Bundesarbeitsgemeinschaft Selbsthilfe von Menschen mit Behinderung, chronischer Erkrankung und ihren Angehörigen e.V.

Dachverband von Selbsthilfe-verbänden

BAG SELBSTHILFE
Kirchfeldstraße 149
40215 Düsseldorf

Telefon 0211.31 00 6-0
Telefax 0211.31 00 6-66
www.bag-selbsthilfe.de

Online-Beratung? Aber sicher! *(Stand Juli 2018)*

Das Internet bringt viele Vorteile mit sich - sei es die Möglichkeit, sich schnell und weitflächig zu informieren, sei es die Möglichkeit, sich umgekehrt selbst zu präsentieren und Informationen zu verbreiten. Darüber hinaus nimmt es immer mehr Einzug in unseren Alltag, sei es um Bankgeschäfte zu tätigen, sei es um Musik zu hören oder Filme anzusehen, sei es den Lichtschalter oder die Jalousien der eigenen Wohnung vom Urlaubsort aus zu betätigen. Vor allem bietet es aber auch die Chance, schnell, kostengünstig und auf einfache Weise mit anderen in Kontakt zu treten und mit ihnen zu kommunizieren. Das nutzen auch viele Selbsthilfeorganisationen, indem sie etwa ein Diskussionsforum bzw. einen Chatroom einrichten oder eine Online-Beratung anbieten.

Doch bekanntlich ist man in der Online-Welt auch zahlreichen Gefahren ausgesetzt, und Kriminelle versuchen, an Daten zu gelangen, um sie dann missbräuchlich zu verwenden, etwa für unrechtmäßige Transaktionen beim Online-Banking, zum Kauf von Waren im Namen des Geschädigten oder zur Weiterveräußerung an interessierte Firmen, die sie dann gezielt zu eigenen Zwecken verwenden. Auch wenn es keinen hundertprozentigen Schutz vor Angriffen im Internet gibt, so lassen sich doch viele Gefahren eindämmen und verringern, wenn bestimmte Sicherungsmaßnahmen ergriffen werden. Die Praxis zeigt jedoch, dass das Problem häufig nicht erkannt wird und dem Thema Sicherheit im Netz zu wenig Aufmerksamkeit gewidmet wird. Das ist umso schlimmer, wenn es sich nicht (nur) um die eigenen Daten handelt, die missbräuchlich verwendet werden, sondern um die Daten Dritter. Gerade auch bei Selbsthilfeverbänden sind immer wieder ein fehlendes Verständnis und eine unzu-

reichende Sensibilität erkennbar, mit personenbezogenen Daten von Betroffenen sorgsam und im Einklang mit den gesetzlichen Datenschutzregelungen umzugehen. Umso wichtiger ist es, sich neben dem Daten*schutz* auch mit der Daten*sicherheit* hinreichend zu befassen. Hierzu soll die vorliegende Übersicht einige wichtige Hinweise für Selbsthilfeorganisationen geben, auf welche diesbezüglichen Aspekte zu achten ist, wenn sie beispielsweise Online-Beratung anbieten, die Möglichkeit zum gegenseitigen Austausch in einem Diskussionsforum anbieten oder auch nur generell im Netz unterwegs und aktiv sind.

Firewall-Schutz

Unter dem Begriff „Firewall“ versteht man einen Filter, der einen Computer vor unerlaubten Zugriffen (aus dem Internet bzw. einem Netzwerk, mit dem der PC verbunden ist) schützt. Mit einer Firewall wird verhindert, dass unbefugte Dritte sich Zugang zu einem Rechner verschaffen und die dortigen Daten einsehen und verändern können; zudem wird verhindert, dass ungewollt Daten des Angreifers auf dem Computer hinterlassen werden (insbesondere in Form von sog. Malware, also z.B. Computerwürmer oder Trojaner). Unerwünschte Programme und unerwünschter Datenverkehrt werden mit Hilfe einer Firewall also blockiert.

Heutzutage ist nahezu jeder Rechner mit dem Internet verbunden und deshalb sollte auch bei keinem Computer ein Firewall-Schutz fehlen. Mit diesem lassen sich also die eigenen Zugriffe auf das Internet und das ggf. verwendete Netzwerk kontrollieren und der Datenverkehr in beiderseitiger Richtung absichern. Verwendete Anwendungen werden geprüft und im Falle gefährlicher oder verdächtiger Aktivitäten wird der Nutzer entsprechend alarmiert.

Man unterscheidet zwischen einer sog. Personal Firewall (auch als Desktop Firewall bezeichnet) und einer sog. Externen Firewall (auch bekannt als Hardware Firewall). Letztere stellt eine Abschirmung durch Verwendung von Hardware-Technologie dar und ist eher in größeren Firmen oder bei Behörden anzutreffen, wo sie in erster Linie den Datenverkehr zwischen zwei Netzwerken kontrollieren und einschränken soll. Im Regelfall und insoweit vor allem bei heimischen privaten Computern wird eine Personal-Firewall verwendet, die als Software direkt auf dem Computer eingerichtet wird.

Eine Firewall ist eigentlich immer bereits beim betreffenden Produkt installiert und wird somit beim Kauf mitgeliefert. Wichtig ist jedoch, dass sie richtig konfiguriert, d.h. optimal eingestellt und natürlich auch aktiviert ist.

In diesem Zusammenhang ist auch zu empfehlen, immer einen modernen Internet-Browser mit möglichst neuesten Sicherheitsmechanismen zu verwenden, wobei aber nur solche Browser-Zusatzprogramme wie PlugIns und Add-ons verwendet werden sollten, die tatsächlich benötigt werden.

Antiviren-Programm

Im Netz sind in hohem Maße als Schadsoftware oder Malware (malicious software) bekannte Programme bzw. Codes unterwegs, die darauf angelegt sind, andere Software zu „infizieren“ und nachteilig zu verändern. Am bekanntesten sind die sog. Computerviren, aber auch Würmer, Trojaner, Spyware oder Adware gehören zur Malware. Sie können Festplatten beschädigen, das Betriebssystem angreifen oder zerstören, Daten löschen, diese aber auch stehlen und somit – je nach Art des Angriffs oder der entwendeten Daten – großen Schaden anrichten.

Der zuvor beschriebene Firewall-Schutz sollte daher immer mit einem effektiven Antiviren-Programm kombiniert werden, wobei zwar viele wirksame Programme kostenlos im Internet heruntergeladen werden können, es aber gerade vor dem Hintergrund der Verarbeitung sensibler Daten Dritter in einer Selbsthilfeorganisation überlegenswert ist, durch eine finanzielle Investition in eine Kauf-Software zusätzlichen Schutz zu erreichen.

Aber auch dann, wenn ein Antiviren-Programm installiert und aktiviert ist, kann es passieren, dass sich Malware auf Ihrem Computer befindet, was sich etwa durch eine langsame Geschwindigkeit, durch häufige „Abstürze“, ein nicht enden wollendes Laden des Betriebssystems oder durch ungewöhnliche Fehlermeldungen zeigen kann. Malware auf Ihrem E-Mail-Konto kann dadurch erkennbar werden, dass Ihnen E-Mails ohne Absender oder ohne Betreff zugesandt werden bzw. umgekehrt, dass von Ihrem E-Mail-Konto Spam-Mails versandt werden.

Hilfreich ist es, einen regelmäßigen Sicherheits-Scan durchzuführen, der bei den meisten Sicherheits- bzw. Antiviren-Programmen automatisch durchgeführt wird. Ist Ihr Computer von Malware befallen, teilt Ihnen das Programm i.d.R. mit, welche Schritte erforderlich sind bzw. nimmt die ersten Schritte zur „Gefahrenabwehr“ (z.B. Verschiebung in den sog. Quarantäne-Ordner) selbst vor. Ein Weiterarbeiten am PC trotz erkannter Malware sollte auf jeden Fall unterbleiben; im Zweifel muss ein IT-Spezialist zu Rate gezogen werden.

Sicherheits-Updates

Achten Sie stets darauf, regelmäßig aktuelle Sicherheitsupdates vorzunehmen bzw. diese automatisch installieren zu lassen. Das betrifft sowohl Ihr Betriebssystem insgesamt als auch einzelne Programme (wie Internet-Browser, Adobe Reader, Flash Player etc.). Veraltete Versionen bieten nicht mehr den erforderlichen Schutz und lassen darüber hinaus oftmals auch nur noch eine eingeschränkte Nutzung des Programms zu.

Benutzer-Konto

Auf das Internet sollte möglichst nur über das sog. Benutzerkonto (mit eingeschränkten Rechten) und nicht über ein Administrator-Konto zugegriffen werden. Die Möglichkeit, sich als Nutzer mit eingeschränkten Rechten anzumelden, bieten nahezu alle Betriebssysteme.

Passwörter

Passwörter sollten möglichst sicher gewählt werden, wobei die Verwendung einer Buchstaben- oder Zahlenreihe („abcde“ oder „12345“) selbstredend genauso vermieden werden sollte wie der eigene Name oder das eigene Geburtsdatum. Am besten eignet sich eine Kombination aus Klein- und Großbuchstaben, Zahlen und Zeichen. Außerdem sollte für jeden einzelnen genutzten Dienst im Netz, für den ein Passwort benötigt wird, ein jeweils eigenes Passwort verwendet werden. Überdies sollten die Passwörter auch regelmäßig geändert werden.

Aufräumen und Sichern

Nicht mehr benötigte Programme sollten deinstalliert werden, damit umso weniger „Angriffsfläche“ vorhanden ist. Im Übrigen sollten regelmäßige „Backups“ vorgenommen werden, um die Daten vor Verlust zu schützen.

Verschlüsselung

Die Verschlüsselung von Nachrichten stellt eine weitere wirksame Maßnahme zum Schutz vor unberechtigten Zugriffen Dritter auf diese Informationen dar.

Eine Verschlüsselung funktioniert vom Prinzip her so, dass die Buchstaben des zu verschlüsselnden Textes anhand einer Ersetzungstabelle gegen andere Buchstaben ausgetauscht werden. Für Hacker ist es heutzutage allerdings recht leicht, eine solch einfache Methode im Wege einer Buchstabenzählung und Vergleichsanstellung zu durchschauen und die verwendete Ersetzungstabelle selbst zu erstellen. Aus diesem Grunde sind moderne Verschlüsselungsverfahren weitaus komplizierter gestaltet und bieten dementsprechend auch weitaus mehr Sicherheit.

Problematisch ist allerdings, dass Verschlüsselungen immer auf Kosten der Leistung gehen, da insoweit Rechenkapazität und Energie benötigt werden. Das bedeutet, dass ein leistungsschwacher Computer im Falle einer Verschlüsselung des Gesamtsystems spürbar langsamer werden kann. Auch sind Daten, die neben verschlüsselten Informationen unverschlüsselt gespeichert oder in der Umgebung aufbewahrt werden, weiterhin nicht hundertprozentig vor Angriffen sicher. Schließlich kann es passieren, dass der Schlüssel aufgrund eines Defekts oder durch Diebstahl (etwa eines USB-Sticks, auf dem er abgelegt ist), verloren geht. Der Schlüssel sollte daher vorsorglich auch auf einer Sicherheitskopie abgelegt werden, die an einem anderen Ort aufbewahrt und unter Verschluss gehalten wird, so dass im Verlustfall immer noch auf die Daten zugegriffen werden kann.

Ferner ist zu berücksichtigen, dass das für eine Verschlüsselung verwendete Passwort hinreichend sicher sein sollte. Dabei ist aber immer mit zu bedenken, dass auch vermeintlich sichere Passwörter grundsätzlich ausgespäht werden können, etwa durch ein von Schadsoftware verursachtes Mitprotokollieren von Tastatureingaben. Nichtdestotrotz ist – wie bereits oben dargestellt – ein Passwort, das z.B. eine Buchstaben- oder Zahlenreihenfolge wie „abcde“ bzw. „34567“ enthält weitaus leichter zu entziffern als ein Mix aus Klein- und Großbuchstaben sowie Zahlen und Zeichen.

Verschlüsselungen können auf verschiedene Weise vorgenommen werden. So besteht etwa die Möglichkeit, im Betriebssystem Verschlüsselungen durchzuführen. Windows bietet zum Beispiel mit dem Encrypted File System (EFS) die Möglichkeit, Dateien und Ordner zu verschlüsseln, die auf Festplatten mit dem Dateisystem NTFS gespeichert sind (verwendetes Dateisystem zu finden unter: „Windows-Explorer“ > Eigenschaften > allgemein). Hierzu ist bei der betreffenden Datei oder dem Ordner

die Rubrik „Eigenschaften“ aufzurufen, wobei dann unter „Erweitert“ die Möglichkeit zur Verschlüsselung gegeben ist. Auch hier es sinnvoll, verwendete Schlüssel und Zertifikate für den Fall eines Datenverlustes oder einer Neuinstallation des Systems extern zu sichern. Dies ist über die Microsoft Management Console möglich.

Auch für Nutzer des Appel Mac OS X – Betriebssystems bestehen Möglichkeiten zur Verschlüsselung, und zwar über FileVault; ab dem Betriebssystem Mac OS X 10.7 (Lion) verschlüsselt FileVault 2 ganze Festplattenpartitionen. Hier geht es aber in erster Linie darum, die gespeicherten Daten bei Verlust des Rechners vor dem Zugriff Fremder zu schützen. Darüber hinaus bietet Mac OS X die Möglichkeit, verschlüsselte Disk-Images anzulegen, worin beliebige Dateien gespeichert werden können.

Neben Verschlüsselungen im Betriebssystem besteht auch die Möglichkeit zur Verschlüsselung mit entsprechenden Software-Programmen, die teilweise sogar kostenlos aus dem Internet heruntergeladen werden können. Hierzu gehören die beiden allein für Verschlüsselungszwecke entwickelten Programme TrueCrypt sowie GNU Privacy Guard for Windows (Gpg4Win). Letzteres ist ein aus mehreren Programmen bestehendes Paket zum Verschlüsseln im Rahmen von Microsoft-Windows-Betriebssystemen und wurde vom Bundesamt für Sicherheit in der Informationstechnik beauftragt. Die Software kann allerdings nur auf bereits bestehende Schlüssel und Zertifikate zurückgreifen, weshalb ein Anwender solche zunächst erstellen oder importieren muss. Gpg4Win eignet sich übrigens auch zur Verschlüsselung von E-Mails.

Neben Software-Anwendungen besteht schließlich auch die Möglichkeit zu einer Hardwareunterstützten Verschlüsselung. So sind vor allem zahlreiche Notebooks bereits von vornherein mit einem Chip ausgestattet, der als Schlüsselspeicher bei der Verschlüsselung von Daten dient (sog. Trusted Platform Module – TPM). Dabei speichert die insoweit genutzte Software Bitlocker bei der Verschlüsselung der Festplatte den zum Entschlüsseln notwendigen Schlüssel auf dem TPM. Bei Änderungen der Systemkonfiguration – etwa durch ein versuchtes Auslesen der Daten - kann die Festplatte nicht mehr entschlüsselt werden, weil der Chip den Zugriff auf den Schlüssel verweigert. Die Bitlocker-Software ist inzwischen auch für externe Datenträger, z.B. USB-Sticks, verwendbar (sog. „Bitlocker to go“).

Darüber hinaus verfügen die meisten Festplatten über eine eingebaute Verschlüsselungsoption. Als Basisschutz dient dabei zunächst die Möglichkeit, dass auf die gespeicherten Daten nur über ein eingegebenes Passwort Zugriff genommen werden kann. Die Daten selbst bleiben in der Regel erst einmal unverschlüsselt und

müssen – wenn gewollt – in einem zweiten Schritt ihrerseits noch verschlüsselt werden.

Hinzuweisen bleibt ferner noch auf moderne Verschlüsselungstechniken wie Festplattengehäuse, die einen Zugriff beispielsweise erst durch einen Fingerabdruck des Berechtigten oder durch Eingabe eines Codes erlauben.

Wichtig für den Bereich der Online-Beratung ist nicht zuletzt die verschlüsselte Kommunikation:

Wer beispielsweise eine E-Mail verschickt, sollte sich darüber im Klaren sein, dass diese grundsätzlich von jedem gelesen werden kann, der diese zum Empfänger „transportiert". Drei Gefahren lauern insoweit: die Vertraulichkeit kann verletzt werden, das heißt ein unbefugter Dritter kann Kenntnis vom Inhalt der Nachricht erlangen; der Absender der Mal ist nicht sicher bzw. kann nicht hundertprozentig als echt identifiziert werden; es besteht die Gefahr, dass der Inhalt der Nachricht verändert wird.

Um diesen Gefahren zu begegnen, sind Verschlüsselungen ein durchaus wirksames Mittel, über das gerade Vereine, die Online-Beratung anbieten oder einen Chatroom eingerichtet haben, nachdenken sollten. Das gilt insbesondere dann, wenn – wie bei Selbsthilfeorganisationen im Regelfall – Gesundheitsaspekte und sonstige höchst persönliche Dinge zur Sprache kommen.

Es gibt zwei Verfahren für die verschlüsselte E-Mail-Kommunikation:

S/MIME ist eine Verschlüsselung, die in vielen Mail-Programmen von vornherein integriert ist, allerdings lässt es sich nur mit einem von einem Anbieter erstellten Zertifikat für die E-Mail-Adresse des Anwenders sinnvoll nutzen.

PGO ist eine kommerzielle Software, wobei es auch die – bereits zuvor erwähnte – frei verfügbare Variante GPG gibt. Für diese Software bestehen Plug-Ins für die meisten E-Mail-Programme. Anders als bei S/MIME können bei GPG alle nötigen Schlüssel selbst erstellt werden. Genaue Informationen zum Verschlüsselungs-programm Gpg4win finden sich u.a. auf der Internetseite www.bsi.bund.de.

Für eine Verschlüsselung ist erforderlich, dass beide Kommunikationspartner über ein Verschlüsselungsprogramm verfügen, das nicht notwendigerweise dasselbe sein muss. Das jeweilige Verschlüsselungsprogramm erstellt sodann einen sog. öffent-lichen sowie einen geheimen Schlüssel. Der öffentliche Schlüssel muss gegenseitig

ausgetauscht werden, damit der jeweilige Kommunikationspartner seine Nachricht mit dem öffentlichen Schlüssel des anderen verschlüsseln kann. Mit seinem geheimen Schlüssel kann der Empfänger die Nachricht sodann entschlüsseln und lesen.

Zusätzlich kann die E-Mail mit einer digitalen Signatur versehen werden, die das Zertifikat und den öffentlichen Schlüssel des Empfängers enthält. Damit kann letzterer feststellen, ob die Mail tatsächlich von dem angenommenen Absender stammt und überdies auch nicht verändert wurde. Es handelt sich hierbei aber nicht um die bekannte E-Mail-Signatur (Name und Webadresse), die al zusätzliche Bestätigung, wer der Versender ist, häufig an E-Mails angehängt wird, und auch nicht um eine sog. qualifizierte elektronische Signatur, die quasi die handschriftliche Unterschrift im EDV-Bereich ersetzt.

Übrigens ist es auch möglich, das Abrufen von E-Mails zu sichern, indem die entsprechenden Verbindungen verschlüsselt werden. Bei Webmailern erkennt man dies daran, dass der Name der Seite bzw. die URL mit „https“ beginnt und überdies meist ein Schloss-Symbol enthält. In Bezug auf die eigenen Mail-Programme ist es ratsam, für das E-Mail-Konto die Verschlüsselungstechnik SSL, TLS oder STARTTLS zu aktivieren.

Mit Hilfe sog. Virtueller Privater Netzwerke (VPN) ist es möglich, im Internet abgetrennt von allen anderen Datenbereichen zu kommunizieren. Möglich ist es insoweit, sich mit seinem Notebook oder Smartphone in ein öffentliches WLAN einzubuchen und sich hierüber mit dem betreffenden VPN (z.B. seines Unternehmens) – i.d.R. verschlüsselt – zu verbinden, wenn das Notebook oder das Smartphone zuvor als eines der Endpunkte des VPN festgelegt worden ist. Das klappt natürlich grundsätzlich auch, wenn man sich von unterwegs mit seinem privaten Netz zuhause verbinden möchte und der eigene Router eine entsprechende VPN-Funktion besitzt.

Vorsicht walten lassen

Eine der wichtigsten Sicherungsmaßnahmen liegt abseits technischer Vorrichtungen und IT-Anwendungen: es kommt in hohem Maße auch auf die eigene Aufmerksamkeit und Vorsicht bei der Nutzung des Internets und beim E-Mail-Verkehr an. Dass das Öffnen von E-Mail-Anhängen unbekannter oder verdächtiger Absender tunlichst unterbleiben sollte, dürfte hinreichend bekannt sein. Nichtdestotrotz passiert es doch immer wieder, sei es aus Versehen, sei es weil mit sog. Pishing-Mails (genauso auch

mit Webseiten, Kurznachrichten o.a.) gearbeitet wird, also Mails die einen anderen Absender vortäuschen. So sind vielen die gefälschten Nachrichten bekannt, bei denen das Logo und sonstige Angaben ihrer Bank oder Sparkasse verwendet werden und den Eindruck erwecken, sie stammen tatsächlich von ihrem Kreditinstitut. Bei näherem Hinsehen fällt allerdings schnell auf, dass es hier wesentliche Angaben fehlen, und wenn dann noch aufgefordert wird, die persönliche PIN oder sonstige vertrauliche Angaben zu machen, sollte die Mail möglichst rasch gelöscht werden.

Vorsicht ist auch beim Surfen im Internet geboten; Webseiten sollten genau angesehen werden, ob es sich wirklich um die gewünschte Seite handelt und nicht um eine nachgemachte, die aufgrund des versehentlichen Eingebens einer falschen Buchstabens in der Adresse stattdessen aufgerufen wurde, bevor man hier weitere Daten eingibt. Auch von Seiten, die aufgrund einer Suchanfrage in der Ergebnisliste der Suchmaschine aufgeführt werden, jedoch unseriös oder undurchsichtig erscheinen, sollten man besser die Finger lassen und gar nicht erst aufrufen. Vor allem sollte man mit der Weitergabe persönlicher Informationen zurückhaltend sein.

beranet – „Selbsthilfe(gruppen) online“

Abschließend noch ein Hinweis auf das von der Agentur Zone35 zusammen mit der BAG SELBSTHILFE entwickelte Software-Feature „Selbsthilfe(gruppen) online“ auf der Basis der Onlineberatungslösung *beranet*, das den Mitgliedsorganisationen der BAG SELBSTHILFE im Rahmen des gleichnamigen Projekts bekannt gemacht worden ist.

Diese Online-Plattform bietet ein optimiertes und individualisierbares Angebot für Selbsthilfeorganisationen, mit ihren Mitgliedern in Kontakt zu treten und auch den Austausch der Mitglieder untereinander, etwa über sog. Chats, zu fördern. Dieses Beratungskonzept beinhaltet selbstverständlich auch Sicherheitsaspekte im Rahmen der jeweiligen vorgeschlagenen Onlineberatungs-Lösung.

Bei Interesse wenden Sie sich bitte an:

BAG SELBSTHILFE e.V. – Frau Sonja Liebherr, Tel: 0211-31006-55
Mail: sonja.liebherr@bag-selbsthilfe.de
(www.beranet.de/selbsthilfe-im-netz)