Die Presse 25.10.2018
Erscheinungsland: Österreich | Auflage: 70.217 | Reichweite: 315.000 (4,2) | Artikelumfang: 51.495 mm² Seite: 21 1/2

Thema: Anwaltskanzlei PHH Wien
Autor: CHRISTINE KARY

Was tun nach einem Hackerangriff?

Cybercrime. Facebook erlebt es gerade: Wer Ziel einer Hackerattacke wird, kann leicht auch ins Visier der Datenschutzbehörde kommen. Hat man Regeln nicht eingehalten, wird es teuer.

VON CHRISTINE KARY

Wien. Vor rund einem halben Jahr der Skandal um die illegale Weitergabe von Nutzerdaten an die britische Analysefirma Cambridge Analytica, kürzlich ein spektakulärer Hackerangriff auf 50 Millionen Nutzerprofile: Facebook hat schon ruhigere Zeiten erlebt. Die Hackerattacke beschäftigt nun auch die Behörden. Die irische Datenschutzkommission prüft, ob sich Facebook an alle Regeln der Datenschutz-Grundverordnung (DSGVO) gehalten hat. Wenn nicht, drohen zusätzlich zum Imageverlust Schadenersatzforderungen und schlimmstenfalls eine Milliardenstrafe. Wobei es nicht nur auf hinreichende Präventionsmaßnahmen ankommt, sondern auch auf das Verhalten nach der Attacke. Das wirft auch für andere Unternehmen Fragen auf: Was muss man tun, wenn man gehackt wurde? Wem muss was gemeldet werden? Und was kann man zur Aufklärung eines Hackerangriffs beitragen?

„Wurden personenbezogene Daten natürlicher Personen z. B. gestohlen, geändert oder gelöscht, muss man das der Datenschutzbehörde melden und die Betroffenen benachrichtigen", sagt Rechtsanwalt Mathias Preuschl zur „Presse". Und das innerhalb eines schmalen Zeitfensters: Für die Meldung an die Behörde hat man 72 Stunden Zeit, eine Verspätung muss man begründen. Auch die Betroffenen sind „unverzüglich" zu informieren. Das wird in der Hektik oft übersehen – oder man schiebt es wegen des drohenden Imageschadens auf die lange Bank, in der Hoffnung, dass sich vielleicht doch noch alles als halb so schlimm herausstellt. Das kann sich jedoch als fataler Fehler erweisen.

Info an jeden Betroffenen

Es reicht auch nicht, einfach eine Warnung auf der eigenen Homepage zu platzieren. Die Datenschutzbehörde ist immer direkt zu kontaktieren, die betroffenen Personen grundsätzlich ebenfalls, sagt Preuschl. Nur ausnahmsweise – wenn die unmittelbare Verständigung mit einem unverhältnismäßigen Aufwand verbunden wäre – reicht für die Information der Betroffenen auch eine leicht zugängliche öffentliche Bekanntmachung, etwa über eine Website.

In jedem Fall muss die Information einfach und verständlich verfasst sein und eine Reihe von Informationen enthalten: Art der Datenverletzung, wahrscheinliche Folgen des Datenlecks, zur Schadensbegrenzung getroffene Maßnahmen, Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Ansprechperson. In der Meldung an die Behörde müssen zusätzlich – so weit wie möglich – die betroffenen Datenkategorien und die ungefähre Anzahl der betroffenen Personen und Datensätze angegeben werden.

Ersparen kann man sich die Meldung an die Behörde nur dann, wenn durch den Hackerangriff kein Risiko für die Rechte Dritter entstanden ist. Besteht kein „hohes" Risiko, kann laut DSGVO die Information der Betroffenen unterbleiben. Das ist vor allem dann der Fall, wenn die von der Verletzung betroffenen personenbezogenen Daten so gesichert sind, dass Unbefugte damit nichts anfangen können. Auch wenn „der Verantwortliche durch nachträgliche Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Person aller Wahrscheinlichkeit nach nicht mehr besteht", muss keine Verständigung erfolgen. Das in kurzer Zeit abzuschätzen, kann allerdings schwierig sein.

Dokumentationspflichten

Mit der Einhaltung der Meldepflicht ist es für die Unternehmen jedoch nicht getan: „Laut DSGVO müssen sie sämtliche Datenschutzverletzungen, damit zusammenhängende Fakten, Auswirkungen und ergriffene Abhilfemaßnahmen dokumentieren", sagt Preuschl und weist auch auf die weiteren Dokumentationspflichten hin, insbesondere zur Führung eines Datenverarbeitungsverzeichnisses. All das diene der Überprüfung der Einhaltung der Datenschutzbestimmungen, solle aber auch die Strafverfolgung allfälliger Täter erleichtern. „Je besser die Dokumentation, desto höher die Chance, dass Hacker letztlich verurteilt werden können", sagt er.

Die Wahrscheinlichkeit, die Täter auszuforschen, hält sich dennoch in Grenzen. Preuschl nennt als Beispiel die immer häufigere Praxis, dass Kriminelle „Lösegeld" für von ihnen gesperrte Daten verlangen, und das oft in Bitcoin. Besonders in letzteren Fällen sei die Wahrscheinlichkeit, die Hacker zu entlarven, eher gering – und übrigens auch die Chance, tatsächlich seine Daten zurückzubekommen, wenn man zahlt. Auch sonst sei im Allgemeinen „davon abzuraten, geforderte Summen zu bezahlen", wenn man das auch in jedem Einzelfall abwägen müsse.

Jedenfalls ratsam sei es aber, die Polizei einzuschalten: „In manchen Fällen hat sie bereits Kenntnis von den Programmen und Vorgangsweisen der Hacker." Das erhöht dann die Wahrscheinlichkeit, dass sich der Schaden an den Daten beheben lässt.

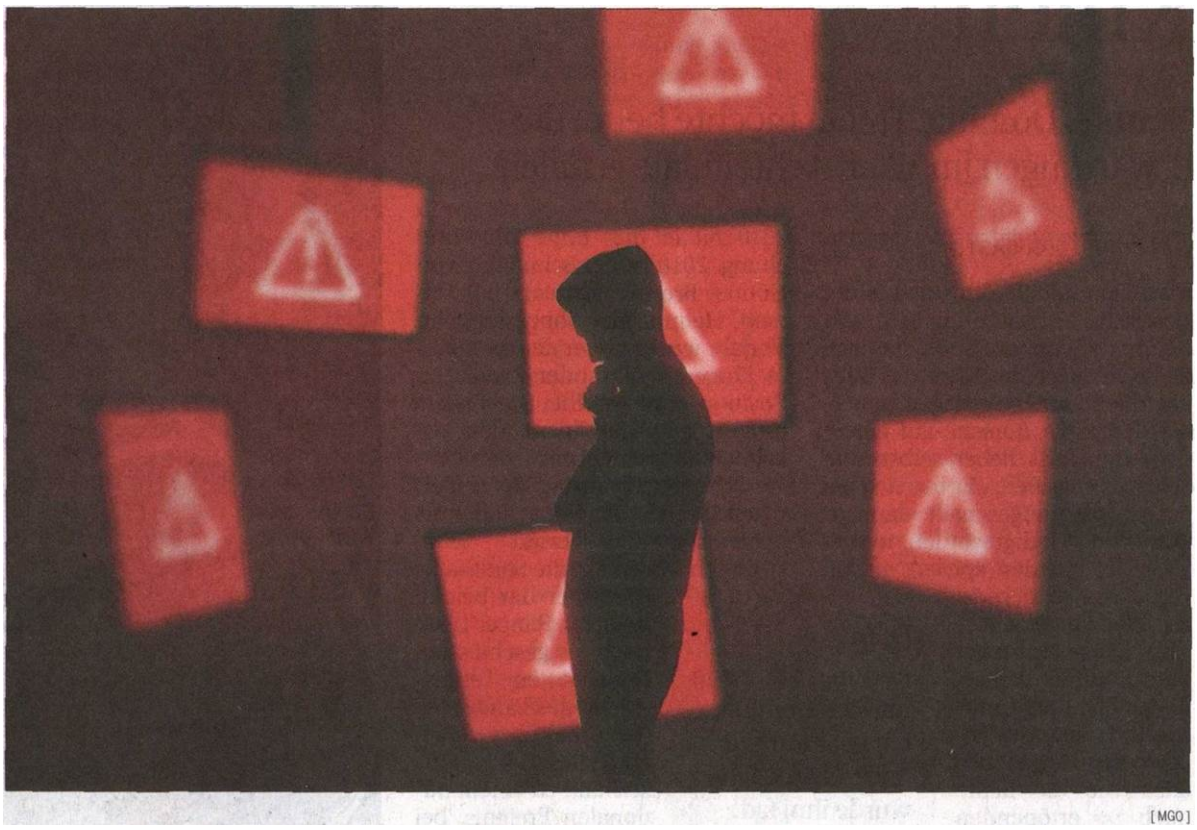
ZUR PERSON

Mathias Preuschl ist Partner bei PHH Rechtsanwälte. Zu seinen Schwerpunkten zählen Wirtschaftsstrafrecht und Compliance, unter anderem ist er auch Vorsitzender des Arbeitskreises IT und Legal Tech des Österreichischen Rechtsanwaltskammertags (Örak). In der Kanzlei PHH fand am 23. Oktober 2018 eine Podiumsdiskussion zum Thema Cybercrime statt.

Die Presse **25.10.2018**
Erscheinungsland: Österreich | Auflage: 70.217 | Reichweite: 315.000 (4,2) | Artikelumfang: 51.495 mm² Seite: 21 2/2

Thema: Anwaltskanzlei PHH Wien

Autor: CHRISTINE KARY



[MGO]