Jörg Völker, Secorvo-Consultant, erklärt die massiven Sicherheitslücken beim Iphone

Veranstalter des Tags der IT-Sicherheit sind KA-IT-Si, Cyber-Forum und die IHK Karlsruhe

Weit mehr als 100 Besucher kamen zum Tag der IT-Sicherheit bei der IHK in Karlsruhe

Walter Opfermann: „Vertraue keinem Praktikanten", vor allem keinen chinesischen

Fotos: Michael Bode

Unbequeme Wahrheiten

Der Tag der IT-Sicherheit in Karlsruhe macht deutlich: Die schöne neue mobile IT-Welt hat auch ihre Schattenseiten. Hacker greifen Unternehmensnetzwerke an, Geheimdienste spionieren deutsche Firmen aus, selbst ein Smartphone mutiert zum Sicherheitsrisiko

Es ist schön. Es ist praktisch. Wer es hat, will nicht mehr darauf verzichten. „Das Iphone ist aus dem Leben vieler nicht mehr wegzudenken“, sagt Jörg Völker, Security Consultant beim IT-Sicherheitsdienstleister Secorvo Security Consulting in Karlsruhe. „Was viele nicht wissen: Das Iphone ist nicht nur eine Datenkrake, es ist auch ein Datenloch“, sagt Völker. Wer bislang glaubte, das Iphone sei ein harmloses Spielzeug, wurde während des Tags der IT-Sicherheit in Karlsruhe eines besseren belehrt.

Rund 100 Besucher waren auf Einladung von Karlsruher Sicherheitsinitiative (KA-IT-Si), der IHK Karlsruhe und des Cyber-forums

> „Trotz aller Sicherheitsvorkehrungen: Das Iphone ist absolut unsicher“

ins Haus der Wirtschaft gekommen, um über die neusten Bedrohungen für die IT-Sicherheit zu diskutieren.

Das Iphone stand bisher nicht unter dem Verdacht, ein Sicherheitsleck zu sein. Wer Applikationen wie Staumelder oder Präsentationsprogramme runterlud, wusste: Apple prüft die Apps auf Herz und Nieren. „Einem Wissenschaftlerteam ist es gelungen, ein schadhaftes App durch die Kontrollen zu schleusen“, sagt Völker. Die Zweifel an Apples Kontrollen wachsen. Zudem ist das Betriebssystem nicht frei von Macken: Gelöschte Daten sind nicht endgültig gelöscht, „auch wenn der Nutzer das glaubt“. Per findigen Programmen lassen sich die Daten relativ einfach wiederherstellen.

Und so kann selbst ein verlorenes Iphone für den Benutzer zum Fiasko werden – erst recht, wenn er empfindliche Daten aus seinem Unternehmen gespeichert hat. „Der PIN-Schutz ist nicht ausreichend“, sagt Völker, der sich in seinem Vortrag ausschließlich auf das Iphone konzentrierte. Mit frei im Internet verfügbaren Tools können die meisten Sicherheitsmechanismen des Iphones umgangen werden. Diese machen sich dann den sogenannten Jailbreak zu Nutze, heißt: Die Sicherheitsvorkehrungen von Apple werden komplett umgangen. Der Hacker hat dann Zugriff auf sämtliche Daten – per „Disk Dump“ selbst auf die gelöschten. Völkers ernüchterndes Fazit: „Trotz aller Sicherheitsvorkehrungen ist das Iphone absolut unsicher. Die wichtigsten Sicherheitsmaßnahmen sind leicht zu umgehen.“

Der Sicherheitsexperte rät daher, einerseits zusätzliche Sicherheitssoftware aufzuspielen. Zum anderen, „und das ist viel wichtiger“, müssen Nutzer, die ihr Iphone beruflich nutzen, für diese Sicherheitslücken sensibilisiert werden. Eine weitere Möglichkeit ist, sicherheitsrelevante Daten vom Iphone fernzuhalten.

Ein noch finsteres Bild der Gefahr für die IT-Sicherheit von Unternehmen zeichnet Walter Opfermann. Der Experte vom baden-württembergischen Verfassungsschutz warnt die Unternehmen eindringlich vor der Bedrohung durch chinesische Spionage. Opfermann lässt Fälle sprechen: Da wird die Außenkonstruktion eines WM-Stadions in Johannesburg per Mini-Kamera analysiert, um an das Know-how von deutschen Firmen zu kommen, chinesische Studenten werden als Spitzel in deutsche Unternehmen eingeschleust, der chinesische Geheimdienst bespitzelt Geschäftsmänner am Flughafen, bricht in Hotelzimmer ein und hackt sich in die Laptops ein. Opfermann warnt: „Die Zahl der Angriffe steigt seit Jahren stark an. Und es sind keine Amateure, die am Werk sind, auch keine normalen Hacker. Die High-Level-Programmiertechniken, mit denen die Firmen attackiert werden, weisen auf staatliche Auftraggeber hin“, so Opfermann.

Was tun? Das Problem, das die Situation noch verschärft: Nicht nur die Angriffe nehmen zu, auch die Unsicherheitsfaktoren: Es gibt immer mehr Schnittstellen und damit komplexere Systeme, die zur Gefahr werden. Ein erfolgreicher Informationsschutz setzt außerdem ein waches Problembewusstsein sowie die aktive Mitwirkung der Mitarbeiter eines Unternehmens voraus. Andreas Fritz vom Energieversorger EnBW zeigt am Beispiel der konzernweiten Sensibilisierungs-Kampagne "Es geht sicher anders!", wie mit einfachen Mitteln das Zusammenspiel von Mensch und Technik einen wirksamen und effizienten Schutz gewährleistet. Das zeigt: Der Tag der IT-Sicherheit bringt nicht nur unbequeme Wahrheiten ans Licht, er liefert auch Lösungen.

rschwarz@econo.de

www.ka-it-si.de
www.cyberforum.de
www.karlsruhe.ihk.de