QGroup präsentiert »Best of Hacks«: Highlights November 2021

Frankfurt am Main, 31. März 2022 – In den vergangenen Monaten haben Ransomware-Angriffe auf große Unternehmen wiederholt Schlagzeilen gemacht. Dahinter stecken meist gut organisierte Banden. Im November wurden beispielsweise die Media-Markt-Saturn Holding GmbH und der Automobilzulieferer Ebersbächer Opfer solcher Cyberattacken.

Die zur Ceconomy AG gehörende **Media-Markt-Saturn Holding GmbH** wurde Opfer eines Ransomware-Angriffs mit dem Krypto-Virus Hive. Sie betreibt in 13 europäischen Ländern insgesamt rund 1000 Märkte der Ketten MediaMarkt und Saturn. Betroffen waren offenbar 3100 Server und damit die Kassen- und Warenwirtschaftssysteme in den Filialen. Die Mitarbeiter wurden angewiesen, die Kassen vom Netz zu nehmen und Computer nicht zu benutzen. Die Media-Markt-Saturn Holding GmbH betonte, dass die Online-Shops nicht betroffen seien und für die Kunden kein Handlungsbedarf bestünde. Die unbekannten Erpresser forderten laut einem Medienbericht 50 Millionen US-Dollar in Bitcoin, um die verschlüsselten Daten wieder freizugeben.

Unbekannten Angreifern ist es gelungen, E-Mails von einem Konto auf Servern des **US Federal Bureau of Investigation (FBI)** zu verschicken. Insgesamt wurden mehr als 100.000 gefälschte Warn-E-Mails verschickt. Die betroffene Hardware wurde vom FBI umgehend vom Netz genommen. Das FBI forderte die Öffentlichkeit auf, weiterhin vorsichtig gegenüber unbekannten Absendern in Mails zu sein. Mittlerweile hat ein Hacker namens "Pompompurin" zu dem Angriff bekannt, der mit der Aktion scheinbar einen Hinweis auf eine schwere Coding-Lücke beim FBI geben wollte. Über das Law Enforcement Enterprise Portal (LEEP) war demnach ein illegaler Zugriff auf das E-Mail-System des FBI möglich, da bei der Registrierung eines Nutzerzugangs ein Passcode im HTML-Code der Webseite weitergegeben wurde. Somit reichte dem Angreifer ein kleines Script, um über diesen Mechanismus Tausende Mails über Server des FBI zu versenden. Diese Möglichkeit wurde mittlerweile vom FBI abgeschaltet.

Auch der schwedische Einrichtungskonzern **Ikea** ist ins Visier von Cyberkriminellen gerückt. Die Angreifer hatten sich Zugang zu den Microsoft-Exchange-Servern des Unternehmens verschafft, indem sie die Schwachstellen ProxyShell und ProxyLogin für Phishing-Angriffe ausnutzten. Daraufhin wurden von kompromittierten E-Mail-Konten Nachrichten an Mitarbeiter von Ikea verschickt, die vermeintlich Antworten auf eine bereits laufende Mailkommunikation waren. Diese waren mit Malware enthaltenden Links oder Anhängen versehen. Das Unternehmen forderte seine Mitarbeiter daraufhin auf, E-Mails, die am Ende eines Links sieben Zahlen enthalten, nicht zu öffnen und an die IT-Abteilung zu melden – auch, wenn sie von vertrauenswürdigen Absendern stammen. Es gab allerdings keine Hinweise darauf, dass Kundendaten kompromittiert wurden.

Die Eberspächer Gruppe GmbH & Co. KG wurde ebenfalls Opfer eines Hackerangriffs. Teile der Produktion und Verwaltung des baden-württembergischen Autozulieferers wurden durch einen Ransomware-Angriff lahmgelegt. Auch die Webseite des Unternehmens war nach dem Angriff nicht mehr erreichbar. Nachdem die Fertigung an allen neun deutschen Standorten vorübergehend stillstand, vermeldete das Unternehmen nach knapp zwei Wochen, dass die meisten Werke Kunden wieder beliefern würden. Weitere Details zum Angriff nannte das Familienunternehmen nicht.

Medienkontakt:

QGroup GmbH
Berner Straße 119
60437 Frankfurt am Main

Lars Bothe
Tel.: +49 69 17 53 63-014
E-Mail: l.bothe@qgroup.de

www.qgroup.de/presse