Fraunhofer SIT

FRAUNHOFER-INSTITUT FÜR
SICHERE INFORMATIONSTECHNOLOGIE

PRESSEINFORMATION
25. Juni 2012

Gleiche Schwachstelle bei 7 Cloud-Speicherdiensten

Cloud-Speicherdienste erlauben Registrierung mit fremden Email-Adressen – Fraunhofer SIT sieht Möglichkeit für Spionage und Verbreitung von Malware.

Sicherheitsexperten des Darmstädter Fraunhofer-Instituts für Sichere Informationstechnologie (SIT) haben festgestellt, dass mehrere Cloud-Speicherdienste bei der Registrierung nicht die angegebene Email-Adresse überprüfen. In Kombination mit Funktionen der Cloud-Speicherdienste wie z.B. File Sharing oder integrierten Benachrichtigungsfunktionen ergeben sich dadurch verschiedene Angriffsmöglichkeiten. So können Angreifer unter falschem Namen etwa Malware in Umlauf bringen oder vertrauliche Daten ausspionieren. Als einer der Träger des Center for Advanced Security Research Darmstadt (CASED) hat Fraunhofer SIT verschiedene Cloud-Speicherdienste untersucht. Dabei fanden die Tester die gleiche Schwachstelle in den kostenfreien Dienstangeboten von CloudMe, Dropbox, HiDrive, IDrive, SugarSync, Syncplicity und Wuala. Eine Beschreibung der möglichen Angriffe und Bedrohungen stellen Mitarbeiter des Fraunhofer SIT am 26. Juni 2012 in Liverpool auf der 11. International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom) vor.

Um die Schwachstelle auszunutzen, brauchen Angreifer keinerlei Programmierkenntnisse. Es genügt, ein Konto zu erstellen und dabei eine fremde Email-Adresse zu verwenden. Anschließend kann der Angreifer unter falschem Namen Schadsoftware verteilen. Bei den Diensten Dropbox, IDrive, SugarSync, Syncplicity und Wuala können Angreifer arglose Computernutzer mit Hilfe der fremden Identität sogar ausspionieren, indem sie sie dazu bringen, vertrauliche Daten für einen gemeinsamen Zugriff in die Cloud zu laden.

Fraunhofer SIT hat die betroffenen Anbieter bereits vor mehreren Monaten informiert. Obwohl die Schwachstelle mit sehr einfachen und bekannten Methoden wie etwa der Versendung einer Email mit Aktivierungslink geschlossen werden kann, gibt es immer noch Anbieter, die keinen Handlungsbedarf sehen. Dr. Markus Schneider, stellvertretender Institutsleiter des Fraunhofer SIT: „Nach unserem Hinweis haben inzwischen Dropbox, HiDrive, SugarSync, Syncplicity und Wuala reagiert.“ Einige dieser Anbieter verwenden zur Vermeidung der Schwachstelle nun die seit langem bekannte Bestätigungsemail, andere setzen Mechanismen ein. “Aus unserer Sicht ist es wichtig, die Verbraucher auf das bestehende Problem hinzuweisen“, so Schneider. „Leider kann man sich nicht vollständig gegen alle Angriffe schützen, selbst wenn man die betroffenen Dienste meidet. Deshalb ist es wünschenswert, dass die Anbieter der Cloud-Speicherdienste die Schwachstelle beseitigen, da dadurch Verbraucher besser geschützt wären.“

Verbraucher, die die betroffenen Dienste nutzen, sollten vorsichtig sein. Wer eine

Redaktion
Oliver Küch | Fraunhofer-Institut für Sichere Informationstechnologie | Telefon +49 6151 869-213
Rheinstraße 75 | 64295 Darmstadt | www.sit.fraunhofer.de | presse@sit.fraunhofer.de

Aufforderung bekommt, Daten aus der Cloud herunter oder in die Cloud zu laden, sollte per Email beim vermeintlichen Absender nachfragen, ob die Aufforderung wirklich von ihm stammt

PRESSEINFORMATION
25. Juni 2012

Redaktion
Oliver Küch | Fraunhofer-Institut für Sichere Informationstechnologie | Telefon +49 6151 869-213
Rheinstraße 75 | 64295 Darmstadt | www.sit.fraunhofer.de | presse@sit.fraunhofer.de