HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCE

LEHRBRIEF

für das Modul

Rechtsgrundlagen 2 – Cybercrime

Autoren: Prof. Dr. Dirk Labudde

Laura Pistorius

Tim Wetterau

Bearbeitungsstand: 17.04.2024

Inhaltsverzeichnis

1 Einleitung

Der Lehrbrief „Gefahren im Internet“ für das Modul Cybercrime I gibt dem Studierenden neben einer Einführung in die Thematik, eine Übersicht über alle notwendigen Begrifflichkeiten. Ein zentraler Punkt wird weiterhin die Frage sein, weshalb das Internet in der heutigen Zeit immer interessanter für Straftaten wird. Aufgrund der Vielzahl an Delikten und deren strafrechtlicher Diskussion ist es nicht möglich, diese vollständig in diesem Lehrbrief zu behandeln. Auf die nachfolgenden Themen wird im Detail eingegangen und weiterführende Literatur angegeben:

- Identitätsdiebstahl
- Phishing
- Internetbanking, Onlinebanking
- Skimming
- Botnetze
- Filesharing (Tauschbörsen)
- Nutzung fremder offener WLAN-Netze
- Softwarepiraterie
- Online-Erpressungen
- Cybermobbing und Cyber-Bullying
- Passwortsicherheit
- DDoS-Attacken

Am Ende des Lehrbriefes werden beispielhafte Handlungsempfehlungen für Unternehmen in Fällen von Cybercrime gegeben.

2 Einführung und Begriffsbestimmungen

Die Geschichte des Internets ist sicher eine der interessantesten, die es gibt. Ursprünglich wurde das Internet in den USA für militärische Zwecke entwickelt und erst zu einem späteren Zeitpunkt auch im akademischen Feld etabliert. Eine Welt völlig frei vom Internet und dessen alltäglichem Nutzen liegt einige Jahrzehnte zurück und ist für die Wenigstens heutzutage noch vorstellbar. Viele Nutzen das sogenannte Netz mehrere Stunden am Tag, ohne sich jedoch einmal gefragt zu haben „Wer hat's erfunden?" und seit wann es eigentlich das World Wide Web sowie Domains, E-Mails, Videos und Webshops eigentlich gibt. Ein Versuch die Geschichte des Internets abzubilden, stellen die Abbildungen 1 und 2 dar.

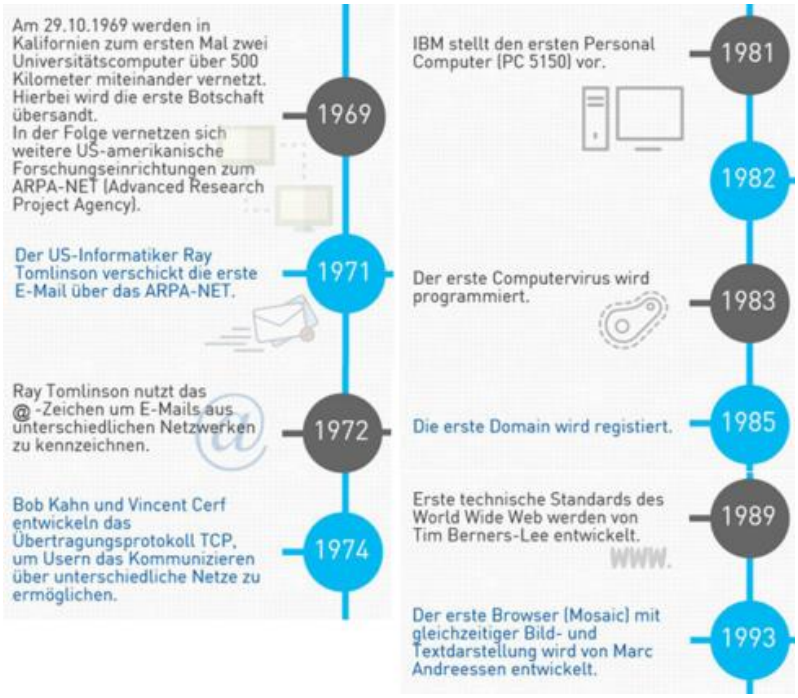


Abbildung 1: Kurzgeschichte Internet bis 1993

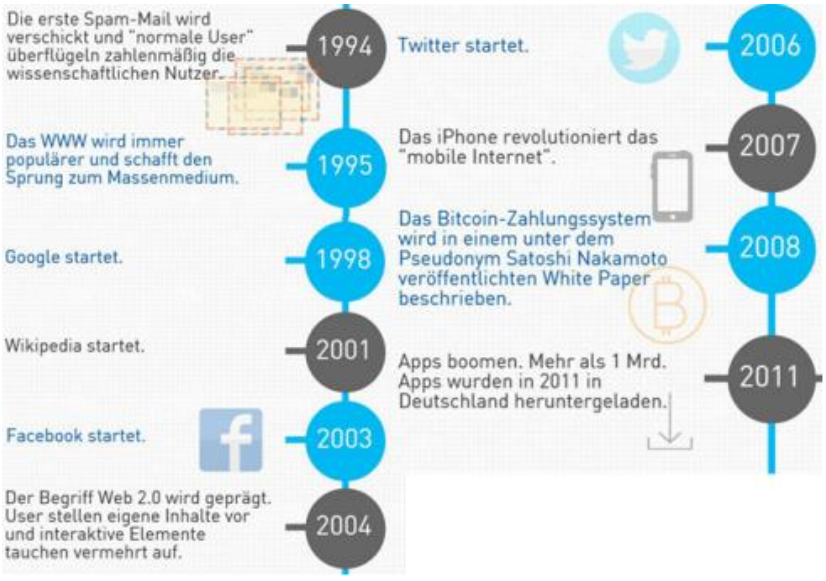


Abbildung 2: Kurzgeschichte Internet ab 1994

Während des „Kalten Krieges“ ging es im Wesentlichen um den Ausbau des Technologievorsprungs gegenüber der damaligen Sowjetunion. Nach der Aufspaltung des Netzes in ein militärisches und in ein öffentliches Netz wurde der Nutzen für die Wirtschaft schnell deutlich. Auch Privatpersonen erkannten die faszinierenden Möglichkeiten des World Wide Webs. Jedoch war die Anwendung noch auf den passiven Konsum beschränkt. Mit der Verbreitung des Mediums Internet und der stetig steigenden Datenmenge nimmt auch das Interesse von Kriminellen an den gespeicherten Daten zu. In einer Unternehmensbefragung von 2013 zu Betroffenheit der Wirtschaft von Cybercrime gaben 33% der befragten Unternehmen an, bereits einmal von Cyberkriminellen angegriffen worden zu sein (illustrativ in Abbildung 3 dargestellt). In nahezu allen Bereichen des täglichen Lebens, sei es der private oder auch der professionelle Bereich, ist die digitale Unterstützung nicht mehr wegzudenken. Vom Smartphone über das Tablet bis hin zu PC und Laptop sind wir in der digitalen Welt unterwegs. Neben dem bereits erwähnten privaten Sektor sind Banken, Krankenhäuser, Versorgungsunternehmen, Polizei und Feuerwehr nur einige wenige Beispiele von Behörden und Industrie, die digital vernetzt sind. Auch Straftäter erkennen das Potenzial des Internets und nutzen dessen Möglichkeiten für das Begehen von Straftaten. Somit ist die Informationstechnik sowohl Ziel als auch Mittel krimineller Bedrohungen.

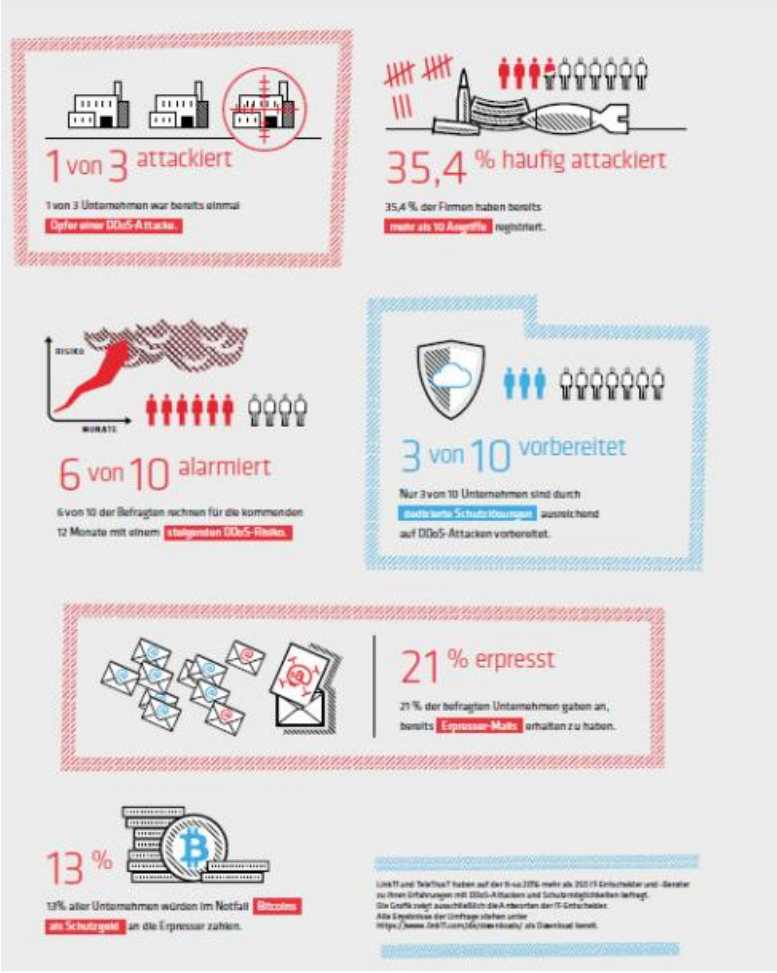


Abbildung 3: DDos-Angriffe in Deutschland

Neben den klassischen Beweismitteln wie Fotoaufnahmen, Akten, Werkzeugen oder Waffen, nehmen digitale Beweismittel einen immer größeren Raum in Ermittlungsverfahren ein. Dies können neben elektronischen Dokumenten, digitalen Bildern, E-Mails, Chatprotokollen auch verschlüsselte Informationen oder Spuren von Angriffen auf Netzwerke sein. Diese Informationen auszuwerten und

zu analysieren ist Aufgabe der IT-Forensik. Zu den Kernaufgaben dieser gehören die Entwicklung und der Test von Werkzeugen und Methoden zur:

- Sicherung
- Untersuchung
- Sichtbarmachung
- Aufbereitung und
- Bereitstellung

digitaler Daten mit dem Ziel der Auswertung durch die beauftragenden Ermittlungsbereiche. Als Beweismittel fallen Datenträger unzähliger Formate, Magnetbänder, Magnetbandkassetten, Fest- und Wechselplatten, Speicherkarten aller Formate, E-Book-Reader, Spielekonsolen, Chipkarten, optische Medien sowie Mobiltelefone/Smartphones und SIM-Karten an. Auch veraltete elektronische Beweismittel wie beispielsweise PDA's und Magnetstreifenkarten oder elektronische Kalender finden sich unter den Sicherstellungen und bedürfen der Untersuchung und Aufbereitung. Darüber hinaus können auch physikalisch defekte Datenträger unter Umständen noch untersucht werden. Arbeitsteilig erzeugt die Abteilung Kriminaltechnik ein Abbild des Speichers, dessen Inhalt im Anschluss von der Abteilung Operative Einsatz und Ermittlungsunterstützung weitergehend untersucht wird. Immer größere Relevanz bekommen Speicherkapazitäten im Internet, so genannte Cloudspeicher. Hier bestehen besondere Herausforderungen bei der Sicherung.

3 Internetkriminalität (Cybercrime)

Die Kriminalität bezieht sich auf die Gesamtheit aller Straftaten, die innerhalb eines bestimmten Rechtsgebiets oder einer Rechtsgemeinschaft gemäß den geltenden Gesetzen geahndet werden. Sie umfasst alle Ereignisse, die einen Verstoß gegen das Strafgesetzbuch und strafrechtliche Nebengesetze darstellen. Dieses komplexe Phänomen berücksichtigt sowohl individuelle Handlungen als auch gesellschaftliche Strukturen.

Der Begriff "Cyberspace" oder auch "Cyber-Raum" bezeichnet einen virtuellen Raum, der sowohl Informationstechnologiesysteme als auch das Internet umfasst. In diesem umfassenden digitalen Raum finden eine Vielzahl von Aktivitäten statt, darunter Kommunikation, Datenübertragung, Transaktionen und vieles mehr. Die Cybersicherheit konzentriert sich auf die Sicherheit dieser digitalen Umgebung und umfasst daher sowohl die Sicherheit von Informationstechnologiesystemen als auch die Internetsicherheit.

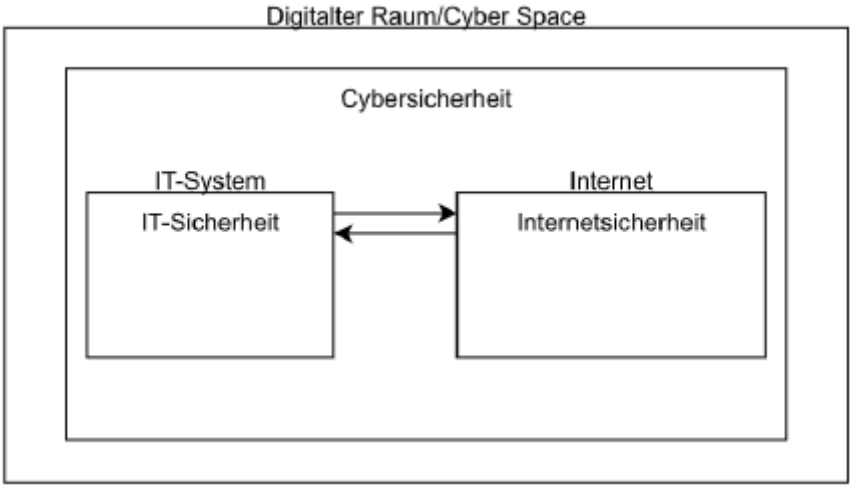


Abbildung 4: Cyber Space und Cybersicherheit

Die Sicherheit von Informationstechnologiesystemen bezieht sich auf den Schutz von Computern, Netzwerken, Servern, Datenbanken und anderen IT-Ressourcen vor Bedrohungen wie Malware, Hacking-Angriffen, Datenlecks und anderen Sicherheitsverletzungen. Dies umfasst auch Maßnahmen wie Firewalls, Antivirensoftware, Verschlüsselungstechniken, Zugangskontrollen und regelmäßige Sicherheitsupdates, um die Vertraulichkeit, Integrität und Verfügbarkeit der IT-Systeme sicherzustellen.

Die Internetsicherheit hingegen bezieht sich auf den Schutz der Kommunikation und der Datenübertragung im Internet. Dazu gehören die Sicherheit von Webanwendungen, E-Mail-Systemen, Cloud-Services, Online-Zahlungen und anderen Online-Diensten. Internetsicherheitsmaßnahmen umfassen die Verschlüsselung von Datenübertragungen (z. B. SSL/TLS), die Authentifizierung von Benutzern (z. B. durch Passwörter oder Zwei-Faktor-Authentifizierung) und den Schutz vor Phishing-Angriffen, Identitätsdiebstahl und anderen Internetbedrohungen.

Aus vielen Studien wird klar, dass das Phänomen Internetkriminalität oder Cybercrime verschiedene Termini besitzt. Unter Cybercrime oder IuK-Kriminalität werden Straftaten verstanden, die unter Ausnutzung moderner Informations- und Kommunikationstechnik gegen diese begangen werden. Dazu zählen:

- alle Straftaten, bei denen Elemente der EDV in den Tatbestandsmerkmalen enthalten sind (Computerkriminalität) oder bei denen die IuK zur Planung, Vorbereitung oder Ausführung einer Tat eingesetzt wird/wurde
- Straftaten im Zusammenhang mit Datennetzen wie z.B. dem Internet
- Fälle der Bedrohung von Informationstechnik
-

Letzteres schließt alle widerrechtlichen Handlungen gegen die Integrität, Verfügbarkeit und Authentizität von elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeicherten oder übermittelten Daten (Hacking, Computersabotage, Datenveränderung, Missbrauch von Telekommunikationsmitteln etc.) ein.

Bei der Begriffsdefinition wird jedoch deutlich, dass diese einen sehr weitläufigen Bereich abdeckt. Dies liegt an den vielschichtigen Varianten der aktuellen Kriminalität unter Einbezug des Internets sowie der dynamischen Weiterentwicklung der Computertechnik. Im Wesentlichen haben sich die zwei Begriffe Computerkriminalität im engeren Sinne und Computerkriminalität im weiteren Sinne durchgesetzt.

3.1 Computerkriminalität im engeren Sinne

Bei der **Computerkriminalität im engeren Sinn** handelt es sich um Delikte, bei denen in den Tatbestandsmerkmalen der jeweiligen Norm (Straftat oder auch Ordnungswidrigkeit) Elemente der elektronischen Datenverarbeitung genannt sind. Darunter fallen beispielsweise der Computerbetrug (§ 263a StGB), das Ausspähen und Abfangen von Daten (§§ 202a, 202b, 202c StGB), die Datenveränderung sowie die Datensabotage (§§ 303a und 303b StGB), Fälschung beweiserheblicher Daten (§ 269 StGB) oder die Störung öffentlicher Betriebe (§ 316b StGB). Daneben befassen sich weitere Gesetze mit diesen Deliktarten. So zum Beispiel das Urheberrechtsgesetz (UrhG), das Bundesdatenschutzgesetz (BDSG), das Telekommunikationsgesetz (TKG), das Gesetz gegen den unlauteren Wettbewerb (UWG) oder das Gesetz über den Schutz von Marken und sonstigen Kennzeichen (MarkenG).

3.2 Computerkriminalität im weiteren Sinne

Unter den Begriff **Computerkriminalität im weiteren Sinn** fallen Straftaten, für deren Durchführung ein elektronisches Datenverarbeitungssystem unter Einbezug von Informations- und Kommunikationstechnik genutzt wird. Dazu zählen zum Beispiel der Warenkreditbetrug, Propagandastraftaten aus extremistischen Kreisen, Gewaltverherrlichung, das Verbreiten von Kinderpornografie oder Beleidigungstatbestände.

Mit der weltweiten Zunahme der Internetnutzung wird die Verbreitung strafbarer Inhalte dieser Kategorien vereinfacht. Aus der Definition lassen sich insofern Tathandlungen ableiten, zu deren Begehung das Internet und vorhandene gespeicherte Daten genutzt (Phishing, Betrug, Urheberrechtsverletzungen, Kreditkartenmissbrauch oder Propagandastraftaten, Cybermobbing), neue Daten generiert und veröffentlicht (Verbreitung von (Kinder-)Pornographie, Verbreitung terroristischer Ideologien, Gewaltdarstellungen, Aufstachelung zum Rassenhass) oder Angriffe auf das Medium Internet selbst durchgeführt werden (Verbreitung von Viren, Würmern und Trojanern, Eindringen in PC-Anlagen zur Datenänderung, Datenlöschung oder zum Datendiebstahl, „Denial of Service“ -Attacken).

3.3 Abgrenzung zum IuK-Strafrecht

Mit dem Begriff Cybercrime wird also auf Handlungen abgestellt, d.h. auf die Erscheinungsformen, Funktionsabläufe, Merkmale und Tathandlungen. Dagegen geht es beim Informations-und-Kommunikationstechnik-Strafrecht (kurz: IuK-Strafrecht), dessen materielle Gesetze über das StGB und einige Spezialgesetze verteilt sind, um die (materiell-) strafrechtliche Bewertung der Erscheinungsformen und Varianten des Cybercrime. Dabei unterfallen dem Cybercrime alle kriminellen Erscheinungsformen, die entweder an informationstechnischen Systemen (IuK-Strafrecht im engeren Sinne) oder durch ihre spezifische Nutzung begangen werden (IuK-Strafrecht im weiteren Sinne).

3.4 Computerkriminalität in der Statistik

Wie für viele andere Phänomene wird über das Problem der Kriminalität in Deutschland Statistik geführt. Besonders hervor sticht dabei die Polizeiliche Kriminalstatistik (PKS). Allerdings hat diese einige Probleme bei der vollumfänglichen Darstellung von Computerkriminalität bzw. Cybercrime im engeren Sinne. Auf die Lösung des beschriebenen PRoblems und weitere Details zur Statistik im Bereich der Computerkriminalität wird im folgenden Kapitel eingegangen.

3.4.1 Kriminalstatistiken

Kriminalstatistiken sind amtliche kriminologische Statistiken, die strafbares und rechtswidriges Verhalten quantitativ erfassen. Sie sind regional begrenzt auf wohldefinierte Gebiete, wie z.B. Staatsgebiete oder Bundesländer. Damit ist der Geltungsbereich der Statistik klar abgegrenzt. Kriminalstatistiken allgemein beinhalten Informationen zu:

- Täter und deren Gruppierungen
- Opfer
- Fälle
- Ermittlungsverfahren
- Schäden
- Strafrechtliche Folgen

Die in Deutschland einschlägigen Kriminalstatistiken sind die folgenden:

- Polizeiliche Kriminalstatistik (PKS) des Bundes
- PKS der Länder
- Bundeslagebilder verschiedener Deliktsbereiche
- Staatsanwaltliche Erledigungsstatistik (StA-Statistik)
- Strafverfolgungsstatistik (in dt. Gerichten abgeurteilte Personen)
- Strafvollzugsstatistik (Demographie, Kriminologie, Bestand der Gefangenen)

3.4.2 Die polizeiliche Kriminalstatistik

Die Polizeiliche Kriminalstatistik (PKS) für die Bundesrepublik Deutschland wird vom Bundeskriminalamt auf der Grundlage, der von den 16 Landeskriminalämtern gelieferten Landesdaten erstellt. Die PKS enthält die der Polizei bekannt gewordenen rechtswidrigen Straftaten einschließlich der mit Strafe bedrohten Versuche, die Anzahl der ermittelten Tatverdächtigen und eine Reihe weiterer Angaben zu Fällen, Opfern oder Tatverdächtigen. Nicht enthalten sind:

- Staatsschutzdelikte
- Verkehrsdelikte
- Ordnungswidrigkeiten
- Delikte, die nicht zum Aufgabenbereich der Polizei gehören (z.B. Finanz- und Steuerdelikte)
- Straftaten, die unmittelbar bei der Staatsanwaltschaft angezeigt werden.

In der PKS werden die der Polizei bekannt gewordenen und durch sie endbearbeiteten Straftaten aufgenommen, einschließlich der mit Strafe bedrohten Versuche und der vom Zoll bearbeiteten Rauschgiftdelikte und eine statistische Erfassung erst bei Abgabe an die Staatsanwaltschaft erfolgt. Nicht enthalten sind Staatsschutzdelikte, Verkehrsdelikte (mit Ausnahme der Verstöße gegen §§ 315, 315b StGB und § 22a StVG), Straftaten, die außerhalb der Bundesrepublik Deutschland begangen wurden, Ordnungswidrigkeiten und Verstöße gegen strafrechtliche Landesgesetze, mit Ausnahme der einschlägigen Vorschriften in den Landesdatenschutzgesetzen.

Die PKS wird jeweils im Frühjahr vom Bundeskriminalamt (BKA) veröffentlicht. Dabei werden in einem Jahr die Statistik des Vorjahres (Berichtsjahres) bekanntgegeben. Seit 2014 erfolgt zudem keine Veröffentlichung mehr in gedruckter Form, sondern ausschließlich digital auf der Webseite des BKA. Dabei kann dort zur Grobübersicht über aktuelle Trends und Phänomene der Bericht des IMK heruntergeladen werden. Für einen detaillierten Einblick in die Statistik werden die Tabellen der PKS veröffentlicht, welche zu jedem Deliktbereich ein separaten Summenschlüssel enthalten.

Im IMK-Bericht können beispielsweise die langfristigen Entwicklungen bis 15 Jahre in die Vergangenheit nachvollzogen werden. Besonders im Bereich Cybercrime können hier signifikante Anstiege festgestellt werden. Zudem gibt der Bericht Aufschluss über Anteile der Tatverdächtigen. Diese werden getrennt aufgeschlüsselt nach Geschlecht, Alter und Anteil an nichtdeutschen TV. Zudem werden die Opfer genauer betrachtet, welche ebenfalls nach den gleichen Kriterien aufgeschlüsselt werden. Besonders betrachtet werden an dieser Stelle Vollstreckungs- und Polizeivollzugsbeamte als Opfer von Kriminalität in Deutschland.

3.4.2.1 PKS-Tabellen

Für die Analyse der der detaillierten Zahlen soll an dieser Stelle eine kurze Erläuterung der PKS-Tabellen zu finden sein. Eine Beispielhafte Tabelle aus der PKS ist in Abbildung 5 zu sehen.

Polizeiliche Kriminalstatistik — **Tabelle 01**
Grundtabelle — Bereich: Bundesrepublik Deutschland (70)
V1.0 erstellt am: 14.02.2023 — Berichtszeitraum: 01.01.2022 bis 31.12.2022

Schlüssel	Straftat	Anzahl erfasste Fälle	%-Anteil an allen Fällen	erfasste Fälle davon: Versuche Anzahl	Versuche in %	Tatortverteilung bis unter 20.000 Einwohner	20.000 bis unter 100.000	100.000 bis unter 500.000	500.000 und mehr	unbekannt	mit Schusswaffe gedroht	mit Schusswaffe geschossen	Aufklärung Anzahl Fälle	Aufklärung in % (AQ)	Tatverdächtige insgesamt	Tatverdächtige männlich	Tatverdächtige weiblich	Nichtdeutsche Tatverdächtige Anzahl	Nichtdeutsche Tatverdächtige Anteil an TV
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
------	Straftaten insgesamt	5.628.584	100,0	414.197	7,4	1.304.904	1.508.727	1.099.424	1.572.975	142.554	4.092	4.442	3.226.935	57,3	2.093.782	1.565.240	528.542	783.876	37,4
000000	Straftaten gegen das Leben	3.077	0,1	1.770	57,5	887	974	566	635	15	8	133	2.732	88,8	3.539	2.950	589	1.270	35,9
010000	Mord § 211 StGB	662	0,0	451	68,1	205	160	122	166	9	3	59	604	91,2	763	654	109	293	38,4
010079	Sonstiger Mord	625	0,0	425	68,0	192	155	114	155	9	3	55	570	91,2	711	604	107	269	37,8
011000	Mord im Zusammenhang mit Raubdelikten	29	0,0	23	79,3	11	4	6	8	0	0	4	26	89,7	46	44	2	23	50,0
012000	Mord im Zusammenhang mit Sexualdelikten	8	0,0	3	37,5	2	1	2	3	0	0	0	8	100,0	8	8	0	2	25,0
020000	Totschlag und Tötung auf Verlangen §§ 212, 213, 216 StGB	1.574	0,0	1.272	80,8	439	518	275	340	2	5	73	1.494	94,9	1.948	1.728	220	823	42,2
020010	Totschlag § 212 StGB	1.549	0,0	1.267	81,8	431	510	271	336	1	5	69	1.469	94,8	1.926	1.712	214	818	42,5
020020	Minder schwerer Totschlag § 213 StGB	1	0,0	1	100,0	1	0	0	0	0	0	0	1	100,0	2	2	0	2	100,0
020030	Tötung auf Verlangen § 216 StGB	24	0,0	4	16,7	7	8	4	4	1	0	4	24	100,0	21	15	6	3	14,3
030000	Fahrlässige Tötung § 222 StGB - nicht i.V.m. Verkehrsunfall -	748	0,0	0	0,0	225	270	147	104	2	0	1	543	72,6	745	508	237	111	14,9
040000	Abbruch der Schwangerschaft §§ 218, 218b, 218c, 219a, 219b StGB	93	0,0	47	50,5	18	26	22	25	2	0	0	91	97,8	96	72	24	52	54,2
040010	Schwangerschaftsabbruch § 218 StGB	92	0,0	47	51,1	18	26	21	25	2	0	0	90	97,8	95	72	23	52	54,7
040020	Schwangerschaftsabbruch ohne ärztliche Feststellung, unrichtige ärztliche	1	0,0	0	0,0	0	0	1	0	0	0	0	1	100,0	1	0	1	0	0,0
040030	Ärztliche Pflichtverletzung § 219c StGB	0	0,0	0	0,0	0	0	0	0	0	0	0	0	0,0	0	0	0	0	0,0
040040	Werbung für den Abbruch der Schwangerschaft § 219a StGB	0	0,0	0	0,0	0	0	0	0	0	0	0	0	0,0	0	0	0	0	0,0
040050	Inverkehrbringen von Mitteln Schwangerschaftsabbruch § 219b StGB	0	0,0	0	0,0	0	0	0	0	0	0	0	0	0,0	0	0	0	0	0,0
100000	Straftaten gegen die sexuelle Selbstbestimmung insgesamt	118.196	2,1	2.902	2,5	35.631	33.298	20.581	23.201	5.485	27	2	98.376	83,2	88.730	79.147	9.583	23.637	26,6
110000	Straftaten gegen die sexuelle Selbstbestimmung §§ 174, 174a, 174b, 174c	37.076	0,7	1.855	5,0	9.036	10.566	7.662	9.411	401	26	2	29.710	80,1	27.922	27.347	575	10.397	37,2
111000	Vergewaltigung, sexuelle Nötigung und sexueller Übergriff im besonders s	11.896	0,2	987	8,3	2.998	3.325	2.393	2.992	188	19	2	9.960	83,7	10.045	9.913	132	3.679	36,6

Abbildung 5: Auszug aus der Grundtabelle T01 aus dem Berichtsjahr 2022 zur Übersicht über die enthaltenen Informationen in der PKS

Vorangestellt sind den Deliktsbereichen Summenschlüssel. Diese dienen der eindeutigen Identifizierung eines beobachteten Delikts. Dabei werden zusammengehörige Delikte im Summenschlüssel im gleichen Zahlenbereich angesiedelt. In der Abbildung gehören bspw. Alle Tötungsdelikte zum Summenschlüssel 10000.

In der folgenden Spalte wird das beobachtete Delikt genauer beschrieben, wobei in der Regel immer der einschlägige Strafrechtsparagraph zu finden ist, gegen die die beschriebene Handlung verstößt. Danach folgt die absolute Anzahl an erfassten Fällen für den Deliktsbereich, sowie die relative Häufigkeit gegenüber der Gesamtzahl an erfassten Fällen im Berichtsjahr. In den darauffolgenden Spalten werden ebenso absolut und relativ die erfassten, strafbaren Versuche dargestellt. Die folgende Tatortverteilung spiegelt wider in welchen Bereichen das Delikt vorrangig beobachtet werden konnte. Dabei erfolgt eine Abstufung der Einwohnerzahl der Städte in Deutschland.

Separat werden ebenfalls Fälle mit Schusswaffengebrauch in der PKS festgehalten. Dabei wird erneut aufgeschlüsselt ob bei dem Fall nur mit der Waffe gedroht oder geschossen wurde.

Eine besondere Zahl spiegelt die Aufklärungsquote in der PKS wider. Für den zutreffenden Deliktsbereich werden die aufgeklärten Fälle erfasst, sowie die Aufklärungsquote als relative Angabe zu den erfassten Fällen im beobachteten Deliktbereich. Schließlich werden die Tatverdächtigen näher betrachtet. Hier wird erneut eine Einteilung in deutsche und nicht-deutsche Tatverdächtige unternommen, welche wiederum nach dem biologischen Geschlecht unterteilt werden.

3.4.2.2 Wichtige Zahlen in der PKS

In der Analyse der einzelnen Informationen in der PKS sind bereits einige wichtige Zahlen vorkommen, welche folgend eine nähere Erläuterung bekommen. Wichtig für die Analyse sind die erfassten Fälle für einen Deliktsbereich. Erfasst sind alle Straftaten und unter Strafe gestellte Versuche, wenn sie der Polizei auf irgendeinem Wege bekannt geworden sind. Dazu zählen das Bekanntwerden durch Anzeige eines Bürgers, Entdeckung einer Straftat durch die Polizei oder das anderweitige Erlangen von Kenntnis über eine Straftat.

Eine weitere wichtige Zahl, welche in der PKS betrachtet wird, ist die Aufklärungsquote. Die Aufklärungsquote ist die relative Anzahl der aufgeklärten Straftaten als Anteil der insgesamt erfassten Straftaten im Berichtsjahr. Dabei wird diese Quote nach der folgenden Vorschrift berechnet:

$$AQ = \frac{aufgklärte\ Fälle \cdot 100}{bekannt\ gewordene\ Fälle}$$

Die Frage stellt sich, wann ein Fall im Rahmen der PKS als aufgeklärt zu bezeichnen ist. Ein Fall ist aufgeklärt, wenn mindestens ein Tatverdächtiger festgestellt werden konnte und dessen Personalien bekannt sind. Dabei kann das Bekanntwerden der Personalien durch ein Ausweisdokument oder eine ED-Behandlung erfolgen.

Interessant ist, dass eine Aufklärungsquote von mehr als 100 % entstehen kann. Das passiert dann, wenn in einem Berichtsjahr mehr Fälle einer Straftat aufgeklärt, als erfasst wurden. Dazu kann es kommen, wenn ein Überhang an Fällen aus vorherigen Jahren besteht, welcher im Berichtsjahr aufgeklärt wurde.

Trotz der detaillierten Darstellung der Kriminalität innerhalb der PKS, kann das Thema Cybercrime nicht vollumfänglich abgebildet werden. Dazu tragen mehrere Faktoren bei, welche im letzten Teil über die PKS noch dargelegt werden sollen. Das erste Problem resultiert daraus, dass die Fälle von Cybercrime nur einmal innerhalb der PKs erfasst werden können. Wird bspw. Ransomware in einem Firmennetz verbreitet, wobei nicht nur Systeme verschlüsselt werden, sondern auch Daten abgezogen werden, kann dies entweder als Vorfall nach § 202a StGB Ausspähen von Daten oder nach § 303a Datenveränderung in die PKS eingehen. Die durch Cyberangriffe entstehenden Schäden werden ebenfalls nicht dokumentiert. Dabei muss betrachtet werden, wie lang ein System ausgefallen ist, als auch die Frage, wie viel Gewinn durch den Ausfall der IT verloren gegangen ist.

Weiterhin sind länderübergreifende Angriffe ein Problem, welches nicht analysiert werden kann. Besonders bei Angriffen, wo nicht ermittelt werden kann, aus welchem geografischen Bereich ein Täter kommt, wird der Tatort als unbekannt aufgenommen, was so in der PKS nicht abgebildet werden kann.

Es kann dazu kommen, dass sich von Berichtsjahr zu Berichtsjahr, die Schlüssel der einzelnen Deliktsbereiche ändern. Das passiert durch sich ständig ändernde Phänomene im Bereich Cybercrime. Das führt wiederum dazu, dass die sich die Zahlen von Jahr zu Jahr schlechter analysieren lassen.

Als letztes Problem ist zu nennen, das Opfer nicht ausreichend analysiert werden. Im Bereich Cybercrime ist vor allem interessant, was nach aktuellen Trends beliebte Ziele bei Angreifern sind. Diese sollte so weit unterschieden werden, dass die Awareness in den entsprechenden Bereich erhöht und gefördert werden kann. Was wiederrum damit einhergeht, dass anhand der Zahlen aus dem vorherigen Berichtsjahr Handlungsmaßnahmen für die kommenden Jahre getroffen werden sollen. [3]

3.4.3 Bundeslagebild Cybercrime

Im Gegensatz zur PKS stellt das Bundeslagebild Cybercrime einen deutlich umfassenderen Blick dar in Hinsicht auf das Phänomen Cybercrime. Ein Lagebild ist eine Sammlung von georeferenzierten echtzeitnahen Daten über ein wohldefiniertes Phänomen. Es beinhaltet vorrangig Informationen von Behörden, Sensoren und Plattformen, die über gesicherte Kanäle übermittelt wurden. Das Ziel eines Lagebildes ist das Teilen der zusammengetragenen Informationen mit anderen informationsbedürftigen Einheiten, um ein Lagebewusstsein zu erlangen und Reaktionsfähigkeit zu verbessern.

Das Bundeslagebild Cybercrime wird vom Bundeskriminalamt (BKA) erstellt und bietet einen umfassenden Überblick über die aktuellen Erkenntnisse und Entwicklungen im Bereich der Cyberkriminalität in Deutschland und reflektiert die Ergebnisse polizeilicher Strafverfolgungsmaßnahmen. Der Fokus des Bundeslagebildes Cybercrime liegt auf Cybercrime im engeren Sinne (CCieS). Delikte, bei denen das Internet hauptsächlich als Tatmittel dient (CCiwS), werden nicht im Bundeslagebild Cybercrime berücksichtigt.

Die statistischen Daten des Bundeslagebildes basieren auf der Polizeilichen Kriminalstatistik (PKS), welche das Hellfeld der polizeilich bekannten Kriminalität abbildet. Aussagen über das Dunkelfeld, also über Straftaten, die der Polizei nicht bekannt sind, können aus den statistischen Grunddaten der PKS nicht abgeleitet werden. Da das Dunkelfeld im Bereich Cybercrime überdurchschnittlich groß ist, ist es von besonderer Bedeutung, externe polizeiliche Erkenntnisse in die Lagebeschreibung einzubeziehen. Daher werden neben den polizeilichen Daten auch Erkenntnisse und Einschätzungen anderer Behörden sowie ausgewählter privatwirtschaftlicher oder wissenschaftlicher Einrichtungen und Verbände in das Bundeslagebild Cybercrime einbezogen.

Wie auch die PKS wird das Bundeslagebild Cybercrime immer für das vorhergehende Berichtsjahr veröffentlicht. Allerdings wird es erst Mitte des Folgejahres veröffentlicht und damit etwa ein viertel Jahr nach der PKS. Das Bundeslagebild besteht nur aus dem Bericht des BKA, welcher phänomenspezifische Informationen enthält und über die genannten Informationen berichtet.

Darüber hinaus umfasst das Bundeslagebild die folgenden Informationen:

- Fallzahlen, Trends und aktuelle Schwerpunkte im Bereich des Cybercrime
- Herausstellen relevanter Phänomenbereiche und deren aktuellen Charakteristika
- Projektion verschiedener Straftaten auf den Bereich des Cybercrime
- Zusammenfassung verschiedener Tätergruppen, Tatorte und Rechtsgebiete des Cybercrime
- Darstellung von Schadenssummen
- Analyse der Strukturen von Tätergruppierungen
- Darstellung relevanter Ereignisse im Bereich Cybercrime

Polizeiliche Kriminalstatistik	Bundeslagebild Cybercrime
Jährliche Zusammenstellung registrierter Kriminalität in Deutschland	Spezialisierte Analyse der Cyberkriminalität in Deutschland und im internationalen Raum
Basiert auf den Daten der Landeskriminalämter	Basiert auf der PKS + Anreicherung durch externe Erkenntnisse und Expertise
Darstellung aller Kriminalitätsbereiche	Konzentration auf Cybercrime im engeren Sinne
Ziel: ➢ Trends aufzeigen ➢ Arbeit der Polizei zu bewerten ➢ Kriminalpolizeiliche Maßnahmen planen	**Ziel:** ➢ Analyse der Täterverhalten ➢ Identifikation der Täterstrukturen ➢ Bedrohungs- und Risikobewertung ➢ Definition von Präventionsmaßnahmen

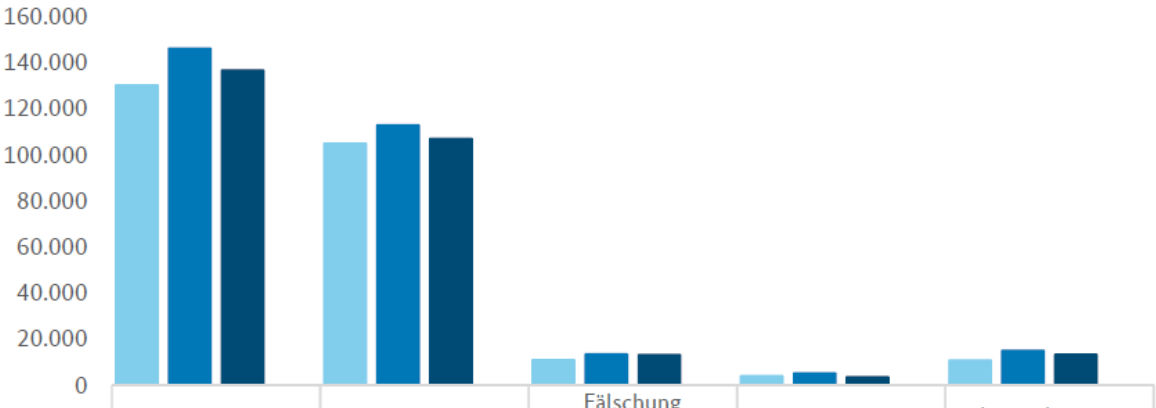
Abbildung 6: Vergleich PKS und Bundeslagebild

3.4.4 Aktuelle Trends und Zahlen

Die Zahlen und Daten aus dem folgenden Kapitel stammen aus dem Bundeslagebild und der polizeilichen Kriminalstatistik aus dem Berichtsjahr 2022. Die Daten besonders in Hinblick auf CCieS entstammen dem Bundeslagebild Cybercrime.

Abbildung 7: Zusammenfassung aus dem Bundeslagebild Cybercrime 2022

Zu sehen ist in Abbildung 7: Zusammenfassung aus dem Bundeslagebild Cybercrime 2022, dass besonders Phishing, DDoS und Ransomware bedeutende Rollen in den letzten Jahren spielen. Innerhalb der PKS finden sich die einzelnen Delikte im Bereich CCieS unter dem Summenschlüssel 897000. Insgesamt stieg die Kriminalität nach der PKS um 11,5% an, wobei die Kriminalität im Bereich CCieS um 6,5 % fiel. Insgesamt stellt Cybercrime an der Gesamtkriminalität einen Anteil von 2,4 % dar. Das ist im Vergleich zu Delikten, wie Diebstahl oder Raub ein vergleichbar geringer Anteil. Dabei ist eine Aufklärungsquote von 29,2 % zu beobachten. Dabei teilen sich die erfassten Fälle in die in Abbildung 8 dargestellten Phänomene:



	CC gesamt	Computerbetrug	Fälschung beweiserheblicher Daten, Täuschungen im Rechtsverkehr bei Datenverarbeitung	Datenveränderung, Computersabotage	Ausspähen von Daten einschl. Vorbereitungs-handlungen und Datenhelerei
2020	130.477	105.049	10.895	3.770	10.763
2021	146.363	113.002	13.390	5.053	14.918
2022	136.865	107.165	13.043	3.451	13.206
Diff. zu 2021	-6,5%	-5,2%	-2,6%	-31,7%	-11,5%

Abbildung 8: Verteilung der Kriminalität auf die Phänomenbereiche

Im Sinne der einschlägigen Strafrechtsparagraphen sind einige besondere Phänomene gut zu beobachten. Im Jahr 2022 waren die folgenden Trends in bemerkenswert und wurden im Bundeslagebild Cybercrime separat behandelt und dargelegt.

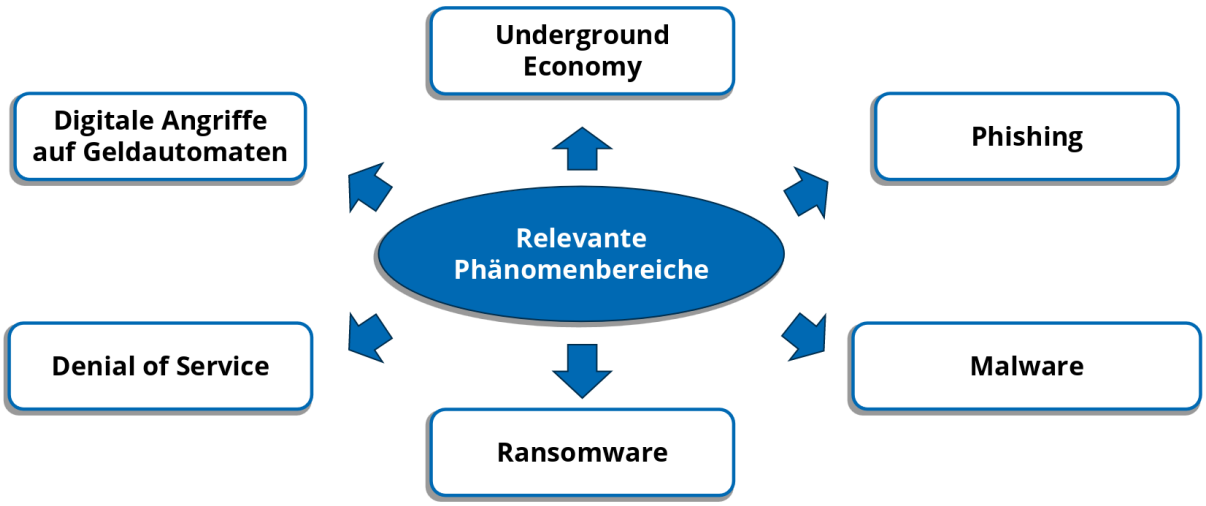


Abbildung 9: Trends aus dem Bundeslagebild Cybercrime 2022

Zum Thema Underground Economy konnte festgestellt werden, dass durch den Takedown des Hydramarkets ein deutlich Rückgang deren Umsatz festzustellen war. Im Jahr 2021 konnte der Markt einen Umsatz von 3,1 Mrd $ verzeichnen, wohingegen 2022 nur noch 1,5 Mrd. $ umgesetzt werden konnten. Ein besonderes zu beachtendes Problem ist Cybercrime as a Service (CaaS) auf den Handelsplattformen im Darknet. Dadurch ist es möglich für mietvertragsähnliche Abkommen Botnetze oder Trojaner für Jedermann zu mieten. Das erleichtert das Angreifen durch nicht technikaffine Menschen immens.

Malware und im Besonderen Ransomware sind nach wie vor ein Thema von großem Interesse. Dabei steigen sowohl die Angriffszahlen an sich als auch das Schadenspotenzial der Angriffe. Mit durchschnittlich 270.000 $ Lösegeldzahlungen pro Angriff konnten die Täter einen Gesamtgewinn von ca. 457 Mio. $ erzielen. Allerdings ist festzuhalten, dass trotz der hohen geforderten Lösegeldsummen immer weniger Unternehmen die Summen bezahlen.

Als größtes Eintrittstor in ein IT-System gilt das Phishing. Dabei wird klassisch die Schwachstelle Mensch ausgenutzt. Schwerwiegend ist, dass Produkte, um Phishing-Angriffe durchzuführen, im Rahmen der Underground Economy erworben werden können. Damit ist es auch für nicht technikaffine Menschen möglich einen solchen Angriff zu fahren.

Als letztes wichtiges Thema ist DDoS anzusprechen. Diese Art von Angriffen hat eine neue Bedeutung im Russland-Ukraine-Krieg gewonnen. Im vorherigen Berichtsjahr wurden DDoS-Angriffe vor allem auf Produkte im Homeoffice-Bereich gefahren. Mittlerweile hat sich das Interesse dieser Angriffe zu einer politischen Motivation gekehrt, um als Waffe im Russland-Ukraine-Cyberkrieg zu fungieren. Allerdings wurden durch die Schließung des Hydra-Markets um weiten weniger Angriffe durch DDoS-as-a-Service festgestellt.

3.5 Das Cybercrime-Phänomen Hacktivismus

Ob aus der Presse oder durch eigenes Erleben ist heute jeder schon mit den Begriffen Hacking, Cybercrime, Cyberspace, Cybermobbing oder digitaler Identitätsklau in Berührung gekommen. Der Begriff Hackerattacke ist in unsere Alltagssprache ebenso eingezogen.

Der Begriff **Hacker** hat eine Metamorphose in seiner Begrifflichkeit durchlebt. Waren am Anfang damit besondere Tüftler gemeint, so wird er heute im Zusammenhang mit Cyberverbrechen benutzt. In den 1960er Jahren tauchte der Begriff Hacker zum ersten Mal in den USA am MIT (Massachusetts Institute of Technology) auf. Hier wurde ein Team von Studenten als Hacker betitelt, die Maschinen auseinander bauten, um sie im Anschluss umzukonstruieren. Ziel war neben dem haptischen Gefühl, eine deutliche Leistungssteigerung. Umtriebige Absichten mit diesen Arbeiten wurden nicht verfolgt.

Die Geburtsstunde des eigentlichen Hackens liegt im Jahr 1969. Wie so oft in der technischen Entwicklung war auch dieses Ereignis durch einen Zufall gefördert. Der Amateurfunker John Draper, später als „Captain Crunch“ bezeichnet, entdeckte, dass eine Spielzeugpfeife, welche in den Frühstücksflocken von Cap’n Crunch als Werbegeschenk enthalten war, benutzt werden kann, um einen Ton zu erzeugen, der Ferngespräche freischaltete. Dieser Tipp machte die Runde und schon konnten Freunde und Bekannte kostenlos telefonieren.

Von diesem zufälligen Ereignis beflügelt gründete sich der erste Computer Club. In den 1980er Jahren sind die Hacker dann aus dem Schatten getreten und wurden auch bald von der breiten Öffentlichkeit wahrgenommen. Der damals erst 17-jährige Kevin Poulsen drang in das ARPAnet (Vorläufer des heutigen Internets) ein. Jedoch war dies nur dem Militär und den führenden Universitäten vorbehalten.

1983 lief in den Kinos der Streifen „Wargames - Kriegsspiele“ von John Badham. Hier wurde die Geschichte eines jungen Hackers erzählt. Durch diesen filmischen Katalysator tauchten 1988 die ersten Computerviren auf. Von nun an musste man den Begriff Hacker eindeutig als negative Begrifflichkeit vor Augen haben. In den 1990er Jahren wurden das gesamte Ausmaß und die dunklen Seiten des Hackens deutlich. Durch das Internet wurden die ersten Straftaten in Bezug auf Cyberkriminalität begangen.

Die Gemeinde spaltete sich bis zum heutigen Tage in eine schwarze und weiße Community. Auf der einen Seite stehen die „Black-Hats“, die aus kriminellen Gründen hacken, und auf der anderen die „WhiteHats “ , die vor allem auf Lücken in Sicherheitssystemen hinweisen wollen. Der Umfang und die Schwere der Taten der Black-Hats nahmen bald gewaltige Dimensionen an. Die ersten Fälle von Online-Banking-Missbräuchen gingen durch die Presse. Dies setzte sich in das 21. Jahrhundert fort. Der Begriff **Cracking**, das Überwinden von Sicherheitshindernissen, machte die Runde und ergänzte die Cyberkriminalität. Das Kopieren von DVDs und Plattformen zum Austausch wurden erschaffen. Aber auch Webseiten wie WikiLeaks wurden erstellt, um sensible und geheime Dokumente der allgemeinen Bevölkerung zugänglich zu machen. Die heutigen Ausprägungen der Hacker und deren Schwerpunktziele sind vielschichtiger geworden. Im Folgenden der Versuch diese zu systematisieren:

Black-Hat: hacken sich mit der Absicht, Schaden anzurichten, in Datensysteme ein. Sie handeln teilweise mit kriminellen Absichten.

White-Hat: richtet normalerweise nur begrenzten Schaden an. Sein Hauptziel ist, Sicherheitslücken im System aufzudecken. Er meldet oft diese Lücken den Verantwortlichen. Man sollte ihm keine kriminellen Absichten unterstellen, doch in einigen Fällen verursachen auch White-Hats Schaden. Um dies zu unterstützen, wurde der **Grey-Hat** in die Familie aufgenommen. Er kann sowohl zur Verbesserung der Systemsicherheit beitragen als auch Schäden anrichten.

Die Gruppe der Wettstreiter bekommen den Namen **Script Kiddies**. Sie haben kaum technische Kompetenzen und bedienen sich der Tools anderer. Nach dem Motto, wer will nicht mal Hacker sein.

Neu ist die Gruppe der **Hacktivisten**. Diese setzen ihr technisches Wissen für einen politischen Zweck ein und verändern zum Beispiel eine Homepage, um politische Botschaften zu verbreiten, oder um auf Missstände aufmerksam zu machen.

Hacktivismus zeichnet sich insbesondere durch eine nichtprofitorientierte und ideologisch motivierte Ausübung von Taten zum Zwecke des Protests und der Propaganda aus und wird überwiegend von Gruppierungen ausgeübt. Diese Gruppierungen haben keine feste Mitgliederzahl, keine Hierarchie und keine Kontrolle und üben häufig auch Aktivitäten ohne hacktivistische Ausrichtung aus (wie z. B. bloßes Hacking oder „Spaßaktionen“ wie bei Anonymous). Einzeltäter sind eher selten, da sich politisches und soziales Engagement in Gruppen ausdrückt. Die Mehrheit (ca. 90 %) der hacktivistisch agierenden Personen sind männlich und zwischen 16 und 30 Jahren alt.

Hacktivisten nutzen ähnliche Vorgehensweisen wie andere Cyberkriminelle – wie z. B. DDoS-Angriffe, Web-Defacements, Ausspähen von Daten etc. – jedoch mit einer anderen Zielrichtung: So agieren Hacktivisten niemals profitorientiert, sondern um sich für ideologische Zwecke und Prinzipien einzusetzen und Sympathisanten zu mobilisieren. Dass dabei dennoch materieller Schaden entstehen kann, zeigen die folgenden Beispiele:

In den Medien wird **Anonymous** meist als Hacker-Kollektiv, -Netzwerk oder -Gruppe beschrieben oder auch als Bewegung. Die Aktivisten distanzieren sich selbst von den Begriffen Hacker und Gruppe. Sie legen Wert darauf, eine „Lebenseinstellung, ein Gedanke, eine Idee“ zu sein. Sie identifizieren sich mit dem Wert der Meinungsfreiheit. Klar ist natürlich: Es ist nicht das abstrakte

Ideal, das vor Computern sitzt und ISIS-Terroristen hinterher hackt. Es sind reale Menschen, die sich im Rahmen ihrer Aktivität für Anonymous nicht mit ihrem Klarnamen erkenntlich machen wollen und wissen, welche technischen Möglichkeiten es gibt, sich im Netz unerkannt zu bewegen.

Anonymous hat es sich zur Aufgabe gemacht, die persönliche Meinungsfreiheit zu verteidigen — online und offline. Auf der deutschen Homepage wird die englische Schriftstellerin Evelyn Beatrice Hall (1868 - 1956) zitiert: „Ich missbillige, was du sagst, aber würde bis auf den Tod dein Recht verteidigen, es zu sagen“. Im Speziellen richtet sich Anonymous nach Selbstaussage gegen die Überwachung im Internet durch Geheimdienste, wie etwa die NSA. In den vergangenen Jahren gerieten aber auch Menschenrechtsverletzungen und Organisationen wie Scientology oder der Ku-Klux-Klan ins Visier der Hacker. Ihr Selbstverständnis formulieren Anonymous wie folgt:

„Wissen ist frei. Wir sind anonym. Wir sind viele. Wir vergeben nichts. Wir vergessen nichts. Rechnet mit uns.“ Wie man sich vorstellen kann, gibt es kein Gründungsprotokoll wie bei einem deutschen Taubenzüchterverein. Anonymous ist viel mehr organisch aus den Untiefen der sogenannten Imageboards im Netz entstanden. Das sind Foren, auf denen Fotos und Texte frei geteilt werden können, ohne dass eine Instanz zensiert oder moderiert. Ein solches Imageboard wurde letztes Jahr etwa zur Veröffentlichung dutzender Fotos aus gehackten Cloud-Accounts von Schauspielerinnen genutzt. Auf diesen Plattformen bewegen sich viele Mitglieder ohne Angabe des Klarnamens oder eines Spitznamens. Sie heißen dann „Anonymous“. Es wird vermutet, dass dieser technische Umstand der Bewegung den Namen gegeben hat. Anfang 2008 trat sie erstmals größer in Erscheinung.

Abbildung 10: Webseite der Organisation Anonymous (http://du-bistanonymous.de)

Die Hacker griffen konzertiert die Scientology-Sekte an. Anonymous hat, soweit bekannt, keine Führung, keine Administration und keine hierarchische Struktur. Die Aktivisten organisieren sich virtuell über Messageboards, verschlüsselte Chats und Wikis. Auch das soziale Netzwerk Twitter wird genutzt. Die Hacker arbeiten unabhängig voneinander oder in kleinen Gruppen. Es gibt keine Mitgliedschaft oder ähnliches. Jeder kann mitmachen, der sich berufen fühlt und dieselben Ziele verfolgt. Wie bereits erwähnt organisierte Anonymous in den vergangenen Jahren eine Reihe von Hackangriffen gegen verschiedene Organisationen. Eine Auswahl der Attacken im Folgenden:

Nach Scientology nahm sich das Netzwerk 2011 die Westboro Baptist Church vor, die als besonders intolerant gilt. Im gleichen Jahr zielte die „Operation Darknet“ gegen Pädophile, die im Netz unerkannt kinderpornografische Inhalte verbreiten konnten.

2012 schaltete Anonymous die Websites von zwei ugandischen Regierungsorganisationen ab, nachdem die dortige Regierung Gesetze verabschiedete, die Homo-, Trans- und Bisexuelle diskriminierte. Im September dieses Jahres wurden 1000 Mitglieder des rassistischen KuKlux-Klans demaskiert. Anonymous stellte ihre Namen und Kontaktdaten online.

Die Maske (Abbildung 11) ist das Symbol der Bewegung, bekannt aus dem Film und Comic „V wie Vendetta“. Der Protagonist kämpft dort gegen ein autokratisches Regime. Anonymous-Aktivisten und -Sympathisanten tragen sie häufig bei Protestaktionen. Vorbild für die Maske ist der Brite und Katholik Guy Fawkes. Er war Offizier im Königreich England und verübte 1605 einen aus heutiger Sicht terroristischen Anschlag: Er ging mit Sprengstoff auf König Jakob I. und das englische Parlament los. Das grinsende Plastikgesicht hat viel zur Bekanntheit von Anonymous beigetragen. Es ist das Gesicht des berüchtigten Guy Fawkes, der vor 400 Jahren das britische Parlament sprengen wollte. Die Maske ist das Erkennungszeichen der Internet-Aktivisten. Bei Demonstrationen und in Video-Botschaften tragen die Mitglieder sie zur Tarnung.

In einem gesonderten Kapitel wird näher auf die Straftäter und eine mögliche Charakterisierung eingegangen.

Hier ein Rat: Hacking bringt nicht nur viele neue Freunde, sondern auch genauso viele neue Feinde.

Abbildung 11: Maske der Gruppierung Anonymous

4 Strafrechtliche Grundlagen

Eine eingehende wissenschaftliche Auseinandersetzung mit der Thematik des Cybercrime findet erst im Ansatz statt. Bereits die Ausgangsfrage, „Was ist strafrechtlich relevantes Verhalten an sich?“, bereitet nicht unerhebliche Schwierigkeiten.

4.1 Allgemeiner Verbrechensbegriff und Bedeutung des Strafrechts

4.1.1 Kriminologie als Lehre vom Verbrechen

Ausgehend von eben genannter Grundfrage befasst sich die Kriminologie als „Lehre vom Verbrechen“ mit den im menschlichen und gesellschaftlichen Bereich liegenden Umständen, die mit dem Zustandekommen, der Begehung, den Folgen und der Verhinderung von Straftaten sowie mit der Behandlung von Straffälligen zusammenhängen[11: § 1 A Rn. 1]. Hierbei bedient sie sich verschiedener Bezugswissenschaften, wie etwa Rechtswissenschaften, Psychologie, Soziologie, Pädagogik, Anthropologie und Ökonomie.

4.1.2 Verbrechen als Grundbegriff

Einen allgemein verbindlichen und überall geltenden Verbrechensbegriff (Verbrechen soll hierbei ganz „untechnisch“ als Bruch von Strafrechtsnormen verstanden werden und nicht – im Sinne der Definition nach § 12 StGB – als ein mit Freiheitsstrafe im Mindestmaß von einem Jahr bedrohter Straftatbestand (in Abgrenzung zum Vergehen für weniger schwerwiegende Delikte, bei denen auch geringere Freiheitsstrafen oder die Verhängung von Geldstrafen in Betracht kommt) gibt es nicht. Verbrechen lässt sich rein juristisch betrachten, kann aber auch in seinen engen Beziehungen zu Kultur, Religion und Moral gesehen werden. So gibt es etwa nach Auffassung der Lehre vom sog. labeling-approach das Verbrechen – wie überhaupt abweichendes Verhalten – als solches gar nicht; vielmehr würde bestimmten Verhaltensweisen erst im Wege konkreter gesellschaftlicher Definitionsprozesse Verbrechensqualität zugeschrieben. Nach der Theorie des Kulturkonflikts von Sellin kann sich Verbrechen demgegenüber auch schlicht als Folge eines Konflikts zwischen divergierenden Normen unterschiedlicher Bevölkerungsgruppen in einer komplexen Kulturgesellschaft ergeben; zu denken wäre etwa an eine Institution wie die süditalienische Vendetta (Blutrache), die in der Heimat als heilige Familien- bzw. Sippenpflicht gilt, in einem rechtsstaatlichen Land, in dem der Staat das Gewaltmonopol inne hat, jedoch automatisch zu gravierenden Normverstößen führt.

Beachte: Eine speziell auf Cybercrime zugeschnittene Kriminalitätstheorie existiert mangels entsprechender (Längs- und Querschnitts-) Analysen sowie evidenzbasierter Forschungsdaten bisher nicht, sodass eine Erklärung für Cybercrime nur unter Heranziehung bereits bestehender Theorien versucht werden kann. Im Zusammenhang mit Cybercrime spielt unter kriminologischer Betrachtungsweise sicherlich der Kontrollgesichtspunkt eine herausgehobene Rolle; etwa die fehlenden Selbstschutzmaßnahmen (z.B. Phishing), die erschwert durchführbaren Überwachungsmaßnahmen der Strafverfolgungsbehörden bei abstrakten Gefährdungsdelikten (z.B. Kinderpornographie) oder die eingeschränkte Selbstkontrolle der Täter (z.B. Cyber-Mobbing). Auch Kosten-Nutzen-Erwägungen sowohl auf Täter- wie auch auf Opferseite, z.B. der Aufwand bei der legalen Beschaffung von immateriellen Gütern wie Filmen und Musik oder der Aufwand bei der Installation von Sicherheitssoftware, ebenso Lerneffekte, Neutralisierungsmechanismen und Routineaktivitäten, sind von Bedeutung.

Grundsätzlich gilt: ein Verhalten wird erst durch normative Wertungen zu dem unter Strafe gestellten Verbrechen. Verbrechen ist somit normbezogen. Die unter Strafe gestellten Verhaltensweisen an sich, d.h. in ihrer rein äußerlichen Erscheinung, brauchen dabei nicht unbedingt sozialgefährlich oder abnorm bzw. unmoralisch zu sein.

Ein Beispiel [11: § 1 C Rn. 8]:

Prof. Dr. Michael Bock nennt hierzu als Beispiel etwa den Geschlechtsverkehr eines 25-jährigen Mannes mit einer 17-jährigen Frau. Vom Biologischen, auch von der heutigen Sexualmoral aus gesehen, ist hiergegen nichts einzuwenden. Je nach Status der beiden können sich nach Bock jedoch ganz außerordentliche Konsequenzen aufgrund strafrechtlicher Bewertung ergeben: Der Mann ist Abteilungsleiter, die ihm unterstellte Frau steht in einem Abhängigkeits- und Ausbildungsverhältnis zu ihm. Das Verhalten des Mannes kann damit bei Vorliegen weiterer Voraussetzungen gem. § 174 Abs. 1 Nr. 2 StGB als sexueller Missbrauch von Schutzbefohlenen bestraft werden. Noch deutlicher werde die Normenabhängigkeit, wenn man den Geschlechtsverkehr der beiden zu einem späteren Zeitpunkt bewertet: Sie haben geheiratet. Das gleiche Verhalten wird jetzt nicht nur als moralische, sondern sogar als rechtliche Pflicht gefordert.

Vor diesem Hintergrund wird deutlich, dass dasjenige, was man unter Verbrechen versteht, sich im Rahmen der Gesellschaftsentwicklung innerhalb der verschiedenen Gesellschaften durchaus und zum Teil erheblich ändern kann. Für die Auseinandersetzung mit dem Begriff des Verbrechens sind daher zwei Umstände von besondere Bedeutung: zum einen das Wissen darüber, dass sich die jeweilige Bewertung der Strafbarkeit in Abhängigkeit vom Wandel in den Sozial- und Moralvorstellungen sowie von kriminalpolitischen Wertentscheidungen ändert (als Beispiele hierfür kann der früher existierende, später infolge des insofern stattgefundenen Gesellschaftswandels jedoch überholte und deshalb 1994 abgeschaffte Straftatbestand des gleichgeschlechtlichen Beischlafs unter Männern nach § 175 StGB genannt werden). Zum anderen bleibt die Tatsache, dass dem jeweils strafrechtlich definierten Verbrechen stets „per definitionem“ ein besonderer Unwert zukommt, wodurch es sich von anderem abweichenden Verhalten – sowohl im Bewusstsein des Straftäters als auch bezüglich der Reaktion der Gesellschaft – abhebt. Das Verbrechen/die Straftat wird damit als sozial abweichendes Verhalten mit Unwertcharakter in seiner schwersten Form angesehen.

4.1.3 Schutzfunktion des Strafrechts

Hieraus leitet sich auch die Rechtfertigung des Strafrechts ab. Indem die Rechtsordnung bestimmte sozialschädliche Verhaltensweisen unter Strafe verbietet, trägt sie dadurch dem Interesse der staatlichen Gemeinschaft an der Erhaltung ihrer Grundwerte und an der Bewahrung des Rechtsfriedens innerhalb der Gesellschaft Rechnung. Nach den Erfahrungen der Menschheitsgeschichte ergibt sich die Rechtfertigung für die Existenz des Strafrechts somit schon aus seiner unbestreitbaren Notwendigkeit für ein gedeihliches Zusammenleben. Durch den Schutz von bestimmten Rechtsgütern (z.B. Eigentum, Freiheit, Leben) dient das Strafrecht der Verwirklichung des Gemeinwohls und der Wahrung des Rechtsfriedens. Es ist dem Grunde eine Schutz- und Friedensordnung, die auf der sozialethischen Wertordnung unserer Verfassung beruht und sich an deren Zielsetzungen zu orientieren hat. Aus dieser Bindung an das Grundgesetz folgt für das Strafrecht die Aufgabe, die elementaren Grundwerte des Gemeinschaftslebens zu sichern, die Erhaltung des Rechtsfriedens im Rahmen der sozialen Ordnung zu gewährleisten und das Recht im Konflikt gegenüber dem Unrecht durchzusetzen. Als ultima ratio ist ein Rückgriff auf das Strafrecht

dabei nur angezeigt bei einem besonders missbilligenswerten Verhalten, mit dem sich der Täter schlechthin gegen die Rechtsordnung aufgelehnt hat. Rechtsgüter sind dabei ideelle Sozialwerte. Man unterscheidet zwischen Individualrechtsgütern, wie Leben, körperliche Unversehrtheit, persönliche Freiheit, Ehre, Eigentum und Vermögen, und Universalrechtsgütern, worunter etwa der Bestand des Staates und seiner freiheitlich demokratischen Grundordnung, die Wahrung von Staatsgeheimnissen und die Rechtspflege fallen.

4.1.4 Sinn und Zweck der Strafe

Man unterscheidet zwischen den absoluten und relativen Strafzwecktheorien.

Absolute Theorien:

Der Begriff absolut (absolutus = losgelöst) soll zum Ausdruck bringen, dass Bestrafung von jeder gesellschaftlichen Wirkung losgelöst ist. Strafe soll rein repressiv wirken, sodass Strafzweck allein die Wiederherstellung der Rechtsordnung durch Zufügung eines gerechten Übels durch den Staat ist. Die Sühnetheorie basiert auf dem Gedanken, dass der Täter sich wegen der begangenen Tat mit der Rechtsordnung wieder versöhnt. An ihr wird kritisiert, dass Versöhnung einen freiwilligen Akt voraussetzt, Strafe demgegenüber gerade ein aufgezwungenes Übel ist. Nach der früher prominent vertretenen (insbes. Immanuel Kant und Georg Wilhelm Friedrich Hegel) Vergeltungstheorie müsse auf Unrecht – getreu dem alttestamentarischen Motto: „Auge um Auge, Zahn um Zahn“ – mit einer in Dauer, Härte und nach Art (Kant) bzw. vom Wert her (Hegel) gleichen Strafe geantwortet werden, um die Gerechtigkeit wieder herzustellen. Sie muss sich insb. vorwerfen lassen, auch stets dann eine Strafe zu fordern, wenn dies gesellschaftlich gar nicht notwendig ist. Außerdem würde sie die Verhängung der in Deutschland abgeschafften Todesstrafe (vgl. Art. 102 GG) für bestimmte Straftaten zur staatlichen Pflicht erheben.

Relative Theorien:

Nach den relativen Theorien soll Strafe rein präventiv wirken. Die Bestrafung ist auf die Aufgabe der Verbrechensverhütung bezogen (relatus = bezogen auf). Es wird hierbei unterschieden zwischen Generalprävention, welche den Blick auf die Allgemeinheit richtet, und der Spezialprävention, die auf den Täter abstellt. Die positive Generalprävention dient dabei der Stärkung des Rechtsbewusstseins und des Vertrauens der Allgemeinheit in die Rechtsordnung, wohingegen die negative Generalprävention zur allgemeinen Abschreckung vor der Begehung von Straftaten heranzuziehen ist. Demgegenüber soll allein der Täter bei der positiven Spezialprävention erzogen/ resozialisiert werden und bei der negativen Spezialprävention von der Begehung weiterer Taten abgehalten werden. Problematisch an diesen Theorien ist, dass hierbei – im Gegensatz zu den absoluten Theorien – keine Begrenzung des Strafmaßes anhand des persönlichen Unrechtsgehalts der Tat erfolgt und der Täter dadurch ggf. allein aus Präventionsgründen unangemessen hart bestraft zu werden droht. Eine hierbei verhängte Strafe würde außerdem gegen Art. 1 Abs. 1 GG verstoßen, da der Verurteilte dadurch zum reinen Objekt staatlicher Verbrechensbekämpfung degradiert würde.

Vereinigungstheorie:

Das deutsche Strafrecht hat sich auf keine der vorgenannten Theorien festgelegt. Vielmehr finden sich in den §§ 46 und 47 StGB alle Strafzwecke wieder. Während nach § 46 Abs. 1 S.1 StGB die Schuld den Bemessungsfaktor für die Strafe im Sinne einer Ober- und Untergrenze bildet (i.S.d. absoluten Theorien), sind innerhalb der Grenzen des sich hierbei ergebenden Beurteilungsspielraumes noch präventive Kriterien für die genaue Straffestsetzung zu berücksichtigen (vgl. § 46 Abs. 1 S. 2 StGB und § 47 StGB). Das Ziel der Strafe ist dabei die Wiedereingliederung des Täters in die

Rechtsgemeinschaft. Neben der Strafe kennt das deutsche Strafrecht auch Maßregeln der Besserung und Sicherung (vgl. § 61 StGB). Deren Zweck ist nicht der Schuldausgleich, vielmehr soll hierdurch einer Wiederholungsgefahr vorgebeugt werden. Das Problem hierbei ist, dass es insofern kein Maß für die Sanktion gibt. Während die Strafe durch die Schuld des Täters begrenzt ist, geht es bei den Maßregeln der Sicherung allein um die Abwehr drohender Gefahren. Dementsprechend kann eine Sicherungsverwahrung auch ohne Weiteres verlängert werden, wenn angenommen wird, dass vom Täter immer noch Gefahr auszugehen droht.

4.2 Schutzgegenstand des IuK-Strafrechts

Der Schutzbereich des IuK-Strafrechts umfasst im Wesentlichen die **Sicherheit und Integrität informationstechnischer Systeme**.

Den Begriff des **informationstechnischen Systems** – **itS** – hat das Bundesverfassungsgericht im Zusammenhang mit seiner Entscheidung vom 27.02.2008 zur Onlinedurchsuchung eingeführt[1]. Dabei handelt es sich um alle technischen Geräte, die ungeachtet ihrer Ausdehnung und ihrer technischen Leistungsfähigkeit der Verarbeitung und Speicherung von personenbezogenen Daten dienen. Nur einfache, unvernetzte Steuerungen der Haushaltselektronik sind hiervon ausgenommen. ItS sind demnach bereits Spielekonsolen, elektronische Notizbücher und Telekommunikationsgeräte.

Die **Informations- und Kommunikationstechnik** – **IuK** – umfasst wiederum die Herstellung solcher itS, und zwar im Sinne der Schaffung, Verarbeitung, Speicherung und Vermittlung von elektromagnetischen Daten unter Einsatz von Elektrotechnik und ungeachtet der physikalischen Trägermedien und der räumlichen Entfernungen.

ItS haben eine erhebliche Bedeutung für die private und berufliche Lebensführung erlangt, sind leistungsfähige Geräte zur Informationsverarbeitung und –speicherung geworden, sind zunehmend vernetzt und ermöglichen dadurch den wechselseitigen Zugriff auf bedeutende persönliche Daten. Die technische Integrität von ItS wird vom Telekommunikationsgeheimnis, vom allgemeinen Persönlichkeitsrecht und dem daraus entwickelten Recht auf informationelle Selbstbestimmung[2] nur unzureichend geschützt, sodass das BVerfG in seiner vorgenannten Entscheidung vom 27.02.2008 noch zusätzlich das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Integritätsschutz) geschaffen hat, um neuartigen Gefährdungen zu begegnen, zu denen es im Zuge des wissenschaftlich-technischen Fortschritts und gewandelter Lebensverhältnisse kommen kann[3].

Folgt man dem vom BVerfG verwendeten Begriff der ItS, so ist der **Schutzgegenstand des IuK-Strafrechts das unter einer einheitlichen Verwaltung und Verantwortung stehende Rechnernetz**. Dabei kann es sich um einzelne autonome Geräte handeln, die sich beispielsweise als Mobiltelefon in ein Telekommunikationsnetz einwählen, oder um einzelne Computer, die ausschließlich mit dem Festnetz verbunden sind. Das LAN im häuslichen Bereich umfasst hingegen alle Computer, die über einen gemeinsamen Router mit einem Anschlussnetz verbunden sind (Gateway). Dadurch entsteht ein lokal begrenztes Verbundsystem, das unter einer einheitlichen Verwaltung und Verantwortung steht, mithin ein LAN ist. Seine Ausbreitung und die Anzahl der ihm angehörenden Komponenten ändern dabei nichts an der verfassungsrechtlichen Beurteilung, dass ein Netz ein selbstständiges ItS ist, wenn es nur unter einheitlicher Verwaltung und Verantwortung steht. Das gilt bis hin zu

[1] 2 BVerfG Urt. v. 27.02.2008 – 1 BvR 370, 595/07, Rn. 202 f.
[2] BVerfG Urt. v. 15.12.1983 1 BvR 209, 269, 362, 420, 440, 484/83.
[3] BVerfG Urt. v. 27.02.2008 – 1 BvR 370, 595/07, Rn. 202 f.

weltweiten Verbünden. Demnach ist auch das Internet ein globaler Verbund aus autonomen Systemen verschiedener Größe (auch mit länder- und kontinentübergreifenden Wide Area Networks – WAN) und fernmeldetechnisch gesehen ein Fernkommunikationsnetz.

Im Endeffekt unterscheidet das BVerfG im Zusammenhang mit dem ItS nicht zwischen seiner jeweiligen Größe und den Komponenten, die ein (Sub-) Netz bilden, sondern fragt nur nach seiner für die Lebensgestaltung relevanten Bedeutung. Dadurch wird nur eine Grenze „nach unten" gezogen, sodass zwar einzelne elektronische Bauteile für sich betrachtet keinen Integritätsschutz auslösen können, wohl aber, sobald sie zu einem größeren System verbunden werden [12: Rn. 43].

4.3 Besonderheiten des Cybercrime und des IuK-Strafrechts

4.3.1 Mehraktige Begehung

Die IuK-Kriminalität wird in den meisten Fällen mehraktig ausgeübt. Zu ihrer Bewertung darf deshalb nicht nur die unmittelbare Erscheinungsform betrachtet werden, denn sie offenbart häufig nur einen Ausschnitt vom gesamten Tatplan und vielfach zeigen erst die unsichtbaren Folgeschritte den strafrechtlichen Gehalt und verweisen auf die richtige materiell-rechtliche Zuordnung. Genannt werden kann hierfür zum Beispiel das Skimming, dessen Zwischenschritt, das Herstellen falscher Zahlungskarten mit Garantiefunktion, und dessen finales Cashing gemäß § 152 b Abs. 1 StGB Verbrechen (i.S.d § 12 StGB) sind, und beim Einsatz von Onlinebanking-Malware, der sich gleichzeitig als gewerbsmäßige Formen des Computerbetruges, der Fälschung technischer Aufzeichnungen und beweiserheblicher Daten darstellt. Wenn dabei eine Bande handelt, wandeln sich die Vorwürfe zu selbstständigen Verbrechenstatbeständen (§ 263 Abs. 5 iVm § 263 a Abs. 2, § 267 Abs. 4 iVm § 268 Abs. 5 oder § 269 Abs. 3 StGB). Allein schon die Verabredung zu solchen Verbrechen steht als besondere Form der Beteiligung nach § 30 StGB unter Strafe. Das bedeutet, dass auch sonst straflose Vorbereitungshandlungen im Einzelfall Ausdruck einer ernsthaften Verbrechensabrede und dadurch strafbar sein können.

4.3.2 Variantenreichtum

Bei der systematischen Darstellung von Cybercrime reicht es nicht aus, seine Erscheinungsformen als einzelne Phänomene zu beschreiben. Vielmehr müssen diese strukturiert, in Gruppen gefasst werden und mit geeigneten Methoden auf Varianten und ähnliche Begehungsformen verbunden werden. Die schlichte Tatsache einer Kontobelastung beim Bankkunden gibt bspw. keine Aussage über das Vorgehen der Täter, sodass mehrere Ablaufvarianten in die Überlegung einzubeziehen sind: Handelt es sich um eine Geldabhebung im außereuropäischen Ausland, kommt Skimming oder Computerbetrug nach einer manuellen Eingabe der Kreditkartendaten in Betracht. Skimming scheidet bei Geldausgaben in Deutschland aufgrund der maschinenlesbaren Merkmale im Kartenkörper und im europäischen Ausland wegen des jetzt flächendeckenden Einsatzes des EMV-Chips grundsätzlich aus. Wenn eine Überweisung auf ein anderes Bankkonto stattfand, kann es sich um einen Kontomissbrauch beim Onlinebanking handeln (Phishing). In Betracht kommen aber auch einzelne unberechtigte Einzugsaufträge im Lastschriftverfahren oder Massen-Einzüge im automatisierten Verfahren. Auch der schlichte Diebstahl der Zahlungskarte des Kunden (auch auf dem Postweg), der Missbrauch durch Angehörige oder unlautere Beanstandungen des Bankkunden sind gedanklich in Betracht zu ziehen. Aus einfach wirkenden Folgen lassen sich deshalb nicht zwingend kriminelle Ursachen schließen.

4.3.3 Formenwechsel

Die Formen des Cybercrime wechseln, um sich verbesserten Abwehrmechanismen und den neuen technischen Entwicklungen anzupassen. Optimierte Virenscanner, Updates von Betriebssystemen und Anwenderprogrammen, mit denen bekannte Schwachstellen geschlossen werden, neue technische Sicherungen wie der EMV-Chip auf Zahlungskarten und die Änderungen im Anwenderverhalten müssen von den Tätern ausgeglichen werden, um weiterhin erfolgreich zu sein. Schon 2007 wurde etwa erkennbar, dass die in Malware und Spams verwendeten Texte (trotz ihrer überwiegenden Herkunft aus Osteuropa) auf dem deutschen Markt fehlerfreier und damit unauffälliger wurden. Das hat sich fortgesetzt, indem die Täter auch den Jargon und die verwendeten Fachwörter ihrer Zielgruppen bei betrügerischen Angriffen und bei der Verbreitung von Malware angepasst haben. Neue Angriffsmöglichkeiten werden schnell ins eigene Repertoire übernommen.

4.3.4 Arbeitsteiliges und modulares Cybercrime

Die Mehraktigkeit im Hinblick auf die Tatausführung und die zunehmende Arbeitsteilung werden von den personellen Strukturen der beteiligten kriminellen Szenen unterstützt. In den meisten Fällen wird von tatgeneigten Schwärmen auszugehen sein, deren Teilnehmer intensiv miteinander kommunizieren, zu Straftaten nicht überredet werden müssen, sich aber nur zu einzelnen abgegrenzten kriminellen Projekten verbinden. Das Bundeskriminalamt (BKA) kommt insofern zu folgender Einschätzung [13, S. 8]: „Das Täterspektrum reicht vom Einzeltäter bis hin zu international organisierten Tätergruppierungen. Gemeinsam agierende Täter arbeiten im Bereich Cybercrime nur selten in hierarchischen Strukturen. Sie kennen sich häufig nicht persönlich und nutzen auch bei arbeitsteiligem Vorgehen die vermeintliche Anonymität des Internets. Die Täterseite reagiert flexibel und schnell auf neue technische Entwicklungen und passt ihr Verhalten entsprechend an. Dienste, die nicht selbst erbracht werden können, werden von anderen hinzugekauft (Cybercrime-as-a-Service).“

4.3.5 Interlokalität

Zum Cybercrime gehören vorwiegend grenzüberschreitende Handlungen, es ist in aller Regel interlokal. Deshalb ist besonders auch nach seinen Tat- und Erfolgsorten zu fragen, um die Zuständigkeit für die Strafverfolgung zu klären. Eine Besonderheit gilt jedoch für die strafrechtlichen Schwergewichte des Cybercrime: das Fälschen von Zahlungskarten mit Garantiefunktion (Skimming), der unbefugte Vertrieb von Betäubungsmitteln, Menschenhandel sowie die Verbreitung von Kinderund Jugendpornographie unterfallen dem Weltrechtsprinzip (vgl. § 6 Nrn. 4 – 7 StGB), sodass in diesen Bereichen auch reine Auslandstaten der deutschen Gerichtsbarkeit unterliegen.

4.4 Grundlagen für die Verfolgung von Cybercrime-Delikten

4.4.1 Polizeiliche Zuständigkeiten

Bei den Landespolizeidirektionen werden Cybercrime-Delikte in der Regel durch örtliche Fachdienststellen bearbeitet oder – z. B. bei schwerwiegenden und überregionalen Fällen – auch durch das jeweilige Landeskriminalamt (LKA). Das Bundeskriminalamt (BKA) unterstützt die Polizeien der Länder bei der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder sonst erheblicher Bedeutung. In bestimmten Fällen kann auch das BKA selbst die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung wahrnehmen und Ermittlungsverfahren führen. Neben der Reaktion des Gesetzgebers auf die Weiterentwicklung der Technik, sowie der

Wendigkeit und dem Einfallsreichtum von Internetkriminellen, kommt er auch den Vorgaben der Europäischen Union nach. Am 1.7.2009 trat die von Deutschland zuvor ratifizierte „**Cybercrime Convention**“ des Europarates in Kraft. Allerdings werden in dieser Konvention keine Straftatbestände festgelegt, sondern Kategorien gebildet, denen jeder Mitgliedstaat seine strafbewehrten Handlungen zuordnen kann oder in Ermangelung entsprechender Tatbestände verpflichtet ist, neue Gesetze zu erlassen. In der Convention on Cybercrime sowie dem Zusatzprotokoll vom 28.1.2003 zum Übereinkommen über Computerkriminalität betreffend der Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art sind folgende Kategorien aufgeführt:

- Straftaten gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und -systemen
- computerbezogene Straftaten
- inhaltsbezogene Straftaten
- Straftaten in Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte
- rassistische und fremdenfeindliche Handlungen

4.4.2 Gesetzliche Grundlagen

Mit dem Inkrafttreten der Cybercrime Konvention in Deutschland am 01.07.2009 wurde das deutsche Strafrecht an die aktuellen Entwicklungen im Bereich der Internet- und Computerstraftaten angepasst. Die folgende Darstellung soll einen Überblick über die einschlägigen Straftatbestände des Strafgesetzbuches (StGB) geben.

Straftatbestände	Kurzbeschreibung des Inhalts
§ 202a StGB Ausspähen von Daten	Das unbefugte Verschaffen eines Zugangs zu Daten, die nicht für den Täter bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung
§ 202b StGB Abfangen von Daten	Das unbefugte Verschaffen von Daten aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage unter Anwendung von technischen Mitteln
§ 202c StGB Vorbereiten des Ausspähens und Abfangens von Daten	Das Vorbereiten einer o. g. Straftat durch das Herstellen, Verschaffen, Verkaufen, Überlassen, Verbreiten oder Zugänglichmachen von Passwörtern, Sicherheitscodes oder Computerprogrammen, deren Zweck die Begehung einer solchen Tat ist
§ 202d StGB Datenhehlerei	Wer durch eine rechtswidrige Tat Daten erlangt, und sich oder anderen diese Daten in der Absicht überlässt, verbreitet oder sonst zugänglich macht um sich oder einen Dritten zu bereichern oder einen anderen zu schaden
§ 263a StGB Computerbetrug	Das Schädigen des Vermögens eines Anderen durch Beeinflussung des Ergebnisses eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung

	unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf. Des Weiteren das Vorbereiten einer solchen Tat durch Herstellung, Verschaffung, Feilhalten, Verwahren oder Überlassung eines Computerprogramms, deren Zweck die Begehung einer solchen Tat ist
§ 269 StGB Fälschung beweiserheblicher Daten	Das Speichern oder Verändern beweiserheblicher Daten zur Täuschung im Rechtsverkehr, so dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder das Gebrauchen solcher Daten
§ 270 StGB Täuschung im Rechtsverkehr bei Datenverarbeitung	Der Täuschung im Rechtsverkehr steht die fälschliche Beeinflussung einer Datenverarbeitung im Rechtsverkehr gleich
§§ 271, 274 Abs. 1 Nr. 2, 348 StGB Mittelbare Falschbeurkundung, Urkundenunterdrückung, Veränderung einer Grenzbezeichnung, Falschbeurkundung im Amt	Das Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern beweiserheblicher Daten zum Nachteil eines anderen, auch das Gebrauchen einer falschen Beurkundung oder Datenspeicherung zur Täuschung im Rechtsverkehr
§ 303a StGB Datenveränderung	Das rechtswidrige Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von Daten
§ 303b StGB Computersabotage	Das erhebliche Stören einer Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, durch 1. Begehung einer Datenveränderung (§ 303a), 2. Eingabe oder Übermittlung von Daten in der Absicht, einem anderen Nachteil zuzufügen, oder 3. Zerstörung, Beschädigung, Unbrauchbarmachen, Beseitigen oder Verändern einer Datenverarbeitungsanlage oder eines Datenträgers

In den weiteren Kapiteln wird auf spezielle Techniken und den strafrechtlichen Bestand vertiefend eingegangen.

4.4.3 Hellfeld vs. Dunkelfeld

Zur Betrachtung von Straftaten müssen vorerst zwei Begriffe eingeführt werden: Hellfeld und Dunkelfeld.

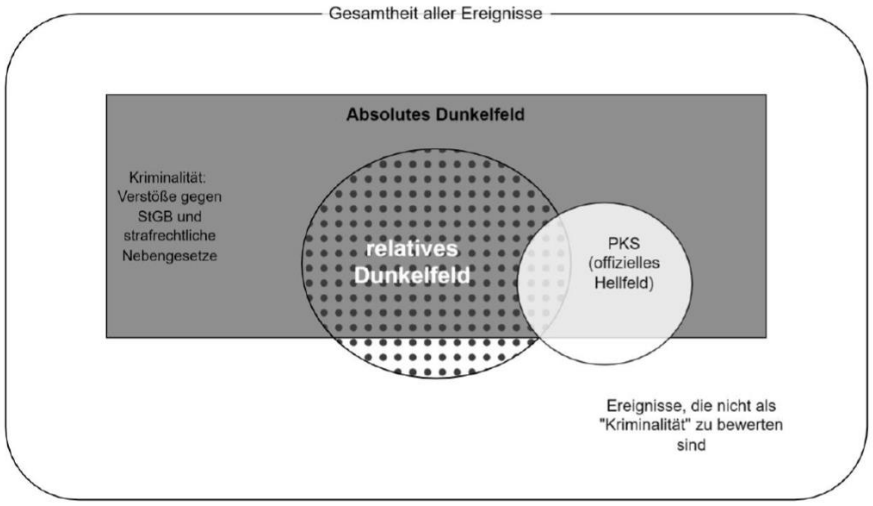


Abbildung 12: Hellfeld, relatives Dunkelfeld und absolutes Dunkelfeld

Das **Hellfeld** bezeichnet die Gesamtheit aller Straftaten, die den Strafverfolgungsbehörden bekannt sind und offiziell registriert wurden. Dies umfasst alle Straftaten, die zur Anzeige gebracht wurden oder anderweitig von den Behörden erfasst wurden. Eine wichtige Quelle für Informationen über das Hellfeld ist die Polizeiliche Kriminalstatistik (PKS), eine statistische Zusammenstellung über polizeilich bearbeitete Kriminalität.

In der PKS werden alle Kriminalitätsphänomene erfasst, mit Ausnahme von Ordnungswidrigkeiten, Verkehrsdelikten und Staatsschutzdelikten. Dies bedeutet, dass die PKS eine umfassende Darstellung der Kriminalität bietet, die von der Polizei bearbeitet wurde, einschließlich verschiedener Formen von Diebstahl, Einbruch, Betrug, Körperverletzung, Raub und anderen Straftaten.

Die PKS ist eine wichtige Informationsquelle für die Analyse von Kriminalitätsmustern, Trends und Schwerpunktbereichen. Sie bietet Einblicke in die Art und Häufigkeit von Straftaten in einer bestimmten Region oder über einen bestimmten Zeitraum und dient als Grundlage für die Entwicklung von Maßnahmen zur Kriminalitätsbekämpfung und -prävention.

Im Gegensatz dazu bezieht sich das **absolute Dunkelfeld** auf die Gesamtheit aller Straftaten, die den Strafverfolgungsbehörden nicht bekannt sind. Diese Straftaten bleiben unentdeckt und werden nicht offiziell registriert, was bedeutet, dass sie nicht in den offiziellen Statistiken zur Kriminalität erscheinen.

Das **relative Dunkelfeld** bezieht sich auf die Straftaten, die den Strafverfolgungsbehörden zwar nicht bekannt sind und daher nicht offiziell erfasst wurden, aber durch Befragungen und Studien bekannt werden. Diese Straftaten werden durch spezielle Umfragen und Studien ermittelt, bei denen Menschen nach ihren Erfahrungen mit Kriminalität befragt werden. Obwohl sie nicht in den offiziellen Statistiken auftauchen, bieten sie dennoch Einblicke in das Ausmaß der Kriminalität, das nicht durch das Hellfeld erfasst wird.

Das Bitkom-Wirtschaftsschutzpanel ist eine Umfrage, die von Bitkom, einem Verband der deutschen IT-Branche, durchgeführt wird. An dieser Umfrage nehmen in der Regel etwa 1000 Unternehmen teil, um Informationen über Themen wie Cybersicherheit und Angriffe zu sammeln.

Durch diese Umfrage werden Unternehmen zu ihren Erfahrungen mit Cyberkriminalität befragt, einschließlich Cyberangriffen, Datenverlust, Hacker-Angriffen, Phishing, Malware-Infektionen und anderen Sicherheitsvorfällen. Die gesammelten Daten ermöglichen es, das Ausmaß und die Art der Cyberkriminalität zu verstehen, die von den Unternehmen erlebt wird, und bieten Einblicke in das relative Dunkelfeld der Cyberkriminalität, das nicht offiziell von den Strafverfolgungsbehörden erfasst wird.

Durch die Analyse des relativen Dunkelfelds können Organisationen und Behörden gezielte Maßnahmen zur Verbesserung der Sicherheit und zum Schutz vor Cyberangriffen ergreifen.

Zusammenfassend bezeichnet das Hellfeld die bekannte Kriminalität, das absolute Dunkelfeld die unentdeckte Kriminalität und das relative Dunkelfeld die durch Befragungen und Studien ermittelte Kriminalität, die den Strafverfolgungsbehörden nicht bekannt ist. Die Untersuchung aller drei Felder ist wichtig, um ein umfassendes Bild der Kriminalitätssituation in einer Gesellschaft zu erhalten.

4.5 Relevante Akteure im Bereich Cybercrime

Im Bereich Cybercrime gibt es verschiedene relevante Akteure, die aus unterschiedlichen Perspektiven agieren.

Perspektive der Täter

Cyberkriminelle können unterschiedliche Motive haben, darunter finanzielle Gewinne, politische Ziele, ideologische Überzeugungen oder bloße Zerstörungslust. Hackergruppen können sich in ihrer Größe, ihren Fähigkeiten und ihren Zielen stark unterscheiden. Einige sind hochgradig organisiert und verfolgen gezielte Angriffe, während andere eher opportunistisch vorgehen und Schwachstellen ausnutzen, um schnell Profit zu machen. Organisierte kriminelle Netzwerke nutzen oft komplexe Strukturen und Ressourcen, um eine Vielzahl von Cyberkriminalitätsaktivitäten durchzuführen, einschließlich Datendiebstahl, Erpressung, Online-Betrug und Verbreitung von Schadsoftware. Staatlich unterstützte Hacker können im Auftrag von Regierungen handeln und spezifische politische, wirtschaftliche oder militärische Ziele verfolgen. Diese Akteure können hochgradig technisch versiert sein und über erhebliche Ressourcen und Unterstützung verfügen.

Perspektive der Opfer

Opfer von Cybercrime können erhebliche finanzielle Verluste erleiden, einschließlich gestohlener Gelder, Kosten für die Wiederherstellung von Daten und Systemen sowie Ausgaben für die Verbesserung der Cybersicherheit. Neben finanziellen Schäden können Opfer von Cyberangriffen auch mit erheblichen Rufschäden und einem Verlust des Vertrauens ihrer Kunden oder der Öffentlichkeit konfrontiert sein. Regierungsbehörden und Unternehmen müssen oft erhebliche Ressourcen investieren, um Cyberangriffe zu untersuchen, zu bekämpfen und sich gegen zukünftige Angriffe zu verteidigen.

Strafverfolgungsbehörden und Regierung

Strafverfolgungsbehörden müssen mit den sich ständig weiterentwickelnden Technologien und Taktiken von Cyberkriminellen Schritt halten, um effektiv gegen Cybercrime vorgehen zu können. Regierungen entwickeln Gesetze, Richtlinien und Strategien zur Bekämpfung von Cybercrime und zur Stärkung der Cybersicherheit. Dazu gehören Maßnahmen zur Verbesserung der Informationssicherheit, zur Förderung der Zusammenarbeit zwischen den Behörden und zur Sensibilisierung der Öffentlichkeit für Cyberbedrohungen. Internationale Zusammenarbeit ist entscheidend, da Cyberkriminalität oft grenzüberschreitend ist. Strafverfolgungsbehörden und Regierungen müssen zusammenarbeiten, um die Täter zu identifizieren, zu verfolgen und zu bestrafen.

Internationale Organisationen in Bezug auf Cybercrime

Internationale Organisationen spielen eine wichtige Rolle bei der Förderung der Zusammenarbeit und des Informationsaustauschs zwischen den Ländern im Kampf gegen Cybercrime. Interpol und Europol unterstützen die Strafverfolgungsbehörden bei der Untersuchung und Bekämpfung von grenzüberschreitenden Cyberkriminalitätsfällen. Die Vereinten Nationen und die Europäische Union setzen sich für die Entwicklung globaler Normen und Standards im Bereich der Cybersicherheit ein und unterstützen die Mitgliedstaaten bei der Stärkung ihrer nationalen Kapazitäten zur Bekämpfung von Cybercrime.

5 Phänomene – Formen von Cybercrime

Cybercrime kann in vielfältigen Formen auftreten und sich ständig weiterentwickeln, da Technologien und Kommunikationsmittel fortschreiten. Bitkom hat im Rahmen der Wirtschaftsschutzumfrage die wichtigsten Trends und Formen identifiziert. Diese sind in zu sehen.

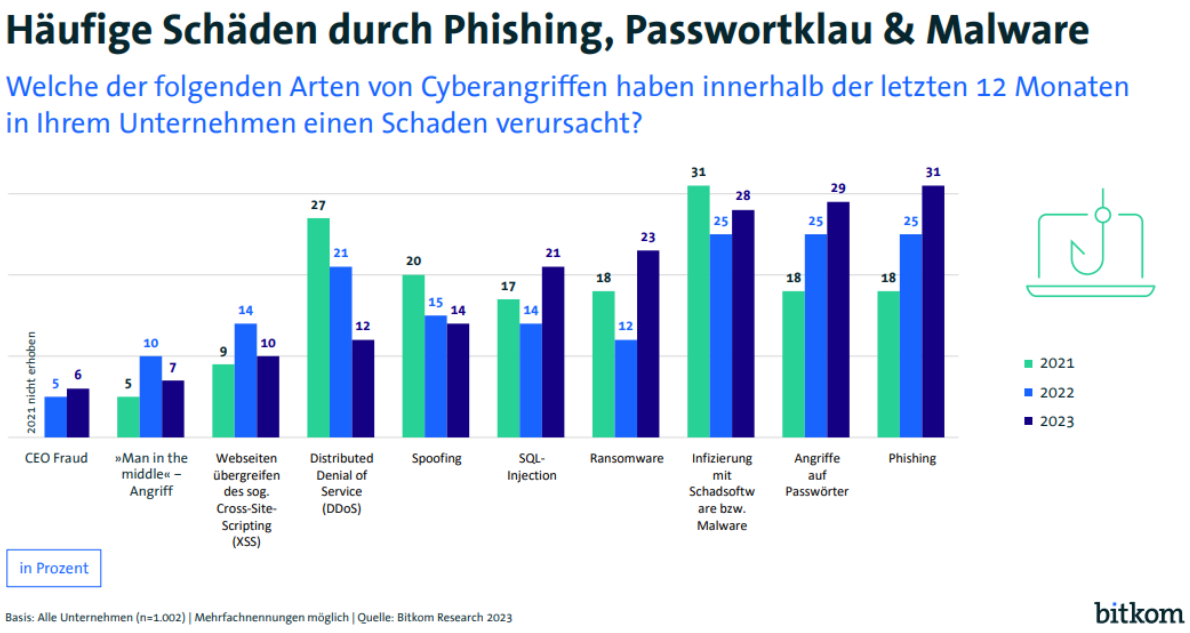


Abbildung 13: Wirtschaftsschutzumfrage 2023 - Häufigste Arten von Cyberangriffen in der Entwicklung von 2021 bis 2023 [Quelle: Bitkom]

Phishing

Phishing ist eine betrügerische Methode, bei der Cyberkriminelle gefälschte E-Mails, Nachrichten oder Websites verwenden, um persönliche Informationen wie Passwörter, Kreditkartennummern oder Bankdaten von ahnungslosen Opfern zu stehlen. Die Auswirkungen von Phishing können vielfältig und ernsthaft sein, sowohl für einzelne Benutzer als auch für Unternehmen und Organisationen. Hier sind einige der häufigsten Auswirkungen von Phishing-Angriffen:

- Identitätsdiebstahl: Phishing-Angriffe zielen oft darauf ab, persönliche Informationen wie Benutzernamen, Passwörter, Kreditkartennummern und Sozialversicherungsnummern zu stehlen. Durch den Diebstahl dieser sensiblen Daten können Angreifer Identitätsdiebstahl begehen und betrügerische Aktivitäten im Namen des Opfers durchführen, wie z.B. das Öffnen von Bankkonten, das Abschließen von Krediten oder das Durchführen von Online-Einkäufen.
- Finanzielle Verluste: Opfer von Phishing-Angriffen können erhebliche finanzielle Verluste erleiden, insbesondere wenn ihre Bankkonten kompromittiert werden oder betrügerische Transaktionen durchgeführt werden. Darüber hinaus können Opfer von Ransomware-Phishing-Angriffen erpresst werden, um Lösegeld zu zahlen, um ihre verschlüsselten Dateien wiederherzustellen.

- Reputationsverlust: Unternehmen und Organisationen, die Opfer von Phishing-Angriffen werden, können einen erheblichen Reputationsverlust erleiden, insbesondere wenn vertrauliche Informationen von Kunden oder Partnern kompromittiert werden. Der Verlust des Vertrauens der Kunden kann langfristige Auswirkungen auf das Geschäft haben und zu Umsatzeinbußen führen.
- Datenverlust: Phishing-Angriffe können dazu führen, dass vertrauliche Daten und Unternehmensinformationen gestohlen oder kompromittiert werden. Dies kann zu einem Verlust von geistigem Eigentum, Wettbewerbsnachteilen und rechtlichen Konsequenzen führen.
- Betriebsunterbrechungen: Wenn Phishing-Angriffe erfolgreich sind und die IT-Infrastruktur eines Unternehmens oder einer Organisation beeinträchtigen, können Betriebsunterbrechungen auftreten. Dies kann zu Produktionsausfällen, verpassten Geschäftschancen und einem Rückgang der Produktivität führen.

Malware

Malicious Software, auch bekannt als Malware, ist eine Art von Software, die entwickelt wurde, um unerwünschte und oft schädliche Funktionen auf einem IT-System auszuführen. Diese Software wird mit böswilliger Absicht erstellt und zielt darauf ab, Schaden zu verursachen, Daten zu stehlen, Systeme zu manipulieren oder den normalen Betrieb eines Computersystems zu stören. Hier sind einige wichtige Merkmale von Malicious Software:

- Definition: Malware ist ein Oberbegriff, der verschiedene Arten von schädlicher Software umfasst, darunter Viren, Würmer, Trojaner, Spyware, Ransomware und Adware. Jede Art von Malware hat ihre eigenen charakteristischen Merkmale und Funktionsweisen.
- Verbreitungswege: Malware kann auf verschiedene Arten in ein Computersystem gelangen, darunter durch infizierte E-Mail-Anhänge, Drive-by-Downloads von kompromittierten Websites, infizierte Datenträger wie USB-Sticks oder CDs, offene Netzwerkschnittstellen oder Ausnutzung von Sicherheitslücken in Softwareanwendungen.

- Ziele: Die Ziele von Malware können vielfältig sein und reichen von der Zerstörung von Daten über den Diebstahl von vertraulichen Informationen bis hin zur Erpressung von Lösegeld durch die Verschlüsselung von Dateien. Einige Malware-Programme dienen auch dazu, Botnetze zu erstellen, um weitere Angriffe durchzuführen oder Spam zu verbreiten.
- Entwicklung für spezifische Plattformen: Malware wird oft für bestimmte Geräte, Systeme oder Betriebssysteme entwickelt, um die Erfolgschancen der Infektion zu erhöhen. Es gibt Malware, die speziell für Windows, macOS, Linux, Android, iOS und andere Plattformen entwickelt wurde.
- Prävention und Bekämpfung: Der Schutz vor Malware erfordert einen mehrschichtigen Ansatz, der den Einsatz von Antivirensoftware, Firewalls, regelmäßigen Software-Updates, sicherem Online-Verhalten und Sicherheitsbewusstseinsschulungen umfasst. Im Falle einer Infektion müssen Malware-Analysen durchgeführt werden, um die Funktionsweise der Malware zu verstehen und geeignete Gegenmaßnahmen zu ergreifen.

Abbildung 14: Arten von Malware

Ransomware

Ransomware ist eine Art von Malware, deren Hauptziel darin besteht, die Daten eines Opfers zu verschlüsseln oder den Zugriff darauf zu blockieren, um dann Lösegeld von den Opfern zu erpressen. Der Begriff "Ransomware" leitet sich von "ransom" (Lösegeld) und "software" ab und beschreibt genau das, was diese Art von Malware tut: Sie sperrt die Dateien des Opfers und verlangt von ihnen eine Zahlung, um die verschlüsselten Daten wiederherzustellen oder den Zugriff darauf freizugeben.

Typischerweise erfolgt die Infektion mit Ransomware durch das Öffnen eines infizierten E-Mail-Anhangs, den Besuch einer kompromittierten Website oder das Ausnutzen von Sicherheitslücken in Softwareanwendungen. Sobald die Ransomware auf dem System eines Opfers aktiv ist, beginnt sie, Dateien auf dem Computer zu verschlüsseln oder den Zugriff auf sie zu blockieren. Dies kann wichtige Dokumente, Fotos, Videos, Datenbanken und andere persönliche oder geschäftliche Dateien umfassen.

Nachdem die Dateien verschlüsselt wurden, wird eine Lösegeldforderung angezeigt, die die Opfer darüber informiert, dass sie eine bestimmte Geldsumme bezahlen müssen, um die Entschlüsselungsschlüssel zu erhalten und ihre Dateien wiederherzustellen. Die Zahlung des Lösegelds erfolgt oft in Form von Kryptowährungen wie Bitcoin, um die Anonymität der Angreifer zu wahren.

Distributed Denial of Service (DDoS)-Angriffe

Ein Distributed Denial of Service (DDoS)-Angriff ist eine Art von Cyberangriff, bei dem ein Angreifer ein System, eine Website oder Netzwerkressourcen durch das Überschwemmen mit schädlichem Datenverkehr überlastet. Der Zweck eines DDoS-Angriffs besteht darin, die Verfügbarkeit der Dienste für legitime Benutzer zu beeinträchtigen oder vollständig zu unterbrechen, indem die Netzwerk- oder Systemressourcen erschöpft werden.

DDoS-Angriff weisen verschiede Merkmale auf:

- Überlastung des Zielsystems: Der Angreifer sendet eine große Menge an Datenverkehr an das Ziel, das häufig ein Server, eine Website oder eine Netzwerkressource ist. Dieser Datenverkehr kann aus einer Vielzahl von Quellen stammen und das Ziel mit einer so hohen Anzahl an Anfragen überfluten, dass es die Last nicht bewältigen kann.
- Auswirkungen auf die Verfügbarkeit: Durch die Überlastung des Zielsystems führt ein DDoS-Angriff in der Regel dazu, dass das System nicht mehr in der Lage ist, legitimen Benutzern den Zugriff auf die Dienste zu gewähren. Dies kann dazu führen, dass die Website nicht mehr erreichbar ist, Serverdienste abstürzen oder Netzwerkressourcen unbrauchbar werden.
- Botnetze: DDoS-Angriffe werden oft von Botnetzen durchgeführt, die aus einer großen Anzahl von kompromittierten Computern oder Geräten bestehen, die unter der Kontrolle des Angreifers stehen. Diese Botnetze können ferngesteuert werden, um synchronisierte Angriffe auf das Ziel auszuführen, was die Effektivität und Intensität des Angriffs erhöhen.
- Verschiedene Angriffsmethoden: Es gibt verschiedene Arten von DDoS-Angriffen, darunter SYN Flood, UDP Flood, HTTP Flood und DNS Amplification. Jede Methode zielt darauf ab, die Netzwerkressourcen auf unterschiedliche Weise zu überlasten und die Verfügbarkeit der Dienste zu beeinträchtigen.

Exploits und Schwachstellen

Ein Exploit ist eine Methode oder ein Programm, das die Ausnutzung einer Schwachstelle in Computersystemen, Softwareanwendungen oder Geräten ermöglicht, um unbefugten Zugriff zu erlangen, Schaden zu verursachen oder andere bösartige Aktivitäten auszuführen.

- Ausnutzung von Schwachstellen: Ein Exploit nutzt Schwachstellen in Software oder Hardware aus, die oft auf Programmierfehlern, Konfigurationsfehlern oder Designschwächen beruhen. Diese Schwachstellen können es einem Angreifer ermöglichen, unautorisierten Zugriff auf ein System zu erhalten, Informationen zu stehlen, Schadcode auszuführen oder das System zu manipulieren.
- Infiltration von Systemen/Geräten: Exploits werden verwendet, um in Computersysteme, Netzwerke oder Geräte einzudringen und Kontrolle über sie zu erlangen. Dies kann durch die Ausnutzung von Sicherheitslücken in Betriebssystemen, Anwendungen, Protokollen oder Diensten erfolgen, um Zugriffsberechtigungen zu erweitern oder Administratorrechte zu erlangen.
- Ursachen von Schwachstellen: Schwachstellen, die von Exploits ausgenutzt werden können, können verschiedene Ursachen haben, darunter Programmierfehler, unzureichende Validierung von Benutzereingaben, fehlende Authentifizierung oder Autorisierung, unsichere Konfigurationen, veraltete Softwareversionen oder fehlende Sicherheitsupdates.

Identitätsdiebstahl

Bei Identitätsdiebstahl verwenden Cyberkriminelle gestohlene persönliche Informationen, wie z.B. Namen, Geburtsdaten, Sozialversicherungsnummern und Kreditkarteninformationen, um sich als jemand anderes auszugeben und betrügerische Aktivitäten durchzuführen. Diese Aktivitäten können das Öffnen von Bankkonten, das Abschließen von Krediten, das Durchführen von Online-Einkäufen, das Beantragen von staatlichen Leistungen oder das Durchführen von illegalen Transaktionen umfassen. Identitätsdiebstahl kann für Opfer finanzielle Verluste, rechtliche Probleme und erhebliche Belastungen verursachen, da sie oft lange damit beschäftigt sind, die Schäden zu beheben und ihre Identität wiederherzustellen.

Datenmissbrauch

Datenmissbrauch bezieht sich auf den unbefugten Zugriff, die Weitergabe oder den Diebstahl von sensiblen Daten, wie z.B. medizinischen Aufzeichnungen, Finanzinformationen oder vertraulichen Unternehmensdaten, mit dem Ziel, diese Informationen für betrügerische Zwecke zu nutzen. Cyberkriminelle können gestohlene Daten für Identitätsdiebstahl, Finanzbetrug, Spamming, Phishing-Angriffe oder den Verkauf auf dem Schwarzmarkt verwenden. Datenmissbrauch kann erhebliche negative Auswirkungen auf die Privatsphäre, die finanzielle Sicherheit und den Ruf der Betroffenen haben und kann auch rechtliche Konsequenzen nach sich ziehen.

Cyberbullying

Cyberbullying bezeichnet die Verwendung von digitalen Technologien, wie z.B. sozialen Medien, Messaging-Apps oder Online-Plattformen, um andere zu belästigen, zu bedrohen, zu beleidigen oder zu diffamieren. Cyberbullying kann in Form von beleidigenden Kommentaren, Drohungen, Verbreitung von Gerüchten oder unangemessenen Inhalten auftreten und kann schwerwiegende Auswirkungen auf die psychische Gesundheit, das Selbstwertgefühl und das Wohlbefinden der Opfer haben. Es ist ein ernsthaftes soziales Problem, das zunehmend Aufmerksamkeit und Gegenmaßnahmen erfordert, um die Sicherheit und das Wohlergehen von Benutzern im digitalen Raum zu gewährleisten.

Hacken und Datenmanipulation

Hacker nutzen Schwachstellen in Computersystemen, Netzwerken oder Softwareanwendungen aus, um Zugriff auf vertrauliche Informationen zu erhalten, Systeme zu manipulieren oder Daten zu stehlen. Datenmanipulation kann verschiedene Formen annehmen, einschließlich der Veränderung von Dateien oder Dokumenten, der Einschleusung von schädlichem Code in Softwareanwendungen oder der Sabotage von Computersystemen. Dies kann zu schwerwiegenden Konsequenzen führen, wie z.B. finanziellen Verlusten, Rufschädigung, Betriebsunterbrechungen oder Datenschutzverletzungen. Unternehmen und Organisationen müssen daher proaktive Maßnahmen ergreifen, um ihre Systeme und Daten vor Hackerangriffen zu schützen und die Integrität ihrer Informationstechnologie zu gewährleisten.

5.1 Identitätsdiebstahl

Was ist die Identität eines Menschen? Die Identität des Menschen umfasst alle Eigenschaften, die einem Menschen zuzuordnen sind und somit geeignet sind, auf diesen hinführen und ihn unverwechselbar zu machen.

Wir alle bewegen uns heute wie selbstverständlich nicht nur in der realen, sondern auch in der virtuellen Welt des so genannten „Cyberspace“. Dabei ist für immer mehr Menschen das Internet zu einem festen Bestandteil ihres Lebens geworden. Es entwickelt sich damit mehr und mehr zu einem sozioökonomischen Raum, in dem die Nutzer einen Teil ihrer Arbeits- und Freizeit verbringen. Einerseits herrscht immer noch eine, wenn auch oftmals vermeintliche Anonymität und Isolation des einzelnen Nutzers vor. Andererseits hat ein Nutzer verschiedene Identitäten, wenn er sich im Internet bewegt: In Chatrooms wird er unter einem selbst gewählten Anonym agieren, beim Online-Shopping verkauft er sein Buch unter einem Pseudonym und beim eBanking ist er unter dem zugewiesenen Benutzernamen aktiv. Diese vielen Identitäten müssen durch den Nutzer gehandhabt werden. Die verschiedenen Identitäten eines Nutzers sind im Internet als eine Web Identität (WebID) abbildbar.

Man unterscheidet bei Web-Identitäten zwei grundlegende Eigenschaften: Die Einfachheit des Rückschlusses von einer WebID auf den Nutzer (offen, pseudonym, anonym) und den Grad der Rechtssicherheit der WebID (allgemein, rechtssicher).

5.1.1 Identität und digitale Identität

Eine Identität ist eine in ihrem Verwendungskontext eindeutige, wiedererkennbare Beschreibung einer natürlichen oder juristischen Person oder eines Objektes z. B. Personengruppe, Unternehmen, Rechner, Programm, Datei.

Eine Identität setzt sich zusammen aus:

- Attributen zur Charakterisierung der Person / des Objektes sowie
- einem in seinem Gültigkeitsbereich eindeutigen Identitätsbezeichner (z. B. Personal-Nummer im Unternehmen, Rechner-Nummer)
- Persönliche Merkmale (Name, Geburtsort, Adresse usw.)
- Körperliche Merkmale (Alter, Größe usw.)
- Fähigkeiten/persönliche Vorlieben (Interessen, Hobbys usw.)

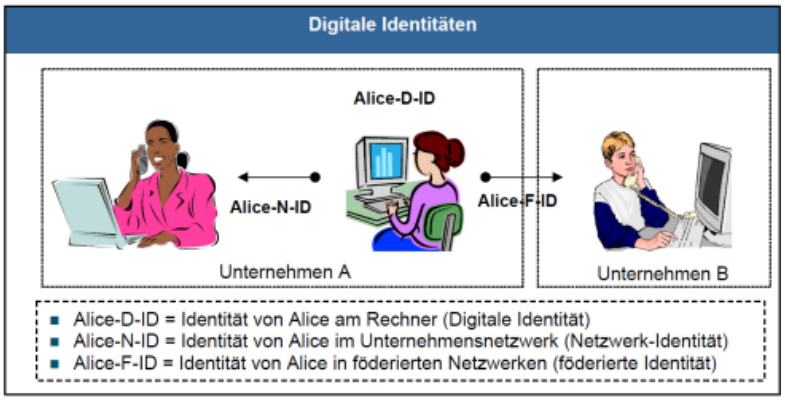


Abbildung 15: Digitale Identitäten

Eine **digitale Identität** (Abbildung 15) ist eine Identität, die von einem Rechner verstanden und verarbeitet werden kann. Die digitale Identität entsteht, indem Attribute einer natürlichen Person

oder eines Objektes in einem Rechner in elektronischer Form sicher registriert werden. Man spricht daher auch vom Identitäts-Lieferanten (engl. Identity Provider, kurz IdP).

Eine **Netzwerk-Identität** ist eine digitale Identität, die innerhalb eines elektronischen Netzwerks, z. B. von einem Unternehmen, verstanden wird.

Eine **föderierte Identität** ist eine Netzwerk-Identität, die in mehreren Netzwerken verstanden wird. Sie setzt eine zuvor in einer diesem Netzwerk registrierte Netzwerk-Identität voraus.

Ein im Zusammenhang mit Cybercrime oft verwendeter Begriff ist der Begriff des (elektronischen) Profils.

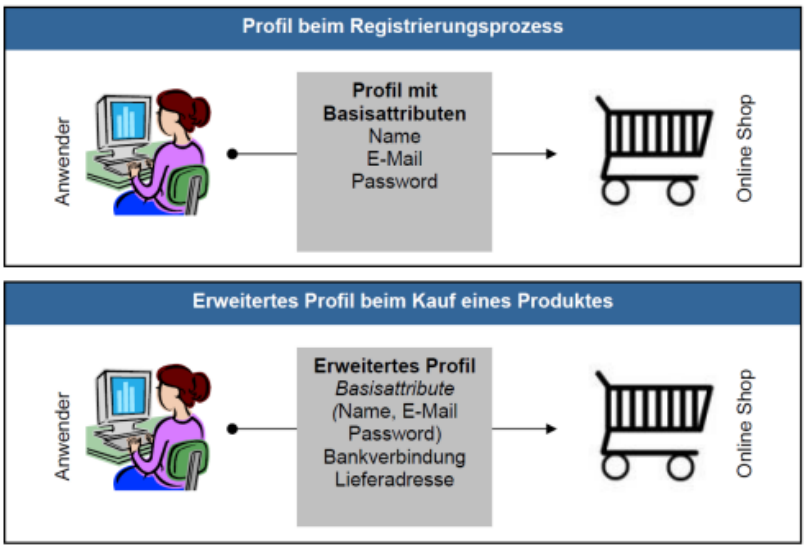


Abbildung 16: Profile

Als **elektronisches Profil** (Abbildung 16) bezeichnet man die bei der Registrierung einer digitalen Identität anzugebenden Attribute, welche zur Erlangung einer bestimmten Dienstleistung im Internet erforderlich sind. Je nach Dienstanbieter bzw. erwünschter Online-Dienstleistung ist ein Profil mehr oder weniger umfangreich. Das Profil eines Kunden wird i. d. R. vom Dienstleister um zusätzliche, für die Geschäftsprozesse erforderlichen Attribute erweitert, z. B. Bankverbindung, Telefonnummern, Lieferadresse, Interessen des Kunden. In der Abbildung 17 ist dies schematisch dargestellt: Im Rahmen eines Registrierungsprozess z. B. bei einem Online-Buchshop gibt der Kunde zunächst seine E-Mail-Adresse sowie ein Passwort ein. Ein Profil mit Basisattributen wird angelegt. Kauft er später ein Buch, so wird seine Bankverbindung und seine Lieferadresse verlangt und dann im erweiterten Profil gespeichert.

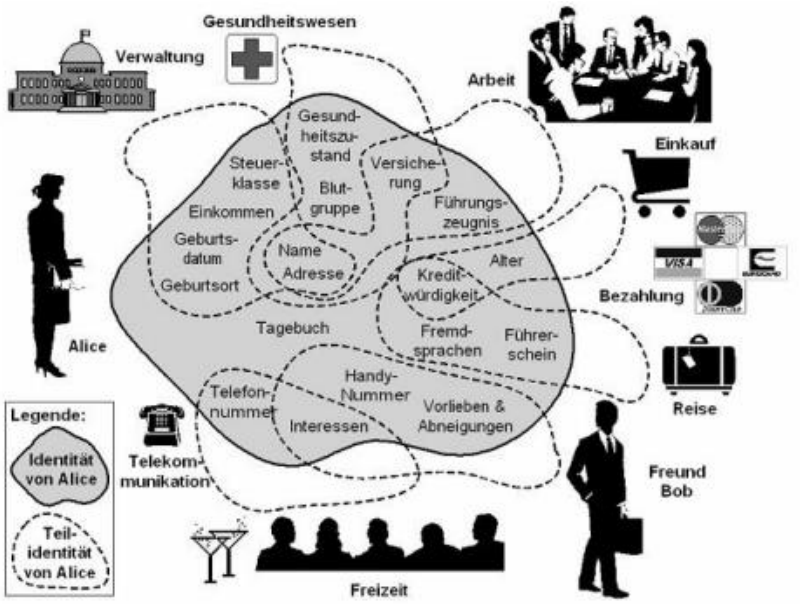


Abbildung 17: Darstellung von WebID-Profilen für verschiedene Anwendungen [4]

5.1.2 Die 5 Säulen der Identität

Identität ist die einzigartige Persönlichkeitsstruktur eines Menschen, das Wer bin ich?, Auf wen beziehe ich mich?, Wer bezieht sich auf mich?, Worüber definiere ich mich? und Was macht mich aus?. Identität ist ein lebenslanger Prozess und zeigt sich in Auftreten, Mimik, Gestik, Sprache und körperlichen Stärken und Schwächen und natürlich im inneren Bild/Selbstbild, Selbstgefühl und Glauben an sich, etc.. Nach H. Petzold kann die Identität mit Hilfe von 5 Säulen dargestellt werden, wie es in der Abbildung 18 zu sehen ist.

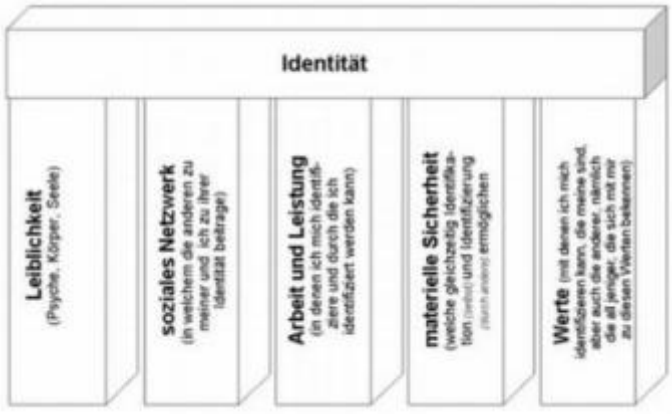


Abbildung 18: 5 Säulen der Identität nach H. Petzold

Was bedeutet die Säulen im Einzelnen?

- **Leib/Leiblichkeit** (Säule 1)
  Leib als Gefäß, das Ich bin, indem ich lebe, meine Gesundheit, meine Beweglichkeit, mein Wohlbefinden, meine Sexualität, meine Belastbarkeit, meine Psyche, meine Gefühle, meine Gelüste, meine Sehnsüchte, Glaubenssysteme und Träume In diesen Bereich gehört alles, was mit meinem Leib zu tun hat, „in mir drin“ ist, mit seiner Gesundheit, seinem Kranksein, seiner Leistungsfähigkeit, seinem Aussehen, mit der Art und Weise, wie sich der Mensch mag und „in seiner Haut“ wohl oder eben auch unwohl fühlt. Auch wie der Mensch von anderen in seiner Leiblichkeit wahrgenommen wird, ob sie ihn anziehend finden oder ablehnen, schön finden oder hässlich, als gesund und vital oder als krank und gebrechlich erleben, etc..
- **Soziales Netzwerk bzw. Soziale Bezüge** (Säule 2)
  Mein soziales Netzwerk, meine Freunde, Familie, Arbeitsplatz, Beziehungen, Ehe, Freizeitgestaltung, Verein Persönlichkeit und Identität werden nachhaltig bestimmt von den sozialen Beziehungen, dem sozialen Netzwerk, also den Menschen, die für jemanden wichtig sind, mit denen er zusammenlebt und arbeitet, auf die er sich verlassen kann und denen er etwas bedeutet. Aber es gehören auch Leute zum sozialen Netzwerk, die ihm nicht wohlgesonnen sind, feindselig gegenüberstehen oder auch schaden.
- **Arbeit und Leistung** (Säule 3)
  Tätigkeiten, Arbeit, mein „Tätigsein“ , mit der ich mich identifiziere und mit der ich identifiziert werde (wichtig ist hier auch die allgemein gehaltene Formulierung „Tätigsein “ , denn auch Erwerbslose, RentnerInnen und Invalide/Berufsunfähige haben sehr wohl Chancen, tätig zu sein oder wieder tätig zu werden...) Ein weiterer Bereich der Identität kann unter der Überschrift Arbeit, Leistung, „tätig sein “ dargestellt werden. Arbeitsleistungen, Arbeitszufriedenheit, Erfolgserlebnisse, Freude an der eigenen Leistung, aber auch entfremdete Arbeit, Arbeitsüberlastung, überfordernde sowie erfüllte oder fehlende Leistungsansprüche bestimmen die Identität nachhaltig.
- **Materielle Sicherheit** (Säule 4)
  Die Identität wird weiterhin beeinflusst von den materiellen Sicherheiten, dem Einkommen, Geld, Materielles wie Nahrung, Kleidung, Lebensbedarf, Weiterbildungsmöglichkeiten, den Dingen, die jemand besitzt, seiner Wohnung oder seinem Haus, aber auch von dem ökologischen Raum, dem er sich zugehörig fühlt, dem Stadtteil, in dem er sich beheimatet fühlt oder wo er ein Fremder ist. Fehlende materielle Sicherheiten belasten das Identitätserleben schwer.
- **Werte und Normen** (Säule 5)
  Moral, Ethik, Religion, Liebe, Hoffnungen, Traditionen, Glauben, Sinnfragen (gesellschaftliche und persönliche und ihr Verhältnis zueinander). Das was jemand für richtig hält, von dem er überzeugt ist, wofür er eintritt und von dem er glaubt, dass es auch für andere Menschen wichtig sei. Das können religiöse oder politische Überzeugungen sein, die „persönliche Lebensphilosophie“, wichtige Grundprinzipien.

5.1.3 Identität eines Menschen in der Forensik

Gemäß § 81b StPO (Strafprozessordnung) bezeichnet eine erkennungsdienstliche Behandlung (ED-Behandlung) die Erfassung personenbezogener Daten durch die Polizei. Zu unterscheiden ist die ED-Behandlung als Maßnahme zur Durchführung des Strafverfahrens von der polizeilichen Präventivmaßnahme. Eine ED-Behandlung umfasst die Aufnahme von Lichtbildern, die Abnahme von Fingerabdrücken sowie die Messung der Körpergröße. Darüber hinaus ist u.a. auch die Erstellung eines Videofilms und mit Zustimmung des Beschuldigten die Tonbandaufnahme der Stimme zulässig.

Die Aufnahme biometrischer Daten, wie es seit November 2005 bei der Ausstellung eines Reisepasses vorgeschrieben ist, ist **keine ED-Behandlung**, weil ja bereits alle Daten des Antragstellers bekannt sind und die Person feststeht. Erkennungsdienstliche Maßnahmen können auch gegen den Willen der betroffenen Person mit unmittelbarem Zwang durchgesetzt werden.

Die Löschung der Daten kann zehn Jahre nach der Erkennung beantragt werden. Der DNA-Abstrich (Mundhöhlenabstrich) darf nur auf richterliche Anordnung bei Straftaten von erheblicher Bedeutung durchgeführt werden.

Folgende gesetzliche Grundlagen gelten im Zusammenhang mit erkennungsdienstlichen Maßnahmen:

- § 24 BPolG (Erkennungsdienstliche Maßnahmen)
- § 81b StPO (Erkennungsdienstliche Maßnahmen bei dem Beschuldigten)
- § 163b StPO (Maßnahmen zur Identitätsfeststellung)
- § 49 AufenthG (Überprüfung, Feststellung und Sicherung der Identität)
- § 16 AsylG (Sicherung, Feststellung und Überprüfung der Identität)
- § 4 PaßG (Paßmuster)
- § 6 PaßG (Ausstellung eines Passes)
- § 86 StVollzG (Erkennungsdienstliche Maßnahmen)

5.1.4 Web-ID und ihre Anwendungseigenschaften

Eine WebID ist eine Netzwerk-Identität oder föderierte Identität und ermöglicht die Nutzung von Dienstleistungen und Informationen im Internet. Sie bezieht sich in der Regel auf Personen, doch sind auch Anwendungen mit Bezug auf Objekte von Rechnern usw. denkbar. Die registrierende Stelle (z. B. Behörde, Bank, Unternehmen) kennt die Identität des Identitätsbezeichners. Die Stelle definiert den Umfang der personenbezogenen Attribute, die ein Nutzer ihrer Dienste angeben muss. Für kostenlose Dienste kann ein Unternehmen bei der Registrierung einer WebID auf das Erfassen von personenbezogenen Attributen und deren Überprüfung verzichten. Gegenüber Dritten, etwa an Geschäftspartner der registrierenden Stelle, werden je nach Situation entweder nur der Identitätsbezeichner oder bestimmte Attribute der Identität offengelegt.

In Online-Transaktionen unterscheiden sich also WebIDs gegenüber Transaktionspartnern vor allem dadurch,

- welche Attribute bei der Registrierung einer WebID erfasst wurden,
- welche Attribute einem Transaktionspartner mitgeteilt werden.

Beides zusammen definiert für die registrierende Stelle bzw. den Transaktionspartner die Einfachheit des Rückschlusses von einer WebID bzw. ihrem Identitätsbezeichner auf die handelnde Person oder Gruppe:

- **Offene Identitäten**: Rückschluss auf die natürliche Person ist direkt möglich, da hinreichend viele persönliche Attribute erfasst bzw. mitgeteilt wurden;
- **Pseudonyme Identitäten**: Rückbeziehung auf die natürliche Person ist für Transaktionspartner über die registrierende Stelle möglich;
- **Anonyme Identitäten**: Rückbeziehung auf die natürliche Person ist auch für die registrierende Stelle nicht möglich.

Zu beachten ist, dass hinter einem pseudonymen Identitätsbezeichner (z. B. X345) durchaus personenbezogene Attribute stehen können. Solche pseudonymen WebIDs sind aus drei Gründen verbreitet:

1. Geschäftsinteresse der Unternehmen, die eine Kunden-Identität registriert haben: Ein Unternehmen ist in der Regel daran interessiert, Kundendaten für sich zu behalten und gegenüber Wettbewerbern zu verbergen.
2. Bereitschaft eines Kunden, personenbezogene Attribute zu liefern: Anbieter von Onlinediensten machen die Erfahrung, dass der Kunde wesentlich mehr Details über seine persönlichen Verhältnisse preiszugeben bereit ist, wenn er darauf vertrauen kann, dass seine Daten hinter einem pseudonymen Identitätsbezeichner verborgen bleiben.
3. Datenschutz: Eine Person beansprucht zumindest den gesetzlich geregelten Schutz personenbezogener Daten vor unerlaubter Verwendung und unerwünschter Verbreitung.

Wegen dieser Vorteile wird in vielen Fällen in Kauf genommen, dass pseudonyme WebIDs im Streitfall zu einem Mehraufwand bei Feststellung der dahinter verborgenen Person führen. Letztlich entscheidet allerdings der Anwendungsfall oder wie beim Online-Banking gesetzliche Regelungen, ob eine Offene WebID erforderlich ist.

Zum Schutz vor unbefugter Nutzung ist die WebID häufig durch eine 2- Faktoren-Authentisierung gesichert. Das heißt, der Nutzer muss im Besitz eines Tokens oder einer Karte sein (Besitzkomponente) und ein geheimes Passwort kennen (Wissenskomponente). Dadurch kann der Transaktionspartner feststellen, ob die handelnde Person diejenige ist, die sie vorgibt zu sein (Authentisierung). WebIDs unterscheiden sich insbesondere auch nach dem Grad der Rechtssicherheit der nach ihrer Authentisierung durchgeführten Transaktionen:

- Für **rechtssichere** WebIDs ist deren Verwendung in OnlineTransaktionen und damit verbundene Rechtsfolgen im Internet durch Gesetze geregelt.
- Bei **allgemeinen** WebIDs sind keine speziellen gesetzlichen Regelungen vorhanden; damit durchgeführte Transaktionen können jedoch auch rechtskräftig sein (Bsp.: Online- Erwerb einer Ware mittels einer nur durch Passwort geschützten WebID). Der juristische Laie kann allerdings bei allgemeinen WebIDs meist nicht erkennen, ob Transaktionen mit allgemeinen WebIDs rechtskräftig sind.

5.1.5 Identitätsdiebstahl und -missbrauch

Der Begriff **Identitätsdiebstahl** wird uneinheitlich ausgelegt. Dem Wortsinn nach ist Diebstahl die Wegnahme einer (fremden beweglichen) Sache, der Identitätsdiebstahl demnach das Aneignen der oben beschriebenen persönlichen Merkmale, die den Schluss auf nur eine Person zulassen. In der Literatur wird aber die Wegnahme immer wieder mit dem Einsatz der gestohlenen Daten vermengt.

Der **Identitätsmissbrauch** bezeichnet den unbefugten Einsatz der erlangten Daten. Für die polizeiliche Praxis macht es Sinn, die beiden Vorgänge ebenfalls zu trennen. Bestimmte Formen des Identitätsdiebstahls sind nicht strafbewehrt. Werden Identitäten erlangt, ist es von Bedeutung, wie sie erlangt wurden, um einen eindeutigen Schuldvorwurf erheben zu können. Dasselbe gilt für den Einsatz der Daten: Wie und wo wurden sie eingesetzt, was wurde damit erreicht und liegt ggf. ein neuer Tatentschluss für den Einsatz vor.

Die Motivation, die Identität einer anderen Person anzunehmen, ist vielschichtig. Hauptzielrichtungen sind die Schädigung des Vermögens des Opfers und die Diskreditierung der Person, deren Identität verwendet wird. So können auf den Namen eines anderen Waren im

Onlinehandel bestellt oder bei Onlineauktionen ersteigert werden. Während die Rechnung an den Geschädigten geht, wird die Warensendung vom Täter entweder in einer Paketstation abgeholt, die zuvor mit den gestohlenen Personalien angemietet wurde. Oder sie wird an einen (gutgläubigen) Warenagenten gesandt, der sie entgegennimmt, umpackt und neu versendet.

Möglich ist auch die Einrichtung eines Fake-Accounts. Über diesen können dann quasi im Namen des Opfers beispielsweise Beleidigungen, sexuelle Anspielungen oder Unwahrheiten – auch unterstellte strafrechtliche Begebenheiten – über dritte Personen verbreitet werden. Nicht unüblich ist neben der Einrichtung eines E-Mail-Accounts mit entwendeten Namen der gleichzeitige Diebstahl des elektronischen Adressbuches derselben Person.

An die Identität seiner Opfer gelangt der Täter durch **dumpster diving**. Zum Beispiel wird bei Banken der Papiermüll neben den Kontoauszugsdruckern oder Abfalleimer bei Großhandelsunternehmen durchsucht. Regelmäßig finden sie dort Kontoauszüge mit Namen und den entsprechenden Kontodaten. Während ein Blick ins Telefonbuch oder auf die Internetseite eines Telefonauskunftsanbieters oftmals die passende Adresse zum Namen bietet, ist die vollständige Anschrift ggf. mit Kundennummer auf der Kassenabrechnung schon aufgedruckt. Da bei der Registrierung zum Beispiel bei einem Einkaufsportal im Onlineverfahren nur die Bankverbindung auf Schlüssigkeit und Gültigkeit überprüfbar sind, kann sich der Täter ein ggf. bei der Anmeldung notwendiges Geburtsdatum ausdenken.

Eine technische Variante, Identitäten zu entwenden, ist die Verwendung von **Malware**. Nach deren Installation werden alle auf dem Rechner gespeicherten Benutzerdaten und Kennwörter in automatisierter Form an die Täterschaft weitergeleitet. Hierzu werden auf dem „Dark Market“ im Internet Toolkits angeboten. In diesen müssen je nach Zielrichtung nur noch Häkchen in vorbereitete Kästchen gesetzt werden, um ein individuelles Schadprogramm zu generieren. Die auf diesem Wege erhaltenen Daten können umgehend bei denselben Firmen eingesetzt werden, auf der auch der Geschädigte angemeldet ist. Ohne Systemeinbrüche oder den Einsatz von Malware können Informationen auf dem Wege des **Social Engineering** oder **Social Hacking** erlangt werden. Auf diese Phänomene wird in einem gesonderten Modul eingegangen.

Was die Täter intensivieren werden, ist der Diebstahl von Kartendaten (Nummer und Gültigkeit der Karte) von Karten mit Bezahlfunktion (z.B. girogo der Sparkassen oder Visa payWave) sowie Mobiltelefonen bzw. Smartphones mit der so genannten NearField-CommunicationTechnology – NFC. Die NFC besteht aus einer Kombination aus drahtloser Verbindungs- und Identifizierungstechnologie (RFID – Radio Frequency Identification). Berührungslos können Busticket oder im Restaurant mit der Kreditkarte oder dem Smartphone bezahlt werden. Es muss mit dem Medium im Abstand von zehn bis maximal 20 Zentimetern über eine Leseeinrichtung gezogen werden. Der in der Karte bzw. im Gerät eingebaute Chip kommuniziert mit dem Terminal. Den bequemen Einsatz von Karte bzw. Telefon nutzt der Täter aus, indem er versucht, mit einer auf seinem Mobiltelefon gespeicherten Applikation die Daten der Debit- bzw. Kreditkarte auszulesen. Hierzu muss er ebenfalls in einem Abstand von ca. 20 cm an sein Opfer herankommen. Gelingen kann das Auslesen, wenn Geldbörse oder Mobiltelefon beispielsweise in der Gesäßtasche getragen werden oder unbeaufsichtigt abgelegt werden. Zum Bezahlen mit diesen Daten ist zwar immer die Verknüpfung von Kartendaten und Inhabernamen notwendig, trotzdem werden diese Daten von Händlern, die nicht sorgfältig prüfen, akzeptiert. Schützen kann sich der Anwender vor dieser Art des Identitätsdiebstahles, indem er die Buchungsfunktion nur einschaltet, wenn er sie aktuell benötigt oder die Debit- bzw. Kreditkarte in einer Metallhülle verstaut.

5.2 Phishing

Phishing ist eine Form der Tricktäuschung oder des Datendiebstahls, bei der mögliche Kunden von ISPs, Geldinstituten, Online-Banking-Anbietern, Behörden usw. als Zielgruppe verwendet werden. Frei übersetzt steht es für das „Abfischen“ dieser persönlichen Daten. Über die Entstehung des Terminus gibt es verschiedene Theorien. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschreibt auf seiner Website phishing als ein aus dem Englischen stammendes Kunstwort: password und fishing, was übersetzt „Passwortangeln“ heißt. Der Informatiker Fox erklärt den Begriff in der Ausgabe der Fachzeitschrift Datenschutz und Datensicherheit als Fischen – fishing – von Kriminellen nach Passwörtern und Kreditkarteninformationen bei Internet-Nutzern. In Anlehnung an die Manipulation von Telefonverbindungen in den 1970er bis 1990er Jahren, dem so genannten phreaking, wurde anstatt des führenden Buschstabens ‚f‘ das ‚ph‘ gewählt. Von der „AntiPhishing Working Group (APWG)“ wird behauptet, dass der Ursprung des Wortes phishing tatsächlich von fishing herrührt, dies aber – wie in Hackerkreisen üblich – mit ‚ph‘ anstatt ‚f‘ geschrieben wird. Wenn Sie Ihre E-Mail-Adresse im Internet zum Beispiel in Online-Formulare oder beim Zugriff auf Newsgroups oder Webseiten eingeben, können die Daten von Crawler-Programmen gestohlen und ohne Ihre Zustimmung für betrügerische Zwecke oder andere Straftaten eingesetzt werden.

5.2.1 Das Konzept hinter Phishing

Phisher erstellen gefälschte Webseiten, die aussehen, wie die Seiten bekannter und vertrauenswürdiger Anbieter. Anschließend wird mit Hilfe von E-Mail-Datenbanken oder zufällig generierten Adressen der Köder ausgeworfen. Eine Nachricht mit einem glaubwürdigen Betreff wird per E-Mail oder Instant-Messenger verschickt. Darin wird nach vertraulichen Daten gefragt, die auf einer Webseite (Verknüpfungen wie „Hier klicken“, URL-Verknüpfungen, Bildverknüpfungen, Textverknüpfungen) oder direkt in einem Formular in der E-Mail eingegeben werden sollen. Die Anfrage erscheint logisch und im Normalfall wird bei Nichtbeachtung mit Folgen gedroht, um eine sofortige Reaktion zu erwirken.

Beispiele für E-Mail-Betreffzeilen:

„Aktualisieren Sie Ihr PayPal-Konto“

„Ihr eBay-Konto wurde gesperrt!“

Meist wird nach den folgenden oder ähnlichen Daten gefragt:

- Nummer der Kreditkarte
- Geheimzahl und TAN für Geldautomaten oder Online-Banking
- Kontodaten
- Sozialversicherungsnummer
- Kennwörter
- E-Mail-Konto-Daten
- andere persönliche Daten

Sobald diese Daten eingegeben wurden, sind sie nicht länger vertraulich oder geheim und werden von den Betrügern für eigene Zwecke missbraucht. Im Normalfall ist es sehr schwierig, sein Geld zurückzubekommen, denn die Phishing-Sites werden bereits nach wenigen Tagen oder sogar Stunden wieder vom Netz genommen.

5.2.2 Phishing-Techniken

Hauptsächlich wird eine vertrauenswürdig erscheinende E-Mail verwendet, über die man auf eine gefälschte Webseite gelockt wird. Einige Phishing-E-Mails enthalten ein Antrags- oder Bestellformular im Nachrichtenteil der E-Mail. Man sollte beachten, dass die entsprechenden Stellen niemals E-Mails mit Formularen versenden oder nach persönlichen Angaben fragen.

Die URL der gefälschten Webseite kann vom richtigen URL abweichen. Aber URLs können auch gefälscht werden:

- **Social Engineering**: Die URL ähnelt der echten URL sehr, was nicht immer auf den ersten Blick auffällt. So kann die URL http://www.volksbank.com mit http://www.volksbank.com gefälscht werden. Die sind doch gleich, meinen Sie? Weit gefehlt! Der Kleinbuchstabe „l“ wurde im Beispiel durch ein großes „i“ ersetzt.
- **Browser-Schwachstellen**: Die gefälschte Webseite könnte ein Skript enthalten, das Sicherheitslücken (Exploits) des Browsers ausnutzt. In diesem Fall wird die korrekte URL angezeigt, aber der Inhalt der Webseite kommt vom betrügerischen Server. Ein Beispiel wäre das Einblenden eines gefälschten Bildes über der eigentlichen Adressleiste des Browsers. Sie können nicht in das Eingabefeld dieser Leiste klicken, um die URL zu markieren. Andere Exploits können ein gefälschtes Eingabefeld anzeigen, sodass Sie sogar in das Feld klicken und die URL markieren können.
- **Pop-ups**: Die Verknüpfung in der E-Mail verweist auf die richtige Webseite, aber ein weiteres Browserfenster wird im Vordergrund geöffnet. Es ist grundsätzlich möglich, die echte Webseite ohne Gefahren zu betrachten, aber das zweite Fenster könnte gefährlich werden. Pop-ups verfügen gewöhnlich nicht über eine Adressleiste, an der sich gefälschte Webseiten erkennen lassen.
- **Keine Adressleiste**: Einige gefälschte Seiten zeigen die Adressleiste gar nicht an. Wenn Sie also nicht darauf achten, könnte es sein, dass Ihnen das Fehlen der Leiste nicht auffällt.

Es gibt weitere Techniken, die zusätzlich oder anstelle von Änderungen der Adressleiste verwendet werden können, um an vertrauliche Informationen heranzukommen.

- **Andere Browser-Schwachstellen**: Über eine andere Schwachstelle im Browser kann auch beliebige bösartige Software heruntergeladen und ausgeführt werden. Dabei kann es sich beispielsweise um einen Trojaner handeln, der alle Tastenanschläge aufzeichnet und den gesamten Internetverkehr überwacht – vor allem, wenn Sie Daten in ein Online-Formular eingeben und absenden.
- **Pharming**: Hier spricht man auch von „Domain Spoofing“. Dabei werden Anwender auf eine gefälschte Webseite umgeleitet. Obwohl die URL im Browser korrekt eingegeben wurde, wird eine gefälschte Webseite aufgerufen. Die korrekte URL wird jedoch ohne Änderung angezeigt. Für eine solche Umleitung muss die Namensauflösung geändert werden. Das ist durch Ändern der TCP/IP-Protokolleinstellungen oder durch einen Eintrag in der Hostsdatei möglich.
- **Man-in-the-Middle**: Das ist wohl die anspruchsvollste Methode, da auf dem lokalen Rechner keine Änderungen erfolgen. Der Phisher sitzt als „Mann in der Mitte“ zwischendrin und leitet Ihre Verbindung auf einen falschen Server um.

5.2.3 Möglichkeiten der Tarnung von Phishing-Versuchen

Folgende Tricks sind dafür bekannt, zur Tarnung gefälschter Webseiten eingesetzt werden (Auswahl):

- gefälschte bzw. manipulierte Tooltipps
- gefälschte E-Mailadressen und Webseiten
- Domain Spoofing (Umleitung auf eine gefälschte Webseite über einen unsichtbaren Text in E-Mails auf HTML-Basis)
- Social Engineering Techniken
- Manipulation der Absenderinformationen
- Reputation der gefälschten Webseiten
- nur Grafiken (kein Text in der E-Mail)

5.2.4 Folgen und Beispiele

Da Phisher so viele verschiedene Techniken oder Kombinationen daraus verwenden, ist es nicht leicht zu erkennen, ob eine E-Mail aus offizieller Quelle stammt oder nicht. Welche Folgen kann es aber haben, vertrauliche Informationen preiszugeben?

- Die Phisher können Ihr Konto belasten
- Sie können neue Konten eröffnen und/oder Dienstleistungs- oder Mietverträge in Ihrem Namen eingehen.
- Sie können eine falsche Identität verwenden und Verbrechen mit Ihren persönlichen Daten begehen.

Auch wenn es heute sehr schwer ist, schadhafte E-Mails schnell zu identifizieren, gibt es einige sichere Hinweise für einen Betrugsversuch. Folgende beispielhafte Auffälligkeiten gelten als Warnzeichen:

- **Grammatik- und Orthografie-Fehler:** Am einfachsten zu durchschauen sind E-Mails, die in fehlerhaftem Deutsch geschrieben sind. Meistens wurden sie nicht in Deutsch verfasst, sondern sind mit einem Übersetzungsdienst aus einer anderen Sprache übersetzt worden. Ein weiterer Hinweis auf solche E-Mails sind Zeichensatzfehler, wie etwa kyrillische Buchstaben oder auch fehlende Umlaute.
- **Mails in fremder Sprache**: Ebenfalls schnell als Phishing zu erkennen sind E-Mails, die auf Englisch oder Französisch verfasst sind. Sollten Sie nicht gerade Kunde einer Bank mit Sitz im Ausland sein, können Sie sicher sein, dass Sie (wenn überhaupt) E-Mails von Ihrer Bank nur auf Deutsch bekommen.
- **Fehlender Name**: Ihre Bank und andere Geschäftspartner wie zum Beispiel Online-Zahlungsdienste sprechen Sie in E-Mails grundsätzlich mit Ihrem Namen an und niemals mit „Sehr geehrter Kunde“ oder „Sehr geehrter Nutzer“. Sehr raffinierte Phishing-Täter haben aber oftmals auch Ihren Namen schon herausgefunden.
- **Dringender Handlungsbedarf**: Wenn Sie via E-Mail aufgefordert werden, ganz dringend und innerhalb einer bestimmten (kurzen) Frist zu handeln, sollten Sie ebenfalls stutzig werden. Insbesondere, wenn diese Aufforderung mit einer Drohung verbunden ist - beispielsweise, dass sonst Ihre Kreditkarte oder Ihr Online-Zugang gesperrt werden.
- **Eingabe von Daten**: Die Aufforderung, persönliche Daten sowie möglicherweise PIN oder TAN einzugeben, ist ein weiterer Hinweis. Banken und Online-Zahlungsdienste werden Sie um so etwas nicht per E-Mail bitten. PIN und TAN werden von Geldinstituten niemals telefonisch oder per E-Mail abgefragt; dies zählt zu den wesentlichen Sicherheitsregeln.

- **Aufforderung zur Öffnung einer Datei**: In immer mehr Phishing-E-Mails werden die Empfänger aufgefordert, eine Datei zu öffnen, die entweder als Anhang der E-Mail direkt beigefügt ist oder alternativ über einen Link zum Download bereitsteht. In unerwarteten E-Mails dürfen Sie eine solche Datei keinesfalls herunterladen oder gar öffnen. Denn in der Regel beinhaltet diese Datei ein schädliches Programm wie ein Virus oder ein trojanisches Pferd. Lassen Sie sich auch von angedrohten Konsequenzen wie zum Beispiel einer Kontosperrung, der Einschaltung eines Inkassounternehmens oder anderen erfundenen Gründen niemals dazu verleiten, eine beigefügte Datei zu öffnen! Bei E-Mails mit einem Dateianhang sollten Sie grundsätzlich misstrauisch sein.
- **Links oder eingefügte Formulare**: Banken versenden in der Regel keine E-Mails, sondern Briefe. Falls Sie doch E-Mails von Ihrer Bank erhalten, so wird diese keine Dateianhänge (wie Formulare, über die eine Eingabe gemacht werden muss) versenden. Banken und andere Dienstleister versenden nur in Ausnahmefällen E-Mails mit Links, auf die der Empfänger klicken soll. Dann geht es beispielsweise um neue AGBs, niemals aber um das Einloggen in Ihr Kundenkonto. Besser ist ohnehin immer, die Internetseite selbst aufzurufen, indem Sie diese in das Adressfeld des Browsers eintippen.
- **Bisher noch nie E-Mails von der Bank erhalten oder kein Kunde**: Wenn Ihre Bank Ihnen nie E-Mails schickt, eventuell Ihre E-Mailadresse gar nicht kennen kann, oder ein anderer Dienstleister sie kontaktiert, mit dem Sie keine Geschäftsbeziehung haben - löschen Sie die E-Mail.
- **Mailheader**: Manche Phishing-Mails sind sehr gut gemacht. Die AbsenderE-Mailadresse scheint vertrauenswürdig, der Link im Text auch, das Deutsch ist flüssig? Trotzdem muss diese E-Mail nicht echt sein. Auch Absenderangaben von E-Mails lassen sich fälschen. Wenn Sie - um letzte Zweifel auszuräumen - das prüfen wollen, müssen Sie sich den so genannten Mail-Header anschauen. Dort steht die IP-Adresse des Absenders. Nur diese ist fälschungssicher und gibt Aufschluss über den tatsächlichen Absender.

Die Abbildung 19, Abbildung 20 und Abbildung 21 zeigen Phishing-Beispiele. Als modern geltende Phishing-Mail setzen nicht mehr auf die Zurücksendung der Daten durch den späteren Geschädigten. Vielmehr soll der Empfänger einem in der Mail platzierten Link folgen, der ihn auf eine gefälschte Internetseite lockt, die mit ihrer Aufmachung beispielsweise der einer offiziellen Bankseite gleicht. Gibt der Kunde dort seine Zugangsdaten ein, werden diese gespeichert und später für ungewollte Transaktionen seitens der Täter genutzt. Trotz intensiver Bemühungen der Banken, ihre Kunden über diese Gefahr aufzuklären, ist die Erfolgsquote dieser Masche weiterhin hoch genug, um den Hochdurchsatzversand solcher Mails zu befürworten. Die allgemeine Skepsis der Bevölkerung gegenüber E-Mails hat jedoch in den letzten Jahren und mit steigender Anzahl verdächtiger Mails mehr und mehr zugenommen, wodurch sich eine leichte Abwehrhaltung gegenüber dieser eingestellt hat. Die erschreckend effiziente Antwort dieser Tatsache von der Täterseite ist der Versand so genannter „Spear-Infektionen“. Darin wird der Kunde mit korrektem Namen von der korrekten Bank angesprochen, was die Trefferquote an Opfern erhöhte. Diese Art der personalisierten Phishing-Mails war so erfolgreich, dass sie weiter verfeinert wurde. Ein Mahnschreiben, welches direkt an den Kunden gerichtet ist und weitere korrekte persönliche Daten enthält, verleitet schnell dazu, dem in der Mail enthaltenen Link zu folgen und damit in die Falle der potenziellen Täter zu gehen. Darüber wird entweder Schadsoftware auf dem Kundenrechner installiert, die später illegale Eingriffe durchführen kann oder die Nutzung der darauf befindlichen Dateien durch den Nutzer verweigert. Erst gegen ein gefordertes Lösegeld sollen diese Dateien wieder zur Verfügung stehen. Weitere Beispiele von bekannten Phishing-Versuchen sind die gefälschten Freundschaftsanfragen auf sozialen Netzwerken. Einem vermeintlichen Freund vertraut man leichter und fällt daher schneller auf falsche Links herein. Als letztes Beispiel sollen die so genannten „Drive-by-Infektionen“ genannt werden.

Hierbei verweisen die Links, die angeklickt werden sollen, auf eine offizielle Seite, der man normalerweise vertraut. Ohne Wissen des Betreibers wurde diese Seite vorher jedoch durch Ausnutzung von internen Sicherheitslücken präpariert. Der ahnungslose Kunde installiert nun nur aufgrund seiner Anwesenheit auf der offiziell sicheren Seite eine unentdeckte Schadsoftware auf seinem System. Die Verbindung dieser Methode mit dem Versand der Links über soziale Netzwerke hat sich als besonders effektiv für die Täterseite herausgestellt, da die Hemmschwelle vieler Menschen bei vermeintlichen Freunden im Netz immer noch deutlich geringer ist.

Abbildung 19: Phishing-E-Mail mit Verlinkung auf falsche Anmeldeinformationen.

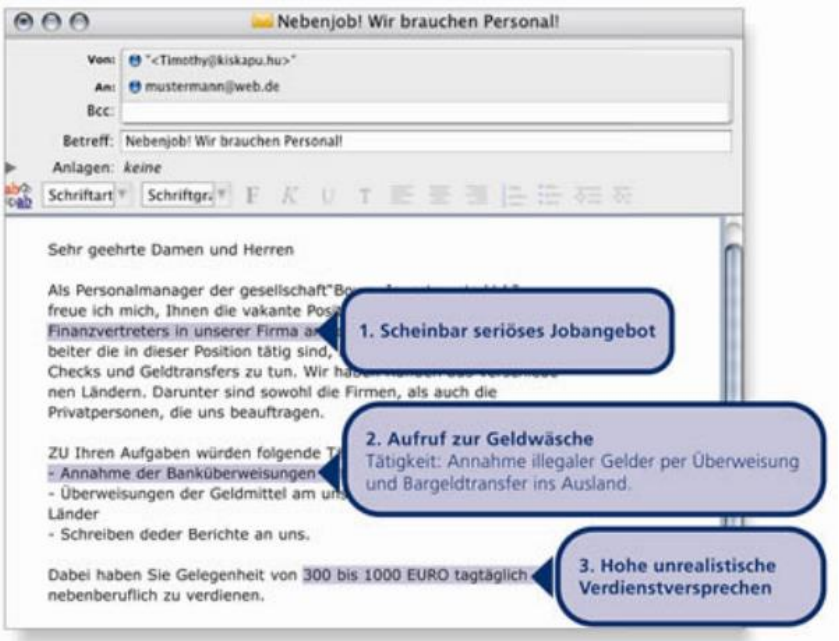


Abbildung 20: Angebliches Jobangebot

Abbildung 21: Beispiel eBay Logindaten

5.3 Skimming

5.3.1 Phänomenbeschreibung

Bei dem Begriff Skimming handelt es sich um den Vorgang des elektronischen Auslesens des Magnetstreifens einer Bank- oder Kreditkarte. Skimming bzw. „to skim“ beduetet abschöpfen, absahnen und bezieht sich demnach auf das Abgreifen sensibler Kundendaten wie z.B. die Karten-PIN.

Um das sogenannte Absahnen zu ermöglichen, werden Geldautomaten auf verschiedene Art und Weisen manipuliert. Die wohl bekannteste Methode ist das Anbringen einer Leseeinheit, der Skimmer, über dem Karteneinzugsschacht. Dieser besteht meistens aus Kunststoff. Eine andere, etwas komplexere Möglichkeit ist das Anbringen einer kompletten nachgebauten Front (front covering), die vor das Geldautomatenbedienfeld gesetzt wird. In dieser befindet sich dann der Skimmer.

Eine dritte, vom Geldautomaten unabhängige Möglichkeit liegt in der Manipulation des Kartenlesers am Türöffner des Eingangsbereichs des Geldinstituts. Sobald die Karte in den Türöffner eingeführt wird, werden alle sensiblen Daten auf dem Anbaugerät gespeichert, dieses zu einem späteren Zeitpunkt entfernt und aus den erlangten Daten ein Kartenrohling, der sogenannte *white plastic* erstellt.

Der Kartenrohling allein nützt den Tätern nichts, denn um Verfügungen über ein Konto ausgespähter Kunden vorzunehmen sind entweder die PIN oder die Unterschrift von diesem notwendig. Um an diese Daten zu kommen, besteht zum einen die Möglichkeit darin, mit Hilfe einer Minikamera die Eingabe der PIN zu filmen oder mit einem über der Tastatur des Eingabefeldes befestigten Aufsatzes auf diesem Wege abzugreifen. In sehr seltenen Fällen befinden sich die Täter in der Nähe und spähen die Daten direkt aus. Wenn die Kartendaten und die zugehörige PIN vorliegen, wird von einem sogenannten Dump gesprochen. Neben normalen Geldautomaten liegen auch sogenannte POS-Terminals und Tankstellen im Fokus der Täter. Im Jahr 2012 verzeichnete das Bundeslagebild „Zahlungskartenkriminalität“ des BKA insgesamt 856 Angriff auf Geldautomaten und 77 Manipulationen von POSTerminals. Die Schwachstellen von den betroffenen EC-Karten/DebitKarten, sind die Magnetstreifen, auf denen sich die notwendigen Da ten für beispielsweise das Bezahlen und Abheben am Geldautomaten befinden. Das Auslesen der Daten der Magnetstreifen stellt kein Problem dar, da über Online-Händler eine Vielzahl von Fertigbaukästen bestellt werden können, die alle notwendigen Software- und Hardwarekomponenten für eben diese Tätigkeit bezogen werden können. Um eine Manipulation und ein Auslesen kundenspezifischer Daten zu verhindern setzen Banken-, Automaten- und Kartenhersteller auf unterschiedliche technische Sicherheitsvariationen.

Unter anderem ist zum Beispiel der Einbau von Induktionsspulen möglich, mit deren Hilfe am Karteneinzugsschacht angebrachte Auslesegeräte erkannt werden. Sobald dies der Fall ist wird der Geldautomat abgeschaltet. Problematisch an dieser Technik ist jedoch der Umstand, dass die Induktionsspulen auch auf andere Metalle reagieren, die entweder beabsichtigt oder unbeabsichtigt vor den Einzugsschacht gehalten werden. Eine andere Technik ist der Einsatz eines modulierten Wechselmagnetfeldes, welches ebenfalls am Karteneinzugsschacht angebracht wird. Sollte sich ein illegal angebrachtes Kartenauslesegerät am Geldautomaten befinden, wird dadurch dessen Magnetkopf gestört und der Aufsatz somit nutzlos.

Neben den vorgestellten Techniken gibt es eine weitere Schutzeinrichtung, die als **Jittering** bezeichnet wird. Diese Technik ist dem einen oder anderen bereits bekannt. Beim Jittering wird die Karte ruckartig in den Einzugsschacht hinein- und wieder herausgezogen. Dadurch wird eine Synchronisation des Magnetstreifens mit der Skimmingeinrichtung verhindert. Sobald jedoch von mit

den Anbaugeräten der Täter die Rohdaten ausgelesen werden, bietet diese Technik keinen zuverlässigen Schutz mehr. Das ruckartige Bewegen der Karte kann ohne Probleme eliminiert und die Daten wieder vollständig ausgelesen werden.

Eine weitere Neuerung zur Sicherheit des Datendiebstahls stellt die Umsetzung des **moduliert maschinenlesbaren Merkmals**, kurz MM-Merkmal dar. In den Karten werden mehrere dielektrische Materialien verbaut, die sich kapazitiv abtasten lassen. Im Geldautomaten werden die Daten, die als MM-Code bezeichnet werden, mit den auf dem Magnetstreifen befindlichen Informationen verknüpft und nur bei einer Übereinstimmung akzeptiert.

Neben dem MM-Merkmal wurde am 01.01.2005 der sogenannte **EMV-Standard** eingeführt. EMV bezieht sich dabei auf die drei Unternehmen Europay International, MasterCard und Visa, die diesen Standard entwickelt haben. Beim EMV-Standard sind die Karten mit einem Mikroprozessor ausgestattet und tauschen alle notwendigen Daten für Transaktionen mit Geldautomaten nur verschlüsselt aus. Voraussetzung ist jedoch, dass die Geldautomaten über die notwendige Technik verfügen. Laut der Herstellerangaben ist dieses Verfahren resistent gegenüber Manipulationen und dem Kopieren von sensiblen Daten. Eine Kommunikation zwischen Karte und Geldautomat kann auch im Offlinemodus durchgeführt werden. Seit dem 01.01.2011 müssen in der EU (SEPA-Raum) alle Geldautomaten und Bezahlterminals mit dem EMV-Standard ausgerüstet sein. Abschließend kann hinzugefügt werden, dass das Ziel dieses Standards in der grundsätzlich sicheren Zahlungsabwicklung und Geldabhebung liegt.

Straftaten, die ebenfalls im Zusammenhang mit einem Geldautomaten stehen:

Weitere Straftaten im Zusammenhang mit einem Geldautomaten sind **Cash Trapping** und **Loop-Trick**. Bei ersterem wird der Schacht des Geldautomaten manipuliert, sodass das Geld darin stecken bleibt und nicht herausgegeben wird. Sobald dieser Umstand auftritt, geht der Kunde möglicherweise von einem Automatendefekt aus und entfernt sich. Die meisten Kunden gehen davon aus, dass das Geld wieder auf das Konto gebucht wird. Sobald die Kunden sich von den Automaten entfernt haben entnimmt der Täter das Geld.

Beim **Loop-Trick** wird die Öffnung des Karteneinzugsschachts mit einem dünnen Band so manipuliert, dass es für den Automaten nicht mehr möglich ist die Karte wieder herauszugeben. Der Täter befindet sich ebenfalls in der Nähe des Geldautomaten und gibt sich als „freundlicher Passant“ aus und schlägt vor den PIN noch ein zweites Mal einzugeben. In diesem Moment versucht der Täter die PIN auszuspähen. Da der Automat wie bereits erwähnt manipuliert ist, wird die Karte selbstverständlich trotzdem nicht wieder ausgegeben. Sobald der Kunde sich von dem Geldautomaten entfernt, entnimmt der Täter die Geldkarte und greift mittels der PIN auf das Konto des betrogenen Kunden zu.

5.4 Ransomware (Online-Erpressungen)

5.4.1 Phänomenbeschreibung

Ransomware ist eine Art von Malware, deren Hauptziel darin besteht, die Daten eines Opfers zu verschlüsseln oder den Zugriff darauf zu blockieren, um dann Lösegeld von den Opfern zu erpressen. Der Begriff "Ransomware" leitet sich von "ransom" (Lösegeld) und "software" ab und beschreibt genau das, was diese Art von Malware tut: Sie sperrt die Dateien des Opfers und verlangt von ihnen eine Zahlung, um die verschlüsselten Daten wiederherzustellen oder den Zugriff darauf freizugeben.

5.4.2 Beispiel: Scareware

Scareware wird der Kategorie Ransomware zugeordnet. Bei Scareware handelt es sich um Schadsoftware, die den Nutzer erschrecken bzw. Angst einjagen soll. Dieser wiederum soll dann Handlungen am PC ausführen, die er sonst nicht getätigt hätte. Klassische Scareware dient dazu, dem Betroffenen zu suggerieren, dass sein Computer mit Viren befallen ist. Sobald dieser Fall eintritt, lösen die Täter gefälschte Hilfsangebote an den betroffenen Nutzer aus. Diese Hilfsangebote sind meistens Downloadvorschläge von kostenlosen Antivirusprogrammen, die den Schaden beheben sollen. Jedoch führen diese Softwareangebote nicht

zu einem positiven Ergebnis, ganz im Gegenteil. Nach wenigen Tagen wird durch das heruntergeladene Antivirusprogramm eine Empfehlung zum Update auf eine zahlungspflichtige Version angeboten, da sonst die Probleme weiter bestehen bleiben würden. Auf diesem Wege erhalten die Täter dann Zahlungen der betroffenen Nutzer. Eine andere Variante besteht in der Verschlüsselung persönlicher Daten, hervorgerufen ebenfalls durch den Download von Antivirensoftware. Erst nach der Zahlung eines Lösegeldes werden die Daten wieder freigegeben. Aggressivere Varianten wie „Ukash- oder BKA-Trojaner“ sperren den infizierten Rechner und geben diesen erst nach einer Strafzahlung wieder frei.

5.4.3 Wege der Infizierung (Beispiele)

5.4.3.1 Drive-by-Download

Eine Möglichkeit einer Infizierung des Rechners ist der sogenannte Drive-by-Download. Wenn ein Nutzer auf einer inkriminierten Webseite unterwegs ist, reicht meist ein Klick aus, um unbewusst und unbeabsichtigt Schadsoftware herunterzuladen und diese auf dem Rechner zu installieren. Das Schadprogramm bzw. die Malware beeinflusst dann den Autostart des jeweiligen Betriebssystems. Da bei jedem Neustart des Computers auch der eingehandelte Trojaner neu gestartet wird, ist eine Löschung von diesem sehr schwer. Die Trojaner können neben der reinen Infizierung des Rechners auch Daten verschlüsseln, die dann erst nach einer Strafzahlung angeblich wieder freigeschalten werden. Neben der Verbreitung schädlicher Links oder Downloads auf Internetseiten mit erotischen Inhalten wurden bereits alltägliche Internetseiten und soziale Netzwerke infiziert.

5.4.3.2 .zip-Trojaner

Eine weitere Methode Rechner erfolgreich zu infizieren ist der Versand von manipulierten E-Mails. Diese Vorgehensweise ist vielen bekannt und wird auch als .zip-Trojaner bezeichnet. Bei dieser Methode erhält der Geschädigte beispielsweise eine E-Mail mit einer Bestellbestätigung von Zalando oder eine Handyrechnung eines Telefonanbieters. Im Anhang der E-Mail befindet sich dann eine .zip-Datei, in manchen Fällen auch eine .pdf-Datei, die nach dem Anklicken die Ransomware auf dem Rechner freisetzen. Die Täter sind sehr einfallsreich und fälschen heutzutage selbst

Finanzdokumente. Wenn der Rechner infiziert wurde öffnet sich ein Popup-Fenster, welches dem Nutzer suggeriert, dass der Rechner vom Bundeskriminalamt, GEZ oder GEMA überwacht und aufgrund von angeblichen Verstößen (Download kinderpornographischer Filme, illegaler Musik, etc.) gesperrt wurde (Abbildung 22). Ziel ist es in allen Fällen Geld von den Nutzern zu erhalten.

Abbildung 22: Variante eines sogenannten BKA-Trojaners

5.4.3.3 Phishing-E-Mails

Eine der häufigsten Methoden zur Verbreitung von Ransomware ist über Phishing-E-Mails. Angreifer senden gefälschte E-Mails, die wie legitime Nachrichten von vertrauenswürdigen Quellen aussehen, und enthalten oft bösartige Anhänge oder Links. Wenn ein Benutzer auf diese Anhänge klickt oder sie öffnet, wird die Ransomware auf dem Computer installiert. Auch bösartige Links auf Websites, in Chatnachrichten oder in sozialen Medien können zur Infizierung führen. Diese Links können zu bösartigen Webseiten führen, die die Ransomware automatisch herunterladen und installieren, wenn der Benutzer darauf zugreift.

5.4.3.4 Schwachstellen in Software

Ransomware kann auch über bekannte Schwachstellen in Softwareanwendungen oder Betriebssystemen verbreitet werden. Angreifer nutzen diese Schwachstellen aus, um bösartigen Code auf dem Computer auszuführen und die Ransomware zu installieren. Es ist wichtig, regelmäßig Sicherheitsupdates und Patches zu installieren, um bekannte Schwachstellen zu schließen und das Risiko einer Infektion zu verringern.

5.4.3.5 Infizierte Dateien, Programme oder externe Geräte

Ransomware kann auch über infizierte Dateien oder Programme verbreitet werden, die aus unsicheren Quellen heruntergeladen wurden. Dies kann Torrents, Raubkopien von Software, Cracks oder Keygens umfassen. Wenn ein Benutzer diese Dateien herunterlädt und öffnet, kann die Ransomware auf dem Computer installiert werden. Auch Externe Geräte wie USB-Sticks, externe Festplatten oder SD-Karten können ebenfalls Ransomware übertragen (Bating), insbesondere wenn sie an einen infizierten Computer angeschlossen werden. Die Ransomware kann sich dann auf das externe Gerät kopieren und sich beim Anschluss an andere Computer weiterverbreiten.

5.5 Internetbanking, Onlinebanking

5.5.1 Warum Internetbanking?

Das Internet ist aus unserer Gesellschaft nicht mehr wegzudenken. Aus diesem Grund versuchen Geld- und Versicherungsunternehmen weltweit ihr Geschäft langsam ins Netz zu verlagern, um einerseits internetaffine Kunden zu gewinnen und um andererseits an Personal einzusparen. Das s.g. Internet- oder Onlinebanking ist per Definition die Ausführung von Bankgeschäften mit direktem Zugriff auf Bankrechner von einem Endgerät, PC oder Smartphone via Datenübertragung. Geldgeschäfte via Computer können jedoch ebenfalls ins Visier von einer modernen Version des Bankräubers geraten, welche ganz ohne panzerknackendes Gerät Geld auf andere Konten transferieren können. Dieses Kapitel beschäftigt sich daher mit den wichtigsten Verfahren und mit möglichen Angriffspunkten beim Onlinebanking.

5.5.2 Techniken

Prinzipiell kann in zwei verschiedene Techniken zum Online-Banking unterschieden werden. Wird eine **Banksoftware** benutzt, muss zunächst eine zertifizierte Software auf den eigenen Rechner installiert werden. Geplante Überweisungen und Geschäfte werden dann zunächst offline vorbereitet und in eine Abfolge von Ausführungsbefehlen umgewandelt. Diese werden dann über eine sichere Verbindung zum Server ausgeführt. Beim Onlinebanking via Browser wird vom Gerät direkt die Webseite des Geldinstituts aufgerufen. Über private Logins werden die Zugänge autorisiert und geschützt, während geplante Transaktionen digital unterschrieben oder bestätigt werden müssen.

Wie beim herkömmlichen Sicherheitstresor gibt es auch beim Onlinebanking keine 100%-ige Sicherheit. Die Schwachstellen im System liegen hier jedoch nicht im Safematerial oder bei den unaufmerksamen Wachmännern, sondern im zugrundeliegenden Programmcode der jeweiligen Zugangssoftware. Wie bei jedem Quellcode geht man davon aus, dass es trotz intensiver Kontrollen etwa einen größeren Bug alle 1000 Codezeilen gibt. Diese Probleme werden zwar ständig verbessert und geupdatet, einen völlig bugfreien Code wird es bei diesem Umfang trotzdem nicht geben. Da bereits 2013 etwas weniger als die Hälfte aller Bankkunden Onlineverfahren benutzen, gibt es auch viele tausend potentielle Augen, die solche Sicherheitslücken ausfindig machen können. Dieser Umstand macht das Banking via Banksoftware theoretisch etwas sicherer, da es hier einfach viel weniger Nutzer gibt. Professionelle Tests haben aber gezeigt, dass sich beide Techniken manipulieren bzw. hacken lassen.

5.5.3 Authentifizierung

Um am Onlinebanking teilnehmen zu können, benötigt jeder Nutzer zuvor vereinbarte Sicherheitsmerkmale, die er über ebenfalls vorher vereinbarte Eingabegeräte auf Abruf vorzeigen kann. Diese Prozedur ersetzt die gängige Unterschrift und die persönliche PIN-Nummer am Bankautomaten. Es gibt grundsätzlich drei verschiedene Nachweismöglichkeiten, die heutzutage Anwendung finden:

Beim **Informationsnachweis** bestätigt der Nutzer seine Beteiligung bzw. sein Wissen am zu tätigenden Geschäft, indem er eine zugeschickte PIN-Nummer eingibt, definierte Sicherheitsfragen beantwortet oder sein Kennwort eingibt. Bekannte Angriffspunkte dieser Prozedur sind das systematische Abgreifen dieser Nachweise per Phishing oder Tastaturausleseprogrammen (Keylogger). Sind die sensiblen Daten einmal akquiriert worden, können sie von fast allen PCs aus benutzt werden, was die potentielle Gefahr weiter erhöht.

Eine weitere, hochfrequent eingesetzte Methode ist die Nutzung bestimmter **Besitztümer**. Dabei wird nur derjenige fürs Banking autorisiert, der eine Liste von Transaktionsnummern (TAN) besitzt und auf Anfrage eine bestimmte davon eingeben kann. Umgangen werden kann dieses System über s.g. Man-in-the-Middle-Angriffe, bei dem die Onlinepräsenzen der Banken vorgetäuscht werden, um solche TAN-Listen zu erhalten. Weitere Beispiele für diese Art des Nachweises sind SecurityTokens, welche physisch an den Rechner angeschlossen werden müssen um pseudozufällige Zahlen mit dem Anmeldeserver zur Authentifizierung auszutauschen und s.g. mTANs, bei denen eine einmalig benutzbare PIN oder TAN an eine vorher festgelegte Mobilfunknummer gesendet wird. Trotz des recht bedienerfreundlichen Aufbaus dieser Methode verzeichnet sie bisher noch keine großen Nutzerzahlen. Die Smartphone-App von der Supermarktkette EDEKA kann ebenfalls in diese Kategorie des Nachweises per Besitztum gezählt werden.

Hier wird eine App installiert, in der sich der Kunde registriert und seine Daten zur Bankverbindung hinterlegen. Diese Verbindung muss zunächst freigeschaltet werden, indem eine Identifizierungsnummer von einer Überweisung aufs eigene Konto (1 Cent) vom Kunden angegeben wird. Nun kann der Kunde die Filiale in der App eingegeben und die PIN benutzen. Nach dieser Authentifizierung erscheint ein scannbarer QR-Code auf dem Smartphone, der an der Kasse eingelesen werden kann. Nach einem Validierungsschritt in der Clearingstelle der Zahlungsdienstelle der Deutschen Post (DBZ) wird der Kassenkraft mitgeteilt, dass der Bezahlvorgang erfolgreich abgeschlossen ist und das nötige Geld per Lastschrift eingezogen wurde. Auch hier gibt es ausnutzbare Schwachstellen. Im Darknet erworbene Kontoverbindungen können beispielsweise für Betrugsversuche verwendet werden.

Zuletzt ist auch der Nachweis der **persönlichen Anwesenheit** zur Authentifizierung möglich. Typischerweise werden dazu biometrische Maße wie der Fingerabdruck, das Gesicht, die Iris oder die Stimme vermessen. Besonders hohe Beliebtheit hat dabei der Fingerabdruckscanner, der das Muster einer Fingerbeere, das als einmalig gilt, aufnimmt und mit einer Datenbank vergleicht. Kopierte Fingerabdrücke oder manipulierte Sensoren führen jedoch recht einfach zu ungewollten falschpositiven Ergebnissen, weswegen man auf diese Art der Authentifizierung bei kritischen Vorgängen verzichten sollte. Über die Eingabe eines vorgegebenen Satzes kann auch das Tippverhalten des Nutzers geprüft werden. Auch hier gibt es potentiell die Möglichkeit, jenes Verhalten über einen Keylogger im Vorhinein zu bestimmen und nachzuahmen.

Um die Anfälligkeit für Straftaten deutlich zu senken, gibt es heute bei vielen Unternehmen eine Kombination aus zwei der eben vorgestellten Methoden. Bei der sogenannten Zwei-Faktoren-Authentifizierung (2FA) wird oftmals der Informationsnachweis mit einem Besitztum verbunden, um ein sichereres Banking zu gewährleisten. Ein Beispiel hierfür ist das klassische Onlinebanking, bei dem

zunächst das Wissen der PIN bei der Anmeldung und dann der Besitz einer TAN bei der Überweisung abgefragt werden. Natürlich besteht auch hier die Möglichkeit, die Sicherheitsverfahren zu umgehen, der immens gesteigerte Aufwand dient dennoch als recht verlässliche Hürde für potentielle Täter.

5.5.4 Ausgewählte Verfahren des Onlinebanking

5.5.4.1 TAN

Bei diesem Prinzip erhält der Kunde anfänglich eine Liste von Transaktionsnummern. Bei jeder getätigten Transaktion kann er nun eine davon auswählen und eingeben. Bereits benutzte Nummern können aus Sicherheitsgründen nicht wiederverwendet werden. Ein Betrugsversuch ist denkbar, indem mehrere TAN bei einem Phishingversuch abgefragt und abgespeichert werden. Auch über Man-in-the-Middle-Angriffe lassen sich Datenbanken mit Kunden-TANs aufbauen. Um das weitestgehend zu unterbinden, gibt es die s.g. **indizierten TAN** (iTAN). Hier sind die Listen zusätzlich durchnummeriert, sodass potentielle Täter nur mit einer kompletten TAN-Liste eine Chance zum Betrug bekommen würden. Man-in-the-Middle-Angriffe, bei denen der Täter sich als die Bank ausgibt und nach einer bestimmten TAN fragen kann, sind aber immer noch möglich.

Es sind auch Fälle bekannt, bei denen Kunden über eine Phishingmail dazu aufgefordert wurden, alle nicht verwendeten TAN der Liste einzutragen, da diese nicht mehr sicher sind. Auch wenn es sich dabei um mehrere hundert Stück handeln kann, wurde der Kunde motiviert, indem sein Rechner bis zur vollständigen Angabe der Nummern blockiert wurde. Auch dieser Angriffspunkt kann egalisiert werden, indem die Nummerneingabe nur mit dem Ausfüllen eines zusätzlichen verzerrten Kontrollbildes (Captcha) möglich ist, welches z.B. die Geburtsdaten enthält, die dem Täter unbekannt sind. Dieses Verfahren ist unter dem Namen **iTANplus** bekannt.

Bei der Nutzung **mobiler TAN** (mTAN) bekommt der Kunde die benötigte Transaktionsnummer auf eine vorher festgelegte Mobilfunknummer per SMS zugesandt. Da hier Zusatzinformationen über die Höhe des Betrags, das Empfängerkonto und die Empfängerbankleitzahl mitgesendet werden, ist eine Überlistung des Systems durch Dritte bei aufmerksamen Kunden nur schwer zu ermöglichen, da die Änderung dieser Daten sofort auffallen würde. Trotzdem gibt es viele Fälle, bei denen die Zusatzinformationen aus Zeitgründen übersehen und die falsche Transaktion in die Wege geleitet wurde. Die mTANs sind aufgrund der sehr hohen Anzahl an Mobiltelefonen in Deutschland und Europa ein weit verbreitetes Mittel des Onlinebankingverfahrens. Auch hier wurde bereits gezeigt, dass es Sicherheitslücken gibt. Über Phishing-Seiten wurden beispielsweise die Mobilfunknummern von Kunden ermittelt und SMS mit der Aufforderung zur Installation von Schadsoftware auf dem Handy versandt. Damit konnten viele Mobiltelefone gekapert und später zur Authentifizierung von ungewollten Transaktionen genutzt werden. Aus diesem Grund sollte auch beim Empfang von mTAN mit Vorsicht vorgegangen werden und zur Prävention von Phishing- oder Schadsoftware ein Anti-Viren-Programm auf dem Mobilfunktelefon vorinstalliert sein.

Das mTAN-Verfahren ist auch mit anderen Endgeräten möglich. Das Gerät dient der Einlese von Bankkarten und bekommt die Transaktionsinformationen über einen Strichcode optisch vom PC mitgeteilt. Die erforderliche TAN und die zusätzlichen Informationen zu Geldbetrag und Konto werden auch hier vor der Durchführung zur Überprüfung angezeigt. Die vollständige Trennung eines solchen TAN-Gerätes vom PC stellt eine weitere Verbesserung der Sicherheit dar und nennt sich, je nach Ausführung, **chip-TAN**, **optic-TAN** oder **sm@rt-TAN**. Bisher verzeichnete Betrugsfälle bei diesem Verfahren zielen auf die Leichtgläubigkeit des Kunden ab, der z.B. dazu aufgefordert wird, den TAN-Generator manuell zu manipulieren oder eine nicht stattgefundene Fehlbuchung zurückzahlen soll.

Beim s.g. **photoTAN-**Verfahren wird ein Mobiltelefon des Kunden von der Bank freigeschaltet und ist anschließend dazu in der Lage, bunte kryptografische Abbildungen (siehe Abbildung 5.1), die einem QRCode ähneln, einzulesen. Trotz der hohen Sicherheit dieses Ansatzes findet man ihn heutzutage kaum in Deutschland, was vor allem daran liegt, das es noch keinen ausreichenden Schutz für die Smartphones selbst gibt. Eine unentdeckte Schadsoftware würde an dieser Stelle ein großes Risiko darstellen. Auch der altbekannte QR-Code kann vom Smartphone aus eingelesen werden, um eine Transaktion zu bestätigen. Da es hier die gleichen Angriffspunkte gibt welche eben beschrieben wurden, ist auch die **qrTAN** (Quick-Response-TAN) noch nicht sehr weit verbreitet.

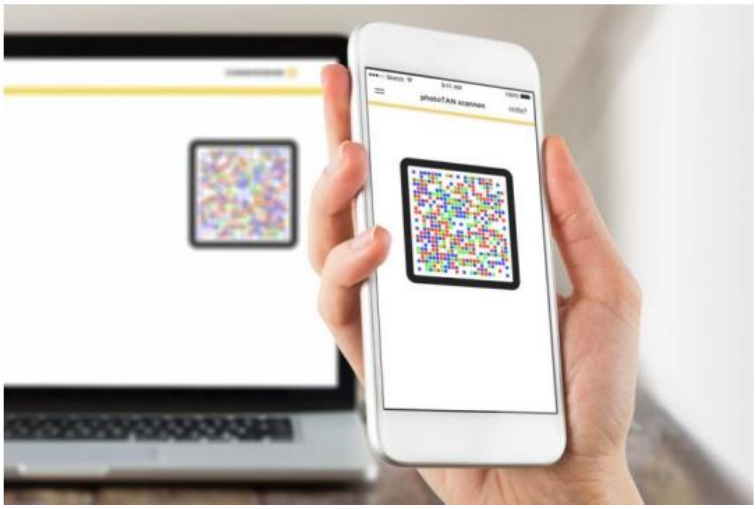


Abbildung 23: Werbeabbildung des photoTAN-Verfahrens einer bekannten Adresse für Onlinebanking. Zu sehen ist die QR-Code-ähnliche bunte kryptografische Abbildung, die vom Smartphone eingescannt und zur Authentifizierung benutzt werden kann.

Die von der Universität Tübingen entwickelte Nahfeldkommunikation für mobile Endgeräte (NFC) lässt sich auch für ein Authentifizierungsverfahren nutzen, welches sich **NFC-TAN** nennt. Dabei erhält der Bankkunde zur Transaktionsbestätigung einen QR-Code, der über eine entsprechende App eingescannt werden kann. Über die NFC-Technologie wird das Smartphone nun zur erneuten Authentifizierung über die Bankkarte gehalten (Karte und Mobiltelefon müssen NFC-fähig sein). Dadurch erhält das Smartphone eine von der Bankkarte errechnete TAN, welche am PC vom Kunden manuell einzugeben ist. Dieser Vorgang gilt als sehr sicher, kann jedoch ebenfalls sicherheitstechnisch untergraben werden, wenn der Kunde seine Aufmerksamkeit verliert und seine angezeigten Transaktionsdaten beispielsweise nicht mehr kontrolliert.

5.5.4.2 FinTS/HBCI

Diese recht kryptische Abkürzung steht für „Financial Transaction Services/Homebanking Computer Interface“ und hat drei Voraussetzungen: Benötigt werden ein internetfähiger PC mit installierter Software der entsprechenden Bank, eine Chipkarte mit enthaltenem Onlinebanking-Schlüssel und einen dafür ausgelegten Kartenleser.

Der Ablauf dieses Verfahrens läuft so ab, dass das Kartenlesegerät zu jeder Transaktionsbestätigung eine digitale Unterschrift von der zugehörigen Chipkarte erhält, auf die von außen nicht zugegriffen werden kann und welche durch mathematische Verschlüsselungsverfahren gebildet wird. Die Unterschrift besteht dabei aus zwei Sequenzen, einem privaten und einem öffentlichen Schlüssel.

Der PIN-vorgesicherte private Schlüssel dient der eigentlichen Authentifizierung, während der Öffentliche an die jeweilige Bank übermittelt wird, um eine Auftragsanfrage zu starten. Aufgrund der sehr kurzen notwendigen Verbindung zum Bankserver und der PC-Tastatur-unabhängigen PIN-Eingabe hat das Verfahren kaum Angriffsstellen für potentielle Täter. Das Kartenlesegerät ist die Hauptkomponente bei diesem System und wird in verschiedenen Klassen der Sicherheit angeboten.

Während die 1. Sicherheitsklasse nur zur Kommunikation mit dem PC fähig ist, gibt es bei der Zweiten bereits eine eigene Eingabetastatur, um mögliche Keylogger fernzuhalten. Die 3. Sicherheitsklasse arbeitet mit einer nicht manipulierbaren Firmensoftware und verfügt über den s.g. SECODER-Standard, was bedeutet, dass auch die Anzeige der Daten im Display nicht manipulierbar ist, solange der Kunde wachsam seine Transaktionsdaten verfolgt. Trotz der hohen Sicherheitsstandards der 3. Klasse findet dieses Authentifizierungsverfahren bisher kaum Anwendung, wodurch es auch kein großes Interesse seitens der Kriminellen gibt.

5.5.4.3 HBCI+

Beim HBCI+ fällt das Kartenlesegerät weg, die Transaktionen werden also lediglich über die PIN und die TAN zugelassen. Aufgrund dieser Tatsache ist dieses Verfahren nicht annähernd so sicher wie das gekoppelte FinTS/HBCI, da es sich nur um eine Art der Authentifizierung handelt und es hier wieder das Gefahrenpotential durch Keylogger oder Man-in-the-middle-Angriffe gibt.

5.5.5 Möglichkeiten der Manipulation und Prävention

Die Sicherheitsmaßnahmen der verschiedenen Verfahren des Internetbanking/Onlinebanking bieten wie der symbolische Tresor immer nur einen begrenzten Schutz vor kriminellen Energien. Dieses Kapitel soll einen Überblick über die bekanntesten Angriffsstrategien geben und gleichzeitig erläutern, welche Gegenmaßnahmen sich bisher etabliert haben.

5.5.5.1 Bekannte Manipulationsmöglichkeiten

Bei allen Arten des Onlinebanking stellt der Kunde für einen kurzen oder längeren Zeitraum eine Verbindung zum Bankserver her, um eine Transaktion durchzuführen. An dieser Stelle gibt es eine recht häufig vorkommende Möglichkeit der Manipulation des Ablaufes. Der Täter verschafft sich dabei Zugriff auf das eventuell unsichere lokale Netzwerk, das von beiden Parteien als Austauschplattform genutzt wird. Damit ist er in der Lage dem Kunden als auch der Bank vorzutäuschen, er wäre der jeweils andere. Er fungiert also, logisch betrachtet, mittig zwischen den beiden Schnittstellen und verändert dort in beide Richtungen die Daten nach seinen Wünschen. Aus diesem Grund wird dieser Vorgang auch **Man-in-the-middle-Angriff** (MITM-Angriff) genannt. Über Botnetze akquirierte Kundenrechner lassen häufig einen solchen Eingriff zu und erlauben die kriminelle Veränderung der Transaktionsdaten während des Austausches über den Bankserver.

Eine Abwandlung dieses Schemas stellt der **Man-in-the-browser-Angriff** dar, bei dem vorher ein Programm zur Manipulation im Browser des Kunden installiert worden sein muss. Diese Software verändert die Transaktionsdaten zwischen Kunde und Bank in Echtzeit, wodurch auch die Kontrolle der angezeigten Zusatzinformationen über Betrag und Konto vom Kunden nicht ausreicht, einen Betrugsversuch festzustellen. Das Fehlen des Geldes kann erst mit einem gedruckten Auszug der Kontodaten nachvollzogen werden, was das Gefahrenpotential steigen lässt.

Eine etwas umfangreichere und schwierigere Art des man-in-the-middleAngriffes ist die komplette Umleitung des Datenverkehrs auf den Täterrechner. Das wird erreicht, indem der Kundenrechner über ein manipuliertes Protokoll (Adress Resolution Protocol - ARP) mitgeteilt bekommt, dass sich die MAC- oder ARP-Adresse des Absenders verändert hat und welche neue Adresse von nun an angewählt werden soll. Nach diesem Eingriff kann die beiderseitige Manipulation der Transaktion wie beschrieben ablaufen, mit der Ausnahme, dass der jeweilige Absenderechner ständig daran gehindert werden muss, ein entsprechendes Verschlüsselungsprotokoll aufzubauen. Diese Art des Vorgehens, welches eine Live-Überwachung des Datenverkehrs benötigt, wird **ARP-Spoofing** genannt.

Die letzte der hier vorgestellten Vorgehensweise setzt eine Manipulation des Domain Name Systems (DNS) voraus, einem Netzwerkdienst welcher dafür verantwortlich ist, einer Domain die jeweilige IP zuzuweisen. Dies funktioniert in der Regel so, dass die vom Kunden eingegebene Bankadresse (URL) in die Bank-IP umgewandelt wird, mit der sich der Kundenrechner dann verbinden kann. Auch wenn solche Abläufe heutzutage meist in Echtzeit ablaufen, gibt es auf älteren aber auch noch auf neueren Betriebssystemen s.g. host-Dateien, die solche IPAdressen von vorigen Aufrufen gespeichert haben. Sollte eine solche host-Datei für die Bank-URL manipuliert worden sein, verbindet sich der Kundenrechner mit der falschen IP, also meist mit der Täterrechner-IP, obwohl die eingegebene URL korrekt geschrieben wurde. Von hier an fungiert der Täter wieder als klassischer man-in-the-middle und verändert die Transaktionen beiderseitig nach seinen Wünschen. Dieser eben beschriebene Eingriff in das Domain Name System nennt man **DNS-Spoofing**.

5.5.5.2 Präventionsmöglichkeiten

Einen vollständigen Schutz beim Onlinebanking kann es nicht geben, die folgend vorgestellten Verhaltensregeln und Maßnahmen sollten bei gewissenhafter und regelmäßiger Ausführung jedoch den Großteil möglicher Angriffe verhindern und außerdem viele Manipulationsversuche gar nicht erst möglich machen.

Wenn auch allgemein bekannt, ist der Besitz eines aktuellen Virenschutzprogramms auf dem benutzten Betriebssystem sehr wichtig, da es die bekannt gewordenen Angriffslücken im System verschließt. Aus diesem Grund sollte es auch regelmäßig aktualisiert werden, um im gegenseitigen Prozess des Wettrüstens zwischen potentiellen Opfern und Tätern im Onlinebanking stets auf dem neuesten Stand zu sein. Die angebotenen Überprüfungen einer solchen Virenschutzsoftware sollten ebenfalls regelmäßig stattfinden. Auch eigene und vor allem fremde Speichermedien lassen sich damit auf versteckte Viren oder andere Schadprogramme überprüfen.

Des Weiteren sind das Einrichten und Einschalten einer Firewall unbedingt notwendig. Sind für einen Computer mehrere Nutzer vorgesehen, bietet es sich an, jedem dieser Nutzer ein eigenes Konto mit eigenem Passwort einzurichten. Die Administratorrechte erhält nur der Besitzer oder eine Vertrauensperson. Eingesetzte Passwörter für die verschiedenen Offline- und Online-Anwendungen sollten sich möglichst nicht gleichen, komplex sein und nicht auf dem Rechner abgespeichert sein. Auch die Aufbewahrung in der Nähe des Rechners kann gefährlich sein.

Beim Aufrufen von Webseiten kann erhöhte Aufmerksamkeit bereits eine Vielzahl an kriminellen Einflüssen verhindern. Ein einfacher Blick auf die tatsächlich angewählte Adresszeile gibt Information darüber, ob es bereits hier Manipulationsversuche gibt. Besonders sicher sind Adressen, bei denen die Daten verschlüsselt übertragen werden. Diese Eigenschaft lässt durch das Kürzel „https“ (Hyper Text Transfer Protocol Secure) und dem zugehörigem Schlosssymbol erkennen (siehe Abbildung 24).

Das Hovern der Maus über dieses Symbol oder ein Linksklick darauf eröffnet weitere Informationen zu Inhaber, Grad der Verschlüsselung und Gültigkeit des zugrunde liegenden Zertifikates.

Eingebettete Links auf allen besuchten Seiten sollten, genauso wie die Werbeeinblendungen, nicht angeklickt oder deren Zielführung zu mindestens wachsam verfolgt werden. Aufforderungen zur Eingabe kritischer Informationen des Kontos für angebliche Verbesserungen der Sicherheit sollten nicht befolgt werden, der Wahrheitsgehalt ihrer Inhalte ist in der zugehörigen Bank abzuklären. Dafür sollte eine offizielle Mailadresse oder Telefonnummer benutzt werden, da bereits diese Daten manipuliert worden sein könnten.

Abbildung 24: Das grüne Schlosssymbol und das Kürzel "https" bedeuten, dass es sich um eine verschlüsselte Verbindung handelt. Nach anklicken des Symbols können weitere relevante Informationen abgerufen werden.

5.6 Cybermobbing, Cyberbullying

5.6.1 Beschreibung des Phänomens

Unter dem Begriff des Mobbings wird im weiteren Sinn das wiederholte bzw. regelmäßige Schikanieren, Quälen und seelische Beeinflussen von Menschen verstanden. Häufig steht damit der Psychoterror am Arbeitsplatz, in der Schule oder auch im Internet in Verbindung, mit dem Ziel den Betroffenen auszusondern und in seiner Würde zu verletzen. Aus dem Begriff des Mobbings hat sich im deutschen Sprachraum das sogenannte Internetmobbing etabliert. Im angelsächsischen Raum hat sich der Terminus Bullying als Synonym manifestiert. Auch in Fachkreisen wird deshalb oft Internet-Bullying gleichbedeutend für den Begriff des Internet-Mobbings verwendet.

Um zu verstehen was das Phänomen des Internet-Bullying umfasst bzw. bewirkt, ist es zunächst wichtig den Begriff Mobbing näher zu beleuchten. Eine geläufige Definition nach Olweus lautet wie folgt: „Ein Schüler oder eine Schülerin ist Gewalt ausgesetzt oder wird gemobbt, wenn er oder sie wiederholt und über einen längere Zeit den negativen Handlungen eines oder mehrerer anderer Schüler oder Schülerinnen aussetzt ist.“ [5].

Laut Definition müssen die vorgenommenen, meist asozialen Handlungen gegenüber dem Betroffenen, wiederholt durchgeführt werden. Einmalige, isolierte Vorgehensweisen gegenüber dem Mitschüler oder Kollegen gelten noch nicht als Mobbingversuch. Nach Olweus Definition wird weiterhin die negativierte Ausübung einer Handlung betont. Darunter zählen sowohl physische Gewalttätigkeiten gegen eine Person als auch psychische Handlungen, wie z. B. übles Nachreden, Beleidigen oder das bewusste Ausschließen einer Person aus der Gemeinschaft.

Unter Berücksichtigung dieser Definition wird deutlich, dass Cyberbullying kein neues Phänomen in der Gesellschaft ist. Vielmehr dient das Mobbing in diesem Zusammenhang als Werkzeug im World Wide Web und ist eine Art der elektronischen Weiterentwicklung des Mobbings von Angesicht zu Angesicht ohne persönlichen Kontakt. Durch schwer kontrollierbare Sanktions- oder Kontrollmechanismen im Netz sinkt zudem auch die Hemmschwelle bei den Beteiligten.

Um sich untereinander über diverse Themen auszutauschen ist es mittlerweile üblich, Mails, Chatforen, Online Communities, oder InstantManager zu nutzen. Damit ist klar, dass diese Medien auch als Plattformen für das Bullying eingesetzt werden, um beleidigende Inhalte oder Gerüchte (z. B. Beleidigungen in sozialen Netzwerken, Präsentation von heimlich aufgezeichneten Videosequenzen mit bloßstellenden Inhalten oder beleidigende SMS o. Anrufe) zu verbreiten. Beck kommentiert dies im Rahmen seines Beitrages im Buck „Online Handbuch“ folgendermaßen: „Zu beobachten sind auch Formen von Cyber-Mobbing und Cyberbullying, also die üble Nachrede und Stigmatisierung, ja Beleidigungen und Bedrohungen von realen Menschen im virtuellen Raum durch verbale oder grafische Darstellungen. Personen werden dann online über längere Zeiträume und zum Teil ohne deren Wissen öffentlich verächtlich gemacht und aus Gruppen (Schule, Arbeitsplatz, Vereine) heraus gedrängt ohne sich dagegen wehren zu können“. [6]

5.6.2 Formen des Cyberbullyings

Im Allgemeinen werden zwei Arten oder Formen des Cyberbullyings unterschieden, das **direkte** und das **indirekte Cyberbullying**. Zur direkten Form zählen das sogenannte Flaming und Stalking. Das Verleumden von Tatsachen, das Annehmen einer falschen Identität (Fake-Account) sowie Betrügereien im Namen des Gemobbten werden im Gesamten zur indirekten Form des Cyberbullyings gezählt. Im Regelfall sind es Beschimpfungen, Beleidigungen, Hänseln, Bedrohungen sowie die Verbreitung von Lügen und Gerüchten. In einer Studie von Schneider et al. werden die Formen des Bullyings und das Ausmaß der bisher bekannten Fälle diskutiert. [7]

Heutzutage ist gerade das Smartphone, neben häuslichen PCs oder Laptops, durch die schnelle Vorort-Verbreitung von Fotos und Videos, das Mittel der Wahl zur Verbreitung entsprechender Mobbing-Attacken. Der Mobber oder fachsprachlich Bully agiert im Gegensatz zum faceto-face Mobbing anonym. Dabei fühlt sich dieser durch den ausbleibenden Augenkontakt mit dem Gegenüber geschützt und muss sich mit möglichen Kommentaren des Opfers nicht auseinandersetzen. Dadurch erfolgt meist eine schnelle Multiplikation der Aggression gegenüber dem Opfer. Auf der Opferseite entsteht hingegen schnell eine große Unsicherheit und Ängste, auch dadurch begründet, dass die Identität des Mobbers unbekannt ist. Im Gegenzug zum direkten Mobbing, bei dem die Identität des einzelnen oder Gruppe meist erkennbar ist, eröffnet das Netz eine unbegrenzte Menge an möglichen Personen, wodurch das Opfer nicht erkennt, wer die Hänseleien oder Beschimpfungen gesehen oder gelesen hat. Dazu kommt, dass sich die Beleidigungen schnell im Netz verteilen und so auch von Personen geteilt werden können, die nicht unmittelbar mit dem Opfer in einer Beziehung stehen. Häufig sind zudem Meldungen noch nach Jahren nachzuverfolgen, da sie einfach kopiert, gespeichert und erneut verbreitet werden können. Dieser Sachverhalt verhindert oftmals, dass Opfer mit den Attacken abschließen können [8].

Aber auch für die Täter stellt die Verbreitung im Netz ein unkalkulierbares Risiko dar, indem die böswillig hochgeladenen Inhalte durch ihn nicht mehr kontrollierbar sind. Es kann nicht beeinflusst werden, wo die Inhalte geteilt werden und wer diese weiter verbreitet. Auch an dieser Stelle ist zu erwähnen, dass die Inhalte über Jahre hinweg beständig sind und dass gerade darüber Rückschlüsse auf den Täter gezogen werden können. Für den Täter nachteilig an dieser Stelle ist, dass Beiträge schwierig aus dem Netz zu entfernen sind, je länger sie darin weilen und je mehr Personen diese Inhalte verbreiten. Im Sinne der Störerhaftung kann er jedoch dazu verpflichtet werden, die strafbaren Inhalte zu löschen.

Der Betroffene sollte wenn möglich die entsprechenden Inhalte, die durch das Cyber-Bullying verbreitet wurden, als Grundlage für eine Strafanzeige, sichern (speichern, Screenshots oder Fotokopien). Weiterhin sollte die jeweilige Internetseite mit Datum und Uhrzeit, auf der die Attacke erfolgte, dokumentiert werden. Dadurch wird die Beweissuche auf elektronischen Geräten des Beschuldigten erleichtert. Der Beschuldigte sollte im besten Fall schriftlich mit einer Fristsetzung aufgefordert werden, die beleidigenden Inhalte zu löschen. Bei unbekannten Personen kann auch der Anbieter der Internetseite dazu aufgefordert werden, die kompromittierenden Inhalte zu entfernen.

Bei Facebook besteht z.B. die Möglichkeit ein Problem zu melden. Als Option erscheint hier „Missbräuchlicher Inhalt“. Hierunter können Fotos, Videos und Beiträge als meldebedürftig ausgewählt werden. Bei Google können ebenfalls entsprechende Inhalte über den Google Support gemeldet werden. Nach dem Aufruf erscheint ein Punkt „Inhalt aus der Google-Suche entfernen“. Damit im Cache der Suchmaschine nicht mehr gesucht wird, müssen zuvor alle entsprechenden Inhalte auf der Seite entfernt und die Seite aktualisiert werden. Auch bei anderen Anbietern existieren Möglichkeiten zum Melden von Inhalten. Neben den Löschmaßnahmen, die durch den Betroffenen selbst durchgeführt werden können, sollte der Sachverhalt durch eine Strafanzeige bei der Polizei gemeldet werden. Bei minderjährigen Personen muss der Strafantrag durch die Erziehungsberechtigten gestellt werden. Das Opfer erhält als Prozessbeteiligter das Recht auf Akteneinsicht durch seinen Rechtsbeistand. Der Zivilklageweg kann ebenfalls beschritten werden [8].

5.6.3 Präventionsmaßnahmen

Es ist wichtig, dass zur Prävention von Cybermobbing die Bezugspersonen von Kindern und Jugendlichen zusammenarbeiten. Hier sind gerade die Eltern und auch Schulen gefragt, die durch Angebote im Lehrbetrieb wirksam dazu beitragen können. Die Angebote sollten sich an den inhaltlichen Grundzügen (Langfristigkeit, Nachhaltigkeit und Zielgruppen) der Präventionsarbeit orientieren. Lehrer und die Schulleitung sollten u.a.: [8]

- sich Wissen über (Cyber-) Mobbing aneignen,
- rechtzeitig einen Interventionskatalog erarbeiten,
- offensiv an das Thema herangehen,
- Mobbing im Unterricht thematisieren,
- sowohl die Vorzüge der medialen Welt als auch auf mögliche Gefahren und Missbrauchsmöglichkeiten hinweisen.

Bei einem Mobbingfall sollten Lehrberechtigte: [8]

- anerkennen, dass Mobbing existiert und darauf reagieren
- mit den Eltern kooperieren
- entsprechende Maßnahmen verhängen
- die Zusammenarbeit mit dem Schulamt und den Präventionsbeamten der Polizei stärken.

Für Schulen stehen verschiedene Programme rund ums Thema und zur Mobbingprävention zur Verfügung: [8]

- PIT - Prävention im Team. PIT ist ein Programm zum sozialen Lernen und zur Kriminalprävention
- Die „Berlin-Brandenburger Mobbingfibel“ beschäftigt sich zum einen theoretisch mit dem Thema Mobbing und zum anderen mit Präventionsmaßnahmen und Hilfsmöglichkeiten im akuten Fall.
- Die EU-Initiative für mehr Sicherheit („klicksafe“) bieten ebenfalls theoretisches Wissen zum Thema Mobbing und Cybermobbing an. Dazu werden entsprechende Materialien, die in den Unterricht eingebunden werden, angeboten.

5.7 Softwarepiraterie

5.7.1 Phänomenbeschreibung

Die Softwarepiraterie ist eine verbreitete Kriminalitätserscheinung und beschreibt die unerlaubte Vervielfältigung und Verbreitung urheberrechtlich geschützter Werke (§ 106 UrhG). Nach der Begehungsweise wird zwischen privater Anwendung und gewerbsmäßigem Handeln (§ 108a UrhG) unterschieden. [9]

Softwarepiraterie kann in die fünf folgenden Haupttypen unterschieden werden:

- Fälschung
- Internetpiraterie
- Softwarepiraterie durch den Endbenutzer
- Übermäßige Client-Servernutzung
- Vorinstallierte Kopien

5.7.2 Strafrechtsnormen

Die Herstellung und Weitergabe von Raubkopien von Computerspielen oder Textverarbeitungsprogrammen erfülle den Tatbestand des § 202a StGB (Ausspähen von Daten) selbst dann nicht, wenn der Kopierschutz umgangen wird, weil der Kopierschutz lediglich einen urheberrechtlichen Zweck erfülle, nicht aber den Zugang zu den Daten ausschließen solle. Dies ist jedoch eine fragwürdige Argumentation, denn der Zugang zu den Daten soll gerade durch den Kopierschutz kontrolliert und gegenüber Unbefugten verwehrt werden.

Die unerlaubte Vervielfältigung und Verbreitung urheberrechtlich geschützter Werke, wozu auch Programme für die Datenverarbeitung gehören (z.B. Herstellung von Raubkopien von Computerprogrammen) ist nach § 106 UrhG (Unerlaubte Verwertung urheberrechtlich geschützter Werke) strafbar.

5.8 Botnetze

Im Bereich Cybercrime spielten sogenannte Botnetze als zentrale Angriffsressource auch 2016 eine bedeutende Rolle. Bei Botnetzen handelt es sich um zahlreiche, per Schadcode infizierte Computer, die ohne Wissen ihrer Besitzer über „Command & Control-Server“ ferngesteuert werden können (Abbildung 25).

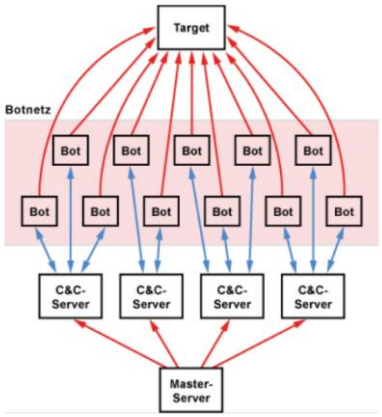


Abbildung 25: Architektur eines Botnetzes

Im Bereich der Underground Economy sind Botnetze und ihre Kapazitäten nach wie vor eine weltweit lukrative Handelsware. Die sogenannten Bot-Herder, die Betreiber der Botnetze, vermieten Bots, durch die beispielsweise mittels DDoS-Attacken gezielte Angriffe auf Unternehmensserver durchgeführt werden, massenweise Spam-Mails versendet werden oder auch gezielte Datendiebstähle erfolgen können. Zur Gesamtzahl der in Deutschland bzw. weltweit in Botnetzen zusammengeschlossenen Rechner können kaum valide Aussagen gemacht werden. Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) und EUROPOL gehen davon aus, dass Deutschland an der Spitze der Statten, die Command & Control-Server hosten, steht. [3]

5.8.1 Wie entstehen Botnetze?

Auf den Opfer-PCs kann die Installation von Schadsoftware für die Besitzer unbemerkt auf verschiedene Art und Weisen erfolgen. Als Beispiele können hier das Öffnen von infizierten E-Mail-Anhängen oder auch „Drive-by-Downloads“ genannt werden. Die Verteilung der Schadsoftware ist aber auch über soziale Netzwerke (z.B. Facebook) möglich. Den Teilnehmern der Netzwerke werden von vermeintlichen Bekannten oder Freunden Nachrichten mit infizierten Anhängen zugesandt. Zur Infektion des Computers kommt es, wenn Anhänge geöffnet oder eingefügte Links angeklickt werden. Durch die zuvor installierte Schadsoftware hat der Täter einen nahezu vollständigen Zugriff auf den infizierten Computer des Opfers. Weitere Verbreitungskanäle sind das Usenet und Tauschbörsen/P2P (Peer to Peer)-Netze, in denen die Schadsoftware meist als Video- oder Sounddatei getarnt zum Download angeboten. [3]

5.8.2 Strafrechtsnormen

Der Tatbestand der Datenveränderung nach § 303a Abs. 1 StGB ist zu prüfen, wenn unbemerkt ein Schadprogramm auf einem fremden Rechner installiert wurde. Das Programm greift auf Systemdateien zu und verändert diese. Der Gesetzgeber fordert keine Funktionsstörung. Auch nicht, dass der User die Datenveränderung sofort bemerkt. Werden mit den zusammengeschlossenen Rechnern auf Befehl des „BotnetMasters“ DDoS-Attacken ausgeführt und der angegriffene Rechner, Server oder sonstiger Teil eines Datennetzes wird in seiner Funktion beeinträchtigt (Systemabsturz) oder muss sogar vom Netz genommen werden, ist zusätzlich § 303b Abs. 1 StGB zu prüfen. Erfolgt die Generierung des Virus, der Kauf, das sich oder einem anderen Verschaffen, das Überlassen, die Verbreitung oder das Sonstzugänglich-machen, um damit mehrere Rechner zu infizieren und diese zu einem Botnetz zusammenzustellen, ist dieser Versuch gemäß § 303b Abs. 5 StGB i.V.m. § 202c Abs. 1 Nr. 2 StGB strafbar.

Wird beispielsweise einem Unternehmen mit einer DDos-Attacke gedroht, die es durch Zahlung einer Geldleistung abwenden kann, ist die Erpressung gemäß § 253 StGB zu prüfen. Das Unheil, mit dem gedroht wird, ist die Schaffung der Funktionsuntüchtigkeit des Hosts, von Rechnern oder Netzwerkkomponenten, in deren Folge das Unternehmen seinem Geschäftszweck nicht mehr oder nicht mehr vollständig nachkommen kann. Wird eine solche Attacke bei ausbleibender Zahlung oder auch trotz Zahlung durchgeführt, kommt noch § 317 StGB (Störung einer Telekommunikationsanlage) zur Prüfung. [10]

5.8.3 Fallbeispiel

Durch eine zeitgleich erfolgte Beschlagnahme von 39 Servern und mehreren Hunderttausend Domains Anfang Dezember 2016 konnte die wohl weltweit größte Infrastruktur zum Betrieb sogenannter Botnetze aufgedeckt und analysiert werden. Allein in Deutschland ist Cyberkriminellen dadurch die Kontrolle über mehr als 50.000 infizierte Computer entzogen worden.

Die weltweit vernetzte Botnetz-Infrastruktur „Avalanche“ haben Täter mindestens seit 2009 für das Versenden von E-Mails mit schadhaftem Code genutzt. Opfer wurden in 180 Statten festgestellt. Bei „Avalanche“ handelte es sich nach bisheriger Einschätzung um die weltweit größte Infrastruktur zum Betrieb eines Botnetzes.

16 Beschuldigte konnten allein auf der Führungsebene dieser kriminellen Vereinigung identifiziert werden. Gegen sieben Tatverdächtige in Deutschland wurden Haftbefehle wegen des Verdachts der Bildung einer kriminellen Vereinigung, des banden- und gewerbsmäßigen Computerbetrugs und anderer Straftaten erlassen.

Dieser Fall verdeutlicht die Erforderlichkeit von internationalen Kooperationen im Phänomenbereich Cybercrime, um derartige Infrastrukturen erfolgreich bekämpfen zu können. [3]

5.8.4 Präventionsmöglichkeiten

Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) stellt fest, dass insbesondere private PC-Nutzer oftmals nicht ausreichend gegen Risiken geschützt sind. Mindestens fünf vom BSI genannte Schutzmaßnahmen sollten umgesetzt sein:

- regelmäßige Installation von den Herstellern bereitgestellten Sicherheitsupdates
- Installation und Nutzung eines aktuellen Virenscanners
- Verwendung einer Personal-Firewall
- Anlage von Benutzerkonten mit eingeschränkten (keinen Administratorrechten) für jeden einzelnen Nutzer
- zurückhaltende Weitergabe persönlicher Daten und ein gesundes Misstrauen gegenüber Datenabfragen, angebotenen Links oder zweifelhaften Inhalten

Zusätzlich kann der heimische PC auf Befall mit Bots überprüft werden und gefundene Programme können von der Festplatte gelöscht werden. [10]

5.9 DDos-Attacken

In der heutigen Zeit zählen DDoS-Attacken zu den häufigsten Cyberattacken. Vor allem in der Industrie und dem Finanzwesen werden diese mächtigen Attacken eingesetzt, um Unternehmen unter Druck zu setzen und hohe Summen als Schutzgeld einzufordern. Auch im Bereich der Cyberspionage gehören DDoS-Angriffe zum Standardrepertoire. Die folgende Pressemeldung soll die Mächtigkeit solcher Attacken verdeutlichen (Abbildung 26).

DDoS-Attacke legt Twitter, Netflix, Paypal, Spotify und andere Dienste lahm

heise online 21.10.2016 22:13 Uhr – Holger Bleich vorlesen

Wegen einer massiven DDoS-Attacke sind die Services großer US-Internetdienste, darunter unter anderem Twitter, Paypal, Netflix und Spotify, am Freitagabend in Teilen der USA und Europas zeitweise nicht zu erreichen.

Abbildung 26: Pressemeldung zu einer DDos-Attacke

Der Security-Journalist und -Blogger Brian Krebs: „[...], dass Hacker ein riesiges Botnet aus Smart Devices aufgebaut haben könnten. Er spricht davon, dass schlecht abgesicherte Geräte, etwa Überwachungskameras, digitale Videorecorder und private Router infiltriert worden sein könnten [...]“

Der Angriff soll über ein Botnetz aus mehr als einer Million Geräten im Internet der Dinge erfolgt sein. Das Botnetz soll später auch für eine rekordverdächtige DDoS-Attacke mit 1,1 Terabit pro Sekunde auf einen französischen Hoster genutzt worden sein.

Ein DDoS-Angriff ist eine spezielle Art der Cyber-Kriminalität. Der Distributed-Denial-of-Service (DDoS) ist ein „verteilter“ Denial-of-Service (DoS), der wiederum eine Dienstblockade darstellt. Diese liegt vor, wenn ein angefragter Dienst nicht mehr bzw. nur noch stark eingeschränkt verfügbar ist. Auslöser ist in den meisten Fällen eine Überlastung der IT-Infrastruktur. Angreifer nutzen diese Art der Cyber-Kriminalität, um von ungeschützten Unternehmen Lösegelder zu erpressen.

Bei einem DDoS-Angriff führen Angreifer die Nichtverfügbarkeit eines Dienstes oder Servers gezielt herbei. Dafür infizieren sie einen oder mehrere Rechner mit Schadsoftware. Die Angreifer missbrauchen dieses infizierte Rechner-Netz, auch Botnetz genannt, ferngesteuert für ihre DDoS-Attacken. Mit dem Botnetz greifen sie parallel ihr Ziel an und beschießen dabei dessen Infrastruktur mit zahllosen Anfragen. Je mehr Rechner zusammengeschaltet werden, desto schlagkräftiger ist die Attacke. Angegriffene Server ohne DDoS-Schutz sind mit den unzähligen Anfragen überfordert, ihre Internetleitung ist überlastet. Websites bauen sich nur noch stark verlangsamt auf oder sind überhaupt nicht mehr verfügbar. Einzelne Kriminelle oder Gruppierungen, politische Aktivisten, Wettbewerber, enttäuschte Kunden – die Liste der Angreifer ist lang. Ihre Motive für einen DDoS-Angriff sind ebenfalls vielfältig: Erpressung, Konkurrenz schädigen, Neid oder Signale gegen politische

Entscheidungen setzen. Das Ziel von Angreifern ist jedoch immer dasselbe: Der dahinterstehenden Organisation soll ein möglichst großer Schaden zugesetzt werden.

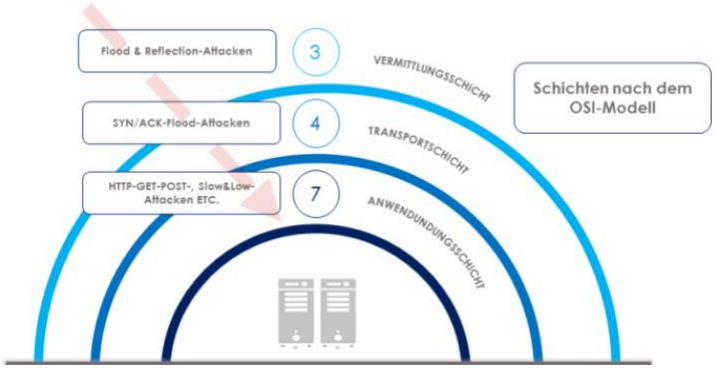


Abbildung 27: DDoS-Attacke nach OSI-Schichten

Cyber-Kriminelle nutzen unterschiedliche Arten von DDoS-Angriffen. Die Methoden lassen sich nach den jeweiligen Schichten ordnen, auf die der Angriff abzielt (Abbildung 27). Eine der häufigsten Methoden ist, Systemressourcen oder Netzwerkbandbreiten zu überlasten (Layer 3 und 4). Als Trend zeichnet sich unter den Cyber-Kriminellen in den letzten Jahren ab, die Angriffe auf die Anwendungsebene (Layer 7) zu verlagern. Muster und Bandbreiten von DDoS-Attacken ändern sich jedoch täglich. Mit dem DDoS-Schutz von Myra sind Sie vor jeglichen Angriffsmustern geschützt.

Im OSI-Schichten-Modell wird beschrieben, welche Voraussetzungen gegeben sein müssen, damit verschiedene Netzwerkkomponenten miteinander kommunizieren können. OSI steht für „Open System Interconnection“ und heißt übersetzt „Offenes System für Kommunikationsverbindungen“. Die Kommunikation geschieht folgendermaßen: Sender und Empfänger senden bzw. erhalten Informationen in einer Anwendung, wie z. B. in ihrem E-Mail-Programm. Diese Information läuft dann von der Anwendung zur Netzwerkkarte, verlässt den Rechner über ein Übertragungsmedium (Kabel oder Funk), läuft darüber vielleicht noch über andere Netzwerkkomponenten, wie beispielsweise einen Hub und erreicht dann über die Netzwerkkarte des Zielrechners die Anwendung des Empfängers. Alle Schritte, die vom Sender bis zum Empfänger gemacht werden müssen, werden während der Übertragung in einem Protokoll festgehalten, damit jede einzelne Station auf diesem Weg weiß, wohin das Paket möchte, woher es kommt und welche Eigenschaften es hat. Damit dieser Weg funktioniert, muss dieser eindeutig festgelegt werden und alle Geräte und jede Software, die in diesem Prozess involviert sind, müssen den Ablauf kennen und dieselbe Sprache sprechen. Diese Normen legt das OSI-Schichten-Modell fest. 1983 wurde dieses Modell von der Internationalen Organisation für Normung (ISO) standardisiert.

Das OSI-Schichten-Modell sorgt durch diesen Standard dafür, dass in einem Netzwerk Komponenten und Software verschiedener Hersteller miteinander arbeiten können.

Da das Thema der Datenkommunikation sehr komplex ist, wurde das OSI-Schichten-Modell in sieben Schichten unterteilt. Die Schichten 1 bis 4 gehören zum Transportsystem. Die Schichten 5-7 sind anwendungsorientierte Schichten. Jede Schicht behandelt eine Anforderung, die für eine funktionierende Kommunikation erfüllt werden muss. Ein vom Sender kommendes, zu übertragendes Datenpaket durchläuft die Schichten 7 bis 1. Jede Schicht fügt dem Datenpaket-Protokoll Information zu, die dann im Protokoll des Datenpaketes stehen. Die Schicht 1 wandelt das

Datenpaket inklusive aller Protokoll-Informationen dann schließlich in technisch übertragbare Daten um und schickt es über das Übertragungsmedium (Kabel oder Funk) weg. Auf der Empfängerseite durchläuft das Datenpaket dann die Schichten in umgekehrter Reihenfolge, nämlich von Schicht 1 bis Schicht 7. Hier werden die Protokoll-Informationen wiederum Schicht für Schicht entfernt, nachdem sie von den einzelnen Schichten interpretiert worden sind.

Ein Angriff schadet betroffenen Unternehmen immer, unabhängig von der gewählten Methode. An den Folgen leiden Unternehmen noch Jahre später. Ein effizienter DDoS-Schutz ist deshalb zentral.

5.10 Tauschbörsen („filesharing“)

5.10.1 Phänomenbeschreibung

Der Begriff filesharing beschreibt das Teilen von Dateien. Treffender formuliert steht es für den gemeinsamen Datenzugriff und bezeichnet die direkte Weitergabe von Dateien unter Nutzern des Internets. In einem Peer-to-Peer-Netzwerk werden Dateien, üblicherweise Musikdateien, aber auch Filme, Textdateien oder Computerprogramme, von einem Nutzer hochgeladen (ins Netz gestellt) und von anderen Nutzern aus dem Netz bezogen (heruntergeladen). Die Daten können entweder auf einer heimischen Festplatte liegen oder auf einem Server gespeichert sein. Mit Hilfe von speziellen Programmen, Browsern oder erweiterten Browsern (Add-on) können die Nutzer auf die Speichermedien zugreifen. „filesharing“ wird sowohl im legalen als auch im illegalen Bereich betrieben.

Im legalen Bereich bieten vor allem noch unbekannte Künstler ihrer Musik an, um ihren Bekanntheitsgrad zu erhöhen oder sich Geld für Server-Kapazitäten zu sparen. Es finden sich aber auch bekanntere Musiker, die ihre Titel per filesharing freigeben, um für eine neue CD Werbung zu machen. Datenangebote, die in einer freien Lizenz veröffentlicht werden, sind ebenfalls legal, wenn es sich um sogenannte Shareware handelt, also freie Software. Das Anbieten von urheberrechtlich geschützten Musiktiteln stellt jedoch einen Verstoß gegen das Urheberrechtsgesetz (UrhG) dar. [10]

5.10.2 Strafrechtsnormen

Das Bereitstellen von Musikdateien in Tauschbörsen bzw. das zur Verfügung stellen auf der eigenen Festplatte zum Herunterladen über Peerto-Peer-Netzwerke stellt einen unerlaubten Eingriff in verwandte Schutzrechte nach §§ 108 Abs. 1 Nr. 4 und 5, 77, 78 Nr. 1, 85, 16, 19a, 109 UrhG i.V.m. § 52 StGB dar. Die Strafbarkeit liegt in der nicht vorhandenen Einwilligung der Rechteinhaber (Komponisten, Textdichter usw.) begründet.

Wenn das Herunterladen von Musikdateien weder unmittelbaren noch mittelbaren Erwerbszwecken dient und soweit zur Vervielfältigung keine offensichtlich rechtswidrig hergestellte oder öffentlich zugänglich gemachte Vorlage verwendet wird, dann ist es zulässig.

Bestimmte Nutzungshandlungen sind durch das Urheberrecht ausdrücklich gestattet. So ist das Kopieren von nicht rechtswidrig hergestellten oder öffentlich zugänglich gemachten Vorlagen zum privaten Gebrauch (Privatkopie) eine Schranke, welche die Recht der Urheber einschränkt. Dieser Kopierzweck ist ausdrücklich erlaubt. Durch diese Privilegierung nicht gedeckt ist jedoch das Bereitstellen von Musiktiteln und Filmen auf Tauschbörsen. Das heißt, es dürfen weder Musikstücke noch Filme aus dem Netz geladen werden, die für jedermann erkennbar rechtswidrig online gestellt wurden. Werden Lieder oder Filme dennoch geladen, stellt dies einen Verstoß nach §§ 53 Abs. 1, 106

Abs. 1 UrhG dar. Nach Abs. 2 ist der Versuch strafbar. Zur Verfolgung der Tat ist ein Strafantrag notwendig (§ 109 UrhG).

Zur Erstellung von Privatkopien (CDs/DVDs) darf der sogenannte Kopierschutz nicht umgangen werden. Wird ein Werk dennoch kopiert, und der Kopierschutz damit „geknackt“ , so stellt dies einen Verstoß nach § 108 Abs. 1 Nr. 1 UrhG (Unerlaubte Eingriffe in technische Schutzmaßnahmen und zur Rechtewahrnehmung erforderliche Informationen) dar.

Die Gegenstände, die zum Kopieren der geschützten Werke gebraucht wurden (PC, Notebook), können als Nebenfolge der Tat eingezogen werden. Die Einziehung ist im Urheberrecht explizit geregelt (§§ 110, 106 UrhG i.V.m. § 74 StGB). Außerdem sind verschiedene andere bürgerlich rechtliche Vorschriften, wie zum Beispiel der Anspruch auf Unterlassung und Schadenersatz (§ 97 UrhG), die Abmahnung im Vorfeld einer gerichtlichen Auseinandersetzung (§ 97a UrhG) sowie der Anspruch auf Vernichtung, Rückruf und Überlassung (§ 98 UrhG) geregelt. [10]

5.10.3 Präventionsmöglichkeiten

Das Bewusstsein der Illegalität ihres Tuns ist bei Computernutzern, die dazu tendieren, Musiktitel und Videodateien auf Tauschbörsen anzubieten bzw. ihr Repertoire dort herunterladen, zu wecken. Auch die Tatsache, dass viele Menschen diese (illegalen) Ressourcen nutzen, ändert nichts am Straftatbestand. Es sind legale Möglichkeiten (musikload, iTunes, Deezer, Spotify oder amazon mp3) anzubieten und zu kommunizieren.

5.11 Benutzung fremder offener WLAN-Netze (vs. Wardriving)

5.11.1 Phänomenbeschreibung

Die Nutzung fremder offener WLAN-Netze (Wireless Local Area Network) wird umgangssprachlich als „Schwarzsurfen“ bezeichnet. Mit einem netzwerkfähigen Laptop, Tablet oder Smartphone werden Wohn- bzw. Industriegebiete vor allem nachts nach unverschlüsselten (offenen) WLAN-Netzen durchforstet. Die in der Netzwerkkarte integrierte Antenne sollte eine möglichst große Reichweite haben. Die sogenannten „Schwarzsurfer“ nutzen die Unwissenheit oder Bequemlichkeit der Netzwerkbetreiber aus. Aufgrund der benutzerfreundlichen Konfiguration der Hardware (Router oder Access-Point) verbindet sich diese nach der Installation im Netzwerk in der Regel selbständig mit dem Internet. Hat der Hersteller der Hardware kein Passwort vergeben, wird häufig auch keines eingerichtet. Für die Verschlüsselung gilt dasselbe. Somit wurde ein offenes Netzwerk eingerichtet, welches auch von unbefugten Personen genutzt werden kann, um Daten zu laden.

Das sogenannte „Wardriving“ wird mit der Tätigkeit des Schwarzsurfens vermischt. Abgeleitet wird der Begriff vom „Wardailing“, bei dem verschiedene Telefonnummernkombinationen zum Auffinden offener Modemzugänge ausprobiert werden.

Echte Wardriver beschränken sich auf das Auffinden und Katalogisieren offener Funknetze, um auf Sicherheitslücken aufmerksam zu machen, diese dem Betreiber zu melden, um die Anzahl unverschlüsselter Netzwerke zu reduzieren. Allerdings herrscht auch eine Grauzone zwischen Schwarzsurfen und Wardriving. Durch die Kennzeichnung aufgefundener WLAN-Netze durch Zeichen („Warchalking“), die den sogenannten „Gaunerzinken“ ähneln, eröffnen die „wahren“ Wardriver Möglichkeiten für andere, offene Zugänge nicht nur zum einfachen Surfen zu nutzen, sondern auch für Angriffe auf das Netz oder auf die verbundenen Rechner, um Daten auszulesen.

5.11.2 Strafrechtsnormen

Das Schwarzsurfen stellt nach einem Beschluss des Landgerichts Wuppertal vom 19.10.2010 keinen Tatbestand dar. Da keine Kommunikation zwischen zwei Kommunikationspartnern stattfand, sah das Gericht keinen Verstoß nach §§ 89, 148 Abs. 1 Nr. 1 TKG. Außerdem stelle die dem Schwarzsurfer zugeteilte IP-Adresse keine Nachricht im Sinne des TKG dar. Die Betreiber werden von den Richtern mit in die Pflicht genommen, denn durch entsprechende Einstellung des Routers wäre ein unbefugtes Einwählen fremder PCs zu verhindern.

Das Gericht sieht ebenfalls keine Strafbarkeit nach §§ 43 Abs. 2 Nr. 3, 44 BDSG, da durch das Nutzen eines fremden WLAN-Netzwerks keine personenbezogenen Daten abgerufen würden. Die vom Router ausgegebene IP-Adresse stelle kein personenbezogenes Datum dar.

Auch ein Verstoß gegen § 202a StGB (Ausspähen von Daten) liege nicht vor, da das Netzwerk nicht gegen unberechtigten Zugang geschützt gewesen sei. Da die Datenübermittlung nicht nur für einen bestimmten Nutzerkreis bestimmt gewesen sei und der Angeschuldigte den Kommunikationsprozess selbst angestoßen habe, scheidet eine Strafbarkeit nach § 202b (Abfangen von Daten) ebenfalls aus.

Es liege auch keine Täuschungshandlung vor, sodass der Tatbestand des Computerbetrugs nach § 263a StGB ebenfalls nicht vorliegt. Den Richtern fehlte es am Täuschungswert beim Einwählen des PC des Angeschuldigten in den Router, da durch die nicht vorhandene Verschlüsselung keine Prüfung der Berechtigung stattgefunden habe.

5.11.3 Präventionsmöglichkeiten

Ähnlich wie bei Tauschbörsen gilt es auch bei Schwarzsurfern die nicht sozialadäquate Handlung zu thematisieren und den moralischen Unrechtsgehalt des Tuns herauszustellen. Die Einsicht des Nutzers fremder ungesicherter Funknetzwerke für sein Unrecht tun muss ausgelöst werden. Auch wenn die Hardware nicht entsprechend abgesichert wurde, darf dies nicht als Aufforderung verstanden werden, das ungeschützte Netzwerk für fremde Zwecke zu nutzen. [10]

6 Verhaltensempfehlungen bei Betroffenheit von Cybercrime-Delikten – Aus Sicht des Unternehmens

Die nachfolgenden Informationen sollen Ihnen Ratschläge und Tipps an die Hand geben, wie Sie sich zunächst im Vorfeld von Cyberangriffen auf solche Szenarien vorbereiten bzw. nach einem eingetretenen Schadensfall verhalten sollten.

6.1 Firmenleitung/Geschäftsführung

6.1.1 Vor Eintritt eines Schadensfalls

Sie sollten in Ihrem Unternehmen bzw. in Ihrem Verantwortungsbereich bereits Verfahrensweisen oder Anleitungen zum Umgang mit Vorfällen bzw. Straftaten aus dem Bereich Cybercrime vorbereitet haben. Insbesondere sollten die Compliance- und Datenschutzbeauftragten in die Planungen eingebunden werden. Die Verfahrensweisen oder Anleitungen sind regelmäßig zu überprüfen und allen Mitarbeitern zugänglich zu machen, die Verantwortung für die Systemsicherheit haben. Die Verfahren sollten konkrete Anweisungen insbesondere zu folgenden Punkten enthalten:

1. Wer hat im Unternehmen welche Verantwortung für die interne Reaktion auf einen Schadensfall?
2. Wer ist die Ansprechstelle für interne und externe Kontakte?
3. Wer sollte innerhalb und außerhalb der Firma unmittelbar verständigt werden?
4. An welchem Punkt sollten die Strafverfolgungsbehörden informiert werden?

Hilfreich ist es auch, firmenintern bereits im Vorfeld festzustellen und erforderlichenfalls festzulegen, welche Protokolle bzw. Logdaten ggf. routinemäßig vom System wie lange erfasst und gespeichert werden und somit im Bedarfsfall als Beweismittel zur Verfügung stehen.

6.1.2 Bei Eintritt eines Schadensfalls

Eventuelle Benachrichtigung von weiteren Geschädigten oder Verkäufern. Wenn Sie von einer bestehenden Schwachstelle in einem Produkt bzw. in einem System erfahren, die gerade ausgenutzt wird, sollten sie potentiell Betroffene (z. B. Hersteller/Entwickler, andere Nutzer o. ä.) informieren oder dafür sorgen, dass diese gewarnt werden. Diese sind darüber hinaus vielleicht in der Lage, Informationen über den Zwischenfall bereitzustellen, von denen Sie selbst keine Kenntnis hatten (z. B. verborgene Codes, laufende Ermittlungen in anderen Bereichen). Somit lassen sich damit vielleicht weitere Schäden an anderen Systemen verhindern.

Benachrichtigung von Betroffenen und der zuständigen Aufsichtsbehörde

Wenn von Ihren Systemen bestimmte personenbezogene Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und dadurch schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdige Interessen der Betroffenen drohen, sind Sie gemäß § 42a Bundesdatenschutzgesetz (BDSG) verpflichtet, dieses der zuständigen Aufsichtsbehörde (Siehe hierzu § 38 Ziffer 6 BDSG. In der Regel handelt es sich dabei um die Datenschutzbeauftragten in den einzelnen Bundesländern.) sowie den Betroffenen mitzuteilen. Die Benachrichtigung der Betroffenen muss unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen wurden und die Strafverfolgung nicht mehr gefährdet wird.

Melden von Straftaten an Strafverfolgungsbehörden

Wenn Sie im Zusammenhang mit einem Vorfall den Verdacht haben, dass dieser eine Straftat darstellen könnte, sollten Sie sich an die dafür festgelegte bzw. vorgeschriebene Vorgehensweise in Ihrer Firma halten und unverzüglich die zuständige Strafverfolgungsbehörde informieren. Folgende Umstände können auf das Vorliegen eines strafrechtlich relevanten Sachverhalts hinweisen:

- Ein unberechtigter Nutzer hat sich in das System eingeloggt bzw. nutzt das System.
- Es laufen ungewöhnliche Prozesse auf dem System, die große Mengen an Systemressourcen in Anspruch nehmen.
- Das System ist von einem Schadprogramm (z. B. Virus, Wurm, Trojaner) befallen.
- Ein Nutzer versucht von außerhalb, z. B. durch intensives Portscanning, in das System einzudringen.
- Innerhalb kurzer Zeit erreicht eine große Menge an Datenpaketen (von einem oder verschiedenen Absendern) das System.

6.2 Systemadministratoren

Erste Feststellung und Beurteilung des Zwischenfalls

Zunächst sollte festgestellt werden, wie viele und welche Systeme auf welche Weise betroffen sind. Gute Indikatoren sind Nachweise, dass auf Dateien oder Protokolle zugegriffen wurde, dass Dateien oder Protokolle erstellt, verändert, gelöscht oder kopiert wurden oder dass Nutzerkonten bzw. Nutzerrechte hinzugefügt oder verändert wurden. Unter Verwendung der Protokollinformationen können nach Möglichkeit

- der unmittelbare Ausgangspunkt des Angriffs,
- die Kennung der Server, zu denen eigene Daten ggf. übertragen wurden und
- die Identität weiterer Geschädigter bestimmt werden.

Sie sollten daran denken, dass ein Eindringling möglicherweise mehrere Programme oder Daten auf dem System installiert hat. Das System kann mit Schadsoftware verseucht sein, dass es schwierig ist, bestimmte Datei- oder Konfigurationsänderungen zu erkennen.

Es sollte nach Möglichkeit darauf geachtet werden, dass die getroffenen Maßnahmen keine Veränderungen am Systembetrieb oder den gespeicherten Daten herbeiführen, durch die der Angreifer feststellen kann, dass er entdeckt wurde. Durch das Einspielen von Sicherungskopien können zudem Spuren vernichtet werden und es besteht keine Gewähr, dass nicht auch schon die Sicherungskopien durch Schadsoftware kompromittiert wurden.

6.2.1 Maßnahmen zur Minimierung anhaltender Schäden

Zur Unterbindung anhaltender Schädigungen durch einen aktuellen Angriff auf das Netzwerk sollten beispielsweise Filter zur Abwehr von Denial-of-Service-Angriffen installiert oder die betroffenen Systeme vollständig oder teilweise vom Rest des Netzwerkes isoliert werden. Im Fall eines unberechtigten Zugriffs sollte entweder der weitere illegale Zugriff blockiert oder die illegale Handlung beobachtet werden, um die Quelle des Angriffs und/oder das Ausmaß des Schadens festzustellen. Bei der Abwägung der Handlungsoptionen sollte bedacht werden, dass der Angreifer bemerken könnte, dass er entdeckt wurde. Er könnte seine Spuren auf den Systemen löschen oder

möglicherweise auch aus Vergeltung gezielte Angriffe starten, um seinen Zugang zu schützen oder Sie später mit erlangten Firmendaten zu erpressen. Beraten Sie sich daher frühzeitig mit den Entscheidungsträgern in Ihrem Unternehmen, um zu entscheiden, ob ein Abkoppeln des Netzes geschäftlich und rechtlich durchführbar und zweckmäßig ist.

Sie sollten ausführliche Nachweise über die Kosten führen, die der eigenen Firma durch die Maßnahmen zur Begrenzung der Schäden aus dem Angriff entstehen, sowie Nachweise über die konkreten Aktivitäten zur Abmilderung des Angriffs. Diese Informationen können im Hinblick auf die Erlangung von Schadenersatz und für spätere strafrechtliche Ermittlungen von Bedeutung sein.

6.2.2 Verzicht auf ein Eindringen in den Quellcomputer bzw. eine Beschädigung des Quellcomputers

Eigene offensive Gegenmaßnahmen, wie z. B. das Zugangverschaffen zum Computer eines Angreifers können – unabhängig vom Motiv – rechtlich unzulässig sein. Da Angriffe häufig auch von kompromittierten Systemen unwissender Dritter ausgehen, kann durch das „Zurückhacken“ somit eventuell das System eines an der Tat letztlich Unschuldigen beschädigt werden.

Wenn erkennbar ist, dass Angriffe aus dem Bereich anderer (als seriös einzuschätzender) Firmen oder Institutionen erfolgen, sollten Sie versuchen, mit den dortigen Verantwortlichen Kontakt aufzunehmen und um Hilfe bei der Abwehr des Angriffs bzw. bei der Feststellung der ursprünglichen Quelle des Angriffs bitten.

6.2.3 Aufzeichnen und Sammeln von Informationen

Erstellen Sie zunächst eine identische Kopie des betroffenen Systems für eine spätere Analyse und als Nachweis für das durch einen Angriff geschädigte System, insbesondere auch zur Aufstellung der entstandenen Schäden und der Kosten für deren Beseitigung. Solche Kopien können bei der Identifizierung von ausgenutzten Schwachstellen, gelöschten Daten und installierten Schadprogrammen sowie zur Unterstützung der Rückverfolgung des Angreifers hilfreich sein. Der Vorteil dieser bitgenauen Sicherungskopien liegt darin, dass sie auch verborgene Dateien und Verzeichnisse, Austauschdaten, gelöschte Daten und Informationen im Speicher umfassen, die Hinweise für die Ermittlung des Angreifers geben können. Wenn zu diesem Zeitpunkt bereits der Verdacht auf strafbare Handlungen vorliegt, sollten Sie schon jetzt die Strafverfolgungsorgane informieren, damit diese die Möglichkeit haben, auch Kopien zu forensischen Zwecken anzufertigen (siehe Nr. 4). Bei Eintritt eines Schadensfalls sollten darüber hinaus Maßnahmen zur Beschreibung und Feststellung aller Ereignisse (Ereignisprotokoll) im Zusammenhang mit dem Schadensfall ergriffen werden. Sie sollten u. a. Folgendes festhalten bzw. veranlassen:

- Sicherung aller relevanten, bereits bestehenden Protokolle bzw. Logdaten.
- Zeitpunkte, d. h. Daten und Uhrzeiten (einschließlich Zeitzone), an denen relevante Ereignisse entdeckt wurden bzw. stattfanden.
- Angaben (Namen, Daten, Uhrzeiten) zu relevanten Telefonanrufen, E-Mails und anderen Verbindungen.
- Identität der Personen, die Aufgaben im Zusammenhang mit dem Schadensfall bearbeiten, eine Beschreibung dieser Aufgaben und der Zeitaufwand.
- Kennung der von dem Angriff betroffenen Systeme, Konten, Dienste, Daten und Netze sowie die Art der Beeinträchtigung.
- Angaben zu Umfang und Art des entstandenen Schadens.

Diesen Nachweisen sollten Kopien aller Systemprotokolldateien und verdächtiger Dateien beigefügt werden. Denken Sie daran, dass Protokolle an verschiedenen Orten abgespeichert sein können (z. B. lokal oder auf zentralen Servern). Die Uhrzeit- und Datumsangaben in den Protokollen sind sehr wichtig, um einen Angreifer zurückzuverfolgen und ihn zu überführen. Daher sollte darauf geachtet werden, dass diese Angaben in den Protokolleinträgen korrekt und mit den jeweiligen Zeitzonen enthalten sind.

6.2.4 Hinweise zum Informationsaustausch

Infizierte Systeme sollten grundsätzlich nicht dazu verwendet werden, um sich über einen Angriff oder die Reaktion darüber auszutauschen. Falls das kompromittierte System (mangels Alternativen) doch für einen Informationsaustausch verwendet werden muss, sollten zumindest alle relevanten Mitteilungen verschlüsselt werden.

Die zuständigen Personen in Ihrer Firma sollten unverzüglich über den Angriff und alle Ergebnisse der bisherigen Analyse informiert werden. Hierzu zählen z.B. Sicherheitskoordinatoren, Manager oder Rechtsberater. Bei Verbindungsaufnahme wird empfohlen, nur geschützte bzw. zuverlässige Kommunikationskanäle zu benutzen. Sollte der Verdacht bestehen, dass der Angreifer ein Insider ist oder eventuell über Insider-Informationen verfügt, können Sie Informationen über den Zwischenfall streng nach dem Grundsatz „Kenntnis nur, wenn nötig“ begrenzen.

6.3 Zusammenarbeit mit der Polizei

6.3.1 Anzeigenerstattung

Die Polizei ist sehr an einer vertrauensvollen Zusammenarbeit mit der Wirtschaft interessiert. Jede Polizeidienststelle kann und wird eine Strafanzeige entgegennehmen. Es empfiehlt sich jedoch, sich direkt an die inzwischen in mehreren Bundesländern eingerichteten Fachdienststellen für Cybercrime-Delikte zu wenden. Darüber hinaus stehen auch in vielen Landeskriminalämtern oder im Bundeskriminalamt zentrale Ansprechstellen zur Verfügung. Zur Identifizierung der für Sie geeigneten Ansprechpartner wird bereits im Vorfeld konkreter Anlässe eine Verbindungsaufnahme mit Ihrer für Cybercrime-Delikte zuständigen Fachdienststelle der Polizei empfohlen.

6.3.2 Ermittlungen und Tatortarbeit

Die Polizei führt auf Grundlage der Strafprozessordnung (StPO) die Ermittlungen zur Erforschung des Sachverhalts im Auftrag der zuständigen Staatsanwaltschaft. Diese besitzt die Verfahrenshoheit bis zu einer späteren Abgabe an das Gericht. Es ist das Bestreben der Polizei, im Rahmen ihrer Ermittlungs- und Tatortarbeit jede unnötige Erregung firmeninterner oder öffentlicher Aufmerksamkeit oder unnötige Störungen der Geschäfts-/Betriebsabläufe zu vermeiden. So ist die Geschäftsleitung einer Firma grundsätzlich erster Ansprechpartner bei allen polizeilichen Ermittlungstätigkeiten, die in Ihrer Firma stattfinden.

Der Polizei ist die Interessenlage der Firmen zu dem Aspekt „Imageschaden“ bekannt. Dem wird versucht, durch entsprechende Anpassung der polizeilichen Maßnahmen zu begegnen. So ist die Polizei grundsätzlich bestrebt, mit nur so vielen Beamten vor Ort zu erscheinen, wie es für Durchführung der zu treffenden Maßnahmen notwendig ist. Wenn es vermeidbar ist, wird auf den Einsatz von uniformierten Beamten verzichtet. Abhängig von der Ausgangsposition besteht die Möglichkeit, dass der Anzeigenerstatter die Polizei bei der Pforte als Geschäftstermin anmeldet.

Neben dem Gespräch mit der Geschäftsführung kann es notwendig sein, Sicherheitsbeauftragte und/oder Systemadministratoren einzubinden. Dann entscheidet sich, ob und inwieweit weitere Beschäftigte der Firma befragt bzw. vernommen werden müssen. Befragungen/Vernehmungen können zur Wahrung der Diskretion wahlweise am Arbeitsplatz oder einem anderen Ort erfolgen.

Als weitere polizeiliche Maßnahmen kann es erforderlich sein, Daten vor Ort von Firmencomputern zu sichern. Dies geschieht in der Regel durch eine so genannte Spiegelung der Daten, d.h., die als grundsätzlich beweisrelevant eingeschätzten Daten der Firma werden vor Ort auf einen von der Polizei mitgebrachten Datenspeicher kopiert. Die Firmencomputer müssen also nicht zwingend sichergestellt bzw. beschlagnahmt werden. Der laufende Betrieb der Firma wird somit im Normalfall nicht weiter beeinträchtigt.

Im Anschluss werden die so sichergestellten Daten insbesondere zur Feststellung tatrelevanter Spuren, zur Gewinnung weiterer Beweismittel bzw. zur Identifizierung von Tatverdächtigen ausgewertet.

Potenzielle Beweismittel, wie z. B. Datenträger, Computerausdrucke oder digital gespeicherte Informationen, können dabei von einer Firma bzw. deren Vertreter als Gewahrsamsinhaber auch freiwillig – ausdrücklich oder stillschweigend – an die Polizei herausgegeben werden. Haben jedoch mehrere Personen Mitgewahrsam, so müssen alle einwilligen, sofern nicht eine alleine verfügungsberechtigt ist. Im Falle einer solchen freiwilligen Herausgabe oder auch dann, wenn der Gewahrsamsinhaber nicht bekannt ist, stellt die Polizei die Beweismittel in der Regel formlos sicher. Eine (förmliche) Beschlagnahme ist hingegen grundsätzlich nur dann erforderlich, wenn die Sachen nicht freiwillig vom Gewahrsamsinhaber herausgegeben werden.

Sollte sich der Tatverdacht gegen einen in der Firma beschäftigten Mitarbeiter richten, wird es ggf. erforderlich sein, seinen Arbeitsplatz zu durchsuchen und sein persönliches Netzwerkprofil sowie seinen E-Mail-Account zu sichern. Die Geschäftsleitung wird grundsätzlich über entsprechende Ermittlungshandlungen in der Firma rechtzeitig informiert. Während laufender Ermittlungen erfolgt durch die Polizei bzw. die Staatsanwaltschaft in der Regel keine Öffentlichkeitsarbeit.

Die Polizei kann nur die Straftaten aufklären, von denen sie Kenntnis erhält. Die Ermittlung, ggf. Festnahme und die Anklage von Straftätern kann neben der Erfüllung des Strafanspruches auch eine abschreckende Wirkung auf andere potenzielle Nachahmungs- oder Wiederholungstäter entfalten und damit einen wichtigen Beitrag für die Sicherheit im Internet darstellen. Darüber hinaus dienen die Erkenntnisse aus Strafverfahren den Sicherheits- und Strafverfolgungsbehörden als Grundlage zur Optimierung bestehender und Entwicklung neuer Präventions- und Bekämpfungsstrategien und tragen somit letztlich zu einem erhöhten Schutz aller Nutzer von informationstechnischen Systemen bei. Insoweit tragen auch Wirtschaftsunternehmen eine besondere Verantwortung, um im Sinne eines ganzheitlichen Ansatzes bei der Bekämpfung der Cybercrime in Deutschland den permanent und immer schneller wachsenden Herausforderungen in diesem Phänomen erfolgreich zu begegnen.

Nützliche Links zum IT-Grundschutz und zur Sicherheit in Unternehmen z.B.:

- https://www.bsi.bund.de
- https://www.sicher-im-netz.de
- https://bitkom.org
- http://www.bmwi.de
- http://asw-online.de

Literatur

[1] Bundesministerium des Innern, *Die Kriminalitaet in der Bundesrepublik Deutschland*.

[2] Bundesministerium des Innern, *Bericht zur polizeilichen Kriminalstatistik 2016*.

[3] Bundeskriminalamt, *Cybercrime Bundeslagebild 2016*.

[4] Marit Hansen, *Webidprofile*.

[5] Dan Olweus, *Gewalt in der Schule: Was Lehrer und Eltern wissen sollten -- und tun können*. (4. durchges. aufl., 1. nachdr.). Bern: Hans Huber.

[6] W. Schweiger und K. Beck, *Handbuch Online-Kommunikation*. Springer, 2010.

[7] C. Schneider, C. Katzer und U. Leest, „Cyberlife-Spannungsfeld zwischen Faszination und Gefahr. Cybermobbing bei Schülerinnen und Schülern“, *Eine empirische Bestandsaufnahme bei Eltern, Lehrkräften und Schülern/innen in Deutschland, Von dem Bündnis gegen Cybermobbing eV, Karlsruhe*, 2013.

[8] M. Büchel und P. Hirsch, *Internetkriminalität: Phänomene-Ermittlungshilfen-Prävention*. CF Müller GmbH, 2020.

[9] I. Wirth, *Kriminalistik-Lexikon*. CF Müller GmbH, 2011.

[10] H. Clages und R. Ackermann, Hg., *Der rote Faden: Grundsätze der Kriminalpraxis,* 13. Aufl. Heidelberg: Kriminalistik, 2017.

[11] M. Bock, Hg., *Kriminologie,* 6. Aufl. München: Beck, 2008.

[12] D. Kochheim, *Cybercrime und Strafrecht in der Informations-und Kommunikationstechnik,* 2. Aufl. CH Beck, 2015.

[13] Bundeskriminalamt, *Cybercrime Bundeslagebild 2018*.

Anmerkung

Dieser Lehrbrief wurde für die Studierenden der Sachverständigenausbildung gemäß ADiF/AFOS im Rahmen des Moduls „Rechtsgrundlagen I“ erstellt. Das Dokument darf nicht außerhalb dieses Rahmens verbreitet, verwendet oder veröffentlicht werden.

Dies liegt nicht zuletzt daran, dass die Quellenangaben nicht vollständig sind. Inhalte dieses Dokuments sind aus verschiedenen öffentlichen Quellen zusammengetragen.