PRESSEMITTEILUNG

QGroup präsentiert Best of Hacks: Highlights Oktober 2017

Frankfurt am Main, 15. Dezember 2017 – Im Oktober wird publik, dass die Anwaltskanzlei Appleby gehackt und vertrauliche Daten der Süddeutschen Zeitung zugespielt und weltweit von Journalisten ausgewertet wurden – die sogenannten „Paradise Papers". Daneben haben es Cyberkriminelle wieder vermehrt auf sensible Nutzerdaten abgesehen. In den Fokus rücken auch Fast-Food-Ketten wie Pizza Hut und Domino's Pizza oder Schönheitskliniken.

The Register berichtet, dass die auf den Bermudas beheimatete Anwaltskanzlei **Appleby** gehackt worden sei. Appleby ist führendes Mitglied des „Offshore Magic Circle", eines weltweiten Netzwerks von Rechtsanwälten, Beratern und anderen Managern, die Firmen in Steueroasen betreuen. Der Hack soll bereits im letzten Jahr passiert sein. Erst auf Nachfrage einer Gruppe von Journalisten hat die Kanzlei den Hack bestätigt. Bei diesem Angriff wurden extrem sensible Daten erbeutet, deren Veröffentlichung die sogenannten „Paradise Papers" erst ins Rollen gebracht haben. Denn mit rund 6,8 Millionen Dokumenten stammt ein Großteil der Daten, die im Rahmen der „Paradise Papers" ausgewertet wurden, aus dieser Kanzlei.

Forrester Research, eines der weltweit führenden Marktforschungs- und Investitionsberatungsunternehmen, wurde Opfer eines Cyberangriffes. Am Freitag teilte Steven Peltzman, Forresters Chief Business Technology Officer, mit, dass ein oder mehrere Hacker die Benutzer-Anmeldeinformationen für den Webseitenzugang auf die für Kunden bereitgestellten Forschungsergebnisse gestohlen haben.

Russische Hacker wurden dank der Malware-Analyse von **Kaspersky** dabei beobachtet, wie sie auf einem PC NSA-Material entdeckt und an sich gebracht haben. Laut einem Bericht der New York Times war Kaspersky von israelischen Agenten infiltriert, die die NSA umgehend alarmierten.

Ein im Jahr 2013 durchgeführter Hackerangriff auf **Microsoft** hat fatale Auswirkungen: Fünf Microsoft Mitarbeiter, die anonym bleiben wollen, geben an, dass damals eine Datenbank von Microsoft angegriffen wurde, in der das Unternehmen Informationen zu Schwachstellen in eigenen Programmen gespeichert hatte. Der Besitz dieser Lücken ermöglichte es den Hackern im Gegenzug, Microsoft-Nutzer weltweit auszuspionieren.

Das Hackerkollektiv Anonymous schaltet sich mal wieder in einen politischen Konflikt ein. Diesmal steht die **Regierung Spaniens** im Fokus. Unter dem Banner #OpCatalunya greifen die Hacker die Webseiten der spanischen Ministerien für Transport und öffentliche Arbeit per DDoS Attacke an.

Zwei Webseiten des Statistik Office des **Parlaments der Tschechischen Republik** wird angegriffen, um die Zahlen der Wählerstimmen bei der Parlamentswahl zu beeinflussen.

Das Wallstreet Journal berichtet, dass russische Hacker das **US-Ministerium für nationale Sicherheit** gehackt und dabei sensible Daten erbeutet haben. Bei den Daten handelt es sich wohl um Strategien zu Cyber-Attacken und zur Cyber-Defensive.

Palo Alto Networks berichtet, dass die APT-Gruppe OilRig **regierungsnahe Organisationen der Vereinigten Arabischen Emirate** angreift.

Unbekannte greifen das **schwedische Ministerium für Transport** per DDoS Attacke an.

Das Handy des Stabschefs des Weißen Hauses, **John Kelly**, wurde komprimiert. Offizielle glauben, dass der Angriff bereits seit Dezember 2016 unbemerkt blieb.

Laut einem Bericht des Wallstreet Journals hacken russische Hacker 4.000 Handys von **NATO** Soldaten.

Hacker greifen die **Far Eastern International Bank** in Taiwan an und erbeuten 500.000 Dollar. Die mutmaßlich aus Nordkorea stammenden Hacker wollten ursprünglich eine Beute in Höhe von 60 Millionen Dollar machen, jedoch gelang es der Bank bis auf 500.000 Dollar alles sicherzustellen.

Forscher von Skyhigh Networks haben einen neuen Cyber-Angriff von KnockKnock, einem bisher unbekannten Botnet, aufgespürt. Dabei handelt es sich um einen komplexen Angriff auf Exchange-Online-Konten als Bestandteil von **Office 365**. Die Attacken gingen von insgesamt 16 Ländern aus. Im Visier der Angreifer sind vor allem automatisierte E-Mail-Accounts, die nicht mit einer bestimmten Person verknüpft sind und in der Regel nicht den strengen Sicherheitsrichtlinien der Unternehmen unterliegen.

Schönheitskliniken rücken immer öfter ins Visier von Hackern. The Dark Overlord brüstet sich damit, die **London Bridge Plastic Surgery** gehackt zu haben. Dabei hat nicht nur sensible Daten zu Patienten erbeutet, sondern auch OP-Bilder.

FireEye berichtet, dass nordkoreanische Hacker **US-Stromkraftwerke** ins Visier nehmen und Angriffe mit spearphishing E-Mails starten.

Die **Hyatt Hotels Corp.**, eine der weltweit größten Hotelketten mit Firmensitz in Chicago, meldet, Opfer eines Hacker-Angriffs geworden zu sein. Die Angreifer hatten es auf das Bezahlsystem abgesehen, das sie mit POS Maleware infizierten, um Bezahlinformationen von Kunden zu erbeuten.

Bithumb, eine der größten Krypto-Wechselbörsen, wird gehackt. Insgesamt sind rund 30.000 Kunden von dem Angriff betroffen.

Nutzer von **Netflix** geraten ins Visier von Hackern. Es wurde versucht, die Konten zu komprimieren, um Profit zu erzielen.

Die Fast-Food-Kette **Pizza Hut** hat einen Cyber-Einbruch zu beklagen. Die Hacker stehlen Kreditkarteninformationen von einigen Kunden. Jedoch soll die Zahl der betroffenen Kunden laut Pizza Hut nicht sehr hoch sein.

Nachdem Hacker in das Computersystem von **Domino's Pizza** eingebrochen sind, erhalten viele Kunden Spam-E-Mails.

Nachdem sich Hacker eine Sicherheitslücke auf der Webseite von **T-Mobile** zu Nutze machen, warnt das Unternehmen seine Kunden davor, dass die Hacker versuchen, die Kontrolle über Sim-Karten zu erlangen.

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

(5.551 Zeichen)