Sind meine Spenderdaten sicher?

Informationssicherheit ist eine Herausforderung für Spendenorganisationen

Auch Spendenorganisationen müssen sich mit Informationssicherheit befassen. Die Intensivierung des Wettbewerbs um neue Spender, die gezielte Spenderansprache durch Nutzung neuer Vertriebswege, zum Beispiel Social Media, und die verstärkte Zusammenarbeit mit Dienstleistern erfordern ein neues Sicherheitsbewusstsein in den Organisationen.

Von ERWIN RECKTENWALD

Persönliche Spenderdaten stellen ein besonders schützenswertes Know-how und Wirtschaftsgut dar und müssen vor Missbrauch und Diebstahl besonders geschützt werden. Wenn Spenderdaten durch gezielte Attacken in die Öffentlichkeit gelangen, kann dies zu einem existenzgefährdenden Reputationsverlust der Spendenorganisationen führen. Die Leitungsebenen der Organisationen müssen sich über die Risiken und Gefahrenpotenziale im Klaren sein, denn sie stehen in diesem Zusammenhang in einer besonderen persönlichen Verantwortung. Vorsorge ist wichtig und erfordert die Etablierung einer Sicherheitskultur in den Unternehmen.

KRITISCH: FAKTOR MENSCH

Die Medien berichten fast täglich über Cyberattacken im Internet und messen dieser Bedrohung die größte Bedeutung bei. In der Praxis setzt sich aber immer stärker die Erkenntnis durch, dass der Mensch in seiner emotionalen Verhaltensweise die größte Schwachstelle darstellt.

Die Beachtung des Datenschutzes und der Datensicherheit ist eine zentrale Herausforderung unserer Zeit und ein besonderes gesellschaftliches Anliegen. Der Datenschutz hat die Aufgabe, die Verarbeitung und den Umgang mit personenbezogenen Daten gesetzeskonform (Bundesdatenschutzgesetz, BDSG) zu gewährleisten. Hierbei ist zu beachten, dass jede Person das Recht hat, selbst über die Freigabe und Verwendung ihrer persönlichen Daten zu entscheiden und zu jeder Zeit Auskunft über die Verarbeitung ihrer Daten einholen kann. Dies muss bei der Gestaltung und Abwicklung der internen und externen Geschäftsprozesse beachtet werden.

DATENSICHERHEIT ALS WETTBEWERBSVORTEIL

Die Gewährleistung der Datensicherheit stellt einen entscheidenden Wettbewerbsvorteil und Differenzierungsfaktor dar, etwa bei der Gestaltung einer vertrauensvollen Zusammenarbeit mit Spendern und Dienstleistern. Außerdem wird hierüber das Image einer Organisation in der Öffentlichkeit wesentlich bestimmt.

Spendenorganisationen sollten über ein angemessenes Sicherheitsniveau verfügen, um einen Datenverlust, eine Datenmanipulation oder die Weitergabe von Daten an Dritte zu verhindern. Folgende Lösungsansätze stehen NPOs für mehr Datensicherheit zur Verfügung: Aufbau und Implementierung eines „Integrierten Sicherheitsmanagements“, zum Beispiel nach dem Standard ISIS 12 für kleine und mittelständische Unternehmen.

Gestaltung und Durchführung von Awareness-Kampagnen und Schulungen zur Sensibilisierung der Beschäftigten, Etablierung von technischen Sicherheitsmaßnahmen zur Gewährleistung eines

angemessenen Basisschutzes (z. B. Virenschutz, Software-Updates, Verschlüsselung) und die Durchführung von Kontrollmaßnahmen (z. B. Audits) bei Dienstleistern.

Empfehlenswert für die Gestaltung und Implementierung von Sicherheitsmaßnahmen ist der neutrale Blick von „außen". Dabei sollte man auf Experten mit Erfahrung in konkreten Sicherheitsvorfällen bauen.

MITVERANTWORTUNG FÜR DIENSTLEISTER

Überträgt man Daten an Dienstleister, gilt nicht das Prinzip „aus den Augen aus dem Sinn". Die Organisation trägt immer eine Mitverantwortung für die Gestaltung der Sicherheit bei den eingebundenen Unternehmen und kann im Schadensfall haftbar gemacht werden. Klare vertragliche Vereinbarungen zum Schutz der Unternehmensinformationen und der persönlichen Daten der Spender müssen geschlossen werden.

Die Spender vertrauen den Spendenorganisationen sensible persönliche Daten an. Dieses Vertrauen müssen die Unternehmen durch sichere Prozesse und technische Sicherheitsmaßnahmen in der Verarbeitung und Speicherung der Daten erfüllen. Folgende Maßnahmen sind hier empfehlenswert: gewissenhafte Auswahl der Dienstleister auf Basis eines Checks der Vertrauenswürdigkeit und Leistungsfähigkeit, regelmäßiger Informationsaustausch und Festlegung von Qualitäts- und Sicherheitslevels (SLAs), Abschluss spezieller vertraglicher Vereinbarungen zu Datenschutz (z. B. Auftragsdatenverarbeitung) und Datensicherheit (z. B. Datenlöschung) sowie Aufsicht und Kontrolle der Dienstleister durch Audits und Sicherheitschecks.

Die Gewährleistung der Sicherheit muss nicht mit hohen Kosten und Investitionen verbunden sein. Eine an den Geschäftsanforderungen ausgerichtete integrierte Planung der Sicherheitsmaßnahmen und ein balancierter Ressourceneinsatz stellen die notwendige Basis für eine effiziente Umsetzung der Maßnahmen in der betrieblichen Praxis dar.

Erwin Recktenwald *ist Management Consultant und Partner von biners – business information security auf dem Gebiet der Geschäftsinformationssicherheit. Er war über viele Jahre in leitenden Funktionen der Deutschen Telekom AG als Geschäftsleiter und Senior Vice President auf nationaler und internationaler Ebene tätig. Sein Beratungsunternehmen erarbeitete gerade gemeinsam mit der ENTERBRAIN Software AG eine neue Sicherheitsstrategie für Spenderdaten.*
▶ *www.enterbrain.ag*