GEFAHR: REPUTATIONSVERLUST DURCH INFORMATIONSABFLUSS

Christian Schaaf,
Geschäftsführer
CORPORATE TRUST Business
Risk & Crisis Management GmbH,
München

Die Reputation einer Firma ist stark abhängig vom Vertrauen der Kunden in die Produkte, die Marke sowie die Vertrauenswürdigkeit des Unternehmens. Gehen vertrauliche Informationen verloren, sei es durch einen Cyber-Angriff, böswillige Mitarbeiter oder einfach nur durch Leichtsinn im Umgang mit Daten, wird das Image beschädigt, weil das Vertrauen in die Zuverlässigkeit des Unternehmens und die Sicherheit seiner Systeme sinkt.

Für Unternehmen besteht zunehmend die Gefahr eines Reputationsverlusts durch einen Informationsabfluss. Immer öfter gibt es Berichte über Cyberattacken, gehackte Passwörter oder Zugriffe auf Firmen-Datenbanken. Informationsabflüsse passieren aber nicht nur durch kriminelle Angriffe, sondern häufig auch durch frustrierte Mitarbeiter, die sich komplette Listen der Kundenstammdaten für eigene Zwecke kopieren, oder einfach aus Leichtsinn, weil ein schnell noch verschicktes E-Mail mit vertraulichen Informationen versehentlich an die verkehrte Adresse ging. Unternehmen sind daher gefordert, Sicherheitsvorkehrungen gegen solche Informationsabflüsse zu treffen um ihre Reputation zu schützen.

Das Vertrauen in die Sicherheit der persönlichen Daten bei einem Lieferanten oder Dienstleistungs-Anbieter spielt eine wesentliche Rolle bei der Bewertung der Seriosität und Zuverlässigkeit. Kein Patient möchte, dass seine Krankenakte beim Hausarzt für jedermann offen einsehbar ist. Jeder, der sich in einer Ehescheidungs-, Steuer- oder Verkehrsrechtssache von einem Rechtsanwalt vertreten lässt, erwartet von der Kanzlei, dass die vertraulichen Informationen dort bestmöglich geschützt werden. Die meisten Menschen in Deutschland möchten auch nicht, dass ihr Gehaltszettel offen im Unternehmen für alle anderen Mitarbeiter bekannt ist. Wir erwarten selbstverständlich, dass damit sensibel und höchst vertraulich umgegangen wird. Kreditkartensysteme oder Anbieter wie Paypal funktionieren sogar nur, weil die Nutzer in die Sicherheit ihrer Zugangsdaten und der Prozesse beim Bezahlvorgang vertrauen. Der Verlust dieses Vertrauens durch einen bekannt gewordenen Informationsabfluss kann sich daher für Unternehmen sehr negativ auswirken.

Einer der deutlichsten Fälle von Reputationsverlust durch einen Informationsabfluss war in den vergangenen Jahren wohl der Angriff auf SONY-Pictures im November 2014. Unbekannte Hacker, die sich „Guardians of Peace" nannten, kurz GOP, waren in das Firmennetzwerk eingedrungen und hatten dort vertrauliche Daten entwendet. Die Täter verschafften sich nicht nur Zugriff auf interne Dokumente und vertrauliche E-Mails, sondern auch auf persönliche Daten der Mitarbeiter, wie zum Beispiel Sozialversicherungsnummern, Passwörter, Lohnabrechnungen, ärztliche Atteste und Auszüge aus dem Strafregister. Darüber hinaus erbeuteten Sie Informationen zu intimen Details von Stars, Digitalkopien noch unveröffentlichter Filme und sogar eine frühe Version des Drehbuchs für den James-Bond-Film „Spectre". Vor der Veröffentlichung der Daten hatten die Täter anscheinend erst versucht, das Unternehmen zur Zahlung von „Lösegeld" zu erpressen und die Veröffentlichung des Films „The Interview" zu verhindern. Durch den Hackerangriff wurde auch bekannt, dass die Co-Chefin von SONY-Pictures, Amy Pascal, in einem E-Mail an ihren Kollegen Scott Rudin, Witze über den mutmaßlichen Filmgeschmack von US-Präsident Barack Obama machte.

Offizielle von SONY-Pictures hatten zwar hinterher oftmals beteuert, dass dieser Vorfall keinen gravierenden Einfluss auf das Firmenergebnis gezeigt hätte, die Fakten sprechen jedoch für sich. Mitarbeiter von SONY-Pictures mussten nach dem Angriff für einige Zeit mit Papier, Stift und Fax arbeiten, weil die Computernetzwerke nicht funktionierten. Amy Pascal musste gut zwei Monate nach dem Vorfall ihren Rücktritt einreichen, weil US-Kommentatoren die Späße in den E-Mails als rassistisch einstuften. Die 47.000 betroffenen Mitarbeiter von SONY-Pictures, deren Daten an die Öffentlichkeit gelangten, erhielten jeweils 10.000 Dollar Entschädigung. Außerdem stellte das Unternehmen 3,5 Millionen Dollar für Gerichtskosten bereit. Der Ruf war erstmal stark beschädigt.

Auch in Deutschland passieren solche Vorfälle. Im Januar 2014 berichteten verschiedene Medien, dass im Rahmen eines Ermittlungsverfahrens der Staatsanwaltschaft Verden ein Fall von großflächigem Identitätsdiebstahl aufgedeckt wurde. Kriminelle erbeuteten circa sechzehn Millionen Konto-Daten. Die E-Mail-Adressen und Passwörter seien gesammelt worden, um über die kompromittierten Adressen mit Hilfe eines sogenannten Botnetzes Spam zu versenden. Botnetzte sind ein Zusammenschluss gekaperter Computer, die meist ohne Wissen der Nutzer mit Schadsoftware infiziert wurden. Diese „Zombie-Rechner" werden dann beispielsweise genutzt, um massenhaft ungewollte E-Mails an eine Adresse zu versenden. Unternehmens-Server, die so mit einer Flut von gleichzeitigen Anfragen konfrontiert werden, können durch die Überlastung außer Gefecht gesetzt werden. Diese sogenannten Distributed Denial of Service-Attacken (DDOS-Attacken) nehmen zu und Unternehmen können sich nur schwer dagegen schützen.

Die Täter bei solchen Angriffen sind meist der Organisierten Kriminalität (OK) zuzurechnen, also Verbrecherbanden, die arbeitsteilig agieren und es darauf anlegen, Unternehmen zu erpressen. Immer stärker verlagern diese Banden ihre kriminellen Aktivitäten in den Cyberraum, weil hier das Entdeckungsrisiko viel geringer ist als in der realen Welt. Sie werben gut ausgebildete IT-Spezialisten an, die übrigens gar keine große kriminelle Energie haben müssen, um Schadsoftware für bestimmte Systeme oder Programme zu programmieren. Der Einsatz des Schad-

DVS-FLYER

Kompakte Informationen über das Berufsbild der

INDUSTRIEVERSICHERUNGS-SPEZIALISTEN

in der versicherungsnehmenden Wirtschaft

- ☑ für Studierende und (Berufs-)Schüler
- ☑ für Hochschulen und Berufsschulen
- ☑ für die versicherungsnehmende Wirtschaft (Personalgewinnung etc.)
- ☑ kostenfreier Bezug und jederzeit nachbestellbar

IHRE ANSPRECHPARTNERIN

zum Thema Aus- und Weiterbildung, inkl. DVS-Flyer

Nicole Neubauer
Tel.: 02 28 / 98 223 44
E-Mail: nicole.neubauer@dvs-schutzverband.de

codes erfolgt dann meist durch eine ganz andere Gruppe und das Erwirtschaften des Geldes, in der Fachsprache „Harvesting" genannt, wieder durch einen anderen Personenkreis. Höchst vertrauliche Informationen wie Geburtsdaten, Kontonummern, Kreditkartendaten oder Online-Zugänge werden von Kriminellen übrigens zunehmend auch im Internet gehandelt, im sogenannten „Darknet". Solche Untergrund-Foren sind meist nur Insidern mit sehr speziellem Know-how zugänglich. Die erworbenen Daten werden genutzt, um damit Konten der Nutzer anzugreifen oder auf Shopping-Portalen einzukaufen.

Bei Angriffen auf Unternehmen wird mit dem Ausfall der Firmen-IT durch eine DDOS-Attacke auf Server oder die Internet-Präsenz gedroht bzw. mit der Veröffentlichung von vertraulichen Firmendaten, die bei einem Hackerangriff erbeutet wurden. Beides könnte für Unternehmen zu einem großen Reputationsverlust führen, also wird in der Regel gezahlt.

Eine neue Dimension an Cyberattacken ist spätestens seit April 2015 erkennbar, als dschihadistische Hacker der Terrororganisation „Islamischer Staat" (IS) den französischen Sender TV5Monde angriffen. Die Attacke brachte den Betrieb der französischen Fernsehsendergruppe mehrere Stunden lang zum Erliegen, weil die Übertragungen zu den Kanälen getrennt wurden. Der Angriff war gezielt und umfassend, so dass nicht nur alle elf Kanäle von TV5Monde ein schwarzes Bild zeigten, sondern auch die Webseite und die Konten in sozialen Netzwerken von den Terroristen kontrolliert wurden. Die Gruppe, die sich selbst als Cyberkalifat bezeichnete, platzierte dort überall ihr Banner und Propaganda des IS. Es ist leicht vorzustellen, welche Auswirkungen vermehrte derartige Angriffe, mit länger andauernden Ausfällen oder kritischen Botschaften, auf die Reputation von TV5Monde und damit das Werbeverhalten der Kunden hätte.

Während erst noch abzuwarten ist, welche Entwicklung die Bedrohung durch Terroristen im Cyberraum nehmen wird, besteht für Unternehmen ein zwar einfacher gelagertes aber trotzdem permanentes Risiko von Informationsabfluss – nämlich durch eigene Mitarbeiter. Verärgerung über Vorgesetzte oder das eigene Vorwärtskommen führen häufig zu Frustration und Abwanderungsgedanken. Das Kopieren sämtlicher Kunden- oder Lieferantendaten, von Bauplänen oder Beschreibungen neuer Entwicklungen wird dann als „Kavaliersdelikt" gesehen. Wenn man vorhat den Arbeitgeber zu wechseln, will man ja möglichst viele Informationen „mitnehmen". Dies führt nicht nur zum Abfluss vertraulichen Know-hows an Wettbewerber, sondern häufig auch zur Verärgerung bei Kunden oder Lieferanten, wenn sie schon wieder von einem Ex-Mitarbeiter ihres aktuellen Geschäftspartners angesprochen werden, der jetzt „unter neuer Flagge segelt".

Darüber hinaus kann Informationsabfluss auch zum Reputationsverlust bei den eigenen Mitarbeitern führen. Wer merkt, dass interne Systeme immer wieder angegriffen werden und keine ausreichenden Sicherheitsvorkehrungen gegen Datenabfluss getroffen wurden, verliert das Vertrauen in die eigene Stärke und Widerstandsfähigkeit des Unternehmens. Gehen dann auch noch persönliche Daten verloren, etwa Gehaltsnachweise oder eigene Adress- und Telefondaten, ist die Verärgerung groß und das Image des eigene Arbeitgebers beginnt zu bröckeln.

> Unternehmen sollten sich generell Gedanken darüber machen, wie mit den eigenen „Kronjuwelen" umzugehen ist.

Unternehmen sollten sich generell Gedanken darüber machen, wie mit den eigenen „Kronjuwelen" umzugehen ist. Dies setzt voraus, dass erst einmal definiert wird, welche Daten schützenswert sind und wo der Informationsabfluss einen Verlust an Wettbewerbsvorteil oder Reputation bedeuten könnte. Dann sollten die Mitarbeiter für das sicherheitsbewusste Verhalten im Umgang mit IT-Equipment, speziell auch zum Verhalten im Internet, sensibilisiert werden. Nur so kann erreicht werden, dass vertrauliche Daten besser geschützt bleiben.

Für jeden Mitarbeiter muss heute klar sein, dass kein Klick im Internet kostenlos ist. Die Währung ist nicht in erster Linie Geld, sondern Informationen über die Nutzer. Sensible Informationen wie Name, Anschrift, Kontaktadressen, Einkaufsverhalten oder besuchte Webseiten sind bares Geld wert, weil damit Rückschlüsse auf das Unternehmen, persönliche Präferenzen oder mögliche Passwörter gezogen werden können. Solche Informationen dienen häufig auch nur dazu, einen „Social Engineering Angriff" vorzubereiten. Unter Social Engineering versteht man den Informationsangriff auf menschliche Quellen. Die Täter versuchen über zwischenmenschliche Beeinflussung bzw. durch geschickte Fragestellung das persönliche Umfeld von Menschen auszuspionieren, meist unter Verschleierung der eigenen Identität, zum Beispiel durch Verwenden einer Legende. Social Engineering hat das Ziel, unberechtigt an Daten, geheime Informationen, Dienstleistungen oder Gegenstände zu gelangen.

Will ein Unternehmen vermeiden, dass vertrauliche Informationen arglos preisgegeben werden, muss es entsprechende Vorkehrungen treffen und die Mitarbeiter über solche Vorgehensweisen der Täter informieren. Die Sensibilisierung der Mitarbeiter, sofern sie professionell, modern und nachhaltig erfolgt, hat auch noch den positiven Nebeneffekt, dass es die Menschen dazu animiert, vorsichtiger mit ihren Smartphones, Tablets oder Notebooks bzw. bei der Kommunikation über die Geräte umzugehen. Wer erst einmal verstanden hat, welche Zugangsmöglichkeiten in das Firmennetzwerk über ein liegengelassenes oder unzureichend geschütztes Smartphone erfolgen können, wer einmal gesehen hat, wie leicht „Fake-E-Mails" erzeugt werden können, die so aussehen als würden sie von einem Kollegen oder sogar Vorgesetzten kommen, der wird sich künftig umsichtiger beim Daten-Handling verhalten.

Viele Unternehmen haben sich ihre Reputation über viele Jahre aufgebaut und das Vertrauen des Marktes hart erarbeitet. Gerade durch die heute sehr viel schnellere Meinungsbildung über Soziale Netzwerke oder Internet-Foren, Stichwort Shitstorm, kann diese Reputation innerhalb von wenigen Tagen zerstört werden. Das Ziel der Unternehmen muss es daher sein, alle Vorsichtsmaßnahmen zu treffen, um einen Datenverlust zu vermeiden. Neben der technischen Absicherung von Netzwerken und Kommunikationsgeräten sollten deshalb auch entsprechende organisatorischen Regelungen getroffen und die Mitarbeiter bei allen Schutzmaßnahmen eingebunden werden, um einen Reputationsverlust durch Informationsabfluss zu vermeiden. ■