Martin Szelgrad (Report Verlag), Peter Oros (Qualysoft-Gruppe), Helmut Leopold (AIT), Josef Pichlmayr (Ikarus), Markus Robin (SEC Consult), Matthias Tischlinger (Energie AG OÖ Telekom), Thomas Hoffmann (RadarServices Smart IT-Security GmbH).

Marketing und Forschung

Über die internationale Rolle österreichischer Cybersecurity-Unternehmen diskutierten Fachleute bei der dritten AIT-Technologieausstellung „Sehen und Verstehen – Cybersecurity".

Cybersecurity-Technologien aus Österreich genießen international vielfach hohes Ansehen, sie werden aber im eigenen Land kaum wahrgenommen. „Wir brauchen Exportunterstützung durch die Spitzenpolitik, aber auch eine größere Selbstvermarktung. Denn durch die immer komplexere Vernetzung wird Cybersecurity zur wichtigsten Herausforderung im privaten und beruflichen Umfeld", sagte Peter Oros, Geschäftsführer der *Qualysoft-Gruppe,* bei einer Podiumsdiskussion anlässlich der Technologieausstellung „Sehen und verstehen – Cyber Security" des *Austrian Institutes of Technology (AIT)* am 30. Mai 2017 in Wien. „Für österreichische IT-Firmen ist das nicht nur eine Herausforderung, sondern auch eine Chance, sich mit ihren Security-Lösungen auf dem Weltmarkt zu etablieren", betonte Oros, dessen Unternehmen mit E-Government- und Cloud-Security-Lösungen in Europa und Asien erfolgreich ist.

„Spitzentechnologie alleine ist nicht entscheidend. Für die internationale Aufstellung braucht es auch Marketing und die Unterstützung österreichischer Behörden", sagte Thomas Hoffmann, Geschäftsführer der *Radar Services Smart IT Security GmbH*.

Josef Pichlmayr, Geschäftsführer der *Ikarus Security Software GmbH* wies darauf hin, dass „noch immer die kritische Masse an Bewusstsein für Cybersecurity" fehle. Bei der *SEC Consult Unternehmensberatung GmbH* sind etwa 80 „White-Hat-Hacker" beschäftigt, um Kunden bei der Aufdeckung von Cybersecurity-Schwachstellen zu helfen. General Manager Markus Robin forderte „bessere Rahmenbedingungen und höhere Investitionsvolumina für die Umsetzung von Cybersecurity in Österreich und eine bessere Vorbereitung auf die im nächsten Jahr in Kraft tretende Datenschutz-Grundverordnung (DSGVO) bzw. die Umsetzung der NIS-Richtlinie in nationales Recht".

Matthias Tischlinger, Leiter der Abteilung Data Services der *Energie AG Oberösterreich Telekom GmbH,* verwies auf die Bedeutung von Cybersecurity gerade für kritische Infrastrukturen wie Smart Grid. Sein Unternehmen arbeite eng mit dem AIT und anderen Forschungseinrichtungen zusammen. „Massenmarktsysteme haben Sicherheitslücken, daher sind Offenheit gegenüber Bedrohungen und ein Threat-Information-Sharing zwischen den betroffenen Unternehmen eine wichtige Voraussetzung für eine sichere Energie-Zukunft", sagte Tischlinger.

Stärkere Vernetzung. „Österreichische Hightech-Unternehmen brauchen sich weltweit nicht zu verstecken. Das akademische Know-how und die Ingenieur-Skills sind da, Österreich ist Weltspitze. Gegen den Ur-Reflex, große internationale Marken zu kaufen, hilft nur ein größeres Selbstbewusstsein", sagte Helmut Leopold, Leiter des Centers für *Digital Safety* und *Security* am AIT. Die Schwierigkeit sei, dass die Forschung die Entwicklungen antizipieren müsse. Man benötige „mehr Mut", um für künftige Herausforderungen mit neuen Lösungsansätzen der Software-Entwicklung gewappnet zu sein und damit echte Marktplätze schaffen zu können, betonte Leopold. Nötig sei eine noch stärkere Vernetzung der innovationsstarken Unternehmen mit der Forschung, waren sich die Teilnehmer der Podiumsdiskussion einig.

Foto: AIT/Milena Krobath