Bundesamt
für Sicherheit in der
Informationstechnik

a | i3
Arbeitsgruppe **Identitätsschutz im Internet**

a-i3/BSI-Symposium 2017

Man in the Sensor

IT-Sicherheit für vernetzte Systeme und Produkte

Das 12. a-i3/BSI Symposium 2017 stand wie in den Vorjahren ganz im Zeichen tagesaktueller Themen. Vertreter aus Wirtschaft, Forschung und Verwaltung stellten am 24. und 25. April aktuelle Probleme aus dem Bereich der IT-Sicherheit vor und diskutierten über Lösungen und Regulierungsmöglichkeiten.

Prof. Dr. Georg Borges und Prof. Dr. Jörg Schwenk gaben einen Überblick über die aktuellen Herausforderungen der Regulierung von IT-Sicherheit, die neben strukturellen Fragen in inhaltlicher Hinsicht zunächst Risiken durch Vernetzung und Bedrohungen durch Ransomware und Botnetze zu bewältigen hat. Darüber hinaus bergen die vertrauenswürdige Identifizierung von Menschen und Maschinen im Internet der Dinge einerseits sowie Verbraucher- und insbesondere Datenschutz andererseits künftig weiterhin Konfliktpotential. Diese Aspekte wurden in den vier Themenbereichen des Symposium interdisziplinär diskutiert.

Themenbereich 1
„IoT - Risiken durch Vernetzung“

Der erste Veranstaltungstag wurde mit dem Themenblock 1 unter dem Titel „IoT – Risiken durch Vernetzung“ eröffnet. Aus technischer Sicht führte **Prof. Dr. Jörg Schwenk** in die Thematik ein und berichtete von gehackten Kühlschränken, ausgesperrten Hotelgästen, DDoS-Angriffen durch kompromittierte Überwachungskameras sowie Sicherheitslücken in Herzschrittmachern.

Den ersten thematischen Vortrag mit dem Titel **„Angriffe auf Embedded Devices“** übernahm **Ralf Benzmüller**, Leiter des G DATA Security Labs. Er stellte zahlreiche aktuelle Beispiele von Angriffen auf Embedded Devices dar. Neben vernetzten Infusionspumpen und Herzschrittmachern seien in praktisch allen Lebensbereichen Angriffe auszumachen, beispielsweise auf

computergestützte Zielvorrichtungen an Gewehren, Babyphones oder Siemens S7-Steuergeräte. Als mögliche Lösungen zur Verringerung der Angriffsrisiken wurden etwa Embedded Firewalls, Anomalieerkennung und Security-by-Design-Lösungen aufgezeigt. Hieraus ließen sich Anforderungen an sichere Geräte ableiten, beispielsweise die Vergabe von individuellen Passwörtern, Behebung von Fehlern durch Software und Firmware sowie der sparsame Umgang mit backdoors.

Prof. Dr. Georg Borges, geschäftsführender Direktor des Instituts für Rechtsinformatik und Inhaber des Lehrstuhls für Bürgerliches Recht, Rechtsinformatik, deutsches und internationales Wirtschaftsrecht sowie Rechtstheorie an der Universität des Saarlandes, stellte mit dem Vortrag **„Rechtsfragen der IT-Sicherheit im Internet of Things“** sodann aktuelle Rechtsfragen dar. Prof. Borges zeigte am Beispiel mobilfunkbasierten Online-Bankings das Problem auf, dass Hersteller von Systemen durch drittschützende Pflichten zur Gewährleistung von IT-Sicherheit verpflichtet werden müssen. Aus regulierungssystematischer Sicht stelle sich die Herausforderung, erwünschtes Verhalten zu identifizieren und durch Rechtsnormen Anreize für die Normadressaten zu setzen, das erwünschte Verhalten zu zeigen. Für eine erfolgreiche Regulierung sei es stets entscheidend, die geeigneten rechtlichen Instumente zur Verhaltenssteuerung zu wählen. Insoweit stellte Borges das Instrumentarium der Co-Regulierung zur Diskussion, das hierfür zahlreiche Vorteile bietet (Bündelung von Fachkenntnis, Verhinderung von chilling effects). Als weitere Herausforderung nannte Borges die Durchsetzung gesetzter Standards. Am Beispiel von Software wurde verdeutlicht, dass die Auslegung von Rechtsbegriffen im zivilrechtlichen Haftungsrecht maßgeblichen Einfluss auf Produktsicherheit nehmen kann.

Prof. Dr. Markus Ullmann: Effektive Verhinderhung von Datenverkettung bei V2X

Jens Müller, Master-Absolvent an der Ruhr-Universität Bochum, zeigte in seinem Vortrag **„Angriffe auf Netzwerkdrucker“** mit einer Live-Demonstration mögliche Angriffsszenarien auf. Die Besonderheit bei Netzwerkdruckern besteht darin, dass sowohl Druckdaten als auch systemrelevante Kommunikation über dieselbe technische Schnittstelle abgewickelt werden, sodass bereits die Möglichkeit des Druckens – ungeachtet der konkreten Druckeranbindung – zur Durchführung von Angriffen ausreichend ist. Während der Live-Demonstration erhielt das Auditorium einen Einblick in die Möglichkeit, Druckaufträge durch Schadsoftware etwa durch das Austauschen von Text zu manipulieren oder sämtliche an den Drucker gesendeten Daten auszulesen. Als mögliche Schutzmaßnahmen nannte Müller die Vermeidung direkter Verbindungen von Druckern zum Internet, die Einrichtung separater Netzwerke für Drucker und die entsprechende Schulung von Mitarbeitern. Perspektivisch müssten Hersteller das Software-Design von Druckern verändern.

Prof. Markus Ullmann, Leiter des Referates „Technologische Grundlagen sicherer elektronischer Identitäten, Chipsicherheit“ im Bundesamt für Sicherheit in der Informationstechnik, berichtete in seinem Vortrag **„Fahrdaten für alle? – Car-2-Car-Kommunikation und die Folgen“** über den aktuellen Stand der Vehicle-to-Vehicle-Kommunikation (V2X). Er stellte sowohl die zugrundeliegende Technologie als auch das Kommunikationsmodell dar. Bei der V2X-Kommunikation ist auch die Übermittlung der Fahrzeugposition vorgesehen. Daher besteht eine zentrale datenschutzrechtliche Anforderung darin, das Erstellen von Bewegungsprofilen sowie eine Zuordnung der pseudonymisierten Daten zu einem bestimmten Fahrzeug zu verhindern. Vorschläge zur datenschutzrechts-konformen Ausgestaltung der V2X-Kommunikation bestehen darin, das Senden und Empfangen entsprechender Nachrichten transparent auszugestalten sowie eine Deaktivierungsmöglichkeit vorzusehen sowie – perspektivisch – in der Reduktion von Nutzdaten und dem selektiven Versand entsprechender Nachrichten

Themenbereich 2 „Ransomware und Botnetze“

Dem schloss sich am Nachmittag der umfangreiche Themenbereich 2 mit dem Titel „Ransomware und Botnetze“ an. **Prof. Dr. Georg Borges** führte in die Thematik ein und hob die Aktualität des Themenbereiches hervor.

Den ersten Vortrag des Themenbereiches mit dem Titel **„Locky Ransomware“** übernahm **Thomas Hungenberg,** IT-Sicherheitsanalyst im Referat „CERT-Bund“ des Bundesamtes für Sicherheit in der Informationstechnik. In seinem Vortrag ging er zunächst auf die Entstehung, die Funktionsweise und Verbreitungswege der Ransomware Locky ein. Hungenberg legte dar, dass Locky autark auf infizierten Rechnern läuft, deren Speicher nach erfassten Dokumenttypen durchsucht und dann verschlüsselt. Die Verbreitung der Ransomware erfolgt via Mailversand mit Schadcode im Dokumentanhang. Anschließend wurde die Struktur der gezielten Kampagnen durch die Täter erläutert, welche im Juli 2016 plötzlich endeten, aktuell ab dem 21. April jedoch wieder beobachteten wurden. Auch Schutzmöglichkeiten gegen Locky wurden thematisiert: Hungenberg rät zur Ausarbeitung eines geeigneten Notfallkonzepts, sowie zu dessen regelmäßiger Pflege, um auf aktuelle Bedrohungen reagieren zu können. Kern dieses Konzepts seinen nicht nur regelmäßige Back-ups auf einem separaten, nicht mit dem Live-System verknüpften System, sondern auch die regelmäßige Prüfung der Updates und der Test der Wiederherstellbarkeit der Back-ups.

Michael von Üchtritz und Steinkirch: Abschaltung von über XXX EDV-Systemen

Michael von Üchtritz und Steinkirch, Chief Digital Officer des Lukaskranken-hauses Neuss, gab in seinem Vortrag **„Sicherheit vor Funktionalität. Zur digitalen Transformation eines Geschäftsmodells“** einen Überblick über den Ransomware-Angriff auf das Lukaskrankenhaus am 10. Februar 2016 sowie über die getroffenen Notfallmaßnahmen mit ihren Auswirkungen auf die betroffenen Personen. Er berichtete von der Herausforderung einen vollständig digitalisierten Krankenhausalltag mit über 300 verschiedenen anwendungsorientierten IT-Systemen innerhalb kürzester Zeit auf analoge Verfahren umzustellen, nachdem die EDV aus Sicherheitsgründen heruntergefahren werden musste. Er betonte, dass die medizinische Versorgung selbst durch den Angriff nicht beeinträchtigt wurde. Dank der sofortigen Bildung eines Krisenstabs, welcher die verschiedenen Netzwerke priorisierte und Lösungen zur Bekämpfung der Ransomware erarbeitete, konnten nach und nach die Systeme wieder aktiviert werden.

Im Anschluss hieran referierte **Dr. Tilman Frosch,** Geschäftsführer der G DATA Advanced Analytics GmbH und Leiter des Notfalleinsatzes im Lukaskranken-haus, in seinem Vortrag **„Schon GEZahlt? Über den besseren Umgang mit Ransomware“** darüber, wie man sich als Opfer eines Ransomwareangriffes verhalten sollte. Er stellte die speziellen Charakteristika von Ransomware im Vergleich zu anderer Malware dar. Der prägende Unterschied liegt darin, dass Ransomware bereits bei der Ausführung erkennbar ist. Sodann wurde auf die Erkennung eines entsprechenden Angriffsfalles eingegangen. Hierzu wurde als Handlungsempfehlung die sorgfältige Erfassung und Auswertung von System- und Netzwerkprotokollen vorgeschlagen. Dr. Frosch ging auch auf das Vorgehen im Krisenfall ein (Incident & Response). Wird ein erfolgreicher Ransomwareangriff festgestellt, können verschiedene organisatorische Maßnahmen, wie bspw. Definierung von Meldeketten und Entscheidungsträgern, Erstellung von Einsatz- und Eskalationsplänen oder die Konzeption eines Recovery-Vorgehens, getroffen werden. Die technische Infrastruktur sollte zudem in der Lage sein, den Vorfall einzugrenzen, um Schäden zu begrenzen. Zum Abschluss des Vortrages wurde kurz auf Fragen wie ein Threat-Modelling für individuelle Kunden eingegangen.

Willi Herzig, Bundesamt für Sicherheit in der Informationstechnik, referierte über den **„Avalanche-Takedown“** vom 30. November 2016 und richtete den Blick insbesondere auf getroffene Maßnahmen, die Betrof-

fene bei der Bekämpfung von Botnetzen unterstützen sollten. Hierbei betonte er, dass das System nach erfolgter Infektion zunächst zu säubern ist, bevor in einem zweiten Schritt ein Schutz gegen zukünftige Angriffe eingerichtet werden soll. Ausführlich wurden Angebote für Bürger dargestellt. So entwickelte das BSI eine Anti-Bot-CD, die in Kooperation mit der Computer Bild vertrieben wurde. Daneben wurde gemeinsam mit dem ECO-Verband ein Antibotnetz-Beratungszentrum gegründet. Weitere Maßnahmen stellen das 2014 geschaffene Provider-Informationssystem sowie die Homepage www.sicherheitstest.bsi.de dar, mit deren Hilfe die Bürger überprüfen können, ob sie von Avalanche betroffen waren und ein Missbrauch ihrer Daten droht. Auf diese Weise konnte eine Unterstützung der Bürger aus der laufenden Operation gewährleistet werden. Anschließend wurde die Funktions-weise von Avalanche dargelegt. Aus der Schadsoftware wurden im Rahmen des Angriffes 830.000 infizierte Domains identifiziert. Mithilfe eines Sanity-Checks wurde Schadsoftware von sonstiger Software separiert und gemeinsam mit mehreren Partnern beseitigt. Die Operation wurde von Europol in Den Haag geleitet. Insgesamt ist die Zahl der Infektionen rückläufig. Avalanche war die bisher größte Botnetzinfrastruktur, für deren Takedown eine internationale Zusammenarbeit erforderlich war.

Prof. Dr. Thorsten Holz: Forschungsprojekt „CAUSE-EFFECT“

Einen Einblick in strafrechtliche Aspekte der Botnetzkriminalität gab **Philipp Ciciliani** vom Bundeskriminalamt in seinem Vortrag **„Strafrechtliche Aspekte der Botnetzbekämpfung“.** Ciciliani begann mit einem allgemeinen Überblick über die Sicht der Strafverfolgung zur strategischen Analyse von Botnetzen und deren Bekämpfung, unter anderem am Beispiel des Angriffs auf Router der Deutschen Telekom AG. Anschließend legte er die materiellrechtliche Sicht und die relevanten Straftatbestände dar. Allen voran von Bedeutung ist § 303b StGB, aber auch §§ 253, 263a und 303a StGB sind von hoher Relevanz. Dazu treten die Vorbereitungstaten aus §§ 202a-d StGB. Der Bereich des Cybercrime unterliegt einem stetigen und schnellen Wandel. Eine dauerhafte Anpassung der Gesetzeslage ist aus diesem Grund unumgänglich. Um die Beseitigungsquote zu erhöhen wird seitens des BKA insbesondere eine erhöhte Kooperation mit den Providern angestrebt.

Prof. Dr. Thorsten Holz, Inhaber des Lehrstuhls für Systemsicherheit an der Ruhr-Universität Bochum, referierte anschließend über **„Moderne Ransomware am Beispiel von Cerber“.** Zu Beginn ging Prof. Holz auf die historische Entwicklung von Ransomware ein. Als einschneidende Entwicklung, die aus seiner Sicht der Ransomware zum Durchbruch verholfen hat, wurde die seit 2013 eingesetzte Ransomware „CryptoLocker“ benannt, bei welcher Bitcoin als Zahlungsmittel verwendet wurde. Sodann ging Prof. Holz auf die Ransomware Cerber im Kontext zum Forschungsprojekt CAUSE-EFFECT ein. Letzteres zielt durch Data-Mining und machnine learning auf die Vorhersage von Angriffen ab. Eine erfolgreiche Cerber-Infektion vorausgesetzt, wurden die allgemeinen Abläufe für dieses Szenario erläutert. Insgesamt ist eine hohe Angriffszahl zu verzeichnen, was bedeutet, dass die Angreifer ihre Verfahren automatisieren müssen. Kann dieser Automatismus erkannt werden, soll es möglich sein auf dieser Grundlage eine Vorhersage über betroffener Server und Domains zu treffen. Anschließend wurden die grundlegenden Schritte zur Identifizierung einer Cerber Domain eingehend dargestellt. Ziel des Vorgehens ist die möglichst frühzeitige Erkennung infizierter Domains. Zum Abschluss des Vortrages gab Holz einen Überblick über die Vorhersageergebnisse von September 2016 bis Februar 2017.

Diskussion mit den Referenten

Zum Abschluss des ersten Veranstaltungstages fand eine **Diskussion mit den Referenten** der Themenbereiche zur **„Bekämpfung von Ransomware und Botnetzen“,** moderiert von **Prof. Dr. Georg Borges**, statt. Im Rahmen der Diskussion wurden verschiedene Fragen aus dem Publikum gestellt. Zunächst wurde thematisiert, ob zur Botnetzbekämpfung nicht eine generelle Basis für alle Botnetze geschaffen werden kann.

Ralf Benzmüller erläuterte hierzu, dass zwar grundsätzlich bei allen Botnetzen eine Basis benötigt wird,

die benötigten Informationen jedoch immer auf eine bestimmte Art herausgesucht werden, die bei verschiedenen Tätern durchaus auch variieren kann, was eine einheitliche Basis zur Bekämpfung unmöglich macht. Auf Nachfrage erläuterte **Philipp Ciciliani**, dass Predictive Policing derzeit nur in anderen Deliktsfällen im Einsatz ist (bspw. im Falle des Wohnungseinbruchsdiebstahls). Im Bereich der Cyberkriminalität sind Zukunftsvorhersagen aktuell schwierig, da nur bestimmte Quellen genutzt werden können. Anschließend erläuterte **Prof. Dr. Thorsten Holz** sein Projekt näher. Insbesondere die Frage, ob infizierte Domains generell abgeschaltet werden sollen oder ein Sanity-Check sinnvoll ist, wurde beleuchtet. Im Rahmen des Projektes soll es verschiedene Teams geben, welche unterschiedliche Ansätze verfolgen und ein Scoring ausführen. Derzeit befindet sich das Vorhaben noch in der Vorbereitungsphase. Start ist im Sommer, das Scoring soll im Herbst erfolgen. „Gute" Domains sollen auch vorhergesagt und identifiziert werden. Anschließend wurden Handlungsmöglichkeiten für Opfer von Ransomware-Angriffen diskutiert. Die Referenten hoben insbesondere heraus, dass bessere Optionen bestehen, als den geforderten Betrag zu zahlen. Zum einen wird im Falle der Zahlung ein kriminelles Geschäftsmodell finanziert und zum anderen sind Fälle bekannt, in denen trotz Zahlung Daten verloren gingen. **Dr. Tilman Frosch** legte dar, dass die Angreifer Dokumente häufig zunächst sammeln, im Falle der Zahlung einige entschlüsseln und erneut Zahlung verlangen, was die Kosten massiv in die Höhe treiben kann. Auch das FBI habe aufgerufen, nicht zu zahlen, wobei auch aus Sicht des FBI nachvollziehbar ist, dass die Variante zu zahlen oft die Günstigste sein kann. Dennoch ist eine Straftat geschehen, die zur Anzeige gebracht werden soll, wie Ciciliani betont. Generell können entsprechend der Ausführungen von Benzmüller zwei Angreifergruppen unterschieden werden: Diejenigen, die langfristig arbeiten möchten (Locky, Avalanche) und diejenigen, die schnell Geld verdienen möchten und die Ransomware schnell schreiben, sodass diese überhaupt nicht funktioniert oder leicht entschlüsselt werden kann.

Prof. Dr. Georg Borges: Generelle Basis zur Botnetzbekämpfung?

Ein Themenwechsel entstand anschließend durch eine letzte Frage aus dem Publikum. Diese war auf den Bereich des eGovernment, den Umgang der Verwaltung mit Daten sowie die Wertigkeit eines verschlüsselten elektronischen Grundbuches ohne Back-up gerichtet. Unter den Diskutanten bestand Einigkeit, dass auch die Verwaltung nicht anders mit Daten umgeht als Privatpersonen oder Unternehmen. Insbesondere mit Blick auf das elektronische Grundbuch haben nach einer Umfrage aus dem Jahr 2017 noch 25 % der Gemeinden kein Konzept zum Datenschutz.

„Sicherheits-TÜV für IT

Seitens des Publikums wurde gefragt, ob es nicht eine staatliche Aufgabe sein müsse, ein sicheres IT-Konzept zu schaffen oder eine Bewegung in diese Richtung zu fördern. Seitens der Referenten ist dies wünschenswert, da Unternehmen aus Kostengründen hier wohl nicht führend handeln werden. **Willi Herzig** hielt fest, dass insgesamt ein Umdenken in der EDV erfolgen müsse. Ähnlich dem TÜV bei Kraftfahrzeugen müsse auch in der EDV eine regelmäßige Sicherheitsüberpüfung und Wartung, eine Art „Sicherheits-TÜV für IT" erfolgen. Eine Umstellung der EDV auf aktuelle Systeme nach 10 Jahren erscheint sinnvoll und anzudenken. Auch Benzmüller forderte rechtliche Sicherheitsstandards für Smart Grid.

Zum Ende der Diskussionsrunde bat Prof. Borges die Referenten, einen Wunsch bezüglich Maßnahmen zur IT-Sicherheit zu äußern. Prof. Holz hob hervor, dass aufgrund wenig interdisziplinärer Zusammenarbeit vieles unkoordiniert läuft und „EDATA" hier zur Problemlösung beitragen soll. **Hungenberg** regte an, dass auch die Endnutzer in bestimmten Fällen den Schaden zu tragen hätten, bzw. selbst handeln sollen, um den Schaden abzuwenden, um das Bewusstsein für Fragen der IT-Sicherheit zu schärfen und die Bereitschaft für Investitionen in diesem Bereich zu erhöhen. Dr. Frosch schloss sich diesem Wunsch an und ergänzte den Wunsch nach konkreteren Vorgaben sowie Maßnahmen zur Einhaltung und Umsetzung dieser. Herzig äußerte den Wunsch nach besserer Kooperation zwischen den einzelnen Ländern und einer Angleichung der Gesetze, um die Ko-

operation zu erleichtern.

Dem schloss sich Ciciliani an und wies darauf hin, dass es internationale Netzwerke gibt, hier aber viel Luft nach oben bleibt. Benzmüller wies zum Schluss darauf hin, dass Verbraucher die IT-Sicherheit ernst nehmen sollten. Bereits bei der Konzeption von Netzwerken soll an Missbräuche gedacht werden, die Netzwerke durch die Betreiber bereits in diesem Schritt bestmöglich abgesichert werden. 100 %-ige Sicherheit muss nicht gegeben sein. Kardinalfehler, die die Erkenntnisse der Vorjahre aufgezeigt haben, müssten aber vermieden werden.

Themenbereich 3 „Vertrauenswürdige Identifizierung“

Den zweiten Veranstaltungstag eröffnete **Bernd Kowalski**, Abteilungspräsident „Sichere elektronische Identitäten, Zertifizierung und Standardisierung“ beim Bundesamt für Sicherheit in der Informationstechnik. Er leitete in den Themenbereich 3 **„Vertrauenswürdige Identifizierung“** ein und hob insbesondere die Relevanz zuverlässiger und vertrauenswürdiger Identifizierung in der digitalen Gesellschaft heraus. Zudem ging Kowalski auf die besondere Rolle des BSI bei der Einhaltung der einschlägigen Vorschriften ein.

Den ersten thematischen Vortrag an diesem Tag übernahm **Dr. Ulf Löckmann** vom Bundesamt für Sicherheit in der Informationstechnik. In seinem Vortrag **„Sicherheit von Video-Identifizierungsverfahren“** referierte er über Fernidentifizierungsverfahren allgemein und Videoidentifizierungsverfahren im Besonderen. Eingangs wurden die Anwendungsgebiete von Fernidentifizierungsverfahren, sowie die Ziele einer sicheren videobasierten Fernidentifizierung (Existenz, Legitimität, Eindeutigkeit) vorgestellt. Der Schwerpunkt des Vortrags lag auf der Untersuchung verschiedener Möglichkeiten zur Video-Manipulation von Ausweisdokumenten, aufgezeigt am Beispiel des neuen deutschen Personalausweises. Von zentraler Bedeutung seien an dieser Stelle die Sicherheitsmerkmale des Personalausweises, die im Videochat überprüft werden können. Dr. Löckmann erläuterte die Erstellung einer manipulierten Ausweisvorlage zu Testzwecken und zeigte anhand einer Videodemonstration, dass im Rahmen einer Videoidentifizierung keine Unterschiede zwischen dem echten und dem manipu-lierten Dokument erkennbar sind. Zum Abschluss des Vortrages wurde auf die Vertrauensniveaubewertung von Verfahren nach der eIDAS-VO eingegangen.

Dr. Thomas Schnattinger: Vorgaben der eIDAS-VO zur Notifizierung nicht operabel

Die Authentifizierung von Nutzern bei Webanwendungen stellte **Prof. Dr. Jörg Schwenk,** Inhaber des Lehrstuhls für Netz- und Datensicherheit an der Ruhr-Universität Bochum und Mitglied des Vorstandes der a-i3, bei seinem Vortrag zur **„Browser-Identifizierung“** in den Mittelpunkt. Eingangs wurden die Komplexität von Webanwendungen, deren allgemeiner Aufbau, sowie die aktuellen Anwendungen dargestellt. Dann ging Prof. Schwenk auf die kryptographischen Elemente im Webbrowser ein, insbesondere beleuchtete er das unter der Schirmherrschaft von Google entwickelte Protokoll Token Binding. In einer Animation wurden die Funktionsweise dieses Protokolls bei einer Two-Factor-Authentication dargestellt und mögliche Angriffsszenarien zum Identitätsdiebstahl sowie die damit einhergehenden Risiken der Verwendung eines Bearer Tokens erörtert. Hier setzt das neue Google Protokoll an. Als Lösungsansatz wurde die Umwandlung von Bearer Tokens in PoP-Tokens vorgeschlagen. Mit der Implementierung von „Crypto API“ setzt Google diese Umwandlung um.

Zum Schluss stellte Prof. Schwenk die Funktionsweise des Token Binding Protocol detailliert dar. Nach seiner Auffassung werden durch die Implementierung und die PoP-Tokens die datenschutzrechtlichen Anforderungen eingehalten.

Dr. Thomas Schnattinger, Bundesamt für Sicherheit in der Informationstechnik, referierte zum Thema **„Notifizierung von Identifizierungsdiensten nach eIDAS“.** Zu Beginn gab er einen allgemeinen Überblick über elektronische Vertrauensdienste und elektronische Identifizierung und erörterte die bestehenden Unterschiede. Er verglich elektro-nische Vertrauensdienste und elektronische Identifizie-

rung im Hinblick auf Aufsicht, Anerkennung und Notifizierung. Weiterhin wurden die Anforderungen an eine eID-Notifizierung erörtert. In diesem Zusammenhang sind die Vorgaben der eIDAS-VO nicht operabel, weshalb zusätzliche Guides veröffentlicht wurden, die die entsprechenden Punkte konkretisieren. Auch der Stand der Notifizierung der deutschen eID sowie die weiteren im Rahmen des Notifizierungsverfahrens erforderlichen Verfahrensschritte wurden präsentiert. Sodann wurde auf die technischen Initiativen und das Gesetz zur Förderung der elektronischen Identifizierung eingegangen. In einer informellen Anfrage haben bereits andere EU-Länder die Einleitung eines Notifizierungsverfahrens angekündigt. Letztlich gab er noch einen Überblick über die Auswirkungen elektronischer eIDs auf Diensteanbieter.

Kowalski dankte den Referenten und zog ein kurzes **Fazit des Themenbereichs:** Als Basis für einen Wandel im Bereich vertrauenswürdige Identifizierung, insbesondere bei großen Herstellern, sieht er die Anforderungen an Daten- und IT-Sicherheit auf dem europäischen Markt.

Horst Samsel: Verbaucher kann Schwachstellen nicht beheben

Themenbereich 4 „Risiken und Sicherheit von Produkten für Verbraucher“

Horst Samsel vom Bundesamt für Sicherheit in der Informationstechnik gab eine Einführung in den Themenbereich 4: **„Risiken und Sicherheit von Produkten für Verbraucher“.** Vor dem Hintergrund des Verbraucherschutzes und millionenfacher Identitäts-missbräuche warf er die Frage nach Schutzmaßnahmen insbesondere mit Blick auf Ransomware auf, welcher im Themenbereich besondere Bedeutung zukommt.

Über die **„Sicherheit von Android-Systemen“** referierten **Thomas Bradler** von der Verbraucherzentrale NRW und **Dr. Jürgen Neumann-Zdralek** vom Bundesamt für Sicherheit in der Informationstechnik. Dr. Neumann-Zdralek betonte den hohen Marktanteil von Android-Systemen, deren Gefahren Kunden nur schwer erkennen können. Er benannte einige bekannte Fälle von Schadsoftware, wie Stagefright Multimedia-Bugs, TowelRoot, PingPongRoot, Dirty Cow, Quadrooter und Gooligan. Bezüglich Schadsoftware liegen große Sicherheitslücken vor, die stetig zunehmen.

Insgesamt bemängelt Dr. Neumann-Zdralek den hohen Wartungsaufwand, der durch eine Vielzahl unterschiedlicher Modelle je Hersteller entsteht. Auch die Versionsvielfalt und die Tatsache, dass ältere Versionen nach kurzer Zeit nicht mehr unterstützt werden, trägt zur Gefahrerhöhung bei. Auch Schutzmaßnahmen zugunsten des Verbrauchers wurden erörtert. Hier wird empfohlen, Herstellerupdates sofort einzuspielen, Updates durch den Google Play Store zuzulassen, Testprogramme für Schwachstellen zu nutzen und Software verantwortungsvoll zu installieren.

Bradler widmete sich im Rahmen seines Vortragsteiles insbesondere dem Thema IT-Sicherheit. Auch er betonte die hohen Risiken für die Verbraucher gerade bei der Nutzung von Online-Banking und ähnlich sicherheitskritischen Anwendungen. Für Nutzer sind die Sicherheitslücken nicht erkennbar, sie erhalten keinerlei Informationen zum richtigen Umgang mit dem Smartphone. Ursächlich hierfür ist eine Vielzahl an Fehlerquellen und beteiligter Anbieter. Hier sind die Hersteller in der Pflicht, rechtzeitig und regelmäßig Updates zur Verfügung zu stellen. Auch die rechtlichen Unwägbarkeiten hinsichtlich des Mängelgewährleistungsrechts bei fehlerhaftem oder unsicherem Betriebssystem sieht Bradler kritisch. Der Verbraucher habe diesbezüglich keine Einblicke, sodass es zu erheblichen Beweisbarkeitsproblemen und Durchsetzbarkeitsproblemen komme. Die Kunden wüssten selbst am Tag des Kaufs nicht, ob aktuell Sicherheitslücken bei einem Modell vorlägen. Es sei daher erforderlich, Verkäufern eine Informationspflicht über Sicherheitslücken, die zum Zeitpunkt des Kaufs bekannt seien, aufzuerlegen. Auch nach dem Vertragsschluss sollte die IT-Sicherheitskompetenz der Kunden beispielsweise durch ein Gütesiegel gestärkt werden. Bei gravierenden Sicherheitslücken müsste größere Transparenz geschaffen werden. Auch rechtlich müsse den Kunden ein Anspruch auf die Behebung von Sicherheitslücken an die Hand ge-

geben werden.

Dr. Thorsten Behling, Partner der WTS Legal Rechtsanwaltsgesellschaft mbH, referierte über die **„Verantwortlichkeit für Produktsicherheit und Datenschutz“.** Er stellte die aktuelle Rechtslage mit Fokus auf der Datenschutzgrundverordnung (DSGVO) und dem Entwurf der e-Privacy-Verordnung dar. Nach Art. 4 Nr. 7 DSGVO knüpft die datenschutzrechtliche Verantwortlichkeit daran an, wer über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Die Sicherheit der Datenverarbeitung sei insoweit eine Kernverantwortung des Verantwortlichen. Neu ist dabei, dass nach Art. 32 DSGVO ein Verfahren zur ständigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit getroffener technisch-organisatorischer Maßnahmen notwendig ist. Aber auch Hersteller haben eine Verantwortung, wenn sie Daten zu eigenen Zwecken nutzen und verwenden. Aus der Verantwortlichkeit für den Datenschutz ergeben sich umfassende Dokumentations- und Nachweispflichten. Bei Verstößen gegen Art. 5 DSGVO können zukünftig empfindliche Bußgelder auferlegt werden. Dies soll den Hersteller ermutigen, den Datenschutz bei Entwicklung und Gestaltung zu berücksichtigen (Erwägungsgrund 78 der DSGVO). Nach seiner Ansicht sollte über eine Charakterisierung einer DSVGO-Inkompatibilität als Sach- oder Werkmangel nachgedacht werden. Gerade bei Standardprodukten müsse das Mängelgewährleistungsrecht Anwendung finden. Produktsicherheits- und Produkthaftungsgesetz spielen nach seiner Meinung in Bezug auf Datensicherheit eine eher untergeordnete Rolle.

Dr. Thorsten Behling: Mängelhaftung für Sicherheitslücken

„Recht auf Nicht-IT-Expertise

Mit der Frage, welche Schutzmöglichkeiten und Schutzpflichten der Staat im Bereich der Digitalisierung gegenüber seinen Bürgern innehat, befasste sich **Dr. Christian Mrugalla**, Leiter des Referates „Schutz der Bürger und Bürgerinnen im Internet“ am Bundesministerium des Innern, in seinem Vortrag **„Sicher und souverän in der Digitalisierung – Was kann und sollte der Staat für den Schutz der Bürgerinnen und Bürger tun?“.** Er erläuterte, dass eine faire Lastenverteilung zwischen Nutzern, Herstellern, Dienstleistern und Providern hergestellt werden soll, von der wir heute noch weit entfernt sind. Eine Spaltung zwischen realer und digitaler Welt ist auf Dauer nicht möglich. Im Cyber-Raum sollte sich der Bürger mit einem fundierten Risiko-Gefühl bewegen, dabei ein „Recht auf Nicht-IT-Expertise“, aber kein „Recht auf Leichtsinn“ haben. Hierzu bleiben die „klassischen“ Aufgaben des Staates wichtig, die Setzung eines gesetzlichen Rahmens, Sensibilisierung und Aufklärung sowie Zertifizierung oder die Förderung von Sicherheitstechnologien. Aktuelle Herausforderungen für den Staat bestehen insbesondere in den Bereichen der Geschäftsbedingungen, mobiler Endgeräte, Sicherheit für Kleinstunternehmen und dem Internet-of-Things für Endverbraucher. Die aktuellen Fragestellungen wurden kurz näher beleuchtet. Gegen Ende des Vortrages ging Dr. Mrugalla auf mögliche Handlungsoptionen ein. Hier nannte er die Schaffung von Sicherheitstransparenz durch Gütesiegel oder Zertifikate sowie neue Haftungsregeln und Versicherungen, um zu gewährleisten, dass Hersteller, Dienstleister und Provider in Zukunft ihrer Verantwortung gerecht werden.

Der anschließende Vortrag widmete sich dem Thema **„Datenschutz und Sicherheit von Instant-Messaging-Protokollen“. Paul Rösler,** Masterstudent der IT-Sicherheit und Doktorand an der Ruhr-Universität Bochum, ging auf die mobile Kommunikation von Parteien über das Internet ein. In erster Linie beleuchtete er marktübliche Apps wie What’s App, Facebook Messenger, etc. Im Unterschied zum E-Mail-Verkehr, bei dem jeder Teilnehmer seine Nachrichten über einen eigenen Provider empfängt und versendet, laufen die Nachrichten bei diesen Diensten über einen zentralen Provider. Im Fokus seiner Forschungsarbeit steht die Sicherung der Privatsphäre der Nutzer. Durch eine Ende-zu-Ende-Verschlüsselung kann nur der Inhalt der Nachrichten, nicht jedoch das Protokoll geschützt werden, welches Aufschluss darüber gibt, ob der Gesprächspartner die Nachricht empfangen und gelesen

hat. Auch Gruppenchats sind als kritisch einzustufen. Hier ist ebenfalls nur der Nachrichteninhalt geschützt, alle weiteren Informationen wie das Hinzufügen neuer Mitglieder jedoch nicht. Der Provider könnte daher neue Mitglieder hinzufügen, Nachrichten löschen oder neu sortieren. Dies könnte die komplette Vertrauenskette brechen. Aus diesem Grund sind einige Protokolle für eine vertrauenswürdige Kommunikation innerhalb der Gruppe nicht verwendbar.

Podiumsdiskussion „Wieviel Sicherheit braucht die Digitalisierung?“

Zum Abschluss des Symposiums fand eine hochkarätig besetzte Podiumsdiskussion zum Thema **„Wieviel Sicherheit braucht die Digitalisierung?“** statt. Die Moderation übernahm **Ulrich Gasper,** verantwortlicher Redakteur der CR, Verlag Dr. Otto Schmidt. Er diskutierte mit **Prof. Norbert Pohlmann,** Leiter des Instituts für Internet-Sicherheit – if(is) der Westfälischen Hochschule, **Robert Stein,** Landtagsfraktion der CDU NRW, **Prof. DDr. Erich Schweighofer,** Universität Wien sowie **Dr. Christian Mrugalla** unter reger Beteiligung des Publikums.

Gasper eröffnete die Podiumsdiskussion mit der Feststellung, dass jede Software im Schnitt 14 Schwachstellen hat und wir sie dennoch täglich nutzen. Dies führt zur Ausgangsfrage der Diskussion: Wieviel Sicherheit braucht die Digitalisierung?

Ulrich Gasper: Jede Software hat 14 Sicherheitslücken – Genutzt wird sie trotzdem.

Prof. Pohlmann will diese Frage unter 3 Gesichtspunkten betrachten: Nutzersicht, Wirtschaftsspionage und Cyberwar. Wägt man alle Kriterien miteinander ab, muss am Ende eine Lösung stehen, mit der sich der Nutzer noch wohlfühlen kann und die dennoch für Wirtschaftsspionage und Cyberwar eine möglichst geringe Angriffsfläche bietet.

Stein betont, dass die Digitalisierung die gleiche Sicherheit benötigt, wie die physische Welt, jedoch aufgrund der Globalität vor besonderen Herausforderungen steht. Prof. Schweighofer greift den Ansatz von Pohlmann auf. Beim Bürger muss langfristig ein Problembewusstsein geschaffen werden und zugleich ein Sicherheitsniveau gefunden werden, bei dem er sich noch wohlfühlen kann. In diesem Bereich sind die Staaten aufgrund der Bedrohung durch Cyberwar aufgewacht.

Dr. Mrugalla schlägt vor, den Menschen in den Mittelpunkt der Digitalisierung zu stellen. Ziele und Vorteile der Digitalisierung können nur erreicht werden, wenn ein angemessenes Sicherheitsniveau besteht. Zum Schutz des Gemeinwohls bzw. gemeinsamer Güter muss eine Art „Digitaler Landfrieden“ geschaffen werden.

Aus dem Publikum wurde eingeworfen, dass die funktionelle Sicherheit ein tragendes Element von Industrie 4.0 und dem IoT darstellt, wozu unsichere Apps mit zahlreichen Schwachstellen eklatant im Widerspruch stehen. Pohlmann bestätigt, dass die IT zunehmend die persönliche Sicherheit beeinträchtigt, bspw. im Falle gehackter Herzschrittmacher oder autonomer Fahrzeuge. Auch Stein zeigte auf, dass Angriffe ggf. lebensbedrohlich werden können und aus diesem Grund ein Rahmenwerk für Unternehmen geschaffen werden muss, das es Unternehmen ermöglicht, höchste Sicherheitsverfahren zu wählen.

Gasper leitete anschließend über zum aktuellen Gesetzesentwurf bezüglich der Fake News. Prof. Schweighofer bezog hierzu Stellung, dass die Wirtschaft keine IT-Sicherheit selbst festlegen kann und die Politik aus diesem Grund verantwortlich ist. Auch Dr. Mrugalla betonte, dass punktuelle Regelungen in manchen Bereichen sinnvoll sind, um die Vorteile der Digitalisierung zu erreichen. Aus dem Publikum wurde ein Vergleich zur analogen Welt mit einer Vielzahl an Sicherheitsregeln gezogen, was die Frage aufwirft, ob in der digitalen Welt nicht eine ähnliche Anzahl an Sicherheitsregeln erforderlich ist. Prof. Pohlmann bestätigte, dass das Vertrauen in der analogen Welt durch Regularien, wie bspw. den TÜV von Autos, gesichert ist. Gleiche Mechanismen sind nach seiner Ansicht auch in der IT erforderlich.

Hierzu kam aus dem Publikum eine Gegenmeinung, dass Technik, Organisation und Recht immer kollidieren. Anstatt zu viel zu regulieren solle Awareness beim User geschaffen werden. Insbesondere würden Schäden häufig zu spät erkannt, Nutzern drohten kei-

ne Strafen, was die Risikobereitschaft erhöht.

„IT-Sicherheit muss Plug-and-Play sein

Es wurde betont, dass IT-Sicherheit Plug-and-Play sein muss. Ein Nutzer will sich in der Regel nicht mit IT-Sicherheit auskennen müssen, aber trotzdem das Level der IT-Sicherheit haben, das Fachleute empfehlen, unter Berücksichtigung der persönlichen Referenzen. Insoweit ist vor die Regulierung zu erwarten, dass der Staat eben eine solche Ordnung schafft. Hier weist Dr. Mrugalla darauf hin, dass bei Durchsetzung dieses Ansatzes die Gefahr besteht, dass punktuelle Freiheitseinschränkungen erforderlich werden. Dies könne jedoch nicht erfolgen, ohne zuerst erst ein Konzept zu schaffen. Im Ergebnis wurde festgehalten, dass die Gesellschaft nicht ohne Regulierung auskommen wird. Der Verbraucher kann nach Ansicht von Stein mit grundlegenden Pflichten wie bspw. regelmäßigen Updates bereits ein gewisses Maß an Sicherheit schaffen, 100 %-ige Sicherheit kann nicht erzielt werden.

Nach einer kurzen Zusammenfassung übergab Gasper das Wort an die Veranstalter Prof. Dr. Georg Borges und Prof. Dr. Jörg Schwenk, die ihrerseits nach einem Überblick über die Vorträge ein kurzes Fazit zogen und den Referenten und Teilnehmern dankten. Gedankt wurde auch dem Center for Advanced Internet Studies (CAIS) für die Förderung des Symposiums.

Informationen zur a-i3 und ihren Tätigkeiten, sowie zum nächsten Symposium finden Sie im Internet auf der Website der a-i3 unter:

www.a-i3.org

Prof. Dr. Norbert Pohlmann (oben), Christian Mrugalla

Das a-i3/BSI-Sympsosium 2017 wurde vom Center for Advanced Internet Studies als interdisziplinäre Forschungsveranstaltung gefördert.
Weitere Informationen: www.cais.nrw

CAIS CENTER FOR ADVANCED INTERNET STUDIES

Medienpartner des a-i3/BSI-Symposiums 2017

CR COMPUTER UND RECHT

itrb IT-Rechts-berater