QGroup präsentiert »Best of Hacks«: Highlights September 2021

Frankfurt am Main, 11. November 2021 – Beim Thema IT-Sicherheit im Unternehmen gelten die Mitarbeiter als das größte Risiko. Denn sie sind das am leichtesten zu überwindende Einfallstor für hochtechnisierte und spezialisierte Angriffe auf das Unternehmen. Im September zeigen das die Angriffe auf die Vereinten Nationen und auch auf die Webseite und die Telegram-Kanäle von Attila Hildmann.

Unbekannte Angreifer haben im Darknet die Zugangsdaten eines UN-Mitarbeiters erworben. Damit konnten sie sich bei der UN-eigenen Projektmanagementsoftware Umoja einloggen und von dort aus weiter in das Netz der Vereinten Nationen eindringen. Eine Zwei-Faktor-Authentifi–zierung hätte dies verhindern können, war aber nicht vorhanden. Mindestens fünf Monate lang hatten die Angreifer Zugang zum Netz der UN. Ziel war es, weitere Nutzerkonten zu kompro-mittieren, um so an weitere Informationen zu gelangen.

Die Webseite und die Telegram-Kanäle von Attila Hildmann wurden von Hacktivisten über-nommen. Ermöglicht wurde dies durch einen ehemalige IT-Helfer Hildmanns, der sich bei den Angreifern meldete und ihnen etliche Daten und Zugangsdaten übergab. Die Hacktivisten hatten so auch Zugriff auf interne E-Mails des rechtsextremen Verschwörungsideologen und Vegan-Kochs.

Unbekannte Hacker haben die IT-Infrastruktur des SRH Klinikverbunds mit Schadsoftware angegriffen. Als Folge wurden deutschlandweit die Computersysteme an fast einem Dutzend SRH Kliniken sicherheitshalber vom Netz genommen. Betroffen seien auch Hochschulen und andere Bildungseinrichtungen der SRH.

Das gesamte Netzwerk von Südafrikas Justizministerium wurde von Ramsomware verschlüsselt. Alle internen und externen Dienste wurden von diesem Angriff beeinträchtigt. So wurde kein Kindergeld mehr ausgezahlt und die Gerichte mussten Aufnahmen von Verhandlungen manuell abwickeln, auch konnten Dokumente nicht automatisiert versendet werden. Viele behördliche Schreiben wurden entweder nicht oder verspätet verschickt. Daten sollen die unbekannten Angreifer allerdings nicht erbeutet haben.

In Neuseeland haben Unbekannte unter anderem die Webseiten mehrerer Finanzinstitute mit DDoS-Attacken angegriffen und zwangen diese kurzeitig außer Betrieb zu gehen. Betroffen waren auch die neuseeländische Webseite der Australia and New Zealand Banking Group (ANZ.AX) und die NZ Post.

(2.295 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