Virtuelle Bedrohungen

Oberst Walter J. Unger, seit 2001 Leiter der Abteilung „Elektronische Abwehr“ und seit 2009 Leiter der Abteilung „Nachrichtendienstliche IKT-Sicherheit“ im BMLVS, über Gefahren aus dem Internet und wie man sich davor schützen kann.

Das ursprünglich auf Bundesheerangehörige beschränkte IKT-Sicherheitsseminar ist seit dem Vorjahr auch für Vertreter anderer Ressorts sowie für Fachleute aus der Wirtschaft und Medienvertreter zugänglich. Welche Überlegungen waren dafür ausschlaggebend?

Unger: Österreich gehört zu den am dichtesten vernetzten Ländern in Europa, die tägliche Nutzung von Informations- und Kommunikationstechnologie ist zur Selbstverständlichkeit geworden. Damit betrifft IKT-Sicherheit nahezu jedermann. Das Bundesheer trägt mit diesen Veranstaltungen dazu bei, das Bewusstsein für IKT-Sicherheit zu heben.

Welche Einrichtungen und Objekte sind im Falle eines Cyberangriffs als Einrichtungen der kritischen Infrastruktur besonders gefährdet?

Unger: Kritisch ist eine Infrastruktur, wenn sie strategisch – das heißt für den Gesamtstaat – von Bedeutung ist. Das österreichische Bundesheer ist mit dem staatlichen Auftrag, Schutz und Hilfe zu leisten, auch dann eine strategische Infrastruktur, wenn andere Organisationen das nicht mehr können. Das Bundesheer hat in den letzten Jahrzehnten enorm in die Modernisierung der IKT investiert. Es muss daher wie andere Organisationen Schutzmaßnahmen zur Verhinderung von Angriffen aus dem Cyberspace treffen. Wenn Sie so wollen, gilt es, die klassischen physischen Objektschutzmaßnahmen auch auf den virtuellen Raum auszudehnen.

Für wie wahrscheinlich halten Sie Cyberterrorismus?

Unger: Terroristen verfolgen eine Kommunikationsstrategie; es geht darum, Angst und Schrecken zu verbreiten, Symphatisanten für die eigene Sache zu gewinnen. Dazu braucht man die Öffentlichkeit. Ich halte daher Cyberterrorismus zwar für möglich, aber solange als wenig wahrscheinlich, als es andere, spektakulärere Möglichkeiten für Anschläge gibt.

Oberst Walter Unger: „Wichtige Systeme müssen von unsicheren Netzen komplett abgeschottet werden.“

Was sollte Ihrer Meinung nach in präventiver Hinsicht getan werden?

Unger: Das Schwergewicht aller Maßnahmen muss in die Prävention gelegt werden. Wichtige Systeme müssen komplett von unsicheren Netzen abgeschottet werden. Wie das Beispiel Stuxnet zeigt, muss dabei auch auf die Einbringung über mobile Datenträger oder durch Wartungsereignisse geachtet werden. Sicherheit muss im gesamten Lebenszyklus eines IKT-Systems prozesshaft umgesetzt werden.

Neben dem Ausbau redundanter, sicherer Netze braucht es Notfallorganisationen, Computer Emergency Response Teams, die vorausschauend die Bedrohungslage permanent analysieren und bei Angriffen die Gegenmaßnahmen koordinieren. Die Einbeziehung verschiedener Behörden sowie privater Unternehmen wird nur funktionieren, wenn Notfallpläne vorbereitet und durchgeübt worden sind. Das sollte sogar im internationalen Rahmen, wie es die ENISA 2010 erstmals versucht hat, geübt werden, denn im Cyberspace gibt es keine nationalen Grenzen.

Sehen Sie auch Nachholbedarf auf legistischer Ebene?

Unger: Recht im Cyberspace ist eine relativ junge Materie und eine Herausforderung für Legisten. Hier gibt es noch viele ungelöste Problemstellungen.

Was ist im Bereich der internationalen Zusammenarbeit bereits geschehen, woran sollte noch gearbeitet werden?

Unger: Das Bundesheer bemüht sich auch im IKT-Sicherheitsbereich um eine enge Zusammenarbeit mit allen europäischen Partnern. Grenzübergreifende Bedrohungen können nur gemeinsam abgewehrt werden.

Wie kann auch der einzelne User dazu beitragen, aus dem Cyberspace drohende Gefahren abzuwehren?

Unger: Jeder im Internet präsente Rechner kann für Angriffe gegen den User oder Dritte missbraucht werden. Es liegt daher im ureigensten Interesse des Nutzers, den eigenen Rechner möglichst gut abzusichern.

Selbstverständlich sollten zum Schutz vor Schadprogrammen täglich aktualisierte Programme wie Firewalls und Antivirenprogramme auf jeden Computer installiert sein. Solche Programme gibt es sogar kostenlos; der Schutz der eigenen Daten und der Privatsphäre sollte uns aber durchaus ein paar Euro wert sein. Darüber hinaus sollte man sich ein gesundes Misstrauen gegenüber diversen Verlockungen und Mails von unbekannten Absendern bewahren. Nur so kann man verhindern, dass der eigene Rechner Teil eines Botnetzes oder zur Spam- und Virenschleuder wird.

Interview: Kurt Hickisch

FOTO: PRIVAT