

Kampf dem internen Datenmissbrauch

Wenn eine sicherheitstechnisch versierte Behörde wie die National Security Agency (NSA) so gründlich ausspioniert werden kann, wie Edward Snowden es konnte, wie sollen sich dann normale Firmen vor Industriespionage schützen? Die Frage beunruhigt heute die meisten Unternehmer, besonders aber jene, die auf einen Cloud-Dienst zugreifen, um über Firmengrenzen hinweg zu kommunizieren. Gibt es in der Informationstechnologie überhaupt eine technische Lösung, die den Unsicherheitsfaktor „Mensch“ in den Sicherheitskonzepten berücksichtigt, ihn als Risiko ausschließt?

Selbst wenn Unternehmensdaten verschlüsselt sind, so ist dies nur eine Scheinsicherheit. Denn die IT-Mitarbeiter haben Zugang zu den Verarbeitungsservern, um notwendige Wartungsarbeiten vornehmen zu können.



Mit IDGARD lassen sich Unternehmensdaten endlich sicher in die Cloud auslagern. Die versiegelte Cloud macht Abhören und Mitlesen unmöglich, da die verschlüsselten Daten weder vom Anbieter noch vom Administrator oder sonst jemandem eingesehen werden können.

Dort aber werden die Daten im unverschlüsselten Zustand verarbeitet. Daher ist vor IT-Mitarbeitern wenig geheim zu halten: Manche Cloud-Anbieter sind sich dieser Sicherheitsrisiken durchaus bewusst und versuchen, sie durch organisatorische Maßnahmen einzudämmen, wie zum Beispiel mit dem „Vier-Augen-Prinzip“. „Rein organisatorische Maßnahmen in Rechenzentren reichen für die Sicherheit der Daten nicht aus“, erklärt dagegen Sicherheitsexperte Ralf Rieken. Der Geschäftsführer des Münchner Unternehmens Unicon GmbH setzt deshalb „mit der Basistechnologie ‚Sealed Cloud‘ vor allem auch auf technische Maßnahmen“. Zu diesen zählen Verschlüsselung, Schutzmechanismen im



Speichermanagement und Datenlöschfunktionen. „Das System sichert die Daten nicht nur bei der Speicherung und beim Transfer auf technische Weise, sondern auch in aktiven Sessions“, führt Rieken weiter aus. So könnten auch IT-Administratoren nicht an die Daten heran.

Sichere Kommunikation übers Netz

Auf der Basis dieser Cloudtechnologie arbeitet die Anwendung IDGARD. Dies ist ein – auch von mobilen Geräten aus einsetzbarer – Kommunikationsdienst, über den sich Daten abhörsicher austauschen oder über Firmengrenzen hinweg chatten lässt und Projekte in einem vertraulichen Online-Workspace geplant und umgesetzt werden können.

Weitere Informationen im Rahmen des Trusted Cloud Programms des Bundesministeriums für Wirtschaft und Energie unter <http://trusted-cloud.de/de/1639.php> oder unter www.idgard.de

IDGARD für Unternehmen im Test

Ein Cloud-Dienst, um Dokumente und Nachrichten zu speichern und auszutauschen – kombiniert mit der Sicherheit der Sealed Cloud. Unternehmen können

- Dokumente und Nachrichten mit Kunden und Partnern austauschen
- versiegelte Datenräume für firmenübergreifende Projektteams nutzen
- auf geschäftliche Unterlagen sicher und mobil zugreifen
- in den Datenräumen auch chatten – eine sichere Alternative zu anderen Chat-Diensten oder zu SMS.

Das alles funktioniert auf PC und Mac, ohne neue Software – ein Browser genügt. Für mobile Endgeräte gibt es entsprechende Apps (iPhone/iPad und Android).

Gleichzeitig dürfte sich mit der Kommunikation über den Dienst die Produktivität steigern lassen, da die Dokumente und Nachrichten projektorientiert abgelegt werden. Sie liegen also dort, wo sie letztendlich auch gebraucht werden. IDGARD informiert auch die Kommunikationspartner automatisch, wenn neue Dokumente oder Nachrichten ankommen.

Jeder Mitarbeiter hat 20 GB privaten Speicher, wo er für Projekte separate Datenräume – Privacy Boxen – anlegt und die Kommunikationspartner in diese einlädt. Alle Mitglieder so einer Privacy Box kommunizieren geschützt – Dokumente, Nachrichten und Chat. Die Bedienung hat sich als einfach und intuitiv erwiesen.