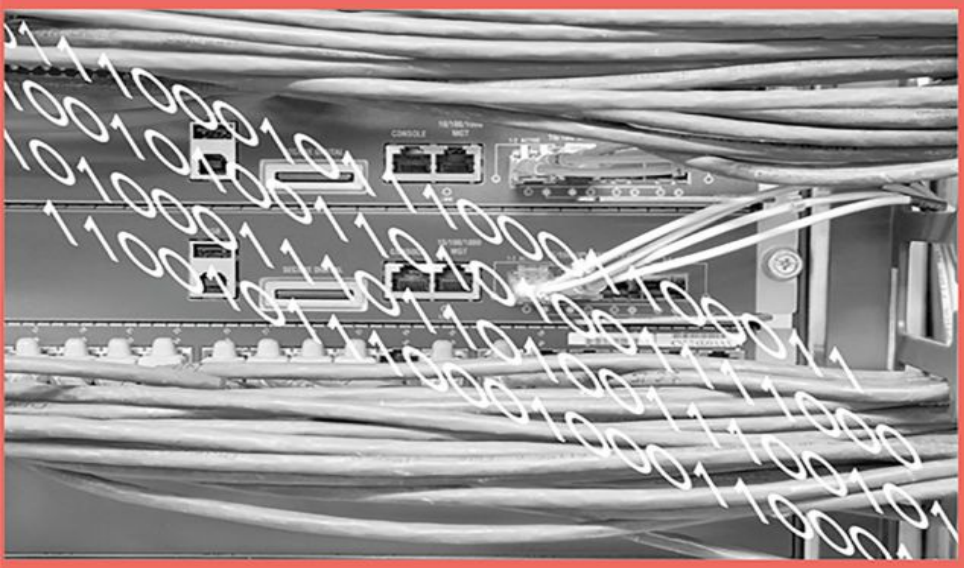
Büchel/Hirsch

Internetkriminalität

Phänomene – Ermittlungshilfen – Prävention

2. Auflage



Kriminalistik

Hinweis des Verlages zum Urheberrecht und Digitalen Rechtemanagement (DRM)

Der Verlag räumt Ihnen mit dem Kauf des ebooks das Recht ein, die Inhalte im Rahmen des geltenden Urheberrechts zu nutzen. Dieses Werk, einschließlich aller seiner Teile, ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Dies gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und Einspeicherung und Verarbeitung in elektronischen Systemen.

Der Verlag schützt seine ebooks vor Missbrauch des Urheberrechts durch ein digitales Rechtemanagement. Bei Kauf im Webshop des Verlages werden die ebooks mit einem nicht sichtbaren digitalen Wasserzeichen individuell pro Nutzer signiert.

Bei Kauf in anderen ebook-Webshops erfolgt die Signatur durch die Shopbetreiber. Angaben zu diesem DRM finden Sie auf den Seiten der jeweiligen Anbieter.

Internetkriminalität

Phänomene – Ermittlungshilfen – Prävention

Von

Michael Büchel

und

Peter Hirsch

2., neu bearbeitete Auflage

Kriminalistik

www.kriminalistik.de

Impressum

Bibliografische Informationen der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

ISBN 978-3-7832-0754-5

E-Mail: kundenservice@cfmueller.de

Telefon: +49 89 2183 7923
Telefax: +49 89 2183 7620

www.cfmueller.de

Vorwort

Nichts ist beständiger als der Wandel! Diese Weisheit, deren Urheberschaft den unterschiedlichen Personen zugeschrieben wird, passt ebenso auf die unterschiedlichen Phänomene der Internetkriminalität. Dabei wird die Wandlungsfähigkeit vor allem den im Netz agierenden Personen zugeschrieben, welche das Netz in unerlaubter Weise zu ihrem (finanziellen) Vorteil nutzen. Als Beispiele lassen sich die professionelleren Phishingmails der letzten Jahre oder die erweiterte Programmierung von Malware, die abwartet bis beispielsweise eine externe Festplatte zur Datensicherung an den Rechner angeschlossen wird und diese dann gleich mitverschlüsselt. Wandlungsfähig müssen dahingehend auch die Ermittler im staatlichen und privaten Bereich sein.

In dieser Neuauflage wurden daher die Phänomene der Internetkriminalität aktualisiert. Neu mit aufgenommen wurden zum Beispiel die Erscheinungen „Sexpressung“ oder der „Video-Ident-Betrug“. Nicht eingearbeitet wurden Betrugsmaschen im Zuge der im Jahr 2020 grassierenden „Corona-Pandemie“, da es sich nicht um neue Phänomene, sondern lediglich einen geänderten Anlass zum Versand von Phishingmails handelt.

Weggefallen sind dafür beispielsweise einige PIN-Verfahren, die das Onlinebanking betreffen. Da diese potenziell unsicher waren, wurden sie durch neue ersetzt.

Die Grundzüge der Computerforensik wurden um einen kurzen Einblick in die „Mobile Forensik“ erweitert. Und schließlich wurde der Überblick über staatliche und private

Organisationen, die sich mit der Bekämpfung der Internetkriminalität im weitesten Sinn beschäftigen. Auch in diesem Bereich gab es einen minimalen Wandel.

Wie auch in der ersten Ausgabe bitten die Autoren um eine kurze Mail für den Fall, dass wir ein Phänomen aufgrund unserer Interpretation falsch dargestellt haben. Die Adresse lautet immer noch wie in der ersten Auflage www.internetkriminalitaet@gmx.net.

Heidelberg, im Mai 2020 *Michael Büchel und Peter Hirsch*

Vorwort zur 1. Auflage

Es gibt bereits eine Vielzahl von Büchern, die sich mit dem Thema Internetkriminalität beschäftigen. Wer also sollte dieses Buch lesen? Es wendet sich an Polizeibeamte in Ausbildung und Ermittler in Ermittlungsgruppen der Dienststellen der Schutzpolizei, die sich einen ersten Überblick über Phänomene der Internetkriminalität verschaffen wollen. Ebenso geeignet ist es für Privatermittler und alle, die sich aus anderen Gründen mit der Materie vertraut machen wollen. Für Berufsgruppen, die fundierte Kenntnisse auf dem Gebiet der Internetkriminalität haben (Strafverfolgung, Forensik zur Auswertung, Penetration von Systemen zur Aufdeckung von Sicherheitslücken oder Prävention), wird es ausreichend sein zu wissen, dass es dieses Werk gibt. Einen essentiellen Mehrwert an Wissen wird diesem Personenkreis die Lektüre nicht verschaffen.

Der Inhalt des Buches ist so aufgebaut, dass zuerst eine kurze Einführung in die Thematik gegeben wird. Dazu gehört neben einem Blick darauf, warum das World-Wide-Web für Straftäter so interessant geworden ist, auch der auf die Schwierigkeiten, die vielschichtigen Möglichkeiten der Begehung von Delikten im, mit dem, durch das und auf das Medium Internet in eine Definition zu fassen. Die Betrachtung der Begriffsbestimmung ist eng verwoben mit den rechtlichen Grundlagen auf nationaler und europäischer Ebene, weswegen auch diese kurz gestreift werden.

In den einzelnen Kapiteln werden aktuelle Phänomene der Internetkriminalität aufgegriffen und beschrieben. Dazu wird

ein bewusst straff geführter Abriss über mögliche Strafrechtsnormen und zivilrechtlicher Bestimmungen gegeben. Straff deshalb, da im Buch die Phänomene als solche im Mittelpunkt stehen sollen und die Autoren davon ausgehen, dass die Themen im Strafrechtsunterricht in der Aus- und Fortbildung tiefergehender behandelt werden. Die im Anschluss an die Erscheinungsformen aufgeführte Checkliste soll die in der Aus- und Fortbildung vermittelte Vorgehensweise zur Sachbearbeitung um praxisnahe Tipps und Hinweise auf mögliche Ermittlungsansätze ergänzen. Breiter Raum wird am Ende eines jeden Kapitels den Präventionsmöglichkeiten geboten. Die Vermittlung dieser Hinweise sollte nicht nur bei einer Anzeigenerstattung gegenüber dem Geschädigten für zukünftiges Verhalten obligatorisch sein, sondern auch bisher nicht betroffene User – auch Polizeibeamte und sonstige Ermittler – vor Nachteilen schützen.

In diesem Zusammenhang darf auf keinen Fall ein Kapitel über die Passwortsicherheit fehlen. Abgerundet wird der Inhalt durch einen Einblick in die Grundzüge der Computerforensik und eine kurze Vorstellung von stattlichen und privaten Organisationen, die sich mit der Bekämpfung von Internetkriminalität im weitesten Sinn beschäftigen.

Ungeachtet gewissenhafter Recherche zu den Inhalten des Buches wird es vorkommen, dass von den Autoren, trotz mehrseitiger Absicherungen, Sachverhalte falsch interpretiert wurden. Sollte dies vorgekommen sein, steckt keine böse Absicht oder Gedankenlosigkeit dahinter. Allerdings würden wir uns in diesem Fall über konstruktive Kritik freuen, die unter www.internetkriminalitaet@gmx.net an uns gerichtet werden kann. Die Kontaktaufnahme in diesem Fall bringt nicht nur uns weiter, sondern es

profitieren in Zukunft alle Leserinnen und Leser, da wir diese Fehlinterpretation dann vermeiden können.

Heidelberg, im Mai 2014 *Michael Büchel und Peter Hirsch*

Inhaltsverzeichnis

3.4 Verband der deutschen Internetwirtschaft e.V. – eco e.V.

Literaturverzeichnis

Beck, K. Ethik der Online-Kommunikation, in: Schweiger/Beck (Hrsg.): Handbuch Online-Kommunikation, 2010

Borges, G. u. a. Identitätsdiebstahl und Identitätsmissbrauch im Internet – Rechtliche und technische Aspekte, 2011

Fox, D. Phishing, in: Datenschutz und Datensicherheit – Recht und Sicherheit in der Informationsverarbeitung und Kommunikation, Ausgabe 6/2005

Ders. Social Engineering, in: Datenschutz und Datensicherheit – Recht und Sicherheit in der Informationsverarbeitung und Kommunikation, Ausgabe 5/2013

Freiberger, H. Die SMS-Masche – Betrugsserie beim Onlinebanking schockiert Kunden, in: Süddeutsche Zeitung, Nr. 246, 69. Jahrgang vom 24.10.2013

Hilgendorf E./Valerius B. Computer- und Internetstrafrecht – Ein Grundriss, 2012

Leymann, H. Mobbing – Psychoterror am Arbeitsplatz und wie man sich dagegen wehren kann, 1993

Mei, Y. Anti-phishing system. Detecting phishing e-mail, Reports from MSI, School of Mathematics and Systems Engineering, 2008

Mitnick, K./Simon, W. Die Kunst der Täuschung – Risikofaktor Mensch, 2011

Olweus, D. Gewalt in der Schule. Was Lehrer und Eltern wissen sollten – und tun können, 2006

Pohlmann, N. Cyber-Sicherheit – Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung, 2019

Leest, U./Schneider, C. Cyberlife II – Spannungsfeld zwischen Faszination und Gefahr, Cybermobbing bei Schülerinnen und Schülern. Zweite empirische Bestandsaufnahme bei Eltern, Lehrkräften und Schülern/innen in Deutschland, 2017

Schneider, D. Phishing, Pharming und Identitätsdiebstahl – von Postbank bis Paypal. Informationstechnische Grundlagen und strafrechtliche Beurteilung der Internetkriminalität, 2006 (Seminararbeit)

Schulz, S./Wolfenstetter, K-D. Web Identitäten – Begriffsbestimmungen und Einführung in das Thema, 2005

Onlinemedien

Alle Onlinemedien wurden letztmalig aufgerufen am 22.4.2020.

BITKOM, Berlin, Beim Onlinebanking sind nur noch die Senioren zurückhaltend https://www.bitkom.org/Presse/Presseinformation/Beim-Online-Banking-sind-nur-noch-Senioren-zurueckhaltend

BITKOM, Berlin, Zwei Drittel nutzen eine App fürs Mobile-Banking“ https://www.bitkom.org/Presse/Presseinformation/Zwei-Drittel-nutzen-App-fuers-Mobile-Banking.

Bundesamt für Sicherheit in der Informationstechnik (BSI), Leitfaden IT-Forensik, Version 1.0.1, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=2Bundesamt für Sicherheit in der Informationstechnik (BSI), Passwörter, https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.htmlBundesamt für Sicherheit in der Informationstechnik (BSI), Passwortdiebstahl durch Phishing, https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/Phishing/phishing_node.html

Bundesamt für Sicherheit in der Informationstechnik (BSI), Presse unter https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/Emotet-Warnung_230919.html

Bundesamt für die Sicherheit in der Informationstechnik (BSI), Technical Guideline BSI TR-03119 Requirements for Smart Card Readers Supporting eID and eSign Based on Extended Access Control, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03119/BSI-TR-03119_V1_pdf.pdf?__blob=publicationFile&v=3

Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 61, Bonn, Gesetz zur Angleichung des Urheberrechts an die aktuellen Erforde Wissensgesellschaft (Urheberrechts-Wissensgesellschafts-Gesetz–UrhWissG), https://www.bgbl.de/xaver/bgbl/start.xav#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s3346.pdf%27%5D__15848

Bundeskriminalamt Wiesbaden, Handlungsempfehlungen für die Wirtschaft in Fällen von Cybercrime, https://zac-niedersachsen.de/archiv/2019-11-06_Flyer_Cybercrime_2019_Web.pdf

Bundeskriminalamt, Wiesbaden, Cybercrime, https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_node.htmlBundeskriminalamt, Wiesbad

Polizeiliche Kriminalstatistik (PKS) 2018, https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2018/pks2018_node.l

Bundesverband deutscher Banken e. V., Berlin „Dubioses Stellenangebot: Finanzagent“ unter https://bankenverband.de/publikationen/broschueren/dubioses-stellenangebot-finanzagent/

Carnegie Mellon University, Pittsburgh, USA, CAPTCHA: Telling Humans and Computers Apart Automatically, www.captcha.net

Duden online, „hosten“, https://www.duden.de/rechtschreibung/hostenEMV Corporation, Hopkinton, USA, „A Guide to EMV Chip Technology“, Version 2.0, November 2014, https://www.emvco.com/wp-content/uploads/2017/05/A_Guide_to_EMV_Chip_Technology_v2.0_20141120122132753.pdf

Euro Kartensysteme GmbH, Frankfurt „Debitkarten Schadensstatistik 2019“ unter https://www.kartensicherheit.de/oeffentlich/aktuelles/alle-artikel/artikel-2020/debitkarten-schadensstatistik-2019.html

Europäische Kommission, RICHTLINIE (EU) 2015/2366 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32015L2366

Europarat, Additional protocol to the convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081 60f

bzw.

Europarat, Zusatzprotokoll vom 28.01.2003 zum Übereinkommen über Computerkriminalität betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art, bereinigte Übersetzung, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008160f

Europarat, Convention of Cybercrime, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561bzw.

Europarat, Übereinkommen über Computerkriminalität, bereinigte Übersetzung, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008157a

European Association for Secure Transactions Ltd (EAST) Edinburgh, „ATM malware and logical attacks fall in Europe“ in „European Payment Terminal Crime Report“ vom 9.10.2019 unter https://www.association-secure-transactions.eu/atm-malware-and-logical-attacks-fall-in-europe/Gruhl, J. (2007): Nicht nur Geheimagenten leben gefährlich – sondern auch „Finanzagenten“. In: Internet-Zeitschrift für Rechtsinformatik und Informationsrecht, www.jurpc.de/aufsatz/20070020.htm

heise online, Technology Review – Das Magazin für Innovation, „Statistik der Woche: Smartphones in Deutschland“, https://www.heise.de/tr/artikel/Statistik-der-Woche-Smartphones-in-Deutschland-4318411.htmlInternet Systems Consortium, Redwood City, USA, Internet Domain Survey Host Count, https://www.isc.org/survey/

IT in der Wirtschaft, Befragung „Cyberangriffe gegen Unternehmen“, vorläufiger Forschungsbericht. https://www.cybercrime-forschung.de/

Kochheim, D. (2012): Skimming. Hintergründe und Strafrecht. In: Der Cyberfahnder, http://www.cyberfahnder.de/doc/Kochheim-Skimming-V3.pdf

Manager Magazin, Hamburg, „Datenleck bei Bonusprogramm Priceless Specials – Hacker stehlen Daten von 90.000 Mastercard-Kunden“, https://www.manager-magazin.de/unternehmen/banken/mastercard-priceless-specials-bonusprogramm-gehackt-a-1282691.html

Medienpädagogischer Forschungsverbund Südwest, Stuttgart, JIM-Studie 2019 – Jugend, Information, Medien, https://www.mpfs.de/fileadmin/files/Studien/JIM/2019/JIM_2019.pdfPichel, A. (2013): The Ghost in the (Portable) Machine: Securing Mobile Banking, http://blog.trendmicro.com/trendlabs-security-intelligence/the-ghost-in-the-portable-machine-securing-mobile-banking

Schröder, H. (2011): Zusammenhang von Brute-Force-Attacken und Passwortlänge, http://www.1pw.de/brute-force.html

Schulportal Thüringen, Gesamtvertrag Vervielfältigungen an Schulen vom 20. Dezember 2018, https://www.schulportal-thueringen.de/get-data/1c1e74ec-1afe-4a47-aec1-ff37341e20f6/Gesamtvertrag_Vervielfaeltigungen-an-Schulen_2018-12-20.pdf

Statista GmbH, Hamburg, Anteil der Nutzer von Online-Banking in Deutschland seit 1998, http://de.statista.com/statistik/daten/studie/3942/umfrage/anteil-der-nutzer-von-online-banking-in-deutschland-seit-1998

Statista GmbH, Hamburg, Anzahl der Smartphone-Nutzer in Deutschland seit 2010, http://de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenutzer-in-deutschland-seit-2010/

Süddeutsche Zeitung Digital, München, n-TAN-Betrug im Online-Banking – Die Masche mit Lolita, http://www.sueddeutsche.de/digital/mtan-betrug-im-online-banking-die-masche-mit-lolita-1.1806264

UN, New York/Wien, 10. Kongress „Prevention of Crime and the Treatment of Offenders“, https://www.unodc.org/documents/congress//Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Rela

Universität des Saarlandes, Saarbrücken, Internet-Zeitschrift für Rechtsinformatik und Informationsrecht, www.jurpc.de/rechtspr/20060091.pdf

Universität Tübingen, NFC-TAN, www.nfc-tan.com

Verizon Communications, New-York, USA; 2019 Data Breach Investigations Report, https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

Wikipedia – Die freie Enzyklopädie, Captcha, http://de.wikipedia.org/wiki/Captcha

Wikipedia – Die freie Enzyklopädie, Intrusion Detection System, http://de.wikipedia.org/wiki/Intrusion_Detection_System

Zeit Online, Hamburg, Hacker haben 38 Millionen Kundendaten erbeutet, http://www.zeit.de/digital/datenschutz/2013-10/adobe-hacker-kundendaten

Abbildungsverzeichnis

I. Einleitung

Inhaltsverzeichnis

Ursprünglich ins Leben gerufen wurde das Internet von den USA im militärischen Bereich. Während des „Kalten Krieges“ sollte der tatsächliche oder vermeintliche Technologievorsprung vor der damaligen Sowjetunion ausgebaut bzw. zumindest gehalten werden. Nach der Spaltung des Netzes in ein militärisches und ein öffentliches erkannten sowohl die Wirtschaft als auch später der private Nutzer die vielfältigen und faszinierenden Möglichkeiten des World-Wide-Webs. Allerdings war die Anwendung noch beschränkt auf den passiven Konsum der angebotenen Inhalte.

Einen Schub erfährt das Medium in der Mitte der 2000er Jahre mit der Implementierung des so genannten **Web 2.0** („Mitmach-Web“ oder „User generated content“). Der User erhält die Möglichkeit, eigene Inhalte zu gestalten. So erfährt das Netz eine attraktive Ausweitung für aktive Anwendungen:

- Informationsplattformen zum Wissenserwerb bzw. -transfer,
- Marktplatz für den privaten respektive unternehmerischen Verkauf und Kauf bzw. das Versteigern und Ersteigern von Waren,
- Plattformen für Dienstleistungen aller Art, wie

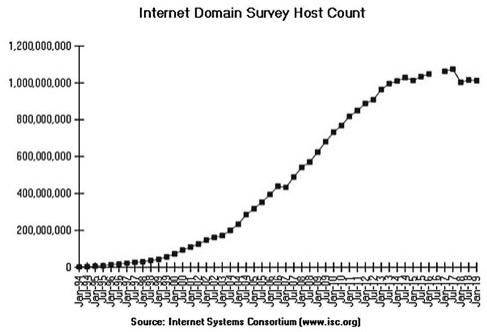
beispielsweise Onlinebanking, Preisvergleichsportale, Onlineberatungen zu verschiedensten Themen,

- Angebote von Musik, Filmen, Videos, Spielen oder Software auf Unterhaltungs- und Medienplattformen,

- Kommunikation, zum Beispiel Wiki, Podcasts, Blogs, oder soziale Netzwerke wie Facebook, Snapchat, Pinterest, Twitter, XING, LinkedIn.

Allerdings ist das Netz nicht nur für den so genannten Privatanwender interessant. Auch Wirtschaft und Industrie profitieren von der Fortentwicklung des weltweiten Netzes.

Abbildung 1:
Anzahl der Hosts im Internet.



Quelle: Internet Systems Consortium

[Bild vergrößern]

Als „Vierte Revolution“ bezeichnet *Martina Koederitz*, zum Erscheinungszeitpunkt des Artikels Vorsitzende der Geschäftsführung bei IBM, in einem Beitrag in der SZ[1]die Verschmelzung des Internets mit den klassischen Domänen der Industrie. Der Artikel gilt als Beleg dafür, dass das Medium Internet neben der rein privaten Nutzung (Kommunikation, Unterhaltung, Medien) sowie der Anwendungen zwischen Privaten und Anbietern von

Dienstleistungen (Banking, Einkauf und Versteigerungen im Netz) immer mehr wirtschaftliche bzw. industrielle Bereiche durchdringt. In diese Richtung deuten auch Begriffe wie Industrie 4.0, Internet der Dinge (IoT), Integrated Industry oder Smart Faktory. Versprochen werden in diesem Zusammenhang eine schnellere Kommunikation, optimierte Prozesse, Vereinfachung und Effizienz.

Zu privaten und auch wirtschaftlichen Zwecken werden eine Vielzahl unterschiedlicher Daten gespeichert. Die Inhalte reichen von persönlichen Angaben (personenbezogenen Daten, Posts, Bildern, Videos zur eigenen Person oder über Fremde usw.) über Bank- und Kreditkarteninformationen (Zugangscodes zum Onlinebanking, Kartennummern, Kontostände, Passwörter für Handelsplattformen usw.) bis hin zu Daten aus Industrie und Wirtschaft (Personaldaten, Kontaktdaten von Kunden und Geschäftspartnern, automatisierte Produktionsabläufe, Konstruktionspläne usw.).

Mit der Verbreitung des Medium Internet und der stetig steigenden Datenmenge nimmt auch das Interesse von Kriminellen an den dort gespeicherten Daten zu. In einer Befragung von 5000 Unternehmen unterschiedlicher Größe und Branchen in Deutschland zur Betroffenheit von Cyberangriffen gaben 41 % der Teilnehmer an, in den vergangenen 12 Monaten Ziel eines Angriffs gewesen zu sein, auf den reagiert werden musste. 65 % gaben an, schon jemals betroffen gewesen zu sein.[2]

Angriffe auf Computeranlagen finden auf unterschiedlichste Weise statt. Identitäten werden gestohlen und zum Nachteil des Opfers wieder neu eingesetzt, Personen werden aufgrund ihrer Internetpräsenz beleidigt und diffamiert, Musik und Filme werden ohne Nutzungsrechte kopiert,