

«Sicherheit ist letztlich immer auch eine Frage des Vertrauens»

Adnovum hat Anfang März zu einem Security-Update in seine Zürcher Lokalitäten geladen. Auf dem Programm standen die neuen Sicherheitsbedrohungen und die Bedeutung von Standards und Produkten für die Informationssicherheit. Marion Ronca

Die NSA-Affäre rund um die Snowden-Enthüllungen gab der Informationssicherheit letztes Jahr neuen Auftrieb. Bevor das frisch geweckte Interesse an der Bedeutung der Informationssicherheit wieder verebbte, lud Adnovum Anfang März zu einem Security-Update in seine Zürcher Lokalitäten. Auf dem Programm standen die wichtigsten aktuellen Bedrohungen, die Bedeutung der Security-Standards und -produkte, die neuen Einfallstore der Cyberkriminellen im Businessumfeld sowie eine Demonstration des Open-Authorization-Protokolls als Massnahme gegen eine unkontrollierte Verbreitung von persönlichen Informationen im Netz.

CEO Christof Dornbierer wies einleitend darauf hin, dass zu Adnovums Kernkompetenzen High-End-Software und Security Engineering zähle. Konkret bedeute das, dass sich das Unternehmen an Projekten beteilige, die nicht «ganz normal» seien oder «kurz vor einer Wand» stünden. Adnovums Freude an kniffligen Aufgaben dürfte sich auch positiv auf die Geschäftslage des Unternehmens auswirken, denn laut Dornbierer konnte Adnovum die letzten Jahre seinen Umsatz verdoppeln. Aktuell beschäftigt das Unternehmen 260 Mitarbeiter in der Schweiz, 100 in Ungarn und 20 in Singapur.

NSA setzt neue Security-Trends

Chief Security Officer Bruno Kaiser zeigte im Anschluss anhand einer Hype-Cycle-Grafik die variierende Sichtbarkeit von Sicherheitsbedrohungen auf. So erhielten 2012 Angriffe auf Mobilgeräte am meisten Aufmerksamkeit, während Phishing und Pharming deutlich weniger als Bedrohungen thematisiert wurden. Dieses Jahr werden gemäss Kaiser neben den noch aktuellen Angriffen auf Mobilgeräte vor allem die Identitätsdiebstähle und immer häufiger auch die Schwächung von Produkten und Standards sowie die Staatsüberwachung im Fokus der Öffentlichkeit stehen.

Für Kaiser stehen die neuen Security-Trends klar im Zusammenhang mit der NSA-Affäre: Die aktuellen Sicherheitsrisiken seien nichts anderes als ein Sammelsurium

von technischen Verfahren, die aktuell von Geheimdiensten angewendet würden. Apples fehlerhaftes SSL-Protokoll ist für Kaiser dafür ein gutes Beispiel. Kurz nachdem Apple den Bug eingeführt hatte, trat das Unternehmen dem NSA-Programm Prism bei. «Ich persönlich würde sagen, dass das kein Zufall war», so Kaisers Fazit.

Die Hauptideen aus der NSA-Affäre sind Kaiser zufolge, dass jedes Gerät und jedes Netzwerk infiltriert werden kann, da Standardisierungsgremien, Staaten und nicht zuletzt auch IT-Hersteller nicht einfach «gut» seien. Die gute Nachricht aber sei, dass kryptographische Algorithmen nach wie vor als sicher gelten würden.

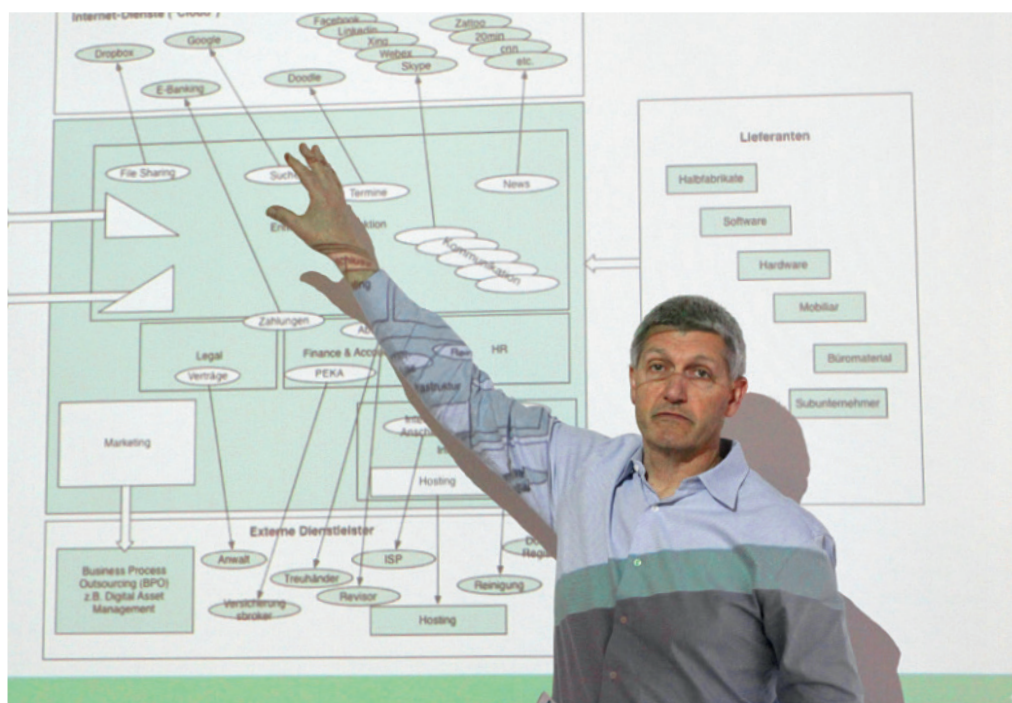
Eine Firewall reicht nicht mehr aus

Gemäss Kaiser haben sich im Enterprise-Umfeld die neuen Gefahren nicht zuletzt aufgrund der verschwimmenden Unternehmensgrenzen vervielfacht. Ein Unternehmen habe heute zahlreiche Schnittstellen zu verwalten, angefangen bei jenen zu den Internetdiensten

wie Google, Doodle, Dropbox etc. Doch auch die Schnittstellen zu externen Dienstleistern, Lieferanten und Kunden würden Sicherheitsrisiken mit sich bringen. Darum reiche es heute nicht aus, eine Mauer aufzuziehen und an einem einzigen Ort den Verkehr zu prüfen. Wie im Schengenraum müssen Unternehmen gemäss Kaiser nicht nur Zutrittskontrollen vornehmen, sondern auch die innere Sicherheit mit Patrouillen überprüfen.

Auch müsste die Verbreitung von heiklen Daten eingedämmt werden - zum Beispiel mit der Methode Privacy by Design, bei der der Erhalt der Privatsphäre im gesamten Engineering-Prozess berücksichtigt wird.

Bruno Kaiser schloss die Veranstaltung mit der Bemerkung, dass Sicherheit letztlich immer auch eine Frage des Vertrauens sei. Er selbst verwalte seine Passwörter mit einem Passwortmanager und vertraue diesem. Adnovum wiederum sei in der bequemen Position, nur sich selbst vertrauen zu müssen und alles selbst zu bauen. Aber das könne freilich nicht jeder.



Bruno Kaiser zeigte Schnittstellen von Unternehmen auf, die Sicherheitsrisiken bergen. Bild: Netzmedien