QGroup präsentiert »Best of Hacks«: Highlights Dezember 2020

Frankfurt am Main, 1. Februar 2021 – Seit im Dezember erstmals über den SolarWinds-Hack berichtet wurde, wird die Liste der betroffenen Unternehmen und Institutionen immer länger und internationaler. Der Hack gilt als historisch. Doch auch weitere Cyberattacken machen zum Jahresende von sich reden.

SolarWinds ist ein auf Netzmanagement-Software spezialisiertes US-amerikanisches Unternehmen. Das Pentagon, das US-Außenministerium, das US-Justizministerium, die Nasa sowie insgesamt 18.000 weitere Organisationen, Behörden und Unternehmen nutzen weltweit eine IT-Management-Software von SolarWinds. Diese Software wurde über den Update-Server von SolarWinds mit Schadcode kompromittiert. Dabei wurde der Trojaner Sunburst verteilt.
Der Angriff wird der russischen Hackergruppe APT29, auch Cozy Bear genannt, zugeordnet.
Zu Kunden von SolarWinds zählen unter anderem auch Unternehmen wie AT&T, Cisco, Mastercard, Microsoft und Siemens. Ein wichtiges Produkt von SolarWinds ist die Orion Platform, eine skalierbare Überwachungs- und Verwaltungsplattform für die gesamte IT-Infrastruktur. Dies ist für Hacker ein attraktives Angriffsziel, da es den Zugang zu den Netzwerken der Kunden ermöglicht.

Unbekannte Hacker haben das US-amerikanische Security-Unternehmen FireEye angegriffen und Hacking-Werkzeuge des Unternehmens gestohlen. Auch versuchten sie, Kundendaten zu stehlen. Zu den Kunden des börsennotierten Unternehmens mit Sitz in Milpitas, Kalifornien, zählen unter anderem auch US-Behörden. Die Angreifer nutzen ungewöhnliche Kombinationen von Angriffswerkzeugen, die teilweise bisher in dieser Form noch nicht in Erscheinung getreten sind. Es wird vermutet, dass die Angreifer im Auftrag des russischen Geheimdienstes handelten.

Die Funke Mediengruppe mit Sitz in Essen war Ziel eines Hackerangriffs. Sämtliche Systeme wurden von außen verschlüsselt, weshalb die gesamte IT heruntergefahren werden musste. Die Attacke hatte Auswirkungen auf die Produktion sämtlicher Tageszeitungen, die von der Funke Mediengruppe herausgegeben werden. Als Folge des Angriffs wurden im Printbereich nur Notausgaben veröffentlicht und die Paywall für E-Paper der Mediengruppe deaktiviert.

Bei einem Cyberangriff auf die Europäische Arzneimittel-Behörde EMA in Amsterdam haben unbekannte Hacker Daten der Pharmaunternehmen Pfizer und Biontech gestohlen. Es handelt sich dabei unter anderem um Dokumente, die im Zusammenhang mit dem Antrag der beiden Unternehmen auf Zulassung ihres Impfstoffs gegen das Corona-Virus stehen.

(2.474 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