Spam-Mails, Social Engineering, Phishing – das sind nur einige der Betrugsmethoden, die im Internet angewendet werden. Wie Sie als Verein oder andere gemeinnützige Organisationen das Internet sicher nutzen können, hat „TechSoup“ in einem 3-teiligen Leitfaden zusammengestellt. Teil 3

Im dritten und letzten Teil des Leitfadens „Mehr Sicherheit im Internet“ erfahren Sie, wo besondere Vorsicht geboten ist und was Sie beachten sollten, wenn Sie Cloud Services nutzen. Außerdem gibt es Tipps zur Aufbewahrung von Offline-Sicherungen.

Ein Artikel von TechSoup USA

9 SEIEN SIE VORSICHTIG, WENN IHR UNTERNEHMEN SOCIAL MEDIA NUTZT.

Besondere Vorsicht ist geboten, wenn Mitarbeiter und Freiwillige im Namen der Organisation Social Media nutzen. Wie bei der Sicherheit sollten neue Mitarbeiter und Freiwillige, wenn sie über Social-Media-Kanäle aktiv werden, verstehen, was von ihnen erwartet wird.

Die Mitarbeiter sollten sich bewusst sein, dass sie in einer Weise posten oder antworten sollten, die mit den Werten Ihrer Organisation übereinstimmt. Sie sollten eine Social-Media-Richtlinie für Ihre Organisation haben.

Wenn mehrere Benutzer ein gemeinsames Konto verwenden, ist es sinnvoll, festzustellen, welche Mitarbeiter wann posten.

Wenn möglich, verwenden Sie ein Social-Media-Publishing-Tool, das es Mitarbeitern ermöglicht, etwas auf den Konten zu veröffentlichen, ohne dass sie direkten Zugriff auf Ihre Social-Media-Konto-Anmeldeinformationen benötigen.

Einige Dienste bieten unterschiedliche Rollen für verschiedene Berechtigungsstufen. Ordnen Sie den Mitarbeitern bei Bedarf Rollen zu.

Wenn Sie Ihre „Fans“ in einem Social-Media-Beitrag „markieren“ oder erwähnen, könnten Sie versehentlich mehr Informationen über sie preisgeben, als Sie glauben. Verwenden Sie diese Funktion also sorgfältig.

Wenn Sie nicht die ausdrückliche Erlaubnis haben, die Bilder Ihrer Förderer zu verwenden, verpixeln Sie deren Gesichter auf Ihren Fotos und Videos.

10 SEIEN SIE VORSICHTIG BEI DER ANMELDUNG UND ÜBERLEGEN SIE, OB SIE DEN ZUGRIFF AUF FREIGEGEBENE DATEIEN EINSCHRÄNKEN SOLLTEN.

Wenn Ihr Unternehmen Cloud Services nutzt, kann jeder mit Zugangsdaten auf den Service zugreifen. Jeder Mitarbeiter oder Freiwillige sollte über ein eigenes Login verfügen.

Viele Dienste verwenden eine Zwei-Faktor-Authentifizierung, bei der ein Login mit einem

sekundären Gerät wie einem Mobiltelefon überprüft werden muss. Aktivieren Sie diese Funktion nach Möglichkeit, insbesondere bei kontenbezogenen Änderungen wie Passwörtern. Die Benutzer müssen auch darauf achten, wem sie Zugang zu Online-Dokumenten und -Dateien gewähren. Dokumente und Dateien, die online sind, sind so konzipiert, dass sie leicht zugänglich sind. Bestätigen Sie die richtigen E-Mails, die Sie verwenden müssen, wenn Sie den Zugriff gewähren, und prüfen Sie, ob die Person sowohl Lese- als auch Schreibzugriff auf den Inhalt benötigt.

11 MACHEN SIE SICH MIT DEN RICHTLINIEN DES CLOUD-ANBIETERS VERTRAUT.

Als Nutzer von Cloud-Diensten sollten Sie sich über die Richtlinien des Anbieters in Bezug auf Datenbesitz und Speicherort im Klaren sein.

Wenn Behörden Ihre Daten anfordern, wird der Dienstleister diesem voraussichtlich nachkommen und Ihre Daten weitergeben. Wenn Ihre Organisation gegen eine Veröffentlichung Ihrer Daten protestieren müsste, dann ist die Cloud nicht die richtige Wahl. Cloud-Daten können auch von Ihren Gegnern leichter anvisiert werden.

Eine „private“ oder „hybride“ Cloud anstelle der Public Cloud kann für Sie besser geeignet sein. Ihre Entscheidung über diese Option hängt von dem Bedürfnis Ihrer Organisation nach Exklusivität ab.

12 OFFLINE-SICHERUNGEN AUFBEWAHREN

Seien Sie darauf vorbereitet, dass der Backup-Dienst nicht verfügbar ist. Dies gilt sowohl für kostenlose als auch für kostenpflichtige Dienste. Überlegen Sie sich, welche Daten Sie in die Cloud stellen möchten, und wie sich die Unzugänglichkeit dieser Informationen auf die Betriebsfähigkeit Ihrer Organisation auswirken würde.

Laden Sie Kopien Ihrer wichtigsten Daten herunter, damit Sie auch dann darauf zugreifen können, wenn der Cloud-Service nicht verfügbar ist. Ihre Daten sollten in einem gemeinsamen Format exportiert werden können, das Sie verwenden können. Wenn dies nicht der Fall ist, überlegen Sie, ob Sie zu einem Anbieter wechseln können, der diese Option anbietet.

Bei Online-Dokumenten gibt es oft einen Audit-Trail der Änderungen. Überprüfen Sie Änderungen regelmäßig, um festzustellen, ob ein ungewöhnliches Verhalten vorliegt.

Quelle: www.hausdesstiftens.org

Related Post


Unsicherheiten der Wolken


Sicherheit im Netz

Sozial ist nicht privat