IT-Sicherheit beginnt mit Wissen

Ein Wettrennen zwischen „Hase und Igel“

| IM GESPRÄCH | **Die Digitalisierung bietet neue Angriffspunkte und ist eine Gefahr für die Innovationskraft des Landes, urteilte die Expertenkommission Forschung und Innovation (EFI) Anfang des Jahres. Der EFI-Vorsitzende ordnet im Gespräch die Empfehlungen des Gutachtens ein und erweitert sie mit Blick auf die Hochschulen.**

Forschung & Lehre: Herr Professor Cantner, einer der Schwerpunkte des EFI-Jahresgutachtens 2020 war die Cybersicherheit. Darin fordern Sie, Forschung stärker zu schützen. Warum?

Uwe Cantner: Trotz andauernder Brisanz des Themas gibt es über IT-Sicherheit kaum repräsentative Erhebungen. Wir haben daher selbst eine Umfrage bei deutschen Unternehmen gestartet, die zeigt, dass Cyberangriffe einen hohen negativen Einfluss auf deren Forschungs- und Innovationskraft haben. Bei Hochschulen verhält es sich ähnlich, wie die prominenten Cyberangriffe auf die Universitäten in Gießen und Bochum gezeigt haben, die nach Abschluss des Gutachtens erfolgten.

Uwe Cantner *ist Vorsitzender der Expertenkommission Forschung und Innovation (EFI) und Wirtschaftsprofessor an der Universität Jena.*

F&L: Wie können Forschung und Hochschulen sicherer gestaltet werden?

Uwe Cantner: Generell über mehr Studiengänge, die Studierende umfassend zu technischen, ökonomischen, ethischen und juristischen Aspekten der Cybersicherheit ausbilden. Über Fachkompetenzen können an Hochschulen innovative Lösungen in der IT-Sicherheit entstehen. Dazu muss auch die Forschung weiter gefördert werden. Hochschulen sind zudem selbst schutzbedürftig, wie die jüngsten Angriffe gezeigt haben. In Deutschland weiß das Hochschulpersonal zu wenig über IT-Sicherheit Bescheid, weil es kaum Schulungen zum Umgang mit Angriffen gibt. Da sollte Abhilfe geschaffen werden, evtl. auch mit verpflichtenden Schulungen. Auf technischer Seite sollten Hochschulen eine möglichst geringe Angriffsfläche bieten, indem die Systeme gespiegelt oder fraktioniert werden und so im Schadensfall entkoppelt werden können. Daten könnten vermehrt auf ausgelagerten Servern unterschiedlicher Anbieter gespeichert werden. Auch an gut aufgesetzten Störmeldungssystemen mangelt es den Hochschulen.

F&L: Können bislang nicht betroffene Hochschulen von Betroffenen lernen?

Uwe Cantner: Angriffsstrategien sind oft hochkreativ und ändern sich laufend. Dennoch kann man grundsätzlich gut von anderen lernen. Gemeinsame technische Schutzsysteme über eine vernetzte IT-Infrastruktur sind dabei nur sinnvoll, wenn diese im Angriffs- und Schadensfall auch entkoppelt werden können. Ein System, das jede Attacke abwehren kann, wird es aber nie geben. IT-Sicherheit ist immer auch ein Wettrennen zwischen „Hase und Igel“. Um in diesem Rennen bestehen zu können, benötigen Hochschulen – wie auch Unternehmen – aktuelle Informationen über Cyberangriffe. Die EFI hat daher vorgeschlagen, zu prüfen, ob die bestehenden Meldepflichten ausgeweitet werden können, um die Informationslage über Cyberrisiken zu verbessern und effektiver mit Cyberbedrohungen umgehen zu können.

F&L: Im selben Bericht fordert die EFI auch ein zentrales „China-Kompetenz-Center“ für deutsche Wissenschaftler. Inwiefern hängt das mit IT-Sicherheit zusammen?

Uwe Cantner: Das Zentrum soll kooperations- und forschungsrelevante Fragen beantworten und so zur Verständigung zwischen Deutschland und China beitragen. Bei Forschungskooperationen ist auch der unterschiedliche Umgang mit Cybersicherheit wichtig. Hier gilt es, ein wechselseitiges Verstehen und eine gemeinsame Sensibilität für Sicherheitslücken zu entwickeln.

F&L: Was können Forschende selbst tun, um ihre Arbeit zu schützen?

Uwe Cantner: Forschende wollen ihre Ergebnisse veröffentlichen, einige Details sollten sie aber ggf. nicht aufschreiben oder bekanntgeben. Bisher waren sie dabei eventuell zu naiv. Hochschulen müssen hier dringend mehr aufklären und sensibilisieren.

Die Fragen stellte Claudia Krapp.