Hochschule für Polizei und öffentliche Verwaltung NRW
Studienort Duisburg, Außenstelle Mülheim an der Ruhr
Fachbereich Polizeivollzugsdienst

Bachelorthesis zum Thema:

# Smarte Vernetzung in Zeiten von Cyberkriminalität

## Fortschritt der Technik aus kriminalistischer Sicht

**Vorgelegt von:**

Björn Kepert
Kurs: MH P 18/02
Einstellungsjahrgang: 2018
[redacted]

Abgabedatum: 10.05.2021

Erstgutachter/in: Dr. iur. Frank Kawelovski M.A.
Zweitgutachter/in: Patrick Rohde M.A.

# Inhaltsverzeichnis

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet und das generische Maskulinum verwendet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

# 1 Einleitung

Der Fortschritt der Technik schreitet unaufhaltsam voran. Gerade im Bereich der Informationstechnik (kurz: IT) und der Elektrotechnik gibt es beinahe täglich Neuerungen, die noch vor einigen Jahren nicht denkbar gewesen wären. Dabei bietet die weltweit wachsende digitale Vernetzung der Gesellschaft enorme Potenziale. Smarte Technik im Fahrzeug, wie zum Beispiel automatisierte Notrufsysteme, sind heute bereits Standard und aus Neufahrzeugen nicht mehr wegzudenken. Zudem zeigt sich eine wachsende Anzahl von Eigenheimen mit smarten Gebäudeleitsystemen. Dabei lässt sich nahezu jedes elektrische Gerät im Haushalt miteinander verbinden und ist somit im Stande mit anderen Geräten zu kommunizieren. Der Eigentümer hat eine Vielzahl von Möglichkeiten auch aus der Ferne darauf zuzugreifen und Prozesse einzuleiten, was sonst nur in persönlicher Anwesenheit möglich wäre.

Doch birgt diese Fülle an Möglichkeiten auch ein hohes Risiko. Gerade im Bereich Cyberkriminalität bietet die smarte Vernetzung im täglichen Leben eine breite Angriffsfläche. Cyberkriminellen werden durch die Vernetzung im Fahrzeug oder im Haus buchstäblich die Türen geöffnet. Dabei ist der Aufwand vergleichsweise gering verglichen mit herkömmlichen kriminellen Handlungen, wie zum Beispiel dem Wohnungseinbruchsdiebstahl. Wo vorher mit Werkzeugen Fenster oder Türen aufgehebelt wurden, reicht jetzt ein internetfähiges Endgerät und jemand, der es bedienen kann. Zudem sind die Möglichkeiten solche Taten zu verfolgen sehr beschränkt und mit großem Aufwand und Expertise verbunden, da die Spurenlage eher diffizil ist und eine neue Herausforderung darstellt. Die Polizei rüstet derweil bundesweit

im Bereich Cybersicherheit auf, jedoch werden immer mehr Angriffe auf sensible Daten registriert. Das Bundeskriminalamt (BKA) führt seit 2010 zusätzlich zu der Polizeilichen Kriminalstatistik ein eigenes Bundeslagebild Cybercrime. Hier wird die Fülle an Straftaten, die im Bereich der Informations-und-Kommunikations (kurz: IuK)-Kriminalität liegen registriert und zusammengefasst.[1]

Es stellt sich die Frage, welche Möglichkeiten durch eine smarte Vernetzung für das tägliche Leben geschaffen werden. Bedeutet dies dabei eher einen Zugewinn für die Sicherheit der Bewohner oder ein Risiko, wenn smarte Gebäudeleitsysteme verbaut sind?

Diese Bachelorarbeit beschäftigt sich mit dem Themenkomplex smarte Vernetzung im privaten Leben und dem Risiko, welches daraus hervorgeht. Außerdem beleuchtet diese Arbeit die Möglichkeiten, die eine smarte Vernetzung der Polizei bietet.

Dafür werden zunächst die Begriffe Smart Home und Smart Car bzw. Connected Car näher erläutert. Dabei soll herausgestellt werden, wie sich die Technik von der Idee hin zum heutigen Stand entwickelt hat und welche Möglichkeiten sich für die Zukunft ergeben. Außerdem soll beleuchtet werden, welche technischen Innovationen derzeit bestehen, die die Sicherheit der Benutzer durch smarte Vernetzung erhöhen. Im Anschluss wird der Bogen zur Kriminalität gespannt, indem zunächst der Begriff Cybercrime näher erläutert wird. Welche Formen es gibt, wie handeln die Täter und weshalb es so schwer ist dies nachzuvollziehen. Des Weiteren wird dargestellt, wie die Polizei im Bereich Cybercrime vorgeht. Danach sollen die Risiken durch kriminelle externe Nutzung von smarter Vernetzung aufgezeigt werden. Wie sicher sind smarte Gebäude und wie geht ein Einbruch mittels IT-Kriminalität von statten? Hier wird vor allem verdeutlicht, mit welchen kriminellen Handlungen vorgegangen wird. Nachfolgend wird die polizeiliche Arbeit an smarten

[1] Vgl. Bundeskriminalamt. Bundeslagebild Cybercrime 2019 (2020). URL: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html (zuletzt aufgerufen 28.04.2021).

Tatobjekten veranschaulicht. Dazu werden zunächst die Begriffe digitale Spuren und IT-Forensik definiert. Abschließend wird aufgezeigt, welche Beweiskraft ein Kraftfahrzeug, welches über smarte Technik verfügt, bietet und wie die Spurensicherung am smarten Objekt erfolgt.

# 2 Definitionen

Die folgenden Begriffe stammen ursprünglich aus dem Englischen, da dies die vorherrschende Sprache, neben Programmiersprachen, im Bereich der Informationstechnik ist. Sie haben jedoch ihren Weg in den deutschen Sprachgebrauch gefunden und sich hier etabliert.

## 2.1 Smart Home

Smart Home, aus dem Englischen übersetzt, bedeutet „intelligentes Zuhause“. Es bezeichnet das technikunterstützte Wohnen, bei dem gewisse Systeme und technische Verfahren in Wohnbereichen verbaut werden, die den Großteil der elektrischen Gerätschaften im Haus miteinander vernetzen und somit eine Kommunikation ermöglichen. Es werden dadurch Wege geschaffen den Status des Zuhauses zu erfassen und automatisiert oder manuell anzupassen. Dabei soll bei einem optimalen Zusammenspiel der Systeme vor allem die Lebensqualität des Verbrauchers erhöht werden. Des Weiteren soll Sicherheit geschaffen und die Energienutzung durch eine effiziente Verknüpfung der Endgeräte und automatisierte Abläufe optimiert werden.[2]

Erreicht wird dies durch eine Kombination mehrerer Akteure, die Teil dieser Vernetzung sind. Die Funktionsweise wird im Folgenden erläutert:

[2] Vgl. Landeskriminalamt Nordrhein-Westfalen (2016). Smart Home Technologie – Smart Home als Ergänzung zu mechanischen Sicherungen. Düsseldorf. S. 3.

Über allem steht das **Eingabegerät** des Nutzers, von dem die Befehle ausgehen und an welches Informationen auf Anfrage hin weitergeleitet werden. Hierfür können sowohl Smartphones oder Tablets, als auch kleinere Geräte wie beispielsweise Lichtschalter oder Geräte zur Sprachsteuerung, verwendet werden. Von hier aus wird ein elektronischer Befehl über das Internet oder aber auch mittels einer Kabelverbindung versandt.

Dieser Befehl trifft auf das sogenannte **Gateway**, also die Schaltzentrale, durch die sowohl jeder Befehl, als auch jede Information geleitet wird. In einem Smart Home System sind dies zumeist kleine Computersysteme, die einerseits an das Internet angeschlossen, aber auch per Kabel oder über das Stromnetz mit den anderen Akteuren vernetzt sind. Zudem werden hier bei automatisierten Prozessen auch Informationen ausgewertet und es können, auch ohne direkten Befehl des Eingabegerätes, neue Befehle erteilt werden.

Weitere Akteure des smarten Gebäudeleitsystems sind **Sensoren**, die im Haus verbaut sind und dem Nutzer, sowie dem Gateway Informationen zum aktuellen Zustand bieten. Ein Beispiel hierfür sind Temperatursensoren oder Helligkeitssensoren.

Daneben agieren die sogenannten **Aktoren**, die Signale über das Gateway erhalten und diese dann ausführen, als Befehlsempfänger. Beispiele für die hier angegliederten Endgeräte sind Heizungen oder Lichtsysteme.[3]

Ein Beispiel für den Ablauf: Der Eigentümer ruft auf seinem Eingabegerät eine App auf, über die sich das Smart Home steuern lässt. Dort wird eine gewisse Temperatur für einen Raum im Haus angegeben. Der Befehl über die Temperaturänderung wird von dem Eingabegerät an das Gateway gesendet. Hier laufen nun die Informationen aller Aktoren und Sensoren des Hauses ein. Das Gateway stellt fest, dass die vom Sensor angezeigte Temperatur nicht dem Befehl des Eingabegerätes entspricht und passt mit einem neuen Befehl die Arbeit des Aktoren, hier dem Temperaturregler der Heizung oder der

[3] Vgl. Verbraucherzentrale Nordrhein-Westfalen. Smart Home: Das "intelligente Zuhause" (2020), URL: https://www.verbraucherzentrale.de/wissen/umwelt-haushalt/wohnen/smart-home-das-intelligente-zuhause-6882 (zuletzt aufgerufen 26.04.2021).

Klimaanlage in dem betroffenen Zimmer an, bis die gewünschte Temperatur erreicht ist.

Man unterscheidet bei Smart Home zwischen kabellosen und kabelgebundenen Systemen. Diese sind dabei jedoch auch miteinander kombinierbar. Bei kabellosen Systemen findet die Kommunikation überwiegend über das Gateway Gerät statt. Also sendet, wie zuvor beschrieben, der Sensor einen Wert an das Gateway und dieses aktiviert mit einem Befehl den Aktor. Hier findet diese Kommunikation zum Beispiel über W-LAN oder Bluetooth statt, was die Flexibilität der einzelnen Geräte erhöht. Der Nachteil ist, dass meist nur die Geräte eines Herstellers bzw. vom Hersteller ebenfalls lizensierte Geräte miteinander interagieren können.[4] Hierbei erhält jedes Gerät eine individuelle Kennung, die sogenannte IP-Adresse, über welche das Gerät eindeutig zu identifizieren ist und somit eine direkte Kommunikation zielgenau aufgebaut werden kann.[5] Kabelgebundene Systeme leiten Informationen komplett über im Gebäude verbaute Kabelleitungen weiter. Somit verfügt jedes in das Smart Home Netzwerk integrierte Gerät, neben der Versorgung mit Strom, auch über ein Datenleitungskabel, dem sogenannten „Bus“. Aus diesem Grund werden diese Systeme auch als Bussysteme bezeichnet. Man kann sich dieses System wie Busfahrpläne vorstellen, in denen gewisse Daten über die Kabelleitung zu ihrem Bestimmungsort transportiert werden. Daher benötigen diese Systeme nicht unbedingt einen Netzwerkknoten wie das oben beschriebene Gateway. Möchte der Anwender aus der Ferne das System steuern, greift dieser auf einen mit dem Internet verbundenen und in diesem Bussystem verknüpften Router zu und sendet von dort die Befehle. Vorteile des kabelgebundenen Systems sind dabei vor allem die Zuverlässigkeit, da keine Funkverbindungen gestört werden können und die höhere Energieeffizienz.[6]

[4] Vgl. Tecklenborg, T. & Stupperich, A. (2018). Häuser mit Smart Home. Technologie als Ziel von Einbrechern. In Kriminalistik 2018 (4). S. 203-207. Siehe S. 204.
[5] Vgl. Appelfeller, W. & Feldmann, C. (2018). Die digitale Transformation des Unternehmens. Systematischer Leitfaden mit zehn Elementen zur Strukturierung und Reifegradmessung. Berlin: Springer Gabler. S. 154.
[6] Vgl. Rosslin, J. R. & Tai-Hoon K. (2010) A Smart Review on Security in Smart Home Development. In International Journal of Advanced Science and Technology. Vol. 15. S. 13-21.

## 2.2 Smart Car

Laut dem Marktforschungsinstitut CSA verbringt der Deutsche durchschnittlich drei Jahre und neun Monat seiner Lebenszeit im Auto.[7] Somit nimmt auch hier die smarte Vernetzung einen immer größer werdenden Stellenwert ein und wird bei höherklassigen Neuwagen bereits serienmäßig verbaut. Diese Fahrzeuge werden als Smart Car oder Connected Car bezeichnet.

Hierbei baut das Fahrzeug über ein Netzwerk, meistens das Internet, eine Verbindung zu anderen Geräten oder Diensten auf und kann somit mit diesen kommunizieren. Dabei werden Informationen aus der Umwelt gesammelt und können als Befehle weitergeleitet werden. Die Möglichkeiten reichen dabei von einfachen Fahrzeuginformationen und Navigation hin zur smarten Verkehrssteuerung, Warnung bei gewissen drohenden Wetterlagen und selbstständiges Absetzen von Notrufsignalen im Falle eines Unfalls.[8] Diese letztgenannte Funktion wird eCall genannt und wurde 2018 durch die EU verpflichtend für Neuwagen eingeführt. Dabei werden bei einem Unfall durch Sensoren oder Knopfdruck gewisse Daten wie die Position, Fahrzeugart, die genaue Zeit, angelegte Sicherheitsgurte etc. an die Notrufnummer übermittelt und eine Telefonverbindung zum Fahrzeug aufgebaut.[9] Wird zunächst ein Herstellerservicecenter informiert, nennt man dies Third-Person-Service (TPS), welcher dann als Filter für tatsächliche Notrufe agiert. Die wichtigsten Aspekte der smarten Vernetzung im Fahrzeug sind die Sicherheit der Insassen, eine effiziente Navigation und der daraus entstehende Umweltschutz, sowie das Entertainment der Insassen. Ermöglicht werden diese Funktionen über ein im Fahrzeug verbautes Steuergerät, die sogenannte Head-Unit, die

[7] Vgl. CSA Research. Citroen. Our Lives in our cars (2016), URL: http://media.citroen.de/file/39/4/etude_csa_research_citroen_our_lives_inside_our_cars_german_data.pdf?_ga=2.85728221.535594185.1617399688-1825253201.1617399688 (zuletzt aufgerufen 25.04.2021) S. 6.

[8] Vgl. BMW. Connected Car. Das vernetzte Auto (2020), URL: https://www.bmw.com/de/innovation/connected-car.html (zuletzt aufgerufen 28.04.2021).

[9] Vgl. Grabowski, T. (2018). Vernetzte Fahrzeuge: Neue Ermittlungsansätze im Strafverfahren? In Kriminalistik 2018(4). S. 208-215. Siehe S. 211.

vergleichbar mit dem oben beschriebenen Gateway alle weiteren Funktionen steuert. So können zum Beispiel bei einem eingehenden Anruf automatisch die Fenster geschlossen werden, ohne, dass der Fahrer dies händisch einstellen muss.[10] Die Fahrzeugdaten werden mittels Netzwerkverbindung von der Head-Unit aus an den Server des Herstellers gesendet und hier gesichert (die sogenannte Cloud-Funktion). Vor allem Daten wie aktuelle Position, Fahrzeugzustand, Schließzustand etc. werden hier erfasst. Der Benutzer kann vom Fahrzeug oder einem anderen Endgerät aus auf diese Daten zugreifen.[11] Das Fahrzeug besitzt eine eigene Sim-Karte und stellt selbstständig die Verbindung zum Internet her, ohne mit einem Smartphone verbunden zu sein. Zusätzlich bietet es sogar eine W-LAN Funktion im Innenraum, sodass die gesamte Kommunikation der Insassen nach Außen über das Fahrzeug generiert werden kann.

# 3 Von der Vision zur Realität

Smarte Vernetzung wird meist als Technik der Zukunft bezeichnet. Dabei entstand die Vorstellung bereits vor knapp 100 Jahren als fiktionale Zukunftsvision. Wie sie sich von der Idee bis heute entwickelte und welche Bereicherungen sich in der Zukunft ergeben werden, wird im folgenden Kapitel erläutert.

## 3.1 Ein historischer Überblick

Die Idee des vernetzten und intelligenten Zuhauses wirkt sehr modern und neu. Dabei wurde die Vision von Haushaltsgeräten, die miteinander

[10] Vgl. Ebd. S. 208.
[11] Vgl. Ebd. S. 209.

kommunizieren und den Bewohnern das Leben erleichtern bereits Anfang der 1920er Jahre geboren. Präsentiert wurde dies in dem Film „Das vollelektrische Haus“ von Buster Keaton (1922). Im Jahr 1939 erschien der Artikel „Das elektrische Haus der Zukunft“ von George H. Bucher, im „Popular Mechanics Magazine“, der sich ebenfalls mit der Vorstellung eines Hauses beschäftigte, das automatisiert den Alltag der Bewohner erleichterte.[12] Aber auch in späteren Filmen wie zum Beispiel die „Zurück in die Zukunft“-Reihe (1985-1990) wurden private Gebäude gezeigt, in denen die Haushaltsgeräte vernetzt sind. Grundsätzlich handelte es sich dabei lediglich um Fiktion, die zu dieser Zeit noch als unvorstellbare Zukunftsvision galt. Allerdings beschrieb Bucher in seinem Artikel durchaus viele Dinge sehr konkret, die heute durch die Technik ermöglicht wurden. Er berichtete von einer zentralen Steuereinheit, die ihre Befehle komfortabel von jedem Ort des Hauses empfangen konnte und von dort die einzelnen im Haushalt eingegliederten Geräte ansteuerte. Im Vordergrund standen derzeit bereits wie heute der Komfort und das erleichterte Leben für die Bewohner. Darunter wurde damals bereits die Beleuchtung, die stimmungsabhängig die Farben variiert, in Buchers Artikel beschrieben.[13]

Tatsächlich begann die technische Umsetzung von smarter Vernetzung in den 1960er Jahren im Bereich der Industrie. Hier wurden Systeme eingerichtet, die automatisch Störungen in der Elektronik meldeten. Dies scheint nicht viel mit der heutigen Vorstellung von Smart Home zu tun zu haben, jedoch wurde hier eine Kommunikationsebene zwischen mehreren Geräten geschaffen, was smarte Vernetzung im Grunde bedeutet.

Mitte der 1970er Jahre wurde erstmalig eine SPS, in Form eines Zentralrechners, in ein Gebäude verbaut. SPS steht für eine speicherprogrammierbare Steuerung, also einen Rechner, der über vorher digital programmierte Steuermodule verfügt. Vorerst werden in Abhängigkeit von bestimmten Informationen, die in das Gerät eingehen, neue Befehle über die Ausgänge

[12] Vgl. Bucher, G. (1939) The electric home of the future. In Popular Mechanics Magazine. Vol. 72 (2). Seite 162 ff.
[13] Vgl. Ebd.

weitergeleitet. Dabei kann digital festgelegt werden, bei welcher Art und welcher Anzahl an Informationen der Befehl entsandt wird. Sie stellten also die innovative digitale Form der älteren, analogen und mechanischen Relaisschaltungen dar und brachten somit Vorteile, wie Verschleißfreiheit, nahmen deutlich weniger Raum ein und boten Möglichkeiten der Fernwartung.[14]

Anfang der 1990er Jahre einigten sich die Hersteller von diversen Elektrogeräten auf ein einheitliches System der smarten Vernetzung. Somit wurde es möglich, dass auch Geräte verschiedener Hersteller miteinander kommunizieren konnten und sich so zentral steuern ließen. Da sich kommerzielle Form des Internets, noch in der Entwicklung befand, wurden für die Vernetzung der Geräte Telefonleitungen verwendet. Dies ermöglicht eine zentrale Bedienung von Steuerungen, wie dem Beleuchtungs – und Heizungssystem.

Der wirkliche Durchbruch gelang erst durch die Entwicklung der Mikroelektronik und dem damit verbunden Internet der Dinge (engl.: Internet of Things – IoT). Das ist die „Verknüpfung eindeutig identifizierbarer physischer Objekte mit einer virtuellen Repräsentation in einer internetähnlichen Struktur“[15], also die Möglichkeit Dinge aus der realen Welt mit der digitalen Welt zu vernetzen. Informationen wie zum Beispiel Zustände von Geräten, können durch Sensoren wahrgenommen und dadurch in eine digitale Information umgewandelt werden, die von da an über das Internet oder lokale Netzwerke kommuniziert werden kann. Ein Beispiel ist die Information, dass die Farbpatrone in einem Druckgerät leer ist. Der Sensor nimmt den Füllstand wahr und wandelt diese physische Information in eine digitale um, die nun an andere Geräte (z.B. einen Computer) weitergegeben werden kann. Somit wird die Lücke zwischen realer und digitaler Welt geschlossen. Diese Neuerung schuf eine Fülle an Möglichkeiten elektronische Geräte sinnvoll im Alltag einzusetzen, ohne dass der Mensch selber jeden einzelnen Prozess steuern

[14] Vgl. IT-Talents. Was ist SPS Programmierung? (2019) URL: https://www.it-talents.de/blog/it-talents/was-ist-sps-programmierung (zuletzt aufgerufen 24.04.2021)
[15] Fuhrich, A. (2016). Internet of Things. In D. Haselbauer (Hrsg.). Handbuch Digitalisierung. Die vernetzte Gesellschaft (S. 107–111). Bonn: ayway media GmbH.

oder mühsam kontrollieren muss.[16] Diese Geräte konnten nun selbstständig miteinander kommunizieren. Neben der industriellen Nutzung konnte dies auch im privaten Bereich mit der Vernetzung von im Haushalt verwendeten elektrischen Geräten angewendet werden. Die technische Grundlage für smarte Geräte wurde geschaffen.

Von da an machte die Technik enorme Fortschritte und entwickelte sich schnell weiter. Zu Beginn der 2000er Jahre wurde smarte Vernetzung, aufgrund des hohen Preises für Hardware und technische Umsetzung, lediglich in Luxusimmobilien verwirklicht. Somit war Smart Home für die wenigsten überhaupt ein Begriff oder in den eigenen vier Wänden realisierbar. In München wurde im Rahmen der Bundesgartenschau 2005 das „Haus der Gegenwart" errichtet. Hier ließen sich erstmals alle elektronischen Vorgänge im Gebäude zentral über einen Touchscreen Monitor steuern. Neben dem Komfort rückte nun auch die Energieeffizienz weiter in den Mittelpunkt. So wurden Systeme und Musterhäuser entwickelt, die zum Beispiel in der kalten Jahreszeit die Fenster geschlossen hielten und die Räume durch eine Belüftungsanlage mit frischer Luft versorgten, oder an warmen Tagen automatische Rollladen aktivierten, die vor direkter Sonneneinstrahlung schützten.[17] Maßgeblich für den weiteren Ausbau der Smart Home Systeme war dabei der Vormarsch des Smartphones und damit die Möglichkeit das vernetzte Haus von überall zu steuern.

Von den Innovationen beeindruckt wuchs die Anzahl der Bauherren, die ihre Häuser mit smarter Technik ausstatten ließen. Mit der steigenden Nachfrage wurde das Angebot an Geräten und Systemen immer größer und die Vielfalt an Funktionen nahm zu. Die Installation von drahtlosen Netzwerken, Bluetooth Verbindungen etc. machten aufwendige und kostenintensive

[16] Vgl. Mattern, F. (2005). Die technische Basis für das Internet der Dinge. In: Fleisch E.n & Mattern F. (Hrsg.) Das Internet der Dinge. (S. 39-66) Berlin: Springer.
[17] Vgl. Smartest Home. Die Historie des Smart Home von 1963 – 2021: Meilensteine. (2021) URL: https://www.smartest-home.com/smart_home_historie_1939_2019/ (zuletzt aufgerufen 29.04.2021).

Verkabelungen überflüssig. Die Realisierung von smarter Vernetzung im eigenen Haushalt wurde so attraktiver.

Die Entwicklung des Connected Car begann dabei deutlich später. Als Vorläufer könnten diverse Rennfahrzeuge gesehen werden, die bereits in den 80er Jahren Fahrzeugdaten automatisiert an den Leitstand senden konnten, um damit jederzeit einen aktuellen Blick auf die Fahrzeugmesswerte zu ermöglichen. Kommerziell wurde die smarte Vernetzung im Fahrzeug allerdings erst im Jahr 1996. Hier wurde durch General Motors in Zusammenarbeit mit Motorola das „OnStar" System entwickelt, welches den Insassen ermöglichte in Notfallsituationen über einen Knopf im Innenraum, meistens am Innenspiegel verbaut, Kontakt zu einem Mitarbeiter des Servicecenters aufzunehmen und diesem den Notfall zu schildern.[18] In den Folgejahren wurden die Systeme von weiteren Herstellern aufgegriffen und weiterentwickelt. In den 2000er Jahren wurde das vorher ausschließlich militärisch genutzte Global Positioning System (kurz: GPS) auch für den zivilen Bereich freigegeben. Dadurch wurde ermöglicht, dass im Notfall auch umgehend der Standort übermittelt werden kann. Neben der Sicherheit wurde nun auch der Komfort verbessert, indem die Telematik Einzug erhielt. Es konnten Fahrzeugdiagnosen direkt an den Hersteller gesendet werden, ohne dass eine Werkstatt aufgesucht werden musste. Ab 2004 wurden die ersten Fahrzeuge mit eigenen Sim-Karten ausgestattet, was eigenständiges Telefonieren und einen Internetzugang ermöglichte. Nach der Einführung des Smartphones 2007 und dem damit verbundenen Erfolg, entwickelte auch die Automobilindustrie Möglichkeiten der Vernetzung. So bot das Fahrzeug nun einen Internet Hotspot und W-LAN im Innenraum, um den Insassen eine sichere Internetverbindung zu ermöglichen.[19] Auch wurden Apps entwickelt, die beispielweise ermöglichen das Fahrzeug zu steuern, Beleuchtungseinrichtungen zu verändern, die Standheizung nach Uhrzeit zu steuern oder Fahrzeugtüren zu öffnen, sowie zu

[18] Vgl. OnStar (2016) The Evolution of OnStar, URL: https://www.onstar.com/us/en/articles/tips/evolution-of-onstar-innovations/ (zuletzt aufgerufen 28.04.2021).
[19] Vgl. BMW. (2020).

verriegeln. Es wäre darüber hinaus technisch bereits möglich über diese Steuerung den Motor per Smartphone zu starten und das Fahrzeug sogar zu fahren.[20]

## 3.2 Der derzeitige Stand

Laut einer Statistik des Statista Digital Market Outlooks von Juni 2020 befindet sich in Deutschland in ca. 7,2 Millionen Haushalten mindestens eine Smart Home Anwendung im Einsatz.[21] Dabei könnte sich die Zahl laut der Prognosen in den kommenden Jahren mehr als verdoppeln. Die meisten Haushalte verwenden die smarte Vernetzung dabei zur Steuerung der Beleuchtung (23%), für die Alarmanlage (18%) oder für die Raumklimatisierung (15 %).[22]

Es ist heutzutage möglich beinahe jedes elektrische Gerät, kabelgebunden oder per W-LAN, mit dem gesamten Netzwerk zu verbinden, wodurch eine Kommunikation ermöglicht wird. So kann sowohl lokal im Gebäude selber, als auch via Internet von jedem anderen Ort, auf das Heimnetzwerk zugegriffen und dies gesteuert werden. Die Möglichkeiten sind weitreichend und erstrecken sich, wie zuvor erwähnt, über die Steuerung der Klimatisierung, die Aktivierung von Staubsaug- oder Mährobotern, über Geräte zur Erhöhung der Sicherheit bis hin zur Steuerung des Energieverbrauchs.[23]

Besonders beeindruckend ist dabei die Möglichkeit eine Vielzahl von Vorgängen, die smart vernetzte Geräte beinhalten auch über Sprachbefehle zu steuern. Das Steuergerät bzw. das Sprachsteuerungsempfangsgerät wird

[20] Vgl. Ebd.
[21] Vgl. Brandt, M. (2020). Smart Home. Deutschlands Haushalte werden immer smarter, URL: https://de.statista.com/infografik/3105/anzahl-der-smart-home-haushalte-in-deutschland/ (zuletzt aufgerufen 26.04.2021).
[22] Vgl. Rohleder, B. (2020). Das intelligente Zuhause: Smart Home 2020. Berlin. Bitkom Research S. 3.
[23] Vgl. CosmosDirect. (2020). Smart Home: Definition, Entwicklung, Vorteile, URL: https://www.cosmosdirekt.de/smart-home/definition/ (zuletzt aufgerufen 05.05.2021).

direkt angesprochen und dadurch aktiviert. Bekannte Beispiele sind Alexa von der Firma Amazon oder Google Home von Google. Nach der Ansprache und der Aktivierung des Gerätes wird ein Befehl ausgesprochen. Der Programmierung sind hierbei nahezu keine Grenzen gesetzt. Ein Beispiel für einen Sprachsteuerungsbefehl wäre „Alexa, aktiviere das Heimkino“. Der Befehl wird bestätigt und an das Steuerungsgerät weitergeleitet. Von hier aus gehen dann diverse Anweisungen an verbundene Geräte. Die Jalousien werden geschlossen, das Licht wird gedimmt, das smarte Fernsehgerät wird gestartet und die damit verbundene Lautsprecheranlage schaltet sich ein.[24]

## 3.3 Ein Blick in die Zukunft

Bereits heute sind die Möglichkeiten, die Smart Home bietet, sehr vielfältig. Nichtsdestotrotz wird Smart Home meistens als Technologie der Zukunft bezeichnet und den meisten Menschen ist gar nicht bewusst, welches Potenzial es bietet. Dabei kommen immer mehr elektrische Geräte auf den Markt, die auch eine Version mit smarter Vernetzung besitzen, wie zum Beispiel der smarte Kühlschrank, das smarte Bewässerungssystem für den Garten oder die smarte Lichtanlage.[25] Zudem ist die Technik nicht mehr ausschließlich für Inhaber von Luxusimmobilien bezahlbar, da immer mehr Produkte auf den Markt kommen und der Preis sich somit nach unten reguliert. Es ist davon auszugehen, dass der smarte Aspekt in Geräten zunehmend zum Standard wird und dieser keine zusätzliche Funktion mehr darstellt. Neben dem Entertainment und dem Komfort gewinnen vor allem auch die Sicherheit, Energieeffizienz, Kommunikation und Nachhaltigkeit immer mehr an Gewicht. Dazu gehört ebenfalls die smarte Vernetzung des Fahrzeugs, also das Connected

[24] Vgl. Wießner, N. (2020). Cyber Security. Welche Bedrohungen und Abwehrmaßnahmen gibt es für Smart Home-Geräte?. Studienarbeit. München: GRIN Verlag S. 14.
[25] Wulf, D. (2020). Smart Home - Visionen für unser Zuhause, URL: https://www.homeandsmart.de/wohnen-in-der-zukunft (zuletzt aufgerufen 25.04.2021).

Car. So ist durchaus denkbar, dass das Fahrzeug dem Smart Home zum Beispiel eigenständig die Ankunftszeit mitteilt, um das Eintreffen des Benutzers vorzubereiten. Dies geschieht indem das Haus auf eine gewünschte Raumtemperatur gebracht wird, sich das Licht anschaltet oder das Essen im Backofen aufgeheizt wird.[26]

Es ist denkbar, dass das Fahrzeug mehr mit seiner Umwelt und anderen Fahrzeugen, sowie Fußgängern kommuniziert. Teile davon sind heute bereits möglich. Zum Beispiel, dass durch Standortermittlungen festgestellt wird wo sich viele Fahrzeuge befinden. Diese Daten können an das Navigationssystem weitergeleitet und somit effizientere Routen berechnet werden. Weiterhin könnten sich durch diese Technik vorausfahrende oder kreuzende Fahrzeuge austauschen, um Kollisionen zu verhindern. Bestimmte Verkehrsdaten könnten genutzt werden, um Lichtzeichenanlagen effizienter zu steuern und somit den Verkehrsfluss zu erhöhen und die Umweltbelastung zu minimieren. Das Fahrzeug dient demnach nicht nur als Fortbewegungsmittel, sondern wird durch die Vernetzung gänzlich in das tägliche Leben integriert, indem es mit anderen smarten Geräten kommuniziert. So wird der über das Smartphone in den digitalen Kalender eingetragene Termin beim Einsteigen in das Fahrzeug automatisch an das Navigationsgerät gesendet, welches dann unter Beachtung der ständig aktualisierten Verkehrsinformationen, die optimale Route berechnet. Außerdem ist die Vernetzung des Fahrzeuges ein weiterer Schritt in Richtung autonomes Fahren.[27]

Allgemein lässt sich sagen, dass sich der Bereich smarte Vernetzung mehr und mehr im Alltag etablieren wird. Besonders entscheidend sind dabei auch die Aspekte, dass sie sich sehr vielseitig verwenden und somit auf aktuelle Gegebenheiten anpassen lassen. Ein aktuelles praktisches Beispiel ist die COVID 19 Pandemie, die viele Unternehmen dazu brachte ihr Personal im Home Office einzusetzen. Aber auch Universitäten und Schulen verlagerten Vorlesungen und Unterricht nach Hause. Hier bekommen smarte Lösungen

[26]Vgl. Ebd.
[27] Vgl. BMW. (2020).

für das Eigenheim einen immer größeren Stellenwert, da man noch mehr Zeit zu Hause verbringt. Ein weiterer Punkt ist die Vielseitigkeit. So könnte Smart Home auch als Unterstützung im Alltag für Senioren verwendet werden, um zum Beispiel gewisse Tätigkeiten im Haushalt, wie Staubsaugen oder Kochen zu übernehmen.[28] Auch Aspekte wie Umweltschutz und Nachhaltigkeit werden bedacht. Diese können berücksichtigt werden, indem alle Komponenten wie Heizung und Belüftungssysteme gemeinsam agieren und somit zum Beispiel verhindern, dass die Heizung in Betrieb ist, während alle Fenster dauerhaft zum Lüften geöffnet sind.

Ein weiterer Begriff der sich in diesem Zusammenhang ergibt sind Smart Cities, also intelligente Städte, in denen eine Vernetzung zwischen allen relevanten elektrischen Geräten, Fahrzeugen und Lebewesen besteht. Sämtliche Daten werden gesammelt, gespeichert und können bei Bedarf genutzt werden. Ziel der Vernetzung ist es, eine Infrastruktur aufzubauen, die es ermöglicht, dass die richtigen Ressourcen zur rechten Zeit am richtigen Ort bereitgestellt werden. Ziel ist, die Effizienz in Städten zu erhöhen, die Umwelt zu schützen und die Sicherheit und den Komfort für die Personen zu erhöhen.[29]

## 3.4 Der Aspekt der Sicherheit

Der Aspekt der Sicherheit ist ein vielbeachteter Bereich des Smart Homes. Welche Komponenten es hierbei gibt und wie diese funktionieren, soll im Folgenden näher erläutert werden.

Zum Sicherheitsaspekt zählt vor allem die Kameraüberwachung im gesamten Außen-, aber auch dem Innenbereich des Objektes. Diese können miteinander vernetzt und auch aus der Ferne, zum Beispiel mit dem Smartphone,

[28] Vgl. Wulf. (2020).
[29] Vgl. EnBW. (2021) Smart Cities, URL: https://www.enbw.com/energie-entdecken/gesellschaft/smart-cities (zuletzt aufgerufen 26.04.2021).

angesteuert werden. Dabei erhält der Benutzer ein aktuelles Livebild und kann, je nach Modell, die Kamera in alle Richtungen bewegen. Durch meist integrierte Infrarotleuchten kann die Kamera auch bei völliger Dunkelheit aufzeichnen und bietet detaillierte Bilder. Zusätzlich wird auch der Ton des Livebildes übertragen und der Benutzer kann sogar über einen in der Kamera verbauten Lautsprecher in den Raum hineinsprechen. Zudem befindet sich die Kamera immer in einem Überwachungsmodus und kann bei Bewegung oder einem Geräusch im videografierten Bereich einen Alarm per E-Mail oder Pushnachricht auf das Endgerät des Benutzers schicken. Dazu wird ein Livemitschnitt auf dem Gerät oder in der Cloud gespeichert und dem Alarm angehängt. Der Benutzer kann sofort reagieren, indem er kontrolliert, wer oder was den Alarm ausgelöst hat. Werden die Kameras mit zusätzlichen Programmen verknüpft, können sie eigenständig gewisse Bewegungsmuster, wie zum Beispiel Sturzbewegungen, analysieren und bei erkannter Gefahr alarmieren. Dies könnte vor allem bei älteren Benutzern zum Beispiel in Seniorenheimen eine große Rolle spielen und mitunter schwere Folgen verhindern.

Ein weiterer Aspekt sind smarte Alarmanlagen. Dazu gehören vor allem Kontakte in Türen oder Fenstern, aber auch Bewegungsmelder in gewissen Bereichen. Sind diese Geräte scharf gestellt und registrieren eine Bewegung wie beispielweise ein Öffnen von Fenster oder Türen, wird der Benutzer ebenfalls auf seinem Endgerät informiert. Je nach Programmierung kann hier auch die Benachrichtigung eines Sicherheitsdienstes erfolgen. Ebenso könnte eine Alarmsirene, mit einem deutlich sichtbaren optischen und hörbaren akustischen Signal, aktiviert werden.[30] Bei einer zusätzlich verbauten und im Smart Home vernetzten Kameraüberwachung wird diese nun automatisch aktiviert bzw. könnte in den betroffenen Bereich geschwenkt werden und die Aufnahmen automatisch speichern. Die meisten smarten Alarmanlagen sind mit einem gesonderten Sabotageschutz ausgestattet, in dem sie sich in einem weiteren gesicherten Gehäuse befinden, welches schwer zu manipulieren ist und über Erschütterungssensoren verfügt, die bei Bewegung am Gerät ebenfalls

[30] Vgl. Home and Smart (2021). Smart Home Sicherheit – wie sicher ist das smarte zu Hause?, URL: https://www.homeandsmart.de/sicherheit (zuletzt aufgerufen 26.04.2021).

alarmieren. Auch eine Notstromversorgung über integrierte Akkus macht die Geräte weniger angreifbar gegen physische Angriffe von außen.[31]

Darüber hinaus gibt es smarte Türklingeln. Stellen diese im Bereich der Haustür eine Bewegung fest oder wird der Knopf der Türklingel betätigt, erhält der Benutzer eine Benachrichtigung und ein Livebild des Eingangsbereiches auf das Endgerät. Über eine Gegensprechanlage kann der Benutzer Kontakt zu der Person vor der Haustür aufnehmen, ohne dass er sich selber im Haus befinden muss. Damit gekoppelt sind oft auch elektronische Türschlösser. Diese lassen sich „individuell per Smartphone, Zahlen-Kombination, Bluetooth-Verbindung, Fingerabdruck oder Karte öffnen und schließen“.[32] Auch eine Gesichtserkennung wäre denkbar, ist allerdings noch nicht ausgereift genug, um den Sicherheitsstandards zu genügen. Eine Türöffnung per Sprachbefehl ist dabei jedoch schon möglich. So kann aus der Ferne zum Beispiel Handwerkern oder den Kindern nach der Schule die Tür geöffnet werden, ohne dass man selber physisch anwesend ist. Ist das Fahrzeug Teil der smarten Vernetzung, könnte sich zudem die Tür oder ein Tor öffnen, sobald dieses die Auffahrt befährt. Gerade im Hotel- oder Ferienwohnungsgewerbe stellt dies eine lukrative Möglichkeit dar. Hier kann Personen temporärer Zutritt ermöglicht werden, ohne den Schlüssel herauszugeben. Zudem stellt das elektronische Schloss oftmals eine Abschreckung dar, da es vermuten lässt, dass weitere Sicherheitstechnik im Haus verbaut ist. Im Notfall lässt sich das Schloss dabei weiterhin mit einem herkömmlichen Schlüssel öffnen und schließen. [33]

Ebenfalls zu den Sicherheitsaspekten eines Smart Homes gehören Systeme wie Rauch- und Kohlenmonoxid-Detektoren. Wird hier ein gewisser Richtwert überschritten, erhält der Benutzer umgehend eine Benachrichtigung. Erfolgt keine Reaktion des Benutzers wird der Serviceanbieter oder der Notruf informiert. Zusätzlich kann eine Aktivierung von optischem und akustischem

[31] Vgl. Wendel, M. (2021). Alarmanlagen Test-Übersicht 2021: Alarmsysteme im Vergleich, URL: https://www.homeandsmart.de/alarmanlagen-test-uebersicht (zuletzt aufgerufen 26.04.2021).
[32] Vgl. Dies. (2020). Elektronische Türschlösser Test 2021: Nachrüstlösungen Vergleich, URL: https://www.homeandsmart.de/tuerschloesser-tueroeffner-smart-home-besten (zuletzt aufgerufen 26.04.2021).
[33] Vgl. Ebd.

Alarm erfolgen. Je nach Programmierung können auch weitere Schritte erfolgen wie zum Beispiel bei einer kritischen Kohlenmonoxid - Konzentration, die Aktivierung der Belüftungsanlage oder das Öffnen der Fenster. Auch kann bei Erkennen einer Gefahr automatisch über die Smart Home Zentrale eine Ausleuchtung des Fluchtweges erfolgen, indem gewisse Lichtsysteme im Haus aktiviert werden, um dem Bewohner eine schnelle und leichtere Orientierung zu ermöglichen.

Im Rahmen der Sicherheit gehören auch Anwesenheitssimulationen zu einer Smart Home Anlage. Laut der polizeilichen Kriminalstatistik wurde 2020 in Deutschland ca. 75.000-mal ein Einbruch polizeilich dokumentiert.[34] Allein in NRW wurde im Jahr 2019 laut Polizeilicher Kriminalstatistik fast 23.000-mal eingebrochen.[35] Die Zahlen sind in den letzten Jahren weiter rückläufig, jedoch stellen Einbrüche immer noch ein bedeutendes Delikt dar. Dabei werden überwiegend Gebäude aufgesucht, in denen sich zur Zeit des Einbruchs niemand aufhält. Eine Anwesenheitssimulation erweckt dabei durch wenige Steuerungen den Eindruck, dass sich Personen im Haus aufhalten. Dazu gehört vor allem die automatische Einschaltung der Beleuchtung in einzelnen Teilen des Hauses. So könnte zum Beispiel morgens und abends die Beleuchtung im Badezimmer oder dem Flur eingeschaltet werden. Dies kann koordiniert über eine Programmierung erfolgen, ohne dass der Benutzer die Lampen einzeln ansteuert. Zusätzlich wird eine künstliche Anwesenheit durch unterschiedlichste Geräusch- und/oder Lichtkulissen erzeugt. Dies kann beispielsweise durch das Einschalten von Musik tagsüber, aber auch durch Lichteffekte, die das Flackern des Fernsehbildes simulieren, erreicht werden. Zudem können Jalousien zu bestimmten Zeiten hoch und herunter gefahren werden, um dem Gebäude einen bewohnten Eindruck zu verleihen. Auch im Außenbereich gibt es diverse Möglichkeiten. Einerseits können dunkle Ecken im Außenbereich automatisch beleuchtet werden können, andererseits können

[34] Vgl. Bundesministerium des Innern, für Bau und Heimat. (2021) Polizeiliche Kriminalstatistik 2020. Ausgewählte Zahlen im Überblick. Berlin S. 16.
[35] Vgl. Landeskriminalamt Nordrhein-Westfalen. (2020). Datenanalytische Bekämpfung des Wohnungseinbruchs in NRW weiter verstärkt, URL: https://polizei.nrw/datenanalytische-bekaempfung-des-wohnungseinbruchs-in-nrw-weiter-verstaerkt (zuletzt aufgerufen 26.04.2021).

automatisierte Gartenarbeiten, wie Rasensprenger oder Mähroboter, den Eindruck erwecken, dass der Garten vor kurzem noch gepflegt worden ist.[36]

# 4 Risiken durch kriminelle Nutzung

Neben der Fülle an Innovationen und Erleichterungen, die Smart Home mit sich bringt, birgt die Installation auch Risiken. Vor allem dann, wenn sie durch kriminelle Handhabung dazu genutzt wird gegen die eigentlichen Bewohner zu agieren. Ein großer Gefahrenbereich ist das Hacking der computer- und internetgestützten Systeme, wodurch Unbefugten sogar das Betreten des Hauses und Umgehen der Sicherheitsvorkehrungen ermöglicht wird. Straftaten dieser Art werden unter dem Begriff Cybercrime zusammengefasst.

## 4.1 Cybercrime

Die offizielle Definition des Bundeskriminalamtes für Cybercrime oder auch Computerkriminalität lautet: „Cybercrime umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne) oder die mittels dieser Informationstechnik begangen werden.“[37] Somit stellen die Delikte im Cybercrimebereich eine enorme Bandbreite dar. Grund dafür sind vor allem die vielfältigen Möglichkeiten, die sich durch das Internet bieten. Der Computer bzw. das

[36] Vgl. Wendel, M. (2020) Anwesenheitssimulation: Diese smarten Möglichkeiten gibt es, URL: https://www.homeandsmart.de/anwesenheitssimulation-im-smart-home (zuletzt aufgerufen 27.04.2021).
[37] Vgl. Bundeskriminalamt. (2021) Cybercrime, URL: https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_node.html (zuletzt aufgerufen 01.05.2021).

Endgerät dient dabei als Tatwerkzeug, Vermittler oder Ziel des Angriffs. Klassische Delikte im engeren Sinne sind der Computerbetrug (§ 263a StGB), das Ausspähen und Abfangen von Daten und deren Verbreitung (§§ 202a-c StGB), die Fälschung beweiserheblicher Daten (§ 269 StGB), Täuschung im Rechtsverkehr bei Datenverarbeitung (§ 270 StGB), Falschbeurkundung bzw. Urkundenunterdrückung im Zusammenhang mit Datenverarbeitung (§§ 271, 274 I Nr. 2, 348 StGB), Datenveränderung (§ 303 a StGB) und die Computersabotage (§ 303 b StGB).[38] Im weiteren Sinne umfasst Cybercrime jedoch auch Delikte, die über das Internet begangen werden, jedoch nicht das Internet selbst betreffen. Beispiele dafür sind der illegale Handel mit Drogen oder Waffen, die Herstellung und Verbreitung von Kinderpornografie oder die digitale Erpressung. Im Folgenden werden nun einige strafbare Handlungen genauer betrachtet.

Ein Begriff, der oft im Bereich Cybercrime genannt wird, ist das „Phishing". Hier wird die digitale Identität eines Opfers entwendet, was oft den Beginn einer strafbaren Handlung im Cybercrime Bereich darstellt. Die digitale Identität ist dabei das Recht bzw. auch die Möglichkeit eines bestimmten Nutzers und seiner Daten, sich im Internet zu bewegen. Dazu gehören auch alle Passwörter und Accounts, die der Nutzer verwendet, zum Beispiel um auf das Online Banking, den E-Mail-Account oder das firmeninterne Netzwerk zuzugreifen.[39] Der Diebstahl selber erfolgt auf unterschiedliche Art und Weise. Meist erhalten die Opfer dubiose E-Mails, die einen Internetlink oder Anhang beinhalten. Oft sind diese Anhänge Microsoft-Office Dokumente, wodurch sie unscheinbar und vertrauenserweckend wirken. Öffnet der Nutzer eines der beiden gelangen Malware, also schädliche Programme, in das IT-System und legen persönliche Daten des Nutzers offen. Diese digitale Identität kann dann durch den kriminellen Nutzer selbst verwendet, oder auch an Dritte verkauft werden, ohne dass der Eigentümer davon überhaupt Kenntnis erlangt. Gelangen folglich Unbefugte in geschützte private bzw. firmeninterne Bereiche,

[38] Vgl. Dannewitz, J. (2020) Cybercrime: Grundlagen über die Delikte im Internet, URL: https://www.dr-datenschutz.de/cybercrime-grundlagen-ueber-die-delikte-im-internet/ (zuletzt aufgerufen 26.04.2021).
[39] Vgl. Bundeskriminalamt. (2020). S. 7.

können hier auch weitere Daten offengelegt werden. Die Begehung weiterer Straftaten ist von hier aus möglich.

Eine weitere Form von Cybercrime ist die Infizierung eines Computernetzwerkes mit „Ransomeware“ und die darauffolgende Erpressung der Privatperson oder des gesamten Unternehmens. Die Bezeichnung stammt dabei vom englischen Wort für Lösegeld „ransom“. Dabei wird Malware, meist über E-Mail Anhänge oder Links in ein Netzwerk eingeschleust. Diese befällt im Anschluss Teile des IT-Systems, wie Netzwerkordner oder Dateien und verhindert den Zugriff des rechtmäßigen Nutzers. Im Anschluss wird dieser aufgefordert ein Lösegeld, meist in Form von Kryptowährung wie Bitcoins, zu zahlen, andernfalls werden die Daten veröffentlicht, gelöscht oder der Zugriff weiterhin gesperrt. Für private Personen kann dies der Verlust einer großen Menge privater und sensibler Daten bedeuten. Durch die Veröffentlichung kann neben finanziellem Schaden auch bedeutender sozialer oder psychischer Schaden entstehen. Für Unternehmen, die auf Computernetzwerke angewiesen sind, kann dies zu einer Einstellung der Geschäftsfähigkeit und somit zu enormen finanziellen Einbußen führen.[40]

Neben den beiden genannten Beispielen, gibt es viele weitere Formen der Kriminalität, die über das Internet erfolgen. Die immer professioneller werdenden Täter agieren sehr gut organisiert und sind meist global vernetzt. Die Fallzahlen sind in den vergangenen Jahren durchgehend steigend. Im Jahr 2019 wurden insgesamt 100.514 Fälle von Cybercrime polizeilich registriert. Dies stellt ein Wachstum von 15,4 % im Vergleich zum Vorjahr dar. Ein Rückgang um 6,6 % zeigte sich bei der Aufklärungsquote auf 32,3 % im Vergleich zum Jahr 2018.[41] Dabei sind hier nur die polizeilich registrierten Straftaten benannt, das sogenannte Hellfeld. Es kann davon ausgegangen werden, dass gerade in diesem Deliktsbereich ein enormes Dunkelfeld besteht. Verursacht wird dieses, da es bei den meisten Angriffen im Stadium des Versuches bleibt, da diese von einem Sicherungssystem abgefangen werden. Außerdem

[40] Vgl. Ebd. S. 20-23
[41] Vgl. Ebd. S. 47

bemerken die meisten Geschädigten gar nicht oder erst sehr viel später, dass sie Opfer eines Cyberangriffs geworden sind. Zudem werden viele Angriffe auf Unternehmen gar nicht erst angezeigt, um das Vertrauen der Kunden nicht zu verlieren oder da der Angriff nach der Zahlung eines Lösegeldes schnell beendet wurde.[42]

In Deutschland ist das Bundeskriminalamt für die Bekämpfung von Cybercrime zuständig. Dazu wurde am 01.04.2020 eigens die Abteilung Cybercrime eingerichtet, die sich vor allem der „Identifizierung, Lokalisierung und strafrechtlichen Verfolgung der kriminellen Akteure“[43] widmet. Erschwert wird dies zunehmend durch die ständige technologische Weiterentwicklung, den daraus resultierenden Raum für Straftaten und die Möglichkeit diese zu Verdunkeln. Wichtig bei der Verfolgung der Straftaten ist vor allem die enge Zusammenarbeit von regionalen, nationalen und internationalen Behörden untereinander. Außerdem sind die Strafverfolgungsbehörden auf Mithilfe aus dem Bereich der Wirtschaft und privater Unternehmen angewiesen.

## 4.2 Sicherheit von Smart Home Gebäuden

Durch die Verwendung von Smart Home Geräten wird das tägliche Leben um ein Vielfaches erleichtert und komfortabler. Jedoch birgt dies auch große Sicherheitslücken für den Nutzer. Da die meisten Smart Home Systeme über das Internet vernetzt sind und darüber kommunizieren, besteht auch das Risiko über eben jenes angegriffen zu werden. So wird der Sicherheitsaspekt vieler einfacher Geräte im Smart Home Bereich aus Kostengründen außer Acht gelassen oder nur geringfügig behandelt. Jedes dieser Geräte stellt einen kleinen Computer dar, der für sich alleine angegriffen werden kann und somit als Einfallstor für Hacker dient. Die kleinste W-LAN gesteuerte Glühbirne

[42] Vgl. Ebd. S. 3
[43] Vgl. Bundeskriminalamt. (2021).

kann ein Sicherheitsrisiko darstellen, von wo aus dem kriminellen Nutzer ein Einstieg in das gesamte System gelingt. Das Endgerät, wie zum Beispiel das Tablet oder das Smartphone, verwendet oftmals keine Authentifizierung oder Verschlüsselung für die Kommunikation mit dem Heimnetzwerk. So können professionell agierende Hacker leicht auf diese Kommunikation zugreifen und sich diese zu Nutze machen. Deshalb sollte darauf geachtet werden, dass diese Geräte immer über die aktuellste Software und somit den optimalen Schutz verfügen.[44]

Ein weiteres Risiko geht von dem allgemeinen Heimnetzwerk aus, in welchem die Geräte miteinander verbunden sind. Auch dieses kann durch Unbefugte infiltriert werden, wodurch diese Einblick in bestimmte Muster und Nutzungen erhalten. Gleichzeitig kann hier auch Schadsoftware in das System gespeist werden, welche dem Nutzer den Zugang zu gewissen Funktionen verwehrt oder Dritten die Kontrolle über Funktionen zusichert.

## 4.3 Wohnungseinbruchdiebstahl

Ein normaler Wohnungseinbruchdiebstahl (gemäß § 244 I Nr. 3 StGB) geschieht meistens schnell, koordiniert und unbemerkt. Dabei stellt dieses Delikt eines der größten Einflüsse auf das Sicherheitsempfinden der Bevölkerung dar. Grund dafür ist neben dem materiellen auch der psychische Schaden, da der Täter in die Privatsphäre der Opfer eingedrungen ist. Vor allem die Angst erneut Opfer zu werden ist dabei sehr hoch. Die Täter haben in über 40 % der Fälle eine Vorbeziehung zum Opfer.[45] Die übrigen gliedern sich überwiegend in Einzeltäter oder organisierte, häufig internationale Banden. Demnach muss nicht jeder Einbruch durchgeplant und koordiniert sein.

[44] Vgl. Tecklenborg et. al. (2018). S. 204.
[45] Vgl. Landeskriminalamt Nordrhein-Westfalen (2017). Forschungsbericht Wohnungseinbruchdiebstahl. Basisbericht. Düsseldorf. S. 16f.

Vielfach handelt es sich auch um kurzentschlossene Taten im Rahmen von Beschaffungskriminalität. Das klassische und professionelle Vorgehen bei Wohnungseinbruchdiebstahl beinhaltet dabei zunächst die Auskundschaftung potenzieller Gebäude, um festzustellen wann ein günstiger Zeitpunkt für den Einbruch vorliegt. Ist dieser Zeitpunkt gefunden wird durch mechanische Gewalt ein Zugang geschaffen. Oftmals geschieht dies durch Aufhebeln des Fensters oder der Türen mittels Werkzeugs wie Schraubendreher oder Stemmeisen, seltener auch durch stumpfe Gewaltanwendung. Befinden sich die Täter im Gebäude wird schnell und koordiniert durchsucht, um innerhalb kürzester Zeit eine möglichst hohe Beute zu erzielen. Im Anschluss wird das Haus in der Regel durch den vorher geschaffenen Zugang auch wieder verlassen. Der Einbruch wird dann erst bei der Rückkehr der Bewohner des Hauses bemerkt.

### 4.3.1 Einbruch in smarte Gebäude - Kabellose Systeme

Im Grunde unterscheidet sich die Vorbereitung von Tätern bei Einbrüchen in Smart Home Gebäude im Vergleich vom reinen Ablauf her nicht wesentlich. Auch hier wird zunächst das Gebäude ausgekundschaftet. Dies erfordert jedoch bei kabellosen Systemen nicht unbedingt die physischen Präsenz des Täters am Tatobjekt. Vielmehr ist es sogar möglich, dass sich der Täter an jedem internetfähigen Ort der Welt aufhält und von hier aus die Observation durchführen kann. Dazu muss der Täter nicht unbedingt über große Kenntnisse im IT-Bereich verfügen. Oftmals veröffentlichen die Opfer selbständig Informationen über ihren gegenwärtigen Aufenthaltsort über die sozialen Netzwerke. So werden Bilder oder Berichte aus dem Urlaub oder zum Beispiel vom Arbeitsplatz veröffentlicht und geben den Tätern darüber wichtige Informationen, wann ein Einbruch möglichst risikolos durchgeführt werden

kann.[46] Gelingt es dem Täter darüber hinaus Zugriff auf die im Haus verbauten und vernetzten elektronischen Geräte zu bekommen, können diese dazu eingesetzt werden die Bewohner auszuspähen. So gelingt der Eingriff auf W-LAN Kameras sehr einfach über das Internet. Sind diese im gesamten Haus verbaut, kann darüber festgestellt werden, wann die Bewohner sich in dem Gebäude befinden, wo sie sich aufhalten und sogar worüber sie sprechen. Durch die gesammelten Informationen werden Bewegungsprofile erstellt, die den üblichen Tagesablauf der Bewohner aufzeigen. Wann verlassen die Bewohner jeweils üblicherweise das Haus und wann kehren sie zurück? Was sind weitere Gewohnheiten, die dienlich sind um einen Einbruch durchzuführen? Gibt es in dem Haus beispielweise einen Hund, der anschlagen könnte? Über die Kameras und andere Tonmedien, wie zum Beispiel das Babyphone, den Sprachassistenten oder auch den smarten Fernseher kann zusätzlich das gesprochene Wort abgehört werden. Auch hier können nützliche Informationen, wie zum Beispiel anstehende Termine, Passwörter bzw. Zugangscodes oder Ablageort von Wertsachen abgegriffen werden. Neben der eigenen Nutzung durch den agierenden Täter, können die gewonnenen Informationen auch an Dritte weitergegeben bzw. verkauft werden. Gerade im Bereich von sehr sensiblem Bild- und Tonmaterial kann dies schwerwiegende Folgen für das Opfer haben.

Ein weiterer Schritt ist der Hack in das Smart Home System selber, um die Netzwerkkommunikation zu bestimmen. Hierdurch kann bestimmt werden, welche Geräte Teil des Smart Home Netzwerkes sind und wie sie untereinander kommunizieren. Da bei kabellosen Systemen die Kommunikation über Funk abläuft, wird dieses Signal abgefangen und aufgezeichnet. So kann der Angreifer im späteren Verlauf das Signal eigenständig nutzen, um zum Beispiel Türen zu öffnen oder Alarmanlagen abzuschalten. Besonders einfach ist dies über W-LAN Systeme, da hier nur ein Nutzername und ein Passwort überwunden werden müssen. Häufig wird dazu ein sogenannter Brute-Force Angriff verwendet.[47] Diese Methode bezeichnet das automatisierte,

[46] Vgl. Tecklenborg et. al. (2018). S. 204.
[47] Ebd. S. 204.

computergesteuerte ausprobieren aller möglichen Kombinationen von Zahlen und Buchstaben einer gewissen Länge. Dabei nimmt die Zeit bis zum Auffinden einer Lösung mit der Länge des Passwortes zu. Die Geschwindigkeit, die das System beim Ausprobieren verwendet ist enorm hoch. So kann ein normaler Computer pro Sekunde bis zu 25 Millionen Zeichenabfolgen ausprobieren.[48] Verbunden mit einem Wörterbuch kann die Methode sogar beschleunigt werden, da nun vorgefertigte Wörter als Passwort eingesetzt werden. Besteht zum Beispiel ein Passwort aus fünf Zeichen, wovon drei Kleinbuchstaben und zwei Zahlen sind, wäre das Passwort innerhalb von 0,03 Sekunden ermittelt. Variiert man nun die Länge und die Abfolge im Passwort, steigt die Zeit. Ein siebenstelliges Passwort aus einem Groß- und sechs Kleinbuchstaben wird vom System erst nach ca. neun Minuten ermittelt.[49] Variiert man weiter und verwendet zudem noch Sonderzeichen steigt die Zeit zur Ermittlung weiter und wird weniger lukrativ für den Täter. Dadurch kann dies einen wirksamen Schutz gegen die Brute-Force Methode darstellen. In der Praxis verwenden jedoch viele Privatpersonen einfache Wörter oder Namen für ihre W-LAN Verschlüsselung. Somit ist diese Hürde schnell überwunden. Sind die Hacker einmal in das System gelangt, werden neue Zugangswege geschaffen, über die sie immer wieder ohne Passwortsperre hineingelangen. Mit den erlangten Daten können nun weitere Angriffe auf einzelne Geräte wie die Türverriegelung erfolgen. Somit wird ein physischer Zugang zum Haus geschaffen. Auch die Kommunikation selber kann angegriffen werden, sodass der rechtmäßige Benutzer keine Informationen von Bewegungsmeldern, der Klingel oder von Schließvorrichtungen erhält. Weiter können Alarmanlagen so deaktiviert werden. Zudem besteht die Möglichkeit, ähnlich der oben beschriebenen „ransomware“ Methode, eine digitale Geiselnahme durchzuführen. Hierbei wird die Kontrolle über das gesamte Smart Home System dem rechtmäßigen Benutzer entzogen und durch den kriminellen Angreifer übernommen. Dieser kann nun Druck ausüben, indem zum Beispiel alle Fenster

[48] Vgl. Kollek, J. (2013). Ein verbesserter PAM basierter Ansatz um „brute-force“ Passwort-Angriffe auf den „secure shell“ service zu erkennen und zu verhindern. Konstanz. Konstanzer Online-Publikations-System (KOPS). S. 7.
[49] Vgl. Ebd. S. 8.

im Haus ständig geöffnet sind, sich smarte Geräte nach Belieben ein und ausgeschalten oder die Heizung deaktiviert wird. Erst nach Zahlung eines Lösegeldes erhält der Eigentümer die Kontrolle über das System zurück.[50]

### 4.3.2 Einbruch in smarte Gebäude - Kabelgebundene Systeme

In Gebäuden mit kabelgebundenen Smart Home Systemen erfolgt die Kommunikation der einzelnen smarten Geräte ausschließlich über Kabelleitungen, zum Beispiel das Bussystem. Da hier der Weg in das System nur über den Zugriff auf das Kabelsystem erfolgen kann, ist zumindest kurzzeitig die tatsächliche Präsenz des Angreifers am Gebäude oder einem mit dem System verbundenen Gerät erforderlich, wodurch die Sicherheit zunächst erhöht wird. Ist ein physischer Zugang in das System gefunden sind die Systeme angreifbar. Veranschaulicht wird dies durch ein Projekt der IT-Sicherheitsfirma Antago. 2014 entwickelten diese ein Gerät mit dem Namen „Erebos“ zur Demonstration der Angreifbarkeit von kabelgebundenen Gebäudeleitsystemen. Sobald Erebos mit dem Kabelleitsystem verbunden wird, zum Beispiel über einen einfachen Lichtschalter, eine Klingel oder Überwachungskamera, beginnt es sogleich damit zu analysieren welche Komponenten im Smart Home System vernetzt sind und welche Funktionen sie erfüllen. Dabei ist das Gerät nur stiller Zuschauer und wird nicht als Eindringling erkannt. Dem Angreifer wird beim Auslesen der Daten eine Liste erstellt, wie das Gebäudeleitsystem im Einzelnen aufgebaut ist und welche Geräte es beinhaltet.[51] Neben der Analyse über die Qualität des Smart Home Gebäudes kann Erebos auch auf dieses zugreifen. Sobald das Gerät eine gewisse Funktionsweise analysiert hat, kann es Befehle herausschicken und somit Teile oder sogar das gesamte System eigenständig steuern. So können beispielsweise

[50] Vgl. Tecklenborg et. al. (2018). S. 205.
[51] Vgl. Dörsam, A. (2014). White Paper – Sicherheit von Gebäudeleitsystemen. Darmstadt. Antago GmbH. S. 6ff.

Alarmanlagen an oder ausgeschaltet, Überwachungskameras gesteuert oder Türen geöffnet werden. Da Erebos selbst über eine Funkantenne verfügt, kann diese Ansteuerung auch aus der Ferne, zum Beispiel mittels Smartphone, erfolgen und dem kriminellen Angreifer somit zum Einbruch verhelfen. Das Gerät ist darüber hinaus akkubetrieben und speist sich den Strom im weiteren Verlauf über das verbundene Gebäudeleitsystem.[52] Auch hier könnte das System wie bereits bei den kabellosen Lösungen, neben der Verwendung mit dem Ziel des Einbruchs, als Druckmittel auf den eigentlichen Benutzer verwendet werden. So kann Erebos einen bestimmten Befehl dauerhaft immer und immer wieder herausschicken, sodass die gesamte Beleuchtung des Gebäudes dauerhaft blinkt, ohne dass der Benutzer Zugriff darauf hat.[53]

# 5 Polizeiliche Arbeit am smarten Tatobjekt

Neben der Sicherheitslücken, über die Täter ihre Angriffe durchführen können, bietet smarte Vernetzung auch Möglichkeiten für neue Ermittlungsansätze, die sich die Polizei zu Nutze machen kann. Hier gilt es jedoch keine mechanischen oder physischen Spuren zu sichern, wie es bei normalen Tatorten der Fall ist. Die ermittlungstechnische Aufgabe besteht darin digitale Spuren zu finden und beweiskräftig zu sichern. Dies stellt eine neue Herausforderung für die Polizei dar.

[52] Vgl. Antago GmbH. (2016) KNX-Security, URL: https://antago.info/knx-sicherheit/ (zuletzt aufgerufen 27.04.2021).

[53] Vgl. Ebd.

## 5.1 IT-Forensik und digitale Spuren

Cybercrime ist eine wachsende Bedrohung für die Wirtschaft und die allgemeine Sicherheit. Um dieser Herr zu werden muss die Polizei neue Wege gehen und ständig auf dem aktuellsten Stand bleiben, um Straftäter verfolgen zu können. Der Bereich der Beweissicherung im Cybercrime Bereich wird als IT- oder digitale Forensik bezeichnet. Ihr Ziel ist es Gefahren im Internet oder anderen Netzwerken zu erkennen, diese Netzwerke zu sichern und Straftaten zu verfolgen. Denn werden Straftaten an oder mit digitalen Daten begangen hinterlässt der Täter meist eine Datenspur, digitale Spur genannt. Die IT-Forensik beschäftigt sich mit der Identifizierung und Sicherstellung der Quellen dieser digitalen Spuren. Ziel ist es diese beweiskräftig zu sichern.

Digitale Spuren entstehen bei jeder Bewegung in einem Netzwerk, bei der Informationen weitergegeben, erhalten, umgesetzt oder gespeichert werden. Dabei befinden sich diese Spuren auf dem Sendegerät, auf dem Sendeweg und dem Empfangsgerät. Sie können so an einer beliebigen Stelle festgestellt bzw. gesichert werden. Somit bilden digitale Spuren gerade im Bereich der IT-Forensik ein wichtiges Beweismittel. Sie lassen sich dabei nicht in bereits bekannte Spurenarten einsortieren, sondern stellen eine neue Art von Spuren dar. In gewissen Deliktsbereichen führen oftmals nur sie zum Täter.[54] Der Computer oder ein anderes elektronisches Medium fungiert neben der Funktion als Diebesgut, auch vor allem als Spurenträger und Tatwerkzeug, auf welchem wichtige Spuren hinterlassen werden.[55] Auf dieser Hardware befinden sich vor allem Spuren wie IP-Adressen, digitale Standortdaten oder Mobilfunkdaten, die gesichert vieles über die Kommunikation von diesem Gerät aussagen. Greift der Täter mit seinem Gerät auf ein anderes Netzwerk zu, wird dies auf beiden Geräten in den sogenannten „Log-Dateien“ bzw. in der Registry verzeichnet und kann später nachvollzogen werden. Auch wenn der

[54] Vgl. Kirchhoff, M. (2013). IuK-Kriminalität (Cyberkriminalität). Grundkompetenzen im Bachelorstudium der Polizei. In Kriminalitsik 2013(7). S. 491-495. S. 491
[55] Vgl. Kawelovski, F. (2020) Kriminaltechnik für Studierende und Praktiker. (3. Auflage). Mülheim an der Ruhr. Kawelovski Eigenverlag. S.259.

eigentliche Angriff vom Opfer unbemerkt geblieben ist. Wichtig kann auch sein welche Dateien wann, wo und weshalb erstellt, verschoben oder verwendet worden sind. Auch dies wird protokolliert und kann später ausgewertet werden. Weiterhin gehören Internetbrowserverläufe zum Bereich der digitalen Spuren und können Erkenntnisse bringen. So können auch bereits gelöschte Dateien wiederhergestellt werden und wichtige Informationen liefern.[56]

Als Spurenträger für digitale Spuren dienen neben dem Computer auch Festplatten und andere Speichermedien, wie Speicherkarten, CDs oder Sticks. Aber auch EC- oder Kreditkarten, Kameras und alle smarten Geräte, die in einem Haushalt verfügbar sein können. Daher auch der smarte Kühlschrank oder die smarte Brille.[57]

Aber nicht nur bei Taten im IuK-Bereich können digitale Spuren ausgewertet werden und zur Ergreifung des Täters führen. Auch bei anderweitigen Delikten lassen sich mit Hilfe von digital hinterlassenen Spuren Rückschlüsse auf die Begehung und den Täter ziehen und letztendlich auch beweiskräftig vor Gericht stellen. In der heutigen modernen Welt ist es fast nicht mehr möglich sich zu bewegen ohne digitale Spuren zu hinterlassen. Alleine durch das Smartphone werden ununterbrochen Informationen gesammelt, weitergegeben und gespeichert. Hinzu kommen Fitnessarmbänder, die dauerhaft die Bewegung aufzeichnen oder Sprachassistenten im häuslichen Umfeld, die sobald ein Schlüsselwort erkannt wird die Aufnahme beginnen. Diese digitalen Spuren werden auf Servern gespeichert und können in gewissen Fällen als Beweismittel für beispielsweise die Anwesenheit des Täters am Tatort zu einem gewissen Zeitpunkt dienen. Wichtig ist es dabei zu beachten, dass digitale Spuren „virtuell und flüchtig“[58] sind. Das bedeutet, dass sie nicht physisch gesichert werden können und somit auch leicht zu manipulieren und unbrauchbar zu machen sind.

[56] Vgl. Kirchoff (2013). S. 492.
[57] Vgl. Ebd. S. 493.
[58] Vgl. Tecklenborg et. al. (2018). S. 205.

Ein wichtiger weiterer Träger von digitalen Spuren ist das moderne Kraftfahrzeug. Wie oben bereits beschrieben sind moderne Fahrzeuge mit netzwerkfähigen Computern ausgestattet, die mit Servern oder anderen Computern kommunizieren, wodurch digitale Spuren hinterlassen werden, die wichtige Aufschlüsse bezüglich der Position des Fahrzeuges zum Beispiel zum Tatzeitpunkt erlauben. Dies soll im Folgenden näher betrachtet werden.

## 5.2 Das Connected Car als Beweismittel

Das Kraftfahrzeug mit smarter Vernetzung kann in einem Ermittlungsverfahren viele sachdienliche Informationen liefern. So wird eine ganze Reihe an wichtigen Informationen gespeichert. Steigen Insassen in das Fahrzeug, verbindet sich das Bordnetzwerk umgehend mit dem bereits gespeicherten Smartphone des Benutzers und synchronisiert Daten wie Anruflisten, Nachrichtenverkehr, aber auch Dateien oder gespeicherte Passwörter. Somit kann relativ genau nachvollzogen werden wann welcher Benutzer das Fahrzeug fuhr. Auch Türöffnungen werden protokolliert, wodurch nachvollzogen werden kann, wie viele Insassen sich wann im Fahrzeug befanden. Zudem liefert das Navigationssystem wichtige Informationen bezüglich der Zeit und des Ortes. Es können daraus Rückschlüsse gezogen werden, wann das Fahrzeug wohin bewegt wurde. Auch Parkpositionen werden dabei aufgezeichnet.[59] Bei Mercedes werden standartmäßig gewisse Informationen wie die Position oder der aktuelle Zustand wie die Tankfüllung, der Kilometerstand oder der Reifendruck automatisch alle zwei Minuten an den herstellereigenen Server gesendet und hier gespeichert. Andere Marken haben eine ähnliche Funktion. Sogar wenn die Navigation ausgeschaltet ist wählt sich das System im

[59] Vgl. Brummer, P. & Hoch, M. (2017). Das Kraftfahrzeug als Beweismittel. Digitale Fahrzeugdaten und ihre polizeiliche Relevanz in der analogen Welt. In Kriminalistik 2017(11). S. 643-648. Siehe S.644.

Hintergrund immer wieder in die aktuelle Funkzelle ein. Dieser Dienst heißt TMC (Traffic Message Channel) und dient dem Empfang von Verkehrsnachrichten, die dann in die Navigation miteinfließen. Dadurch kann mit und ohne eingeschaltetem Navigationsgerät nachvollzogen werden, welche Strecke das Fahrzeug wann zurückgelegt hat. Einfacher machen es dabei noch digitale Kontrollgeräte. Im Güterverkehr, zumeist zur Überwachung von Lenk- und Ruhezeiten eingesetzt, enthalten und speichern sie zusätzliche wichtige Informationen über den eingewählten Fahrer, das Fahrzeug und die zurückgelegte Strecke. Doch auch in normalen PKW befinden sich digitale Kontrollgeräte, wie Event-Data-Recorder (EDR) oder Unfalldatenschreiber (UDS), die im Fall einer Kollision diese wichtigen Fahrzeuginformationen protokollieren und abgreifbar machen. Sogar der Fahrzeugschlüssel kann verwendet werden, da auch hier diverse Informationen über das Fahrzeug gespeichert werden. Besonders bei Fahrzeugen mit einem Keyless-Go System, also einer elektronischen funkgesteuerten Vorrichtung, die den Schlüssel erkennt, ohne, dass dieser verwendet werden muss. Die Türen lassen sich, ohne das Fahrzeug manuell aufzuschließen, öffnen und der Motor per Knopfdruck starten, ohne dass der Schlüssel in der Zündung steckt. Gerade hier werden viele Informationen bezüglich des Fahrzeuges, wie zum Beispiel Kilometerstand, Tankinhalt und Fahrzeugidentifikationsnummer auch auf dem Schlüssel gespeichert.[60] Diese Daten können später durch die Polizei genutzt werden. Dabei ist vor allem wichtig, dass die Daten korrekt gesichert werden, damit sie beweiskräftig sind und nicht mehr manipuliert oder unbrauchbar gemacht werden können.

Rechtlich gesehen, sollte das Fahrzeug Gegenstand der Tat oder Tatmittel sein, gilt nach dem Legalitätsprinzip gemäß § 152 Abs. 2 StPO i. V. m. § 163 Abs. 1 StPO, dass beweiserhebliche Daten zu sichern sind. In der Praxis wird das Fahrzeug zu diesem Zweck sichergestellt bzw. beschlagnahmt. Dies erfolgt im Sinne der Strafverfolgung gemäß §§ 94, 98 StPO. Es sollte darauf geachtet werden, dass kein Unbefugter Zugriff auf das Fahrzeug haben kann,

[60] Vgl. Ebd. S. 644.

da beweiserhebliche Daten schnell manipuliert und gelöscht werden können. Zu diesem Zweck sollte das Fahrzeug möglichst nicht bewegt, nicht gestartet oder anderweitig angesteuert werden. Auch ein Fernzugriff auf das Fahrzeug via Internet ist möglich. Daher sollten die weiteren Schritte zügig und durch fachkundiges Personal erfolgen. Nach der Sicherstellung müssen möglichst viele Daten aus dem Fahrzeug gesichert werden. Dies erfolgt entweder über das Auslesen von Datenspeichern über im Fahrzeug verbaute Schnittstellen wie zum Beispiel USB oder durch den Ausbau der zentralen Steuereinheit.[61] Regelmäßig geht es dabei vor allem um das Infotainment System, welches als höhergestellte Koordinationseinheit über allen einzelnen Steuergeräten agiert und somit deren Daten empfängt, speichert und weitergibt. Hier können nun beweisträchtige Daten bezüglich der Navigation, Standorte und Routen, Telekommunikation, Kontaktlisten, synchronisierte Daten und Fahrverhalten erlangt werden. Daraus ergeben sich Rückschlüsse über den Zeitraum um die Tat und können somit auch zur Identifikation von dem oder den Täter/n führen. Je nach Hersteller und verwendeter Soft- und Hardware im Fahrzeug (am Beispiel BMW) werden sogar Daten wie Kamerabilder (Dashcam oder Umfeldkameras), Fahrverhalten und Geodaten aufgezeichnet, die sich der Fahrzeughersteller zu Forschungszwecken zu Nutze macht. Auch diese Daten können gesichert werden und sachdienliche Hinweise liefern. Diese gesicherten Daten müssen dann in ein Gesamtbild von Ermittlungsergebnissen verpackt werden und können so einen belastenden Beweischarakter erhalten. Wichtig ist bei der Sicherung von Daten vor allem die Sachkunde, da durch Fehler eine erhebliche Menge an Daten verloren gehen kann, welche bestenfalls zur Aufklärung einer Straftat beigetragen hätten.[62]

Es ist davon auszugehen, dass das Internet für die Fahrzeuge der Zukunft einen immer größeren Stellenwert einnehmen wird. Gerade im Bereich des autonomen Fahrens ist eine Vernetzung des Fahrzeuges mit seiner Umwelt unabdingbar. Somit wird die Technik immer weiter voranschreiten, wodurch

[61] Vgl. Ebd. S. 645.
[62] Vgl. Bortoluzzi, C. & Wallimann, P. (2019). Fahrzeugforensik in der Praxis. Herausforderungen und Chancen für die Strafverfolgung. In Kriminalistik-Schweiz. 2019(12). S. 761-765. Siehe S. 761.

auch der Bereich der IT-Forensik im Fahrzeug immer wichtiger werden wird. Es bedarf einer Menge an Schulungen und Fortbildungen, um den Fortschritt der Technik nicht zu verlieren und Schritt halten zu können.

## 5.3 Spurensicherung in smarten Gebäuden

Im Vergleich zu herkömmlichen Einbrüchen in Gebäude, wo vor allem materielle Spuren, wie Hebelspuren an den Zugängen und daktyloskopische Spuren (Fingerabdruckspuren) im Gebäude hinterlassen werden, ersetzen beim Einbruch in smarte Gebäude in der ersten Phase des Einbruchs digitale Spuren die herkömmlichen. Dabei ist die Art des Zugriffs entscheidend. Geht der Täter über ein kabelloses System an das Gebäude heran, so wird meistens eine Verbindung zwischen dem Täter-Computer und der Steuereinheit des Smart Homes aufgebaut. Hier werden erste Spuren auf beiden Geräten hinterlassen. Vor allem wenn zusätzlich noch Daten im Opfer Netzwerk erstellt oder verändert werden, befinden sich Hinweise darauf in der Registry bzw. den Log-Dateien. Zusätzlich wird in der kabellosen Verbindung durch den Internetprovider auch ein Nachweis (IP-Adressen), zumindest temporär, darüber geführt, welche Geräte miteinander kommuniziert haben. Somit befinden sich die Daten nicht unbedingt greifbar auf Speichermedien wie Festplatten oder Speicherchips, sondern auch im Internet selber, was die Anforderung an die Beweismittelsicherung erhöht.[63]

Wird auf ein kabelgebundenes System zugegriffen muss, wie zuvor erwähnt, ein physischer Zugriff auf das System erfolgen. Hier können dabei je nach Vorgehen und Ort des physischen Zugriffs, herkömmliche Spuren wie,

[63] Vgl. Labudde, D. ,Czerner, F. & Spranger, M. (2017). Einführung. In: Dirk Labudde & Michael Spranger (Hrsg.). Forensik in der digitalen Welt: Moderne Methoden der forensischen Fallarbeit in der digitalen und digitalisierten realen Welt. Berlin: Springer-Verlag GmbH, S. 1-22.

daktyloskopische oder Werkzeugspuren hinterlassen werden. Mit der oben genannten ‚Erebos'-Technologie wird das System angezapft und der Täter kann jede Funktion im smarten Gebäude eigenständig steuern. Dabei ist das von der Sicherheitsfirma Antago entwickelte Gerät ‚Erebos' auch gegen forensische Untersuchungen gesichert, indem es, selbst bei Entdeckung, keinerlei Rückschlüsse auf den Urheber zulässt.[64] Allerdings handelt es sich hierbei um eine Technologie, die speziell entwickelt wurde und der Vorführung dient und nicht unbedingt durch potenzielle Täter verwendet werden kann.

Die Suche nach digitalen Spuren gestaltet sich somit ebenso aufwendig wie zum Beispiel die Suche nach DNA-Material an einem Tatort. Zunächst muss bereits beim ersten Angriff sehr schonend durch die Polizei vorgegangen werden. Dabei müssen sich die eingesetzten Kräfte über das Vorhandensein und den Schutz dieser Spuren im Klaren sein, um mögliche digitale Spuren nicht unbrauchbar zu machen. So können bereits durch das Mitführen eines Smartphones am Tatort, welches sich in das bestehende W-LAN einwählt bzw. nur durch das W-LAN registriert wird, schon wichtige digitale Einträge, die Hinweise auf den Täter liefern könnten, überschrieben werden.[65] Da es sich um eher neuartige Technik handelt, müssen die Beamten, durch Aus- und Fortbildung, für dieses Thema sensibilisiert werden. Das Vorgehen nach dem erfolgten Einbruch ist zunächst die Sicherung der Daten gegen fremden Zugriff, da auch hier die Möglichkeit besteht aus der Ferne Daten zu löschen oder zu manipulieren. Somit muss umgehend durch fachkundiges Personal ein Abbild, ein sogenanntes Image, der Speichermedien erstellt werden. Dabei werden die Daten auf einen polizeilichen Datenträger gespiegelt, wodurch eine Momentaufnahme festgehalten wird, die dann analysiert werden kann. Diese Analyse besteht vor allem daraus gewisse Kommunikationen im Netzwerk nachzuvollziehen. Hier wird überprüft welches Gerät wann und wie auf welches andere Gerät eingewirkt hat. So kann nachvollzogen werden durch wen beispielsweise Vorgänge wie das Deaktivieren der Sicherheitsvorrichtungen

[64] Vgl. Dörsam. (2014). S. 8.
[65] Vgl. Hahn, A. (2017). Der „Smart-Ort" als Tatort – wie neue digitale Spuren die Ermittlungsarbeit verändern. In Die Kriminalpolizei. 2017(3). S. 4-7. Siehe S. 6.

wie Überwachungskameras, Bewegungsmelder oder Alarmanlagen zu einem bestimmten Zeitpunkt erfolgt sind. Dies geschieht wie zuvor bereits erwähnt, durch die Analyse der Log Dateien. Wenn hier kein Hinweis auf den tatsächlichen Täter gelingt, kann zumindest der genaue Zeitpunkt bestimmt werden, wann der Einbruch erfolgte. Haben sich die Täter durch die Überwindung der Sicherheitsvorrichtungen und das Öffnen der Tür mittels Hack der Schließanlage Zugang verschafft, zeigt sich durch die physische Anwesenheit das übliche Spurenbild bei Einbrüchen, wie Werkzeugspuren, Schuhabdruck/-eindruckspuren, daktyloskopische Spuren, DNA-Spuren etc. Dabei hängt das Ausmaß dieses Spurenbildes wie bei jedem Einbruch von der Professionalität der Täter ab.[66]

Betrachtet man die Tätertypologie bei Einbrüchen, so stellt man fest, dass der klassische Einbruch durch nahezu jede Art von Täter vom Kleinkriminellen oder Beziehungstäter, über den Beschaffungskriminellen bis hin zu gut organisierten internationalen Banden verübt wird. Der Einbruch in ein smartes Gebäude stellt dabei höhere Anforderungen an den Täter. Diese Taten sind im Voraus geplant, gut organisiert und benötigen das technische Wissen und entsprechendes Equipment zur Durchführung. Somit sind dies keine Taten, die lediglich der Beschaffung dienen oder auf geringe Beute abzielen. Hier agieren vorwiegend professionelle Banden.[67]

Eine weitere Besonderheit von Tatorten im Smart Home Bereich, stellt die Gefährdungslage für die eintreffenden Polizeibeamten dar. Durch den Zugriff des Täters auf die gesamte Haussteuerung, kann sich dieser selber der Sicherheitstechnik ermächtigen und ist somit der Polizei gegenüber im Vorteil, durch beispielweise die Nutzung der Überwachungskameras. Aber auch andere Technikelemente, wie die Beleuchtung im Haus oder Ablenkung durch Einschalten der Musikanlage bzw. das Aktivieren von gewissen Haushaltsgeräten, können die polizeiliche Arbeit im ersten Angriff bzw. der

[66] Vgl. Tecklenborg et. al. (2018). S. 205.
[67] Vgl. ebd. S. 206.

Durchsuchung von smarten Gebäuden erheblich beeinträchtigen und erhöhen dadurch das Gefährdungspotenzial.[68]

Die rasante Entwicklung der Technik erfordert somit auch hier das stetige Aus- und Fortbilden in den Reihen der IT- Forensik. Dies beginnt beim ersteintreffenden Beamten vor Ort und geht bis hin zum Spezialisten, welcher später die digitalen Spuren auswertet. In jeder Phase der Ermittlungen können dabei Fehler entstehen, die für die Beweiskraft oder Existenz von Spuren maßgebliche Folgen haben können. Es ist somit unabdingbar, dass alle Bereiche für dieses Thema sensibilisiert werden, damit das Vorgehen möglichst schonend und professionell erfolgt. So müssen auch Vernehmungstechniken angepasst werden, um an diesen speziellen Tatorten die richtigen Fragen zu stellen und Beweise schnell und effektiv sichern zu können. Fehler wie das Ausschalten eines elektrischen Gerätes oder dem Besitzer nochmal einen letzten Zugriff zu gewähren dürfen im Rahmen der professionellen Spurensicherung nicht begangen werden. Im besten Fall sollten Spezialisten der IuK- Ermittlung hinzugezogen werden. Bis zum Eintreffen ist die Situation statisch zu halten.[69] Da der digitale Tatort neue Anforderungen an die Ermittler stellt, ist auch der Einsatz von speziellen digitalen Tatortteams denkbar, die sich rein auf die digitalen Spuren vor Ort konzentrieren. Fraglich ist dabei inwieweit es zu Überschneidungen zwischen der klassischen Spurensicherung und der digitalen Spurensicherung kommt, wobei entschieden werden muss welcher Art von Spur hier eine höhere Gewichtung zugesprochen wird.[70]

# 6 Fazit

Smarte Vernetzung ist heutzutage längst keine Zukunftsvision mehr. Es ist neben der künstlichen Intelligenz die Technik, die unsere Zukunft maßgeblich

[68] Vgl. Kawelovski. (2020). S. 269.
[69] Vgl. Kirchhoff. (2013). S. 493.
[70] Vgl. Hahn. (2017). S. 6.

beeinflussen wird. Dabei ist abzusehen, dass sie sich mehr und mehr im täglichen Leben etablieren und dieses sogar ein Stück weit bestimmen wird. Der Gedanke, dass alle elektronischen Geräte in der Umgebung miteinander kommunizieren, fasziniert den Menschen seit Anfang des 20. Jahrhunderts. Dabei sind schon heute die Möglichkeiten schier unbegrenzt und das Potenzial noch lange nicht ausgereizt. Die smarte Vernetzung bietet im Eigenheim, auch als Smart Home bezeichnet, die Möglichkeit alle smarten im Haushalt befindlichen Geräte miteinander zu verbinden, zentral zu verwalten und sogar mit Internetzugriff, aus der Ferne zu steuern. In einem smart vernetzten Eigenheim ist es dabei möglich, bestimmte Abfolgen oder ein Zusammenspiel zu kreieren, sodass Abläufe auch automatisiert bzw. durch das System alleine gesteuert werden, ohne dass der Benutzer selber den Befehl dazu geben muss. Dadurch wird der Komfort in smarten Gebäuden deutlich erhöht. Darüber hinaus zeigt sich eine Verbesserung der Effizienz und der Sicherheit. Doch der Gedanke und die Möglichkeiten der smarten Vernetzung gehen weit über das Eigenheim hinaus. Auch das Fahrzeug gehört mittlerweile in die vernetzte Welt und integriert sich hier als vollwertiges Mitglied. Die Connected Cars können mit dem Benutzer, anderen Fahrzeugen und der allgemeinen Umgebung kommunizieren. Dabei geht es vor allem um Energieeffizienz, Umweltschutz und die Sicherheit aller am Straßenverkehr Beteiligten. Denkt man noch einen Schritt weiter, besteht die Vision der Smart Cities, in denen jedes Mitglied vernetzt ist und dadurch positive Aspekte wie der Fortschritt und die Energiewirtschaft gesteigert werden können.[71]

Mit am bedeutungsvollsten für den Anwender ist die Sicherheit, die durch technische Hilfsmittel und das Zusammenarbeiten der Geräte erreicht wird. So baut das Connected Car im Falle einer Kollision, eine Sprachverbindung zu einem Notfallservice auf und sendet gleichzeitig die Standortdaten, wodurch Hilfe schnell und effektiv erfolgen kann. Im Gebäudebereich gelingt dies vor allem durch Überwachungstechnik wie Kameras, Bewegungsmelder und Alarmanlagen. Daneben gibt es vernetzte Rauch- bzw. Kohlenmonoxid-

[71] Vgl. Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit. (2017). Smart City Charta. Bonn. S. 8f.

Melder, die bei Gefahr alarmieren, gleichzeitig durch das Smart Home System eine Notfallbeleuchtung aktivieren und die Belüftung einleiten. Zudem gibt es Systeme die die Anwesenheit der Benutzer im Gebäude simulieren, indem Beleuchtungen zu typischen Zeiten eingeschaltet werden, das Radio über Tag läuft oder Lichteffekte erzeugt werden, die einem Fernsehbild entsprechen. Fasst man diese technischen Mittel zusammen, stellt der Zugewinn der Sicherheit den positivsten Nutzen von Smart Home dar. Durch das Zusammenspiel der einzelnen Komponenten, die automatisierte Übertragung von Notfällen und dem Erkennen von Gefahren im Bereich des Straßenverkehrs, aber auch im Gebäude am Beispiel der Feuer- und Gaswarnanlagen kann die Technik sogar lebensrettenden Charakter haben. Und das voll automatisiert.

Doch je technischer und vernetzter das gesamte Haus wird, desto angreifbarer macht man sich auch gegenüber krimineller Übergriffe. Hier ist vor allem der Bereich Cybercrime zu nennen, der stetig wächst und schwer zu kontrollieren ist. Die Deliktsbereiche, in denen Begehung mittels Cybercrime erfolgen kann, werden immer umfangreicher. Aufgrund der schweren Verfolgbarkeit bleibt zu vermuten, dass das Dunkelfeld in diesem Bereich erheblich größer ist als das Hellfeld.[72]

Auch der kriminelle Zugriff auf smarte Gebäudeleitsysteme, mit dem Ziel der Datengewinnung oder sogar der Beschaffung des Zugangs zum Gebäude, fallen unter den Deliktsbereich des Cybercrimes. Dem Täter bieten sich hierbei Möglichkeiten auf das Smart Home System zuzugreifen, die Personen und das Innere des Gebäudes auszuspähen, Alarmanlagen zu deaktivieren und Türen zu öffnen, ohne tatsächliche Gewalt anzuwenden. Der Angriff gelingt in den meisten Fällen, ohne dass der Täter selber physisch vor Ort sein muss.

Die Möglichkeiten sich gegen den unbefugten Zugriff zu schützen sind oft gering. Standardmaßnahmen, wie die ständig aktuelle Gerätesoftware zu verwenden, Passwörter so sicher wie möglich zu gestalten oder niemand unbefugtem Zugriff auf das Netzwerk oder einen Teil des Systems zu gewähren,

[72] Vgl. Bundeskriminalamt. (2020).

sollten strikt durchgeführt werden. Dabei reicht der kriminelle externe Zugriff auf das Smartphone des Eigentümers, welches im System integriert ist, aus, um dem Täter Zugriff auf das System zu gewähren.[73] Allerdings ist es heutzutage bei den meisten Geräten nicht die Frage, ob sie gehackt werden können, sondern wann.[74] Der Wohnungseinbruchsdiebstahl in smarte Gebäude, unter Nutzung der smarten Technik, stellt aktuell noch eine Seltenheit dar. Steigen die Zahlen der Smart Homes, werden auch die kriminellen Zugriffe zunehmen.

So rückt die Entwicklung der Strafverfolgung in diesem Bereich besonders in den Vordergrund. Vorrangig dabei ist der Bereich der IT-Forensik, welcher sich mit dem Erkennen und Sichern von digitalen Spuren beschäftigt. Smarte Tatorte sind jetzt noch Einzelfälle, allerdings nimmt die Präsenz von digitalen Spuren auch an herkömmlichen Tatorten zu.[75] So können Informationen, die aus Fahrzeugen als Tatmittel gewonnen werden, eine genaue Darstellung der Tatabfolge bieten und somit wichtige Hinweise auf den Täter liefern, auch bei klassischen Delikten. Da digitale Spuren virtuell und somit einfach zu manipulieren bzw. sogar zu zerstören sind, gilt es hier vor allem schnell, präzise und professionell zu agieren. Gerade dem Schutz der Spur wird dabei vor allem durch Unkenntnis zu wenig Bedeutung beigemessen. So kann das eingeschaltete Smartphone der Polizisten am Tatort schon digitale Spuren des Täters verwischen. Daraus resultierend muss auch die kriminaltechnische Arbeit an diesen Tatorten umfassend angepasst werden. Hier sind digitale Spuren meist der einzige Hinweis auf den Täter. Es ist somit dringend notwendig, dass dieser Bereich in Aus- und Fortbildung deutlich intensiviert wird, da gerade in der Phase des ersten Angriffs, die Gefahr digitale Spuren zu zerstören am höchsten ist und es meist eine gewisse Zeit in Anspruch nimmt, bis Experten der IT-Forensik vor Ort sind. Eine Qualifikation und Sensibilisierung dieses Themas aller im täglichen Dienst befindlichen Einsatzkräfte ist also

[73] Vgl. Landeskriminalamt Niedersachsen. (2021). Smart Home & Smart Living, URL: https://www.polizei-praevention.de/themen-und-tipps/basisschutz-empfehlungen/smarthome-smartliving (zuletzt aufgerufen 27.04.2021).
[74] Vgl. Dörsam. (2014). S. 5.
[75] Vgl. Hahn. (2017). S. 6.

zwingend erforderlich, um möglichst umfangreich digitale Spuren an immer mehr Tatorten sichern zu können, statt diese unwissentlich zu verwischen.[76]

[76] Vgl. Ebd. S. 6 -7.

# 7 Literaturverzeichnis

**Literatur**

**Appelfeller, W. & Feldmann, C.** (2018). Die digitale Transformation des Unternehmens. Systematischer Leitfaden mit zehn Elementen zur Strukturierung und Reifegradmessung.Berlin: Springer Gabler.

**Bortoluzzi, C. & Wallimann, P.** (2019). Fahrzeugforensik in der Praxis. Herausforderungen und Chancen für die Strafverfolgung. In Kriminalistik-Schweiz. 2019(12). S. 761-765.

**Brummer, P. & Hoch, M.** (2017). Das Kraftfahrzeug als Beweismittel. Digitale Fahrzeugdaten und ihre polizeiliche Relevanz in der analogen Welt. In Kriminalistik. 2017(11). S. 643-648.

**Bucher, G.** (1939) The electric home of the future. In Popular Mechanics Magazine. Vol. 72(2). Seite 162 ff.

**Bundesministerium des Innern, für Bau und Heimat.** (2021) Polizeiliche Kriminalstatistik 2020. Ausgewählte Zahlen im Überblick. Berlin.

**Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit.** (2017). Smart City Charta. Bonn.

**Dörsam, A.** (2014). White Paper – Sicherheit von Gebäudeleitsystemen. Darmstadt. Antago GmbH.

**Fleisch E. & Mattern F.** (Hrsg.). (2005). Das Internet der Dinge. Berlin: Springer.

**Fuhrich, A.** (2016). Internet of Things. In D. Haselbauer (Hrsg.). Handbuch Digitalisierung. Die vernetzte Gesellschaft (S. 107–111). Bonn: ayway media GmbH.

**Grabowski, T.** (2018). Vernetzte Fahrzeuge: Neue Ermittlungsansätze im Strafverfahren? In Kriminalistik 2018(4). S. 208-215.

**Hahn, A.** (2017). Der „Smart-Ort“ als Tatort – wie neue digitale Spuren die Ermittlungsarbeit verändern. In Die Kriminalpolizei. 2017(3). S. 4-7.

**Haselbauer, D.** (2017) Handbuch Digitalisierung. Bonn: ayway media GmbH.

**Heckmanns, L.** (2017). Szenario-Analyse zu smartem Einbruchschutz in deutschen Haushalten. Münster. LIT Verlag.

**Kawelovski, F.** (2020). Kriminaltechnik für Studierende und Praktiker. (3. Auflage). Mülheim an der Ruhr. Kawelovski Eigenverlag.

**Kirchhoff, M.** (2013). IuK-Kriminalität (Cyberkriminalität). Grundkompetenzen im Bachelorstudium der Polizei. In Kriminalitsik 2013(7). S. 491-495.

**Kollek, J**. (2013). Ein verbesserter PAM basierter Ansatz um „brute-force" Passwort-Angriffe auf den „secure shell" service zu erkennen und zu verhindern. Konstanz. Konstanzer Online-Publikations-System (KOPS).

**Labudde, D. ,Czerner, F. & Spranger, M.** (2017). Einführung. In: Dirk Labudde & Michael Spranger (Hrsg.). Forensik in der digitalen Welt: Moderne Methoden der forensischen Fallarbeit in der digitalen und digitalisierten realen Welt. Berlin: Springer-Verlag GmbH.

**Mattern, F.** (2005). Die technische Basis für das Internet der Dinge. In: Fleisch E., Mattern F. (Hrsg.) Das Internet der Dinge. (S. 39-66) Berlin: Springer.

**Möllers, F.** (2016). Smart-Home-Systeme in Zeiten digitaler Kriminalität. In Datenschutz und Datensicherheit. 40. S. 497-502.

**Rohleder, B.** (2020). Das intelligente Zuhause: Smart Home 2020. Berlin. Bitkom Research.

**Rosslin,J. R. & Tai-Hoon, K.**(2010) A Smart Review on Security in Smart Home Development. In International Journal of Advanced Science and Technology. Vol. 15. S. 13-21.

**Landeskriminalamt Nordrhein-Westfalen** (2016). Smart Home Techologie – Smart Home als Ergänzung zu mechanischen Sicherungen. Düsseldorf.

**Dies.** (2017). Forschungsbericht Wohnungseinbruchdiebstahl. Basisbericht. Düsseldorf.

**Tecklenborg, T. & Stupperich, A**. (2018). Häuser mit Smart Home. Technologie als Ziel von Einbrechern. In Kriminalistik 2018(4). S. 203-207.

**Wießner, N.** (2020). Cyber Security. Welche Bedrohungen und Abwehrmaßnahmen gibt es für Smart Home-Geräte?. Studienarbeit. München: GRIN Verlag.

## Internetquellen

**Antago GmbH.** (2016) KNX-Security, URL: https://antago.info/knx-sicherheit/ (zuletzt aufgerufen am 27.04.2021).

**BMW**. (2020). Connected Car. Das vernetzte Auto, URL: https://www.bmw.com/de/innovation/connected-car.html (zuletzt aufgerufen 28.04.2021).

**Bundeskriminalamt**. (2020). Bundeslagebild Cybercrime 2019, URL: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html (zuletzt aufgerufen am 28.04.2021).

**Dies.** (2021) Cybercrime, URL: https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_node.html (zuletzt aufgerufen am 01.05.2021).

**CosmosDirect**. (2020). Smart Home: Definition, Entwicklung, Vorteile, URL: https://www.cosmosdirekt.de/smart-home/definition/ (zuletzt aufgerufen am 05.05.2021).

**CSA Research**. (2016). Citroen. Our Lives in our cars, URL: http://media.citroen.de/file/39/4/etude_csa_research_citroen_our_lives_inside_our_cars_german_data.pdf?_ga=2.85728221.535594185.1617399688-1825253201.1617399688 (zuletzt aufgerufen am 25.04.2021).

**Dannewitz, J.** (2020) Cybercrime: Grundlagen über die Delikte im Internet, URL: https://www.dr-datenschutz.de/cybercrime-grundlagen-ueber-die-delikte-im-internet/ (zuletzt aufgerufen am 26.04.2021).

**EnBW**. (2021) Smart Cities, URL: https://www.enbw.com/energie-entdecken/gesellschaft/smart-cities (zuletzt aufgerufen am 26.04.2021).

**Home and Smart** (2021). Smart Home Sicherheit – wie sicher ist das smarte zu Hause?, URL: https://www.homeandsmart.de/sicherheit (zuletzt aufgerufen am 26.04.2021).

**IT-Talents**. (2019). Was ist SPS Programmierung?, URL: https://www.it-talents.de/blog/it-talents/was-ist-sps-programmierung (zuletzt aufgerufen am24.04.2021).

**Landeskriminalamt Niedersachsen.** (2021). Smart Home & Smart Living, URL: https://www.polizei-praevention.de/themen-und-tipps/basisschutz-empfehlungen/smarthome-smartliving (zuletzt aufgerufen am 27.04.2021).

**Landeskriminalamt Nordrhein-Westfalen**. (2020). Datenanalytische Bekämpfung des Wohnungseinbruchs in NRW weiter verstärkt, URL: https://polizei.nrw/datenanalytische-bekaempfung-des-wohnungseinbruchs-in-nrw-weiter-verstaerkt (zuletzt aufgerufen am 26.04.2021).

**OnStar** (2016) The Evolution of OnStar, URL: https://www.onstar.com/us/en/articles/tips/evolution-of-onstar-innovations/ (zuletzt aufgerufen am 28.04.2021).

**Smartest Home**. (2021). Die Historie des Smart Home von 1963 – 2021: Meilensteine, URL: https://www.smartest-home.com/smart_home_historie_1939_2019/ (zuletzt aufgerufen am 29.04.2021).

**Verbraucherzentrale Nordrhein- Westfalen**. (2020). Smart Home: Das “intelligente Zuhause“, URL: https://www.verbraucherzentrale.de/wissen/umwelt-haushalt/wohnen/smart-home-das-intelligente-zuhause-6882(zuletzt aufgerufen am 26.04.2021).

**Wendel, M.** (2021). Alarmanlagen Test-Übersicht 2021: Alarmsysteme im Vergleich, URL: https://www.homeandsmart.de/alarmanlagen-test-uebersicht (zuletzt aufgerufen am 26.04.2021).

**Dies**. (2020). Elektronische Türschlösser Test 2021: Nachrüstlösungen Vergleich, URL: https://www.homeandsmart.de/tuerschloesser-tueroeffner-smart-home-besten (zuletzt aufgerufen am 26.04.2021).

**Dies.** (2020) Anwesenheitssimulation: Diese smarten Möglichkeiten gibt es, URL: https://www.homeandsmart.de/anwesenheitssimulation-im-smart-home (zuletzt aufgerufen am 27.04.2021).

**Wulf, D**. (2020). Smart Home - Visionen für unser Zuhause, URL: https://www.homeandsmart.de/wohnen-in-der-zukunft (zuletzt aufgerufen am 25.04.2021).