QGroup präsentiert »Best of Hacks«: Highlights August 2020

Frankfurt am Main, 01. Oktober 2020 – Im August kommt es unter anderem zu einem Leak bei Intel und das Fuhrpark-Dienstleistungsunternehmen der Bundeswehr sowie die neuseeländische Börse werden gehackt. Vor dem Hintergrund der Präsidentschaftswahl in den USA rückt auch der US-amerikanische Social-News-Aggregator Reddit in den Fokus von Hackern.

Von einem ungeschützten Server beim US-amerikanischen Chiphersteller **Intel** wurden über 20 GByte an Daten geleaked. Die Dateien stammen anscheinend aus dem Intel-Resource-and-Design-Center, in dem Informationen zur Verwendung durch Kunden, Partner und andere externe Parteien gespeichert sind, die sich für den Zugriff registrieren müssen. Enthalten sind u. a. Chipsatz-Firmware, Dokumentationen zu Intels Management Engines und Quellcodeteile.

Unbekannte Hacker haben sich Zugang zum IT-Netz der **BwFuhrparkService GmbH**, das Fuhrpark-Dienstleistungsunternehmen für die Bundeswehr, verschafft. Die Gesellschaft gehört zu 75,1 Prozent dem Verteidigungsministerium und zu 24,9 Prozent der Deutschen Bahn AG. Sie übernimmt auch den Fahrdienst des Deutschen Bundestags. Alle Netzverbindungen nach außen und in Richtung der Kunden – Verteidigungsministerium, Bundeswehr, Deutscher Bundestag wurden daraufhin unterbrochen. Das IT-Netz wurde zunächst per E-Mail mit dem Erpressungstrojaner „Emotet“ infiziert. Dieser hat dann den Erpressungstrojaner „QakBot“ und die Schadsoftware „Cobalt Strike“ nachgeladen.

Wenige Wochen vor der Präsidentschaftswahl in den USA gerät der Hack des US-amerikanischen Social-News-Aggregator **Reddit** in die Schlagzeilen. Auf der Website, auf der registrierte Benutzer Inhalte einstellen bzw. anbieten können, wurden mehrere Konten von Moderatoren diverser Sub-Reddits von Unbekannten gekapert. Offenbar waren diese Konten nicht durch eine Zwei-Faktor-Authentifizierung geschützt. So war es den Angreifern möglich, über diese Konten für die Wiederwahl des amtierenden US-Präsidenten Donald Trump zu werben.

Unbekannte Angreifer haben die Server der einzigen neuseeländischen Börse, **New Zealand Exchange (NZX)**, mit Hilfe von DDoS-Attacken lahmgelegt. Der Handel wurde mehrfach ausgesetzt. Der neuseeländische Geheimdienst wurde eingeschaltet.

(2.174 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