PRESSEMITTEILUNG

QGroup präsentiert Best of Hacks: Highlights Januar 2016

Frankfurt am Main, 23. März 2016 – Im Januar geraten im Zuge der bevorstehenden Wahlen in Amerika neben Präsidentschaftsanwärter Donald Trump auch hohe US-amerikanische Funktionsträger ins Visier von Hackern. Sensible Daten stehen weiterhin hoch im Kurs im Bereich der Cyberkriminalität, aber der Hack beim Flugzeugteilehersteller FACC zeigt, dass Unternehmen auch um ihre Finanzen fürchten müssen.

Die Hacker von New World Hacktivists hacken die Website donaldjtrump.com von **Donald Trump**. Die Seite ist daraufhin temporär nicht erreichbar. Die Hackergruppe zeigt sich auch verantwortlich für die Hacks der BBC Website an Silvester.

Nachdem die Crackas With Attitude (CWA) bereits im Vorjahr die Kontrolle über den E-Mail-Account von CIA Direktor John Brennan erlangt haben, schlagen die Teen-Hacker nun wieder zu. Diesmal leiten sie alle an **National Intelligence Chef James Clapper** eingehenden Anrufe an das "Free Palestine Movements" weiter.

Crackas with Attitude behaupten, die Kontrolle über alle privaten Kommunikationsmittel von **Obamas Berater für Wissenschaft und Technologie, John Holdren**, erlangt zu haben. Genau wie beim letzten Hack, dem der CIA Chef zum Opfer fiel, leiten die Hacker alle Anrufe an die private Telefonnummer von Holdren an das Free Palestine Movement weiter. Der Vorfall gilt als besonders peinlich, da Cybersecurity durchaus ein Thema ist, mit dem ein Berater für Technologie vertraut sein sollte.

Beim US-amerikanischen Cloud-Service-Anbieter **Linode** führt eine Langzeit DDos-Attacke zu einem Datenleck. Sensible Daten wie Benutzernamen, E-Mail-Adressen und Passwörter gehen verloren. Linode muss einen kompletten Passwort Reset in die Wege leiten.

Ein Hacker, der sich „Lorde Bashtien" nennt, verschafft sich Zugriff auf sensible Informationen der **Polizei von Miami**. Persönliche Informationen von 80 Polizeibeamten werden veröffentlicht. Das Miami Police Department, die Miami-Dade Police und die Miami Beach Police sind betroffen.

Hacker, die sich „Anonymous Conservative" nennen, defacen **2016iowacaucus.com**. Die Website zeigt Besuchern vorübergehend eine Nachricht der Hacker sowie ein Video gegen den Präsidentschaftskandidaten Donald Trump an. Der Hack wurde durch positive Aussagen über Trumps Kandidatur von Sarah Palin, der Gouverneurin von Alaska, ausgelöst.

Die Finanzabteilung des Flugzeugteileherstellers **FACC** wird von unbekannten Hackern angegriffen. Die unbekannten Hacker haben nicht wie üblich sensible Firmendaten im Visier, sondern erbeuten 50 Millionen Euro. Bei Veröffentlichung dieser Tat fiel der Aktienkurs von FACC um 17 %.

Unter dem Bannern #OpSaudi und #OpNimir zeigte Anonymous seinen Unmut über die Hinrichtigungen in Saudi Arabien, die kürzlich stattfanden. Gleich mehrere wichtige Websiten der **saudi-arabischen Regierung** werden lahmgelegt. Insbesondere die Seite des Verteidigungsministeriums ist für zwei Tage nicht erreichbar.

McAffe berichtet von einer neuen Masche, durch die **chinesische Bankkunden** unbekannten Hackern zum Opfer gefallen sind. Den Opfern werden dabei Phishing-SMS zugesendet, in denen

ein Link enthalten ist. Wird dieser Link angeklickt, kommen die Angreifer problemlos an die Login-Daten der Kunden.

Unbekannte Angreifer benutzen bei einer neuen Betrugsmasche private Dell-Kundendaten. Das legt den Verdacht nahe, dass bei **Dell** ein Datenleck vorliegt.

Bei **Interixon** fand ein Datenverlust im Costumer-Relationship-Managment System (CRM) statt. Davon könnten 23.200 Benutzer des Dienstes betroffen sein.

Das Hackerkollektiv Anonsec behauptet, in das Netzwerk der **NASA** eingedrungen zu sein. Angeblich wurde die Kontrolle über eine Drohne gewonnen und auf private Daten von Mitarbeitern zugegriffen. Die Hacker beschreiben online ihre vorgehensweise bis ins Detail hinein. Die Motivation hinter dem Hack scheint die reine „Freude am hacken" zu sein. NASA streitet jedoch vehement ab, dass der Hack je stattgefunden hat.

Der Hacker „Black-Sky" veröffentlicht kostenlos für alle verfügbar die Daten von 5.108 Usern der russischen **Toyota**-Website (Toyota.ru) auf der Website pasted.co.

Die ukrainischen Behörden entdecken einen Angriff auf den **Flughafen von Kiew** von russischen Servern aus. Die Angriffe sorgen für eine Überprüfung aller Verteidigungssysteme der ukrainischen Regierung. Im Dezember kam es bereits zu einem Blackout in ukrainischen Städten, der ebenfalls von russischen Hackern ausgelöst wurde. Eine Verbindung zur russischen Regierung konnte jedoch nicht festgestellt werden.

Die belgische Bank **Crelan** wird Opfer einer Betrugsmasche. Den Betrügern gelingt es 70 Millionen Euro zu erbeuten. Die Angreifer erlangten Zugriff durch einen BEC (Business E-Mail Compromise).

Die Website (faithless.co.uk) der britischen Band **Faithless** wurde bereits im September letzten Jahres gehackt, die Betreiber gaben dies aber erst im Januar diesen Jahres bekannt. Bei dem Angriff wurden persönliche Daten von 18.000 britischen Fans gestohlen.

Medienkontakt:

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

Dirk Kopp
Tel.: +49 69 17 53 63-014
E-Mail: d.kopp@qgroup.de

(4.878 Zeichen)