Wer gehackt wurde, muss eine weite Haftung befürchten

Cyber Security. Ob Patienten- oder Kundendaten: Hacker-Attacken werfen viele juristische Fragen auf.

VON GEORG KRESBACH

[WIEN] Erst vergangene Woche veröffentlichte Anonymous Austria, ein loser Zusammenschluss von österreichischen „Hacktivisten", auf ihrem Twitter-Account einen Link zu den Daten von rund 25.000 Exekutivbeamten mit Vornamen, Nachnamen, Adresse und Geburtsdatum. Nur wenige Tage später gab die Gruppierung bekannt, 600.000 Datensätze der Tiroler Gebietskrankenkasse erlangt zu haben. In beiden Fällen sind die Quellen der Daten unbekannt.

Cyber Security und das mit Sicherheitsverletzungen verbundene rechtliche Risiko stellt Unternehmen und auch staatliche Einrichtungen weltweit vor neue Herausforderungen. Unternehmen mit großer öffentlicher Präsenz, die zudem über sensible Kundendaten verfügen, gelten als besonders gefährdet. Weltweite Beachtung erfuhr das Thema Cyber Security

> Wie intensiv muss ein Datenangriff sein, damit von einem systematischen und schwerwiegenden Datenmissbrauch die Rede sein kann?

etwa durch das als Aktivismus betriebene Hacking („Hacktivism") des Sony PlayStation Network im April dieses Jahres. Sony hatte sich in einschlägigen Kreisen unbeliebt gemacht, da es Umgehungen des Kopierschutzmechanismus der PlayStation 3 rechtlich verfolgte. Das war für „Hacktivisten" offenbar Grund genug, sich in das Sony PlayStation Network einzuhacken, das von über 77 Millionen Nutzern verwendet wird. Die Hacker legten das Netzwerk für mehr als drei Wochen lahm und stahlen die Kreditkartendaten der Nutzer. Die Schäden werden von Sony mit 171 Millionen US-Dollar beziffert. Anfang September dieses Jahres wurde DigiNotar gehackt, ein Anbieter, der unter anderem Zertifikate für elektronische Signaturen des gesamten niederländischen eGovernments ausstellte. DigiNotar steht wegen dieses Vorfalls nunmehr vor der Insolvenz. Motiv des Hackings soll das Verhalten der niederländischen UN-Soldaten 1995 in Srebrenica gewesen sein.

Anonymous Austria sorgt seit dem Sommer auch hierzulande für Unruhe. Im Juli dieses Jahres drangen die Hacker in die Websites der SPÖ, der FPÖ sowie der Grünen ein und kompromittierten so personenbezogene Daten von Zigtausenden von Usern. Noch im selben Monat drangen Mitglieder von Anonymous Austria auch in die Kundendatenbank der GIS Gebühren Info Service GmbH ein. Über 210.000 Kundendatensätze, größtenteils mit Kontonummer, wurden kopiert und nachfolgend teilweise im Internet veröffentlicht.

Gesetz mit unklaren Begriffen

Spätestens diese Fälle führen nur allzu deutlich vor Augen, dass dringender Handlungsbedarf besteht, um sich gegen derartige Angriffe, die regelmäßig über elektronische Netze erfolgen, zu wappnen. Andernfalls können die betroffenen Unternehmen – abgesehen von massiven Imageschäden – auch haftungsrechtlichen Folgen seitens ihrer Kunden ausgesetzt sein. Zentrale Pflicht jedes Unternehmens ist daher, die Sicherheit personenbezogener Daten nach § 14 Datenschutzgesetz (DSG) durch angemessene, dem Stand der Technik entsprechende Maßnahmen zu gewährleisten. Weiters werfen Attacken aus dem Cyberspace die Frage auf, wie Unternehmen mit bereits eingetretenen Sicherheitsvorfällen umzugehen haben. Neben möglichen Schadenersatzpflichten sind für viele Unternehmen insbesondere ihre Pflichten zur Information der Betroffenen (Data Breach Notification) weitestgehend unklar: Seit der DSG-Novelle 2010 haben Unternehmen die Betroffenen von Sicherheitsverletzungen in geeigneter Form zu informieren, wenn die Daten „systematisch und schwerwiegend" unrechtmäßig verwendet wurden und den Betroffenen ein Schaden droht *(§ 24 Abs 2a DSG)*. Diese etwas unglücklich formulierte Gesetzesbestimmung bereitet wegen der Verwendung mehrerer unbestimmter Gesetzesbegriffe in der Praxis große Auslegungsschwierigkeiten: Wie intensiv muss ein Datenangriff erfolgen, damit von einem systematischen und schwerwiegenden Datenmissbrauch die Rede sein kann?

Abgesehen von den gesetzlichen Vorgaben des Datenschutzgesetzes kann die Pflicht zur Data Breach Notification für Unternehmen aber auch kraft Vertrags bestehen: Selbst wenn mit den Kunden keine explizite Regelung getroffen wurde, wie nach einer Sicherheitsverletzung vorzugehen ist, gilt nach ergänzender Vertragsauslegung Folgendes: Das Unternehmen hat seine Kunden jedenfalls dann zu informieren, wenn dem Kunden infolge der Sicherheitsverletzung ein Schaden droht, den die Kunden bei zeitgerechter Information abwenden könnten.

Unternehmen sind daher gut beraten, sich mit ihren Pflichten zur Data Breach Notification auseinanderzusetzen, bevor es zu Sicherheitsverletzungen kommt. Dies ermöglicht nicht nur eine bessere Krisenkommunikation im Ernstfall, sondern versetzt Unternehmen erst in die Lage, ihre Pflichten durch effiziente vertragliche Gestaltung zu präzisieren und in gewissen Grenzen auch zu reduzieren.

Versteckt hinter der Guy-Fawkes-Maske, dem Symbol der Anonymous-Gruppe, machen sich die österreichischen Hacker an sensible Daten heran. [APA/Helmut Fohringer]

Industriespionage bleibt geheim

Neben „Hacktivism" stellt die Industriespionage ein weiteres Sicherheitsrisiko für Unternehmen dar. Die Tatsache, dass wesentlich seltener über Fälle der Industriespionage berichtet wird, liegt vor allem daran, dass die Täter – im Unterschied zu Hacktivisten – ihre System-Einbrüche geheim halten und selbst die betroffenen Unternehmen oft keine Kenntnis von dem Vorfall erlangen.

In diesem Zusammenhang hat sich der Begriff „Advanced Persistent Threat" (APT) etabliert, der Bedrohungen beschreibt, die von hoch qualifizierten und mit erheblichen Ressourcen ausgestatteten Angreifern (z. B. weltweit darauf spezialisierte Unternehmen oder fremde Staaten) ausgehen und sich gegen einzelne, gezielt ausgewählte Unternehmen richten. Um die rechtlichen und wirtschaftlichen Risken, die sich daraus ergeben, zu reduzieren, ist ein ganzheitlicher Ansatz zu Cyber Security erforderlich, der auch den globalen rechtlichen Schutz von geistigem Eigentum umfasst.

Dass Industriespionage auch in Österreich ernst zu nehmen ist, verdeutlicht ein Fall, der vergangene Woche vor dem Straflandesgericht Klagenfurt abgeurteilt wurde: Ein Ingenieur eines österreichischen Windtechnologieunternehmens soll von einem chinesischen Mitbewerber durch die Zusage eines profitablen Dienstvertrages dazu angestiftet worden sein, sich wertvolle Betriebsgeheimnisse zu verschaffen und diese dann preiszugeben. Der Ingenieur wurde (noch nicht rechtskräftig) zu einer Haftstrafe von drei Jahren, davon ein Jahr unbedingt, verurteilt. Der Gesamtschaden soll sich auf 250 Millionen US-Dollar belaufen.

Die Risken im Bereich Cyber Security sind vielfältig und einem ständigen Wandel unterworfen. Unternehmen sollten ihre Pflichten genau kennen, um Risken zu minimieren und um im Ernstfall effizient reagieren zu können.

Dr. Georg Kresbach ist Partner der Wolf Theiss Rechtsanwälte GmbH. Wolf Theiss veranstaltet am 13. Oktober das „Cyber Security Forum" (in Englisch). Anmeldung: marco.arienti@wolftheiss.com

In Kürze

Gerichtsgebühren: Anwälte mit Entwurf nicht zufrieden

Die Rechtsanwälte sind mit dem Gesetzesentwurf zu den Kopiergebühren bei Gericht nur teilweise zufrieden. Rupert Wolff, Präsident des Rechtsanwaltskammertages, begrüßt zwar, dass vom Gericht angefertigte Kopien statt 1,10 künftig nur mehr 0,60 Euro pro Seite kosten sollen, aber er sieht nicht ein, dass für selbst angefertigte Kopien 0,30 Euro (bisher 0,60) bezahlt werden sollen.

Wirtschaftskanzleien konnten Umsätze steigern

Die meisten der größten Anwaltskanzleien in Österreich konnten ihre Umsätze im Inland im Vorjahr steigern. Nach Erhebungen des deutschen Fachverlags Juve musste nur Branchenprimus Wolf Theiss (Jahresumsatz: 51,9 Mio. Euro) einen Rückgang des Umsatzes in Österreich um 6,7 % hinnehmen. Besonders stark (plus 18,5 %) wuchs nach diesen Erhebungen der Umsatz von CMS Reich-Rohrwig Hainz, Nummer acht im Juve-Größenvergleich (17,6 Mio. Euro Umsatz). Schönherr war mit 51,8 Mio. Euro Umsatz Wolf Theiss dicht auf den Fersen. Drittgrößte im Ranking sind Freshfields Bruckhaus Deringer, die den weitaus größten Umsatz pro Berufsträger (769.000 Euro) aufweisen.

LOB UND ANERKENNUNG

Präsident Dr. Michael Auer

Am 23. 9. 2011 hat in Eisenstadt der Anwaltstag 2011 stattgefunden, an dem sehr Interessantes zur Effizienz der Justiz im europäischen Vergleich zu erfahren war.
Die Kommission für die Effizienz der Justiz des Europarats (CEPEJ) hat auf der Datenbasis 2008 einen Bericht vorgelegt, der Aufmerksamkeit verdient.
Die CEPEJ wurde im Jahre 2002 gegründet und besteht aus Experten aus allen 47 Mitgliedsstaaten des Europarats. Ihre Aufgaben sind die Steigerung der Effizienz und funktionellen Verbesserung der Justiz, wie die Stärkung des Vertrauens in die Justiz in allen Mitgliedsstaaten. Der Zweck dieser Kommission ist die Förderung der Implementierung der Instrumente des Europarats zur Justizorganisation (Europäische Standards), die Schaffung von Entscheidungsgrundlagen für die Justizpolitik im Sinne der Bürger und eine Reduzierung der Belastung des Europäischen Gerichtshofs für Menschenrechte.
Seit ihrer Gründung werden die europäischen Justizsysteme analysiert und bewertet, Verfahrensdauer und Zeitmanagement aufgelistet und Umfragen zur Förderung der Qualität der Justiz in Europa samt Handbuch und Qualitätschecklisten erarbeitet.
Durchgeführt wurde eine quantitative und qualitative vergleichende Beurteilung, an der 45 Mitgliedsstaaten oder 730 Mio. europäische Bürger beteiligt waren.
Wussten Sie, dass die Justiz jeden Österreicher im Jahr € 77,9 (monatlich € 6,49) kostet? Damit kommt die österreichische Justiz unserer Volkswirtschaft vergleichsweise günstig.
Wussten Sie, dass die österreichischen Justizausgaben z. B. rund 1,5 mal geringer als jene der als sehr effizient bekannten Gerichtsstruktur der Niederlande sind?
Wussten Sie, dass Österreich die Justiz betreffend die drittniedrigsten Personalsausgaben in Europa hat, wobei der Durchschnitt bei 70 % des Budgetaufwandes Justiz und in Österreich bei 50 % liegt?
Wussten Sie, dass die Anzahl der „nicht richterlich Bediensteten" je Richter in Österreich aufgrund des IT-Einsatzes relativ gering ist?
Wussten Sie, dass Österreich das Zivilrecht betreffend, keine Verfahrensrückstände aufbaut und im streitigen Zivilverfahren laufend abarbeitet?
Wussten Sie, dass Österreich, was die Anhängigkeitsdauer von Verfahren betrifft, im Spitzenfeld liegt? Außerstreitiges Verfahren 68 Tage (EU-Durchschnitt 114 Tage), Streitiges Verfahren 129 Tage (282 Tage EU-Durchschnitt). Im Jahre 2008 haben in Österreich streitige Scheidungssachen, gemessen an der durchschnittlichen Verfahrensdauer, 180 Tage und im EU-Durchschnitt 228 Tage gedauert.
Die Leistungen der österreichischen Justiz können sich im europäischen Vergleich hervorragend behaupten.
Das verdient Lob und Anerkennung! Ehre, wem Ehre gebührt!

EINE SERIE DER RECHTSANWALTSKAMMER WIEN
WWW.RAKWIEN.AT

Judikatur

ÖBB will Fahrgäste nicht entschädigen: EuGH am Zug

Laut einer EU-Verordnung müssen Eisenbahnen ihre Fahrgäste bei großen Verspätungen entschädigen. Die ÖBB lehnen dies aber ab, wenn höhere Gewalt schuld an der Verspätung ist. Höhere Gewalt liegt laut ÖBB auch dann vor, wenn der Zug aus dem Ausland verspätet eintrifft. Der Verwaltungsgerichtshof ruft nun den Gerichtshof der EU an *(EU 2011/0009)*: Er soll klären, ob die ÖBB-Ansicht EU-konform ist.