PRESSEMITTEILUNG

QGroup präsentiert Best of Hacks: Highlights Mai 2019

Frankfurt am Main, 30. Juli 2019 - Im Mai gab es erneut politisch motivierte Cyberangriffe der Hamas auf israelische Institutionen. Ebenfalls hatten es Hacker auf sensible Kundendaten unterschiedlicher Unternehmen abgesehen. Auch wurde wieder einmal eine Bitcoinbörse Opfer von Cyberkriminellen.

Nachdem die Hamas einen schweren Cyberangriff auf die Infrastruktur Israels gestartet hatte, sah sich die **Regierung Israels** gezwungen, das Cyber Operations Center der Hamas per Luftangriff zu attackieren. Jedoch gibt die Regierung nicht bekannt, welche Schäden der feindliche Cyberangriff hinterlassen hat oder was das genaue Ziel des Angriffs gewesen ist. In einem Statement der Regierung heißt es lediglich, dass es das Ziel des Angriffs gewesen sei, die Lebensqualität der Israelischen Bürger einzuschränken.

Während der Ausstrahlung des Eurovision Song Contest in Israel hackt die Hamas den Webauftritt des übertragenden Senders **KAN**. Es werden animierte Explosionen gezeigt.

Wieder einmal wird eine Bitcoinbörse erfolgreich von Cyberkriminellen ausgeraubt. Diesmal trifft es die Bitcoinbörse **Binance**. Die Hacker verschaffen sich zunächst Zugriff auf Zugangsinformationen von Kunden und Angestellten, um dann in einem zweiten Schritt Bitcoin im Wert von ca. 41 Millionen Euro abzugreifen.

Der Online-Publisher **WIRED** wurde von Unbekannten gehackt. Die Angreifer hatten im April über mehrere Tage Zugriff zu Kundenkonten und damit auch auf die Bezahlinformationen. Das Magazin hat seine Kunden umgehend über den Vorfall informiert.

Chinesischen Hackern ist es 2016 fast gelungen, eine Hintertür für das Fernwartungsprogramm **TeamViewer** einzubauen. Erst jetzt wurde dieser Vorfall publik. Das Nachrichtenmagazin "Der Spiegel" hatte den Angriff aufgedeckt. Das Unternehmen TeamViewer äußert sich dahingehend, dass eine Veröffentlichung des Angriffs nicht erfolgte, da "größerer Schaden verhindert werden konnte".

Die Nachrichten-App **Flipboard** hatte von Juni 2018 bis April 2019 ungebetene Gäste im System. Hacker hatten sich Zugriff auf die Datenbank des Unternehmens verschafft und konnten in diesem Zeitraum sämtliche Kundeninformationen auslesen. Erst im April hat das Unternehmen den Einbruch bemerkt und seine Kunden umgehend informiert.

Einen Monat nachdem es einen Cyberangriff auf Kundendaten gegeben hatte, wird der IT-Dienstleister **Citycomp Service GmbH** von Unbekannten erpresst. Die Erpresser drohen damit, die erbeuteten Kundendaten zu veröffentlichen, wenn das Unternehmen kein Lösegeld zahlt.

Das Bezahlsystem eines Online-Shops des Premier League Teams **Leicester City FC** wurde von Hackern so präpariert, dass die Bezahlinformationen der Kunden an die Hacker übermittelt wurden.

Medienkontakt:

QGroup GmbH
Phoenix Haus
Berner Straße 119

Bela Schuster
Tel.: +49 69 17 53 63-078
E-Mail: b.schuster@qgroup.de

60437 Frankfurt am Main
www.qgroup.de/presse

(2.644 Zeichen)