Identitätsdiebstahl im Internet: Wie er funktioniert und wie man sich schützen kann

Autoren: Alexander Wragge, David Pachali

Eine E-Mail-Adresse, ein Facebook-Profil, ein Onlinebanking-Account – im Internet identifizieren wir uns gegenseitig über Datenströme. Das Problem: Cyber-Mobber können uns damit das Leben schwer machen. Kriminelle können unsere digitale Identität für Betrügereien missbrauchen. Ein Überblick zum Thema Identitätsdiebstahl.

Die Kreditkarte ist weg. Auch das Telefon. Der Pass. Kathrin B. ist in Glasgow ausgeraubt worden. Sie braucht Hilfe. 1.900 Euro muss sie zusammenbekommen, um wieder nach Hause zu fliegen. Das schreibt sie in einer E-Mail. Betreff: „Dringend“. Weiter unten steht die Adresse einer schottischen Filiale der Western Union, einem Anbieter weltweiter Bargeld-Transfers. Dorthin soll ich ihr Geld schicken. Sie erwartet meine „schnelle Reaktion“. Das Seltsame ist nur, Kathrin B. ist gar nicht in Schottland, sondern bei mir in der Küche.

Erfahrungen wie diese haben schon viele gemacht. Betrüger hacken ein E-Mail-Postfach oder den Account eines Sozialen Netzwerks und betteln bei sämtlichen Kontaktpersonen um Geld. Immer wieder hat die Masche Erfolg.

Bei den gefälschten Mails handelt es sich nur um eine mögliche Form, wie Identitätsmissbrauch aussehen kann. Das digitale Zeitalter eröffnet auch Betrügern ganz neue Möglichkeiten, sich persönliche Daten anderer zu verschaffen und eine fremde Identität vorzutäuschen. Sie eröffnen unter fremden Namen Ebay-Accounts und prellen ihre Kunden, sie gehen mit fremden Kreditkartendaten auf Einkaufstour, sie spähen Onlinebanking-Zugänge aus und räumen Konten leer.

Bankdaten und E-Mail-Konten beliebtes Ziel

Die Täter sind dabei an allen Arten und Ausprägungen von digitalen Identitäten interessiert, die sie in kriminellen Geschäftsmodellen verwenden könnten. Dazu gehören zum Beispiel Zugangsdaten für Kommunikationsdienste wie E-Mail, Skype oder Soziale Netzwerke. Auch Zugänge zu Onlineshops, Banken, Auktionsportalen und Buchungssystemen für Flüge, Hotels oder Mietwagen sind für sie interessant. Dem Bundeskriminalamt wurden 2014 rund 6.984 Fälle von Phishing beim Onlinebanking gemeldet. Dabei fangen Betrüger mit gefälschten E-Mails oder Webseiten Zugangsdaten ab, um an fremdes Geld zu gelangen. Durch neue, sichere Verfahren sank die Zahl in

den letzten Jahren zunächst, stieg dann aber wieder an – ein Wettrennen zwischen Anbieter und Angreifer, wie oft in der IT-Sicherheit.

Häufig werden auch fremde Computer und E-Mail-Konten gekapert, um sie zu sogenannten Botnetzen zusammenzuschließen. Solche „Zombie-Rechner" versenden dann zum Beispiel unbemerkt vom Nutzer massenhaft Spam. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) machte 2014 auf zwei Fälle von enormen Ausmaßen aufmerksam. Forscher und Strafverfolgungsbehörden hatten dabei Botnetze ausgehoben, die im ersten Fall rund 16 Millionen, im zweiten rund 18 Millionen geklaute E-Mail-Adressen und Passwörter umfassten, darunter mehrere Millionen aus Deutschland. Oftmals merken die Geschädigten zunächst nicht, dass ihre Rechner infiziert sind und ihre digitale Identität missbraucht wird.

Identitätsklau ermöglicht auch Cyber-Mobbing

Hinter vorgetäuschten Identitäten im Internet müssen aber nicht immer finanzielle Motive stecken. Sie sind auch ein Weg, andere zu mobben. Manche Mobber nehmen in Sozialen Netzwerken eine fremde Identität nur deshalb an, um die echte Person zu peinigen oder ihren Ruf zu schädigen. Im Namen ihrer Opfer schreiben sie Liebes- und Hass-Mails, offenbaren der Welt vermeintliche politische Ansichten und angebliche sexuelle Vorlieben, stellen peinliche Fotos ins Netz, usw.

Nutzerprofile müssen dafür nicht gehackt, sondern können auch gefälscht werden. In Belgien erregte 2011 der Fall einer Frau Aufsehen, die bei Facebook ein Fake-Profil ihres Vorgesetzten anlegte. Die Besucher konnten den Eindruck gewinnen, der Mann gehe fremd. Die Angestellte wurde zu sieben Monaten Haft auf Bewährung und einer Geldstrafe verurteilt, unter anderem wegen Computerbetrugs, Stalking und Verletzungen von Persönlichkeitsrechten.

Identitätsdiebstahl und die Folgen

Die Folgen von Identitätsdiebstahl können für die Betroffenen gravierend sein. Es kann Monate dauern, sich gegen falsche Zahlungsforderungen zu wehren, wenn ein Doppelgänger erst einmal auf Beutezug war. Erlebt hat den Albtraum die Journalistin Tina Groll. Sie schildert auf ihrer Webseite, wie ihre Identität für Betrügereien missbraucht wurde. Bis Grolls Ruf wieder hergestellt war, musste sie einen kostspieligen und mühsamen Kampf mit Behörden, Unternehmen, Auskunfteien und Inkassobüros ausfechten. Doch es gibt Möglichkeiten, dem Identitätsdiebstahl vorzubeugen. Außerdem sollte man wissen, was im Fall eines Falles zu tun ist.

Identitätsdiebstahl ist eine Frage der Daten

Um einer anderen Person die Identität zu klauen, bedarf es oftmals nur weniger Informationen. Allein mit dem Geburtsdatum, dem Namen und der Adresse einer Person lässt sich häufig bereits Schindluder treiben. Beispielsweise lassen sich auf dieser Datengrundlage teilweise Verträge mit Mobilfunkanbietern ändern oder abschließen. Unter Umständen muss man hierbei nur vorgeben, eine Kundenkennzahl oder ein Kennwort verlegt zu haben, um einen Anbieter mit schlechten Vorkehrungen gegen Identitätsdiebstahl zu täuschen.

„Viele Verbraucher sind sich nicht bewusst, was für eine wichtige Information das Geburtsdatum ist“, sagt Florian Glatzner vom Verbraucherzentrale Bundesverband (VZBV). Auch wenn in Deutschland bei vielen Geschäftsvorgängen in der Regel ein Personalausweis und Bankdaten benötigt werden – unbedarft sollte man sein Geburtsdatum nicht preisgeben. Denn selbst ein Warenkreditbetrug lässt sich bereits mit dem Namen, der Adresse und dem Geburtsdatum eines anderen einfädeln. Betrüger bestellen Produkte, und die Rechnung landet bei der Person, deren Identität missbraucht wurde.

Auch elektronischer Identitätsnachweis bietet Angriffsfläche

Vom 2010 eingeführten elektronischen Personalausweis versprach sich die Bundesregierung unter anderem neue Möglichkeiten des Identitätsnachweises im Internet. Der neue Ausweis verfügt zum einen über Funktionen für Behörden, zum anderen für Firmen und Geschäfte. Auch mehrere Jahre nach seinem Start ist die Nachfrage bei Bürgern und Unternehmen jedoch überschaubar. Ende 2013 ließ weniger als ein Drittel der Inhaber den Online-Identitätsnachweis freischalten, der bei Neuausstellungen und beim „elektronischen Aufenthaltstitel“ für Nicht-EU-Bürger angeboten wird.

Die Skepsis ist verständlich: Mit Sicherheitsproblemen bei den Lesegeräten startete das Projekt; der Bund Deutscher Kriminalbeamter nannte die Technik „veralteten Elektroschrott“. Kritiker wiesen auf grundlegende Schwächen des Modells hin, Ausweis und Online-Identifikation zu verbinden. So bedeute es für Inhaber des elektronischen Personalausweises ein zusätzliches Risiko, wenn Betrüger dessen umfangreiche Zusatzfunktionen nutzen könnten. Für die lange Lebensdauer eines Ausweises sei es zudem nicht möglich, sichere Verfahren zu garantieren. Es muss sich zeigen, ob das System solche Hürden in Zukunft überwinden und die Kritiker eines Besseren belehren kann.

Die Tricks der Datendiebe

In der unpersönlichen Kommunikation via Internet sollen Daten die Frage beantworten, mit wem wir es zu tun haben. Umgekehrt lässt sich aus Daten eine Identität zusammenbasteln und vortäuschen. Der eigene Name, das Geburtsdatum, die Adresse – die

Verbreitung dieser Grundinformationen lässt sich im digitalen Zeitalter nur schwer kontrollieren. In jedem Fall müssen sensible Daten wie Passwörter zu Diensten wie dem Onlinebanking, Sozialen Netzwerken und E-Mail-Accounts geschützt werden. Hier einige Gefahrenquellen im Überblick:

Datenlecks in Unternehmen

Nahezu machtlos ist der Nutzer, wenn Firmen seine Daten verlieren. Das passiert selbst Konzernen mit besonders sensiblen Daten. So wurde etwa im Frühjahr 2014 bekannt, dass Angreifer bei Ebay einen laut Unternehmensangaben „großen Teil" der 145 Millionen Kundendatensätze kopieren konnten. Die Täter sollen sich Zugang zu Mitarbeiterkonten verschafft haben und konnten darüber Namen, E-Mail- und Postadressen, Telefonnummern, Geburtsdaten und verschlüsselte Passwörter erbeuten. Für Kriminelle sind die Datenschätze von Firmen ein attraktives Gut. Mittlerweile existiert ein Schwarzmarkt für solche Datensammlungen.

Phishing

Beim Phishing verleiten gefälschte Internetseiten, E-Mails und SMS die Internetnutzer dazu, ihre Passwörter, PINs oder TANs selbst preiszugeben. Beispielsweise bauen Betrüger die Webseiten von Finanzinstituten nach, um Benutzer zu täuschen. Eine andere Möglichkeit ist, im Namen der Bank gefälschte Mails zu verschicken, die zur Eingabe von Passwort und TANs auffordern. Ausführliche Informationen bietet der Artikel „Vorsicht Falle – Betrug im Internet" von iRights.info und klicksafe (siehe „Mehr Informationen" unten).

Schadsoftware

Der Klassiker, um sich Schadsoftware einzufangen, sind Dateianhänge in E-Mails, hinter denen sich schädlicher Code verbirgt. Eine modernere Variante davon sind gefälschte Anhänge bei Nachrichten in Sozialen Netzwerken und bei Chat-Diensten oder getarnte Links auf Schadsoftware. Eine weitere Methode besteht darin, dass Angreifer schädlichen Code auf Webseiten einschleusen. Betroffen davon waren bislang nicht nur vergleichsweise dubiose Internetseiten. Auch seriöse Angebote wie die Nachrichtenseiten großer Medienunternehmen können hier Opfer werden, wenn sie etwa Werbung über externe Quellen einbinden lassen.

Beim Besuch entsprechender Seiten wird dann im Hintergrund Schadsoftware heruntergeladen, sofern Sicherheitslücken beim Nutzer und schlecht eingerichtete Systeme das zulassen. Beim sogenannten „Drive-by-Exploit" muss man dafür gar nichts anklicken.

Solche Schad- und Spähsoftware kann von Betrügern vielfältig eingesetzt werden. Sie fertigt beispielsweise heimlich Screenshots des infizierten Computers an, protokolliert unbemerkt die Eingabe von Passwörtern (Keylogging), und versendet die erbeuteten Daten unbemerkt an die Hintermänner. Auch einige TAN-Verfahren beim Onlinebanking lassen sich austricksen. Kriminelle klinken sich dann zum Beispiel unbemerkt in den Datentransfer zwischen Kunde und Bank ein (Man-in-the-Middle-Attacken) und lenken Überweisungen oder Daten um.

Unsichere Netzwerke und Verbindungen

Der amerikanische Programmierer Eric Butler zeigte 2010 mit dem Programm „Firesheep“, wie leicht Dritte in ungesicherten WLAN-Netzen den Datenverkehr mitschneiden können – jedenfalls dann, wenn keine anderen Vorsichtsmaßnahmen getroffen werden. Damit gab er auch großen Webdiensten einen Anstoß, ihre Dienste stärker über gesicherte Verbindungen anzubieten. Ist der Datentransport dagegen nicht verschlüsselt, kann ihn jeder ohne weiteres einsehen und somit an persönliche Daten des Nutzers gelangen. Heutzutage kann man von Webdiensten mit Benutzerkonten erwarten, sichere Verbindungen als Standard anzubieten – erkennbar am „HTTPS“ in der Browserzeile. Das ist etwa bei Facebook, Google, Wikipedia und vielen anderen Webdiensten der Fall, aber leider gibt es nach wie vor Ausnahmen.

Smartphones und Apps

Das Smartphone wird noch häufig als Angriffsziel übersehen. Auch hier gibt es Schadprogramme, die speziell für die mobilen Endgeräte programmiert sind. Viele, gerade kostenlose Apps sammeln zudem alle möglichen Daten vom Telefon und übermitteln sie weiter. In der Regel werden diese Daten an Werbeanbieter oder die Entwickler selbst geschickt, doch Missbrauch kann auch dort ansetzen.

Nach wie vor senden manche Apps Daten unverschlüsselt an die Server von Unternehmen. So können Angreifer sie im Datenverkehr gezielt abfangen. Besondere Vorsicht sollte man auch bei Dritt-Anwendungen etwa für Facebook walten lassen. Versprechen solche Zusatzprogramme, Profilbesuche anzuzeigen oder virtuelle Blumen zu verschicken, ist Skepsis angebracht. Die erste Funktion gibt es gar nicht, die zweite ist womöglich nur Tarnung, um Zugang zu bestimmten Nutzerdaten zu bekommen.

Wie kann ich mich schützen?

Hundertprozentig schützen kann man sich vor Identitätsdiebstahl nicht. Dennoch können verschiedene Verhaltensweisen das Risiko deutlich verringern. Einige gehören ohnehin zur allgemeinen Vorsicht bei der Nutzung des Internets, manche sind speziell auf die Gefahren des Identitätsdiebstahls zugeschnitten.

Die wichtigsten werden hier vorgestellt:

- **Sichere Passwörter wählen:** Auch wenn es unbequem scheinen mag, sollten für unterschiedliche Onlinedienste stets auch unterschiedliche Passwörter verwendet werden. Sonst können sich Kriminelle mit einem erbeuteten Passwort von einem Konto zum nächsten weiterhangeln, zum Beispiel vom E-Mail-Postfach über Ebay bis zu Facebook. Passwörter sollten regelmäßig geändert werden und niemals aus Familiennamen, Haustieren, Geburtsdaten und ähnlichen Angaben bestehen. Ausführliche Hinweise bietet etwa die Webseite des BSI (siehe „Mehr Informationen“ unten).
- **Doppelte Anmeldesicherheit nutzen**: Viele Webdienste bieten heute eine sogenannte Zwei-Wege- oder Zwei-Faktor-Authentifizierung an. Das Prinzip: Beim Einloggen bekommt man einen Code aufs Handy geschickt, etwa per SMS. Man kann es häufig auch so einstellen, dass dies nur bei neuen, unbekannten Geräten nötig ist. Einige Anbieter wie Dropbox oder Google unterstützen auch spezielle Apps, die solche Codes erzeugen. Wenn ein Konto auf diese Weise abgesichert ist, kann sich ein Angreifer selbst dann nicht in das Onlinekonto einloggen, wenn ihm Zugangskennung und Passwort in die Hände fallen.
- **Geräte und Systeme aktuell halten:** Besonders der Internetbrowser, das Betriebssystem und Antivirensoftware sollten ständig auf aktuellem Stand gehalten werden. Solche Aktualisierungen schließen häufig Sicherheitslücken, die Angreifer sonst ausnutzen können.
- **WLAN und fremde Geräte mit Bedacht nutzen**: Öffentliche WLAN-Netzwerke, etwa im Café oder in Bibliotheken, bedeuten dann ein Risiko, wenn man sie gedankenlos nutzt. Sind sie ohne Passwort unverschlüsselt zugänglich, ist im Prinzip auch der eigene Datenverkehr für andere im selben Netzwerk unverschlüsselt, sofern man ihn nicht anderweitig absichert. Um sich zu schützen, sollte man Webseiten wie Facebook stets nur über „HTTPS“ im Browser aufrufen und im Mailprogramm verschlüsselte Verbindungen aktivieren – beides empfiehlt sich nicht nur in offenen Netzen, sondern immer. Auch sogenannte VPN-Dienste („Virtual Private Network“) bieten zusätzlichen Schutz in fremden WLANs, indem der Datenverkehr stets durch einen verschlüsselten Tunnel wandert. Besonders sensible Anwendungen wie Onlinebanking sollten nur vom eigenen Endgerät betrieben werden, um viele Risiken zu umgehen, die in Internetcafés oder öffentlichen WLAN-Netzwerken lauern können.
- **Verdächtige Datensammler erkennen:** Es empfiehlt sich immer, einen Augenblick innezuhalten und zu überlegen, bevor man seine Daten online in Formulare eingibt. Wie seriös ist die Reisebuchungsplattform oder die Spendenorganisation? Was steht in den Allgemeinen Geschäftsbedingungen, wer ist überhaupt Anbieter oder Betreiber laut Impressum? Vor allem, wenn jemand im Internet gezielt nach Pass-

wörtern oder Kontodaten fragt, sollten die Alarmglocken schrillen; egal ob der Absender nun Ebay, die eigene Hausbank oder ein persönlicher Freund zu sein scheint. Banken fordern grundsätzlich keine solchen vertraulichen Daten per E-Mail oder Telefon an.

- **Datensparsamkeit:** Daten, die gar nicht erst herausgegeben werden, können auch nicht missbraucht und geklaut werden. Generell sollten personenbezogene Daten daher nur nach genauer Prüfung und mit entsprechender Vorsicht preisgegeben werden. Wenn man etwa sein korrektes Geburtsdatum überhaupt in Sozialen Netzwerken angeben will, dann muss man es nicht gleich mit der ganzen Welt teilen. Wer Veranstaltungen wie Klassen- oder Vereinstreffen organisiert, sollte Teilnehmerlisten mit personenbezogenen Daten wie Geburtsdatum und E-Mail-Adresse nicht öffentlich ins Netz stellen. Gewerbetreibende sollten ihre Bankverbindung nicht auf ihrer Webseite veröffentlichen, wenn es nicht erforderlich ist.
- **Apps und Dienste prüfen**: Bei Apps sollte man sich genau anschauen, auf welche Daten und Funktionen sie zugreifen können. Oft sind kostenlose Apps, Umfragen und Gewinnspiele nur dafür gemacht, Daten zu sammeln. Will etwa eine Taschenlampen-App das Adressbuch einsehen, sollte man skeptisch werden. Auch wenn Webdienste anbieten, bei der Registrierung nach Freunden zu suchen (wofür häufig das eigene Adressbuch hochgeladen wird), sollte man vorsichtig sein. Bei manchen Diensten werden dann zudem Werbemails an alle Personen im Adressbuch versendet.
- **Kontrolle und Überblick behalten:** Schließlich empfiehlt es sich, regelmäßig die eigenen Kontoauszüge zu prüfen und im Internet zu recherchieren, welche Daten über einen selbst dort kursieren. Öffentlich einsehbare Informationen kann man mit Suchmaschinen finden – wer mehrere nutzt, findet gelegentlich auch Seiten, die sonst unentdeckt blieben. Darüber hinaus hat man als Nutzer ein Recht, zu erfahren, welche Daten Unternehmen über einen speichern. Stößt man auf falsche Daten oder solche, die nicht mehr gebraucht werden, hat man einen Anspruch auf Berichtigung oder Löschung. Mehr Hinweise bietet der Artikel „Meine Daten, meine Rechte und wie man sie durchsetzt“ auf iRights.info (siehe „mehr Informationen“ unten).

Erste Hilfe: Was tue ich im Fall von Identitätsdiebstahl?

Wenn alle Vorsicht nichts geholfen hat und jemand die eigene Identität missbraucht, gilt es schnell zu handeln. Hinweise können sein, dass unerklärliche Abbuchungen vom Bankkonto erfolgen, unberechtigte Zahlungsforderungen eingehen oder Passwörter für Benutzerkonten nicht mehr akzeptiert werden. Dann sollte man der Sache sofort nachgehen und nicht auf ein Missverständnis oder einen Zufall hoffen. Banken, Onlinewarenhäuser, Auktionsplattformen müssen sofort über Unregelmäßigkeiten informiert werden. In der Regel bieten sie 24-Stunden-Hotlines. Man sollte sofort versu-

chen, entsprechende Zugänge und Benutzerkonten zu sperren. Zur Sicherheit empfiehlt es sich im Zweifel, sämtliche Passwörter auch von noch nicht betroffenen Diensten zu ändern.

Ist der eigene E-Mail-Account oder das Profil in einem Sozialen Netzwerk gekapert worden, sollte das Passwort sofort zurückgesetzt werden (über die Funktion „Passwort vergessen“) und der Anbieter kontaktiert werden, etwa über den Support. Freunde und Bekannte sollte man schnell über Betrugsversuche im eigenen Namen aufklären.

Rechtliche Schritte bei Identitätsdiebstahl

Wer durch Identitätsmissbrauch zu Schaden kommt, sollte Strafanzeige stellen, ob es nun um Geld geht oder den eigenen Ruf. Zwar gibt es hierzu keine spezielle Gesetzgebung, allerdings sind die derzeit bekannten Formen des Identitätsdiebstahls und Identitätsmissbrauchs dennoch strafbar. Wenn Angreifer personenbezogene Daten erlangen und missbrauchen, werden Gesetze übertreten, etwa das Verbot des Ausspähens und Abfangens von Daten und des Computerbetrugs. Auch Unternehmen machen sich möglicherweise strafbar oder verhalten sich gesetzeswidrig, wenn sie personenbezogene Daten ihrer Kunden verlieren oder ohne Erlaubnis an Dritte weitergeben.

Auch Cyber-Mobbing in Verbindung mit Identitätsmissbrauch ist rechtswidrig und kann unter anderem gegen das Persönlichkeitsrecht, das Stalking-Verbot und andere gesetzliche Regelungen verstoßen. Weiterführende Hinweise und Rat zum Thema finden sich auch unter „Mehr Informationen“ unten.

Wer finanziell geschädigt wurde, hat vor Gericht weit bessere Chancen, wenn er sorgfältig mit seinen Daten umgegangen ist. Beispielsweise verlangen die AGB von Banken dem Kunden eine besondere Vorsicht beim Onlinebanking ab. Seit 2009 ist die Haftung bei Onlinebanking-Betrugsfällen für die Betroffenen auf 150 Euro beschränkt. Allerdings gilt das nicht, wenn sich der Kunde grob fahrlässig verhält. Beispiele sind hier, wenn jemand seine Onlinebanking-Kennnummern freigiebig an Dritte preisgibt oder auf allzu offensichtliche Betrugsversuche hereinfällt. Welches Verhalten genau als „grob fahrlässig“ eingestuft wird, hängt immer vom Einzelfall ab. In jedem Fall haftet der Kunde nur, bis er seine Bank über den Missbrauch informiert hat. Umso schneller der Missbrauch gemeldet wird, desto besser.

Doch auch wenn Identitätsdiebstahl strafbar ist, ist die Strafverfolgung der Täter oft schwierig. So lassen sich beispielsweise Phishing-Webseiten zwar lokalisieren, sind aber auf Servern auf der ganzen Welt verstreut. Für die Behörden ist Identitätsmiss-

brauch daher oft nur schwer zu ahnden. Deshalb ist es umso wichtiger, sorgsam mit seinen Daten umzugehen, um sich so vor Angreifern zu schützen.

Mehr Informationen

- www.klicksafe.de/irights und http://irights.info/kategorie/klicksafe
  - Vorsicht Falle – Betrug im Internet (Philipp Otto)
  - Cyber-Mobbing, Cyberbullying und was man dagegen tun kann (John Hendrik Weitzmann)
- www.klicksafe.de/materialien
  - Broschüre: Ratgeber Cyber-Mobbing – Informationen für Eltern, Pädagogen, Betroffene und andere Interessierte
- www.klicksafe.de/cybermobbing
  - Ausführliche Informationen zum Thema Cyber-Mobbing
- http://irights.info/?p=24053
  - Artikel: Datenschutz: Meine Daten, meine Rechte und wie man sie durchsetzt
- www.klicksafe.de/themen/datenschutz
  - Alles rund um das Thema „Datenschutz“
- www.bsi-fuer-buerger.de
  - Sicherheitstipps vom Bundesamt für Sicherheit in der Informationstechnik (BSI)
- www.bka.de/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html
  - Bundeskriminalamt (BKA): Lagebilder Cybercrime 2010-2014

Alexander Wragge, David Pachali. Stand 11/2015