Simulation der Auswirkung einer Explosion anhand eines 3D-Modells für den Stadtteil Schwabing in München.

Connected Cars: In vernetzten Autos gibt es viele Funktionen, die für polizeiliche Ermittlungen interessant sein können.

Digitale Gefahren

Vernetzte Fahrzeuge, virtuelles Polizeieinsatzkräftetraining sowie Gefahren bei „Smart-Home"-Technologien waren Themen beim Symposium „Neue Technologien" im November 2017 in Fürstenfeldbruck.

Die Zahl der vernetzten Autos nimmt weltweit zu. In neuen Fahrzeugen sind bis zu 80 Steuergeräte verbaut, die mit Sensoren Fahr- und Fahrzeugdaten speichern. Tobias Grabowski von der Hochschule der Polizei Rheinland-Pfalz referierte über neue Ermittlungsansätze im Strafverfahren mit vernetzten Fahrzeugen. Laut Grabowski gibt es Funktionen in den Infotainmentsystemen der Autos, die für polizeiliche Ermittlungen interessant sein können, etwa für Beweiszwecke bei einem Unfall oder wenn das Fahrzeug von Kriminellen verwendet worden ist. Dazu zählen das Fahrverhalten, die Länge gefahrener Strecken, Ziele des Navigationsgerätes und Handydaten gekoppelter Handys. Einen Ermittlungsansatz biete auch die E-Call-Funktion bei Fahrzeugen. Diese Funktion könne nicht nur Informationen wie den Unfallort aufzeichnen, sondern sie sammle Daten und kann Bewegungsprofile erstellen.

„Fahrzeugforensik ist ein Teil der digitalen Forensik, der bisher zu wenig Aufmerksamkeit geschenkt worden ist", sagt Tobias Grabowski. Er tauscht sich in der Kfz-Forensik mit Kollegen aus anderen Ländern aus, darunter mit den Kfz-Forensik-Experten des österreichischen Bundeskriminalamts.

Datenschutz bei Fahrzeugen. Über das Problem des Datenschutzes bei Fahrzeugdaten referierte Maximilian Weidmann vom Bayerischen Landeskriminalamt. Die Übermittlung von Fahrzeugdaten an den Hersteller sei ein Datenschutzproblem, das auch die Polizei betreffe. Fahrzeugdaten werden über eine SIM-Karte im Fahrzeug an den Hersteller übertragen, diese Funktion ist bei den *BMW*-Fahrzeugen standardmäßig eingeschaltet. Sie kann nur über Verlangen des Fahrzeugbesitzers abgeschaltet werden. Ein deutsches Bundesland hat neue *BMW*-Streifenwagen geleast. Mit der Firma *BMW* sei vertraglich festgelegt, dass die in die Streifenfahrzeuge eingebauten SIM-Karten von der *BMW AG* beim Netzbetreiber abgemeldet werden. Für die neuen *BMW*-Streifenfahrzeuge sei nur der E-Call (Notruf 112) gewährleistet, der ab 2018 für die Erlangung der Betriebserlaubnis von Neufahrzeugen vorgeschrieben ist. Weitere Daten werden nicht übermittelt.

Schutz vor terroristischen Bedrohungen. Univ.-Prof. Dr. Norbert Gebbeken, Professor für Baustatik an der Universität der Bundeswehr München, informierte über „Sicherheitsanalysen und Schutz baulicher Infrastrukturen bei terroristischen Bedrohungen". Zu seinen Fachgebieten gehört der Schutz der Bevölkerung vor Terrorismus und Naturkatastrophen durch bauliche Maßnahmen. Angriffe auf Menschen oder Infrastrukturen können durch Fahrzeuge, Flugzeuge, Waffen, Bomben oder Gegenstände erfolgen. Er und sein *BauProtect*-Team simulieren zum Beispiel Sprengstoffanschläge und deren Auswirkungen in einem dicht bebauten Gebiet. Dazu haben sie ein 3D-Modell des Münchener Stadtteils Schwabing erstellt. In den Szenarien geht es darum, die Wucht der Detonation und deren Folgen auf die umliegende Infrastruktur zu ermitteln. „Aufgrund des Ergebnisses des simulierten Anschlags können wir eine Gefährdungsanalyse für den betreffenden Bereich erstellen", erklärte Gebbeken. Bei der Gefährdungsanalyse geht es zunächst um eine Risikoeinschätzung: Wer oder was, soll vor welchen Gefahren geschützt werden? Geht es um Einrichtungen der kritischen Infrastruktur oder um andere Objekte oder um Personen? Sind Personen- oder Sachschäden zu erwarten? Darauf aufbauend gilt es Schutzmaßnahmen zu definieren: Bauliche, technische und organisatorische Maßnahmen.

Als bauliche Schutzmaßnahmen vor Anschlägen mit Pkws oder Lkws wurden zum Beispiel in vielen Städten Poller verbaut oder große Betonklötze als Barrieren platziert. Das sei laut Gebbeken mitunter gefährlich. Poller und Barrieren könnten schwere Lkws, die mit großer Geschwindigkeit fahren, nicht aufhalten; sie könnten sich als gefährliche Gegenstände erweisen, die gegen Menschen geschleudert würden. Man könne mit baulichen Maßnahmen Zufahrtsbeschränkungen schaffen, die wie

Fotos: Zapp2photo/Fotolia, Universität der Bundeswehr

Projekt ViPOL: Einsatzorientierte Ausbildung von Polizeikräften durch realistische Handlungssimulation in einer vernetzten Trainingsumgebung.

Poller funktionieren, aber nicht so aussehen – etwa Grünflächen vor schützenswerten Objekten, in denen Lkws stecken bleiben. Bei Versuchen haben Gebbeken und sein Team Sträucher als Explosionsschutz getestet. Dabei hätten sich Thuja-Hecken als nützlich erwiesen. Sie hätten Explosionen fast unbeschadet überstanden und die Druckwelle um mehr als 60 Prozent reduziert. Engmaschige Streckgitter würden etwa vor Trümmern schützen. Geflechte aus Metall könnten Fahrzeuge stoppen. Ein Wasserfilm hinter den Geflechten könnte die Druckwelle einer Explosion abschwächen. Künstliche Hügel vor Objekten wären in der Schutzwirkung effektiver als eine Wand.

Virtuelles Polizeieinsatzkräftetraining. DI Markus Herkersdorf, Geschäftsführer von *TRiCAT,* einem Unternehmen im Bereich virtueller 3D-Lern- und Arbeitswelten, stellte das Projekt *ViPOL* (Virtuelles Polizeieinsatzkräftetraining) vor und sprach über Chancen und Herausforderungen, die sich durch 3D-Simulation, künstliche Intelligenz und *Virtual-Reality*-Technik für die Polizeiarbeit ergeben.

Im Projekt *ViPOL* geht es um einsatzorientierte Ausbildung von Polizeikräften durch realistische Handlungssimulation in einer vernetzten Trainingsumgebung. „Die Trainingsteilnehmer müssen sich nicht mehr im gleichen Raum befinden, jeder kann mit einem Computer irgendwo sitzen und daran teilnehmen“, erklärte Herkersdorf. Szenarien, die Polizisten mit verteilten Rollen in einem virtuellen Team durchspielen können, werden durch Einsatztrainer erstellt, etwa ein simulierter Verkehrsunfall, die Ankunft der Polizisten am Unfallort, die ersten Maßnahmen oder die Zusammenarbeit zwischen Bodenkräften mit Hubschrauber-Einsatzkräften. „Man kann solche Szenarien realitätsnah durchspielen. Die Erfahrungen fließen dann in den Echtbetrieb ein. Ziel ist es, Handlungskompetenz zu erwerben“, erklärte Herkersdorf.

ViPol bietet neben dem Training von Einsatzszenarien, die in der Wirklichkeit teuer, aufwendig oder gefährlich wären, Kommunikations-, Nachbesprechungs- und Feedbackmöglichkeiten. Die 3D-Software ermöglicht es, nach einem Training das komplette Szenario aus beliebigen Perspektiven zu rekonstruieren und erneut erlebbar zu machen – einschließlich aller Handlungen und der vollständigen Kommunikation.

Gefahren bei „Smart-Home“-Technologien. Dr. Florian Huber, Researcher und Projekt-Koordinator bei dem Wiener Beratungs- und Forschungsunternehmen *SYNYO,* berichtete über Schwachstellen bei „Smart-Home“-Anwendungen. Sicherheitsforscher von *Check Point Software Technologies Ltd*. haben zum Beispiel eine Schwachstelle in der „Smart-Home“-Anwendung *SmartThinQ* entdeckt. Die Lücke ermöglichte es, Live-Kamerabilder eines Saugroboters von *LG* abzurufen, da der Saugroboter über eine Kamera verfügt und mit einer App ferngesteuert wird. Kunden können via App auf die Kamera zugreifen und kontrollieren, ob zu Hause alles in Ordnung ist. *Check-Point*-Mitarbeitern gelang der Zugriff auf den Saugroboter, indem sie mit einem gefälschten Profil die *LG*-Cloud anzapften. Mittlerweile wurde ein Update für die App bereitgestellt.

Automatisch gesteuerte Heizungen, Lüftungen, Türen, Fenster, Markisen, Jalousien und Lampen sowie manuell über mobile Geräte wie Smartphones kontrollier- und manipulierbare Systeme gehören genauso zu „Smart Home“ wie „Smart Metering“ und „Smart Grid“. In Zukunft könnten auch „Smart Books“, „Smart Clothes“ oder „Smart-Health-Applikationen“ integriert werden.

„Smart-Home“-Systeme sind identifizierbar, lokalisierbar und vernetzt. Die meisten Smart-Home-Geräte sind über einen Router mit externen Netzwerken verbunden. Viele Benutzer vernachlässigen die Sicherheit ihres Routers. Hacker können daher relativ leicht über einen Router in das Smart-Home-Netzwerk eindringen und die Kontrolle über die Geräte übernehmen. Viele Benutzer verwenden die ab Werk eingestellten Passwörter für die meisten Geräte gleichen Systems, um die Nutzung einfacher zu machen. Das macht es wiederum einfacher für Hacker, in die Systeme einzudringen. Die Software der Geräte wird außerdem nur selten upgedated. Wenn Firmware- und System-Updates übersehen werden, steigt die Gefahr.

Bedrohungsfelder. Derzeit kann von fünf zentralen Bedrohungsfeldern und -szenarien für „Smart-Home“-Systeme ausgegangen werden: Heizung/Thermostate, Unterhaltung/Smart TV, Sicherheit, Kommunikation und Beleuchtung. Ein Thermostat sammelt zum Beispiel Informationen über alle Personen, die im Haus leben. „Intelligente Thermostate“ wissen, wann jemand zu Hause ist, was ihre Zeitpläne sind, wann sie schlafen und welche Temperaturen sie bevorzugen. Viele Smart-TVs sind mit einer Kamera ausgestattet.

Cyber-Angreifer, die das Gerät hacken, können diese Kamera dann verwenden, um Personen auszuspionieren, selbst wenn der Fernseher ausgeschaltet ist. Aufgrund eines Mangels an Sicherheitsstandards können Hacker die Benutzung des Smart-TVs sperren und Lösegeld für die Entsperrung verlangen. Viele Anwender steuern ihre Si-

FOTO: TRICAT

cherheitssysteme mit einer Smartphone-App. Diese Systeme können Alarmanlagen, Garagentoröffner, Türschlösser, Überwachungskameras oder Gesichtserkennungssysteme umfassen. Cyber-Angreifer könnten zum Beispiel feststellen, ob die Haustür versperrt ist, während jemand weg ist. Angreifer können das Garagentor öffnen, die Überwachungskameras abschalten oder die Alarmanlage.

Smart-Home-Kommunikationssysteme umfassen etwa Videokonferenzgeräte, Computer oder Smartphones. Hacker können unberechtigten Zugriff erlangen, ohne Spuren zu hinterlassen. Sie können wertvolle Informationen (Bankdaten, Kreditkarten-Nummern oder Firmeninformationen) durch Angriffe stehlen, Telefongespräche mithören oder E-Mails überwachen. Hacker, die Zugang zu den Beleuchtungssystemen eines „Smart Home“ erhalten, können die Beleuchtung eines Hauses steuern. Sie können auch den Strom eines Hauses steuern und so einen erheblichen Mehrverbrauch (und somit Kosten) verursachen. Über einen „Smart-Meter“ können sie die Stromabrechnung manipulieren. Die Gefahren gehen dabei jedoch nicht nur von den „Smart-Home“-Geräten selber aus, sondern auch vom zentralen Hub, der diese Geräte kontrolliert: dem Smartphone.

FOTO: KASPARS GRINVALDS/FOTOLIA

Smart-Home-Netzwerk: Viele Benutzer vernachlässigen die Sicherheit ihres Routers.

„IoThreats“. Florian Huber stellte das österreichische KIRAS-Sicherheitsforschungsprojekt „IoThreats“ vor. Es befasst sich mit der zunehmenden Angreifbarkeit von Systemen des Internet of Things (IoT), wobei der Fokus auf „Smart-Home“-Technologien und Anwendungen gelegt wird. Projektpartner sind die *SYNYO GmbH,* die *Joanneum Research Forschungsgesellschaft mbH,* das *Austrian Center for Law Enforcement (ALES)* der Universität Wien und das Bundesministerium für Inneres. „IoThreats“ zielt darauf ab, potenzielle Bedrohungs- und Angriffsszenarien zu sammeln, zu evaluieren und gemeinsam mit dem primären Bedarfsträger BMI zu validieren.

Symposium. 200 Fachleute aus fünf europäischen Staaten nahmen am 7. internationalen Symposium „Neue Technologien“ zum Thema „Next Generation Internet“ am 7. und 8. November 2017 in Fürstenfeldbruck in Deutschland teil. Kooperationspartner der Veranstaltung waren die Bundeskriminalämter Österreich und Deutschland, das eidgenössische Bundesamt für Polizei („fedpol“) sowie die Landeskriminalämter Bayern und Baden-Württemberg. Es gab 13 Vorträge, darunter über „Maschinelles Lernen zur Unterstützung von Analysten in der polizeilichen Ermittlungsarbeit am Beispiel von Daten aus sozialen Netzwerken“, „Vernetzung privater und öffentlicher Sicherheit“, „forensische Bild- und Videoanalysesysteme“ sowie die Vorstellung des EU-Projekts „Innovation throught Law Enforcement Agencies Networking“ (ILEAnet). *S. L.*