IT-Sicherheit

Tipps und Trends zum Entfernen von Dateien und zum Managen von Passwörtern

von RAin Heike Mareck, externe Datenschutzbeauftragte, Dortmund

| Haben Sie sich oder haben Ihre Mitarbeiter Ihnen schon einmal folgende Fragen zum Thema Datenschutz gestellt? „Wie lösche ich Dateien unwiderruflich, wenn ich den alten Computer entsorgen will?“ oder „Wie und wo kann ich Passwörter sinnvoll managen?“ |

Grundsätzliches

Ein Blick auf die Website (https://www.bsi-fuer-buerger.de) des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist wichtig. Unter „Aktuelles“ und „Empfehlungen“ finden Sie Hinweise und Tipps, zum Beispiel zu aktueller Schadsoftware. Legen Sie sich diese Website auf Ihre Leseliste.

Das BSI befasst sich mit Fragen rund um die IT-Sicherheit und gehört zum Bundesministerium des Innern. Ziel des BSI ist es, den sicheren Einsatz von Informations- und Kommunikationstechnik in der Gesellschaft zu ermöglichen und voranzutreiben. Kennen Sie niemanden, der sich mit der IT-Sicherheit auskennt? Dann können Sie sich telefonisch (unter 0800 2741000 kostenlos aus dem deutschen Fest- und Mobilfunknetz Montag bis Freitag von 8:00 bis 18:00 Uhr) oder per E-Mail (mail@bsi-fuer-buerger.de) mit Ihren Fragen zu Themen der IT- und Internetsicherheit an das BSI wenden.

PRAXISTIPP | Das BSI bietet mit dem „Bürger-CERT (Computer Emergency Response Team) “ (www.iww.de/s2413) einen kostenlosen Warn- und Informationsdienst, der kleine Unternehmen über Schwachstellen, Sicherheitslücken und andere Risiken informiert.

„Computerleichen“ richtig loswerden

Die Lebensdauer eines Smartphones, eines Computers oder eines Notebooks wird zunehmend kürzer. Entweder man gibt seine technischen Geräte an Dritte weiter, entsorgt sie gleich generell oder tauscht sie gegen eine Prämie ein. Doch wie entsorgt man die darauf befindlichen Daten?

In jedem Fall sollten Sie sichergehen, dass alle Daten überschrieben sind. Das BSI empfiehlt, spezielle Software zu nutzen, die kostenlos heruntergeladen werden kann. Solche Gratisprogramme sind zum Beispiel: „DBAN" und „Parted-Magic". Unter www.iww.de/s2414 finden Sie eine Anleitung, wie Sie DBAN bzw. Parted-Magic für das Überschreiben von Festplatten nutzen können.

Passwörter richtig erstellen und sicher managen (lassen)

Kennen Sie das? Sie sind neu auf der Website und benötigen dort ein Passwort. Entweder Sie greifen auf Ihr altbekanntes und häufig genutztes Passwort zurück oder Sie generieren das 154. Passwort in Ihrem Leben. Ihr Problem: Der erste Fall ist unsicher, ein Hacker könnte dann auf viele Ihrer Konten zugreifen. Im zweiten Fall haben Sie spätestens nach einer Woche das Passwort vergessen.

„Getoppt" wird das sicherlich nur noch, falls Sie ein einziges Passwort für alles nutzen. Unter den Top-Ten der beliebtesten deutschen Passwörter im Jahr 2016 befanden sich „Hallo", „Password", „Schatz" oder „Schalke04". Kein Wunder also, dass Hacker diese Passwörter auch zuerst ausprobieren. Wie kann hier Abhilfe geschaffen werden?

Unter www.iww.de/s2415 erhalten Sie wichtige Tipps zum Erstellen sicherer Passwörter. Dort erfahren Sie, was eine „Zwei-Faktor-Authentifizierung" ist, wie sie funktioniert und für höhere Sicherheit sorgen kann.

Doch was tun, wenn Sie über viele Passwörter verfügen? Sie auf einen Zettel zu schreiben und ständig mit sich herumzutragen, ist keine Lösung. Hier kann Ihnen ein Passwort-Manager helfen. Das sind Programme, die Passwörter und Benutzernamen mittels Verschlüsselung und eines komplexen Masterpassworts verwahren. Natürlich gibt es auch Nachteile: Vergessen Sie Ihr „Masterpasswort", sind im schlechtesten Fall alle Daten verloren. Dennoch: Die Vorteile überwiegen, wenn Sie viele Passwörter verwalten und voraussichtlich noch mehr hinzukommen werden. Das BSI empfiehlt u. a. den kostenlosen Passwort-Manager Keepass (https://keepass.info).

Gab es schon Zugriffe auf Ihre persönlichen Zugangsdaten?

Im Internet gibt es unterschiedliche Portale, mit denen Sie prüfen können, ob unberechtigt auf Ihre persönlichen Zugangsdaten zugegriffen wurde. Das BSI nennt hier das deutschsprachige Angebot der HPI Identity Leak Checker (https://sec.hpi.de/ilc/) und den internationalen Anbieter „Have I been pwned" (https://haveibeenpwned.com/). Aber: Eine Aussage zur Qualität und Aktualität der dort hinterlegten Daten kann man nicht treffen.

Das BSI weist zudem auf Folgendes hin: Für Zugangsdaten wird häufig die Kombination aus E-Mail-Adresse und Passwort verwendet. In den genannten Datenbanken wird meist nur die E-Mail-Adresse mit dem Datenbestand abgeglichen. Erhält man die Meldung, dass die E-Mail-Adresse im Datenbestand ist, kann sich das auf jeden Account beziehen, bei dem diese E-Mail-Adresse zum Zugang genutzt wird. Eine direkte Zuordnung ist nicht möglich.

PRAXISTIPP | Bevor Sie Ihre Daten in einen cloudbasierten Dienst überführen, sollten Sie sich die AGB und die Datenschutzerklärung des jeweiligen Herstellers genau ansehen. Für Sie ist wichtig zu wissen, wo der Cloud-Dienste-Anbieter und der Server seinen Sitz hat. Damit erfahren Sie, welchem Datenschutzrecht die Daten unterworfen sind.