Las Vegas

# Schnelles Handeln nach Cyber-Attacke

## [03.04.2020] Las Vegas wurde Anfang Januar Opfer einer Ransomware-Attacke. Dank Cloud Data Management konnten die betroffenen Datensysteme zeitnah wiederhergestellt werden.

Anfang Januar 2020 mussten die Website und mehrere Dienste der Stadtverwaltung von Las Vegas im US-Bundesstaat Nevada infolge einer Ransomware-Attacke vom Netz genommen werden. Das meldet das Unternehmen Rubrik. Nach Angaben der lokalen Presse sei der Vorfall vermutlich von einem Phishing-Angriff per E-Mail ausgegangen. Etwas mehr als 24 Stunden später hätte sich die Lage jedoch bereits wieder normalisiert. Die Stadtverwaltung Las Vegas informierte: „Nach dem gestrigen Cyber-Sicherheitsvorfall haben wir den vollen Betrieb wiederaufgenommen, und alle Datensysteme funktionieren wieder normal. Dank unserer Software-Sicherheitssysteme und des schnellen Handelns unseres IT-Personals konnten wir glücklicherweise eine potenziell verheerende Situation vermeiden.“ Ein anschließender weiterer Tweet versicherte den Followern, dass keine Daten verloren gegangen und keine persönlichen Daten gestohlen worden seien.
Die Stadtverwaltung von Las Vegas nutzt seit einiger Zeit das Cloud Data Management von Rubrik, berichtet das Unternehmen.

**Malware verschlüsselt Daten**

Durch die Umstellung hätte die Stadtverwaltung von Las Vegas eine schnelle Wiederherstellung ihrer Datensysteme durchführen und so bereits Ausfälle kritischer Dienste verhindern können. Lester Lewis, Deputy IT Director, erklärt: „Rubrik ist ein sehr wichtiger Partner, wenn es darum geht, wie wir jetzt unsere Prozesse ausführen. Da wir die Entscheidung getroffen haben, eine Smart City zu sein, müssen wie alle anfallenden Daten auch schützen.“
Ransomware wird nach Angaben von Rubrik auch im kommenden Jahrzehnt noch ein Thema sein. Dabei verschlüsselt eine Art Malware die Daten auf dem infizierten Computer, bis der Benutzer den Malware-Akteuren im Austausch für den Verschlüsselungscode ein Lösegeld bezahlt. Ransomware könne ohne diesen Code fast unmöglich entschlüsselt werden. Aber selbst wenn der Benutzer der Lösegeldforderung nachkommt, sei nicht garantiert, dass er alle seine Daten zurückerhält. Werde das Lösegeld nicht bezahlt, werde der Verschlüsselungscode gelöscht. Wenn keine effektive Technologie zur Datenwiederherstellung im Einsatz ist, seien die Daten für immer verloren.

(co)

Stichwörter: IT-Sicherheit, International, USA, Las Vegas, Rubrik, Cyber-Attacke, Malware, Ransomware, Cloud Data Management