Persönliche Datenverwaltung: Wem gehören Daten überhaupt?

Thorsten Freitag, 2013-18-07

IT Pro in Großbritannien berichtete vor Kurzem, dass das Marktforschungsunternehmen Gartner strengere Kontrollen bei der persönlichen Datenverwaltung fordere. Wir alle wissen, dass wir unsere persönlichen Daten strikt von Unternehmensdaten trennen und alle erforderlichen Maßnahmen ergreifen sollten, um diese Daten zu schützen. Aber sind wir ehrlich – viele von uns tun dies nicht und setzen Daten somit dem Risiko von Angriffen aus.

Ergebnissen einer F5-Umfrage zufolge, die im April während der Infosecurity UK durchgeführt wurde, sagten 83 Prozent der Teilnehmer aus, dass sie sich nicht sicher seien, ob ihr Unternehmen einheitliche Sicherheits- und Verfügbarkeitsrichtlinien in der gesamten IT-Infrastruktur einhalte. Viele Menschen bezweifeln offenbar, dass ihre Daten im IT-System ihres Unternehmens sicher sind, gefährden diese jedoch weiterhin.

Gartner prophezeit, dass 90 Prozent aller Unternehmen bis zum Jahr 2019 persönliche Daten auf ihren IT-Systemen gespeichert haben werden, die sie weder besitzen, noch steuern können. Es handelt sich also um immense Datenmengen, die einen großen Reiz auf Cyberkriminelle ausüben, für die persönliche Daten enorm wertvoll sind und als Sprungbrett zu den Unternehmensdaten gelten.

Durch die Einführung von offiziellen Richtlinien zur persönlichen Datenverwaltung wissen Mitarbeiter genau, was sie auf den IT-Systemen der Unternehmen speichern dürfen und was nicht. So werden sowohl die Daten als auch die Unternehmensinfrastruktur geschützt. Richtlinien zur persönlichen Datenverwaltung werden die Gesamtsituation sicherlich verbessern. Die Kombination mit einem kontextsensitiven Netzwerk könnte das Problem jedoch ein für alle Mal aus der Welt schaffen.

Wenn ein Unternehmensnetzwerk die Quelle des Datenverkehrs geografisch, nach Gerät und nach Authentifizierung eindeutig identifiziert, kann es auf der Grundlage dieser Informationen intelligente Entscheidungen treffen. Es könnte also unterscheiden, ob der Zugriff eines Mitarbeiter auf persönliche Mails oder Unternehmensdaten erfolgt, oder ob eine App verwandt wird. Weiterhin könnte erkannt werden, ob Informationen von Cyberkriminellen abgefangen werden.

Sollte es Zweifel bezüglich der Sicherheit einer Verbindung oder eines Geräts geben, könnte das Netzwerk sich effektiv schützen, noch bevor irgendein Schaden angerichtet werden würde. Das Netzwerk wäre gesichert und die richtigen Mitarbeiter würden die richtigen Daten zur richtigen Zeit erhalten, wodurch sie effektiv und ohne das Risiko eines Angriffs arbeiten könnten.

Gartner gibt an, dass immer mehr Unternehmen externe Serviceanbieter für die Verwaltung ihrer Kreditkartendaten beauftragen, anstatt diese auf den eigenen Systemen zu speichern. Dies könnte in naher Zukunft auch für persönliche Daten gelten. Die strikte Trennung zwischen persönlichen und geschäftlichen Daten ist der erste Schritt in die richtige Richtung. Kontextsensitive Systeme spielen eine wichtige Rolle bei der Aufrechterhaltung der Sicherheit und Verfügbarkeit beider Datentypen.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc. Corporate Headquarters info@f5.com	F5 Networks Asia-Pacific apacinfo@f5.com	F5 Networks Ltd. Europe/Middle-East/Africa emeainfo@f5.com	F5 Networks Japan K.K. f5j-info@f5.com