Ministerium für Finanzen
Baden-Württemberg

08.01.2018

IT

Kryptomining-Angriff auf Server des Landesamts für Besoldung und Versorgung - Service sicherheitshalber eingeschränkt

Nach einem Hacker-Angriff auf die Anmeldeserver des Landesamts für Besoldung und Versorgung in Fellbach sind die Online-Services aus Sicherheitsgründen vorübergehend abgeschaltet worden. Der Angriff ist Anfang des Jahres entdeckt worden. Bei der Attacke wurden einzelne Rechenprozesse gestoppt; der Versuch, weitere Software auf dem Server zu installieren, wurde durch die Sicherheitssysteme abgewehrt.

Ziel des Angriffes war es offenbar, Rechenleistung zu kapern. In Zusammenarbeit mit dem Beauftragten der Landesregierung für Informationstechnologie, Stefan Krebs, dem Innenministerium, Landeskriminalamt, BITBW und spezialisierten Unternehmen wird der Vorfall umfassend untersucht. Staatsanwaltschaftliche Ermittlungen wegen des Verdachts des Ausspähens von Daten und des Verdachts der Computersabotage sind bereits eingeleitet. „Die Zusammenarbeit lief sehr schnell an und war unkompliziert“, sagte der Sprecher.

„Es gibt keine Anzeichen dafür, dass es den Angreifern gelungen ist, auf Kundendaten zuzugreifen oder diese abzuziehen“, erklärte ein Sprecher des Finanzministeriums. In erster Linie seien die Anmeldesysteme für Dienstreisen, die Jobticket-Anmeldung und der Zugang zur elektronischen Beantragung von Beihilfe betroffen. Sie wurden vom Netz genommen. Alle Abrechnungssysteme für die Bediensteten des Landes mit den entsprechenden sensiblen Daten laufen auf anderen, abgetrennten Servern. Sie sind nicht betroffen.

Bis die Systeme wieder zur Verfügung stehen, wurden die Landesbehörden am heutigen Montag informiert, Beihilfe- und Dienstreise-Anträge in Papierform abzuwickeln. „Das ist zwar etwas unbequem, aber wir wollen auf Nummer sicher gehen. Im Zuge der landesweiten IT-Neuordnung und Bündelung der IT-Systeme stand das alte System ohnehin gerade vor der Ablösung. Eine neue Version des Kundenportals ist bereits im Pilot-Betrieb. Diese soll in rund zwei Wochen an den Start gehen“, sagte ein Sprecher.

Hintergrund Kryptomining

Seit Herbst 2017 kam es in Deutschland immer wieder zu Übergriffen, bei denen Rechenleistung abgezweigt wurde. Mit der gekaperten Rechenleistung zahlreicher Computer schürfen die Hacker Kryptowährungen wie Monero oder Ethereum. Kryptowährungen sind auf ein dezentrales Netzwerk vieler Computer angewiesen und jeder, der Rechenleistung zur Verfügung stellt - egal ob eigene oder gekaperte - bekommt einen Anteil. Der Angriff auf den Landesserver könnte im Zusammenhang mit einer weltweit laufenden Attacke stehen. Die Ermittlungen laufen noch.

http://fm.baden-wuerttemberg.de/de/service/presse-und-oeffentlichkeitsarbeit/pressemitteilung/pid/kryptomining-angriff-auf-server-des-landesamts-fuer-besoldung-und-versorgung-service-sicherheitsha/