Breitband/IT

BVS: PC und Daten sichern.

Datenschutz wird groß geschrieben. Gerade in Zeiten immer neuer Abhör- und Datenspionageskandale kann der Benutzer (engl. User) mit ein paar einfachen Maßnahmen für erheblich mehr Datensicherheit sorgen. Der Bundesfachbereiches EDV und Elektronik des BVS Bundesverband öffentlich bestellter und vereidigter sowie qualifizierter Sachverständiger e.V. geben nützliche Informationen und Tipps, wie der Verbraucher seine Daten besser schützen kann.Persönliche Daten gehören nicht in fremde Hände. Doch wie macht man Tablet, Laptop und PC sicher? Nicht erst seit dem Abhörskandalen ist klar, dass Verbraucherdaten gespeichert werden.

Datenträger

Ob soziale Netzwerke, Online-Shopping oder Mailversand – die persönlichen Daten werden ausgewertet und benutzt. Die (Un-) Sicherheit von IT-Systemen, der Verlust der Privatsphäre der Daten und die Angst, ständig und überall überwacht zu werden, hat spätestens seit der NSA-Überwachungsaffäre den Verbraucher erreicht. Die Möglichkeiten, Daten abzugreifen und auszuwerten, scheinen unbegrenzt und gleichzeitig besteht in vielen Bereichen eine immer größere Abhängigkeit von vernetzten IT-Systemen. Was kann man dennoch tun, um wenigstens einen Teil seiner Daten und Kommunikation, vor den Blicken Dritter zu schützen? Die öffentlichen bestellten und vereidigten Sachverständigen des Bundesfachbereiches EDV und Elektronik empfehlen, zunächst private Daten mit zuverlässigen und öffentlich prüfbaren

Verfahren zu verschlüsseln. Das open-source Werkzeug wie zum Beispiel TrueCrypt bietet beispielsweise die Möglichkeit, ganze Datenträger oder auch nur Sammlungen von Dateien sicher zu verschlüsseln, so der BVS. Es sei für die gängigen Betriebssysteme frei verfügbar und sein Quelltext liege offen und werde von einer großen, sicherheitsbewussten Community intensiv geprüft. Bisher seien hier keine Hintertüren bekannt, die es erlauben würden, die Verschlüsselung einfach zu brechen.Auch für die E-Mail Kommunikation gibt es Werkzeuge, die ein Mitlesen oder Manipulieren von Nachrichten durch Dritte sicher unterbinden können. So genannte asymmetrische Verschlüsselungsverfahren wie zum Beispiel PGP (Pretty Good Privacy), die auch als freie open-source Implementierungen für alle gängigen Betriebssysteme und mit einfachen Integrationsmöglichkeiten in übliche E-Mailprogramme verfügbar sind, ermöglichen eine sichere Kommunikation, für die aktuell keine praktikablen Angriffsmöglichkeiten bekannt sind. Mit dem Einsatz derartiger Werkzeuge steigt allerdings auch der Aufwand für das Merken von sicheren Passworten oder den Austausch von Schlüsseln mit seinen Kommunikationspartnern. Die aktuellen Implementierungen erleichtern dies dem Nutzer allerdings so weit wie möglich, so dass diese Techniken heutzutage auch von ganz normalen Anwendern im Alltag eingesetzt werden können.

Will der Verbraucher seine Daten in der Cloud ablegen, oder sie über diese synchronisieren, sollte er die aktuellen Bedingungen des jeweiligen Providers genau unter die Lupe nehmen und ggf. nachfragen, wo die eigenen Daten gespeichert werden, welche Gesetzte für die Speicherung und den Datenschutz gelten und welche Drittanbieter eventuell beteiligt sind. Deutsche und Europäische Gesetzte schützen private Daten dabei in der Regel besser, als Regelungen anderer Staaten. Im Zuge der NSA-Überwachungs-Affäre erhöhen mehr und mehr Provider ihre Sicherheitsvorkehrungen, um einen Zugriff auf gespeicherte Daten auf nichtoffiziellen Wegen oder die nachträgliche Entschlüsselung gespeicherter Daten zu erschweren. Wer hier die Sicherheit noch weiter erhöhen will, sollte seine Daten mit den eingangs genannten Werkzeugen zusätzlich verschlüsseln, bevor sie den Weg in die Cloud antreten.

Die 10 IT-Sicherheitsgebote des BVS

1. Denken Sie immer an das Prinzip der Datensparsamkeit. Geben Sie immer möglichst wenige persönliche Daten preis, das gilt sowohl im Internet als auch im normalen Leben.

2. Wenn es auf Anonymität ankommt, benutzen Sie Pseudonyme und Mailadressen, die keine Rückschlüsse auf Ihren Namen ermöglichen für Anmeldungen in sozialen Netzwerken, Foren, Blogs und Newslettern. Setzten Sie Anonymisierungsdienste ein.

3. Überprüfen Sie die Sicherheits- und Datenschutzbestimmungen Ihres E-Mail-, Cloud- und Internet-Providers. Anbieter, die an deutsche Bestimmungen gebunden sind und Ihre Daten ohne Ausnahme in Deutschland bzw. der EU speichern und verarbeiten, bieten in der Regel einen viel größeren Schutz Ihrer Daten, als internationale Anbieter. Achten Sie auf die Verwendung von „forward secrecy“, einem kryptografischen Verfahren, dass eine unerlaubte, nachträgliche Entschlüsselung von Daten verhindert.

4. Speichern Sie Ihre Adressbücher und Kontaktdaten nicht unverschlüsselt im Internet. Überprüfen Sie die Einstellungen Ihres Smartphones hinsichtlich Zugriffsrechten von Apps auf Ihre Adressbücher und entfernen Sie diese Zugriffsrechte bei allen Anwendungen, die diese Rechte nicht unbedingt benötigen.

5. Verwenden Sie auf Ihren Geräten aktuelle Viren- und Schadsoftwarescanner. Achten Sie darauf, dass der Anbieter Ihrer Software regelmäßige Signaturupdates in möglichst kurzen Zeitabständen automatisch zur Verfügung stellt, am besten mehrmals täglich.

6. Aktivieren Sie die Firewall Ihres Internet-Zugangsrouters. Setzen Sie auch auf Ihren Geräten geeignete Firewalls ein und erlauben Sie nur Anwendungen, die Sie wirklich kennen, einen Zugriff auf das Netzwerk und Internet.

7. Achten Sie bei sensiblen Arbeiten im Internet, z.B. beim Online-Banking, auf verschlüsselte Verbindungen und gültige Sicherheitszertifikate der Webserver. Lesen Meldungen zu Zertifikatsfehlern genau und ignorieren Sie diese nur in Ausnahmefällen und wenn Sie sich absolut sicher sind. Fragen Sie bei Zertifikatsfehlern auf einem Nicht-Internetweg (persönlich, per Telefon,…) auch Ihrem Dienstleister, z.B. Ihrer Bank, nach.

8. Klicken Sie keine Links an, die Ihnen per E-Mail unaufgefordert übermittelt werden. Geben Sie keine persönlichen Daten und erst Recht keine Bank- und Zugriffsdaten auf Webseiten ein, wenn Sie per E-Mail dazu aufgefordert werden.

Banken und andere seriöse Anbieter werden Sie nicht auf diese Weise kontaktieren und geheime Daten anfordern.

9. Verwenden Sie sichere, ausreichend lange Kennwörter, die aus einer Mischung von Groß- und Kleinbuchstaben, Zahlen und erlaubten Sonderzeichen bestehen. Verwenden Sie Passwörter nicht mehrfach. Verwenden Sie statt dessen geprüfte Passwort-Managementprogramme, wie z. B. die Open source Anwendung KeePass.

10. Verschlüsseln Sie sensible Daten zusätzlich selbst mit sicheren Verfahren (Truecrypt, PGP, etc.) bevor Sie diese per E-Mail versenden oder in der Cloud speichern. Achten Sie auf die Sicherheit Ihrer Schlüssel und bewahren Sie diese so sorgfältig wie Ihren Haus- oder Safeschlüssel auf.

Sachverständige in Ihrer Nähe können Sie im Sachverständigenverzeichnis unter http://www.bvs-ev.de/svz/des BVS finden. Weitere Informationen unter www.bvs-ev.de