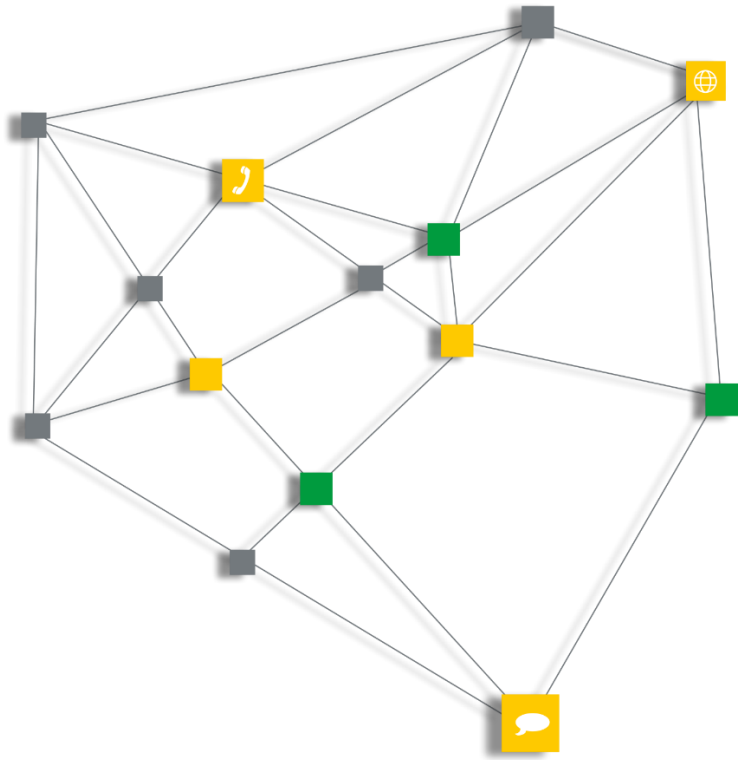
BWV
Regional
Arbeitsgemeinschaft
Kompetenz*DIGITAL*



Kompetenz***DIGITAL***

IT-Grundlagen
Schwerpunkt Social Media
Datenschutz

Big Data Trends / data analytics
Use Cases in der
Versicherungsbranche
Datenanalysen für Maßnahmen
zur Kundenorientierung

JRC Training J. Roth
Walter-Gieseking-Str. 14
30159 Hannover
0511-4751840
info@jrctraining.com

www.**JRC-TRAINING**.com

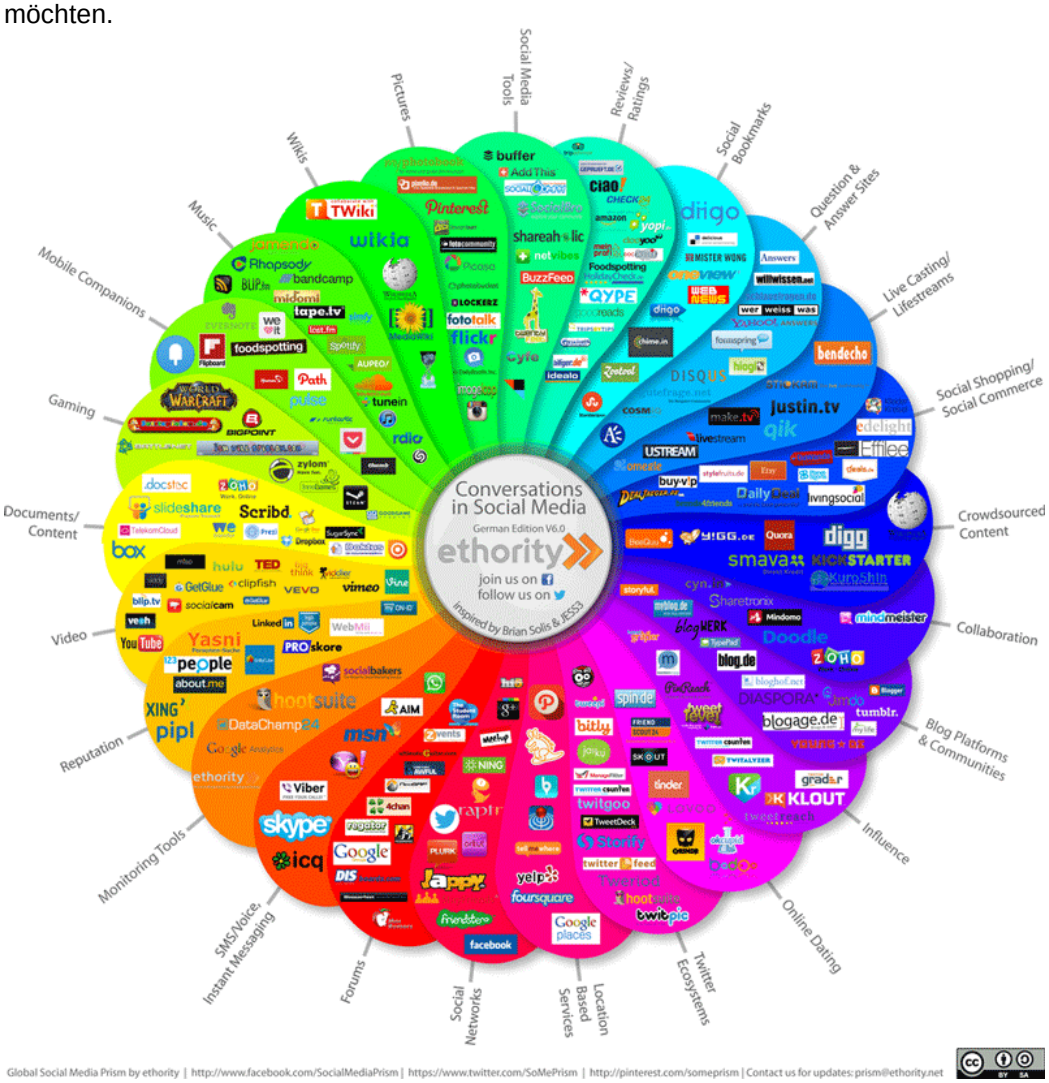
Inhaltsverzeichnis

Beim Einsatz von Big Data kristallisieren sich zwar zunehmend erfolgreiche Anwendungsbereiche heraus, nach wie vor kritisch für deren Einsatz ist die Datenlage - nach der Daten-Sondierung stellen viele Unternehmen fest, dass die Digitalisierung ihrer Datenbestände bereits fortgeschritten ist, alte "Datenhalden" aber abgebaut oder weitere Daten erhoben werden müssen.
Zukunftstrend Data Science: Innerhalb der Versicherungsbranche haben insbesondere die Bereiche Tarifcontrolling, Marketing und Vertrieb die Möglichkeit, mit Data Science Kunden und Interessenten zielgerichteter ansprechen und Prozesse zu steuern. Innovative Big Data Ansätze ermöglichen es, Optimierungspotenziale der klassischen Versicherungsprozesse auszuschöpfen.

1 IT-Grundlagen: Schwerpunkt Social Media, Datensicherheit, "Social Networks"

1.1 Große Erreichbarkeit öffnet neue Märkte

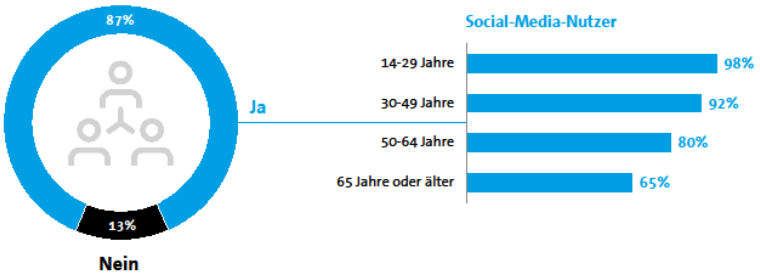
Social Media ist schon lange kein Jugend- oder Nischenphänomen mehr, sondern hat sich innerhalb weniger Jahre zu einem festen Teil unseres Lebens entwickelt. Heute gehören die Anbieter der Social Medias für viele Internetnutzer in der digitalen Welt einfach dazu, über ein eigenes Profil im Social Network präsent und erreichbar zu sein.
Zunehmend ergänzen und ersetzen Social Media in vielen Bereichen klassische Online-Funktionen und werden darum zunehmend für Unternehmen interessant, die mehr oder neue Leistungen bei hoher Erreichbarkeit anbieten möchten.



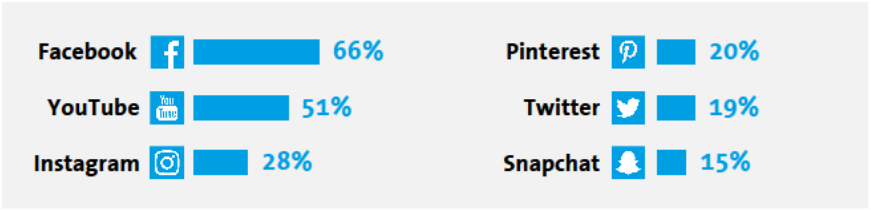
Das "Social Media Prism": Eine nahezu unüberschaubare Menge von "Social Media Networks" …

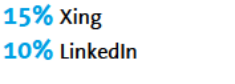
Etwas Statistik? (Quelle: BitKom Research, 2017)

Im Schnitt sind deutsche Internetnutzer in drei sozialen Netzwerken angemeldet; am aktivsten ist die Gruppe der 14- bis 29 Jahren.

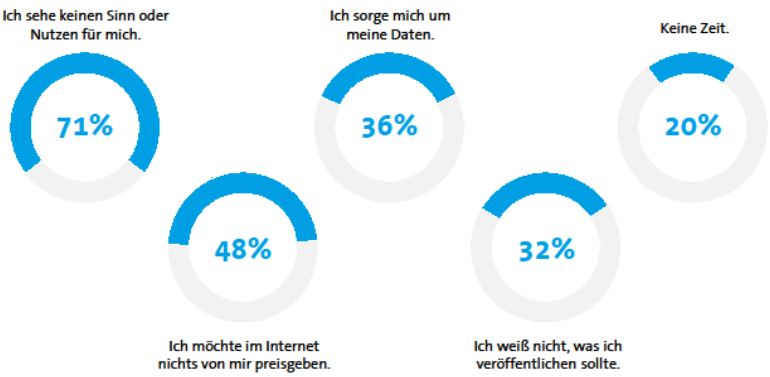


facebook und instagram dominieren den Markt; Xing und linkedin haben aber als für Unternehmen interessante Anbieter einen Anteil von 25 % (gerechnet nach den Usern der letzten 3 Monate).



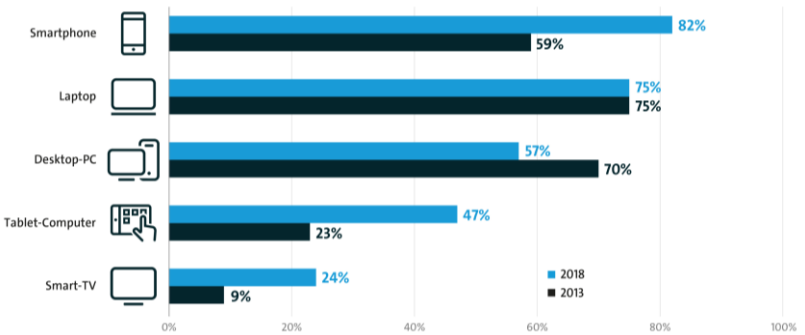


Interessant ist der Blick auf diejenigen, die Social Media ablehnen - Berechtigte Gründe!

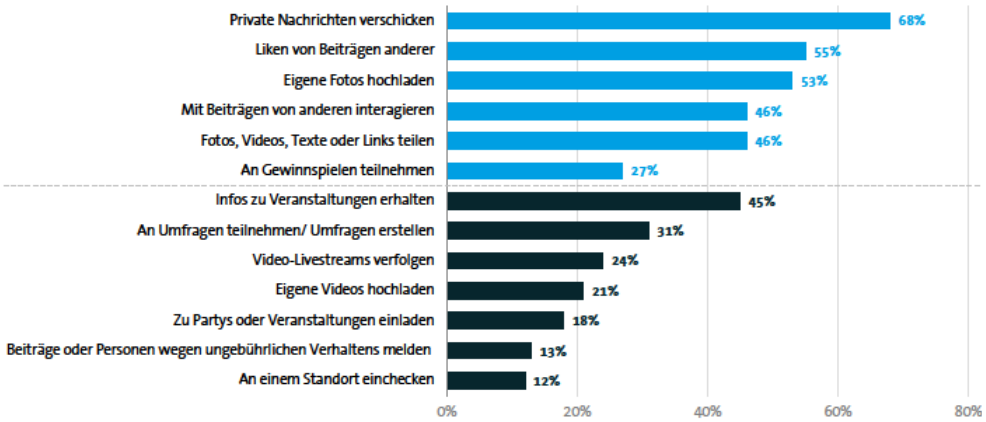


Einsatzfelder sozialer Netzwerke

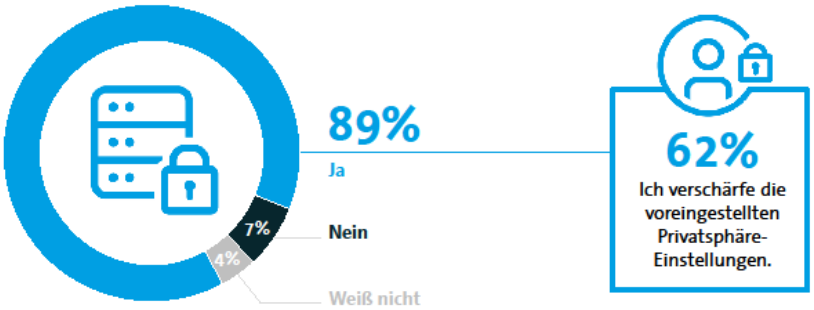
"Mobile First" Geräte-Präferenzen für den Zugriff auf soziale Netzwerke



Verteilung der Aktivitäten



Und die Datensicherheit?



1.2 Noch hat facebook nicht das Monopol

Ein Überblick der aktuellen Social Networks mit Blick auf unternehmerischer Bedeutung (Stand 02-2019).

LinkedIn	"Karriereplattform": Bietet neben den Standard-Funktionen (Seiten erstellen, teilen) spezielle Funktionen für geschäftliche Kontakte und Aktionen. 2,99 Mrd. $, 0,5 Mrd Nutzer, Microsoft-Unternehmen; Alternative zu facebook
Instagram	Ein soziales Netzwerk, welches sich auf das Veröffentlichen und Ansehen von Bildern und Videos spezialisiert hat ~ 1 Mrd Nutzer, facebook-Unternehmen. Fotos werden manipuliert und verändert, darum mangelnde Authentizität.
Facebook	Dient zur Selbstdarstellung und Freigeben ("Teilen") von Texten und Bildern, die von anderen bewertet werden können ("liken"). 2,27 Mrd. $ Die hohe Zahl der Benutzer (~1 Mrd) verspricht eine hohe Erreichbarkeit, allerdings qualitativ nur bedingt geeignet, da die Inhalte nicht "nachhaltig" sind, also Aktuelles sofort durch neue Inhalte anderer überlagert wird, von der Datensicherheit her bedenklich da Besucher rücksichtslos ausgeforscht werden und Inhalte manipulativ angezeigt werden (zB Themen ohne Wissen des Profilinhabers bei anderen hervorgehoben oder zurückgesetzt werden).
Flickr	Teilen von Bildern und sehr kurzen Videos, die dann von anderen Nutzern kommentiert werden können
Google+	Bietet neben dem Erstellen eines Profils oder einer Seite und dem Teilen von Beiträgen auch Funktionen wie Videotelefonie oder das Einteilen der Kontakte in verschiedene Gruppen an
Pinterest	Ermöglicht das Erstellen und Sammeln einer eigenen Bilder-Pinnwand
Snapchat	Ein Instant Messaging Dienst, der nur auf dem Smartphone funktioniert mit der Besonderheit, dass Inhalte nach einer bestimmten Dauer „im Nirvana“ verschwinden
Tumblr	Ein soziales Netzwerk, in dem man Inhalte in Form eines Blogs teilen und anderen Blogs folgen kann

Twitter	Eine Social Network, bei dem 140-Zeichen Kurznachrichten öffentlich geteilt werden können. Sehr beliebt ist hier der Einsatz von Hashtags zur Verschlagwortung
Xing	"Karriereplattform": Interessant für Unternehmen, denn neben der Erstellung eines eigenen Profils ist es auch möglich, Stellenangebote aufzugeben oder Veranstaltungen zu teilen
YouTube	Videoportal, in dem hochgeladene Videos und eigene Aufnahmen veröffentlicht werden können.

1.3 Sich korrekt in Social Networks bewegen - Ein Glossar

Active Sourcing	Aufbau und Instandhaltung einer Beziehung zu potenziell neuem Personal.
Analytics	Ein System, welches alle Daten eines Unternehmens sammelt und analysiert, sodass diese als Informationsquelle herangezogen werden können.
App	Kurz für ‘Applikation’. Eine Anwendungssoftware, überwiegend für mobile Geräte, aber auch für Computer.
Banner	Werbeanzeige auf einer Webseite.
Blogging	Ein Blog ist ein Online Tagebuch, auf dem der Besitzer (Blogger), verschiedene Inhalte beliebig teilen kann.
Buzz	Die Verbreitung "Mund zu Mund", bedeutet User reden über ein bestimmtes Thema über einen bestimmten Zeitraum: Je mehr geredet wird, desto mehr Buzz wird erzeugt.
Contents	Inhalte die auf (Social Media) Netzwerken, Blogs, etc. im Internet in Form von Beiträgen veröffentlicht werden.
Creative Commons	Eine Organisation, welche verschiedene Standard-Lizenzverträge veröffentlicht, wodurch freie Inhalte im Internet bestehen.
Crowdsourcing	Das Übertragen von Aufgaben, bspw. eine Entscheidung treffen, an die eigene Community.
Derailing / Trolling	Die bewusste Provokation mit dem Ziel, alle Aufmerksamkeit auf sich selbst zu lenken und somit jegliche vernünftig sowie sachlich geführte Debatte aus dem Ruder laufen zu lassen.
Digital Detox	Der Verzicht auf ein elektronisches Gerät und der Nutzung des Internets für eine gewisse Zeit, um danach wieder kreativer und produktiver zu sein.
Digital Transformation	Die Veränderung eines Unternehmens durch digitale Medien.
PM (private Message)	Eine Nachricht, die auf sozialen Netzwerken privat an eine oder mehrere Personen versandt wird.
Favorisieren	Das Favorisieren von Tweets ist mit dem Liken von Beiträgen zu vergleichen. Favorisierte Tweets werden in die persönliche Favoritenliste eingetragen und sind so stets wiederzufinden.
Follower	Andere User folgen Ihren Aktivitäten.
Following	Es werden einem stets deren aktuellste Beiträge angezeigt und man wird über deren Aktivitäten auf dem Laufenden gehalten.
FOMO (Fear of missing out)	Bezeichnet die Angst, überwiegend auf sozialen Netzwerken, etwas zu verpassen und/oder die eigene Zeit falsch zu verbringen.
Hashtag	Als # dargestellt wird das Thema eines Beitrages in einem sozialen Netzwerk gekennzeichnet. Diese Beiträge werden auch schneller von anderen Nutzern gefunden
Liken/Gefällt mir	Das Markieren eines Beitrags mit einem ‘Like’ signalisiert dem Ersteller des Beitrags, dass einem der Beitrag gefällt, bzw. dass man ihm zustimmt
Monitoring	Social Media Monitoring dient dem kontinuierlichen Überwachen der Online Aktivitäten eines Unternehmens zu dessen Produkten, Schlagworten und Kundenmeinungen.
Pinnen	Man markiert ein Bild auf einer Webseite und weist es einer Pinnwand zu. Wie als würde man ein Bild an eine echte Pinnwand mit einer Reißzwecke heften.
Posten	Einen Beitrag in einem sozialen Netzwerk/Blog/Forum etc. veröffentlichen.
Retweeten	Einen Beitrag bei Twitter an die eigenen Anhänger weiterleiten

Shitstorm	Sturm der Entrüstung, der sich durch Social Media und viraler Effekte schnell verbreiten kann.
Social Bookmarking	Das Verwalten von eigenen virtuellen Lesezeichen.
Social Business	Die Nutzung von sozialen Medien im Unternehmen, um die Produktivität zu erhöhen.
Social Media	Interaktive Plattformen, die es Personen und Gruppen ermöglichen, Inhalte zu erstellen, zu teilen, zu diskutieren und zu modifizieren
Social Media Content/Inhalte	Digitale Medienarten/typen wie Bilder, Video, Text die mit Hilfe digitaler technischer Geräte erstellt und verarbeitet und dann über verschiedene Plattformen verbreitet werden.
Social Media Recruiting	Die Suche nach neuem Personal via sozialen Netzwerken, wie z.B. XING.
Spam/Spamming	Unerwünschte Beiträge oder Nachrichten auf sozialen Netzwerken. Auch übertrieben häufiges Posten oder Versenden von Nachrichten.
Tag/Taggen	Bezeichnet das Markieren eines anderen Beitrags mit einem sogenannten ‘Tag’, einem Schlagwort.
Targeting	Werbung schalten für eine bestimmte Zielgruppe.
User Generated Content	Inhalte, die von Nutzern/Kunden erstellt werden. (Neben Owned Media, Paid Media die dritte Contentart)
Wiki	Ein System, durch das möglichst schnell Informationen gesammelt und abgerufen werden können.

2 Informationssicherheit ist Systemschutz

Informationssicherheit bezeichnet als Oberbegriff die Eigenschaften von informationsverarbeitenden und -lagernden (technischen oder nicht-technischen) Systemen, die die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen. Sie dient dem Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von wirtschaftlichen Schäden und der Minimierung von Risiken.
In der Praxis orientiert sich die Informationssicherheit an der internationalen ISO/IEC-27000-Reihe. Im Bereich der Evaluierung und Zertifizierung von IT-Produkten und -systemen findet die Norm ISO/IEC 15408 (Common Criteria) Anwendung.

Der Mangel an Computersicherheit ist eine vielschichtige Bedrohung; ist einmal die Sicherheit eines Systems verletzt worden, muss es als kompromittiert betrachtet werden, was Maßnahmen zur Verhinderung weiterer Schäden und ggf. zur Datenrettung erfordert.

2.1 Begriffe im Überblick

IT-Sicherheit	Zu den Aufgaben der IT-Sicherheit gehört der Schutz von Organisationen (zum Beispiel Unternehmen) und deren Werten gegen Bedrohungen. Zudem soll wirtschaftlicher Schaden verhindert werden.
Computersicherheit	Computersicherheit: die Sicherheit eines Computersystems vor Ausfall (man spricht von ungeplanter oder geplanter Ausfallzeit, "downtime") und Manipulation (Datensicherheit) sowie vor unerlaubtem Zugriff
Datensicherheit	ist ein häufig mit dem Datenschutz verknüpfter Begriff, der sich aber anders definiert: Datensicherheit hat das *technische* Ziel, Daten jeglicher Art in ausreichendem Maße gegen Verlust, Manipulationen und andere Bedrohungen *zu sichern*. Hinreichende Datensicherheit ist eine Voraussetzung für einen effektiven Datenschutz. Das BDSG nennt den Begriff der Datensicherheit lediglich in § 9a im Zusammenhang mit dem ebenfalls nicht näher definierten „Datenschutzaudit“.
Datensicherung	Datensicherung ist ein Synonym für das englischsprachige Backup, Sicherung, es war der ursprüngliche gesetzliche Begriff für Datensicherheit.

Angriffe und Schutz	Unter einem Angriff auf den Datenschutz oder Datensicherheit (repräsentiert durch zum Beispiel ein Computersystem) versteht man jeden Vorgang, dessen Folge oder Ziel ein Verlust des Datenschutzes oder der Datensicherheit ist. Auch technisches Versagen wird in diesem Sinne als Angriff gewertet.
Statistische Sicherheit	Ein System wird dann als sicher bezeichnet, wenn für den Angreifer der Aufwand für das Eindringen in das System höher ist als der daraus resultierende Nutzen. Deshalb ist es wichtig, die Hürden für einen erfolgreichen Einbruch möglichst hoch zu setzen und damit das Risiko zu reduzieren.
Absolute Sicherheit?	Ein System ist dann absolut sicher, wenn es *jedem* denkbaren Angriff widerstehen kann. Die absolute Sicherheit kann nur unter besonderen Bedingungen erreicht werden, die aber die Arbeitsfähigkeit des Systems oft erheblich einschränken (isolierte Systeme, wenige und hochqualifizierte Zugriffsberechtigte).

2.2 Der Systemangriff: Zweck und Mittel

Während im Firmenumfeld die ganze Themenbreite der Computersicherheit Beachtung findet, verbinden Privatanwender mit dem Begriff "Computersicherheit" primär den Schutz vor Viren und Würmern oder Spyware wie Trojanischen Pferden.
Mittlerweile existieren "Schad-Baukästen" im Internet, die neben einer Anleitung auch alle notwendigen Bestandteile für das einfache Programmieren von Viren liefern bzw. fertige Programme, die bereits beim Aufrufen einer Internetseite den Rechner übernehmen oder permanent Daten übermitteln. Nicht zuletzt schleusen kriminelle Organisationen Viren auf PCs ein, um diese für ihre Zwecke (UBE / UCE, DoS-Angriffe etc.) zu nutzen. So entstanden bereits riesige Bot-Netze, die auch illegal vermietet werden

Die typischen Angriffsformen sind

- Schadsoftware, sog. Malware, zu denen unter anderem Computerviren, Trojaner und Würmer gehören
- Ransomware, die den Zugriff auf Daten und Systeme einschränkt und dessen Ressourcen erst gegen Zahlung eines Lösegelds wieder freigibt
- Social Engineering, das Angreifen, Ausspionieren oder Täuschen einer Person, also eine Betrugsform
- Advanced Persistent Threats (APT), bei denen der Angreifer sein Ziel sorgfältig aussucht
- Unerwünscht zugesandte E-Mails (Spam); (klassische Spam, Schadprogramm-Spam und Phishing)
- Botnetze
- Distributed Denial of Service (DDoS)-Angriffe
- Drive-by-Exploits und Exploit-Kits, die Schwachstellen in Browser, Browser-Plugins oder Betriebssystemen ausnutzen
- Identitätsdiebstahl, wie zum Beispiel Spoofing, Phishing, Pharming oder Vishing,
- Seitenkanalangriffe – also solche Angriffe, die Nebeneffekte (Laufzeitverhalten, Energieverbrauch) beobachten und so Rückschlüsse auf die Daten ziehen; dies findet insbesondere bei Schlüsselmaterial Anwendung
- Und: Physischer Einbruch zum Stehlen sensibler Daten wie Schlüssel oder zum Platzieren von Malware sowie - schlicht und einfach- Fehlbedienung durch Personal oder zugangsberechtigte Personen

2.3 Maßnahmen zur IT-Sicherheit

Maßnahmen werden im Rahmen der Erstellung eines Sicherheitskonzeptes an den Wert der zu schützenden Unternehmenswerte angepasst: Zu viele Maßnahmen bedeuten hohe finanzielle, organisatorische oder personelle Aufwände. Zudem treten Akzeptanzprobleme auf, wenn die Mitarbeiter nicht genügend in den Prozess der IT-Sicherheit eingebunden werden. Implementiert man zu wenig Maßnahmen, bleiben für Angreifer lohnende Sicherheitslücken offen.

- Management: Top-Down Ansatz
  Informationssicherheit ist grundsätzlich eine Aufgabe der Leitung einer Organisation oder eines Unternehmens. Insbesondere die Verabschiedung von Informationsschutz- und Sicherheitsrichtlinien (Security Policy) ist Aufgabe des obersten Managements.

- Operative Maßnahmen
  Maßnahmen sind unter anderem physische, beziehungsweise räumliche Sicherung von Daten, Zugriffskontrollen, das Aufstellen fehlertoleranter Systeme und Maßnahmen der Datensicherung und die

Verschlüsselung.

- Zugangsbeschränkungen auf Nutzereben
  Zu den Sicherheitsmaßnahmen, die von jedem Verantwortlichen für die Informationssicherheit in Unternehmen, aber vor allem auch von privaten Nutzern von Computern und Netzwerken für die Informationssicherheit getroffen werden können, gehört die
  - Zugangskontrolle, der berechtigte Zugang zu Computersystemen und Anwendungssoftware
  - Eingeschränkte Benutzerkonten: Moderne Betriebssysteme verfügen daher über die Möglichkeit, die Benutzerrechte einzuschränken, so dass zum Beispiel Systemdateien nicht verändert werden können
  - Restriktive Konfiguration: Da Benutzer typischerweise (nur) die mit dem Betriebssystem gelieferten sowie die von ihrem Administrator installierten Programme verwenden ist es möglich, Benutzern die Rechte zum Ausführen von Dateien nur dort zu gewähren, wo das Betriebssystem und die installierten Programme abgelegt sind (und sie nicht schreiben können), und überall dort zu entziehen, wo sie selbst schreiben können. Schädliche Programme, die beispielsweise von einer infizierten Webseite heruntergeladen und vom Benutzer unbemerkt als sog. „Drive-by-Download“ im Cache des Browsers abgelegt werden, werden damit unschädlich gemacht. Die Datenausführungsverhinderung aktueller Betriebssysteme wendet dieselbe Restriktion im virtuellen Speicher an.

- Antiviren-Software verwenden
  Wenn Daten aus dem Internet oder von Mailservern heruntergeladen oder von Datenträgern kopiert werden, besteht immer die Möglichkeit, dass sich darunter auch schädliche Dateien befinden: Weder Vertrauen noch Antivirenprogramme können aber vor allen schädlichen Dateien schützen: eine vertrauenswürdige Quelle kann selbst infiziert sein, und Antivirenprogramme können neue sowie unbekannte Schädlinge nicht entdecken. Der "normale" Benutzer wiegt sich zudem durch Werbeaussagen wie „bietet umfassenden Schutz gegen alle Bedrohungen“ in trügerischer Sicherheit und wird zu riskanterem Verhalten verleiten.

- Diversifikation
  Eine weitere Maßnahme zur Reduktion der Gefahren besteht in der Diversifizierung von Software, also darin, Software von verschiedenen, auch nicht marktführenden Anbietern zu verwenden. Die Angriffe von Crackern zielen oftmals auf Produkte von großen Anbietern, weil sie bei kriminellen Angriffen damit den größten Gewinn erzielen und ansonsten gegebenenfalls den größten „Ruhm“ erlangen. Insofern kann es ratsam sein, auf Produkte von kleineren und weniger bekannten Unternehmen oder zum Beispiel auf Open-Source-Software zurückzugreifen

- Firewalls verwenden
  Für Angriffe, die ohne das aktive Zutun des Nutzers drohen, ist es unerlässlich eine Netzwerk-Firewall oder Personal Firewall zu installieren. Viele unerwünschte Zugriffe auf den Computer und unbeabsichtigte Zugriffe vom eigenen Computer, die vom Benutzer meist gar nicht bemerkt werden, können auf diese Weise verhindert werden. Die Konfiguration einer Firewall ist nicht trivial und erfordert Kenntnis der Vorgänge.

- Sandkästen
  "Sandboxes" sperren ein potentiell schädliches Programm ein. Im schlimmsten Falle kann das Programm lediglich den Sandkasten zerstören. Beispielsweise gibt es keinen Grund, weshalb ein PDF-Reader auf OpenOffice-Dokumente zugreifen muss. Der Sandkasten wäre in diesem Fall „alle PDF Dokumente und sonst nichts“. Techniken wie AppArmor und SELinux ermöglichen den Bau eines Sandkastens

- Aktive Inhalte deaktivieren
  Bei aktiven Inhalten handelt es sich um Funktionalitäten, die die Bedienung eines Computers vereinfachen sollen. Das automatische Öffnen beziehungsweise Ausführen von heruntergeladenen Dateien birgt jedoch die Gefahr, dass diese schädliche Codes ausführen und den Rechner infizieren. Um dies zu vermeiden, sollten aktive Inhalte, wie zum Beispiel ActiveX, Java oder JavaScript, so weit wie möglich deaktiviert werden

- Sensible Daten verschlüsseln
  Daten, die nicht in Hände Dritter geraten sollen, müssen durch geeignete Maßnahmen, wie z.B. GPG oder Device-Encryption-Software verschlüsselt werden. Dies betrifft Daten, die zwischen zwei Rechnern ausgetauscht werden oder die sich auf Massenspeichern befinden, die sehr sensibel sind (z.B. Kreditkartennummern) und während des Surfens im Internet. Ein Zugriff darf nur möglich sein, wenn die Beteiligten über den richtigen Schlüssel verfügen. Gefährdet sind z.B. unverschlüsselte, kabellose Netze, wie z.B. nicht konfigurierte WLANs, da hier Unbefugte Zugriff auf die Daten und die Kontrolle über den ungeschützten Computer erlangen könnten. Auch für Behörden/Unternehmen ist Datensicherheit, vor allem der Datentransport, ein sensibles Thema. Geschäftsprozesse erfordern die mobile Verfügbarkeit von z.B. Kunden- oder Kontodaten. Bei der Datenaufbewahrung und dem -transport müssen sich Behörden/

Unternehmen auf Sicherheit verlassen können. Gelangen sensible Daten in unbefugte Hände, entsteht meist ein irreparabler Schaden, z.B. wenn die Daten verbreitet oder missbraucht werden. Um dies zu verhindern, müssen neben der Verschlüsselung auch die Zugriffskontrolle und Erstellung, Speicherung und Zerstörung des kryptographischen Schlüssels beachtet werden. Es ist zu beachten, dass immer alle drei Sicherheitskriterien berücksichtigt werden müssen. Hat eines dieser Kriterien eine Sicherheitslücke, so wird dadurch die ganze Sicherheitskette gefährdet. Somit können für den sicheren Datentransport nur spezielle externe verschlüsselte Speichermedien genutzt werden.
Die Wahl einer passenden Verschlüsselung entscheidet über die Grundlage zum Erreichen eines höchsten Maßes an Datensicherheit. Für höchste Anforderungen an Datensicherheit empfiehlt das Bundesamt für Sicherheit in der Informationstechnik, die AES Verschlüsselung mit einer Schlüssellänge von 256-Bit im CBC-Modus zu verwenden. Der CBC-Modus sorgt dafür, dass jeder Block mit einem anderen AES-Schlüssel verschlüsselt wird. So werden bei der Verschlüsselung jedes neuen Sektors auch die Informationen von dem vorher verschlüsselten Block miteinbezogen.
Passwörter, persönliche Identifikationsnummern (PIN) und Transaktionsnummern (TAN) sollten nicht unverschlüsselt gespeichert oder übertragen werden, z.B. auf http: Seiten.

- Laufzeitumgebungen verwenden
  Für die Generierung und Wartung sicherer Software ist es sehr nützlich, schon bei der Softwareentwicklung strukturiert zu programmieren und leicht überschaubare und erlernbare Werkzeuge zu verwenden, die möglichst enggefasste Sichtbarkeitsregeln und gekapselte Programmmodule mit eindeutig definierten Schnittstellen erlauben.[14] Durch eingeschränkte Freiheiten bei der Programmierung, wie zum Beispiel die Beschränkung auf einfache Vererbung oder das Verbot von Zirkelbezügen oder kritischen Typumwandlungen, wird in der Regel zugleich das Potential von Programmfehlern eingeschränkt. Dabei ist es auch sinnvoll und hilfreich, bereits getestete Software durch geeignete Maßnahmen wiederzuverwenden, wie zum Beispiel durch die Verwendung von Prozeduren oder objektorientierten Datenstrukturen.
  Entwickler von Software, die zum sicheren Datenaustausch zwischen Rechnern eingesetzt wird, müssen moderne Entwicklungssysteme und Programmiersprachen einsetzen, da ältere Systeme häufig Sicherheitslücken haben und nicht über die entsprechende Sicherheitsfunktionalität verfügen. Sichere Software ist nur in entsprechenden, modernen und sicheren Laufzeitumgebungen lauffähig und sollte mit Entwicklungswerkzeugen (wie zum Beispiel Compilern) erstellt werden, die ein möglichst hohes Maß an inhärenter Sicherheit bieten, wie zum Beispiel Modulsicherheit, Typsicherheit oder die Vermeidung von Pufferüberläufen.
  Auch bei Geräten, die nicht in einem Rechnernetz beziehungsweise im Internet der Dinge betrieben werden, kann die Informationssicherheit durch geeignete Entwicklungssysteme und Laufzeitumgebungen erhöht werden. Datenverlust durch unzuverlässigen Programmcode (Computerabsturz) kann vorbeugend zum Beispiel durch compilergenerierte Überprüfung von Indizes von Datenfeldern, unzulässigen Zeigern oder nach dem Auftreten von Programmfehlern durch Ausnahmebehandlung in der Laufzeitumgebung vermieden werden. Ferner ist es in objektorientierten Laufzeitumgebungen unerlässlich und auch in anderen Systemen sicherer, eine automatische Speicherbereinigung durchzuführen, damit nicht versehentlich Speicherplatz freigegeben wird.
  Manche Entwickler vertrauen auf die Verifikation von Programmcode, um die Korrektheit von Software zu verbessern. Ferner ist es möglich, bereits implementierte Software durch bestimmte Verfahren, wie zum Beispiel die Verwendung von Proof-Carrying Code, erst während der Laufzeit zu überprüfen und deren Ausführung bei der Nichteinhaltung von Sicherheitsrichtlinien zu verhindern.

- Und nicht zuletzt: Sensibilisierung und Befähigung der Mitarbeiter
  Ein wichtiger Aspekt in der Umsetzung von Sicherheitsrichtlinien ist die Ansprache der eigenen Mitarbeiter, die Bildung von sogenannter IT-Security-Awareness. Hier fordern die ersten Arbeitsrichter den Nachweis der erfolgten Mitarbeitersensibilisierung für den Fall eines etwaigen Verstoßes gegen die Firmenrichtlinien.
  Zusätzliche Bedeutung bekommt diese menschliche Seite der Informationssicherheit außerdem, da Industriespionage oder gezielte, wirtschaftlich motivierte Sabotage gegen Unternehmen nicht allein mit technischen Mitteln ausgeführt werden. Um ihren Opfern zu schaden oder Informationen zu stehlen, nutzen die Angreifer beispielsweise Social Engineering, das nur abzuwehren ist, wenn die Mitarbeiter über mögliche Tricks der Angreifer orientiert sind und gelernt haben, mit potenziellen Angriffen umzugehen. Die Mitarbeitersensibilisierung variiert typischerweise von Unternehmen zu Unternehmen von Präsenzveranstaltungen über webbasierte Seminare bis hin zu Sensibilisierungskampagnen.
  Der Fokus verschiebt sich dabei inzwischen von der reinen Sensibilisierung („Awareness“) hin zur Befähigung („Empowerment“) der Anwender, eigenverantwortlich für mehr Sicherheit im Umgang mit IT-gestützten Informationen zu sorgen. In Unternehmen kommt dabei dem „Information Security Empowerment“ der Führungskräfte besondere Bedeutung zu, da sie Vorbildfunktion für ihre Abteilungsmitarbeiter haben und dafür verantwortlich sind, dass die Sicherheitsrichtlinien ihres Verantwortungsbereiches zu den dortigen Arbeitsabläufen passen – eine wichtige Voraussetzung für die Akzeptanz.

3 Datenschutz ist Personenschutz

Beim Datenschutz geht es nicht um den Schutz von allgemeinen Daten vor Schäden, sondern um den Schutz personenbezogener Daten vor Missbrauch
Der Schutz personenbezogener Daten stützt sich auf das Prinzip der informationellen Selbstbestimmung. Geschützt werden muss dabei die Privatsphäre, d. h. Persönlichkeitsdaten bzw. Anonymität müssen gewahrt bleiben. Datenschutz verlangt über die Datensicherheit hinaus den Ausschluss des Zugangs zu Daten mit unberechtigtem Lesen durch unbefugte Dritte.

3.1 Die sog. Datenschutz-Grundverordnung (DSGVO)

Die DSGVO gilt ab 25. Mai 2018 unmittelbar in allen Staaten der Europäischen Union.

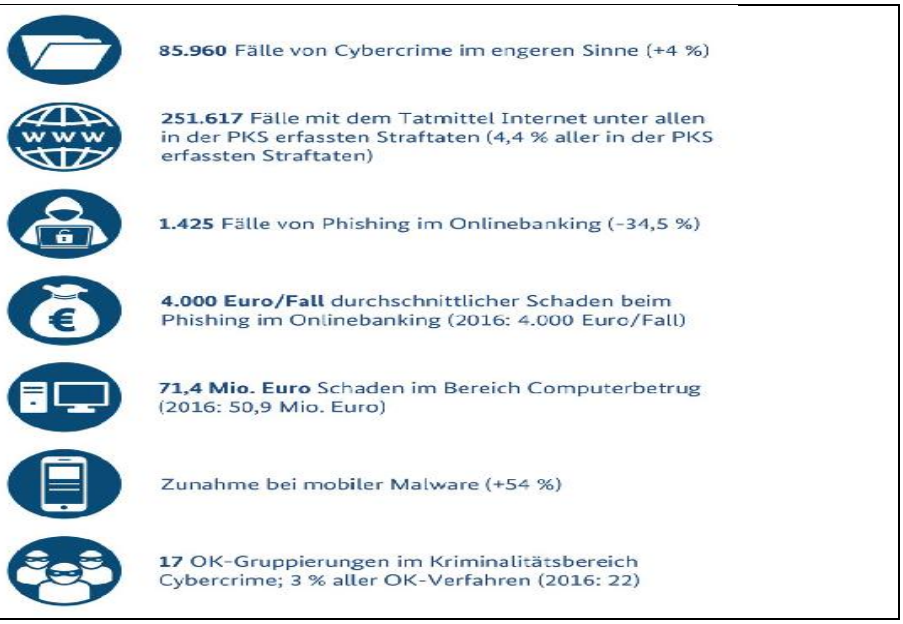
- "Personenbezogene Daten"?
  Auch in dieser Neuregelung bleibt, wie schon beim BDSG, der Begriff der „personenbezogenen Daten“ im Artikel 4 weiterhin weit gefasst: „Personenbezogene Daten“ [sind] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann; …

- "Verarbeitung" personenbezogener Daten
  Weiterhin gilt, dass die Verarbeitung personenbezogener Daten nur aufgrund eines Erlaubnistatbestands zulässig ist. Diese sind im Artikel 6 aufgeführt:
  - Die betroffene Person hat ihre Einwilligung gegeben;
  - die Verarbeitung ist für die Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen erforderlich;
  - die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich;
  - die Verarbeitung ist erforderlich, um lebenswichtige Interessen zu schützen;
  - die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt;
  - die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich. Im letzten Fall ist eine Interessensabwägung gegenüber den Interessen der betroffenen Person erforderlich.

- Die DSGVO führt im Artikel 5 explizit folgende sechs Grundsätze für die Verarbeitung personenbezogener Daten auf:
  - Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
  - Zweckbindung (Verarbeitung nur für festgelegte, eindeutige und legitime Zwecke)
  - Datenminimierung („dem Zweck angemessen und erheblich sowie auf das […] notwendige Maß beschränkt“)
  - Richtigkeit („es sind alle angemessenen Maßnahmen zu treffen, damit [unrichtige] personenbezogene Daten unverzüglich gelöscht oder berichtigt werden“)
  - Speicherbegrenzung (Daten müssen „in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es […] erforderlich ist“)
  - Integrität und Vertraulichkeit („angemessene Sicherheit der personenbezogenen Daten […], einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung“)

Der Verantwortliche muss die Einhaltung der Grundsätze nachweisen. Die Nichteinhaltung dieser Grundsätze und der Rechenschaftspflicht kann mit einem "angemessenen" Bußgeld in Höhe von bis zu 20 Millionen EUR oder im Fall eines Unternehmens von bis zu 4% seines gesamten weltweit erzielten Jahresumsatzes geahndet werden (Art. 83 Abs. 5a).

3.2 Speziell: Cybercrime

Etwas Statistik - Zum Umfang der Cyber-Kriminalität: Das Bundeskriminalamt hat 2017 eine Statistik zu Cyber-Kriminalität veröffentlicht.	

Eine andere Aussage der BitKom, die aber wg. der geringen Anzahl der Befragten (1017 Personen) nicht repräsentativ ist: Jeder zweite deutsche Internetnutzer (49 Prozent) ist in den vergangenen zwölf Monaten Opfer von Cybercrime geworden. Tatsächlich liegt die Zahl eher bei 30% (lt. BKA 2015).

Interessant ist aber die Verteilung:
- 43% wurden mit Schadprogrammen wie Viren infiziert
- 19% wurden die Zugangsdaten zu Online-Diensten wie Sozialen Netzwerken oder Online-Shops gestohlen,
- 16% beim Online-Shopping oder Online-Banking betrogen worden.
- Bei 8% wurden persönliche Daten illegal genutzt
- 8% berichten von massiven Beleidigungen bis zu Stalken, Mobben oder sexueller Belästigung im Netz.

… und die Folgen und Schritte:
- 54% ist dabei ein finanzieller Schaden entstanden.
  Nur 28% haben wegen des Angriffs einen IT-Experten hinzugezogen
- 16% haben Waren bezahlt, die nicht angekommen sind oder für privat online verkaufte Waren kein Geld erhalten haben.
  Nur 8% haben einen Rechtsanwalt eingeschaltet,
- 4% haben fremde finanzielle Transaktionen auf ihrem Konto oder mit ihrer Kreditkarte festgestellt

Die Bereitschaft, eine Versicherung gegen finanzielle Schäden durch Cybercrime abzuschließen, ist allerdings gering: Nur 6% sagen, dass sie auf jeden Fall eine solche Police abschließen werden oder bereits einen entsprechenden Schutz besitzen und 13% können sich vorstellen, künftig eine solche Versicherung abzuschließen.

3.3 Das Darkweb ist nicht illegal!

Das Darkweb, auch fälschlicherweise als Darknet bezeichnet, beschreibt in der Informatik ein Peer-to-Peer-Overlay-Netzwerk, dessen Teilnehmer ihre Verbindungen untereinander manuell herstellen. Dieses Konzept steht im Gegensatz zu konventionellen Peer-to-Peer-Netzwerken, bei denen zumeist die Verbindungen zu den Clients fremder Personen automatisch und willkürlich initiiert werden.
In einfachen Worten ausgedrückt: Es gibt im Darkweb keine feste IP-Adresse, sondern die eigene, ursprüngliche IP-Adresse wird durch andere Rechner ersetzt mit einer neuen IP-Adressen.

Das Darkweb ist damit Bestandteil des "normalen" Web und kein eigenes "Net".

Der Zugang über einen Tor-Browser ist nicht verboten (wie gerne in den Medien dargestellt) und bietet ein höheres Maß an Sicherheit, da einem Angreifer der Zugriff auf das (eigene) Netzwerk nicht ohne weiteres möglich ist – oder er im Idealfall gar nichts von der Existenz des Netzwerks weiß.

Um neue Personen in Gruppen oder Plattformen zu integrieren, müssen diese gewöhnlich von anderen Teilnehmern eingeladen oder akzeptiert werden. Eine Teilnahme kann auch nur über Privilegien möglich sein.

Aufgrund der Eigenschaften des Darkwebs, sog. "onion"-Webseiten zu erstellen, due nur über das Darkweb aufgerufen werden können, bietet es tiefgreifende Möglichkeiten für kriminelle Aktivitäten, hier etwa die häufig betonten Drogen- oder Waffengeschäfte.

Es gibt viele Studien über den Anteil der illegalen Dienste, eine Anfang Februar 2016 veröffentlichte Studie des britischen "Thinktanks International Institute for Strategic Studies" stufte diesen bei 57% von 5205 untersuchten aktiven Seiten im Darknet inhaltlich als „illegal“ ein. Jedoch sind auch diese Studien nicht repräsentativ, da es keine Möglichkeit gibt überhaupt festzustellen, wie viele onion-Seiten im Darkweb existieren. Zudem wird nicht berücksichtigt, dass auch "normale" Seiten illegal im Darkweb bedient werden.
Kriminalistische Schätzungen gehen auf einen Anteil der Illegalität von 30%, wie also auch beim normalen Internet.

Der legale Anteil der Darkweb-Nutzung liegt im anonymen Besuchen von Webseiten des Internets, den Hidden Services wie Mailboxen und Foren und speziellen Informationsplattformen für Journalisten, Menschenrechts-organisationen, Whistleblowern oder politisch Verfolgten
Und ein Netz ohne Zensur, Nachverfolgung und Überwachung hat nicht nur Vor-, sondern eben auch Nachteile.

4 RPA und KI - Die neue digitale Kompetenz

Die Zukunft der Versicherung ist digital. Kunden wollen Waren, Informationen und Dienstleistungen jederzeit und überall auf Knopfdruck erhalten. Dazu sind klassische Versicherungsunternehmen aber noch nicht in der Lage. Kunden wollen Produkte und Dienstleistungen - auch Versicherungen - einfach mit dem mobilen Endgerät ordern und verwalten. Darauf sind klassische Versicherungskonzerne oft nicht gut vorbereitet.

Stellen Sie sich vor, Sie fahren auf der Autobahn, als ausgerechnet in einer Baustelle Ihr Hintermann zu dicht auffährt und Ihre Stoßstange rammt. Zum Glück ist es nur ein Blechschaden.
Der Schadensverursacher macht schnell ein paar Fotos per Smartphone und schickt diese gemeinsam mit Ihren Kontaktdaten an seinen KfZ-Versicherer. Wenige Minuten später hat das System bereits die Kosten grob geschätzt und gibt die Reparatur in einer Werkstatt Ihrer Wahl frei - ohne polizeiliche Unfallaufnahme, lange Staus auf der Autobahn und speziellen Gutachter. Sie erhalten per E-Mail die Nummer, unter der der Schaden bearbeitet wird. Ein Foto der Rechnung ein paar Tage später reicht aus, und Sie erhalten den Schadensbetrag binnen 24 Stunden auf Ihr Konto erstattet.

Papierbasierende Prozesse sind noch die Regel
Das Potenzial ist enorm - gerade in einer daten- und informationsgetriebenen Branche wie dem Versicherungswesen. Doch die Realität sieht anders aus. Papierbasierende Prozesse sind eher die Regel als die Ausnahme. Vieles wird immer noch manuell erledigt. Das ist zeitintensiv und bindet viele Mitarbeiter, die sonst andere Aufgaben erledigen könnten.

Die Gründe für den geringen Digitalisierungsgrad in der Versicherungsbranche sind vielfältig:
Erstens verlangt das Versicherungsaufsichtsgesetz (VAG), dass Lebensversicherungen, Krankenversicherungen sowie Schaden- und Unfallversicherungen in **rechtlich eigenständigen Unternehmen** betrieben werden. Das hat zur Folge, dass **ein Kunde innerhalb eines Konzerns in unterschiedlichen IT-Systemen geführt** wird, die teilweise nicht imstande sind, Daten untereinander auszutauschen.

Zweitens hat **Fusionitis hat zu heterogener IT geführt:** Der Kosten- und Wettbewerbsdruck hat in den vergangenen Jahren dazu geführt, dass kleinere Versicherungsunternehmen von den "Großen" aufgekauft wurden.
So waren laut Bafin im Jahr 2017 insgesamt 528 Versicherungsunternehmen in Deutschland operativ tätig, knapp **15 Prozent weniger** als zehn Jahre zuvor. Das Ergebnis ist auch hier ein **Flickenteppich unterschiedlicher IT-Software und Hardware mit vielen Schnittstellen**, die nicht kompatibel sind. Veraltete IT-Systeme aus dem 1990er Jahren erschweren zusätzlich eine Systemintegration.

Drittens kämpfen etablierte Versicherer mit **festgefahrenen Denkweisen und Konkurrenz von innen**. Konzerne wie die Allianz, die mit eigenen Versicherungsvertretern arbeiten, haben es deutlich schwerer, gleichzeitig eine digitale Direktversicherung anzubieten, sie würde in Konkurrenz zum eigenen Vertriebskanal stehen. **Lange Entscheidungswege** und starre Hierarchien tun ihr Übriges, um die Einführung digitaler Lösungen auf die lange Bank zu schieben.

Die Folge: Die wenigsten Versicherer besitzen ein modernes IT-System, das es ihnen erlauben würde, Kundendaten über die gesamte Vertragslaufzeit und alle Schnittstellen zu bündeln. Sie verfügen also nicht über ausreichend hochwertige und korrekt klassifizierte Trainingsdaten, anhand derer die Algorithmen lernen können.

RPA ist ein wichtiger Zwischenschritt
Als Zwischenschritt setzen viele Versicherungsunternehmen heute auf robotergestützte Prozessautomatisierung, kurz Robotic Process Automation (RPA). Im Unterschied zur klassischen Automatisierung in Fertigungsanlagen kommen hier keine physischen, sondern virtuelle Roboter zum Einsatz, die bislang manuell bearbeitete, repetitive Aufgaben eigenständig erledigen. **Dabei ahmen die Software-Roboter menschliche Tätigkeiten am Computer nach**; eine aufwändige Systemintegration ist nicht notwendig.

Die Vorteile der Technologie sind offensichtlich: Die Software-Bots lassen sich problemlos und ohne Programmierkenntnisse in bestehende IT-Landschaften integrieren. Die Prozesse laufen schneller und fehlerfreier, die Kosten sinken. Laut einer Studie der Beratungsgesellschaft Capgemini setzen bereits über 40 Prozent der Unternehmen RPA ein.

Besonders geeignet ist RPA für häufig wiederkehrende, strukturierte Tätigkeiten, die festen Regeln folgen. So können Software-Roboter die Migration großer Datenmengen, den Abschluss von Neuverträgen oder die Anpassung von Bestandspolicen beschleunigen. Allerdings arbeiten Software-Roboter ausschließlich deterministisch und sind auf einfache Arbeitsprozesse beschränkt. **Sie sind nicht in der Lage, flexibel auf Abweichungen zu reagieren**, beispielsweise wenn Daten unvollständig oder fehlerhaft eingegeben werden.

KI lernt selbständig
Vielversprechender ist hier der Einsatz künstlicher Intelligenz. KI bezeichnet dabei Computer, die in der Lage sind, mehr oder weniger stark assistiert und mehr oder weniger **selbständig Probleme zu lösen und aus "Erfahrung" lernen**, ohne dass vorab bestimmte Regeln vorgegeben werden.

So kann KI weit mehr als typische Prozesse wie den Abschluss von Policen oder die Abwicklung von Schadensfällen zu beschleunigen. Sie wird sowohl zu einer **genaueren Bewertung von Risiken** als auch zu **personalisierten Produkten** führen. Je genauer Versicherer über ihre Kunden Bescheid wissen, desto stärker können sie Risikoprofile verfeinern, Preise anpassen und maßgeschneiderte Angebotspakete schnüren.

Perspektivisch **hilft KI in Kombination mit Sensoren und intelligenten Geräten auch bei der Prävention**. In der Industrie werden Maschinen bereits gewartet, bevor es zu teuren Stillständen in der Produktion und Fertigung kommt. Telematik-Tarife in der Kfz-Versicherung belohnen einen umsichtigen Fahrstil. Dabei zeichnen technische Hilfsmittel wie eine mit Sensoren ausgestattete Box oder eine Smartphone-App das Fahrverhalten des Autobesitzers auf.

5 "use cases": Typische digitale Anwendungsbereiche in der Versicherungspraxis

Nachfolgend finden Sie neun aktuelle Trends für den Einsatz von Big Data durch den Data Scientist.

5.1 Predictive Analytics - Simplified Underwriting

Die Vereinfachung des Policierungsprozesses.

Eine zeit- und entsprechend kostenintensive Arbeit beim Abschluss einer Versicherung stellt die **Risikoprüfung** dar: Hier sind sehr detaillierte Informationen nötig, die bisher noch mit umfangreichen, teils improvisierten Fragebögen gesammelt werden. Je nach Versicherungsart handelt es sich dabei auch um langwierige sowie kostenintensive Prozesse, z.B. Abfrage von Vorerkrankungen und medizinische Untersuchungen bei Kranken- und Pflege(zusatz-)versicherung.

Eine **Kategorisierung der Kunden** schafft hier Effizienz: Low-Risk-Kunden werden in Zukunft mit prädiktiven Algorithmen anhand von umfangreichen Profil- und Verhaltensdaten identifiziert. Diesen Kunden kann damit ein vereinfachter Prozess zur Risikoprüfung angeboten werden. Durch diese Maßnahme werden sowohl die Customer Experience als auch die internen Prozesse verbessert.

5.2 Customer Clustering

Ein besseres Verständnis der verfügbaren Daten zur optimalen Kundenidentifikation

Ein wichtiges Element bei einer gezielten und optimierten Kundenansprache stellt die **Identifikation der vorhandenen, relevanten Kundengruppen** dar. Dabei bereitet vor allem die Ermittlung der Kriterien einer sinnvollen Kundensegmentierung für Vertriebs- und Marketingzwecke Schwierigkeiten.

In diesem Fall können zum einen fortgeschrittene Kalkulationstechniken wie die Pivot / Cube-Funktionalität oder sogenannte "Unsupervised Machine Learning" -Techniken eingesetzt werden.
Dabei erkennt ein Algorithmus Gemeinsamkeiten in großen Datensätzen, ohne dass ihm bestimmte Zielwerte vorgegeben werden.

Dafür wird eine **Kombination aus Bestandsdaten und externen Daten** verwendet, in denen Gemeinsamkeiten erkannt und gruppiert werden sollen (Clustering). Die Ergebnisse dieses Prozesses führen zu einer Kundensegmentierung, die dazu genutzt werden kann, die jeweilige Kundengruppe optimal anzusprechen.

5.3 Life-Changing Events / Customer Lifetime Value

Steigerung der Vielfalt an Lebensversicherungen durch Bedarfsprognosen
Versicherungsprodukte begleiten den Kunden ein Leben lang

Lebensversicherungen werden in sehr unregelmäßigen Intervallen gekauft - ggf. eben nur einmal im Leben. Hinzu kommen anhaltende Niedrigzinsphasen, die diese Art der Versicherung unattraktiv machen.
Umso wichtiger wird es für Versicherer, die Lebensversicherung attraktiv zu gestalten die entscheidenden Momente im Leben zu erkennen, in denen eine Lebensversicherung interessant wird.

Die Kaufentscheidung erfolgt häufig nach lebensverändernden Ereignissen wie das Erreichen eines bestimmten Alters, Heirat oder Geburt eines Kindes. **Kundenbezogene Lebensdaten**, wie sie etwa in Social-Media-Daten oder der Verkaufshistorie verfügbar sind, ermöglichen eine genaue Vorhersage dieser Ereignisse. So können kundenindividuelle Bedarfsprognosen erstellt und Kunden gezielt mit entsprechenden Angeboten beworben werden.

Es ist eine Binsenweisheit, dass sich unser Leben schnell und gravierend ändern kann: Aktuell ändern sich die Lebensumstände massiv. Kaum jemand der jüngeren Generation wird ein Leben lang einen einzigen Beruf oder ständig dieselbe Verantwortung ausüben. Zu einer schwierigen Herausforderung wird dieser Umstand dann, wenn Versicherungen Produkte anbieten, die ihre Kunden ein Leben lang begleiten. Umso wichtiger ist es heute, Kundenpotenziale für die gesamte Lebensdauer zu bewerten.

Die Berechnung des Customer Lifetime Value hilft Versicherungen in dieser Situation: Kundenspezifische Profile ermöglichen die **Schätzung des Kundenwerts** und rechtfertigen **Investitionen in deren langfristige Bindung**.
Dabei reichen Bestandsdaten nicht aus, um solche Profile zu bilden, es müssen externe Datenressourcen herangezogen werden, um die Daten entsprechend anzureichern. So gelingt eine exakte Kundenbewertung anhand von genaueren Datenauswertungen.

5.4 KI-unterstütztes Claim Management

Bewertungsunterstützung von Versicherungsansprüchen.

Die Bewertung setzt Informationen aus heterogenen, teilweise analogen Kundendokumenten voraus. Das stellt Versicherer vor zwei Herausforderungen: Die zeitintensive Analyse der Unterlagen und deren Digitalisierung.

Eine Lösung dieses Problems ist der **Einsatz Künstlicher Intelligenz (KI)**, genauer gesagt, der Einsatz maschinellen Lernens. Lernfähige Erkennungsalgorithmen helfen Versicherungen dabei, Dokumenttypen zu klassifizieren und besonders wichtige Abschnitte zu identifizieren.

Digitale Bildverarbeitung und Texterkennung erschließen zudem ein großes Automatisierungspotenzial, wenn es um die Auswertung von analogen Dokumenten geht. KI-unterstützte Algorithmen im Claim Management führen damit zu einer größeren Effizienz im Nachforderungsmanagement.

5.5 Second Medical Opinion

Durchschnittlich 15% – 20% aller Diagnosen sind falsch.

Durch die großen Fortschritte im Bereich der künstlichen Intelligenz in den letzten Jahren können künftig Fehldiagnosen reduziert werden, da intelligente Algorithmen in wenigen Minuten viele Millionen Fälle miteinander vergleichen oder Bild- und Textdatenbanken mit existierenden Diagnosen einbeziehen.
Ärzte können in Zukunft ihre Diagnosen mit Big Data-Ergebnissen untermauern oder überprüfen lassen. Patienten steht auf diese Weise die Möglichkeit zur Verfügung, mit geringem Aufwand eine zweite Meinung einzuholen. Dadurch steigt die Sicherheit, rechtzeitig die richtige Diagnose zu erhalten.

Dies bedeutet für Versicherungen ein enormes Einsparpotenzial: Nicht nur die Anzahl von Fehlbehandlungen können durch den Einsatz von KI reduziert werden, sondern auch die damit verbundenen Rechtsstreitigkeiten und Schadensersatzforderungen werden drastisch reduziert.

5.6 Das Smart-Home-Konzept

Früherkennung von Schäden für ein stimmiges Sachversicherungspaket

Neben Komfort und Energieeinsparung die Sicherheit in einem Smart Home das wichtigste Argument für Kunden.

Das stellt für Versicherungen eine große Chance dar: Sie können Hausüberwachungsdienste mit Wohngebäude-versicherungen bündeln und ihren Kunden so ein umfassendes Gesamtpaket anbieten, da ungewöhnliche Ereignisse und Auffälligkeiten über Sensordaten dann identifiziert und im besten Fall sogar vermieden werden, wenn Sie vom regelmäßigen Muster abweichen.

So kann das Auftreten eines Wasserschadens frühzeitig indiziert werden, wenn der Druck und Wasserdurchfluss über Sensoren erfasst wird. Ein Schaden an der Leitung, der ein permanentes oder großes Austreten von Wasser zur Folge hat, kann somit schnell erkannt und ein Wasserschaden vermieden werden.
Darüber hinaus können Versicherungen ihren Kunden eine mobile App anbieten, die den Kunden über das Schadensrisiko, wie zum Beispiel durch bestimmte Wetterereignisse oder einen eingeschalteten Herd, informiert.

Individuelle Zusatzversicherungen können in diesem Rahmen angeboten werden und die erste Kommunikation in einem Schadensfall kann direkt über die App laufen. Die Möglichkeiten, den Kunden zusätzliche Serviceangebote anzubieten, sind vielfältig: Ebenso denkbar sind „Assistance Services“ wie der automatisierte Anruf bei einem Reparaturservice, wie mittlerweile im Kfz-Bereich angeboten.

5.7 Telematik-Tarife sparen Geld

Der Fahrstil entscheidet über die Höhe der Kfz-Versicherung

In einem "Smart" oder "Connected" Car sind zahlreiche Sensoren verbaut, die unter anderem Aufschluss über den **Fahrstil des Fahrers** geben. Auch ältere Fahrzeuge lassen sich mithilfe einer Box, die entsprechende Daten liefert, zu einem vernetzten Auto aufrüsten.

Bei Telematik-Tarifen erklären Versicherte sich dazu bereit, **Daten über ihr Fahrverhalten an eine Versicherung zu übermitteln**. Diese wiederum bietet vergünstigte Tarife oder Prämien an, sollten die Daten auf ein entsprechend sicheres Fahrverhalten verweisen. Dazu werden beispielsweise Faktoren wie Einhaltung der Höchstgeschwindigkeiten sowie das Brems- und Beschleunigungsverhalten beurteilt, aber auch andere Faktoren wie die Nutzungs- und Standzeiten einbezogen.

Besonders **Fahranfänger**, die aufgrund ihrer Risikogruppe höhere Beiträge bezahlen müssen, können von Telematik-Tarifen profitieren – sogar in doppelter Hinsicht. Einerseits sinken ihre Beiträge, wenn sie ihre Daten an die Versicherung übermitteln. Andererseits gewöhnen sie sich einen sicheren Fahrstil an und tragen somit insgesamt zur Steigerung der Sicherheit des Straßenverkehrs bei.

5.8 Healthy-Living und FrailtyCare - Konzepte

Gesundheitsversorgung und Krankenversicherung basieren auf neuen Technologien und Datenanalysen.

Hier werden Gesundheitsversicherung und krankheitspräventiven Dienstleistungen kombiniert: Technologie und Data Science gehen dabei Hand in Hand: Fitness-Tracker beispielsweise generieren **biometrische Daten**, deren Analysen Aufschluss über den Gesundheitszustand seiner Träger gibt.

Wearables können beispielsweise auch registrieren, ob sich ein Patient lange nicht bewegt hat und liefert so einen Indikator über dessen gesundheitliches Befinden. In diesen Zusammenhang reiht sich auch das Frailty-Care-Konzept ein, bei dem die **Gesundheitsversorgung von älteren, gebrechlichen oder schwachen Menschen** im Fokus steht.

Medizinische Geräte und Sensoren liefern auch hier die Grundlage für Ferndiagnosen. Sobald ein potenziell gesundheits- oder sogar lebensgefährliches Ereignis eintritt oder sich auch nur anbahnt, können diese Werte nicht nur registriert, sondern präventiv Gegenmaßnahmen ergriffen werden, wie ein Signal auslösen, welches das zuständige Pflegepersonal, Angehörige oder Ärzte informiert.

6 Data Analytics / Data Mining - Massendatenanalyse zur Effizienzsteigerung

"Data Analytics" und "Big Data" sind Begriffe, die sich in den letzten Jahren in den Medien sowie auf Konferenzen und Seminaren des Versicherungssektors einer großen Beliebtheit erfreuen.
Damit immer verbunden ist die Aussicht auf erhebliche Kostenersparnisse und die Erhöhung des Prämienvolumens als ideale Lösung, um den derzeit schwierigen Marktbedingungen erfolgreich zu begegnen.
Unter **Data Analytics** wird die über das klassische Reporting/Monitoring hinausgehende **Massendatenanalyse** verstanden, die auf Grundlage unternehmensinterner oder -externer Daten unabhängig von Quelle, Struktur oder Volumen durchgeführt wird. Diese Analysen erfolgen üblicherweise unter Anwendung von Methoden aus der Mathematik oder Informatik, etwa Statistik und Data Mining und werden zur Entscheidungsfindung im operativen oder strategischen Unternehmenskontext verwendet.

Data Analytics wird als ein geeignetes **Werkzeug zur Effizienzsteigerung** etwa durch Digitalisierung und zur Erweiterung der Prämienbasis erachtet.
Zugleich wird Data Analytics auch als strategisches Merkmal gesehen, um sich von den Mitbewerbern zu differenzieren. Eine der größten Herausforderungen ist das derzeitige Niveau der Datenqualität bei Versicherungsunternehmen (im Gegensatz zu Google, amazon & Co.).

Die Bedeutung einer guten Datenqualität sollte im Unternehmen klar werden, z.B. für Kundendaten (für Vertrieb, Betrieb, Schaden), statistische Daten für die Produktentwicklung und die Prämienkalkulation (u.a. für Telematiktarife) Statistische Daten für das Risikomanagement, Controlling, Rechnungswesen/Kostenrechnung, Kapitalanlagen, Solvency II, …

Im Hinblick auf Google oder amazon sollten auch die wesentlichen Unterschiede (z.B. die Freiwilligkeit / Unbekümmertheit der Kunden im Umgang mit ihren Daten, aber auch die Frage, wem gehören die Daten eigentlich?) aufgeworfen werden.

Typische konkrete Aufgaben für den Einsatz von Data Analysis:

- "Entwickeln Sie eine komplette Social Media-Strategie, bei der die einzelnen Schritte (Idee, Kriterien, Analyse, Entscheidung, Planung, Präsentation, mögliche Umsetzung) klar erkennbar sind; idealerweise erstellen Sie einen Prototyp (mindestens aber eine Präsentation)".
  Es reicht nicht aus, einfach zu entscheiden, „Wir bauen eine Facebookseite“, sondern es wird z.B. begründet, für welche Kunden, welche Produkte, mit welchen Inhalten dies geplant wird, wer die Verantwortung für Inhalt und Pflege hat, wie man den Kunden ansprechen möchte und welche sonstigen (u.a. rechtlichen) Rahmenbedingungen beachtet werden müssen.
- Der Vorstand erteilt die Aufgabe, ein neues Versicherungsprodukt zu entwickeln, welches ausschließlich digital vertrieben werden soll.
- Mitarbeiter haben die Aufgabe erhalten, einen 24-Stunden-Schadenservice einzurichten, welches online unterstützt und bei den Kunden bekannt gemacht werden soll.