Cirosec hackt die Microsoft-Cloud

IT-Defense-Konferenz, Köln

Cirosec hackt die Microsoft-Cloud

geschrieben von LANline/Dr. Wilhelm Greiner am 13.02.2014

Auf der Sicherheitskonferenz IT-Defense, die das Heilbronner Security-Beratungsunternehmen Cirosec von 12. bis 14. Februar in Köln veranstaltet, präsentierte Joshua Tiago, Senior Consultant bei Cirosec, den Einbruch in einen Micrsoft Team Foundation Server (TFS) mittels manipuierter Unit-Tests. Der Angriff funktioniert laut Tiago deckungsgleich auch für die in der Microsoft-Azure-Cloud gehostete Variante des TFS. Microsofts Antwort auf die Meldung der Schwachstelle lässt sich paraphrasieren als: „It's not a bug, it's a feature."

Mlt TFS können mehrere Entwicklerteams auf dem gleichen Server parallel an ihren jeweiligen Projekten arbeiten. Der Hack von Cirosec zeigt, dass es durch manipulierte Unit-Tests möglich ist, das Rechte- und Rollenkonzept des TFS zu unterlaufen und den Server unter die Kontrolle des Angreifers zu bringen.

Eine Eskalation der Privilegien ermöglichte es Joshua Tiago, Zugriff auf eine interaktive Kommandozeile zu erhalten. Von dort aus gelang es ihm zudem, die Firewall zu überwinden und Administratorpasswörter abzugreifen, wie er auf der Bühne der IT-Defense in Köln demonstrierte.

Laut Tiago findet sich diese Build-Services-Schwachstelle „eins zu eins" auch in der Cloud-Variante des TFS, die Microsoft auf Azure betreibt. Er habe dies nachvollziehen und sich „in der Cloud ein bisschen umsehen" können.

Recht ernüchternd ist die Reaktion Microsofts, die Tiago dem IT-Defense-Publikum schilderte: Auf die Meldung der Schwachstelle inklusive detaillierter Beschreibung im August 2013 hin habe ihn Redmond drei Monate auf Antwort warten lassen, um dann zu verlautbaren, dies sei „per Design" so vorgesehen - kein Bug also, sondern ein Feature. Denn Entwickler eines Unternehmens würden a priori als vertrauenswürdig eingestuft - eine Annahme, die insbesondere im Cloud-Kontext nur schwer aufrechtzuerhalten sein dürfte.

Cirosec empfiehlt, sich nicht auf das Rechtekonzept von TFS zu verlassen und deshalb kritische Projekte ausschließlich auf einem dedizierten TFS-Server zu betreiben.

Die IT-Defense - eine immer wieder sehr spannende Security-Konferenz - fand dieses Jahr zum zwölften Mal statt. Auf der IT-Defense referierten in der Vergangenheit bereits IT-Security-Größen wie Bruce Schneier, Kevin Mitnick, Mikko Hyppönen oder auch der jüngst verstorbene Barnaby Jack. Die Keynote hielt diesmal Marcus Ranum - ein Bericht hierzu folgt in Kürze auf LANline.de.

Weitere Informationen zu Cirosec finden sich auf www.cirosec.de.