Vortrag

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Ulrich Kelber

„Keynote – „Informieren, sensibilisieren, beraten – Aufgaben des Datenschutzes gegen internetbasierte Straftaten“

beim 12. Bonner Dialog für Cybersicherheit „Identitätsdiebstahl, Doxing, Datenschutz“

Uni Bonn (Campus Poppelsdorf, Hörsaal 2)
Endenicher Allee 19c, 53115 Bonn,
04. Juli 2019 – 17:30 bis 18:00 Uhr

Es gilt das gesprochene Wort

Sehr geehrter Prof. Meier,

sehr geehrte Partner des Bonner Dialoges für Cybersicherheit,

sehr geehrte Damen und Herren!

Vielen Dank für die Einladung zum 12. Bonner Dialog für CS. Ich freue mich, die Keynote sprechen zu dürfen.

Bonn ist genau der richtige Ort für eine solche Veranstaltung. Bonn ist „IT-Hotspot“ in Deutschland mit großen digital affinen Unternehmen und Behörden wie der Telekom, der Post, der Postbank, aber natürlich auch mit dem BSI, der Bundesnetzagentur, dem Bundeskartellamt, Steuerbehörden, IT-Zentren, dem BfJ, dem Kommando Cyber- und Informationsraum sowie meinem Haus, dem BfDI. (Aktuell arbeiten wir mit einer knapp 180 Personen starken Besatzung in Bonn und werden weiter wachsen.)

Gleichzeitig gibt es rege Forschung im IT-Sicherheitsbereich z.B. an der Uni Bonn, der Hochschule Bonn/Rhein-Sieg und der Fraunhofer Gesellschaft. Dieser Schwerpunkt zeigt sich nicht zuletzt im Cyber Security Cluster Bonn.

Schon in meiner Zeit als Bonns Bundestagsabgeordneter war es mein Ziel, die Förderung und Vernetzung von Wissenschaft, Forschung & Lehre, Wirtschaft, Behörden, öffentlichen Institutionen und „normalen“ Bürgern zu unterstützen, aktuelle Themen gemeinsam zu diskutieren und zukunftsorientiert zusammenzuarbeiten. Das Cyber Security Cluster Bonn ist das beste Beispiel für eine solche fruchtbare Zusammenarbeit, deshalb bin ich der Einladung besonders gerne gefolgt.

Datendiebstahl, Identitätsdiebstahl, Doxing, Datenleaks und wie wir die Kontrolle über unsere Daten erhalten (oder zurückerhalten) ist das Thema des heutigen Abends. Da macht es Sinn, sich zunächst einmal anzuschauen, was denn die häufigsten Straftaten im Internet sind.

Nach der Internetseite e-recht24.de[1] sind die häufigsten Straftaten im Internet bzw. mittels des Internets begangen:

1. **Betrug**
2. **Beleidigung, üble Nachrede und Verleumdung** (vor allem im Bereich der Sozialen Netzwerke)
3. **Verletzung des Rechts am eigenen Bild**
4. **Urheberrechtsverletzung**
5. (und das kommt jetzt vielleicht ein wenig überraschend, aber passt zur Jahreszeit) **Wohnungseinbruch** (Grüße aus dem Urlaub!, falsche Privatsphäreneinstellungen, IoT??? …)

[1] https://www.e-recht24.de/news/strafrecht/11001-checkliste-die-haeufigsten-straftaten-die-mithilfe-des-internets-begangen-werden.html

Laut einer Studie des Bitkom aus 2017[2]

- kommen Angriffe mit Schadprogrammen, Identitätsdiebstahl und Betrug am häufigsten vor
- erstattet aber nur jeder sechste Betroffene Anzeige
- gibt es nur ein geringes Interesse an Versicherungen gegen Cyberkriminalität

In der im Oktober 2017 veröffentlichten Studie berichtet der BITKOM, dass ca. jeder zweite Internetnutzer in Deutschland bereits Geschädigter von Cybercrime geworden sei, aber nur 18% dieser Geschädigten haben Anzeige bei der Polizei oder Staatsanwaltschaft erstattet.

Das wird uns sicher gleich in der Diskussion noch beschäftigen, denn offensichtlich haben viele Geschädigte nicht das Gefühl, dass eine Anzeige erfolgreich sein könnte, also ihnen zu Rückzahlungen verhilft oder zur Verhaftung von Tätern führt.

[2] https://www.bitkom.org/Presse/Presseinformation/Cybercrime-Jeder-zweite-Internetnutzer-wurde-Opfer.html

Gleichzeitig fehlt hier neben den Straftaten noch ein ganz wichtiger Bereich, das sind die großen „Datenkraken“ wie Amazon, facebook, Google mit samt ihren Tochterunternehmen oder kleineren Konkurrenten. Diese sammeln unsere Daten und Daten über unser Verhalten und Daten über unsere Aktivitäten in kaum vorstellbarer Menge, kombinieren, lokalisieren und werten sie aus, um sie dann teuer in Form von personalisierter Werbung, Score-Werten u.ä. zu verkaufen.

Das tun sie aus der eigenen Sicht legal, weil sie sich vor der Nutzung ihrer Dienste zumeist eine globale Erlaubnis eingeholt haben oder andere über Tracker und ähnliches die Daten sammeln lassen. Dabei entstehen nicht nur gefährliche Datensammlungen über uns alle als Individuen und damit auch über die Gesellschaft getreu des Mottos „Datensatz ist Datenmacht“.

Datensammlungen, die übrigens wegen der daraus resultierenden Vorhersehbarkeit, ihrer Dauerbeobachtungen und ihrer möglichen Entsolidarisierungsbeförderung ein Sprengsatz für eine freiheitliche Gesellschaft sind.

Diese Datensammlung sind auch ein attraktives Ziel von Kriminellen und fragwürdigen Dienstleistungen, die Datenkonzerne lassen dabei oft die notwendige Sorgfalt im Schutz der Daten vermissen.

Ich bin übrigens der Überzeugung, dass diese Datenkonzerne bei großen Teilen ihres Geschäftsmodells gegen die DSGVO verstoßen.

Dass wir noch von keinen spektakulären Strafen gegen einen der Internetriesen wegen des Verstoßes gegen die DSGVO gehört haben, liegt daran, dass wir mit der DSGVO zwar endlich wirksam durchgreifen können. Aber alle Beschwerden gegen Facebook, Apple, Amazon und Google werden zunächst von der irischen und der luxemburgischen Datenschutzbehörde geprüft, weil die Firmen dort ihre europäischen Sitze haben.

Die Kolleginnen und Kollegen dort haben reichlich zu tun, vor allem ein gänzlich anderes Verwaltungsverfahren als wir und wohl auch andere Rechtsauffassungen im Detail. Deshalb wird es leider noch dauern, bis es zu ersten Entscheidungen kommen wird. Diese trifft nicht Irland allein, sondern es wird im europäischen Datenschutzausschuss abgestimmt.

Der gesetzliche Schutz unserer Daten wird dabei nicht allein über das Datenschutzrecht erfolgen können. Das Bundeskartellamt hat Facebook in einer bedeutenden Entscheidung weitreichende Beschränkungen bei der Verarbeitung von Nutzerdaten auferlegt. Andreas Mundt, Präsident des Bundeskartellamtes begründete diese Entscheidung wie folgt:

„*Facebook darf seine Nutzer künftig nicht mehr zwingen, einer faktisch grenzenlosen Sammlung und Zuordnung von Nicht-Facebook-Daten zu ihrem Nutzerkonto zuzustimmen.Die Kombination von Datenquellen hat ganz maßgeblich dazu beigetragen, dass Facebook einen so einzigartigen Gesamtdatenbestand über jeden einzelnen Nutzer erstellen und seine Marktmacht erreichen konnte. Der Verbraucher kann in Zukunft verhindern [gemeint ist nach Umsetzung der Entscheidung], dass Facebook seine Daten ohne Beschränkung sammelt und verwertet.“*

Ich begrüße diese wegweisende Entscheidung ausdrücklich und hoffe sehr, dass die Gerichte, die facebook angerufen hat, die Entscheidung des Kartellamtes bestätigen. Alternativ könnte Herr Zuckerberg, der ja jetzt so gerne über Datenschutz redet, den Einspruch seiner Firma zurücknehmen. Es würde der Glaubwürdigkeit von facebook helfen, sonst bleibt der Verdacht „Talking ist cheap“.

Kriminelle und Datenkonzerne, die die Daten ihrer Nutzerinnen und Nutzer nicht immer ausreichend schützen, führen zu Datendiebstahl und Identitätsklau.

„Identitätsdiebstahl wird zur Regel“[3] hat übrigens schon der 25. Tätigkeitsbericht des BfDI 2013-2014 festgestellt.

Damals, im Jahr 2014 wurde das BSI im Zuge strafrechtlicher Ermittlungen in zwei Fällen über das Aufdecken umfassender Datensätze mit gestohlenen Identitäten informiert.

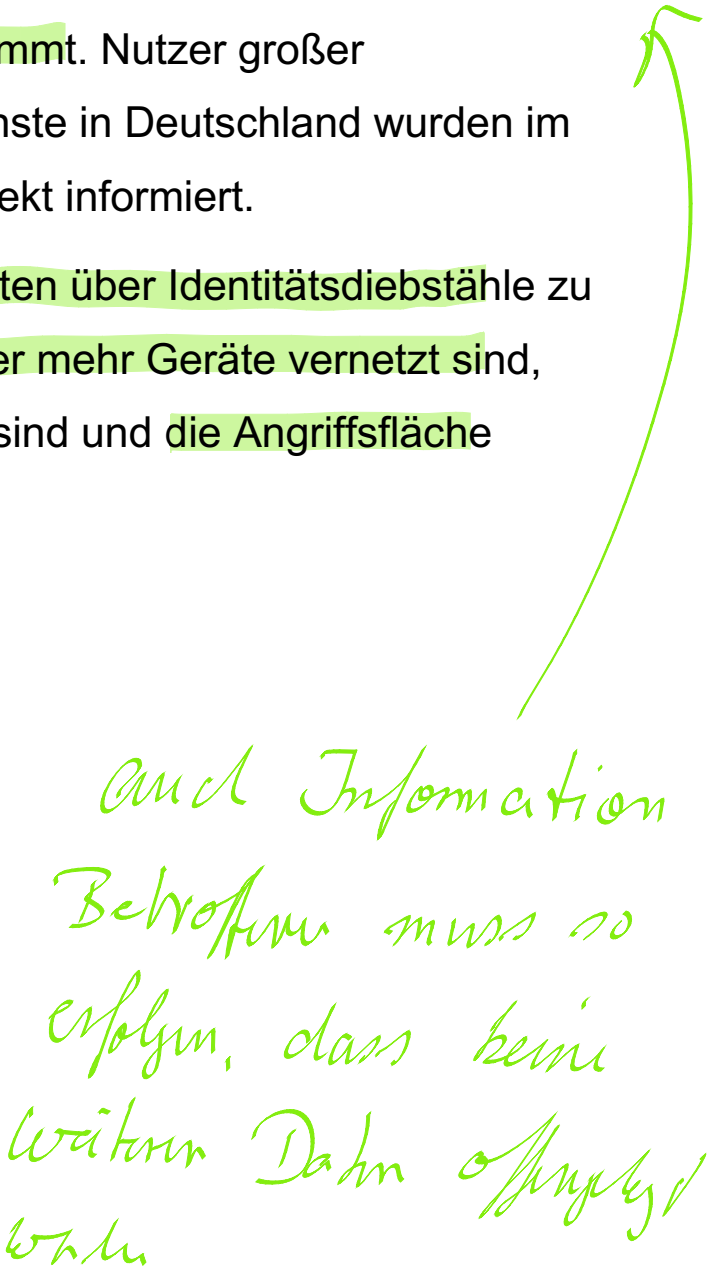
Es handelte sich zum einen um einen Datensatz mit 16 Millionen Identitäten, der bei einer Analyse von Botnetzen durch Forschungseinrichtungen und Strafverfolgungsbehörden gefunden worden war. Im zweiten Fall waren es weitere 18 Millionen Identitäten, die bei Ermittlungen durch die Staatsanwaltschaft im Rahmen eines laufenden Verfahrens gefunden wurden.

[3] 25. Tätigkeitsbericht des BfDI
https://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/25TB_13_14.pdf

Diese Daten wurden dem BSI zur Verfügung gestellt, damit es die Betroffenen entsprechend informiere. Das BSI hat daraufhin einen Warndienst für Internetnutzer zur Abfrage der eigenen Betroffenheit auf einer speziell hierfür vorgesehen Website www.sicherheitstest.bsi.de entwickelt und bereitgestellt.

Wird ein Datum erkannt, so wird der Nutzer mittels einer E-Mail hierüber informiert. Das BSI hat diese Art der Meldeverfahren vorab mit meinem Haus abgestimmt. Nutzer großer Internetprovider und E-Mail-Dienste in Deutschland wurden im zweiten genannten Fall auch direkt informiert.

Zukünftig ist mit weiteren Berichten über Identitätsdiebstähle zu rechnen, allein schon, weil immer mehr Geräte vernetzt sind, immer mehr Daten gespeichert sind und die Angriffsfläche zunimmt.



Auch bei zukünftigen Fällen diesen werden die Anbieter hoffentlich ihre Nutzer entsprechend informieren. Hier ist allerdings zu beachten, dass sich ggf. auch Dritte mit gefälschten Meldungen an Nutzer wenden. Vorsicht ist insbesondere dann geboten, und ich hoffe, das wissen jetzt wirklich nicht nur die interessierten Personen hier im Raum, wenn gefordert wird, die Nutzer solle (weitere) Daten von sich zur Behebung des vermeintlichen Problems preisgeben.

Zum Thema „Sicheres Surfen“ haben wir ein Faltblatt erstellt, dass auf unserer Internetseite www.datenschutz.bund.de abgerufen werden kann, einige Exemplare liegen aber auch aus.

Zu den letzten Datenfunden hat auch das Hasso Plattner Institut in Berlin einen Identitätscheck eingerichtet, mittels dem man testen kann, ob man von den Datenfunden betroffen ist.

Positiv erwähnen möchte ich die Anti-Botnetz-Initiative des eco Verbandes, die zu einem deutlichen Rückgang von infizierten Rechnern in Deutschland geführt hat (Start der Internetseite botfrei.de in 2010). Auch Ermittlungen gegen die Betreiber von Botnetzen waren erfolgreich, wenn gut ausgebildete Mitarbeiterinnen und Mitarbeiter der Sicherheitsbehörden in die Lage versetzt wurden, ihre bestehenden Befugnisse zu nutzen und die Botnetze zu zerschlagen.

Ich sage das vor dem Hintergrund, dass ich befürchte, dass die hyperaktive Diskussion über immer neue Befugnisse der Sicherheitsbehörden, darunter Grundrechtseingriffe, immer neue Straftatbestände und immer höhere Strafen von dieser wichtigen, aber anstrengenderen Arbeit ablenken soll: Ressourcen für die Sicherheitsbehörden und gut ausgebildetes Personal vorzuhalten. Damit die Behörden ihre Arbeit machen können. Das ist nicht schlagzeilenträchtig, aber erfolgsversprechender. Und wertschätzt die Bürgerrechte.

Wie können wir uns vor diesen Gefahren schützen?

Auf Datensicherheit und Datenschutz setzen, vom Anfang bis zum Ende, also vom Bau der Rechner, über die Entwicklung der Software, die genutzte Infrastruktur bis zum Endnutzer. Für alle muss gelten, den Schutz und die Sicherheit der Daten von Anfang an mitzudenken und mitzuentwickeln.

Die Unternehmen sollten dabei die IT-Sicherheit und den Datenschutz nicht als „Kostenfaktor“ sondern vielmehr als „Innovationsmotor„ begreifen. Sie sind Qualitätsmerkmale, mit der man Vertrauen schafft und Wettbewerbsvorteile schafft.
Wer die strengen europäischen Regeln beherrscht und umsetzt, kann damit weltweit punkten und Geschäfte machen.
Deswegen wird es Zeit für Zertifizierungen und Siegel für Produkte und Dienstleistungen, die ein hohes Datensicherheits- und Datenschutzniveau nachweisen können.

IT-Sicherheitsgesetz 2.0 setzt so etwas voraus

DSGVO auch

Wie kann man dabei anfangen?

Datenschutz by default: Z.B. bei allen Programmen und Produkten wird generell die datenschutzfreundliche Voreinstellung eingerichtet. Erinnern sie sich noch an die Router, die ungesichert ausgeliefert wurden?

Für alle Authentifizierungsfälle und Logins wird grundsätzlich eine Zwei-Faktor-Authentisierung eingesetzt, also Passwort und Fingerabdruck, Karte und Pin, TAN und Stimmerkennung. Dies mag manchmal nervig sein, aber es schützt nicht nur die eigenen Daten, sondern erschwert auch deren Missbrauch. Und warum nicht innovativ sein und Datensicherheit/Datenschutz bequem machen? Warum arbeiten daran die US-Firmen und nicht die deutschen Firmen, die sich ohnehin daran halten müssen?

Facebook - Fall

Der Doxing-Angriff zu Beginn des Jahres bekannt wurde, hat gezeigt, dass Promis und PolitikerInnen zunehmend zum Ziel von Cyberattacken werden. Der Fall löste eine Debatte über das Thema Datensicherheit aus und führte zu der Frage, wie Politikerinnen und Politiker, aber auch Bürgerinnen und Bürger besser geschützt werden können.

Der Fall reiht sich ein in eine immer längere Liste von - zum Teil viel schwerwiegenderen - Vorfällen, bei denen Daten aus dem Internet unberechtigt verarbeitet und Dritten zugänglich gemacht wurden.

Er verdeutlicht einmal mehr, wie wichtig das Bewusstsein um die eigenen Daten ist. Doch Bewusstsein alleine reicht natürlich nicht, um böse Absichten vollständig verhindern zu können. Es muss auch auf die richtigen Mittel zur Verhinderung gesetzt werden. Und diese müssen dann auch angewendet werden. Wissen, was man falsch macht, mag ein nettes Lebensmotto sein, aber ein Desaster in einer digitalen Gesellschaft in Bezug auf Datensicherheit und Datenschutz.

Die Daten konnten insbesondere auch deshalb gesammelt und veröffentlicht werden, weil die Passwörter zu privaten E-Mailkonten, Cloud-Diensten und sozialen Netzwerken zu leicht zu erraten waren oder leicht recherchiert werden konnten. Weil einfach zu ergreifende Schutzmaßnahmen nicht ergriffen wurden. Weil man facebook für den Login in andere Dienste verwendet hat.

Ich empfehle allen, denen spätestens der Doxing-Vorfall die Augen geöffnet hat, drei Konsequenzen, die ich hier kurz umreißen möchte:

Erstens brauchen wir natürlich einen verbesserten Eigenschutz. Nutzerinnen und Nutzer müssen noch stärker dafür sensibilisiert werden, wie schnell unzureichender Eigenschutz zu einem echten Erdrutsch führen kann, der dann auch andere in Mitleidenschaft zieht. Es ist wichtig, dass sie in ihrem eigenen Interesse und im Interesse ihrer Mitmenschen ihre eigenen Sicherheitsanforderungen hoch halten.

Hier gibt es viele Möglichkeiten, die oft hinlänglich bekannt sind, aber dann doch der eigenen Bequemlichkeit zum Opfer fallen. Dazu gehören starke Passwörter, die sich für jeden Dienst unterscheiden, eine sparsame und verschlüsselte Verwendung von Cloud-Diensten sowie der Einsatz von Verschlüsselung auch im privaten Bereich.

Ansonsten hilft auch eine gesunde Skepsis bzw. der gesunde Menschenverstand z.B. beim Öffnen von E-Mail-Anhängen. Nein, Angela Merkel hat nicht jedem Bundestagsabgeordneten von ihrer Privatadresse eine eMail geschickt mit einer Anlage, die man anklicken sollte. Jeder muss außerdem bei der Nutzung sozialer Medien genau überlegen, welche privaten Details überlassen bzw. veröffentlicht werden – und welche besser nicht.

Zweitens: Selbstverständlich sollten endlich alle Anbieter von Diensten ihre Systeme so sicher wie möglich gestalten und sie sollten im Fall von Hackerangriffen klar zur Mithilfe verpflichtet werden. Die Anbieterverantwortung muss verbessert werden. Erforderlich sind eine Implementierung geeigneter Sicherheitsmaßnahmen und die Sicherstellung einer schnellen Reaktion bei Sicherheitsvorfällen.

Wir werden als Europäischer Datenschutzausschuss noch verbindlich festlegen, welche Sicherheitsmaßnahmen mindestens notwendig sind, um die Vorgaben der DSGVO zu erfüllen. Werden diese von den Anbietern nicht ergriffen, liegt ein Datenschutzverstoß vor. Erste Bußgelder sind z.B. bei Unternehmen, die Paßwörter im Klartext gespeichert haben, schon ausgesprochen worden. Und nein, man kann nicht z.B. auf die Verschlüsselung bei der Übertragung von sensiblen personenbezogenen Daten verzichten, nur weil man sich davor eine Einwilligung dafür besorgt hat.

Es gibt Hinweise, dass Internetunternehmen bei der Eindämmung des Doxing-Fall und anderen Leaks zu langsam waren und nicht ausreichend genug mitgearbeitet haben. Wichtig wäre z.B. gewesen, sofort die betroffenen Links auf Twitter zu den geleakten Daten, die Short-URLs, abzuschalten, die längst durch viele neutrale Accounts retweetet worden waren, aber mit dem Abschalten des Accounts des Verursachers allein eben nicht mitgelöscht wurden. Dann wäre die Verbreitung der Daten extrem verlangsamt und verringert worden. Jetzt werden Familienfotos und andere private Dinge von Personen des öffentlichen Lebens immer wieder im Netz auftauchen. Das ist hochproblematisch.

Und **drittens** müssen die Datenschutzbehörden bei Cyberangriffen die auch personenbezogene Daten gefährden, unverzüglich informiert werden.

Die Datenschutz-Aufsichtsbehörden müssen in die Prozesse der Sicherheitsbehörden bei der Bearbeitung entsprechender Vorfälle eingebunden werden. Denn IT-Sicherheitsrisiken sind regelmäßig auch Datenschutzrisiken.

Wenn die zuständigen Datenschutzbehörden aus den Medien von Schutzlücken erfahren, ist das eindeutig zu spät. Wir haben spezifische Befugnisse und spezifische Erfahrungen, wenn es um den Schutz personenbezogener Daten geht. Diese müssen zum Schutz der Betroffenen unmittelbar zum Einsatz kommen.

Die veröffentlichten Daten verdeutlichen einmal mehr, wie wichtig der Datenschutz in unserer digitalen Welt ist. Für mich ist insbesondere wichtig, jetzt die richtigen Lehren aus dem Vorfall zu ziehen.

Die politische und mediale Aufmerksamkeit wollen wir nutzen, um für einen sensibleren Umgang mit personenbezogenen Daten in der digitalen Welt zu werben. Hier sind Provider, Dienste-Anbieter, IT-Sicherheitsbehörden, Datenschutz-Aufsichtsbehörden und herstellerunabhängige Institutionen gefordert, um Ihren Beitrag zu konkreten Hilfestellungen für alle Menschen im privaten, beruflichen und somit auch im politischen Umfeld zu leisten.

Hiermit kann schlussendlich auch eine positive Veränderung im bewussten Umgang mit personenbezogenen Daten in allen Lebenslagen – sowohl der analogen als auch der digitalen Welt – erzielt werden.

Dabei gilt, dass nur die Daten verlorengehen können, die zuvor an einer Stelle gesammelt wurden. Deswegen sollten auch die Anbieter nur die Daten erheben und speichern, die für das Produkt oder die Dienstleistung wirklich benötigt werden. So wie es die DSGVO vorschreibt.

Der Staat muss eine sichere IT-Umgebung fördern und darf sie nicht gefährden. Die Zweckbindung gespeicherter Daten, das Verbot von Tracking und eine starke Verschlüsselung aller digitalen Kommunikation und aller gespeicherten Daten sind unabdingbar für eine demokratische digitale Gesellschaft.

Jeder Ansatz, zur Förderung bestimmter Technologien die Zweckbindung zu lockern, Verlagen und anderen Branchen das Tracking von Bürgern im Web zu erlauben oder zur Erleichterung von Ermittlungstätigkeiten Hintertüren in Verschlüsselungen einzubauen, erodieren die Basis für diese demokratische, digitale Gesellschaft. So würde die Überwachung durch Privatkonzerne legalisiert und digitale Straftaten erleichtert.

Die Entscheidung darüber fällt in den nächsten ein oder zwei Jahren. Stichworte sind IT-Sicherheitsgesetz, ePrivacy-Verordnung und neue Gesetze im Sicherheitsbereich. Wir stehen an einer Weggabelung der Digitalisierung.

Ich danke Ihnen für Ihre Aufmerksamkeit.

(diese Seite nur optional, ist vielleicht eher für die Diskussionsrunde von Interesse)

Aktuelle Phänomene Bundeslagebild Cybercrime 2017 des BKA[5]

Ransomware – Digitale Erpressung (Fallbeispiel Verschlüsselungssoftware WannaCry)

Schadprogramme werden als Hauptproblem oft durch SPAM-Mails verteilt (aber auch Drive by Download ist ein Problem).

Laut dem BSI-Bericht „Die Lage der IT-Sicherheit in Deutschland 2017“ wird die Gesamtzahl der Schadprogrammvarianten für Computersysteme auf über 600 Mio. geschätzt. Tendenz steigend.

Es gibt auch weitere Schadsoftware wie Banking-Trojaner, Keylogger, Adware und Spyware. Problem Botnetze, DDOS-Angriffe, Mobile Malware und Diebstahl digitaler Identitäten/Phishing im Online-Banking.

Und durch neue Entwicklungen kann fast jeder Smartphone-Nutzer Opfer einer Straftat werden.

---

5 https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2017.html