FH Hagenberg: jährliche IKT-Sicherheitskonferenz „Security-Forum“

IT und Management

Das Security-Forum 2024 des Hagenbergerkreises bot eine Mischung aus Informationstechnik, Recht und praktischer Umsetzung.

Der Verein „Hagenberger Kreis zur Förderung der digitalen Sicherheit“ veranstaltete am 22. und 23. Mai 2024 in der Fachhochschule Hagenberg das Security-Forum, eine IKT-Sicherheitskonferenz. Diese findet seit 2003 jährlich statt. Der Verein setzt sich aus Studierenden und Absolventen des Studiengangs „Sichere Informationssysteme“ der Fachhochschule zusammen und hat sich zum Ziel gesetzt, das Sicherheitsbewusstsein im Hinblick auf die Informations- und Telekommunikationstechnik sowohl von Unternehmen als auch in privaten Haushalten zu stärken.

Der Verein veranstaltet auch Vorträge und Workshops an Schulen. Beim Security-Forum lag der Schwerpunkt auf den Bereichen Technik und Management. Bei den Vorträgen zu informationstechnischen Themen ging es etwa um den aktuellen Stand der Malware-Entwicklung (Tobias Wicke), automatisierte Phishing-Erkennung (Joachim Kerschbaumer) oder neue Wege in der Cryptoasset-Forensik zur Bekämpfung der Cyber-Kriminalität (Bernhard Haslhofer).

Datensicherheit. Die zehn besten Wege, Daten zu verlieren, zeigte Hannes Kasparik vom IT-Unternehmen *Veeam* auf. Wer denkt, dass Datensicherung nur etwas für Überbesorgte ist oder dass das der Cloud-Provider oder die benutzten Programme tun würden, der irrt sich. Sollte der Angreifer auch Zugriff auf Back-up-Daten haben, sind auch diese mitverschlüsselt, etwa im Fall eines Ransomware-Angriffs. Nicht nur derartige Angriffe können zu einem Desaster führen, sondern auch klassische Schadensereignisse wie etwa Hochwasser.

Wer sein Restore-System nicht testet und auf das bloße Back-up vertraut, läuft ebenfalls Gefahr, dass letztlich ein Wiederanlauf nicht gelingt. Den Zugriff auf verschiedene Systeme durch eine übergreifende Plattform zu automatisieren, birgt die Gefahr, dass mit einem Schlag alle erfassten Systeme ausgeschaltet werden. Die Datensicherung sollte, selbst, wenn das teuer ist und Speicherplatz kostet, nach der 3-2-1 Regel erfolgen, die besagt, dass drei Kopien angefertigt werden, zwei davon auf unterschiedlichen Medien. Das letzte Backup sollte unveränderbar ausgelagert werden, mit einem „Luftspalt“ *(air-gap)* zum übrigen System, sodass keine unmittelbare Beeinflussung mehr erfolgen kann. Darauf zu vertrauen, dass Daten zwar auf mehreren Laufwerken gespeichert werden, aber logisch als ein Laufwerk angesehen werden (RAID-System), kann ebenso zu Datenverlust führen wie das Vertrauen darauf, dass der Cloud-Provider keine Daten verliert. Sollte der Anbieter von Back-up-Software Schutz vor Ransomware versprechen, und würde solche entdeckt werden, ist es bereits zu spät.

Sicherheitsbewusstsein in der IT zu stärken, soll Spaß machen, meinte ein junges Team der *Raiffeisenbank International*. Dies könne in Form von monatlichen, zweistündigen Meetings zu einem Jour-Fix in entspannter Atmosphäre stattfinden. Mit Quiz-Formaten

Foto: Kurt Hickisch

oder Capture-the-Flag-Wettbewerben könnten die Teilnehmenden motiviert und mit Stickern ein Gruppenbewusstsein gebildet werden. Anhand eines Puppenhauses könnten Sicherheitsprobleme eines Smart-Homes erörtert werden.

Auf ebenso ungezwungene Weise befassten sich Eddy Willems (Belgien) und Righard Zwienenberg (Niederlande) mit dem Thema künstliche Intelligenz am Beispiel ChatGPT. Als Beginn des Dialogs zwischen Mensch und Computer sahen sie das von Joseph Weizenbaum 1966 am MIT entwickelte Programm *Eliza* an, das mithilfe eines strukturierten Wörterbuchs Anfragen beantwortete.

Large-Language-Models (LLM) entwickelten sich in der Folge rasch weiter bis zu Anwendungen wie ChatGPT und damit generierten Texten, beispielsweise für Kinderbücher. Gefährlich wird die Entwicklung, wenn persönliche Daten missbraucht oder Schadcodes entwickelt werden. Bilder, Videos und die Stimme können durch künstliche Intelligenz verfälscht und daraus neue Inhalte erzeugt werden. Sichtlich Freude bereitete den Vortragenden, die KI mit der Frage hinters Licht zu führen, wie die letzten zehn Ziffern der Zahl π lauten oder, eine bestimmte Uhrzeit auf einem Ziffernblatt und nicht digital darzustellen.

DSGVO. Rechtsanwalt Thomas Schweiger aus Linz berichtete über richtungweisende gerichtliche Entscheidungen zum Datenschutzrecht und deren Konsequenzen. Mit Urteil vom 5. Dezember 2023, C-807/21 („Deutsches Wohnen“) hat der EuGH entschieden, dass es für die Verhängung einer Geldbuße gegen eine juristische Person nicht erforderlich ist, eine natürliche Person zu identifizieren, die im Rahmen der unternehmerischen Tätigkeit und im Namen der juristischen Person gehandelt hat.

Für die Anwendung des Art. 83 DSGVO ist keine Handlung und nicht einmal eine Kenntnis über den Verstoß des Leitungsorgans erforderlich (Randziffer 77). Es genügt ein bei der juristischen Person festgestelltes Organisationsverschulden. Diese Rechtsauffassung wurde vom Verwaltungsgerichtshof, der ein bei ihm anhängiges Verfahren bis zu dieser Entscheidung ausgesetzt hatte, mit Erkenntnis

Security Forum: Referenten Robert Kolmhofer und Thomas Schweiger

vom 1. Februar 2024, Zl. Ra 2020/04/0187-20, übernommen, was zur Aufhebung einer Entscheidung des Bundesverwaltungsgerichts geführt hat. In Österreich sind eine Reihe von Verfahren gegen Großunternehmen mit Geldbußen in Millionenhöhe anhängig.

Im Urteil vom 4. Mai 2023, C-300/21 („Österreichische Post AG“) hat der EuGH zur Frage des Schadenersatzes (Art. 82 DSGVO) zum Ausdruck gebracht, dass eine Kausalität zwischen Verstoß und dem (materiellen oder immateriellen) Schaden erforderlich ist. Ein bloßer Verstoß gegen die DSGVO reicht für die Haftung nicht aus und es stellt auch nicht jede negative Folge eines solchen Verstoßes einen ersatzfähigen immateriellen Schaden dar.

Dem Sachverhalt zum Urteil des EuGH vom 14. Dezember 2023, C-340/21, liegt zugrunde, dass durch einen Hackerangriff auf eine bulgarische Behörde mehr als sechs Millionen Menschen betroffen waren. Der immaterielle Schaden wurde in der Befürchtung gesehen, dass die personenbezogenen, ohne Einwilligung veröffentlichten Daten künftig missbräuchlich verwendet würden oder dass die Person selbst erpresst, angegriffen oder sogar entführt würde. In dem vorliegenden Fall einer Auftragsverarbeitung trägt der Verantwortliche die Beweislast dafür, dass die von ihm getroffenen Sicherheitsmaßnahmen (technisch und organisatorisch, TOMs) im Sinn des Art. 32 DSGVO geeignet waren.

Die Konsequenz dieser Judikatur sei, so der Referent, dass, bei Vertragsbeziehungen nach dem Konsumentenschutzgesetz, Massenverfahren wegen Schadenersatz nicht auszuschließen wären und sich die Beweislast immer mehr zum Verantwortlichen verschiebe.

Whistleblowing. In Umsetzung der EU-RL 2019/1937 wurde in Österreich das Hinweisgeber/-innenschutzgesetz (HSchG, BGBl I Nr. 6/2023) erlassen, das seit 25. Februar 2023 in Kraft ist. Es betrifft Unternehmen und juristische Personen des öffentlichen Sektors mit jeweils 50 oder mehr Arbeitnehmer/-innen oder Bediensteten. Diese Normadressaten wurden verpflichtet, innerhalb von sechs Monaten ein internes Hinweisgebersystem einzurichten. Für Unternehmen und juristische Personen des öffentlichen Sektors mit weniger als 250 Arbeitnehmer/-innen bestand eine Übergangsfrist bis zum 17. Dezember 2023.

Nach Einschätzungen aus der Beraterpraxis hätten mehr als die Hälfte der in Betracht kommenden Unternehmen noch kein Hinweisgeber/-innensystem eingeführt und ungefähr zwei Drittel hätten kaum Informationsmaßnahmen gesetzt, berichtete Georg H. Jeitler von der Wirtschaftsprüfungs- und Steuerberatungsgesellschaft *Grant Thorton Austria*. Weniger als 10 Prozent hätten bisher ernsthafte Schulungsmaßnahmen durchgeführt.

Das Gesetz verlangt den Betrieb einer „internen Stelle“, an die sich der Hinweisgeber richten kann. Nach § 12 HSchG ist diese Stelle mit den zur Erfüllung ihrer Aufgaben notwendigen finanziellen und personellen Mitteln auszustatten, hat unparteilich und unvoreingenommen vorzugehen und es sind Vorkehrungen für eine unbefangene Entgegennahme und Behandlung von Hinweisen zu treffen. Die Einrichtung einer bloßen Website reicht nicht aus und es könnte sich eine Auslagerung dieser internen Stelle vielfach als sinnvoll erweisen, sagte der Referent.

Es fehle oft das Verständnis für den (beiderseitigen) Wert einer Hinweisgeberkultur. Durch die richtige Gestaltung des Systems könne eine Verbesserungskultur geschaffen werden. Eine gelebte Fehler- und Feedbackkultur würde Potenzial freilegen und könnte durch Belohnungen (Bounty-Programme) besondere Anreize bieten. Allerdings sollte individuelles Fehlverhalten nicht in Hinweise zur Person münden, weil dann die Gefahr bestehe, dass das Hinweisgebersystem als „Vernaderungssystem“ angesehen werde. Vielmehr sollte in kollegialem Feedback Bewusstsein für

FOTO: KURT HICKISCH

Audi-Max der FH Hagenberg: Das Security-Forum des „Hagenberger Kreises zur Förderung der digitalen Sicherheit“ findet seit 2003 jährlich statt

Arbeitssicherheit geschaffen werden. Das Hinweisgebersystem solle als Korrektiv wirken. In der Praxis stelle es eine Herausforderung dar, die Vertraulichkeit der Identität des Hinweisgebers sowie betroffener Personen auch intern zu wahren und den Zugriff unbefugter Personen auszuschließen, was entsprechendes IT-Management erforderlich mache.

Klein- und Mittelbetriebe, die oft keine eigene Compliance-Struktur aufweisen, stünden vor dem Problem, dass sich Interessenskonflikte ergeben. Relevante Meldungen würden durch Betriebsblindheit, soziale Erwünschtheit oder Gruppendruck falsch eingeordnet. Die Geheimhaltung sei schwierig oder die Rolle eines internen Ermittlers führe zu sozialen Verwerfungen. Im Einzelfall können sich hinsichtlich eingelangter Hinweise Probleme durch große Komplexität ergeben. Fragen der Glaubwürdigkeit und der Verlässlichkeit der Quelle, wie schwerwiegend die Vorwürfe sind, wie dringlich die Behandlung ist – etwa, weil die Sicherheit von Produkten oder Mitarbeiter gefährdet ist oder flüchtige Beweise vorab gesichert werden müssen. Bei Kernthemen sei mit ungefähr ein bis zwei Fällen pro Jahr je 100 Beschäftigten zu rechnen, bei ausgeweiteten Themenfelder ein Mehrfaches davon.

Normen. Robert Kolmhofer, Leiter des Departments Sichere Informationssysteme an der FH OÖ, Standort Hagenberg, gab einen Überblick über den Cyber Resilience Act (CRA) der EU, der vom EU-Parlament bereits im März 2024 formal verabschiedet wurde und noch formell vom Rat angenommen werden muss, bis eine Verlautbarung im Amtsblatt der Europäischen Union erfolgen kann. Bisher ist diese Veröffentlichung noch nicht erfolgt. Ab dieser müssen nach 21 Monaten Vulnerabilities (Schwachstellen) und Cyberincidents (Cyberangriffe) von den Herstellern gemeldet und nach 24 Monaten Security-Anforderungen in den Produkten implementiert sein. Nach 36 Monaten muss die Verordnung vollinhaltlich umgesetzt sein. Sie betrifft die Hersteller, Importeure und Vertreiber von Produkten mit digitalen Elementen. Ziel dieser Verordnung ist es, durch technische und organisatorische Maßnahmen die Cybersecurity von Produkten mit digitalen Elementen (Hard- und Software), die eine Datenverbindung aufweisen (vernetzte Produkte), zu verbessern. Es müssen ausreichende Updates gegen Schwachstellen zur Verfügung gestellt und Informationen für Anwender hinsichtlich ausreichender Cybersecurity von Produkten und deren sicheren Einsatz verbessert werden.

Die Liste der betroffenen Produkte ist lang und nicht abschließend definiert. Sie umfasst unter anderem Smartphones, Tablets, Computer, industrielle Steuerungssysteme, Geräte des Internet of Things, Wearables, Software, Spielkonsolen, Smart Vehicles, medizinische Geräte und Microcontroller. Bei etwa 90 Prozent aller Produkte wird eine Selbsteinschätzung ausreichen. Der Rest wird entweder eine Standardanwendung betreffen (Klasse I) oder bedarf einer Auditierung durch Externe (Klasse II).

Kurt Hickisch

securityforum.at, hagenbergerkreis.at

FOTO: KURT HICKISCH