Digitale Sicherheit für frauenspezifische Einrichtungen

Helga Hansen

Neben Strategien und Tipps, die die Betroffenen von digitaler Gewalt und ihre Sicherheit in den Fokus nehmen[1], ist es wichtig, sich die digitale Sicherheit von Organisationen und Einrichtungen genauer anzuschauen. Einige grundsätzliche Hinweise, etwa zur Erstellung sicherer Passwörter, gelten wie zuvor beschrieben. An anderer Stelle müssen aber andere Entscheidungen getroffen werden.

Im ersten Schritt geht es um mögliche Bedrohungsszenarien, deren konkrete Bewertung vermutlich in jeder Einrichtung unterschiedlich abläuft. Der in diesem Artikel beschriebene Plan zur digitalen Sicherheit ist adaptiert aus dem Guide »Your Security Plan« (2019) der US-amerikanischen Bürgerrechtsorganisation Electronic Frontier Foundation (EFF), die zu Themen wie Datenschutz und Überwachung aufklären sowie Betroffene vor Gericht vertreten. Anschließend folgen Tipps zum strukturierten Absichern der digitalen Infrastruktur, angelehnt an die CIS Controls V7.1 (2019) – Empfehlungen des Center for Internet Security (CIS), einem Zusammenschluss von Firmen, Organisationen und Forschungseinrichtungen rund um das Thema Internet-Sicherheit.

Bedrohungsszenarien

Je mehr Zeit und Geld zur Verfügung stehen, umso bessere digitale Sicherheitsmaßnahmen können umgesetzt werden – aufgrund der eingeschränkten

1 Siehe Beitrag: Digitale erste Hilfe und Sicherheitsprinzipien für Berater*innen bei digitaler Gewalt.

Finanzierung von frauenspezifischen Einrichtungen ist beides oft Mangelware. Dennoch lassen sich mit einigen einfachen Überlegungen wichtige Grundlagen schaffen. Um vernünftig einschätzen zu können welche Maßnahmen realistisch sind, gilt es zunächst, die eigene Lage hinsichtlich möglicher Bedrohungen zu bewerten. Die EFF schlägt dafür im Security Plan fünf Fragen vor, die übrigens auch bei der Sicherheitsbetrachtung nicht-digitaler Güter funktionieren.

Was gilt es zu schützen?
Zu den digitalen Gütern, die geschützt werden müssen, gehören zum einen Informationen wie Kontaktdaten, Nachrichten, E-Mails und Dateien. Zum anderen können dies auch elektronische Geräte sein, wie z.B. Diensttelefone. Welche (sensiblen) Daten in europäischen Beratungsstellen gesammelt, gespeichert und weitergegeben werden, muss seit der Einführung der Datenschutzgrundverordnung (DSGVO) bereits dokumentiert sein. Die DSGVO bietet einen guten Anlass, die Praxis der Datensammlung und -verarbeitung zu überprüfen und gegebenenfalls zu überdenken.

Vor wem müssen Daten/Geräte geschützt werden?
Diese Überlegung ist grundlegend für einen umfassenden Plan. Hierbei kann es sich um Personen handeln (z.B. Partner von Klientinnen, Antifeminist*innen) oder aber Vereinigungen, die feministischen Organisationen schaden wollen (z.B. antifeministische und/oder rechte Gruppen). Je nach den Schwerpunkten ihrer Arbeit und konkreten Fällen könnten auch Behörden wie die Polizei oder Ausländerbehörde ein Interesse haben auf ihre Informationen zurück zu greifen. Schließlich können selbst zufällige Hacker*innen-Angriffe oder die Datenauswertung durch Internetfirmen prinzipiell ein Problem darstellen.

Wie schwerwiegend sind die Konsequenzen, wenn etwas schief geht?
Bei Angriffen durch (Ex-)Partner von Klientinnen besteht die Gefahr, dass eine gewaltausübende Person die neue Telefonnummer oder den Aufenthaltsort ihres Opfers herausfindet und unerwünscht Kontakt aufnimmt bzw. die Person gefährdet. Hacker*innen sind nicht unbedingt an konkreten Informationen interessiert – wenn eine Schadsoftware den Rechner unbenutzbar macht, kann es aber viel Zeit und Geld kosten, bis die Arbeit in der Einrich-

tung wieder möglich ist. Auch bei Angriffen durch Organisationen ist dies eine Gefahr.

Wie wahrscheinlich ist es, dass etwas schief geht?
Ebenso unterschiedlich wie die Auswirkungen sind die Wahrscheinlichkeiten, ob etwas eintritt. Daher ist es wichtig mit Computerfachpersonen Szenarien durchzuspielen und zu überlegen, welche Angriffe vorstellbar oder wahrscheinlich erscheinen.

Wie viele Ressourcen stehen zur Verfügung?
Die letzte Vorüberlegung ist die Frage, wieviel Zeit und Geld aufgewendet werden kann, um Bedrohungen abzuwenden. Dabei gilt: Absicherung kostet, aber etwas Sicherheit ist besser als keine Maßnahme. Wenn das Geld nicht für einen neuen Router reicht, ist eine veraltete Verschlüsselung immer noch besser als keine Verschlüsselung einzurichten. Der Aufwand hingegen ist etwas, was NGOs aufbringen müssten, wenn sie ihre Organisationen auch digital schützen wollen. Mit diesen Überlegungen im Hinterkopf ist es Zeit, die eigene digitale Infrastruktur durchzugehen.

Hardware überprüfen

Mit Hardware sind alle elektronischen Geräte gemeint. Um diese zu überprüfen ist es wichtig, zunächst eine Bestandsaufnahme zu machen; hierzu gehört die Auflistung aller Rechner, Smartphones, Router, Sticks etc., die im Büro oder an anderer Stelle für dienstliche Tätigkeiten genutzt werden. Wie bei Listen für die Verwendung von Schlüsseln ist es wichtig, in der Aufstellung deutlich zu machen, wer über welche Geräte verfügen bzw. nicht verfügen darf. Auch über ihre privaten Smartphones, die sie mit ins Büro bringen, sollten sie einen Überblick haben, um unbekannte Geräte schnell zu erkennen. Sollte jemand in der Beratungsstelle tatsächlich oder vermeintlich eines vergessen haben, ist Vorsicht geboten, denn es könnte zum Ausspionieren genutzt werden. In einem solchen Fall ist es wichtig, das Gerät auszuschalten und sicher aufzubewahren.

Um in der Beratungsstelle die digitale Sicherheit der betroffenen Frauen zu überprüfen und zu verbessern, kann es sinnvoll sein, Internetzugänge für Klientinnen bereit zu stellen. Während für die eigenen Rechner möglichst Kabel genutzt werden sollten, ist das Anschließen von weiteren Rechnern an das

eigene Netzwerk ein Einfallstor für Schadsoftware. Daher ist es sinnvoll ein WLAN für Klientinnen und Besucher*innen einzurichten, das nur in Beratungen genutzt wird und dessen Zugangsdaten regelmäßig geändert werden. Alle drahtlosen Netzwerke sollten nur verschlüsselt genutzt werden. Bei digitalen Notfällen, wie dem Auffinden von Spionagesoftware, sind USB-Sticks und DVDs sehr hilfreich, mit denen ein Rechner neu aufgesetzt werden kann. Es ist daher sinnvoll, diese für sich und Klientinnen vorzuhalten, damit die Geräte schnell wieder einsetzbar sind.

Software überprüfen

Mit Software sind sämtliche Programme gemeint. Ähnlich wie bei der Überprüfung der Hardware ist eine Auflistung der Programme sehr wichtig. Bei Windows-Rechnern ist sie über die Systemsteuerung und bei Mac-Rechnern über den Systembericht zu finden. Wichtig ist regelmäßig zu überprüfen, ob es Programme gibt, die länger nicht genutzt wurden; diese sollten gelöscht werden. Bei Unsicherheiten, ob ein Programm wichtig ist, hilft meist eine Google-Suche weiter.[2] Auch ist zu überlegen, ob die bisher verwendeten Programme die besten Lösungen sind. Ein positives Kriterium ist, dass es regelmäßige Updates gibt, mit denen Sicherheitslücken geschlossen werden. Ein weiteres Kriterium ist etwa, ob Programme oft Ziel von Hacker*innen-Angriffen sind, wie etwa Microsoft Word. Mit dem Einsatz der Open-Source-Software LibreOffice lässt sich das vermeiden – sie nützt aber nichts, wenn die Berater*innen mit dem Programm nicht arbeiten können. Daher gilt es, eine Balance zwischen Sicherheit und realistischen Anwendungsmöglichkeiten zu finden.

Diese Hinweise gelten auch innerhalb von Programmen: In den Einstellungen ist zu sehen, ob und wenn ja, welche Erweiterungen installiert sind. Je nach Programm können diese Zusätze »Plugins« oder »Add-ons« heißen. Besonders im Browser werden Plugins gern beim Download völlig anderer Software als unerwünschte Zugabe installiert, um beispielsweise die Standardsuchmaschine zu ersetzen. Im Zweifelsfall können Browser-Plugins einfach gelöscht werden. Eine Ausnahme sind Plugins zum Blocken von Werbung und Tracking. Über Werbung wird manchmal schädliche Software verbreitet, für

2 Siehe Beitrag: Digitale erste Hilfe und Sicherheitsprinzipien für Berater*innen bei digitaler Gewalt.

deren Ausbreitung man nicht einmal auf die Anzeige klicken muss. Der Fachbegriff dafür lautet »Malvertising«, eine Kombination der englischen Begriffe »Malware« für Schadsoftware und »Advertising« für Werbung. Erweiterungen wie AdBlock Plus oder uBlock Origin blockieren Werbung.

Up-to-date bleiben

Da das Internet ein schnelllebiges Medium ist und ständig neue digitale Geräte erscheinen, ist es wichtig, auf dem Laufenden zu bleiben, um aktuelle Bedrohungen und Gegenmaßnahmen einschätzen zu können. Das gilt auch für die eingesetzte Software, die stets auf dem neusten Stand sein sollte. Dazu kann inzwischen bei vielen Programmen die Funktion Auto-Update aktiviert werden, mit der neue Updates automatisch installiert werden. Wird ein Virenscanner genutzt, sollte dieser sich ebenfalls eigenständig selbst, wie auch die verwendeten Virendefinitionen, regelmäßig aktualisieren.

Immer wieder werden Passwörter von E-Mail- und Social Media-Accounts etc. geknackt und öffentlich gepostet (geleakt). Eine Möglichkeit sicherzugehen, dass Accounts der Beratungsstelle nicht betroffen sind, ist eine Überprüfung bei Diensten wie dem »Identity Leak Checker« des Hasso-Plattner-Instituts. Ebenso ist es wichtig im Blick zu behalten welche Datenlecks bekannt werden. Sinnvoll ist schließlich, regelmäßig sich selbst, bzw. die eigene Einrichtung in Suchmaschinen und Social Media zu suchen, um zu überprüfen, ob die Daten aktuell sind und keine Informationen zu finden sind, die geheim bleiben sollten. Das Einrichten eines »Google Alerts« kann dabei sehr hilfreich sein und viel Zeit sparen. Soziale Netzwerke und Google bieten außerdem Möglichkeiten, um falsche Ergebnisse zu melden – meist sind dazu aber Accounts nötig.

Rechte-Management

Eine grundlegende Frage für jede Organisation sind die Zugriffsrechte, also wer auf was zugreifen darf oder nicht. Neben Beschränkungen für Nutzer*innen-Accounts sind dabei auch Passwörter wichtig. Auch hier sorgt eine Auflistung dafür, dass im Blick bleibt, über welche Netzwerke, Accounts etc. die Beratungsstelle kommuniziert und wer welche Rechte hat oder haben soll. Alte und ungenutzte Konten sollten in diesem Prozess gelöscht werden.

Ob Windows-, Mac- oder Linux-Rechner – auch in Betriebssystemen haben die Nutzer*innen-Konten unterschiedliche Rechte. Admin-Rechte und das entsprechende Passwort ermöglichen die Installation von jeglicher Software. Ein Administrator*innen-Konto ist daher auf jedem Rechner nötig, sollte aber nur bei Bedarf genutzt werden. Für die tägliche Arbeit sollten stattdessen Konten mit begrenzten Rechten eingesetzt werden. Sie erlauben unter Windows immer noch die Installation einiger Software und das Ändern einiger Einstellungen.

Ältere Windows-Versionen umfassen noch Gast-Accounts, mit deren Zugangsdaten keine Software installiert werden kann. Um Gäste-Konten unter Windows 10 zu ermöglichen, muss die Kommandozeile genutzt werden. Das klingt zunächst oft einschüchternd, bedeutet aber in der Praxis nur wenige Klicks, die entsprechende Anleitungen im Internet erläutern. Die Windows-10-Home-Edition unterscheidet immerhin zwischen Familienmitgliedern und »anderen Benutzern«. In den Einstellungen werden diese »Kontotypen« unter »Konten« verwaltet. Inzwischen drängt Hersteller Microsoft dabei auf den Einsatz eines Microsoft-Kontos und die Angabe von Kontaktdaten. Das Anlegen von lokalen Nutzer*innen-Accounts ist aber ohne diese Angaben möglich. Der Schutz vor unerwünschten Zugriffen ist nur effektiv, wenn ein Rechner konsequent gesperrt wird, sobald der Schreibtisch verlassen wird.

Für die Auswahl von Passwörtern gilt, dass diese möglichst lang sein sollten; außerdem sollte für jeden Account ein anderes Passwort gewählt werden. Sie sollten geändert werden, sobald es einen konkreten Anlass gibt, etwa beim Personalwechsel. An dieser Stelle ist der Einsatz von Passwortmanagern unbedingt zu empfehlen, mit denen sehr lange Passwörter generiert und einfach ausgetauscht werden können. Selbst häufige Wechsel durch kurzzeitig tätige Praktikant*innen oder Freiwillige sind dann kein Problem. Neben Programmen, die für Einzelpersonen gedacht sind, gibt es auch Lösungen für Firmen und Organisationen. Diese können so eingestellt werden, dass Nutzer*innen die Zugangsdaten für verschiedene Accounts gar nicht selbst kennen müssen, sondern allein ihr Passwort für den Passwortmanager. Allerdings kosten die Programme Geld: meist handelt es sich um Abos, die abhängig von der Zahl der Nutzer*innen teurer werden. Manche Programme können auf eigenen Servern installiert werden, während andere auf Cloud-Dienste setzten. Hier muss abgewägt werden, welche Lösung für die Einrichtung die sinnvollste ist.

Neben dem Passwort ist bei der Zwei-Faktor-Authentifizierung (2FA) ein zweiter Faktor in Form eines Codes oder Hardware-Schlüssels nötig, um sich in Rechner, Programme oder Konten einzuloggen. Wenn der zweite Faktor

fehlt, da zum Beispiel das Handy verloren gegangen ist, an das ein Code gesendet wird, ist allerdings auch der Zugriff zum Account unmöglich. Sinnvoll ist daher, zwei 2FA-Methoden zu nutzen. Dies können entweder zwei komplett unterschiedliche Methoden sein oder es wird eine Methode doppelt genutzt. Bei Hardware-Schlüsseln hieße dies, zwei Schlüssel zu nutzen und einen stets bei sich zu tragen, während der andere für Notfälle sicher aufbewahrt wird. Wer eine 2FA-App nutzt, sollte die App neben dem Smartphone auf einem zweiten Gerät, wie einem Tablet oder Zweit-Telefon, installieren.

Weitere Einstellungen

Unbekannte Hardware wie USB-Sticks, Festplatten oder CDs sollte grundsätzlich nicht sorglos in Rechner eingesteckt werden. Da es sich manchmal nicht vermeiden lässt und um bei Versehen ein Stück sicherer zu sein, sollte zumindest das automatische Abspielen unterbunden werden. In den Einstellungen von Windows kann dies unter »Geräte« im Punkt »Automatische Wiedergabe« eingestellt werden.

Einige Dokumente und Informationen müssen lange vorgehalten werden. Um sie sicher aufzubewahren, sind wiederkehrende Backups notwendig. Im Idealfall stellt man dies mit der 3-2-1-Regel sicher: Es sollten drei Kopien wichtiger Daten existieren, die auf zwei unterschiedlichen Datenträgern untergebracht sind, wobei jeder Datenträger an einem anderen Ort steht. In der Praxis bedeutet dies beispielsweise die Originaldatei auf dem Rechner, eine Kopie auf einer lokalen Festplatte und eine Kopie in einer Cloud-Lösung. Neben Festplatten sind USB-Sticks und CDs mögliche Backupmedien, die aber jeweils Nachteile haben. Sticks gehen aufgrund ihrer Größe schneller verloren und selbst wiederbeschreibbare CDs können nicht so oft genutzt werden wie Festplatten. Mit der 3-2-1-Regel sollte sowohl beim Verlust oder Diebstahl von Geräten, wie auch bei digitalen Angriffen mindestens eine Kopie erhalten bleiben. Statt die Kopien per Hand anzulegen und zu aktualisieren, sollte eine Software eingesetzt werden, damit die Backups automatisch und regelmäßig erfolgen. Unter Windows lässt sich zum Beispiel das Tool »Duplicati 2« nutzen, während Macs mit »Time Machine« bereits eine vorinstallierte Lösung mitbringen. Beim Einsatz von Backup-Software sollte darauf geachtet werden, welche Ordner und Dateien mitgesichert werden und welche ignoriert werden sollen. Wie bereits angesprochen, spielt dabei auch der Datenschutz eine Rolle. Zu Beginn ging es in den Bedrohungsszenarien darum kritisch zu

schauen, welche Daten tatsächlich gespeichert werden müssen. Die nächste Frage ist: Wo werden sensible Daten gespeichert? Sie sollten möglichst verschlüsselt gespeichert werden. Dabei werden Dateien in einen digitalen Tresor gelegt, der nur durch die Eingabe eines Passworts und ggf. eines zweiten Faktors geöffnet werden kann. Dazu gibt es ebenfalls Programme: Unter Windows etwa »VeraCrypt«, während Macs mit »FileVault« bereits ein Programm von Haus aus mitbringen. Verschlüsselung und Backup werden am besten so kombiniert, dass verschlüsselte Daten ins Backup gehen, wobei wiederum die Hinweise zu sicheren Passwörtern und Zwei-Faktor-Authentifizierung gelten.

Das physische Abschließen ist eine weitere Möglichkeit, also das althergebrachte Aufbewahren von Speicher- und Backupmedien in einem abgeschlossenen Schrank. Ähnlich wie bei Akten sollte schließlich klar sein, wann und wie Daten gelöscht werden, wenn sie nicht mehr vorgehalten werden müssen. Wichtig ist auch hier am Ende, dass eine Lösung gefunden wird, die tatsächlich angewendet wird, statt sich die sicherste Lösung zu überlegen und dann nie umzusetzen. Verschlüsseln lässt sich auch Kommunikation. Leider ist die E-Mailverschlüsselung mit OpenPGP seit jeher etwas umständlich, da einiges an Software installiert und eingestellt werden muss. Inzwischen ist OpenPGP nicht mehr zu empfehlen, da die Einbindung in die meisten E-Mailprogramme fehlerhaft ist. Allerdings funktioniert dies mit E-Mails kaum, so dass sensible Informationen nicht per E-Mail ausgetauscht werden sollten. Eine Alternative sind Messenger-Apps auf dem Smartphone, die Nachrichten von sich aus verschlüsseln.

Schadsoftware und Phishing vermeiden

Trojaner[3] und ähnliche Schadsoftware werden inzwischen in E-Mails versendet, die auf den ersten Blick kaum zu erkennen sind. Sie scheinen von Leuten zu sein, mit denen bereits Kontakt besteht; oft beziehen sie sich sogar auf zuvor selbst geschickte E-Mails. Die problematische Software versteckt sich im Anhang, in Form von Word-Dokumenten oder Archiven. Bei der Textverarbeitungssoftware Word nutzen Angreifer*innen sogenannte Makros aus. Das sind Programme-im-Programm, mit denen sich in Microsoft-Office-Anwendungen die Arbeit vereinfachen lässt. Anstatt immer wiederkehrende

3 Trojaner sehen oberflächlich nach nützlichen Programmen aus, um unerwünschte Funktionen zu verstecken.

Aufgaben jedes Mal von Hand auszuführen, erledigen Makros sie selbsttätig auf Knopfdruck, wie etwa das Einfügen einer speziell vorformartierten Tabelle in Textdokumente. Da sie von Kriminellen oft missverwendet werden, sind Makros heute im Office-Programm standardmäßig deaktiviert. Kommt nun ein Word-Dokument mit Schadsoftware, zeigt diese als Erstes beim Öffnen eine gefälschte Fehlermeldung, damit Makros wieder aktiviert wird und die Schadsoftware ausgeführt werden kann. Eine andere Technik sind Datei-Archive wie ZIP-Dateien, die entpackt und entschlüsselt werden müssen. Der Schlüssel wird praktischerweise in der gleichen Mail mitgesendet. Normalerweise gilt: Wer verschlüsselte Dateien verschickt, sollte den Schlüssel mindestens in einer zweiten E-Mail oder noch besser über einen anderen Weg der Kommunikation verschicken. Derartige sinnlose Sicherheitsmaßnahmen sind ein Hinweis auf unredliche Absichten. Im Zweifelsfall ist es hilfreich, bei ungefragt zugesandten Dokumenten zum Telefonhörer zu greifen und nachzuhaken. Virenscanner erkennen die Schädlinge derzeit leider nicht zuverlässig. Auf keinen Fall sollten Anhänge mit der Endung .exe geöffnet werden. EXE-Dateien sind Windows-Programme, auch wenn die Dateiendung meist ausgeblendet wird. Heute werden Schädlinge allerdings nur noch selten so offen versendet.

Manche Schadsoftware verschlüsselt dafür die eingebauten und angeschlossenen Festplatten und verlangt für die Freigabe der Daten ein Lösegeld. Das lohnt sich bei Beratungsstellen zwar nicht, ist aber keine Garantie, dass es nicht passiert. Deswegen sind Backups wichtig, denn mindestens eine Kopie aller nötigen Informationen ist dann noch vorhanden. Eine Alternative zu Microsoft Office sind die kostenlosen Programme »LibreOffice« und »OpenOffice«, bei denen die Angriffe auf Makros nicht funktionieren.

Im besten Fall erkennt entweder der E-Mail-Provider oder das eigene E-Mail-Programm kritische Mails. Einen Mailcheck stellt die IT-Nachrichtenseite heise online unter https://heise.de/security/dienste/Emailcheck-2109.html bereit. Über die Seiten lassen sich Test-E-Mails verschicken, um zu überprüfen, ob das E-Mail-Programm oder der Virenscanner die Schädlinge erkennt. Wenn ein Rechner infiziert ist, hilft nur, gleich den Internetzugang zu kappen, damit auf keinen Fall weitere Computer gefährdet werden. Anschließend muss das Betriebssystem neu installiert werden[4].

4 Siehe Beitrag: Digitale erste Hilfe und Sicherheitsprinzipien für Berater*innen bei digitaler Gewalt.

Neben Schadsoftware ist Phishing ein Problem. Hierbei werden meist Zugangsdaten für Webseiten kopiert, indem erst E-Mail-Benachrichtigungen von Banken oder Sozialen Netzwerken gefälscht werden und auf ebenso gefälschte Webseiten verweisen. Um sich davor zu schützen, sollten Links in einer E-Mail immer genau angesehen werden, bevor sie angeklickt werden. Noch sicherer ist es, die Adresse der Webseite von Hand im Browser einzutippen. Eine weitere Möglichkeit ist, Links erst zu kopieren und in ein ganz einfaches Textverarbeitungsprogramm, das keine Formatierungen unterstützt, einzufügen, wie den vorinstallierten Microsoft Editor. Er zeigt direkt den eingefügten Text an, sodass man kontrollieren kann, ob die Adresse auf eine vertrauenswürdige oder gefälschte Webseite führt.

Weiterbildung und Notfallpläne

Nachdem mögliche Szenarien erkannt sind und im Idealfall Vorsichtsmaßnahmen getroffen wurden, muss ein Plan für Angriffe erarbeitet werden. Wichtig für diesen Notfallplan ist die erste Ansprechperson. Auch ist es wichtig sich im Vorfeld zu überlegen, wer die Entscheidungen trifft und wer jeweils das Backup erstellt. Hilfreicher Teil eines Notfallplans sind zudem Kontaktdaten von weiteren Einrichtungen, Firmen oder der Polizei an die sie sich wenden könnten. Im Falle eines Angriffs ist eine möglichst genaue Dokumentation der Vorfälle unerlässlich. Diese Dokumentation ist nicht nur für eine eventuelle Strafverfolgung sinnvoll, sondern auch für die eigene Analyse und die Einführung von nötigen Gegenmaßnahmen.

Alle Pläne nützen nichts, wenn sie nur im Schrank liegen und niemand davon Ahnung hat. Stattdessen sollten sie zunächst als Grundlage für eine interne Weiterbildung von Nutzen sein. Alle Mitarbeiter*innen sollten prinzipiell mit der elektronischen Ausstattung der Räume und Geräte und den vorgestellten Best-Practice-Empfehlungen vertraut sein, sowohl zum Schutz der eigenen Arbeit als auch zur Beratung der Klient*innen. Wichtig ist hierbei zu fragen, an welchen Stellen die Mitarbeiter*innen sich Weiterbildungen oder Unterstützung wünschen; vorstellbar ist auch, dass Leitungen diese Fortbildungen verpflichtend einführen.

Literatur

Center for Internet Security (Hg.) (2019): »CIS Controls«. https://cisecurity.org/controls/ [Zugriff: 4.7.2020].

Electronic Frontier Foundation (Hg.) (2019): »Surveillance Self-Defence. Your Security Plan«. https://ssd.eff.org/en/module/your-security-plan [Zugriff: 15.6.2020].