Meinung

NUTZEN SIE DIE CLOUD, ABER...

Prof. Dr. Hartmut Pohl
IT-Sicherheitsexperte der Gesellschaft für Informatik und Geschäftsführer der Softscheck GmbH

Cloud-Nutzung darf nicht nur Vertrauenssache sein. Vielmehr müssen in angemessenen Zeitabständen (und auch bei Modifikationen anlassbezogen) wiederholte, vollständige Security-Tests zur detaillierten Überprüfung des Sicherheitsniveaus von unabhängigen Prüfern erwartet werden. Standardisierte Cloud-Security-Assessment-Fragebögen beispielsweise sind in jedem Fall hilfreich – aber keineswegs ausreichend.

Gefährlich ist die Meinung, größere Datenmengen (Big Data) könnten gar nicht mehr (wirtschaftlich) abgesichert werden. Denn Sicherheitsmaßnahmen wie eine Sicherheitsstrategie, Zugriffskontrolle (AIM) usw. sind völlig mengenunabhängig. Geld sparen mit IT gehört bereits heute der Vergangenheit an: Wichtiger wird zunehmend die Absicherung der für die Aufrechterhaltung des Betriebs notwendigen Daten.

In Zeiten internationaler politischer Unsicherheit nehmen die IT-Risiken zwischen Nationen noch stärker zu, als sie schon in der Vergangenheit waren. Die immer wieder der NSA unterstellte Industriespionage und (in jüngerer Zeit) insbesondere die Sabotage wird von vielen Nachrichtendiensten und kriminellen Gruppen und kriminellen Unternehmen international erfolgreich betrieben und nimmt – auch innerhalb der EU – stark zu: Die vielen Meldungen über erfolgte Angriffe auf praktisch alle Branchen wie Maschinenbau, Energie, Banken und Versicherungen bis hin zu lebensunterstützenden Geräten in Krankenhäusern – dem gesamten Gesundheitsbereich und IT, um nur einige zu nennen. Auch dem Logistikbereich kommt eine erhebliche Bedeutung zu angesichts der unverzichtbaren Versorgung der Bevölkerung mit Lebensmitteln, Wasser und Medikamenten.

Vielfach wird die Cloud-Nutzung in kleinen Unternehmensbereichen mehr ausprobiert. Zum systematischen Einsatz von Clouds ist eine Sicherheitsstrategie unverzichtbar mit einer Risikoanalyse und Bewertung der vorgesehenen Daten. Die Strategie muss selbst in den kleinsten Unternehmen formuliert werden, um mögliche Datenabflüsse und Veränderungen zu verhindern.

Die Verschlüsselung der Daten ist für Vertraulichkeit zwar unverzichtbar bei der Übertragung von und zur Cloud und in ihr. Allerdings müssen die Daten für die Verarbeitung entschlüsselt werden. Bei schlecht implementiertem Authentication and Identity Management fließen dann wertvolle Daten schon mal an unberechtigte Dritte und Angreifer. Die immer wieder gern diskutierte homomorphe Verschlüsselung ist (leider noch) nicht marktreif. Darüber hinaus müssen wirkungsvolle Maßnahmen zur Erreichung von Integrität und Verfügbarkeit ergriffen werden – schließlich konnte im Einzelfall nicht zum vereinbarten Zeitpunkt auf Daten zugegriffen werden.

Alle Sicherheitsmaßnahmen – und auch die Mandantenfähigkeit müssen ständig (automatisiert) auditiert werden. Erfahrungsgemäß sind in fast allen IT-Produkten (Software, Firmware, Apps und Systems – auch embedded) von Angriffen ausnutzbare Sicherheitslücken – insbesondere die noch nicht veröffentlichten Zero-Day-Vulnerabilities – enthalten. Dies gilt auch für die Cloud steuernde Software und die Anwendungen. Um die Sicherheitslücken zu identifizieren, reicht ein Penetration Test überhaupt nicht aus.

Vielmehr muss ein ISO 27034-basierter Security Testing Process (Stand der Technik) eingesetzt werden, um die Sicherheitslücken zu identifizieren. Eingesetzt werden dazu folgende fünf Methoden: Security Requirementsanalyse, Überprüfung des Designs mit Threat Modeling, Überprüfung des Quellcodes mit Static Source Code Analysis, dem klassischen Penetration Testing und letztlich Untersuchung des ausführbaren Codes mit Fuzzing – Dynamic Analysis. In naher Zukunft sind dazu auch Zertifizierungen nach der ISO 27034 zu erwarten.

Nutzen Sie die Cloud, sie ist nicht gefährlich – sie muss und kann aber gut abgesichert werden. Vertrauen ist zwar gut – aber überprüfen Sie sorgfältig das jeweils angebotene Sicherheitsniveau, ob es tatsächlich Ihren Anforderungen standhält.