Cyber-Crime-Forum: Thomas Goiser, Theresa Philippi, Peter Gridling, Philipp Nauschnegg

Digitale Resilienz stärken

Cyber-Angriffe stehen zunehmend im Zusammenhang mit geopolitischen Entwicklungen. Künstliche Intelligenz eröffnet Angreifern neue Möglichkeiten und bietet zugleich Chancen für den Schutz digitaler Systeme.

Künstliche Intelligenz, die Schwachstelle Mensch und neue Schutzmaßnahmen standen im Mittelpunkt des von *LSZ – Future Connections* veranstalteten Cyber-Crime-Forums am 23. Juni 2026 in Wien. Den Auftakt machte die „nächste Generation" der IT-Sicherheit: Schülerinnen und Schüler der HTL Spengergasse präsentierten Projekte aus dem Wahlfach „Ethical Hacking". Sie zeigten sich überzeugt, dass künstliche Intelligenz zwar neue Bedrohungen schaffe, aber das Potenzial besitze, digitale Systeme sicherer zu machen.

Neue Bedrohungen. Cyber-Angriffe stehen zunehmend im Zusammenhang mit geopolitischen Entwicklungen und globalen Lieferketten, betonte Hans Irlacher, Senior Account-Director bei *Recorded Future*. Kriminelle nutzen künstliche Intelligenz, um Phishing-Mails professioneller zu gestalten, und tauschen sich in Darknet-Foren über potenzielle Ziele aus. Häufig dienen unzureichend geschützte Zulieferer als Einfallstor. Irlacher verwies auf eine *KPMG*-Studie, wonach nahezu alle österreichischen Unternehmen innerhalb eines Jahres Ziel von Cyber-Angriffen werden; sieben Prozent der Angriffe sind erfolgreich.

Auch für Unternehmen verändert KI die Sicherheitslage. Clive Finley, Field CTO EMEA, betonte die wachsende Bedeutung von KI für die Cyber-Sicherheit. Laut *Global Cybersecurity Outlook* des Weltwirtschaftsforums sehen 94 Prozent der Befragten KI als wichtigste Entwicklung der kommenden zwölf Monate. Unternehmen müssten den Einsatz von KI-Anwendungen steuern und ihre Sicherheitsstandards verbessern. Dennoch verfügen 34 Prozent über kein Security-Protokoll und 72 Prozent über kein formales Security-Awareness-Training.

Sebastian Schrittwieser, Senior Scientist an der Universität Wien, warnte vor den Risiken durch KI-Agenten. Diese können eigenständig Aufgaben ausführen und auf Daten sowie externe Dienste zugreifen, erkennen manipulierte Inhalte jedoch nicht zuverlässig. Deshalb seien eingeschränkte Berechtigungen und wirksame Sicherheitsmaßnahmen unverzichtbar.

Cyber-Angriffe. Kein Computersystem sei vor Angriffen geschützt, betonte Matthias Träger, Regional Central-Europe-Sales-Director von *HPE Zerto Software*. Das größte Risiko bleibe der Mensch. Ein Back-up reiche oft nicht aus, da Sicherungen in zu großen Zeitabständen erfolgen oder selbst von Schadsoftware verschlüsselt werden können. Eine kontinuierliche Analyse der Datenströme und Wiederherstellungspunkte im Sekundentakt reduzierten den Datenverlust im Ernstfall auf ein Minimum.

Wie gravierend die Folgen eines Ransomware-Angriffs sein können, zeigte Philipp Nauschnegg, Geschäftsführer des Versicherungsunternehmens *Cyber & Crime*, anhand eines Falles. Als die Attacke entdeckt wurde, waren sämtliche Daten – einschließlich der Backups – verschlüsselt. Da das geforderte Lösegeld von 400.000 Euro nicht bezahlt wurde, entschied sich der Betrieb für den Neuaufbau seiner IT-Infrastruktur. „Hacker verlangen meist drei bis sechs Prozent des Jahresumsatzes als Lösegeld", sagte Nauschnegg.

In interaktiven Sessions diskutierten

Foto: LSZ/Jenia Symonds de Montfort

die Teilnehmer mit den Referenten über Herausforderungen der Cyber-Sicherheit – vom Schutz sensibler Daten bis zur Wiederherstellung von IT-Systemen nach einem Cyber-Angriff.

EU-Recht. Rechtsanwältin Katharina Raabe-Stuppnig gab einen Überblick über die wichtigsten EU-Rechtsvorschriften zur Cybersicherheit und zum Datenschutz. Zu den zentralen Regelwerken zählen neben der DSGVO die NIS-2-Richtlinie, der Cyber-Resilience-Act (CRA), der AI-Act und der Data-Act. Während NIS-2 die Cybersicherheit betroffener Einrichtungen und ihrer Lieferketten stärkt, legt der CRA Sicherheitsanforderungen für digitale Produkte fest. Der AI-Act regelt den Einsatz künstlicher Intelligenz, der Data-Act den Zugang zu Industriedaten.

Schutz von Wissen. In einer von Thomas Goiser vom *Austrian Center for Intelligence, Propaganda and Security-Studies (ACIPSS)* moderierten Podiumsdiskussion diskutierten Experten über Wirtschafts- und Wissenschaftsspionage sowie den Schutz des Know-hows österreichischer Universitäten und Unternehmen.

Peter Gridling, Präsident der Gesellschaft für Technologie- und Wissensschutz und ehemaliger Direktor des BVT, erläuterte, wie Wissenschaftsspione über Studierende, Gastwissenschafter oder Forschungskooperationen Zugang zu wissenschaftlichem Know-how erhielten. Ebenso würden Forschende anderer Staaten diskreditiert, um den Einfluss eigener Wissenschaftler zu stärken.

Wie Hochschulen ihr Wissen schützen, erläuterte Theresa Philippi, Leiterin der Abteilung Compliance & Recht sowie Datenschutzbeauftragte der Fachhochschule Technikum Wien: „Wir schicken niemanden mit einem Laptop voller Daten in gewisse Länder. Wenn eine Person aus einem dieser Länder zu uns kommt, holen wir Informationen über sie ein." Zudem überprüft die Fachhochschule bei Bedarf Ausbildungsnachweise und sensibilisiert ihre Mitarbeiter für Anzeichen möglicher Wissenschaftsspionage.

Dass Sicherheitslücken oft an unerwarteter Stelle entstehen, zeigte Berufsdetektiv Alexander Datzer anhand eines Falls. In einem Softwareunternehmen gelangten sensible Informationen nicht über eigene Mitarbeiter, sondern über eine Beschäftigte eines externen Reinigungsunternehmens nach außen. Eine einmalige Sicherheitsüberprüfung garantiere die Integrität von Mitarbeitern nicht dauerhaft, betonte Datzer.

Songcontest. Zum Abschluss gaben Jörg Scheiblhofer, CISO des *ORF*, und Martin Pils, Geschäftsführer von *PILS Cyber-Defence* und Head of Cybersecurity-Operations des Eurovision Song Contests 2026, Einblicke in das Cybersecurity-Konzept. „Wir haben gewusst, dass wir angegriffen werden", sagte Pils. Als Frühwarnsystem dienten OSINT-Recherchen und Darknet-Monitoring; über *CERT.at* flossen zudem Informationen internationaler CERT-Organisationen ein. Entscheidend sei die enge Zusammenarbeit mit den Sicherheitsbehörden gewesen: Während der Show-Woche koordinierte ein Cyberlagezentrum die Maßnahmen gemeinsam mit dem Bundesministerium für Inneres und der Landespolizeidirektion Wien. *Rosemarie Pexa*