verbraucherzentrale
Nordrhein-Westfalen

STELLUNGNAHME

Zur Anhörung im Rahmen des Ausschusses für Digitalisierung und Innovation

„Lehren aus Hackerangriff ziehen – IT-Sicherheit in NRW verbessern“, Antrag der Fraktion der AfD, Drs. 17/4803

sowie

„IT-Sicherheit in Nordrhein-Westfalen stärken – Freiheit sichern“, Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN, Drs. 17/5056

am Donnerstag, den 16. Mai 2019

6. Mai 2019

Herausgeber

Verbraucherzentrale
Nordrhein-Westfalen e.V.

Der Vorstand
Wolfgang Schuldzinski
Mintropstraße 27
40215 Düsseldorf

www.verbraucherzentrale.nrw

Die Verbraucherzentrale NRW bedankt sich für die Einladung zur Anhörung des Ausschusses für Digitalisierung und Innovation „Lehren aus Hackerangriff ziehen – IT-Sicherheit in NRW verbessern“, Antrag der Fraktion der AfD, Drs. 17/4803 sowie „IT-Sicherheit in Nordrhein-Westfalen stärken – Freiheit sichern“, Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN, Drs. 17/5056 und nimmt gerne wie folgt Stellung.

1. WACHSENDE BEDEUTUNG DER IT-SICHERHEIT FÜR VERBRAUCHERINNEN UND VERBRAUCHER

Die Digitalisierung und Vernetzung des Verbraucheralltags birgt eine Reihe von Chancen und Innovationspotential, zugleich aber auch gewisse Risiken für Verbraucherinnen und Verbraucher.[1] So entstehen beispielsweise neue Möglichkeiten des Zugriffs auf Kundendaten, oft ohne dass die Kunden sich dessen bewusst sind, sowie neue Einfallstore für Kriminelle. Je größer die Digitalisierung den Verbraucheralltag durchdringt, desto größer sind die Angriffsmöglichkeiten und desto schwieriger gestaltet sich die Kontrolle der persönlichen Daten.

Die Hackerangriffe auf Accounts von Politikerinnen und Politiker bringen das Thema IT-Sicherheit und Datensicherheit aktuell in den Fokus der politischen und medialen Wahrnehmung. Allerdings ist dies kein neues Thema, sondern leider sind Unternehmen wie auch Verbraucherinnen und Verbraucher schon seit Längerem immer wieder Opfer von Cyberangriffen. Diese Risiken steigen insbesondere dann, wenn die genutzte IT nicht hinreichend vor Angriffen Dritter gesichert ist.

Insbesondere automatisierte und autonome Systeme bieten vielfältige Angriffsmöglichkeiten, denen Verbraucher im Umgang mit digitalen Medien begegnen. Verbraucherinnen und Verbraucher sind daher auf eine funktionierende und vor allem sichere IT angewiesen.

Umfänglich hat die Verbraucherzentrale NRW in ihrer Stellungnahme zur „Strategie für das digitale Nordrhein-Westfalen: Teilhabe ermöglichen – Chancen eröffnen“ zu den Herausforderungen, die IT-Sicherheit und Datensicherheit an die Landesregierung, an die Verbraucherinnen und Verbraucher selbst und auch an die Verbraucherzentrale NRW stellen, Stellung genommen, auf die wir an dieser Stelle gerne verweisen.[2]

Darüber hinaus stellen wir gerne zusammenfassend die Aktivitäten der Verbraucherzentrale NRW in Sachen „Datensicherheit“ vor.

2. AKTIVITÄTEN ZUR IT-SICHERHEIT DURCH BERATUNG UND INFORMATION

Beim Phänomen des „Doxing“ können die publizierten Informationen auf unterschiedliche Weise „erbeutet“ werden, etwa durch Hacking oder durch einen allzu sorglosen Umgang den eigenen Daten. Wir verkennen nicht, dass auch die Verbraucherinnen und Verbraucher einen Beitrag zur IT-Sicherheit leisten müssen. Die Verbraucherzentrale NRW hat bereits frühzeitig auf die zunehmenden Risiken und Gefahren für Verbraucherinnen und Verbraucher reagiert und bietet eine breite Palette an Aktivitäten zur IT-Sicherheit mit präventivem Ansatz.

---

[1] Bala/Schuldzinski (Hrsg.), Schöne neue Verbraucherwelt? Big Data, Scoring und das Internet der Dinge, Beiträge zur Verbraucherforschung5. Düsseldorf: Verbraucherzentrale NRW.

[2] https://www.verbraucherzentrale.nrw/politik-nrw/verbraucherpolitik.

2.1 Verbraucherinformation und -beratung im Rahmen unseres Angebots „Datenschutz in der digitalen Welt

In 21 unserer 61 Beratungsstellen beraten wir Verbraucherinnen und Verbraucher zum Datenschutz in der digitalen Welt, wozu auch Fragen zur Datensparsamkeit und zum sicheren Umgang mit dem Internet und den hierfür genutzten Endgeräten wie Smartphone, Tablet und PC gehören. Ziel ist es, die Selbstverantwortung der Verbraucherinnen und Verbraucher zu stärken, etwa durch gezielte Sicherheitsmaßnahmen wie sicheren Passwortschutz oder den Verzicht auf den Download von Programmen aus unbekannten Quellen. Daher informieren und beraten wir Verbraucherinnen und Verbraucher gerade auch zu diesen relevanten Sicherheitsthemen. Hierzu und zu richtigen Sicherheitseinstellungen im Browsern haben wir bereits so genannte „Krypto-Parties“ mit den Bürgerinnen und Bürgern veranstaltet und gemeinsam mit dem Chaos Computer Club und dem Landeskriminalamt NRW die Sicherheitseinstellungen mitgebrachter mobiler Geräte wie Laptops und Smartphones überprüft und optimiert.

Ein weiterer Schwerpunkt besteht in Vortragsreihen mit den Themen „Sicher Online shoppen“, „Digitaler Nachlass“ und einem Überblick über den „Digitalen Datenschutz“. Auch Informationsmaterial wie die Broschüre „Ihre Daten, Ihre Rechte“ mit den wichtigsten Betroffenenrechten nach der DSGVO wurden anlässlich des Inkrafttretens der Datenschutzgrundverordnung produziert.

Weitere Themen im Beratungsangebot waren u.a. vernetztes Spielzeug wie die vom Bundesamt für Sicherheit in der Informationstechnik zurückgerufene Puppe „Kayla“ und neben Fragen zu sozialen Netzwerken wie Facebook und WhatsApp auch das Thema Smart Home. Insbesondere die neuen digitalen Sprachassistenten wie Amazon Alexa und Google Home führen zu einer erhöhten Nachfrage und Beschwerden von Verbraucherinnen und Verbrauchern. Gleiches gilt für die Einführung der DSGVO, die zu vielerlei Unsicherheiten auf Seiten der Verbraucherinnen und Verbrauchern führte, die im Rahmen von Beratungsgesprächen geklärt werden. Eine zum Start der DSGVO eigens konzipierte Internetseite erklärt die Betroffenenrechte und stellt Musterbriefe für deren Geltendmachung zur Verfügung.[3]

Die Verbraucherzentrale NRW wird daher lokal wie auch überregional zunehmend als kompetenter Ansprechpartner zum Themenkomplex Datenschutz und Datensicherheit in der digitalen Welt wahrgenommen.

2.2 Phishing-Radar

Die Schwachstelle Mensch zeigt sich insbesondere anhand von betrügerischen Phishing-Mails, die versuchen, Kunden von Banken und Online-Händlern wie z.B. Amazon dazu zu bringen ihre Zugangsdaten preiszugeben. Hier leistet die Verbraucherzentrale bereits seit 2010 einen wichtigen Beitrag zum Schutz der Kunden durch das „Phishing-Radar“. [4] Unter diesem Begriff veröffentlicht die Verbraucherzentrale NRW in ihrem Internetangebot aktuelle und Basisinformationen rund um gefakte E-Mails oder Internetseiten und trojanischen Pferden. Der „Phishing-Radar“ ist darauf

[3] https://www.verbraucherzentrale.nrw/ihre-daten-ihre-rechte

[4] https://www.verbraucherzentrale.nrw/phishing-radar.

gerichtet, vor aktuellen Angriffen in Bezug auf Identitätsdiebstahl und das Ausspähen von sicherheitsrelevanten persönlichen Daten zu warnen und zu schützen.

Erhielt das Phishing-Radar in den Jahren 2010 und 2011 von betroffenen Verbraucherinnen und Verbrauchern täglich gerade mal 20 bis 30 E-Mails, sind es heute zehn Mal so viele. Im „Phishing-Radar“ wurden mittlerweile weit **über 500.000 Meldungen** zu betrügerischen Angriffen ausgewertet, Warnhinweise auf unserer Homepage, per Twitter[5] und einer eigenen Facebook-Gruppe[6] sowie über Pressemitteilungen veröffentlicht und Verbraucherinnen und Verbrauchern präventive und reaktive Ratschläge zu sicherheitsrelevantem Verhalten gegeben. Eine FAQ-Liste etwa gibt Tipps zum weiteren Vorgehen[7] oder es wird erklärt, wie Verbraucherinnen und Verbraucher betrügerische E-Mails erkennen können und welche Schutzmaßnahmen möglich sind[8]. Viele Informationen, wie z.B. „Phishing und trojanische Pferde - Angriffe auf den eigenen PC erkennen und abwehren“ stehen hier auch zum Download bereit.[9] Auch für Jugendliche wird das Thema Phishing eigens im Online-Jugendmagazin der Verbraucherzentrale NRW aufbereitet.[10]

Die Meldungen des „Phishing-Radars“ stellen wir seit 2018 monatlich auch dem Bundesamt für Sicherheit in der Informationstechnik zur Verfügung gestellt und sie finden so Eingang in die Arbeit dieses Bundesamtes.

Hier besteht Potenzial, die Reichweite des Phishing-Radars zu steigern, indem auch die NRW-Verwaltung und –Behörden – etwa im eigenen Internetauftritt – auf die Betrugswarnungen verweisen.

2.3 Verbraucherinformationen in unserem Internetangebot sowie in den sozialen Netzwerken

Zu Fragen der Datensicherheit informiert die Verbraucherzentrale NRW über ihr Internetangebot auf www.verbraucherzentrale.nrw, über das Online-Jugendmagazin der Verbraucherzentrale NRW „Checked4you“[11] sowie über die Sozialen Netzwerke Facebook und Twitter.

Unter anderem zu Themen wie „Sichere Passwörter – So geht’s“[12], „"Single-Sign-On": Riskanter Login für alle Internetseiten“[13], anlässlich des Cambridge Analytica-Skandals „So verbieten Sie Apps bei Facebook den Zugriff auf Ihre Daten“[14], „Datenschutz und

---

[5] Twitter: @vznrw_phishing.

[6] Facebook-Gruppe „Phishingradar Verbraucherzentrale NRW“.

[7] https://www.verbraucherzentrale.nrw/wissen/digitale-welt/phishingradar/phishingmails-kein-tag-ohne-betrug-6052.

[8] https://www.verbraucherzentrale.nrw/wissen/digitale-welt/phishingradar/so-lesen-sie-den-mailheader-6077

[9] https://www.verbraucherzentrale.nrw/sites/default/files/2018-11/Phishing_und_trojanische_Pferde_Angriffe_auf_den_eigenen_PC_erkennen_und_abwehren.pdf.

[10] https://www.checked4you.de/computer-internet/e-mails/phishing-und-pharming-103840.

[11] Vgl. nur beispielhaft ein Artikel zur sicheren Passwortgestaltung: https://www.checked4you.de/computer-internet/internet/gutes-passwort-schlechtes-passwort-150172.

[12] https://www.verbraucherzentrale.nrw/wissen/digitale-welt/datenschutz/sichere-passwoerter-so-gehts-11672.

[13] https://www.verbraucherzentrale.nrw/wissen/digitale-welt/soziale-netzwerke/singlesignon-riskanter-login-fuer-alle-internetseiten-13704.

[14] https://www.verbraucherzentrale.nrw/wissen/digitale-welt/soziale-netzwerke/so-verbieten-sie-apps-bei-facebook-den-zugriff-auf-ihre-daten-24601.

Datensicherheit: Tipps im Überblick“[15], „Apps: Zugriff auf die Daten der Freunde“[16], „Abzocke mit Facebook-Profilen Ihrer Freunde“[17], „So erhöhen Sie den Datenschutz bei Twitter“[18], „So löschen Sie Ihr Profil bei Facebook“[19], „WhatsApp-Alternativen: Die Datenschutzregeln im Überblick“[20] und zu vielen anderen Themen sind wir mit Basisinformationen für Verbraucherinnen und Verbrauchern aber auch immer aktuell auf bestimmte Sicherheitslücken reagierend präsent. So haben wir auf die aktuellen Cyberattacken unmittelbar auf unserer Homepage mit der Information „Datenleaks vorbeugen: Mit Daten geizen, eigene Infos schützen“ reagiert,[21] darauf hingewiesen, dass Facebook Millionen Passwörter unverschlüsselt speicherte[22] und auch zum Trojaner „Emotet“ hat die Verbraucherzentrale NRW eine aktuelle Meldung verfasst.[23] In diesen Wurde das Profil gehackt, finden insbesondere Jugendliche auf der Seite des Online-Jugendmagazins der Verbraucherzentrale NRW eine Übersicht von Notfall-Adressen der Diensteanbieter.[24]

2.4 Für alle Angebote steht auch schriftliches Informationsmaterial zur Aushändigung oder zum Download bereit

Diverse Materialien (Flyer und Broschüren) stehen auch als schriftliches Informationsmaterial in den Beratungsstellen bereit. Zum Thema IT-Sicherheit zählen hierzu insbesondere „Schadprogramme – So schützen Sie sich“ in Kooperation mit dem Landeskriminalamt NRW, „Big Data! Und ich? Die wichtigsten Tipps zum Schutz deiner Daten“ (im Rahmen des BMJV-geförderten Projekts Wirtschaftlicher Verbraucherschutz), „Phishing-Radar“, „WLAN-Absicherung – Tipps zur richtigen Absicherung des eigenen WLAN-Anschlusses“ (im Rahmen des BMJV-geförderten Projekts Wirtschaftlicher Verbraucherschutz), „Mit Sicherheit online einkaufen. Vor dem Klicken Rechte checken.“, „Ihre Daten gehören Ihnen – Datensparsamkeit lohnt sich“ (gemeinsam mit der Landesbeauftragten für Datenschutz und Informationssicherheit), „Abzocke per Smartphone. Hilfe bei ungewollten Abos“ oder „Digitaler Nachlass: So sorgen Sie vor“.

2.5 Vorträge in Schulen, bei Initiativen in NRW-Städten, in den Beratungsstellen

Die Verbraucherzentrale NRW hält teilweise projektfinanziert durch das BMJV-geförderte Projekt Wirtschaftlicher Verbraucherschutz, teilweise institutionell finanziert

---

[15] https://www.verbraucherzentrale.nrw/wissen/digitale-welt/datenschutz/datenschutz-und-datensicherheit-tipps-im-ueberblick-11910.

[16] https://www.verbraucherzentrale.nrw/wissen/digitale-welt/datenschutz/apps-zugriff-auf-die-daten-der-freunde-12575.

[17] https://www.verbraucherzentrale.nrw/wissen/digitale-welt/soziale-netzwerke/abzocke-mit-facebookprofilen-ihrer-freunde-24071.

[18] https://www.verbraucherzentrale.nrw/wissen/digitale-welt/soziale-netzwerke/so-erhoehen-sie-den-datenschutz-bei-twitter-13728.

[19] https://www.verbraucherzentrale.nrw/wissen/digitale-welt/soziale-netzwerke/so-loeschen-sie-ihr-profil-bei-facebook-24724.

[20] https://www.verbraucherzentrale.nrw/wissen/digitale-welt/datenschutz/whatsappalternativen-die-datenschutzregeln-im-ueberblick-13055.

[21] https://www.verbraucherzentrale.nrw/wissen/digitale-welt/datenschutz/datenleaks-vorbeugen-mit-daten-geizen-eigene-infos-schuetzen-33521.

[22] https://www.verbraucherzentrale.nrw/aktuelle-meldungen/digitale-welt/facebook-speicherte-millionen-passwoerter-unverschluesselt-34923.

[23] https://www.verbraucherzentrale.nrw/aktuelle-meldungen/digitale-welt/emotet-gefaehrlicher-trojaner-beantwortet-empfangene-emails-35502.

[24] https://www.checked4you.de/computer-internet/internet/profil-gehackt-adressen-f%C3%BCr-den-notfall-351495.

durch das Beratungsangebot „Datenschutz in der Digitalen Welt“ Vorträge in Schulen, bei Initiativen und zahlreichen Kooperationspartnern in NRW-Städten sowie in den Beratungsstellen. Ziel ist es, die jeweils angesprochenen Verbrauchergruppen und in Schulen insbesondere Jugendliche für den Schutz der Privatsphäre zu sensibilisieren und ihnen Instrumente zur digitalen Selbstverteidigung an die Hand zu geben.

Hervorzuheben sind die Durchblick-Module für Schüler der Sekundarstufen I und II, die im Projekt Wirtschaftlicher Verbraucherschutz, welches vom Bundesministerium der Justiz und für Verbraucherschutz gefördert wird, angeboten werden. Im Jahr 2018 gab es allein insgesamt ca. 100 Veranstaltungen zu Themen wie „Smartphone und Internet“ und „Big Data und Co.“

2.6 Untersuchungen des Marktwächters Digitale Welt

Der Marktwächter „Digitale Welt“ ist ein Frühwarnsystem mit dem der Verbraucherzentrale Bundesverband und die Verbraucherzentralen der Länder den digitalen Markt aus Perspektive der Verbraucherinnen und Verbraucher beobachten und analysieren. Der Marktwächter wird vom Bundesministerium der Justiz und für den Verbraucherschutz projektgefördert. Bei der Verbraucherzentrale NRW ist der Marktwächter mit dem Schwerpunktthema „Nutzergenerierte Inhalte“ angesiedelt.

Die Untersuchungen des Marktwächters haben häufig auch die Prinzipien von **privacy by design** (Datenschutz durch Technikgestaltung) und **privacy by default** (datenschutzfreundliche Voreinstellungen) im Blick. Alle Untersuchungsergebnisse werden u.a. maßgeblichen Stakeholdern in Politik und Wirtschaft zugeleitet mit dem Ziel, Missstände aufzuzeigen und sich hieraus ableitende Verbesserungen zu fördern oder anzustoßen.

Unter anderem wurden folgende Untersuchungen von der Verbraucherzentrale NRW durchgeführt:

a. **Wearables**: Geprüft wurden 12 Anbieter von Wearables und die dazugehörigen Apps (Android und iOS). Die Untersuchung umfasste eine rechtliche Analyse der Datenschutzerklärungen, eine technische Analyse und eine Verbraucherbefragung. Gegenstand der technischen Analyse war u.a. auch die Datensicherheit und zwar inwieweit die im Rahmen der Wearables-Nutzung generierten Daten vor dem Zugriff durch Unbefugte geschützt sind (welche Schnittstellen sind vorhanden, welche Schwachstellen, ist die Datenübertragung verschlüsselt) und ob Möglichkeiten zur Einflussnahme und Kontrolle der Daten durch Verbraucherinnen und Verbraucher bestehen.

b. **Digitale Sprachassistenten**: Geprüft wurden Amazon Echo mit dem dazugehörigen Sprachassistenten Amazon Alexa und Google Home mit dem dazugehörigen Sprachassistenten Google Assistent. Hier wurde geprüft, ob die Geräte nur auf das vorher festgelegte Aktivierungswort oder auch auf dem Aktivierungswort ähnlich klingenden Wörtern reagieren und welches Sicherheitsniveau das Ecosystem der Sprachassistenzsysteme aufweist (Hersteller-App, Sprachassistent und Backend-Server der Anbieter).

c. **Vernetztes Spielzeug**: Es wurde ein Marktüberblick zu vernetzten Spielzeugen erstellt und der Spielzeugroboter ANKI Cozmo durch das Bundesamt für Sicherheit in der Informationstechnik technisch hinsichtlich Datenschutz- und Datensicherheitsaspekte geprüft. Prüfpunkte waren vor allem: Welche Schnittstellen und Verbindungen gibt es? Werden Daten lokal oder in einer Cloud gespeichert? Sind diese Schnittstellen angreifbar und Schwachstellen identifizierbar? Ist die Datenübertragung verschlüsselt?

Alle Untersuchungen sind abrufbar unter www. marktwächter.de.

2.7 Kooperation mit dem Bundesamt für Sicherheit in der Informationstechnik

Die Verbraucherzentrale NRW pflegt mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) im Rahmen eines Memorandums of Understanding eine enge Zusammenarbeit, um die Informationssicherheit für Verbraucherinnen und Verbraucher zu stärken, ihnen beim Umgang mit Missbräuchen zur Seite zu stehen und um Internetsabotage wirksam zu bekämpfen. Neben wechselseitigen Verlinkungen im Rahmen der Öffentlichkeitsarbeit im Internet und über soziale Medien zu sicherheits- und verbraucherrelevanten Sachverhalten steht auch die inhaltliche Zusammenarbeit durch den technischen Sachverstand des BSI und die rechtliche Expertise der Verbraucherzentrale NRW im Vordergrund. So lässt die Verbraucherzentrale NRW im Rahmen eines Verbandsklageverfahrens klären, welche Informationspflichten Verkäufer treffen, wenn diese Smartphones mit nicht mehr behebbaren Sicherheitslücken an Verbraucherinnen und Verbraucher verkaufen. Das Gerät wurde zuvor vom BSI auf Sicherheitslücken nach dem CVE-Standard getestet.[25]

Neu ist die Mitarbeit der Verbraucherzentrale NRW in der Allianz für Cybersicherheit, ein vom BSI ins Leben gerufenes Netzwerk zum Schutz vor Cyberattacken, das nach anfänglicher Konzentration auf den unternehmerischen Bereich nun auch Verbraucherinnen und Verbraucher mit in den Fokus genommen hat. Hier hat sich die Verbraucherzentrale NRW 2018 erstmals am Cyber Security Month (ECSM) mit Beiträgen zur Sicherheitseinstellungen in sozialen Netzwerken beteiligt. Auch am ECSM 2019 ist die Teilnahme mit dem Thema Phishing-Radar geplant.

2.8 Kooperation mit dem Landeskriminalamt NRW

Seit ca. 7 Jahren besteht außerdem eine Kooperation mit dem Landeskriminalamt NRW, insbesondere im Themenbereich Betrug und Abzocke. Neben Aktionen wie etwa zu Fake Shops wird z.B. auch gemeinsam Material erstellt, z.B. Flyer „Schadprogramme – So schützen Sie sich.“ oder der „Leitfaden zum Datenschutz – ich habe doch nichts zu verbergen – Datensparsamkeit lohnt sich trotzdem“.

Im Herbst 2019 wird es außerdem eine NRW-weite Aktion zum Thema Passwortsicherheit geben. Die Kreispolizeibehörden werden hierbei gemeinsam mit den 61 Beratungsstellen über Datenleaks aufklären und über entsprechende Schutzmaßnahmen informieren.

3. VERBRAUCHERRECHTLICHES UND –POLITISCHES ENGAGEMENT

Neben Information und Wissensvermittlung engagiert sich die VZ NRW auch im Rahmen ihrer Verbandsklagebefugnis und ihrer verbraucherpolitischen Arbeit für eine Verbesserung der Verbraucherposition ein.

3.1 IT-Sicherheit

Im Feld der technologischen Entwicklung kommt der Sicherheit der eingesetzten Systeme eine hohe Bedeutung zu. Ist der Mensch das schwächste Glied in der IT-Sicherheitskette, kommt der **datenschutzfreundlichen Technikgestaltung** (privacy by design und privacy by default) eine zentrale Rolle zu, wie sie bereits in der Daten-

[25] Vgl. hierzu die Ausführungen unter 3.3. Kennzeichnung von Sicherheitsmerkmalen.

schutzgrundverordnung angelegt ist. Allerdings richten sich diese Vorgaben lediglich an die für die Datenverarbeitung Verantwortlichen und nicht an die Hersteller. Im Rahmen einer Evaluation der Datenschutzgrundverordnung sollte sich die Landesregierung daher dafür einsetzen, dass auch die Hersteller künftig vom Anwendungsbereich der Datenschutzgrundverordnung erfasst werden. Neben der Stärkung der zivilrechtlichen Klagebefugnisse müssen auch die Datenschutzaufsichtsbehörden entsprechend ausgestattet werden, die Vorgaben der Datenschutzgrundverordnung durchzusetzen und bei der Meldung von Datensicherheitsvorfällen durch Unternehmen diesen nachgehen zu können. Gerade die verpflichtende Anzeige für Unternehmen im Fall eines Datenlecks ist wichtig, um Folgeschäden zu vermeiden. Bei künftigen Datensicherheitsvorfällen sollten die Datenschutzaufsichtsbehörden direkt in die Informationskette eingebunden werden (nicht nur BKA, LKA und BSI wie im Doxing-Fall).

Darüber hinaus sollten die Prinzipien der datenschutzfreundlichen Technikgestaltung (privacy by design und privacy by default) auch im Rahmen des EU-Gesetzgebungsprozesses der ePrivacy-Verordnung fest verankert werden, um die Datensicherheit und Vertraulichkeit in der elektronischen Kommunikation sicherzustellen. Anbieter elektronischer Kommunikationsdienste sollten verpflichtet werden, besondere IT- Sicherheitsvorkehrungen vorzunehmen, etwa dass sie keine Passörter wie „passwort“ akzeptieren und die Zwei-Faktor-Authentifizierung verpflichtend einbauen. Dies gilt insbesondere für E-Mail-Dienste, über die sich die Passwörter anderer Accounts zurücksetzen lassen. Außerdem sollte klar geregelt werden, dass die Kommunikation zwischen Nutzern Ende-zu-Ende-verschlüsselt wird, soweit die Anbieter die Endpunkte kontrollieren, wie z.B. in einer App.[26]

Zudem müssen Verbraucherinnen und Verbraucher der Technik auch vertrauen können, denn Vertrauen ist unabdingbar für die Akzeptanz digitaler Geschäftsmodelle und schließlich auch für die Demokratie.

Automatisierte und autonome Systeme bieten allerdings vielfältige Angriffsmöglichkeiten, denen Verbraucher im Umgang mit digitalen Medien begegnen. Diese Risiken steigen insbesondere dann, wenn die genutzte IT nicht hinreichend vor Angriffen Dritter gesichert ist. Wenn etwa Millionen von Zugangsdaten von Online-Diensten im Internet kursieren, ist weniger die mangelnde Sensibilisierung der Nutzerinnen und Nutzer das Problem, sondern die mangelnde Datensicherheit bei den Anbietern. Unautorisierte Zugriffe können dazu führen, dass unzulässiger Weise der Datenverkehr mitgeschnitten wird. Zudem bieten etwa die im Internet der Dinge über Cloud-Dienste verbundenen Fernseher, Webcams, Thermostate oder Router über die Möglichkeit der Fernsteuerung potentielle Angriffsziele. Verbraucherinnen und Verbraucher sind daher auf eine funktionierende und vor allem sichere IT angewiesen.

IT-Sicherheit umfasst alle Aspekte, die sich auf die Sicherheit von Daten im Sinne einer Wahrung der Verfügbarkeit, Vertraulichkeit und Integrität dieser Daten richtet. Dass beim Thema IT-Sicherheit ein enormer Nachholbedarf besteht, erkennt das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem aktuellen Bericht zur Lage der IT-Sicherheit in Deutschland ausdrücklich an. Tatsächlich erscheinen in immer kür-

[26] Bei E-Mail-Diensten ist eine Verschlüsselung aufgrund der diversen E-Mailclient weitaus schwieriger. .

zeren Abständen Meldungen über Sicherheitslücken in Softwareprogrammen, wie z. B. Betriebssystemen, oder IT-Hardware.[27]

Sicherheitsaspekte für smarte Geräte geraten aber leider immer noch zu leicht unter die Räder. Einem Bericht der EU-Kommission zufolge, spielt IT-Sicherheit und Datenschutz bei der Entwicklung von Smart-Home-Produkten kaum eine Rolle – zumindest dann nicht, wenn es sich um günstige Kleingeräte mit geringem Kundenbindungspotenzial handelt. Die Hersteller argumentieren, dass IT-Sicherheit teuer sei und von den Kunden beim Preis des Produkts nicht honoriert werde. Dabei kann es aber nicht in der alleinigen Entscheidungsgewalt der Hersteller liegen, zu klären, welche Sicherheitsmechanismen diese Systeme enthalten müssen, sondern es muss Vorgaben für überprüfbare Mindeststandards entsprechend dem Stand der Technik und kompetente Aufsichtsbehörden geben. Hier sehen wir eine Herausforderung für die Landesregierung, die die Schaffung solcher Sicherheitsstandards als wichtigem Technologiestandort Deutschlands fördern und fordern sollte.

3.2 Haftung für Sicherheitslücken

Dies wirft die Frage nach Pflichten der IT-Hersteller und deren etwaiger Haftung für Sicherheitslücken in ihren IT-Produkten auf. Um ein Eindringen von Schadsoftware in die eigenen Systeme zu verhindern und Angreifern keine Möglichkeit zur Ausnutzung dieser Schwachstellen zu bieten, ist es unabdingbar, stets die aktuellsten Sicherheitsupdates zu installieren. In der Praxis blieben Sicherheitslücken aber leider oft über Monate bestehen oder werden von den IT-Herstellern gar nicht behoben. Teilweise ist bei IT-Produkten – insbesondere im Bereich von vernetzten Produkten für die Nutzung in Verbraucherhaushalten, wie z. B. Glühbirnen – noch nicht einmal eine Update-Möglichkeit vorgesehen.

Die geltende Rechtslage wird den Anforderungen nicht gerecht und es ist eine gefährliche Situation ohne staatliche Regulierung entstanden. Denn de facto besteht eine Haftungsfreizeichnung der Unternehmen, die z. B. wegen ihres Standorts, etwa im asiatischen Raum, nicht zur Schließung von Sicherheitslücken verpflichtet werden können und quasi keine Haftung für Nachteile fürchten müssen, die durch den Angriff bei den Nutzerinnen und Nutzern entstanden sind. Die bestehenden Haftungslücken können aber aus verbraucherpolitischer Sicht nicht toleriert werden, weil sie die Verantwortung für die IT-Sicherheit in unverhältnismäßiger Weise auf die Nutzerinnen und Nutzer abwälzen, während die IT-Hersteller in kommerzieller Absicht ein Produkt auf den Markt bringen und dadurch eine Gefahrenquelle für die Nutzerinnen und Nutzer eröffnen.

Zum Schutz der Verbraucherinnen und Verbraucher muss daher eine verbraucherfreundliche IT-Sicherheitspolitik die erheblichen Schutzlücken de lege ferenda schließen. Angesichts der zunehmenden Gefahren durch Angriffe auf die alltäglich genutzten IT-Systeme bei gleichzeitiger Nachlässigkeit einer adäquaten Sicherheitsupdate-Politik der IT-Hersteller ist der Regulierungsbedarf offensichtlich. Es muss sichergestellt werden, dass Verbraucherinnen und Verbraucher IT-sichere Produkte erwerben können und zumindest für eine erwartbare Dauer mit relevanten Sicherheitsupdates versorgt

[27] Der Angriff auf u.a. die Speedport-Router der Telekom Deutschland Ende 2016 führte zu einer großflächigen Störung von 900.000 Anschlüssen. Dabei nutzten die Angreifer eine Sicherheitslücke aus, um einen Schadcode auf den Router aufzuspielen, um so in die vernetzten Häuser der Telekom-Kunden einzudringen.

werden.[28] Zwangs-Updates ohne Veranlassung des Eigentümers, die die Funktionalität einschränken oder ändern können, sollten untersagt sein.

Für Mängel vernetzter Produkte sollte nicht nur der Verkäufer einstehen müssen, der oftmals, wenn der Fehler im eingebetteten System (embedded system) zu finden ist, zur Fehlerbehebung nicht in der Lage sein wird. Hier wäre eine gewährleistungsähnliche Herstellerhaftung oder eine Garantiehaftung des Herstellers, die neben den kaufrechtlichen Gewährleistungsansprüchen stehen sollte, eine bedenkenswerte Lösung, für die der Gesetzgeber bald die Weichen stellen sollte. Zeitlich sollte der Anspruch an die Gewährleistungsfrist des Produktes angepasst werden.

Darüber hinaus ist aber auch mit dem zunehmenden Autonomiegrad der Produkte und der damit einhergehenden eigenständigen Abgabe von Willenserklärungen die aktuelle Rechtsgeschäftslehre vor eine Herausforderung gestellt. Wenn intelligente Geräte selbstständig den Einkauf erledigen, muss der Gesetzgeber dafür sorgen, dass offene Fragen zeitnah abschließend geklärt werden. Hierzu gehört beispielsweise die Überlegung, welche gesetzlichen Informationspflichten (bspw. Preisauszeichnungen) gelten, inwieweit die Vorschriften zum Widerruf Anwendung finden und welche Beteiligten Vertragspartner sind. Darüber hinaus müssen die Konsequenzen bei Fehlfunktionen autonomer Anwendungen, die zu fehlerhaften oder nicht vom Verbraucher gewollten Entscheidungen führen, durch den Gesetzgeber geklärt werden.

Wir sehen es als Aufgabe der Landesregierung an, sich in diesem Sinne für die Belange der Verbraucherinnen und Verbraucher Nordrhein-Westfalens und der auch ebenfalls betroffenen gewerblichen Nutzer einzusetzen und die Initiativen zur Schließung dieser sicherheitsrelevanten Rechtslücken auf Bundes- und ggf. auch Europaebene voranzutreiben und einer sicherheitskonformen Lösung zuzuführen.

3.3 Kennzeichnung von Sicherheitsmerkmalen

Neben der Selbstverantwortung der Verbraucherinnen und Verbraucher muss auch berücksichtigt werden, dass viele Menschen unsicher im Umgang mit dem Internet und den „neuen Medien“ sind, weil ihnen die notwendigen digitalen Kompetenzen fehlen. Zudem ist es beim Kauf von elektronischen Produkten für Verbraucherinnen und Verbraucher aber auch nicht erkennbar, welche Produkte nach dem Stand der Technik sicher sind und wie lange sie beispielsweise mit Sicherheitsupdates gepatcht werden. Diese Informationen sind aber wichtig, um gute und informierte Kaufentscheidungentreffen und sich reflektiert verhalten zu können. Die vielfach reklamierte digitale Sorglosigkeit von Verbraucherinnen und Verbrauchern kehrt sich daher in vielen Fällen zu einer digitalen Schutzlosigkeit um.

Verbraucherinnen und Verbraucher sollten schon beim Kauf erkennen, ob es sich um ein sicheres Produkt handelt und wie lange dies so sein wird, wenn das in Rede stehende IT-Produkt auf die stetige Versorgung mit Sicherheitspatches angewiesen ist. Wir benötigen daher neben Maßnahmen zur Bildung von Kompetenzen auch aussagekräftige Kennzeichnungen am Produkt. Das BMI und das BMJV haben im Februar einen elektronischen Beipackzettel für Router angekündigt. Im Dialog mit den Herstellern hat das Bundesamt für Sicherheit in der Informationstechnik Standards zur IT-

[28] Die EU-Richtlinie über bestimmte Aspekte des Warenhandels, welche Ende März sieht u.a. vor, dass Verbraucher, die Waren mit „digitalen Elementen“ kaufen, ein Recht auf Erhalt notwendiger Updates innerhalb eines Zeitraums haben, der vom Verbraucher als angemessen erwartet werden kann. Insoweit besteht noch Konkretisierungsbedarf.

Sicherheit für Router festgelegt. Mittels eines QR-Codes sollen Verbraucherinnen und Verbraucher überprüfen können, ob das Gerät, das sie kaufen möchten, tatsächlich diesen Standard einhält. Geprüft wird vom BSI, das in regelmäßigen Abständen Kontrollüberprüfungen durchführt.[7]

Dieser elektronische Beipackzettel hat den Vorteil, dass Verbraucherinnen und Verbraucher sich laufend über die Sicherheit ihres Geräts informieren können. Der elektronische Beipackzettel ist auf den ersten Blick eine Lösung, die vertrauensbildend sein kann und als wettbewerbsrelevante Verbraucherinformation von Unternehmen hoffentlich erkannt wird. Wichtig ist allerdings, dass die Verbreitung solcher QR-Codes nicht bei Routern stehen bleibt, sondern dass es bald noch weitere Mindeststandards für Produkte wie zum Beispiel Smartphones geben wird, die heute bereits zum Verbraucheralltag gehören werden. Die Verbraucherzentralen sind bereit diesen Prozess zu begleiten und zu unterstützen, aber auch – wenn es notwendig ist – unsere kritische Stimme einzubringen.

Die rechtlichen Fragestellungen in Bezug auf die Notwendigkeit von Hinweisen zu Sicherheitslücken und Updatezeiträumen beim Kauf eines unsicheren und nicht mehr gepatchten Smartphones29 klärt die Verbraucherzentrale NRW aktuell in einem vor dem Landgericht Köln anhängigen Musterverfahren30. Händler, die Smartphones zum Kauf anbieten, sollten unserer Rechtsauffassung nach zumindest auf bestehende Sicherheitslücken nach CVE-Standard hinweisen müssen. Denn nur so werden Verbraucherinnen und Verbraucher vor dem Kauf in die Lage versetzt, den Sicherheitsstand des Geräts zu bewerten und sicherzustellen, dass sie nicht ein Gerät erwerben, von dessen Nutzung aufgrund von Sicherheitslücken abgeraten werden muss. Gegenstand dieses Verfahrens ist ferner, ob eine Informationspflicht des Händlers darüber anzunehmen ist, wie lange nach Angabe des Herstellers mit der fortwährenden Beseitigung auftretender Sicherheitslücken zu rechnen ist. Denn nur, wenn Verbraucherinnen und Verbraucher (anders als heute) zum Zeitpunkt des Kaufs wissen, wie lange sie mit Sicherheitsupdates rechnen können, ist eine informierte Kaufentscheidung unter Einbeziehung der Wertigkeit eines Smartphones möglich.

Aus unserer Sicht sind daher auch landespolitische Initiativen zur Förderung von IT-Sicherheit erforderlich, anknüpfend an das Informationsdefizit und Kompetenzdefizit von Verbraucherinnen und Verbrauchern. Diese können neben den bildungspolitischen Aktivitäten auch regulatorische Maßnahmen bzw. das Einbringen von Initiative auf Bundesebene wie z. B. im Bundesrat, auf länderübergreifender Ebene in entsprechenden Arbeitskreisen, umfassen. Die Verbraucherzentrale NRW engagiert sich bereits – wie oben im Kapitel 2 dargestellt – vielfältig mit analogen und digitalen Informationsangeboten, mit Vorträgen in Schulen, Bildungseinrichtungen und unseren Beratungsstellen, um Verbraucherinnen und Verbrauchern im Themenfeld IT-Sicherheit eigene Handlungsmöglichkeiten aufzuzeigen und sie über Gefährdungspotentiale zu informieren. Unsere Aktivitäten sind aber nur „ein Tropfen auf einem heißen Stein“. Es bedarf weiterer Anstrengungen und Informationskampagnen, um möglichst viele Menschen zu

---

[29] In Zusammenarbeit mit dem BSI wurden Smartphones mit dem Betriebssystem „Android 4.4 Kitkat“ in einem Kölner Elektronikmarkt gekauft. Das BSI hat das Gerät auf Sicherheitslücken nach dem CVE-Standard (Common Vulnerabilities Exposures), einem Industriestandard zur Benennung von Sicherheitslücken in Computersystemen, getestet. Von 28 Sicherheitslücken, auf die die Software das Gerät geprüft hat, beinhaltete das Betriebssystem des Smartphones 15. Einen Hinweis auf mögliche Sicherheitslücken des Betriebssystems war der Werbung für das Smartphone vor Ort nicht zu entnehmen.

[30] LG Köln, Az. 31 O 133/17.

erreichen, die von der Landesregierung umfassen gefördert werden sollten. Die Verbraucherzentrale NRW ist gerne bereit hieran auch weiterhin mitzuwirken und ihren Beitrag zu leisten.