Siegerehrung Cybersecurity-Competition: Landeshauptmannstellvertreterin Gaby Schaunig überreichte Preise und Urkunden an die drei besten Teams

Cyber-Sicherheit für Unternehmen

Beim Cybersecurity-Day im Lakeside Park Klagenfurt wurden die neuesten Entwicklungen, Bedrohungen und Lösungsansätze in der Cyber-Sicherheit diskutiert und die Gewinner der Cybersecurity-Competition geehrt.

Zum zweiten Mal fand am 13. November 2024 im Lakeside Park in Klagenfurt der Cybersecurity-Day statt. Die Veranstaltung wurde von der Wirtschaftskammer Kärnten, der Universität Klagenfurt und dem Lakeside Park, unterstützt vom Kompetenznetzwerk DIH Süd, ausgerichtet. Verantwortlich für die Programmgestaltung war Universitätsprofessor Peter Schartner von der Alpen Adria Universität Klagenfurt.

Dem Motto „24 Stunden Cybersecurity“ folgend, gab es am Vortag eine Cybersecurity-Night, verbunden mit einer erstmals durchgeführten Cybersecurity-Competition, bei der 17 Teams, bestehend aus 60 Schülerinnen, Schülern und Studierenden mit modernsten Tools an der Analyse und Abwehr von Cyber-Bedrohungen arbeiteten. Die Siegerehrung erfolgte im Rahmen der Tagung, wobei die Preise und Urkunden für die drei besten Teams von Landeshauptmannstellvertreterin Gaby Schaunig überreicht wurden.

FOTO: KURT HICKISCH

Malware historisch. Den Beginn der Malware-Entwicklung setzte Markus Leeb von der Alpen-Adria-Universität mit dem Morris-Worm aus 1988 an, der, programmiert vom amerikanischen Informatiker Robert T. Morris, Rechner im MIT infizierte und Systemausfälle verursachte. Der Michelangelo-Virus wurde am 6. März 1992 ausgelöst und erlangte mediale Aufmerksamkeit. Tag und Monat stimmten mit dem Geburtstag Michelangelos überein, daher die Bezeichnung.

Der Melissa-Virus von 1999 war einer der ersten Makroviren. Er versendete sich selbst an die ersten 50 Kontakte in der Adressenliste des Benutzers mit einer Liste pornografischer Websites. Der Programmierer David Lee Smith wurde in den USA zu 20 Monaten Haft und 5.000 Dollar Strafe verurteilt.

Der Love-Letter-Wurm von 2000 war ebenfalls ein Makrovirus, der sich wie ein Kettenbrief selbstständig an alle Kontakte im Adressbuch des Outlooks verschickte und in verschiedenen Dateien und Verzeichnissen duplizierte. Der auf den Philippinen lebende Urheber des Wurms, der Informatikstudent Onel de Guzman, ging straffrei aus, weil es auf den Philippinen keinen entsprechenden Straftatbestand gab.

Die Hackergruppe 29A, die in Russland/Tschechien vermutet wurde, startete am 25. Jänner 2003 und nutzte Schwachstellen (Buffer-Overflows) aus, die sechs Monate zuvor von Microsoft gepatcht worden waren. In den ersten 30 Minuten erfolgten 75.000 Infektionen, insgesamt etwa 250.000.

Der im Jänner 2007 aufgetretene Virus Storm verbreitete sich über E-Mails und führte zum Blockieren von Rechnern durch Überlastung (DDoS-Angriffe). Die Zahlen über die infizierten Rechner schwanken zwischen einer und 50 Millionen.

Vorläufer der nunmehr gängigen Ransomware-Angriffe war der 1989 aufgetretene AIDS-Trojaner, der, als angebliche Information über AIDS, per Post auf 5,25 Zoll-Disketten verschickt wurde und sich bei Aufruf installierte. Die Namen von Dateien wurden ver-

Cybersecurity-Day: Experten präsentierten künftige Trends, rechtliche Aspekte von KI, sichere Softwareentwicklung und Penetrationstests

schlüsselt. Durch Überweisung von 189 Dollar an ein Postfach in Panama konnten Anweisungen zum Wiederherstellen der Dateien erhalten werden.

Der nunmehrige Einsatz künstlicher Intelligenz wird, so Leeb, zu einer Automatisierung und Optimierung von Schadcodes führen. Polymorphe, sich selbstständig verändernde Malware wird die Aufdeckung erschweren. Maschinelles Lernen wird zu gezielteren Angriffen führen. Social-Engineering wird mithilfe von Deepfakes erleichtert werden.

Innentäter. Durch einen Innentäter kann es, wie Dominik Mocher vom NTS Netzwerk der Telekom Service AG aufzeigte, zur Veröffentlichung sensibler Unternehmensdaten kommen, und damit einhergehend zu Imageschäden, oft verbunden mit finanziellen und rechtlichen Konsequenzen. Cyber-Versicherungen helfen in solchen Fällen nur eingeschränkt. Innentäter können auch Türöffner für Angriffe auf die Lieferketten sein.

Zu prüfen ist, ob die Security Awareness im Unternehmen ausreichend verankert ist und es einen Prozess zur präventiven Erkennung von Fehlkonfigurationen gibt. Es stellt sich zudem die Frage, ob die Sichtbarkeit relevanter Ereignisse gewährleistet ist und ein Angriff automatisiert unterbunden werden kann.

Über die Anforderungen, die aus dem Blickwinkel des mittlerweile in Kraft getretenen, ab 11.12. 2027 geltenden Cyber Resilience Act (CRA) der EU (VO 2024/2847) auf die Software-Entwicklung zukommen, berichtete Stefan Jakoubi von SBA Research. Eine Darstellung des Inhalts der Verordnung findet sich im Magazin „Öffentliche Sicherheit“ Nr. 9-10/24, Seite 107.

NIS-2 und Lieferketten. Die Netz- und Informationssicherheitsrichtlinie 2 der EU ist eine Weiterentwicklung der ursprünglichen NIS-Richtlinie, die seit 2016 europaweit gilt. NIS-2 verlangt von Unternehmen, nicht nur im eigenen Bereich technische und organisatorische Sicherheitsmaßnahmen (TOMs) zu etablieren sowie Cyber-Bedrohungen zu identifizieren, sondern auch die Lieferketten bei der Bewertung von Sicherheitsrisiken zu berücksichtigen. Die von Lieferanten ausgehenden Risiken müssen bereits im Beschaffungsprozess evaluiert werden (Business Impact Analyse – BIA), erläuterte Lukas Kulmitzer von der Eurofunk Kappacher GmbH.

Es ist zu ermitteln, ob das Lieferunternehmen Zugriff auf sensible Informationen oder auf die System- bzw. Netzwerkinfrastruktur hat; physischer Zutritt zu kritischen Geschäftsbereichen möglich ist; prozessuale Abhängigkeiten vom Lieferanten bestehen; welche Auswirkungen ein Ausfall auf Kunden hat und inwieweit der Lieferant ersetzbar ist. Empfohlen wird, sich in Verträgen entsprechend abzusichern und sich Auditrechte zusichern zu lassen, samt laufendem Monitoring.

Cyber Incident Response. Das 2008 gegründete CERT.at (Cyber Emergency Response Team) ist, wie Wolfgang Rosenkranz, der Geschäftsführer des Unternehmens, ausführte, das offizielle nationale Computernotfallteam nach dem NIS-Gesetz. Die Hauptfunktion ist die einer Drehscheibe für cyberkritische Informationen im Netzwerk mit anderen nationalen CERTs. CERT.at ist nicht die Feuerwehr für Unternehmen, die von einem Angriff auf ein Computersystem betroffen sind. Diese werden an entsprechende Dienstleister verwiesen. Incident Response muss strategisch vorbereitet sein, vom Training über aktuelle Listen bis zu Ausweicharbeitsplätzen. Zu fragen sei, ob man nach einer Risikoanalyse mit eigenem Personal auskommen kann oder ein professioneller Dienstleister beauftragt werden muss. Sollte ein Unternehmen den aktuellen Cybersecurity-Vorgaben (NIS-2, DORA, etc) nicht nachkommen können, müsste das Geschäftsmodell überdacht werden.

Auf nationaler Ebene sind BKA, BMI, BMLV und BMEIA für die Cyber-Sicherheit zuständig und bilden den Inneren Kreis der Operativen Koordinierungsstruktur (IKDOK), unterstützt von der Operativen Koordinierungsstruktur (OpKoord). Einen Ressourcenpool bildet die Polizei, die, wie Rosenkranz hervorhob, eine Ausbildungsoffensive gestartet hat. Über einen weiteren Pool von eigenen Cyber-Kräften verfügt das Bundesheer, vor allem auch durch die Miliz, in der sich entsprechende Experten befinden. „Die Verteidiger sind immer noch mehr als die Angreifer“, sagte Rosenkranz.

Künstliche Intelligenz. Seit 1. August 2024 ist die KI-Verordnung der EU (auch: AI-Act), VO (EU) 2024/1689, in Kraft, berichtete Sonja Janisch von der Universität Salzburg. Grundsätzlich ist die Verordnung ab 2. August 2026 anzuwenden, die Verpflichtung zur KI-Kompetenz (Awareness schaffen; Art 4) und das Verbot des Anbietens/Nutzens von verbotenen Praktiken (Art 5) jedoch bereits seit 2. Februar 2025. Die KI-VO hat das Ziel, einen einheitlichen Rechtsrahmen für die Entwicklung, das Inverkehrbringen, die Inbetriebnahme und die Verwendung von KI unter Gewährleistung von Gesundheit, Sicherheit und Grundrechten herzustellen. Sie verfolgt einen risikobasierten Ansatz, von unannehmbarem über hohes, begrenztes bis

FOTO: LAKESIDE PARK

Vortragende beim Cybersecurity-Day: Christian Inzko, Markus Leeb, Peter Schartner, Sonja Janisch, Wolfgang Rosenkranz

zu minimalem Risiko. Die VO betrifft insbesondere Anbieter und Betreiber. Sie enthalte, so Janisch, nur wenige innovationsfördernde Maßnahmen, sondern hauptsächlich Verbots- und Produktsicherheitsvorschriften für KI. Nicht geregelt sind beispielsweise Haftungsfragen, die teilweise in der mittlerweile am 8. Dezember 2024 in Kraft getretenen Produkthaftungs-RL der EU (RL 2014/ 2853) ihre Regelung gefunden haben. Diese RL muss von den Mitgliedstaaten bis 9. Dezember 2026 umgesetzt werden.

Unberührt bleibt durch die KI-VO die DSGVO (Art 2 Abs 7 KI-VO). Die KI-VO erweitert urheberrechtliche Haftungsrisiken, unter anderem wegen der Verpflichtung zur Erstellung einer EU-Urheberrechtsstrategie für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck, bei deren schuldhafter Verletzung Geldbußen zusätzlich zu den Ansprüchen nach dem Urheberrechtsgesetz (UrhG) drohen. Die Geldbußen können bis zu 15 Millionen Euro oder drei Prozent des weltweiten Jahresumsatzes vom vorangegangenen Geschäftsjahr betragen, je nachdem, welcher Betrag höher ist (Art 101 KI-VO).

Urheberrechtlich ist, so Janisch, KI-generierter Output im Regelfall nicht geschützt, weil keine eigentümliche geistige Schöpfung eines Menschen vorliegt. Der KI-Anbieter ist kein Urheber und auch ist die KI weder Urheber noch Erfinder im Sinn des Patentgesetzes.

Der KI-generierte Output genießt keinen urheberrechtlichen Schutz, weil in der Regel keine ausreichende menschliche Bestimmung vorliegt. So darf die Maschine nur ein Hilfsmittel sein. Werden die Anweisungen jedoch immer weiter verfeinert, sodass letztlich im Ergebnis eine eigentümliche geistige Leistung zu sehen ist, kann das urheberrechtlich wieder von Relevanz sein (Urteil des Beijing Internet Court).

Wenngleich KI-generierter Output in den meisten Fällen frei nutzbar ist, kann eine Urheberrechtsverletzung vorliegen, wenn der Output urheberrechtlich geschützte Elemente enthält und in ein dem Urheber vorbehaltenes Verwertungsrecht eingegriffen wird. Der Nutzer haftet dann bei Veröffentlichung für etwaige Urheberrechtsverletzungen. Trainingsdaten wie Texte, Fotos, Videos können urheberrechtlich geschützt sein, wobei das Training selbst eine urheberrechtliche Nutzungshandlung (Vervielfältigung; § 15 UrhG) darstellt. Die Vervielfältigung von rechtmäßig zugänglichen Werken für Text- und Data-Mining ist als freie Werknutzung nach § 42h Abs 6 UrhG zulässig, außer, es wäre ein Nutzungsvorbehalt mit maschinenlesbaren Mitteln erklärt worden („Opt-out“).

Die Verpflichtung zur Einhaltung des EU-Urheberrechts besteht auch für ein Training außerhalb der EU (ErwGr 106 der KI-VO). Andernfalls wird Art 53 KI-VO verletzt, wenn das KI-Modell in der EU in Verkehr gebracht wird. Bei in Drittstaaten trainierter KI sollte man Vorsicht walten lassen, riet Janisch für die Praxis. IT-generierter Output sollte nicht ungeprüft übernommen werden. Diesen mit einer individuell eigenartigen Leistung eines Menschen zu ergänzen, kann Urheberrechtsschutz bewirken. Wer als Rechteinhaber nicht will, dass seine Inhalte als Trainingsdaten verwendet werden, kann dem widersprechen. Zu überlegen ist die Aufnahme von KI-Klauseln in Verträgen mit Arbeitnehmern oder Kunden.

Überhaupt sollte man sich rechtzeitig mit den Regelungen der KI-VO befassen und, verpflichtend seit 2. Februar 2025 (Art 4), Awareness schaffen. Zu empfehlen sind weiters eine Bestandsaufnahme der im Unternehmen verwendeten KI; deren Einstufung nach dem jeweiligen Risiko; eine Evaluierung der sich aus der VO ergebenden Verpflichtungen und Bestimmung von verantwortlichen Personen für die umzusetzenden Maßnahmen.

KI in der Verwaltung. Das Amt der Kärntner Landesregierung plant 2025 den Einsatz von generativer KI in der Verwaltung zur internen Nutzung, berichtete Christian Inzko von dieser Behörde. Das in Aussicht genommene System wird aus Sicherheitsgründen auf eigener Hardware gehostet und ohne Verbindung zum Internet betrieben (on-premise). Damit ist auch ein höheres Maß an Vertraulichkeit und Datenschutz gegeben und trotz anfänglich höherer Kosten wird langfristig eine Kostenersparnis gegenüber dem Abonnement kommerzieller Produkte erreicht. Bis Ende 2024 läuft das Einlesen landes- und fachspezifischer Informationen. Mit Beginn 2025 soll der praktische Einsatz erfolgen. „Kärnten GPT“ befindet sich derzeit im Live-Betrieb. Häufig wiederkehrende telefonische Anfragen sollen mit Hilfe von Sprachassistenten in Text umgewandelt und die generierten Antworten wiederum in Sprache ausgegeben werden. Das Problem dabei sind Dialekte sowie, dass Slowenisch und Italienisch berücksichtigt werden müssen. Im Förderungswesen soll die KI Dokumente und maschinenlesbare Rechnungsbelege erkennen und unmittelbar verarbeiten, sodass den Sachbearbeiter nur mehr maschinell nicht bearbeitbare Belege erreichen. Als Hilfe im Gesetzgebungsverfahren kann die KI-Texte vergleichen und Unterschiede ermitteln.

Smart Metering. Smart Meter sind intelligente Messgeräte, die in ein Kommunikationssystem eingebunden sind. Fragen, die sich insbesondere beim Einsatz intelligenter Stromzähler ergeben, sind die Gefahr eines Blackouts durch einen Hacker-Angriff; dass Daten missbräuchlich verwendet werden könnten („Gläserner Mensch“) oder Rückschlüsse auf Lebensgewohnheiten gemacht werden könnten. Hierzu berichtete Heinz Sitter, Leiter IT Business Solutions der Kärntner Elektrizitäts AG, über sicherheitstechnische Erkenntnisse nach zehnjährigem Betrieb eines solchen Systems und schilderte die Vorkehrungen, die zur Abwehr dieser Gefahren getroffen wurden.

Als Aussteller waren an Bildungseinrichtungen neben der Universität Klagenfurt mit ihrem Studienangebot und Joanneum Research auch der Digital Information Hub (DIH) Süd vertreten, der, als Service für Klein- und Mittelbetriebe, Informationsworkshops und Qualifizierungskurse anbietet.

Der Cybersecurity-Day 2025 ist für Mitte November 2025 bereits in Vorbereitung. *Kurt Hickisch*

FOTOS: KURT HICKISCH