreifern gestohlene legitime E-Mail-Accounts. Ein weiterer Modus Oprandi sei das aggressive Eindringen in ein System via Brute-Force-Angriff, also um den Versuch, ein Passwort oder einen Benutzernamen zu knacken oder eine verborgene Webseite oder den Schlüssel zu finden. Dabei nutzten Täter mangelhaft geschützte Remote-Desktop-Protokolle (RDP). Über diese würden wiederum Schadprogramme oder missbräuchlich eingesetzte Pentesting-Tools[19] eingeschleust, betont das BKA. In der Folge würden Daten ausgespäht und an die Täter weitergeleitet.

2.1 Cyberangriffe auf die Wirtschaft und öffentliche Einrichtungen

Mit dem Begriff **Big Game Hunting** (eigentlich: Großwildjagd) werden Cyberangriffe auf herausragende Wirtschaftsunternehmen, Einrichtungen, Organisationen bzw. Unternehmen im Bereich der KRITIS[20] bezeichnet.
Das BKA konstatierte für das Jahr 2020, in dem vor allem dem Gesundheitswesen und der öffentlichen Verwaltung eine besondere Bedeutung zukam, eine Intensivierung des „Big Game Hunting“. Als Beispiel nannte das Amt den im Dezember 2020 bekanntgewordenen Netzwerkeinbruch bei dem US-amerikanischen Technologie-Unternehmens „SolarWinds“, durch den über

die unternehmensseitigen Aktualisierungen der Software „Orion“[21] persistent, also dauerhaft und schwer abbaubare Zugriffe auf die IT-Netzwerke von Kunden möglich waren. Weltweit waren über 18.000 Systeme betroffen, darunter KRITIS und Behörden. Die Kompromittierung von „Orion“ gilt als einer der bisher größten und schwerwiegendsten Cyberangriffe der Kriminalgeschichte.[22]

2.2 Diebstahl digitaler Identitäten – Neuer Modus Operandi im Bereich Mobile Payment

Für das Jahr 2020 vermeldete das BKA erstmals Betrugshandlungen im Zusammenhang mit Mobile Payment. Bargeldlose Bezahlungen mittels Kreditkarten sollen durch die Nutzung sog. Token, also einer Hardwarekomponente zur Identifizierung und Authentifizierung von Benutzern, eigentlich effektiver und sicherer werden. Gleichwohl ist es Tätern über Phishing und Social Engineering gelungen, an für das Online-Banking notwendige Daten zu gelangen und im weiteren Verlauf der Tathandlungen sog. One Time Passwords, die z.B. für den Implementierungsprozess (Enrolement) von Kreditkartennummern in Apple Pay und Google Pay erforderlich sind, zu aktivieren und anschließend betrügerisch einzusetzen. Die Täter nutzten in der Folge die Bezahlfunktion von Smartphones an POS-Terminals vor Ort bei unterschiedlichen Vertragsunternehmen mittels Near Field Communication[23] zur betrügerischen Erlangung von Waren.[24]

2.3 Angst vor Identitätsdiebstahl und -missbrauch ist groß

Laut einer 2019 veröffentlichten Studie des Cyber-Sicherheitsanbieters F-Secure machen sich neun von zehn Verbrauchern zumindest grundsätzlich Sorgen darüber, dass ihr Bankkonto gehackt werden könnte, um ihr Geld zu stehlen (89%), sie Opfer von Online-Shopping-Betrug werden könnten (87%) oder jemand mithilfe ihrer Identität eine Straftat begeht (87%).[25] Mittlerweile ist auch die Sorge bei Unternehmen, etwa im Bereich E-Commerce, groß, dass man Opfer von „Identitätsbetrug“ werden könnte. Begriffe wie „**Cyber Security Awareness**“ oder „**Phishing Awareness**“ (Awareness svw. Problembewusstsein) etwa zum Schutz vor Passwortdiebstahl mittels Phishing-Mails erleben Hochkonjunktur.[26]

3 Konsequenzen/Herausforderungen

Identitätsdiebstahl und -missbrauch im Internet als Bestandteil der Computerkriminalität verunsichern einerseits Nutzer des Internets oder digitaler Anwendungen, verursachen bei Privatpersonen wie Unternehmen z.T. erhebliche Schäden und stellen für die Sicherheitsakteure eine zunehmende Herausforderung dar. Folgt man der von Balschmiter bereits 2017 entwickelten These, dass ein Teil des Hellfeldes klassischer Kriminalitätsformen offensichtlich in das Dunkelfeld moderner Computerkriminalitätsdelikte übergegangen ist,[27] sind die Positivinterpretationen des Rückganges der Fallzahlen in der Polizeilichen Kriminalstatistik[28] jedenfalls kritisch zu hinterfragen. Zwar ist der Anteil der Cybercrimedelikte (Computerkriminalität – PKS-Summenschlüssel 897000) an der Gesamtkriminalität in den vergangenen Jahren leicht gestiegen (2018: rd. 2% [110.475 Fälle]; 2020: rd. 2,46% [130.611 Fälle]), eine signifikante Erhellung des Dunkelfeldes ist damit jedoch keinesfalls verbunden. Und auch ein tatsächliches Widerspiegeln der Verlagerung großer Teile des gesellschaftlichen Lebens in die digitale Welt als gesellschaftliche Realität ist daraus nicht abzuleiten. Da weder eine echte Erhellung des Cybercrime-Dunkelfeldes erfolgte und auch die Ressourcen der Sicherheitsbehörden in diesem Deliktsbereich offenbar nicht in dem Maße wie die Verlagerung gesellschaftlichen Lebens in die digitale Welt stattfand, verstärkt wurden, existiert hier erheblicher Handlungsbedarf. Es ist daher Rüdiger zuzustimmen, der bereits 2019 im Rahmen der BKA-Herbsttagung eine deutlich verstärkte Internetpräsenz der deutschen Polizeien forderte und zudem ein Nachdenken über die Einführung des Opportunitätsprinzips bei derartigen Delikten anregte.[29]

Anmerkungen

1. Der Autor studierte Rechtswissenschaften an der Humboldt-Universität zu Berlin. Berufliche Stationen waren u.a.: Leitung verschiedener Kripo-Dienststellen, Kriminalistik-Dozent an der damaligen Polizei-Führungsakademie in Münster-Hiltrup (2001-2005), Leitung der Hochschule der Sächsischen Polizei (FH) in Rothenburg/O.L. (2005-2013) und die Leitung der Abteilung Auswertung und Ermittlungen im Landeskriminalamt Sachsen (2015-2019) sowie die Vertretung der Polizei Sachsen in den Kommissionen Wirtschaftskriminalität und Organisierte Kriminalität der AG Kripo. Der Autor ist Dozent im Masterstudiengang „Kriminologie, Kriminalistik und Polizeiwissenschaft“ an der Ruhr-Universität Bochum und im Masterstudiengang „Öffentliche Verwaltung – Polizeimanagement“ an der Deutschen

Hochschule der Polizei sowie im Masterstudiengang „Kriminalistik“ an der Hochschule der Polizei des Landes Brandenburg. Er ist Gründungsmitglied der Deutschen Gesellschaft für Kriminalistik e.V. Erreichbarkeit: ralph-berthel@web.de.

2. Es wird dabei nicht verkannt, dass der Begriff „Identität“ in unterschiedlichen Wissenschaftsgebieten auch unterschiedlich definiert wird. Aus psychologischer und pädagogischer Sicht spielt etwa die Identitätsbildung nach Erikson, die in erster Linie die psychosoziale Entwicklung des Menschen betrachtet, eine wichtige Rolle. In verschiedenen Definitionen des Begriffs Identität werden Eigenschaften von Identitäten neben natürlichen Personen auch Entitäten, Gegenständen oder Objekten zugeordnet. Aus juristischer Sicht liefert die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr Anhaltspunkte zur Beschreibung dessen, was mit der Identifizierung von Menschen und damit auch deren Identität verbunden werden kann. Dort heißt es in Art 2 a): „Als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind“.
3. Alle im Text verwendeten Internetadressen wurden letztmalig am 19.9.2021 aufgerufen.
4. Der Begriff „Daten“ wird hier für gesammelte einfache, isolierte Fakten, die einer Interpretation bedürfen, verwendet. Informationen sind hingegen bewertete, d.h. bereits interpretierte Daten, die für den Nutzer für die Lösung einer spezifischen Aufgabenstellung hilfreich sind. (Berthel, Ralph, Lapp, Matthias, Kriminalstrategie, 2017, S. 74).
5. BSI, Die Lage der IT-Sicherheit in Deutschland 2020, S. 18.
6. Pollmann, Malte, Ostler, Ulrike, Was ist digitale Identität und ist sie sicher? Datencenter Insider, 25.08.2021, www.datacenter-insider.de/was-ist-digitale-identitaet-und-ist-sie-sicher-a-1050665/.
7. BSI, 2020, S. 18.
8. Vgl. u.a. BKA, Cybercrime, Bundeslagebild 2020, 2021, S. 12.
9. Reuter, Caroline, Was bedeutet kompromittiertes Konto? 1.9.2021, alleantworten.de/was-bedeutet-kompromittiertes-konto.
10. BSI, Social Engineering – der Mensch als Schwachstelle, www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social-engineering_node.html.
11. BSI, Glossar der Cyber-Sicherheit, www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Informationen-und-weiterfuehrende-Angebote/Glossar-der-Cyber-Sicherheit/Functions/glossar.html^{2}=132814.
12. Vgl. Kaspersky, Was ist Spoofing? www.kaspersky.de/resource-center/definitions/ip-and-email-spoofing.
13. Avira, Spoofing, Phishing, Pharming: drei Methoden des Identitätsdiebstahls im Internet, 12.4.2018, www.avira.com/de/blog/avira-identity-scanner-schutz-vor-identitaetsdiebstahl.
14. Ebd.
15. Das BKA definiert Cybercrime im engeren Sinne als Straftaten, die sich gegen das Internet, informationstechnische Systeme oder deren Daten richten. BKA, 2021, S. 42.
16. BKA, 2021, S. 9.
17. BKA, 2021, S. 12.
18. Bei „Have I Been Pwned“ (HIBP), dt. „Wurde ich erwischt? Wurde ich gehackt?“ handelt es sich um die Website des unabhängigen Sicherheitsforschers Troy Hunt, der ermittelt, ob eine E-Mail-Adresse in einem öffentlich gewordenen Hack auftaucht.
19. Penetrationstests prüfen die Vulnerabilität von IT-Systemen gegenüber Angriffen. Sie sind grundlegender Bestandteil von IT-Sicherheits- und Schwachstellenanalysen.
20. KRITIS (Kritische Infrastrukturen) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Bundesamt für Sicherheit in der Informationstechnik, Kritische Infrastrukturen, Definition und Übersicht, (https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/einfuehrung_node.html).
21. „Orion“ ist eine IT-Management und -Monitoring-Software, die weltweit eingesetzt wird.

22. Ausführlich vgl. BKA, 2021, S. 29f.
23. Bei Near Field Communication (NFC), also Nahfeldkommunikation, handelt es sich um einen Übertragungsstandard zum kontaktlosen Austausch von Daten zwischen zwei Geräten in einer Entfernung von 10 bis 20 cm. Die Geschwindigkeit ist dabei auf 424 Kilobits pro Sekunde beschränkt. Beide Geräte können sowohl Daten senden als auch empfangen (https://www.netzwelt.de/nfc/index.html).
24. Ausführlich vgl.: BKA, 2021, S. 17.
25. F-Secure, „Identity Protection Consumer (B2C)“, Ist Identitätsdiebstahl das Cyber-Verbrechen, das wir am meisten fürchten? Eine Verbraucherumfrage zu den Themen „Identitätsdiebstahl und Cyber-Kriminalität“. www.f-secure.com/de/press/p/neue-studie-bestaetigt-die-angst-vieler-internetnutzer-vor-identitaetsdiebstahl.
26. Vgl. z.B. BSI, Awareness, www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Faktor-Mensch/Awareness/awareness_node.html.
27. Balschmiter, Peter, et al. Landeskriminalamt Mecklenburg-Vorpommern, Fachhochschule für öffentliche Verwaltung, Polizei und Rechtspflege des Landes MV, Ernst-Moritz-Arndt Universität Greifswald, Erste Untersuchung zum Dunkelfeld der Kriminalität in Mecklenburg-Vorpommern. Abschlussbericht, 2017, S. 54.
28. Bundesministerium des Innern, für Bau und Heimat, Kriminalstatistik 2020: Straftaten auf niedrigstem Stand seit 1993, Pressemitteilung, 15.4.2021.
29. Berthel, Ralph, Ausgrenzung, Hass und Gewalt – Herausforderungen für den Rechtsstaat und die Sicherheitsbehörden - Mit einem Bericht zur 65. Herbsttagung des Bundeskriminalamtes, DIE POLIZEI, 2020, S. 107.