DER GROSSE DATENKLAU

Hackerangriffe, Viren und sonstige Gefahren im Cyberspace sind fast schon zur Tagesordnung geworden. Im vorangegangenen Artikel haben wir ausführlich über das Thema IT-Sicherheit berichtet. Wir stellen nun zwei hochrangigen Tiroler Experten die Frage, wie man sich bestmöglich dagegen schützt und die Kontrolle wieder so gut wie möglich zurückgewinnt! // Text: Doris Helweg, Fotos: Julia Türtscher, pro.media

Prof. Dr. Günther Specht leitet die Forschungsgruppe „Datenbanken und Informationssysteme (DBIS)" am Institut für Informatik der Universität Innsbruck

Prof. (FH) Dr. Peter J. Mirski ist Leiter Department & Studiengänge am Management Center Innsbruck, Studiengänge „Management, Communication & IT"

Ohne Frage hat die Kriminalität im Cyberspace zugenommen und kaum jemand kann wirklich sagen, was mit all unseren Daten, sei es am Smartphone oder auf unserem Computer, passiert. Fest steht allerdings auch, dass nach aktuellen Untersuchungen der IT-Security-Experts-Group in der Wirtschaftkammer viele Private und sogar Unternehmen ihre Daten viel zu wenig schützen. Wir sprechen mit zwei Experten.

„DAS WICHTIGSTE IST, BEIM THEMA DATENSCHUTZ UNTER DEN MITARBEITERN DAS ENTSPRECHENDE BEWUSSTSEIN FÜR GEFAHREN ZU SCHAFFEN. TECHNIKEN GIBT ES VIELE, DOCH DIE MEISTEN WERDEN NICHT EINGESETZT."
Prof. Dr. Günther Specht

ECO.NOVA: **Was raten Sie Unternehmern oder insbesondere auch Behörden in puncto Datenschutz? Wie kann man vor allem heikle Daten bestmöglich schützen?**

PROF. DR. GÜNTHER SPECHT: Das Wichtigste ist, unter den Mitarbeitern das entsprechende Bewusstsein für Gefahren, die Awareness, zu schaffen. Techniken gibt es viele, doch die meisten werden nicht eingesetzt. Wer verschlüsselt schon seine E-Mails? Oder wem ist bewusst, was Datenschutz wirklich bedeutet, dass z. B. verschiedene Attributkombinationen eine Person bereits eindeutig identifizieren, ohne den Namen zu nennen? Beruf und Postleitzahl des Wohnorts reichen in Tirol oft aus. Wir sagen dazu Sekundärschlüssel. Überlegen Sie, welche zwei oder drei Merkmale Sie eindeutig identifizieren. Oder wer setzt digitale Signaturen ein? Auch für Dokumente, die das Haus nicht verlassen, um wenigstens hinterher Rechtssicherheit zu erhalten? Hier ist uns die Video- und Audiobranche weit voraus. Datenschutz beginnt im Kopf. Die beste Technik nützt nichts, wenn der Wert der Daten nicht allen klar ist und man selbst Daten „freiwillig" zur Verfügung stellt.

PROF. (FH) DR. PETER MIRSKI: Wesentlich ist, dass jedes Unternehmen eine Datenstrategie formuliert und gemeinsam mit Mitarbeitern festlegt, wie mit Daten umgegangen wird. Das beginnt mit der Auswahl von anerkannten und standardisierten Frameworks, z. B. COBIT 5, die in der Unternehmensstruktur festlegen, wie Daten verarbeitet, gespeichert und ausgewertet werden. Wir sehen immer wieder, dass das Thema Datenschutz in Unternehmen deutlich unterbewertet wird und die Hoffnung auf technischen Lösungen liegt. Tatsächlich können technische Lösungen aber erst greifen, wenn verbindlich festgelegt wurde, welche Daten schützenswert sind, wer auf diese Daten zugreifen darf, wann Daten aufbewahrt oder gelöscht werden müssen etc. Ebenfalls ist es wichtig, Datenschutz als festen Bestandteil der Unternehmenskultur zu verstehen und damit laufend bestehende Prozesse zu analysieren, transparent zu gestalten und zu kontrollieren, um die Sicherheit des Unternehmens auch zukünftig bestmöglich zu garantieren.

Die EU-Datenschutzverordnung hat zwar durch die zahlreichen Vorfälle an Gewicht gewonnen, ist aber immer noch nicht verabschiedet. Was halten Sie von Sanktionen, wie sie zum Beispiel in Großbritannien schon praktiziert werden?

MIRSKI: Die Datenschutzverordnung ist generell notwendig und zeigt in ihrer intensiven Diskussion im Europaparlament, wie unterschiedlich hier die Meinungen und Herangehensweisen unterschiedlicher Staaten sind. Sanktionen sind aus unserer Sicht – so wie sie derzeit gestaltet sind – mehr als Signal zu verstehen, halten aber selten davon ab, Straftaten zu begehen, weil die Höhe der Sanktion selten den zu erwartenden Gewinnen aus datenschutzrechtlichen Verstößen entspricht.

SPECHT: Das ist schwierig. Da müssen Sie heute viel globaler denken. Nicht einmal EU-weite Verordnungen reichen aus. Die Gesetze hinken in der IT den technischen Möglichkeiten immer um Jahre hinterher. Wichtiger ist daher, die Sicherheits- und Betriebssysteme und die Firewalls aktuell zu halten und alle Jahre bewusst geplant bei sich von befreundeten Firmen einbrechen zu lassen. Dann lernen Sie auch die verborgenen Schwachstellen sehr schnell kennen.

Was macht die Universität Innsbruck in dieser Richtung?

SPECHT: Wir sehen am Institut für Informatik Security als ein zentrales Thema an, auch in der Ausbildung. Am In-Day am 27. November 2014 haben wir ein eigenes Security-Lab eröffnet. Dazu findet für unsere Studierenden sogar ein Workshop von Kaspersky statt. Eine eigene Stiftungsprofessur für IT-Security wird gerade eingerichtet. Hier passiert viel.

Kann man Systeme hundertprozentig vor Angriffen schützen?

SPECHT: Natürlich nicht. Aber man muss dem Angreifer ja nicht auch noch die Türe aufhalten. Wenn es beliebig schwer wird, wird auch der Angreifer eine Kosten-Nutzen-Rechnung machen. Wenn wir zurückblicken, hat ja sogar die gesamte Informatik eine ihrer Wurzeln im Codebrechen. Denken Sie nur an die Enigma und an Alan Turing. Nach ihm ist sogar der Nobelpreis der Informatik, der Turing-Award, benannt.

MIRSKI: Nein, das ist wahrscheinlich völlig unmöglich. Jedenfalls besteht ein hoher Zielkonflikt zwischen dem Aufwand, dem Sicherheitsnutzen und der in der Praxis notwendigen Flexibilität und Funktionalität.

Welche Gefahren lauern in mobilen Endgeräten? Gibt es überhaupt noch Privatsphäre und wie kann man sich diese erhalten?

MIRSKI: Mobile Endgeräte schaffen zunächst einmal einen hohen Nutzen – sowohl im privaten als auch im geschäftlichen Umfeld. Das Problem liegt nun darin, dass beide Welten miteinander verschmelzen und ein technisches System nicht ohne weiteres zwischen privater und geschäftlicher Nutzung unterscheiden kann. Zudem können mobile Endgeräte viele Daten mitführen und werden zunehmend mit Funktionen für das alltägliche Leben ausgestattet – beispielsweise mit Bezahldiensten. Wenn man die Funktionalität einer vernetzten, einer „smarten" Welt nützen will, ist der Preis, der dafür zu bezahlen ist, jedenfalls die Aufgabe der Privatsphäre. Wer das nicht will, muss sich eindringlich mit jeder erweiterten Funktion oder Dienstleistung auseinandersetzen und einzeln abwägen, ob der erwartete Nutzen höher ist als das damit verbundene Risiko.

SPECHT: Auch hier gilt es in erster Linie die Awareness, das Bewusstsein für Gefahren, zu schärfen. Warum muss eine einfache Auskunfts-App auf dem Smartphone oder am Tablet Zugriff auf meine integrierte Kamera oder mein Adressbuch haben? Beim Installieren bleibt nur die Möglichkeit des Zustimmens oder Abbrechens. Oft gehen so „mit Zustimmung" sensible Daten nach außen. Wenn ein Service frei ist, finanziert er sich eben meist über die Weitergabe von Benutzerdaten oder sogar Benutzerdateien. Viele Apps laufen nach dem Schließen weiter und versenden weiterhin Daten. Um dies zu verhindern, müssen sie explizit über die Prozessansicht beendet werden, was entweder nicht bekannt ist, oder aus Bequemlichkeit nicht gemacht wird. Wir haben dazu in der Forschungsgruppe DBIS eine hochinteressante App namens Awarenessy im Rahmen einer Bachelorarbeit von Benedikt Stricker entwickelt, die frei verfügbar ist und aufzeigt, was das Handy gerade alles von sich preisgibt. Man ist überrascht und schockiert. Lösungen liegen in der sorgfältigen Auswahl, u. U. auch dem Verzicht auf nützliche Apps oder dem vorherigen Cracken des Handys und dem Aufspielen einer anderen Firmware und dem somit erst möglichen Sperren bestimmter Ausgaben. Aber dann verlieren Sie die Herstellergarantie, da Handys nur mit der Originalsoftware betrieben werden dürfen, auch wenn es Ihr Eigentum ist. Wer sich nicht in diesen Graubereich begeben will, sollte genau hinsehen, welche Apps, mit welchen Freigabewünschen, er sich oder auf Firmenhandys installiert. Weniger ist oft mehr.

„DIE DATENSCHUTZVERORDNUNG IST GENERELL NOTWENDIG UND ZEIGT IN IHRER INTENSIVEN DISKUSSION IM EUROPAPARLAMENT, WIE UNTERSCHIEDLICH HIER DIE MEINUNGEN UND HERANGEHENSWEISEN UNTERSCHIEDLICHER STAATEN SIND."
Prof. Dr. Peter Mirski