youngOVE Graz
Krenngasse 37/5, 8010 Graz
young.graz@ove.at

Semester Opening des youngOVE Graz

Zu Beginn des Sommersemesters 2014 veranstaltete der youngOVE Graz erstmalig ein Semester Opening an der TU Graz. Dazu wurde Dipl.-Ing. Thomas Bleier, Leiter des IT Security Forschungsprogramms am Austrian Institute of Technology (AIT) eingeladen, einen Impulsvortrag zu halten.

Komplexe IT-Systeme

Die Komplexität unserer IT-Systeme steigt stetig. Flog man vor etwa 40 Jahren mit 7.500 Zeilen Softwarecode zum Mond, sind in einem modernen Auto heute bereits wesentlich mehr Codezeilen enthalten. Mit der steigenden Komplexität und Vernetzung steigt auch das Risiko, dass Angriffe verheerende Folgen haben. Unser tägliches Leben wird immer mehr von Technologien wie Smart Grid, Smart Home aber auch E-Government geprägt. Das IT-Security Forschungsprogramm des AIT entwickelt Methoden und Tools, um die Systeme sicherer zu machen und beschäftigt sich dabei hauptsächlich mit drei Anwendungsbereichen: „Smart Grid“, „Cloud Computing“ sowie „National Cyber Security“, wobei es darum geht, kritische Infrastruktur gegen Cyber-Angriffe zu schützen.

Technische Hintergründe

Der Impulsvortrag von Dipl.-Ing. Bleier trug den Titel „Unsere IT wird abgehört – Wie funktioniert das eigentlich?“ und beschäftigte sich mit den technischen Hintergründen. Gerade seit den Veröffentlichungen von Edward Snowden ist dieses Thema in den Fokus der Experten gerückt.

Aus welchem Grund wird unsere IT überhaupt abgehört? In erster Linie, um sich gegenüber dem Gegner einen Vorteil durch mehr Information zu verschaffen. Dabei betreibt längst nicht nur die NSA derlei Aktivitäten; es ist davon auszugehen, dass auch andere Dienste, die über ein ähnliches Budget verfügen, solche Aktionen durchführen.

Welche Methoden werden dabei eingesetzt? Einerseits handelt es sich um passive Analysen von Daten, wie beispielsweise das Auslesen der Positionsdaten von einem Foto, das auf einer Social Media-Seite hochgeladen wird. Zu diesen Daten gelangt man etwa durch Umleitung der Daten. Diese Datenumleitung hat allerdings den Nachteil, dass die Umleitungsrouten mitnotiert werden, wodurch es nachvollziehbar ist, wer die Daten abgehört hat.

Eine weitere Methode ist das Abhören von Dark Fiber. Ein Dark Fiber galt lange Zeit als abhörsicher. Spätestens seit den Veröffentlichungen Edward Snowdens weiß man

allerdings, dass dies nicht der Fall ist. Durch gezielte Manipulation können auch Daten aus einem Dark Fiber abgehört werden.
Der Vortragende warf in weiterer Folge die Frage auf, ob der Internetdatenverkehr auch manipuliert werden kann und beantwortete selbst gleich mit „ja“. Dabei wird beim Aufruf einer bestimmten Seite eine manipulierte Seite als Antwort geschickt, die schneller bei der anfragenden Stelle ist als die Originalseite. Diese manipulierte Seite kann in weiterer Folge durch Schadsoftware den PC infizieren und das System so übernehmen. Es ist sogar möglich, ein File während dem Down- oder Upload zu manipulieren und somit zu verändern. Auch so genannte „Man in the Middle“-Angriffe werden eingesetzt. Dabei handelt es sich um Angriffe auf SSL/TLS-Verbindungen. Dabei wird ein gefälschtes, aber gültiges Zertifikat eingesetzt. In diesem Bereich gibt es Entwicklungen, die versuchen dieses Problem zu beheben, wie beispielsweise Certificate Pinning, bei dem der Browser abspeichert, welches Zertifikat eine Seite verwendet. Hat diese Seite plötzlich ein anderes Zertifikat, so erscheint eine Fehlermeldung. Hier ist dann jedoch der Nutzer gefragt, der auf die Fehlermeldung entsprechend reagieren muss!
Abschließend wies Dipl.-Ing. Bleier darauf hin, dass es neben den im Vortrag thematisierten noch zahlreiche weitere Manipulationsmöglichkeiten gibt, wie etwa der Zugriff auf Endgeräte durch das Eindringen über Schwachstellen, durch Manipulation von Server Hardware, durch manipulierte Kryptographie oder auch radarbasiertes Abhören über manipulierte Bildschirmkabel, USB-keylogger, Ethernet Ports oder Ähnliches.

Resümee

Als Resümee des Vortrags kann festgehalten werden, dass es kein 100 % sicheres System gibt. Die Probleme der IT benötigen mehr Aufmerksamkeit. Erfreulicherweise steigt das Bewusstsein, dass es wichtig ist, auf das Know-how innerhalb von Europa aber auch auf nationaler Ebene einen Fokus zu legen, um sich aus der Abhängigkeit amerikanischer oder anderer Länder zu entziehen.
Der youngOVE Graz bedankt sich recht herzlich bei Dipl.-Ing. Thomas Bleier für seinen sehr interessanten und aufschlussreichen Vortrag. Das Semester Opening fand einen gemütlichen Ausklang am Buffet.

Thomas Hager
youngOVE Graz

youngOVE Graz
Krenngasse 37/5, 8010 Graz
young.graz@ove.at