QGroup präsentiert »Best of Hacks«: Highlights Juli 2021

Frankfurt am Main, 08. August 2021 – Im Juli haben Hacker bei einem der größten Hacker-angriffe der letzten Jahre auf einen Schlag hunderte Unternehmen ins Visier genommen. Letztlich waren bis zu 1500 Unternehmen aus aller Welt betroffen. Dazu zählen unter anderem auch die Schwedische Supermarktkette Coop.

Unbekannte Hacker haben eine Schwachstelle in der Fernzugriffs- und Wartungssoftware VSA des US-amerikanischen Unternehmens **Kaseya** ausgenutzt, um bei deren Kunden die VSA-Server mit Ransomware zu befallen. Kaseya hatte zu diesem Zeitpunkt ca. 36.000 Kunden. Darunter waren auch einige Dienstleister, weshalb es zu einem Dominoeffekt kam und auch deren Kunden teilweise von diesem Cyberangriff betroffen waren. Letztlich wurden so um die 800–1500 Unternehmen aus etwa 17 Ländern Opfer der Cyberattacke.

Die **Landkreisverwaltung Anhalt-Bitterfeld** hat den Katastrophenfall ausgerufen, nachdem ihr Netzwerk durch den Befall von Ransomware zum Großteil lahmgelegt wurde. Nach dem Angriff wurden alle kritischen Systeme vom Netz getrennt, um einen weiteren Datenabfluss zu verhindern. Die Landkreisverwaltung war damit größtenteils nicht arbeitsfähig.
Der Katastrophenfall wurde ausgerufen, weil viele finanzielle Belangen von Bürgern betroffen waren. Darunter fallen etwa die Auszahlung der Sozialhilfe oder die Jugendhilfe. Die Angreifer haben Lösegeld gefordert. Der letzte Katastrophenfall im Landkreis Anhalt-Bitterfeld war im Jahr 2013 wegen des Hochwassers ausgerufen worden. Damit jeder der 900 Computer der Ver-waltung den Sicherheitsvorkehrungen entspreche, wurde ein Hilfsantrag an die Bundeswehr gestellt.

Beim Online-Banking der Commerzbank-Tochter **Comdirect** kam es zu einem Datenleck. Kunden, die sich ihre Kontoumsätze als CSV-Datei exportieren wollten, wurden teilweise die Kontoauszüge anderer Kunden angezeigt. Die Kontoübersicht wurde von Comdirekt daraufhin für einige Stunden abgeschaltet. Betroffene Kunden und die zuständige Datenschutzbehörde wurden informiert.

Durch menschliches Versagen wurden die Daten von 13.000 Bürgern der **Stadt Essen**, die sich für eine Corona-Schutzimpfung angemeldet hatten, per E-Mail an 700 Empfänger versendet. Der Landesdatenschutz wurde daraufhin informiert und die 700 Empfänger wurden gebeten, den Irrläufer zu löschen. Eigentlich sollten die 700 Empfänger lediglich darüber informiert werden, dass sie aufgrund verkürzter Öffnungszeiten einen anderen Termin wahrnehmen sollen. Die Empfänger-Liste wurde aus einer Excel-Datei generiert, allerdings wurden die Daten aus dieser Datei vor dem Absenden der E-Mail nicht wieder entfernt. So wurden Namen, Anschrift und Geburtsdatum, vielfach auch Telefonnummer und E-Mail-Adresse sowie der Impfstatus zahlreicher Bürger weitergegeben.

(2.700 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