QGroup präsentiert »Best of Hacks«: Highlights November 2020

Frankfurt am Main, 16. Dezember 2020 – Im November erlangte die Aktion eines niederländischen Journalisten große mediale Aufmerksamkeit: Daniel Verlaan verschaffte sich unberechtigt Zugang zu einer Videokonferenz der EU-Verteidigungsminister und zeigte damit einmal mehr auf, wie wichtig ein ganzheitliches IT-Sicherheitskonzept ist.

Dem niederländischen Journalisten Daniel Verlaan gelang es, sich unberechtigt Zugang zu einer Videokonferenz der EU-Verteidigungsminister zu verschaffen. Im Vorfeld hatte die niederländische Verteidigungsministerin Ank Bijleveld über Twitter ein Foto von ihrer Teilnahme an der Konferenz veröffentlichen lassen. Auf diesem Foto waren fünf der sechs Ziffern des Zugangscodes für die Videokonferenz sichtbar. Diese Gelegenheit packte Verlaan beim Schopfe und schmuggelte sich in die Konferenz. Der EU-Außenbeauftragte Josep Borrell bemerkte den unbekannten Teilnehmer, der nach kurzer Aufklärung der Situation die Konferenz wieder verließ.

Mit Hilfe von Social Engineering haben sich unbekannte Angreifer Zugriff auf Zugangsdaten von Mitarbeitern des Domainregistrars und Hosting-Anbieters GoDaddy verschafft. Diese nutzten sie dann, um Attacken auf Kryptogelddienstleister durchzuführen. So erlangten die Täter Kontrolle über eine zentrale Domain der Handelsplattform Liquid und hatten dadurch weiteren Zugang zur Infrastruktur wie etwa dem Dokumentensystem. Auch der Miningdienst Nicehash war von dieser Attacke betroffen.

Advantech, ein Hersteller von Industrie-Computern, wurde Opfer eines Angriffs mit der Ransomware Conti. Dabei handelt es sich um den Nachfolger von Ryuk, dem weltweit Systeme zum Opfer fielen. Die unbekannten Angreifer verlangen für die Herausgabe der verschlüsselten Daten 12,5 Millionen US-Dollar. Es wurden auch Geschäftsdaten kopiert, mit deren Veröffentlichung sie drohen.

Im Internet wurde eine ungeschützte Elasticsearch-Datenbank mit 300.000 Spotify-Zugangsdaten entdeckt. Die Datenbank stammt nicht vom Musikstreamingdienst Spotify selbst, sondern vermutlich von Kriminellen. Es ist anzunehmen, dass die Zugangsdaten über sogenannte Credential-Stuffing-Angriffe erlangt wurden.

(2.203 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