idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Press release

Technische Universität Darmstadt
Jörg Feuck
06/20/2011
http://idw-online.de/en/news428952

Research results
Information technology
transregional, national

Erhebliche Sicherheitsbedrohung durch sorglose Cloud-Nutzung

CASED-Wissenschaftler finden sensible Daten von Nutzern der Amazon Web Services Wissenschaftler des Darmstädter Forschungszentrums CASED haben große Sicherheitsmängel in zahlreichen virtuellen Maschinen in der Amazon-Cloud entdeckt. Von 1100 untersuchten öffentlichen Amazon Machine Images (AMIs), auf denen Cloud-Dienste basieren, waren rund 30 Prozent so verwundbar, dass Angreifer teilweise Webservices oder virtuelle Infrastrukturen hätten manipulieren oder übernehmen können.

Ursache ist der fahrlässige Umgang von Amazon-Kunden mit AMIs. Zur Prüfung solcher Maschinen haben die CASED-Wissenschaftler einen Schwachstellenscanner entwickelt, der im Internet unter http://trust.cased.de/AMID kostenlos heruntergeladen werden kann.

Dank steigender Popularität, einfacher Benutzbarkeit und großen Preisvorteilen bieten immer mehr Firmen und private Nutzer zahlreiche Dienste in der Cloud an. Während Experten die Sicherheitsaspekte der zugrundeliegenden Cloud-Infrastruktur bereits ausgiebig diskutieren, werden die Fehler beim Aufbau solcher Dienste häufig noch stark unterschätzt. Wie schwerwiegend die Folgen mangelnder Sorgfalt von Cloud-Kunden sein können, zeigt eine aktuelle Untersuchung der Forschungsgruppe um Prof. Ahmad-Reza Sadeghi am Center for Advanced Security Research Darmstadt (CASED).

Die Forscher des Fraunhofer SIT in Darmstadt und des System Security Labs der TU Darmstadt untersuchten Dienste, die von Kunden des Cloud-Anbieters Amazon Web Services (AWS) veröffentlicht wurden. Obwohl AWS auf ihren Webseiten ausführliche Sicherheitsempfehlungen geben, fanden die Forscher in mindestens einem Drittel der Fälle fehlerhafte Konfigurationen und sicherheitskritische Daten wie Passwörter, kryptographische Schlüssel und Zertifikate. Mit diesen Informationen können Angreifer etwa kriminelle virtuelle Infrastrukturen betreiben, Webdienste manipulieren oder Sicherheitsmechanismen wie Secure Shell (SSH) aushebeln.

„Das Problem liegt klar auf Kundenseite und nicht bei den Amazon Web Services. Wir gehen davon aus, dass auch Kunden anderer Cloud-Anbieter sich und andere durch ihre Unwissenheit und Nachlässigkeit gefährden“, betont Prof. Sadeghi. In Abstimmung mit dem Sicherheitsteam von Amazon Web Services wurden die betroffenen Kunden informiert.

Pressekontakt:

Fraunhofer SIT Darmstadt
Oliver Küch, Rheinstraße 75, 64293 Darmstadt
Tel.: +49 6151 869-213, E-Mail: oliver.kuech@sit.fraunhofer.de

MI-Nr. 48/2011, Grauenhorst

Attachment 48-2011-Cloud http://idw-online.de/en/attachment9700