QGroup präsentiert »Best of Hacks«: Highlights Juni 2020

Frankfurt am Main, 03. August 2020 – Datenverletzungen und Cyberangriffe auf kritische Infrastruktursysteme stellen eine immer größer werdende Bedrohung dar. Umso wichtiger ist es, die Daten zu schützen. Doch leider haben Hacker immer wieder leichtes Spiel, weil Daten ungeschützt abrufbar sind. So geschehen im Juni beispielsweise bei Bluekai und zahlreichen Online-Datingplattformen.

Unbekannte Hacker haben eine Sicherheitsverletzung genutzt und bei dem in Texas ansässigen Webdesign- und Hosting-Unternehmen **Netsential** 269 Gigabyte Daten von US-Polizeibehörden erbeutet und veröffentlicht. Die Sammlung, die Daten aus über zwei Jahrzehnten enthält, wird als „BlueLeaks“ bezeichnet. Staatliche Einrichtungen nutzen den Dienstleister für ihr Fusion Center, um polizeiliche und nachrichtendienstliche Informationen auszutauschen. Die erbeuteten Daten bestehen aus Polizeiberichten und -unterlagen und enthalten Namen, E-Mail-Adressen, E-Mails samt Anhängen, Telefonnummern, Fotos und Videos sowie PDF-, ZIP- und CSV-Dateien. Auch Kontoverbindungsdaten von Verdächtigen sind in den Daten enthalten. Dass auch Daten von verdeckten Ermittlern enthalten und diese somit in Gefahr sein könnten, ist nicht auszuschließen. Denkbar ist auch, dass Gruppen des organisierten Verbrechens durch den Datendiebstahl Zugriff auf Daten hatten, die sie nun für ihre Machenschaften nutzen könnten.

Eine ungeschützte Datenbank des US-amerikanischen Online-Vermarkters **Bluekai** war frei im Netz abrufbar. Die Cloud-basierte Big-Data-Plattform sammelt pseudonymisierte Nutzerdaten durch Tracking von Webseiten. Insgesamt soll dabei etwas mehr als ein Prozent des gesamten Webtraffics gescannt werden. Die Datenbank enthielt daher Milliarden von Nutzerdaten wie Namen, Adressen, E-Mail-Adressen und weitere personenbezogene Angaben sowie Zahlungsvorgänge.

Falsch konfigurierte S3 Buckets sorgen immer wieder dafür, dass Unternehmen unbemerkt vertrauliche Daten öffentlich ins Netz laden. Besonders brisant ist es, wenn es sich bei diesen Unternehmen um Nischen-Datingplattformen handelt. So hatte auf einem ungesicherten Amazon S3 Bucket jeder Zugriff auf über 20 Millionen Dateien, darunter unter anderem Dateien mit Bildern und Sprachaufnahmen der **Dating-Apps 3some, Cougary, Gay Daddy Bear, Xpal, BBW Dating, Casualx, SugarD und Herpes Dating**. Auch Profilinformationen, private Unterhaltungen, Screenshots von Chatverläufen und Zahlungsvorgängen waren frei zugänglich.

Unbekannte Hacker haben sich über Malware Zugriff auf einen internen Server von **Honda** am Standort Tokio verschafft. Sie konnten so auf das interne E-Mail-System sowie ein System der Qualitätsprüfung zugreifen. Als Folge des Angriffs musste der japanische Autohersteller in mehreren seiner Werke die Produktion einstellen. Betroffen waren hiervon Standorte in den USA, in Südamerika und in Indien. Die Mitarbeiter wurden angewiesen, ihre Dienstrechner nicht hochzufahren. (2.882 Zeichen)

Medienkontakt:

QGroup GmbH
Berner Straße 119
60437 Frankfurt am Main
www.qgroup.de/presse

Lars Bothe
Tel.: +49 69 17 53 63-014
E-Mail: l.bothe@qgroup.de