QGroup präsentiert »Best of Hacks«: Highlights Januar 2020

Frankfurt am Main, 26. Februar 2020 – Die Ursache von Datenlecks sind oftmals nur fehlerhaft gesetzte Sicherheitsregeln. Doch das Gros der Sicherheitslücken wird von cyberkriminellen Angriffen verursacht – im Januar unter anderem beim Chemiekonzern Lanxess, dem österreichischen Außenministerium und der Stadt Potsdam.

Fehlerhaft gesetzte Sicherheitsregeln ermöglichten den Zugriff auf eine Datenbank von **Microsoft** über das Internet. In dieser Datenbank befanden sich 250 Millionen Supportfälle des internationalen Hard- und Softwareentwicklers, die unter anderem sensible Kundendaten wie E-Mail-Adressen, aber auch vertrauliche interne Notizen von Microsoft-Support-Mitarbeitern enthielten.

Im Netzwerk von **Lanxess** wurde eine Spionagesoftware entdeckt, die wohl eigens für den Einsatz beim Kölner Chemiekonzern konzipiert wurde. In welchem Umfang darüber Daten abgeflossen sind, ist nicht bekannt.

Das Netzwerk des **Außenministeriums von Österreich** sieht sich seit Wochen Hackerangriffen aus Russland ausgesetzt. Sämtliche Gegenmaßnahmen konnten den Cyberangriff bisher nicht vollständig abwehren oder gar beenden. Erschwert wird dies durch die Tatsache, dass das Netzwerk laut Ministerium in Betrieb bleiben muss, da zahlreiche Vertretungen des Landes in der ganzen Welt darüber vernetzt seien.

Nachdem bei Netzzugängen Ungereimtheiten auftraten, hat die **Stadt Potsdam** ihre Server vom Netz genommen. Die Stadtverwaltung war während dieser Zeit nicht per E-Mail erreichbar. Unbekannte Angreifer haben scheinbar versucht, Daten von den Servern abzurufen und einen Schadcode hochzuladen.

Medienkontakt:

QGroup GmbH
Berner Straße 119
60437 Frankfurt am Main
www.qgroup.de/presse
(1.860 Zeichen)

Lars Bothe
Tel.: +49 69 17 53 63-014
E-Mail: l.bothe@qgroup.de