PRESSEMITTEILUNG

QGroup präsentiert Best of Hacks: Highlights Dezember 2018

Frankfurt am Main, 15. Februar 2019 - Im Dezember wird publik, dass chinesische Hacker scheinbar jahrelang Regierungsbehörden und Technologieunternehmen ausspioniert haben. Ebenfalls kommt ans Tageslicht, dass die Regierung Tschechiens seit 2016 von russischen Spionen gehackt wurde und dass die Charity Organisation Save the Children an einen Internetbetrüger eine Million Euro verloren hat.

US-Behörden zufolge hat eine chinesische Hackergruppe, die in der Szene als APT10 (Advanced Persistent Threat 10) bekannt ist, jahrelang im Auftrag der chinesischen Regierung weltweit **Regierungsbehörden** und **Technologieunternehmen** ausspioniert. Die Hacker hätten Schadsoftware platziert und Daten abgefischt. Zwischen 2006 bis 2018 seien so bei Behörden und Unternehmen aus unterschiedlichen Branchen in mindestens zwölf Ländern Hunderte Gigabyte mit heiklen Daten gestohlen worden. Neben großen Technologieunternehmen wie **HPE** und **IBM** seien Firmen aus zahlreichen Branchen von den Attacken betroffen, darunter Autozulieferer, Hersteller von Laborinstrumenten, der Banken- und Finanzsektor sowie Firmen aus den Bereichen Telekommunikation, Informationstechnologie, Medizinausrüstung, Biotechnologie, Pharma, Bergbau, Öl- und Gasförderung, Luftfahrt und Weltraumforschung.

Die **Regierung Tschechiens** gibt bekannt, dass sich russische Spione angeblich in mehrere Netzwerke der Regierung gehackt haben. Die Angreifer sollen sich seit 2016 im Netzwerk aufgehalten haben. Die Spione sollen Teil der Hackergruppe Turla und APT28 (Fancy Bear) sein.

Ein Kommunikations-Netzwerk der **Europäischen Union** wurde vermutlich jahrelang von chinesischen Hackern ausspioniert. Die New York Times berichtete von dem Vorfall. Demnach seien streng vertrauliche Dokumente auslesbar gewesen. Darunter auch Dokumente zur Einschätzung der weiteren Zusammenarbeit mit US-Präsident Donald Trump sowie ein Bericht, der andeutet, dass Russland Atomwaffen auf der Krim stationiert hat. Die Angreifer haben durch eine im Kommunikations-Netzwerk platzierte Malware immer wieder Dokumente kopiert.

Ein Mitarbeiter der Charity Organisation **Save the Children** erhält eine E-Mail mit der Anweisung, eine Million Euro an ein angegebenes Konto zu überweisen. Im Anhang der E-Mail befinden sich angeblich offizielle Dokumente, die die Überweisung genehmigen und bestätigen. Für den Mitarbeiter scheint alles ganz normal. Es ist nicht die erste Überweisung mit einem solch hohen Betrag, die von ihm durchgeführt werden soll. Später fragt sich die Führungsetage, warum der Organisation eine Million Euro fehlen und warum in Pakistan kein Geld für eine Solaranlage angekommen ist. Schnell wird klar, dass die Organisation Opfer eines Internetbetrügers geworden ist. Der Mitarbeiter hatte eine Million Euro auf ein privates Konto in Japan überwiesen. Der Betrug erfolgte bereits im Mai 2017, die Details wurden allerdings erst viel später veröffentlicht.

Wie das Bundesamt für Sicherheit in der Informationstechnologie (BSI) bestätigte, wurde der in München ansässige Maschinenbaukonzern **KraussMaffei Group** von Hackern angegriffen. Die Angreifer legten dabei mehrere Rechner lahm und versuchten ein Lösegeld zu erpressen. KraussMaffei ging auf die Forderungen nicht ein. Als Folge des Angriffs musste die Produktion an mehreren Standorten gedrosselt werden.

Medienkontakt:

QGroup GmbH Bela Schuster

Phoenix Haus
Berner Straße 119
60437 Frankfurt am Main
www.qgroup.de/presse

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

(3.267 Zeichen)