PRESSEMITTEILUNG

QGroup präsentiert Best of Hacks: Highlights März 2018

Frankfurt am Main, 29. Mai 2018 - Im März fanden die Präsidentschaftswahlen in Russland statt und somit rückte auch die Regierung Russlands in das Visier von Hackern. Darüber hinaus werden Vorfälle von Cyberspionage im Nahen Osten sowie in Ostafrika bekannt und auch Cyberattacken auf türkische Finanzdienstleister.

Anlässlich der Präsidentschaftswahl in Russland rückt die **Regierung Russlands** in den Fokus von Hackern. Im März greifen sie die Webseiten der Wahlkommission und des Militärs mit DDoS-Attacken an. Um ihren Unmut über die Wahl deutlich zu machen, greifen die Hacker nicht ein- oder zweimal an, sondern starten insgesamt sieben Angriffe. Doch auch diese konnten die Wiederwahl von Putin nicht verhindern.

Kaspersky Lab warnt vor einer hoch entwickelten Form der Cyberspionage, die bereits seit 2012 im **Nahen Osten sowie in Ostafrika** verbreitet ist. Die Malware Slingshot attackiert und infiziert die Systeme ihrer Opfer über kompromittierte Router. Informationen werden heimlich und effektiv ausgespäht, indem der entsprechende Netzwerkverkehr in Datenpaketen versteckt und ohne Spuren zu hinterlassen wieder aus dem regulären Datenstrom ausgelesen werden kann. Unter den Opfern befinden sich, bis auf eine Regierungseinrichtung, fast nur Einzelpersonen.

Experten von McAfee berichten, dass die nordkoreanische Hackergruppe Hidden Cobra **Institutionen des türkischen Finanzsektors** infiltrieren wollte. Mit einer breit angelegten Phishing-Kampagne versuchten die Hacker, Zugang zu sensiblen Netzwerken zu erlangen.

Der italienische Fußballclub **Lazio Rom** fällt auf eine E-Mail von Betrügern ein. Die E-Mail, die angeblich vom niederländischen Club Feyenoord Rotterdam stammt, forderte Lazio Rom auf, einen offenen Betrag aus dem Transfer von Stefan de Vrij in Höhe von 2 Millionen Euro auf ein Konto in den Niederlanden zu überweisen. Gesagt, getan. Die Italiener überweisen das Geld und stellen eine Woche später fest, dass der Feyenoord Rotterdam kein Geld erhalten hat. Die Betrüger sind zu diesem Zeitpunkt längst über alle Berge.

Ein Standort von **Boeing** in den USA (South Carolina) hat es verpasst, rechtzeitig seine Windows-Systeme zu updaten. Die Konsequenz ist, dass die berüchtigte Malware WannaCry das System infiziert und Benutzerdateien verschlüsselt hat.

Der US-Sportartikelhersteller **Under Armour** hat einen Hackerangriff auf seine Kalorienzähler-App "MyFitnessPal" bekannt gegeben. Die Attacke betrifft etwa 150 Millionen Nutzerkonten. Die Angreifer konnten Nutzernamen, E-Mail-Adressen und Passwörter erbeuten. Persönlichere Informationen sind nicht in Gefahr, da die App diese nicht abfragt.

Fortnite, ein neues und aktuell beliebtes Online-Spiel für den PC und die Konsole, weist Sicherheitslücken auf. Für einige Spieler, die ihre Kreditkarteninformationen angegeben haben, um Erweiterungen zu kaufen, sind für das eigentlich kostenfreie Spiel erhebliche Kosten angefallen. Grund hierfür sind Hacker, die Accounts gekapert und darüber Einkäufe getätigt haben.

Die **UK National Lottery** informiert sämtliche angemeldeten Kunden darüber, dass Hacker an Login-Informationen gelangt sind. Daher werden die Kunden gebeten, umgehend alle ihre Passwörter zu ändern.

Medienkontakt:

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

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

(3.143 Zeichen)