

Cloud-Computing vergrößert die Hebelwirkung

Cloud-Computing, übersetzt „Rechnerwolke“, ist das aktuelle Trend-Thema. Cloud-Computing ist im Grunde eine Form des Modells SaaS (Software as a Service), das heißt anstatt eigener Software auf eigener Hardware im eigenen Netzwerk zu nutzen, kauft man die Bereitstellung der Anwendung als Service ein. Der Betrieb der Applikation auf entsprechender Hardware erfolgt durch einen IT-Dienstleister; der Zugriff erfolgt über das Internet. Bereits weitverbreitete Beispiele für Cloud-Anwendungen sind zum Beispiel Onlinealben oder E-Mail-Dienste wie Google-Mail.

Diese neue Technologie der Datenverarbeitung hat viele Vorteile. Unabhängig davon, wo man sich gerade befindet, sind die Daten immer zugreifbar und abrufbar, und es gibt weitere gute Gründe wie Leistung und Skalierbarkeit dem Trend des Cloud-Computing zu folgen. In der Hauptsache werden es Kostenvorteile sein, die die Unternehmen hierzu bewegen. Das

Cloud-Computing bietet die Möglichkeit, sich teures Spezialwissen sowie hohe Lizenz- und Wartungskosten für Hard- und Software zu teilen.

Doch wie jede Medaille hat auch diese ihre Schattenseiten, denn natürlich setzt auch die cyberkriminelle Szene Cloud-Computing für ihre Zwecke ein. Stand heute ist es nötig, viele einzelne Computer oder Firmennetzwerke mit Schadsoftware zu infiltrieren, doch künftig könnte die Hebelwirkung viel größer sein. Ist der Zugang zu einer Cloud erst einmal hergestellt, könnte der Kriminelle nicht nur die Daten von einer einzelnen Person oder eines Unternehmens abschöpfen sondern gleich von Hunderten oder Tausenden. Natürlich gibt es Sicherheitsmechanismen, um den Datendiebstahl aus einer Cloud zu verhindern. Doch die sogenannten „schwarzen“ IT-Experten verzeichnen bereits erste Erfolge beim Einsatz des Cloud-Computing für die Underground-Economy.