Bedrohung aus dem Netz

Die zunehmende Cyberkriminalität verleiht dem Thema Datenschutz auch für kleine Unternehmen eine nicht zu unterschätzende Brisanz.

Ein vollständiger Schutz gegen Internetkriminalität ist derzeit technisch nicht möglich, DSGVO-konformer Umgang mit Kundendaten schützt Finanzdienstleister aber davor, nach Zwischenfällen auch noch bestraft zu werden.

Die zunehmende Digitalisierung bewirkt zwar weiterhin Produktivitätsgewinne und ermöglicht Dienstleistungen, die analog nicht darstellbar waren, dafür bezahlt man allerdings auch einen Preis, der vordergründig nicht wahrgenommen wird: Die Sicherheit unserer Daten ist zunehmend gefährdet. Das Bundeskriminalamt bezifferte die Zahl der Anzeigen für das erste Halbjahr 2019 mit rund 13.000 Fällen, im Jahresvergleich ist das ein Zuwachs um 50 Prozent. Auf unterschiedlichste Weise wird versucht, Privatpersonen, Unternehmen und öffentliche Einrichtungen zu betrügen, zu erpressen oder ihre Daten zu stehlen. Zugangsdaten zu Bank- und Kryptowährungskonten zählen neben Kreditkartendaten zur bevorzugten Beute von kriminellen Akteuren im Internet, aber grundsätzlich werden auch alle anderen Datensätze von Namen über Adressen bis zu Telefonnummern gestohlen. Dass auch große Unternehmen wie die amerikanische Bank One, die Hotelkette Marriott oder der Aluminiumkonzern Norsk Hydro Opfer solcher Angriffe wurden, zeigt, dass es jeden treffen kann. Erfolgreiche Angriffe durch Hacker verursachen in der Regel nicht nur einen Image-, sondern auch einen massiven finanziellen Schaden – sogar dann, wenn den betroffenen Kunden kein unmittelbarer finanzieller Schaden entsteht. Die US-Großbank Capital One, der von einer Hackerin mehr als 100 Millionen Datensätze von potenziellen Kreditkartenkunden gestohlen wurden, geht davon aus, dass 100 bis 150 Millionen US-Dollar an Kosten für Rechtsberatung, die Benachrichtigung von Kunden und die Umstellung der Technik anfallen werden.

Strafen durch Behörden

Hinzu kommt, dass Unternehmer in solchen Fällen auch noch mit Strafen rechnen müssen, nämlich dann, wenn man ihnen nachweisen kann, dass sie ihre Kundendaten nicht gesetzeskonform geschützt haben. In Deutschland wurde erst kürzlich gegenüber einem Lieferdienstanbieter eine Strafe von 195.000 Euro verhängt, da dieser nach Ansicht der Behörde gleich mehrfach gegen Datenschutzvorgaben verstoßen hat. Noch massiver griff 2019 die britische Datenschutzbehörde ICO durch: Die Fluggesellschaft British Airways und Marriott Hotels wurden vom Information Commissioner's Office (ICO) zu Strafzahlungen in Höhe von 180 beziehungsweise 99 Millionen Pfund verdonnert.

In Österreich wurden bisher nur eine Handvoll Strafen verhängt – die höchste lag bei 4.800 Euro. „Diese Fälle beziehen sich ausschließlich auf den Bereich der unerlaubten Videoüberwachung. Diese wären aber wohl auch vor Inkrafttreten der DSGVO schon zu ahnden gewesen, es ist lediglich die Sensibilität gestiegen und damit die Zahl der Fälle bei der Datenschutzbehörde", erklärt Wolfgang Millner, Geschäftsführer beim Wiener IT-Sicherheitsdienstleister Rentea. Bisher folgt die Datenschutzbehörde (DSB) in Österreich noch dem Motto „Verwarnen vor strafen", das muss allerdings nicht so bleiben.

FMA zeigt Interesse

Besonders sorgfältig müssen Unternehmen agieren, die mit sensiblen personenbezogenen Daten zu tun haben. Dazu zählen insbesondere Wertpapierfirmen, Vermögensberater und Versicherungsvermittler. Obwohl die DSGVO seit 2018 in Kraft ist, wurde sie nach Ansicht von Fachleuten noch nicht in allen Unternehmen vollständig implementiert. Der Unternehmensberater und Datenschutzexperte Andreas Dolezal meint: „Wir sind immer noch sehr weit davon entfernt, dass eine breite Masse die Pflichten der DSGVO erfüllt." Dolezal legt hier eine Tempoverschärfung nahe, weil das Thema IT-Sicherheit und Datenschutz zunehmend in das Interessenfeld der Finanzmarktaufsicht rücke. Dem Vernehmen nach wird bei einigen Wertpapierfirmen und deren Erfüllungsgehilfen bei Vor-Ort-Prüfungen bereits gezielt in diese Richtung nachgefragt. Sich dem Thema IT-Sicherheit stärker anzunehmen, kann somit in mehrfacher Hinsicht von Vorteil sein.

In der Praxis rät IT-Experte Millner, vor allem beim Datenaustausch mit Kunden besondere Vorsicht walten zu lassen. Während Banken und Versicherungsunternehmen mittlerweile über eigene Portale für den sicheren und rechtskonformen Datenaustausch verfügen, hinken die kleinen Unternehmen hier oftmals noch hinterher. Millners Erfahrung: „Vom

DI(FH) Wolfgang Millner, Rentea: „Sensible Daten sollten grundsätzlich nur verschlüsselt übertragen werden."

Andreas Dolezal: „Das Thema IT-Sicherheit wird leider immer noch auf die leichte Schulter genommen."

Makler zum Kunden ist mir so eine Lösung noch nicht untergekommen. Hier wird meist noch auf E-Mail gesetzt. E-Mails werden aber meist unverschlüsselt versendet und liegen dann unter Umständen auch noch lang auf Servern außerhalb der Geltungsbereichs der DSGVO, was aus rechtlicher und technischer Sicht ein Problem ist." Im ersten Schritt empfiehlt der IT-Spezialist dazu, sensible Daten grundsätzlich nur verschlüsselt zu übertragen. Wer dies per E-Mail mache, könne zu versendende PDFs beziehungsweise komprimierte Dateien (ZIP-Files) verschlüsseln. Der Schlüssel müsse allerdings dementsprechend lang sein und unbedingt auf einem anderen Weg übermittelt werden. Wer Cloud Services zur Datenspeicherung beziehungsweise zur Übertragung nutze, sollte grundsätzlich europäische Dienste verwenden und die Daten nur für begrenzte Zeit in der Cloud speichern. Bei der Frage, welche Cloud-Dienstleister geeignet seien, helfe die Wirtschaftskammer. Mit dem von der Kammer ins Leben gerufenen Gütesiegel „Austrian Cloud" werden Anbieter ausgezeichnet, die Daten nur im Inland speichern. Bisher finden sich bereits 28 Unternehmen mit einem entsprechenden Gütesiegel in der Firmensuche der Wirtschaftskammer.

Einen Lösungsansatz liefert auch Millner selbst mit seinem Dienst s-transfer.at. Das Tool ermögliche eine DSGVO-konforme und sichere Datenübertragung. Die Daten werden dabei auf österreichischen Servern zwischengespeichert und nach spätestens sieben Tagen gelöscht. So wird ein „Datenfriedhof" vermieden, der Angriffspunkt einer Cyberattacke werden könnte. Außerdem prüft s-transfer alle transferierten Daten auf Schadprogramme wie Viren, Würmer und Trojaner.

Gedanken muss man sich auch über die dauerhaft sichere Aufbewahrung von Kundendaten machen, auch die Frage, wer Zugriff auf die Daten habe, sei zu klären „Nicht jeder Mitarbeiter benötigt immer Zugriff auf alle relevanten Kundendaten", meint Millner.

Der Datenschutzexperte betont, dass es beim Thema IT-Sicherheit keineswegs nur um die Einhaltung von Formalismen gehe. Im Ernstfall könne es zu einer massiven Beeinträchtigung der Aufgabenerfüllung kommen – „etwa wenn Ransomware alle Daten verschlüsselt, man erpresst wird und keinen Zugriff mehr auf Kundendaten hat".

Nach Einschätzung von Dolzeal wird die Bedrohung dennoch vielfach unterschätzt: „Das ist auch kein Wunder, schließlich haben viele ganz andere Sorgen und sind wegen der vielen anderen ebenso umfangreichen regulatorischen Vorgaben überlastet. Es geht derzeit daher in erster Linie darum, die Berater für dieses Thema zu sensibilisieren. Vielen wird die Notwendigkeit, in diesem Bereich tätig zu werden, leider erst bewusst, wenn etwas passiert. Dabei kann man schon mit relativ einfachen Maßnahmen gegensteuern." Zwar weisen Dolezal wie auch Millner darauf hin, dass es keinen 100-prozentigen Schutz gegen Cyberkriminalität gebe. Man sollte, so Millner, allerdings zumindest die offensichtlichen „offenen Scheunentore" schließen. Die wichtigsten zehn Punkte, um die Eintrittswahrscheinlichkeit eines Vorfalls zu minimieren, hat Millner daher zusammengefasst (siehe Kasten).

»Wir sind immer noch kilometerweit davon entfernt, dass eine breite Masse die Pflichten der DSGVO erfüllt.«

Andreas Dolezal, Unternehmensberater

GEORG PANKL | FP

10 Tipps vom Profi zum Thema IT-Sicherheit

1. Meine Systeme (Laptop und Handy) mit **Virenscannern** ausstatten. Die meisten E-Mail-Provider bieten zu geringen Mehrkosten einen Virenscanner für E-Mails an.
2. Die **Browser-Sicherheitseinstellungen** streng setzen (auch wenn es oft nervt, es schützt ein wenig vor ungewollten Klicks).
3. **Sichere Passwörter** und **Passwortmanager** (Browser-Plug-ins oder auch Keepass) verwenden und diese mit einem sicheren Masterpasswort verschlüsseln. Das Masterpasswort sicher außerhalb des Systems aufbewahren.
4. Sensible Daten grundsätzlich **nur verschlüsselt übertragen.** E-Mail ist kein sicheres Übertragungsmedium. Im Prinzip kann ich auch PDFs oder ZIPs verschlüsseln und dann per E-Mail schicken. Der Schlüssel sollte sehr lang sein und unbedingt auf einem anderen Weg übertragen werden.
5. **Sensible Daten nur kurz** auf Systemen die vom Internet aus verfügbar sind (**Cloud-Systeme, aber auch E-Mailserver**) belassen.
6. Wo immer möglich unbedingt eine **2-Faktor-Authentifizierung** verwenden.
7. **Nicht auf alles klicken,** was in der Mailbox landet: Falls ein E-Mail täuschend echt aussieht, trotzdem die **Absendeadresse prüfen.**
8. Den **Bildschirm immer sperren,** wenn ich nicht davor sitze. Gerade in Gemeinschaftsbüros wird mit dieser einfachen Sache oft fahrlässig umgegangen.
9. Ein **regelmäßiges Back-up** auf einem **separaten, sicher verwahrten Speichermedium** erstellen.
10. Einen **Notfallplan** haben, falls etwas passiert (Meldepflichten aus Datenschutzgesetzgebung, Information betroffener Kunden, wer kann helfen, die Systeme wieder instandzusetzen, usw.).

Quelle: Rentea