IT, Recht und Gesellschaft

Neben technischen Fragen wurden beim 16. Security-Forum am 2. und 3. Mai 2018 in der FH Hagenberg auch rechtliche und gesellschaftspolitische Fragen der Informationstechnik behandelt.

Aus 68 Likes kann mit Analyseverfahren die Hautfarbe des Nutzers zu 95 Prozent ermittelt werden, zu 85 Prozent seine sexuelle Orientierung und politische Einstellung. Aus der Auswertung von 150 Likes kennt man ihn besser als seine Eltern ihn kennen, und aus 350 Likes kennt man ihn besser als er sich selbst." Damit zeigte OberstdG Mag. Walter Unger, Leiter des Cyber-Abwehrzentrums des Bundesheeres, beim *16. Security Forum* des Hagenberger Kreises auf, wie tiefgreifend Informationen ausgewertet werden können. Die Gesamtzahl der bisher weltweit gespeicherten Daten liegt im Bereich von Zetta-Bytes (Sextillionen; 10^{21} Bytes). Um das bisher gespeicherte Videomaterial zu sichten, würde ein Mensch 14,5 Milliarden Jahre brauchen. Den Wahrheitsgehalt der gespeicherten Informationen und ihre Seriosität zu prüfen, ist kaum möglich, und bei den derzeitigen Spannungsverhältnissen in der Welt kommt der Kampf um die öffentliche Meinung dazu.

Hybride Konfliktformen machen Cyber-Angriffe auf die Stromversorgung und die Informations- und Kommunikationstechnik wie Cloud, GPS oder Galileo, soziale Medien, wahrscheinlich, und das mit sehr kurzen Vorwarnzeiten. Bemerkt werden die Angriffe meist erst, wenn der Schaden eingetreten ist.

Die technischen Trends entwickeln sich vom *Internet of Things (IoT)* zum *Internet of Everything (IoE)* in der *Smart World*. 2020 werden 50 Milliarden Dinge an das Internet angeschlossen sein.

Fachhochschule Hagenberg: Das jährliche Security Forum fand 2018 zum 16. Mal statt.

Mit dem *5G*-Netz, dessen Frequenzen noch 2018 versteigert werden, wird man im Netz, bildlich gesprochen, statt auf einer Autobahn mit vier Spuren auf einer mit 20 Spuren unterwegs sein.

Die neuen Technologien werden die Arbeitswelt radikal verändern. Blockchain-Techniken werden vertrauenswürdige Dritte ersetzen können, beispielsweise bei einer Digitalisierung des Grundbuchs die Tätigkeit von Rechtsanwälten oder Notaren auf diesem Gebiet. Supermärkte ohne Kassen, die gekaufte Waren berührungslos verrechnen, werden den Einzelhandel verdrängen. Ersatzteile werden mit Auswirkungen auf die Logistik nicht mehr geliefert, sondern im 3D-Druck hergestellt. Maschinen sind schneller, machen weniger Fehler, können rund um die Uhr arbeiten, was zu einer weiteren Automatisierung führen wird. Oberst Unger zitierte die Bundesministerin für Digitalisierung und Wirtschaftsstandort, Dr. Margarete Schramböck, wonach 60 Prozent der heutigen Schüler einen Beruf ausüben werden, den es derzeit nicht gibt.

Die meisten Unternehmen können ohne IT nicht bestehen. Das Risiko sind die Schwachstellen in Programmen. Täglich werden drei bis fünf neue Schwachstellen entdeckt, führte Unger unter Verweis auf die „Schwachstellenampel" des deutschen *CERT* aus *(www.cert-bund.de/overview)*. 70 bis 80 Prozent der Fehler werden durch schlecht ausgebildete oder unvorsichtige Mitarbeiter verursacht. Gezielte Angriffe werden häufiger. Schadprogramme werden industriell gefertigt *(Crime as a Service – CaaS)*. Terroristen und Kriminelle nützen den Cyber-Raum. Cyber-Angriffe werden auch zur Beeinflussung der öffentlichen Meinung durchgeführt. Abwehrstrategien bestehen unter anderem darin, die Zahl der Angriffsflächen zu reduzieren und Redundanzen aufzubauen. Mit der Österreichischen Strategie für Cyber Sicherheit (ÖSCS) liegt seit 2013 ein Konzept zum Schutz des Cyber-Raums vor.

Nutzung von Daten. Den Satz: „Wer nichts zu verbergen hat, der hat auch nichts zu befürchten", bezeichnete Dr. Wolfgang Schnabl, *Business Protection (www.business-protection.at)*, für den IT-Bereich als nicht zutreffend. Je mehr Daten über jemanden bekannt sind, umso angreifbarer wird er. Es würden sogar Wahlkampagnen auf Datenanalysen gestützt, indem zielgerichtet Mails mit politischen Inhalten verschickt werden. Der Datenschutz müsse verhindern, dass personenbezogene Daten zweckwidrig ausgewertet werden. Selbst wenn diese Daten verschlüsselt würden, blieben sie personenbezogen. „In der IT gibt es nichts, was nicht personenbezogen wäre", sagte Schnabl. Nach Erwägungsgrund 30 der DSGVO fallen auch IP-Adressen und Cookie-Kennungen unter die zu schützende Daten. Allgemein werde, dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit c DSGVO) folgend, davon ausgegangen, dass Logfiles nach einigen Wochen zu löschen seien. Damit aber werde es schwer, langfristig geplanten Angriffen (ATPs) auf die Spur zu kommen. Im Durchschnitt würden derartige Angriffe in den USA nach 200, in Europa erst nach 277 Tagen erkannt.

Dass man mit den in sozialen Medien verbreiteten persönlichen Daten und Mitteilungen sorgsamer umgehen sollte, werde durch die Website *pleaserobme.com* deutlich. An „Freunde" oder „Follower" verschickte Meldungen über Urlaubsantritte können durch Verknüpfung mit anderen Daten und mit

FOTO: KURT HICKISCH

Geo-Daten zur Einladung für Einbrecher werden.

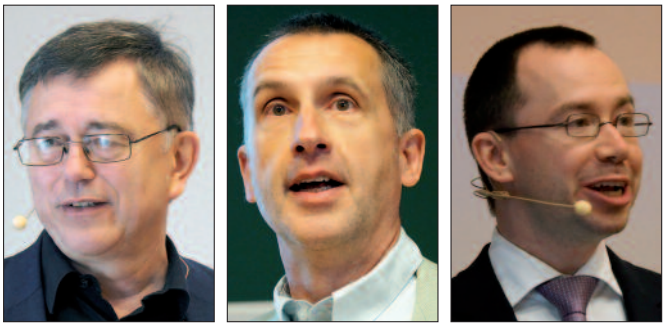
Im Prinzip sei, sagte Schnabl, die Verarbeitung personenbezogener Daten verboten, sofern diese Verarbeitung sich nicht auf ein Gesetz, eine vertragliche Regelung oder die Zustimmung des Betroffenen gründe. Die Zustimmung setze Freiwilligkeit und Informiertheit voraus und könne jederzeit widerrufen werden. Sei keine dieser Voraussetzungen für eine Verarbeitung gegeben, könnte eine solche auf ein überwiegendes Interesse des Auftraggebers oder dritter Personen gestützt werden. Durch technische und organisatorische Maßnahmen müssen die Integrität der Daten, deren Vertraulichkeit und Verfügbarkeit gesichert werden.

Im Grunde genommen würden die Art. 24 (Verantwortung des für die Verarbeitung Verantwortlichen) und 32 DSGVO (Sicherheit der Verarbeitung) ein Datenschutz-Management ähnlich der ISO 27.000-Reihe umschreiben.

Strukturierung von Daten. Um den Verpflichtungen nach der DSGVO beispielsweise hinsichtlich des Rechtes eines Betroffenen auf Auskunft, Richtigstellung oder Löschung seiner Daten nachkommen zu können, ist erforderlich zu wissen, wo sich dessen Daten befinden. „80 Prozent aller Daten in Unternehmen sind unstrukturiert“, sagte Georg Beham, *Grant Thornton Advisory GmbH (www.grantthornton.at),* unter Berufung auf eine Untersuchung des IT-Marktforschungsunternehmens *Gartner*. In ebenso vielen Unternehmen besteht laut dem Wirtschaftsmagazin *Forbes* wenig Wissen über den Inhalt dieser Daten.

Um in den unstrukturierten Daten die personenbezogenen Daten zu identifizieren, werden die Daten mittels forensischer Technologie *(eDiscovery)* aufbereitet, was Ko-Referent Roland Pucher, *Grand Thornton,* erläuterte. Zu untersuchende Speicherorte können E-Mail-Systeme, Netzlaufwerke sein oder Archivsysteme. In einer Vorstufe wird die vollständige Datenstruktur einschließlich der Metadaten eingelesen, ohne dass der Dateninhalt verarbeitet wird. Darauf folgt eine Datenreduktion durch Filterung der Datenmenge anhand von Metadaten wie beispielsweise Datentyp, Zeitstempel, Dateigröße, Pfad, usw. Bilddaten (PDF, Bilder u. a.) werden mit Hilfe der Texterkennung (OCR) aufbereitet, um den Inhalt von gescannten Dokumenten (Rechnungen, Verträge) verarbeiten zu können. Die Daten werden in Kategorien klassifiziert.

Datenrechtsexperten Georg Beham und Roland Pucher (Grand Thornton Advisory).



Security-Forum 2018 in Hagenberg: Cyber-Abwehrexperte Oberst Walter Unger (BMLV), Wolfgang Schnabl (Business Protection) und Rechtsanwalt Lukas Feiler.

Die Auswertung ermöglicht die Identifikation personenbezogener Daten, lässt ersehen, wo vertrauliche Dokumente wie etwa Verträge abgelegt sind, und identifiziert die „Kronjuwelen“ *(Assets)* eines Unternehmens. In der Folge bildet sie durch die Transparenz der Datenstrukturen die Grundlage für eine dem Datenschutz konforme Vorgangsweise.

Datensicherheit. Nach Art. 32 der DSGVO sind bei der Verarbeitung von Daten dem Risiko angemessene Sicherheitsmaßnahmen zu treffen, wobei der Stand der Technik, die Einführungskosten und die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung zu berücksichtigen sind sowie die unterschiedliche Eintrittswahrscheinlichkeit und die Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen. Somit sind die Kosten von Sicherheitsmaßnahmen gegenüber den Risiken für die Betroffenen abzuwägen, wie Rechtsanwalt Dr. Lukas Feiler, *Baker McKenzie (www.bakermckenzie.com),* ausführte.

In der Praxis wird das betriebswirtschaftliche Risiko für ein Unternehmen im Vordergrund stehen. Es drohen Schadenersatz und Sammelklagen, Geldbußen und Image-Schäden.

Die von der DSGVO bezeichneten Maßnahmen bestehen in der Pseudonymisierung und Verschlüsselung personenbezogener Daten; in der Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste auf Dauer sicherzustellen sowie, die Verfügbarkeit nach einem Zwischenfall rasch wie-

HAGENBURGER KREIS

Security-Forum

Seit 2003 veranstaltet der Verein „Hagenberger Kreis zur Förderung der digitalen Sicherheit“, jährlich das „Security-Forum“. Die über 560 Mitglieder des Vereins setzen sich aus Studenten und Absolventen der Studiengänge „Sichere Informationssysteme SIB und SIM“ der Fachhochschule Hagenberg in Oberösterreich zusammen. Geboten werden Vorträge organisatorischen und technischen Inhalts zu aktuellen Fragen der IKT-Sicherheit, mit einer Abendveranstaltung, die zum Networking dient. In den Foyers sind Unternehmen mit Ausstellungsständen vertreten.

Zum 16. „Security-Forum“ am 2. und 3. Mai 2018 in der Fachhochschule Hagenberg waren über 260 Teilnehmer registriert.

www.hagenberger-kreis.at

www.securityforum.at

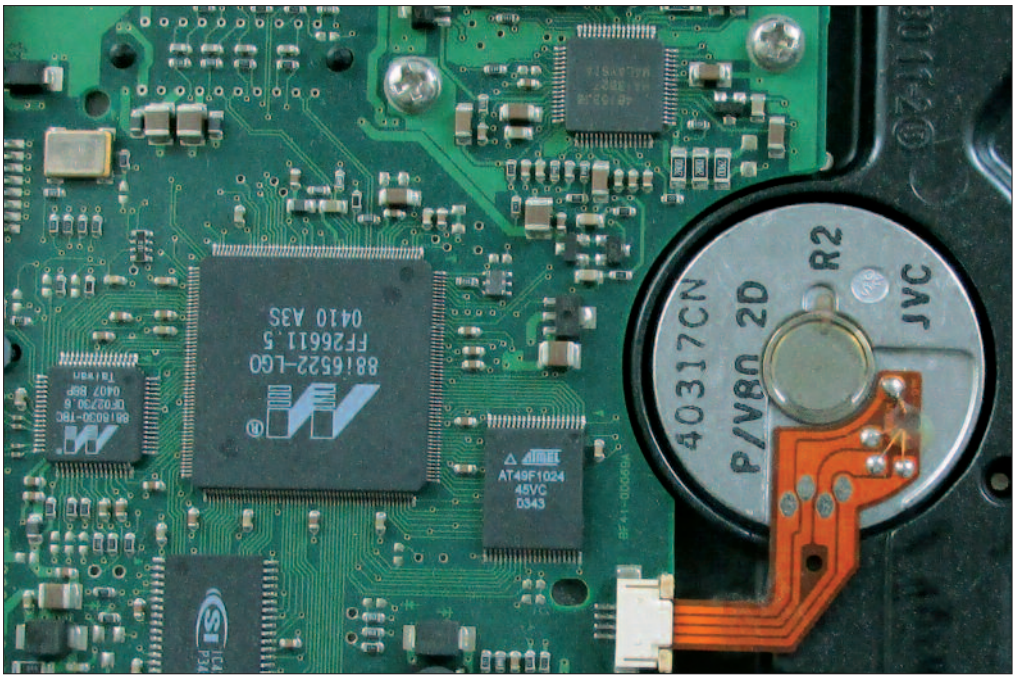
FOTOS: KURT HICKISCH

derherzustellen *(Incident Response Capabilities)*. Ferner sind Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Sicherheitsmaßnahmen *(Audits)* zu installieren.

Diese Maßnahmen lassen sich nach Feiler ihrer Art nach einteilen in technische, organisatorische oder physische. Nach der Wirkungsweise können sie in präventive, detektivische, reaktive und abschreckende Maßnahmen unterteilt werden. Aus dieser Einteilung ergibt sich eine Matrix derart, dass beispielsweise eine präventive Maßnahme aus technischer Sicht aus einer Firewall besteht, organisatorisch das Vier-Augen-Prinzip eingeführt und physisch ein gesicherter Zugang hergestellt wird. Abschreckend wirken technisch Warnmeldungen, organisatorisch Disziplinarbestimmungen und physisch Bewachungsmaßnahmen.

Der Auftragsverarbeiter hat eine dokumentierte Weisung des Verantwortlichen zu befolgen (Art. 28 Abs. 3 lit. a DSGVO). Sollte dieser eine Weisung erteilen, gewisse Sicherheitsmaßnahmen nicht durchzuführen, trifft den Auftragsverarbeiter eine Warnpflicht. Er hat dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mitzuteilen.

Eine unbefugte Offenlegung oder ein unbefugter Zugang verletzen die Vertraulichkeit personenbezogener Daten; Veränderungen die Integrität; Vernichtung oder Verlust bedeuten die dauerhafte Verletzung der Verfügbarkeit. Der Verantwortliche hat eine Meldepflicht an die Datenschutzbehörde, wenn die Verletzung zu einem Risiko für Betroffene führt (Art. 33 DSGVO). Die Meldung ist unverzüglich zu erstatten, möglichst binnen 72 Stunden, per E-Mail *(dsb@dsb.gv.at)*. Die Betroffenen hat der Verantwortliche zu benachrichtigen, wenn die Verletzung zu einem hohen Risiko für sie führt (Art. 34 DSGVO). Die Benachrichtigung hat unverzüglich zu erfolgen, per Brief, E-Mail oder sonstiger elektronischer Nachricht, sofern dies keinen unverhältnismäßig hohen Aufwand erfordert; sonst durch öffentliche Bekanntmachung. Als Beispiele nannte Feiler den vergessenen Laptop, die verirrte E-Mail oder durch Ransomware eingetretene Schäden, sofern kein Back-up der Daten besteht. Den Auftragsverarbeiter trifft eine unverzügliche Meldepflicht gegenüber dem Verantwortlichen (Art. 33 Abs. 2 DSGVO), ohne dass eine bestimmte Form vorgeschrieben wäre.



Datenverarbeitung: „80 Prozent aller Daten in Unternehmen sind unstrukturiert."

Sowohl der Verantwortliche als auch der Auftragsverarbeiter sind für die Einhaltung der Grundsätze der Verarbeitung verantwortlich. Es gilt ein Strafrahmen von bis zu 20 Millionen Euro oder vier Prozent des weltweiten Umsatzes – wobei die Datenschutzbehörde bei erstmaligen Verstößen von Verwarnungen Gebrauch machen wird (§ 11 DSG idF Z 8 Datenschutz-DeregulierungsG 2018, BGBl I 2018/24). Allerdings ist nicht jede Sicherheitsverletzung ein Verstoß gegen die DSGVO. Nachdem es hundertprozentige Sicherheit nicht gibt, wird zu berücksichtigen sein, ob angemessene Sicherheitsmaßnahmen eingeführt wurden. Ein Regress zwischen dem Verantwortlichen und dem Auftragsverarbeiter ist möglich, etwa, wenn der Auftragsverarbeiter seine Warnpflicht verletzt hat. Eine vertragliche Regelung zur Tragung von Geldbußen erscheint ratsam. Bei nicht angemessenen Sicherheitsmaßnahmen hat jeder Betroffene Anspruch auf Ersatz des materiellen und immateriellen Schadens, wobei Verantwortlicher und Auftragsverarbeiter solidarisch haften, bei Möglichkeit des Regresses. NGOs können im Namen von Betroffenen klagen, nicht allerdings in Bezug auf Schadenersatz (§ 28 DSG idF Z 15 Datenschutz-DeregulierungsG). Alle Ansprüche können dort geltend gemacht werden, wo der Beklagte eine Niederlassung (z. B. Tochtergesellschaft) hat.

Darknet. „Innerhalb einer Stunde hätte meine Frau, eine normale PC-Userin, sich im Darknet eine Pistole beschaffen können", berichtete Eddy Willems, Autor des Sachbuchs „Cybergefahr", und gab einen Einblick in die „Underground-Economy 4.0". Abgeschirmt durch das Tor-Netzwerk, hat sich ein regelrechter Markt mit Webshops entwickelt, wo mit Waffen, Drogen, Kreditkarten, falschen Identitäten und kriminellen IT-Dienstleistungen gehandelt wird. Die Installation von Schadsoftware auf 1.000 Rechnern ist um 70 US-Dollar zu haben, ein Botnetz-Aufbau im Gesamtpaket um 5.000 US-Dollar. Vergleichsweise billig sind E-Mail-Adressen: 100.000 um 7,5 US-Dollar. Es gibt Preislisten für An- und Verkauf von Kreditkarten. Unter den über 100 virtuellen Währungen dominiert im Darknet Bitcoin. „Money-Mules" bringen gegen eine Gebühr das virtuelle Geld in die reale Welt.

Kurt Hickisch

FOTO: WERNER SABITZER