Vorbeugung und Datenschutz

Organisatorische, technische und rechtliche Aspekte der Sicherheit in der Informationstechnik waren Schwerpunkte beim 15. österreichischen IT-Sicherheitstag in Salzburg.

Das Risiko sitzt vor dem Bildschirm“ – dieser oft gehörte Satz beschreibt den Mitarbeiter, dem es beim Arbeiten am Computer am nötigen Bewusstsein für Gefahren seines Handelns fehlt, der unreflektiert vor sich hinarbeitet oder am Arbeitsplatz auf virenverseuchten Internetseiten surft. Vielleicht geht fahrlässigerweise auch das Handy verloren, auf dem sich Firmendaten befunden haben. Die Entwicklung könnte in Richtung des frustrierten Mitarbeiters gehen, von dem ein höheres Risiko ausgeht, sagte Dipl.-Ing. (FH) Robert Schoblik vom Redaktionsbüro *SRG.at (www.srg.at)* am 14. November 2018 beim 15. österreichischen IT-Sicherheitstag in Salzburg.

Die Gründe dafür sieht Schoblick in der heutigen Arbeitswelt der IT-Spezialisten. Anstelle der früheren Einstellung auf Dauer wird heute von Unternehmen überwiegend auf Zeit- oder Werksvertrag oder auf Leiharbeiter gesetzt. Das Stammpersonal wird so gering wie möglich gehalten, um flexibel zu sein. Dadurch schwindet die Bindung des Arbeitnehmers zum Unternehmen, was mit einem Loyalitätsverlust einhergeht. Firmen, vor allem KMUs, bilden nicht mehr selbst aus, sondern kaufen Know-how zu. Die qualifizierte Ausbildung an sich ist lediglich die Eintrittskarte in den Arbeitsmarkt; was zählt, ist die Erfahrung im Berufsleben. Der Arbeitnehmer steht im Auswahlverfahren vor dem Problem, seine Fachkenntnisse nachzuweisen, und muss auf teure Zertifikate ausweichen.

Datenschutz: „Das Risiko sitzt vor dem Bildschirm.“

Autodidaktisches Engagement ist nicht messbar. Weiterbildung im Unternehmen selbst ist für dieses eine Kostenbelastung; der Arbeitnehmer muss „performen“. Die vernachlässigte Möglichkeit der Weiterbildung im Unternehmen bedeutet bei der raschen Entwicklung in der IT (kurze „Halbwertszeit“ des Wissens) für den Arbeitnehmer einen Verlust an Qualifikation.

Der „Fachkräftemangel“ täuscht laut Schoblick insofern, als er aus im Ingenieursbereich allgemein gemeldeten offenen Stellen hochgerechnet wird, aber nur ein Bruchteil der offenen Stellen gemeldet wird. Die digitale Transformation könnte gesellschaftliche Verwerfungen nach sich ziehen, zumal brauchbare Lösungen wie nachhaltige Ausbildungsprogramme erst erarbeitet werden müssten.

Cloud-Computing umfasst die Bereitstellung von IT-Infrastruktur über das Internet. Im Wesentlichen geht es, wie Mag. Ingo Braun, *Benn-Ibler Rechtsanwälte GmbH (www.benn-ibler.com),* ausführte, um die Bereitstellung von Anwendungssoftware *(Software as a Service – SaaS),* den Zugriff auf Programme *(Platform as a Service – PaaS)* und den Zugriff auf virtualisierte IT-Ressourcen wie etwa Speicherplatz, Rechenleistung, Netzwerke oder sogar ganze Rechner *(Infrastructure as a Service – IaaS)*. Die Cloud kann öffentlich zugänglich betrieben werden *(Public Cloud),* im Gegensatz zur *Private Cloud,* mit der Mischform der *Hybrid Cloud*. *Community-Clouds* werden für einen kleineren Nutzerkreis betrieben, etwa von Universitäten, Genossenschaften.

Das Problem liegt darin, dass man Daten aus der Hand gibt; sie befinden sich in der „Wolke“. Das kann für den Kunden den Verlust der Vertraulichkeit, der Integrität und der Verfügbarkeit seiner Daten bedeuten, kann Compliance-Vorgaben wie Datenschutz-Richtlinien verletzen, birgt das Risiko von Know-how-Verlust und bringt eine Abhängigkeit vom Anbieter mit sich. Dieser kann insolvent werden, Rechner können beschlagnahmt werden, oder es können, bei ausländischen Anbietern, politische Risiken und Rechtsunsicherheit dazukommen. Der Dienstleister wiederum wird in Anbetracht des großen Volumens der bei ihm verwalteten Daten hohe technische, personelle und organisatorische Sicherheitsvorkehrungen vorhalten müssen. Dennoch können Sicherheitslücken in der Hard- und Software auftreten, Systeme mangelhaft abgesichert sein oder Daten kopiert oder weitergegeben werden.

Abhilfe bietet die Verschlüsselung der in die Cloud eingespeisten Daten, wenn die Ver- und Entschlüsselung beim Endkunden und nicht in der Cloud erfolgt. Der Nachteil ist, dass die Schlüssel und die Software auf den Endgeräten vorhanden sein müssen, und es kann nicht gleichzeitig an einem Dokument gearbeitet werden. Ferner ist eine Verschlüsselung nur so sicher wie die Personen, die Zugriff auf das Masterpasswort des Servers haben.

Wie jedes Computersystem, ist auch das Cloudsystem strafrechtlich geschützt vor widerrechtlichem Zugriff (Hacking) (§ 118a StGB) oder vor Störung der Funktionsfähigkeit, etwa durch DDos-Attacken (§ 126b StGB). Die elektronisch verarbeiteten/gespeicherten Daten sind strafrechtlich vor Angriffen geschützt nach § 119a StGB (missbräuchliches Abfangen von Daten) oder § 126a StGB (Datenbeschädigung). Wie mit jedem anderen Computersystem können auch über die Cloud Delikte wie Betrug (§ 146 StGB) oder Erpressung (§ 144 StGB) begangen werden,

FOTO: ADOBE STOCK/SDECORET

oder es können kriminelle Inhalte wie etwa Kinderpornografie (§ 207a StGB) verbreitet werden. Bezüglich Haftungsfragen, die sich aus der Sorgfaltspflicht von leitenden Organen von Unternehmen ergeben (§§ 84 und 99 AktG, § 25 GmbHG, § 347 UGB), empfahl Braun, sorgfältig zu sein bei der Auswahl von Cloud-Anbietern und bei der Vertragsgestaltung.

Handy-Signatur. Ein neues, noch in Entwicklung befindliches Konzept der österreichischen *E-ID* (Handy-Signatur) stellte DI Kevin Theuermann, *E-Government Innovation Center (EGIZ; www.egiz.gv.at),* vor. In der bisherigen Konzeption der Handy-Signatur müssen nach dem Start der gewünschten Anwendung am PC Handynummer und Signatur eingegeben werden sowie der über SMS erhaltene, fünf Minuten lang gültige TAN-Code. Das stammt aus der Zeit, als PCs und Laptops die meist gebräuchlichen Endnutzergeräte waren und das mobile Gerät nur für den Erhalt der TAN gedacht war. Die Zwei-Faktoren-Identifizierung zum Identitätsnachweis ergibt sich aus dem Wissen (Mobiltelefonnummer und Signatur-Passwort) sowie dem Faktor Besitz, nämlich des Handys und der SMS-TAN.

Heutige Smartphones bieten sichere Authentifizierungsmethoden wie Fingerprint, Face- und Voice-Recognition, Irisscanner, und verfügen über sichere Hardware-Elemente, die nicht auslesbar sind und in denen kryptografische Schlüssel (privater Schlüssel eines asymmetrischen Verfahrens) abgelegt werden können. Damit kann der Authentifizierungsprozess mit dem Handy selbst durchgeführt werden, durch die Erzeugung einer elektronischen Signatur mit dem privaten Schlüssel. Der Zugriffsschutz wird durch die Authentifizierungsmethoden wie etwa den Fingerprint gewährleistet. Das Smartphone allein reicht für die Signierung einer Anwendung aus; Security und Usability sind in einem Gerät vereint.

Wolfgang Feiel (Rundfunk und Telekom-Regulierungs-GmbH): Weitere EU-Rechtsetzungsvorhaben in der IT-Sicherheit.

Informationstechnologie. Das Internet of Things (IoT; vielfach auch als Maschine-zu-Maschine Netzwerk, *M2M,* bezeichnet) definierte DI (FH) Alexander Marx, *conova communications GmbH (www.conova.com),* als ein System von miteinander verbundenen Geräten, Maschinen, Objekten und Gegenständen, die mit einer eindeutigen Kennung identifizierbar und fähig sind, Daten über sich und ihre Umwelt auszutauschen. Den Prognosen nach, wird es 2020 20 Milliarden dieser Geräte geben, 2050 50 Milliarden. Damit steigen die Gefahr und die Schwere von Angriffen. Dazu kommt, dass die einzelnen Devices und Sensoren schon aus Kostengründen kaum über eine für die Funktion hinausreichende Rechenkapazität verfügen, was zu Lasten der Sicherheit geht. Das begünstigt den Zusammenschluss dieser Geräte zu Botnetzen, mit denen bereits jetzt DDos-Angriffe mit kaum noch beherrschbaren 1,35 Tbits/sec erfolgen. Die Frage ist auch, wie die in den Geräten vorhandene Software aktualisiert und steigenden Sicherheitsanforderungen gerecht werden kann.

„In der realen, physischen Welt hatte der Mensch im Zuge der Evolution Zeit, sich Gefahren anzupassen“ sagte DI Philipp Reisinger, *SBA Reserch (www.sba-research.org).* „Die Cyber-Welt ist demgegenüber evolutionär noch Neuland“. Das Arpanet als Vorläufer des Internet wurde erst von knapp 50 Jahren entwickelt, den PC gibt es seit 40 Jahren, Smartphones, heutzutage alltäglich, erst seit etwas mehr als zehn Jahren. Bewusstsein gegenüber den neuen Risiken, etwa im Hinblick auf die Privatsphäre, auf Datenlecks und Datendiebstahl sowie -manipulation, müsse sich erst ausbilden. Die Angreifer sind nicht sichtbar; es fehlt die Täter-Opfer-Beziehung als Hemmschwelle. Hinzu tritt, dass die Risiken in der Cyber-Welt nicht direkt greifbar sind und die Folgen zeitverzögert eintreten, sodass der unmittelbare Lerneffekt ausbleibt.

Strafverfolgung und Gerichtsbarkeit hinken den schnellen, keine Ländergrenzen kennenden Entwicklungen hinterher und sind durch unterschiedliche territoriale Rechtssysteme beschränkt. Beide, die reale und die virtuelle Welt, müssten ineinander verschmelzen, sagte Reisinger.

Neben der DSGVO und der NIS-RL (EU) 2016/

FOTO: KURT HICKISCH

IT-SICHERHEITSTAG

Praxisnahe Lösungen

Die Forschungsgruppe *Systemsicherheit (www.syssec.at)* der Alpen-Adria-Universität Klagenfurt unter der Leitung von Assoc. Prof. DI Dr. Peter Schartner veranstaltet jährlich den österreichischen IT-Sicherheitstag, abwechselnd in Klagenfurt und an der Fachhochschule Salzburg. An dieser fand am 14. November 2018 der 15. IT-Sicherheitstag mit 120 Teilnehmern statt. Bei den Sicherheitstagen, die unter dem Aspekt praxisnaher, wirtschaftlich vertretbarer Lösungen stehen, werden organisatorische, technische und rechtliche Aspekte der Informationstechnologie behandelt. Die Forschungsgruppe veranstaltet weiters die jährliche *D-A-CH-Security,* bei der auf wissenschaftlicher Ebene der aktuelle Stand der IT-Sicherheit in Deutschland, Österreich und der Schweiz erörtert wird. Der 16. IT-Sicherheitstag wird im Oktober 2019 in Klagenfurt stattfinden.

1148, die in Österreich durch das Netz- und Informationssicherheitsgesetz (NISG) umgesetzt wird, bestehen in der EU weitere Rechtsetzungsvorhaben betreffend die IT-Sicherheit, über die Dr. Wolfgang Feiel, *RTR GmbH (www.rtr.at),* berichtete. Das aus fünf Richtlinien bestehende Telekommunikationsrecht soll in einer Richtlinie, dem bereits ausverhandelten *Europäischen Kodex für elektronische Kommunikation (EECC)* zusammengefasst werden *(COM(2016) 590 final)*. Hingegen würden die Verhandlungen zu einer Verordnung betreffend den Schutz der Privatsphäre in der elektronischen Kommunikation *(E-Privacy-Verordnung; ePVO)* stocken; der Abschluss sei ungewiss.

15. IT-Sicherheitstag an der FH Salzburg: Experten referierten über organisatorische, technische und rechtliche Aspekte der IT-Sicherheit.

Datenschutzbeauftragter. Nach § 37 Abs. 1 DSGVO sind Datenschutzbeauftragte (DSBA) zu benennen, wenn die Datenverarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird; von Unternehmen nur dann, wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, deren Kerntätigkeit eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich macht oder diese Tätigkeit in der umfangreichen Verarbeitung sensibler Daten (Art. 9) oder von strafrechtlichen Verurteilungen und Straftaten (Art. 10) besteht. Außerhalb dieser Fälle kann ein Datenschutzbeauftragter freiwillig bestellt werden.

Der Datenschutzbeauftragte hat nach Art. 39 zumindest den Verantwortlichen oder Auftragsverarbeiter und die Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach den datenschutzrechtlichen Bestimmungen zu unterrichten und zu belehren. Er hat die Einhaltung dieser Bestimmungen zu überwachen, die an den Verarbeitungsvorgängen beteiligten Mitarbeiter zu schulen und mit der Aufsichtsbehörde zusammenzuarbeiten.

Jede Person, der wegen eines Verstoßes gegen die DSGVO ein Schaden entstanden ist, hat Anspruch auf Schadenersatz gegenüber den Verantwortlichen oder den Auftraggeber (Art. 82 Abs. 1). Der Schaden, der im Zivilrechtsweg geltend zu machen ist, kann in Geld messbar sein (materieller Schaden) oder als Schadenersatz für „nachteilige Gefühle“ (immaterieller Schaden). Ein solcher Schaden wird nur ausnahmsweise ersetzt, etwa im Fall von Schmerzengeld, oder eben bei Verletzung des Datenschutzes.

„Primärer Adressat der datenschutzrechtlichen Pflichten ist der Verantwortliche, also das Unternehmen“, erläuterte Univ.-Prof. Dr. Peter Mader, Universität Salzburg, zur Frage der Haftung des Datenschutzbeauftragten. Sanktionen wie Schadenersatz oder Geldbußen drohen daher dem Unternehmen und nicht direkt dem DSBA als (nur) „aktivem Berater“. Allerdings kann er nach allgemeinem Schadenersatzrecht haftbar werden, etwa bei eigenem Verstoß gegen Verschwiegenheitspflichten (Art. 38 Abs. 5) oder falscher Beratung des Unternehmens. Voraussetzung ist, dass der DSBA hierbei rechtswidrig und schuldhaft gehandelt hat. Inwieweit der DSBA im Wege des Regresses haftbar gemacht werden kann, weil vom Unternehmen einem verletzten Dritten gegenüber Schadenersatz geleistet werden musste, richtet sich danach, ob der DSBA Arbeitnehmer des Unternehmens (interner DSBA) oder diesem auf Vertragsbasis verpflichtet ist (externer DSBA; Art. 37 Abs. 6 DSGVO).

Ein interner DSBA ist hierbei nach § 4 DHG insofern privilegiert, als die Höhe der Regressforderung nach dem Grad des Verschuldens abgestuft wird. Wurde der Schaden durch ein Versehen zugefügt, kann das Gericht den Ersatzanspruch mäßigen oder, wenn der Schaden durch einen minderen Grad des Versehens zugefügt worden ist, ganz erlassen. Bei einer „entschuldbaren Fehlleistung“ hat der Dienstgeber gegenüber dem Dienstnehmer keinen Rückgriffsanspruch. Zu berücksichtigen sind dabei die besondere Verantwortung bei der Tätigkeit, deren „Schadensgeneigtheit“ und die Bedingungen der Dienstleistungserbringung.

Ein externer DSBA haftet aus dem Geschäftsbesorgungsvertrag. Ein „Haftungsprivileg“ kommt ihm nicht zu Gute. An ihn ist der erhöhte Sorgfaltsmaßstab eines „Sachverständigen“ zu legen. Unternehmen, die Aufgaben eines Datenschutzbeauftragten als Dienstleister übernehmen, rät Mader, in den Verträgen entsprechende Haftungs-Ausschlussklauseln (die Haftung für leichte Fahrlässigkeit kann ausgeschlossen werden) zu vereinbaren und eine Haftpflichtversicherung abzuschließen.

Kurt Hickisch

Fotos: Kurt Hickisch