Digitale Erste Hilfe und Sicherheitsprinzipien für Berater*innen bei digitaler Gewalt

Jenny-Kerstin Bauer und Helga Hansen

Die Beratung von Frauen, die von digitaler Gewalt betroffen oder bedroht sind, bringt einige Herausforderungen mit sich, denn digitale Angriffe gegen Frauen sind vielfältig: Manche sind technisch ausgefeilt, andere sehen nur so aus. Zudem ist das Internet ein schnelllebiges Medium, welches Täter*innen immer neue Möglichkeiten bietet digitale Gewalt auszuüben. In diesem Artikel finden Berater*innen zunächst eine kurze Checkliste mit drei Punkten, um schnell digitale Erste Hilfe leisten zu können. Anschließend erklären wir grundlegende Sicherheitsprinzipien für den Umgang mit digitalen Geräten und der Internetnutzung. Die Sicherheitsprinzipien sind aus der psychosozialen Beratungsarbeit mit Frauen, die von digitaler Gewalt betroffen sind, entstanden und mit Wissen aus der Informations- und Kommunikationstechnologie weiterentwickelt worden.

Um auf dem neuesten Stand zu bleiben ist es sinnvoll, sich regelmäßig z.B. bei Technik-Magazinen zu informieren. Leider ist deren Schwerpunkt oft die Absicherung gegen gewiefte Hacker*innen oder staatliche Datensammlung. Bei Angriffen aus dem sozialen Umfeld können völlig andere Maßnahmen nötig sein. In der Beratung müssen mit den betroffenen Frauen Lösungen gefunden werden, die in der jeweiligen Situation tatsächlich umsetzbar sind. Um das Thema digitale Gewalt im sozialen Nahraum vermehrt in die Technik-Magazine zu bringen ist es sinnvoll, die Probleme und Strategien in Leser*innenbriefen an die Technik-Journalist*innen zurückzugeben. Spezielle Informationen zur Sicherheit für Betroffene von digitaler Gewalt finden Sie auch auf der Seite des bff: Bundesverband Frauenberatungsstellen und Frauennotrufe *www.aktiv-gegen-digitale-gewalt.de* und auf dem Infoportal für sichere Handynutzung *www.mobilsicher.de*.

Checkliste: Erste-Hilfe

Bestandsaufnahme machen

Um effektiv Erste Hilfe zu leisten, muss zunächst geklärt werden, ob die gewaltausübende Person oder jemand anderes Zugriff auf die persönlichen elektronischen Geräte wie das Smartphone, Fitnessarmband, den Router oder Rechner hatte. Wenn ja, sollten diese Geräte als erstes auf Spyware und Freigaben geprüft werden. Fitnessarmbänder sollten dann nicht mehr getragen werden. Auch die elektronischen Geräte und »smarte Spielzeuge« der Kinder (wie zum Beispiel sprachgesteuerte Teddybären und alles, was mit einer App verbunden ist) sollten gesichtet und überprüft werden.

Wenn die Betroffene mit dem Gewalttäter zusammengewohnt hat oder er smarte Elektronikgeräte im Haushalt installiert hat, müssen außerdem SmartHome-Geräte wie etwa smarte Türöffner, Jalousien oder Heizungssysteme überprüft und möglichst der Internet-Router zurückgesetzt werden.

Ein erhöhtes Sicherheitsrisiko für die Betroffene besteht, wenn der Gewalttäter über Wissen aus dem Bereich der Informations- und Kommunikationstechnologien verfügt. Dieses sollte in der Beratung gezielt abgefragt werden, relevant sind hierbei Berufstätigkeit oder auch Hobbys und Interessen.

Sicherheitsbasis schaffen

Um sich einen Überblick zu verschaffen, ist es notwendig, systematisch alle vorhandenen Online-Konten (E-Mail-Adressen, Social Media Accounts, Online-Dienste oder Online-Dating-Accounts) aufzulisten und zu vermerken, welche E-Mail-Adressen und Handynummern die betroffene Frau bzw. ihre Kinder dafür verwenden. Als erstes ist es wichtig, bei allen alten E-Mail-Adressen die Passwörter zu ändern. Deutlich sicherer ist hierbei die sogenannte Zwei-Faktor-Authentifizierung – also ein zweistufiges Anmeldeverfahren.[1]

Zentral für weitere Schritte ist ein eigenes E-Mail-Postfach, auf das niemand sonst Zugriff hat, da praktisch jeder Online-Dienst zur weiteren Kommunikation die Angabe einer E-Mail-Adresse verlangt. Eventuell muss daher eine neue E-Mail-Adresse eingerichtet werden und diese als Kontakt in den

1 Siehe hierzu die Ausführungen zu »Sichere Passwörter und Codes« im weiteren Verlauf dieses Artikels. Siehe außerdem Beitrag: Digitale Sicherheit für frauenspezifische Einrichtungen.

vorhandenen Online-Konten und Diensten geändert werden. Anschließend sollten alle weiteren Passwörter geändert werden: Vom heimischen WLAN über den Internet-Router bis hin zu Social Media Accounts und Diensten wie Netflix oder Einkaufsdiensten (wie z.B. Amazon). Letzteres ist wichtig, damit der Täter der betroffenen Person nicht noch ökonomischen Schaden zufügen kann. Damit die Betroffene online handlungsfähig bleibt, ist es wichtig sie mit dem privaten Modus von Internet-Browsern vertraut zu machen.[2] Dies ermöglicht ihnen den eigenen, aber auch fremde Rechner zu nutzen, ohne Spuren zu hinterlassen. Wenn nicht ausgeschlossen werden kann, dass der Gewalttäter heimlich mitliest, bzw. smarte Geräte überwacht, sollte auf das Speichern von sensiblen Daten auf den Geräten verzichtet werden.[3]

Beweissicherung

Bei all diesen Maßnahmen ist es wichtig, die von digitaler Gewalt Betroffenen dabei zu unterstützen, die Beweise genau zu dokumentieren.[4] Wie bei analoger Gewalt ist es durchaus vorstellbar, dass es für die Betroffenen zunächst ausgeschlossen erscheint gegen die Gewalt juristisch vorzugehen. Auch in diesem Fall ist es wichtig, die Beweise für alle Fälle zu sichern.

(Präventive) Sicherheitsprinzipien bei digitaler Gewalt

Sichere Passwörter

Passwörter sind die wichtigste Sicherheitshürde. Sie verhindern, dass eine gewaltausübende Person die Benutzer*innenkonten in sozialen Netzwerken oder E-Mail-Konten einer betroffenen Frau einsehen kann. Der erste Schritt ist, für jeden passwort-geschützten Dienst ein anderes Passwort zu verwenden. Passwörter sind umso sicherer, je länger sie sind. Viele Online-Dienste prüfen das Passwort inzwischen schon beim Erstellen auf Länge und weitere Kriterien und geben eine eigene Sicherheitsabschätzung ab.

2 Siehe hierzu die Ausführungen zu »Surfen mit privater Sitzung« im weiteren Verlauf dieses Artikels.

3 Siehe hierzu die Ausführungen zu »Speicherung sensibler Daten« im weiteren Verlauf dieses Artikels.

4 Siehe hierzu die Ausführungen zu »Beweissicherung und Kontaktaufnahme Seitenbetreiber*innen« im weiteren Verlauf dieses Artikels.

Ein sicheres Passwort hat mindestens zwölf Zeichen. Es enthält Groß- und Kleinbuchstaben, Ziffern und geläufige Sonderzeichen wie »!« und »?« (vgl. klicksafe/Institut für Digitale Ethik (IDE) der Hochschule der Medien Stuttgart 2018: o.S.). Wichtig ist, dass es sich nicht aus dem eigenen Namen, dem einer nahestehenden Person, einem Geburtsdatum oder einer Telefonnummer ableiten lässt. Eine Möglichkeit ist, verschiedene Worte und Zahlen zu kombinieren wie: *Kabel-Wetterballon!2020*. Alternativ lässt sich auch ein Satz als Ausgangsbasis nehmen: *H*eute *w*erde *i*ch *m*it *v*iel *F*reude *E*is *u*nd *S*chokolade *e*ssen. Aus den Anfangsbuchstaben der Wörter ergibt sich mit der Kombination von einem Sonderzeichen «!« und einer Jahreszahl: *HwimvFEuSe!2023*. Diese Passwörter können in abgewandelter Form für jedes Konto angepasst werden, wobei Sie möglichst mehrere Teile verändern. Beispielsweise für Facebook gilt: *HwimvFEuSe!2023* und für das E-Mail-Konto gilt: *M*orgen *w*erde *i*ch *m*it *v*ielen *n*etten *M*enschen *P*izza *u*nd *P*asta *e*ssen = *MwimvnMPuPe?2022* oder *Kabel-Flugzeug?2020*. Wird kein Passwortmanager verwendet, ist das sicherste Passwort eines, das sich die Person merken kann, ohne es sich aufschreiben zu müssen. Es nützt nichts, wenn es regelmäßig zurückgesetzt werden muss oder die Person sich selbst von ihren Accounts aussperrt.

Bei Einbrüchen und Hacks von Webseiten und sozialen Netzwerken werden gerne Passwörter entwendet, die von fahrlässigen Betreiber*innen offen abgespeichert wurden – diese können auch in die Hände der gewaltausübenden Person geraten. Einige Dienste bieten an, diese Datenlecks auf eigene Informationen zu untersuchen, wie etwa der »Identity Leak Checker« des Potsdamer Hasso-Plattner-Instituts. Auf *https://sec.hpi.de/ilc/search?lang=de* können Sie anhand ihrer E-Mail-Adresse abfragen, welche Zugangs- oder Identitätsdaten und Passwörter im Internet offengelegt werden. Zu überprüfen sind auch alte E-Mail-Adressen, die die Betroffene vielleicht seit Jahren nicht mehr genutzt hat.

Wurde ein Passwort bei mehreren Accounts genutzt, ist es in einem Leck veröffentlicht worden oder hat die gewaltausübende Person Kenntnis von Passwörtern, sollten diese unbedingt geändert werden. Ohne konkreten Anlass ist es ansonsten selten sinnvoll, Passwörter zu ändern oder dies sogar regelmäßig zu tun. Die Anzahl der zu merkenden Passwörter wird schnell so groß, dass es schwierig ist, den Überblick zu behalten und die Gefahr steigt, sich schließlich aus einem eigenen Account komplett auszusperren. Stattdessen macht der Einsatz eines Passwortmanagers Sinn. Diese Programme, wie etwa »1Password«, speichern die Zugangsdaten zu verschiedenen Konten und schlagen sichere Passwörter vor. Um sie zu nutzen, muss man sich nur

das Master-Passwort merken und ggf. einen zweiten Faktor nutzen. Ein Passwortmanager ermöglicht das Merken der ansonsten schwer zu merkenden langen, aber sicheren Passwörter. Verschafft die gewaltausübende Person sich allerdings Zugriff auf das Smartphone und das Passwort zum Passwortmanager, sind alle dort gespeicherten Zugangsdaten für sie einsehbar. Eine Sicherheitsmaßnahme ist daher, nur eher unwichtige Passwörter dort abzulegen und das E-Mail-Passwort weiter per Hand einzugeben.

Sichere Codes

Ein Zugriffs- oder Passcode schützt zum Beispiel ein Smartphone in Form eines Zifferncodes, eines Musters, durch Gesichtserkennung oder einen Fingerabdruck vor fremden Zugriffen auf das Telefon. Eine starke Bildschirmsperre besteht aus mindestens sechs, besser aus acht Ziffern. Der Code sollte nicht geläufige Ziffernfolgen wie das Geburtsdatum des Kindes oder die eigene Postleitzahl enthalten. Muster als Zugriffscodes sind relativ leicht zu erraten, vor allem, wenn die gewaltausübende Person häufig die Gelegenheit hat, die Eingabe zu beobachten.

Die praktische Entsperrung mit dem Fingerabdruck ebenso wie die Gesichtserkennung (Face ID) ist umstritten. Fingerabdrücke und das Gesicht sind grundsätzlich öffentlich sichtbar und damit eher wie Benutzer*innennamen zu betrachten. Werden sie verlangt, ist es allerdings schwerer, das Smartphone heimlich zu entsperren. Durch die Eingabe des Zugriffscodes lassen sie sich schließlich aber meist umgehen.

Passwort-Wiederherstellung

Eine häufige Taktik zum Kapern eines Accounts ist der Versuch, das Passwort zurücksetzen zu lassen. Dabei wird meist ein neues Passwort von den Seitenbetreiber*innen in einer E-Mail verschickt, weshalb es so wichtig ist, über ein E-Mail-Konto ohne Zugriff der gewaltausübenden Person zu verfügen. Manchmal gibt es auch Sicherheitsfragen nach dem Namen des ersten Haustiers oder dem Namen des Kindes. Diese sind für Personen aus dem Umfeld leicht zu erraten. Daher sollte bei den Antworten gelogen werden – aber nachvollziehbar, denn man muss sich die Antwort schließlich selbst merken können. Sinnvoll ist ein System, wenn Facebook nach dem Geburtsort fragt, wie etwa F-Hannover und A-Hannover wenn die gleiche Frage bei Amazon auftaucht.

Zwei-Faktor-Authentifizierung

Ist ein Benutzer*innenkonto durch eine Zwei-Faktor-Authentifizierung (2FA) oder auch zweistufiges Anmelden geschützt, erfolgt das Einloggen in zwei Schritten. Zuerst wird, wie gewohnt, das Passwort eingegeben und dann eine zweite Methode bzw. ein zweiter Faktor genutzt. Beispielsweise wird ein zeitlich begrenzt gültiger Sicherheitscode per E-Mail oder SMS verschickt, der nach dem Passwort eingegeben werden muss. Viele Online-Dienste (Soziale Netzwerke, Messengerdienste oder E-Mail-Anbieter*innen) ermöglichen mittlerweile diese Funktion. Die Aktivierung erfolgt meist unter Einstellungen im Menü zu Sicherheit und Privatsphäre. Durch die zwei Schritte ist das Benutzer*innenkonto theoretisch sehr gut vor dem Zugriff der gewaltausübenden Person geschützt, weil es nicht mehr ausreicht nur das Passwort zu kennen. Praktisch gibt es in den unterschiedlichen Methoden jeweils Schwächen, sodass der Einsatz abgewogen werden muss. In Zukunft sollte sich hier noch einiges verbessern.

Am sichersten sind unabhängige Geräte, wie etwa ein TAN-Generator beim Online-Banking. Es gibt zum Beispiel die »YubiKeys« – kleine Schlüssel, die auf den ersten Blick an USB-Sticks erinnern. Sie können am Schlüsselbund getragen und über USB mit dem Rechner oder Smartphone verbunden werden, um sich beim Anmelden bei verschiedenen Diensten zu identifizieren. Trotz hohem Sicherheitsstandard sind solche Hardware-Schlüssel bisher nur begrenzt bei Online-Diensten nutzbar – Apple und Google haben in den letzten Monaten beständig daran gearbeitet Hardware-Schlüssel zu unterstützen. Mit IOS 14 soll das z.B. für iCloud kommen und seit kurzem funktionieren YubiKeys auch mit Google-Apps auf iPhones.

Eine Alternative sind spezielle Apps wie »Google Authenticator« oder »Authy«. In dieser App werden die gewünschten Dienste registriert. Bei jeder Anmeldung wird von der App ein Code als zweiter Faktor generiert. Wie die Hardware-Schlüssel werden die Apps allerdings auch noch nicht von allen Diensten unterstützt. Ein weiterer Nachteil von beiden Methoden: Geht der Hardware-Schlüssel oder das Smartphone mit der App verloren, ist der Zugang zu den Diensten verloren. Inzwischen wird eine Kombination aus zwei aktivierten 2FA-Methoden empfohlen.

Schließlich gibt es die Möglichkeit einen Einmal-Code per SMS oder E-Mail zu bekommen. Das ist derzeit die am weitesten verbreitete 2FA-Methode, aber auch die unsicherste. Mit einem Anruf bei der Mobilfunkfirma und persönlichen Informationen kann sich die gewaltausübende

Person neue SIM-Karten für bekannte Telefonnummern beschaffen. SMS und Anrufe landen danach auf der neuen Karte – wer ansonsten nur über Messenger telefoniert und schreibt, merkt dies unter Umständen nicht einmal. Bis Anfang 2020 konnten Nutzer*innen bei Facebook über die für die Zwei-Faktor-Authentifizierung angegebene Telefonnummer gefunden werden, auch wenn sie die Nummer von ihrem Profil verbergen ließen.

Smartphone-Einstellungen absichern

Über GPS und die Standortübermittlung können die Bewegungen anderer Personen überwacht und kontrolliert werden. Auch Mikrofone und Kameras können über entsprechende Apps zum Spionieren genutzt werden. Gerade Android-Smartphones mit älteren Betriebssystemen geben Apps viele Freiheiten. Als erstes sollten daher in der Beratung alle installierten Apps einzeln durchgegangen werden.[5] Wichtig ist hierbei zu klären, ob die betroffene Person alle Apps selbst heruntergeladen hat bzw. ob jede App und jedes Programm einen Nutzen für sie hat. Unbekannte oder nicht mehr genutzte Apps sollten gelöscht werden. Werden sie später doch noch einmal gebraucht, können sie meist einfach wieder installiert werden. Auch ist es wichtig, die Freigaben für Ortungsdienste, Mikrofon und Kamera in den Einstellungen zu überprüfen. Mobilitäts-Apps wie von der Bahn finden mit dem aktuellen Standort schneller den nächsten Bus, ein Spiel wie »Candy Crush« benötigt ihn aber nicht. Daher sollten unnütze Freigaben konsequent abgeschaltet und dauerhafte Standortabfragen gekappt werden, wenn das Programm selbst geschlossen ist. Manch ältere Android-App verweigert anschließend ihre Funktion; im Zweifelsfall ist es sicherer, sich ein alternatives Programm zu suchen. Es ist durchaus möglich, Apps den direkten Zugriff auf alle eigenen Bilder und Videos zu verweigern und diese bei Bedarf trotzdem zu verschicken. In den Bilder-Apps gibt es dafür die Share-Funktion, die ohne Freigaben auskommt und das Bild nur gezielt weitergibt.

Über spezielle Ortungsfunktionen lassen sich Smartphones und andere elektronische Geräte auf den Meter genau lokalisieren. Bei Android-Smartphones geht dies über die Funktion »Mein Gerät finden« und bei dem iPhone über »Mein iPhone suchen«. Diese Funktion sollte ausgeschaltet bzw. durch sichere Passwörter und eine Zwei-Faktor-Authentifizierung geschützt sein. Wenn betroffene Frauen diese Funktion weiterhin nutzen wollen, um

5 Siehe hierzu die Ausführungen zu »Spionage-Software« im weiteren Verlauf dieses Artikels.

Geräte bei Verlust aus der Ferne sperren zu lassen, gibt es auch eine Alternative ohne Ortung. Nötig ist dafür die IMEI (*I*nternational *M*obile Station *E*quipment *I*dentity) Nummer des Smartphones. Sie wird angezeigt, wenn die Tastenkombination *#06# angerufen wird. Mit dieser Nummer kann das Smartphone bei Verlust durch den Netzbetreiber bzw. die Polizei gesperrt werden.

Neben der Ortungsfunktion ist es wichtig, die Webcams bei Laptops und Computern im Blick zu haben und möglichst abzudecken, damit beispielsweise die gewaltausübende Person diese nicht durch Hacken oder eine Spionage-Software kontrollieren und somit ständig überwachen kann. Dafür eignet sich bereits ein kleines Monitorputztuch mit Kleberückseite oder ein einfaches Post-it. Sollte das Statuslicht der Kamera unerwartet angehen, ist dies ein Hinweis darauf, dass die am Computer arbeitende Person und ihre Umgebung von außen betrachtet und gehört wird.

Spionage-Software

Während einige Apps nur aus Bequemlichkeit Mikrofone und Kameras anschalten und damit das Gegenüber überwachen, ist dies der Hauptzweck von sogenannten Spionage-Softwares, Spy-Apps oder Stalkerware.[6] Die gängigsten Möglichkeiten eine Spionage-Software unerkannt auf einem Smartphone oder einem Computer zu installieren sind:

- Spionage-Software wurde durch eine E-Mail oder einem Nachrichten-Anhang unabsichtlich selbst heruntergeladen, weil die Software beispielsweise als Katzenbild oder wichtiges Dokument getarnt war.
- Anti-Diebstahl-Software (wie z.B. »Cerberus«), die auf den ersten Blick sinnvoll und praktisch wirkt, kann als Spionage-Software missbraucht werden.
- Die gewaltausübende Person hatte einmal direkten physischen Zugriff auf das elektronische Gerät und hat in dieser Zeit Spionage-Software installiert, z.B. kurz nach einem Telefonat und vor der Sperrung des Bildschirms.
- Die gewaltausübende Person hatte Zugang zu Cloud-Diensten der Person, die sie überwachen will und die Spionage-Software funktioniert über diesen Dienst.

6 Siehe Beitrag: Individuelle Strategien im Umgang mit geschlechtsspezifischer digitaler Gewalt.

Ein möglicher Hinweis auf die Existenz von Spionage-Software auf einem Smartphone ergibt sich, wenn Klient*innen berichten, dass der gewaltausübenden Person viele Informationen und Aufenthaltsorte bekannt sind. Auch ein sehr schnell entleerter Akku kann ein Indiz für eine Spionage-Software sein, denn durch das ständige Abfangen und Auslesen der Daten werden die Geräte spürbar langsamer als gewohnt und der Akku ist schneller leer (vgl. Bleich 2018: 76). Hier ist es wichtig in den Benachrichtigungen zu überprüfen, ob das Smartphone den Ortungsdienst erlaubt, wenn kein Programm offen ist.

Für die Installation von Spionage-Apps sind meist spezielle Rechte nötig. Bei Android-Smartphones heißt diese unautorisierte Veränderung »Rooten« und beim iPhone »Jailbreak«. Android-Smartphones lassen sich mit der App »Rootchecker« überprüfen. Ein weiterer Hinweis auf Android-Spionage-Apps sind Einträge in den Sicherheits-Einstellungen zum Standort. Dort sollten nur »Mein Gerät finden« und »Google Pay« zu sehen sein. Weitere Einträge sollten deaktiviert werden. »Jailbreaks« sind derzeit nur auf älteren Versionen des iPhone-Betriebssystems möglich. Verdächtige Apps heißen »Cydia«, »Electra« und »Pangu« und sind etwa auf der Seite *www.zjailbreak.com* zu finden. Manche Apps wie das Spiel »Pokémon Go« verweigern die Arbeit, wenn sie einen Jailbreak erkennen und können so Hinweise geben. Neuere iPhones sind vor allem über die iCloud anfällig. Anti-Viren-Programme waren lange nutzlos in diesem Zusammenhang. Seit einiger Zeit nehmen die Hersteller*innen das Problem aber ernster: »Kaspersky« und »TrendMicro« erkennen inzwischen geläufige Spionage-Programme (vgl. Coalition Against Stalkerware 2019: o.S.; Gierow 2019: o.S.).

Das Zurücksetzen bzw. das Neuaufsetzen von Geräten kann eine wirkungsvolle Strategie sein, um sich der Überwachungssoftware zu entledigen. Trotzdem wird nicht jede Software damit nachhaltig gelöscht. Im Zweifelsfall sollten IT-Spezialist*innen hinzugezogen bzw. die Geräte ausgetauscht und die Passwörter geändert werden.

Speicherung sensibler Daten

Falls sich eine gewaltausübende Person Zugriff zu einem Smartphone der (Ex-)Partner*in verschafft hat, kann sie dort alle abgespeicherten, sensiblen Daten einsehen. Vom Abfotografieren von Dokumenten (wie etwa Krankenkassenkarten, Briefe mit Terminen bei Behörden oder Gerichten) oder der Pässe der Kinder ist daher abzuraten. In der Beratung sollte daher gemein-

sam besprochen werden, wo Klient*innen ihre sensiblen Daten speichern und wie sie eine Sicherheitskopie ihrer Daten und möglicher Beweise erstellen können. Optionen dafür sind deutsche Cloud-Dienste (wie »MagentaCloud«), die den Anforderungen der europäischen Datenschutz-Grundverordnung (DSGVO) entsprechen, externe Festplatten oder USB-Speichersticks. Letztere sollten nach Möglichkeit neu gekauft werden, da die gewaltausübende Person über vorhandene Sticks Spionage-Software auf einen Rechner schleusen kann. Smartphone-Backups sollten über Kabel auf dem Rechner erstellt werden.

Um Smartphones und Tablets nutzen zu können, sind eine Apple-ID (iPhone) oder ein Google-Konto (Android) nötig, die mit dem jeweiligen Gerät verknüpft werden. Darüber drängen die beiden Anbieter ihren Nutzer*innen auch gleich die eigenen Cloud-Services auf, von denen allerdings abzuraten ist. Ist der gewaltausübenden Person das Passwort bekannt, können sensible Daten von anderen Rechnern oder Smartphones eingesehen werden. Gerade bei iPhones ist die iCloud eine Schwachstelle, über die etwa Spionage-Software installiert werden kann, obwohl Apple ansonsten oft die besseren Sicherheitseinstellungen vorgibt.

Hat die gewaltausübende Person wichtige Dateien gelöscht, können diese gegebenenfalls wiederhergestellt werden; hier lohnt ein Blick in den Papierkorb des Geräts. Solange der nicht geleert wurde, können die Daten einfach zurückgelegt werden. Sind Dateien dort nicht mehr zu finden, sollten am Rechner keine weiteren Aktionen durchgeführt werden, weil die Speicherbereiche von Windows-Rechnern oft nur zum Überschreiben freigegeben, aber nicht physisch gelöscht werden. Solange die Daten nicht überschrieben wurden, können sie mit kostenlosen Tools wie »TestDisc« und »Disk Drill« wiederhergestellt werden, die es im Internet gibt.

Router, Bluetooth und WLAN als Sicherheitsrisiko

Grundsätzlich gilt derzeit: Kabel sind sicherer als drahtlose Verbindungen. Wenn möglich sollten daher der Internetzugang und Geräte wie Tastaturen oder Lautsprecher über Kabel angeschlossen werden. Die nächstbesten Alternativen sind verschlüsselte Verbindungen, die die Eingabe eines Passworts oder Pins erfordern. Egal ob zu Hause Kabel oder WLAN genutzt wird – der Internetanschluss sollte gut abgesichert werden. Bereitgestellt wird er heute meist von einem Router, alle Einstellungen können nur hierüber verändert werden. Dazu muss das Smartphone oder ein Rechner über das WLAN oder

ein Kabel mit dem Router verbunden sein. Anschließend wird die Router-Adresse im Browser aufgerufen. Diese besteht meist aus einer Zeichenfolge wie 192.168.1.1 oder 192.168.0.1 oder bei einer »Fritzbox« über fritz.box – die passende Adresse steht meist auf der Unterseite des Routers oder im Handbuch. Mit dem Hersteller*innennamen und der Typenbezeichnung lässt sie sich auch im Internet ermitteln. Anschließend verlangt der Router eigene Zugangsdaten (einen Benutzer*innennamen und ein Passwort), die meist ebenfalls auf der Unterseite des Geräts vermerkt sind. Wurden die Daten bereits geändert oder sind nicht auffindbar, lässt sich der Router über den Reset-Knopf zurücksetzen und nutzt dann vorgegebene Zugangsdaten wie den Benutzer*innennamen »admin« und das Passwort »password«. In den Router-Einstellungen müssen diese Standardangaben dann gleich wieder geändert werden. Außerdem kann man in den Einstellungen überprüfen, welche Computer, Smartphones und Smart-Home-Geräte den Internetzugang nutzen.

Für das heimische WLAN sollte der Netzwerkname so gewählt sein, dass kein Rückschluss auf das verwendete Router-Modell möglich ist. Wichtig ist auch die Netzwerkverschlüsselung, um keine Daten offen einsehbar zu verschicken. Dabei sollte das Protokoll WPA2 (oder wenigstens WPA) ausgewählt werden. Schließlich muss ein sicheres Passwort für das WLAN vergeben werden. Offene, nicht-passwortgeschützte WLAN-Netzwerke bieten Möglichkeiten für Fremde und damit auch für gewaltausübende Personen, besuchte Seiten auszuspionieren, wenn sich ein Laptop oder Smartphone mit diesen verbindet. Am einfachsten ist es, die WLAN-Funktion grundsätzlich zu deaktivieren und nur dann einzuschalten, wenn ein bekanntes, sicheres WLAN genutzt wird. Wird dennoch ein offenes WLAN eines seriösen Anbieters genutzt, etwa in einer Bücherei, sollte darauf geachtet werden, keine unbekannte Software herunterzuladen und Anmeldedaten nur dann auf einer Webseite einzugeben, wenn diese verschlüsselt aufgerufen wurde – also https in der Adresse steht. Danach sollte das WLAN aus der Liste bekannter Netzwerke gelöscht werden, um späteres, ungewolltes Verbinden zu verhindern. Das gleiche gilt für den Umgang mit Bluetooth. Auch diese Funktion sollte nur zum Gebrauch eingeschaltet und anschließend wieder deaktiviert werden. In den Bluetooth-Einstellungen lässt sich ebenfalls überprüfen, welche Geräte bereits angeschlossen waren und sich automatisch verbinden würden. Werden neue Geräte angeschlossen (das sogenannte Pairing), sollten diese möglichst die Eingabe eines Pins verlangen. Achtung: »Deaktiviert« ist nicht immer »deaktiviert«. Es reicht nicht aus, im Kontrollmenü der Smartphones die Bluetooth- oder WLAN-Funktion auszuschalten. Das Kontrollmenü

ist ein Schnellzugriff zu den Einstellungen des Smartphones und lässt sich durch Wischen von oben oder unten auf dem Display anzeigen. Um die Funktionen wirklich abzuschalten, muss im Einstellungsmenü des Smartphones »WLAN deaktivieren« und »Einstellungen – Bluetooth deaktivieren« ausgewählt werden. Ansonsten aktivieren sich Bluetooth und WLAN immer wieder von selbst.

Smart-Home-Geräte

Weniger Stromverbrauch, bequeme Steuerung von Elektrogeräten aus der Ferne und stromintensive Arbeiten zu günstigen Zeiten erledigen: Intelligente Haushaltsgeräte versprechen viel Komfort, können in unbefugten Händen aber zum Alptraum werden. Ähnlich wie beim Einsatz von Spionage-Software weiß die Person, die die Geräte installiert hat, genau Bescheid, wer wann zu Hause ist und welche Geräte wie lange nutzt. Außerdem können sie dafür sorgen, dass elektronische Geräte sich merkwürdig verhalten, indem sie scheinbar wie von selbst angehen oder etwa mitten in der Nacht Musik abspielen. Dies kann eine Fehlfunktion sein oder der bewusste Versuch, Personen zu destabilisieren, indem sie beginnen an ihrer Wahrnehmung zweifeln; ein Verhalten das als »Gaslighting« bekannt ist. Daher kann es hilfreich sein nach Vorfällen zu fragen, wenn Klient*innen angeben, an »ihrem Verstand zu zweifeln«. Sie können auch ein Hinweis auf digitale Gewalt durch Smart-Home-Geräte sein. Um diese Fernsteuerung zu unterbinden, ist es am wichtigsten zu wissen, ob und welche Dinge im Haus »smart« sind. Im besten Fall sind sie allen Bewohner*innen eines gemeinsamen Haushalts bekannt. Recht verbreitet sind inzwischen Glühbirnen, Steckdosen, Bewegungsmelder und Lautsprecher wie Amazons »Alexa«, die meist auch über ein Mikrofon verfügen. Glühbirnen können einfach rausgedreht und mit der aufgedruckten Bezeichnung im Internet überprüft werden, ob es sich um eine einfache oder intelligente Birne handelt. Lautsprecher und Bewegungsmelder sind manchmal sehr unauffällig, aber meist in Hör- und Sichtweite aufgestellt – in einer selten genutzten Abstellkammer macht ein Bewegungsmelder schließlich keinen Sinn. Smarte Steckdosen fallen derzeit noch gut auf, weil es sich meist um Zwischenstecker handelt. Dennoch ist es sinnvoll in der Beratung bei Verdacht auf digitale Gewalt nachzufragen, ob eine Steckdose ausgetauscht wurde und alle angeschlossenen Geräte zu überprüfen. Jedes smarte Gerät braucht Strom und das meist mehr, als eine Batterie zur Verfügung stellen könnte. Außerdem brauchen smarte Geräte meist Internetzugang und hin-

terlassen so nachverfolgbare Spuren im Router. Schauen Sie auch, ob es in der Umgebung ein offenes oder neues WLAN gibt, über das die Geräte laufen könnten, so kann sich ein Überblick über die möglichen bestehenden smarten Geräte verschafft werden.

Das einfachste Mittel gegen unerwünschte SmartHome-Geräte ist den Stecker zu ziehen. Sollen sie grundsätzlich weiter betrieben werden, hilft ähnliches Vorgehen wie bei Smartphones und Rechnern: Zurücksetzen auf Werkseinstellungen, sichere Passwörter nutzen, Zwei-Faktor-Authentifizierung einrichten, Tracking-Berechtigungen ausschalten und gegebenenfalls die Hersteller*innen um Hilfe bitten. So sollte etwa das Mikrofon smarter Lautsprecher ausgeschaltet sein, wenn niemand zu Hause ist. Bei tragbarer Elektronik wie Fitnessarmbändern und Smartwatches gelten diese Regeln ebenfalls. Wer Kontrolle über seine SmartHome-Geräte hat, kann diese auch gezielt nutzen und z.B. zufällig Lichter angehen lassen, wenn niemand zu Hause ist, um Anwesenheit vorzutäuschen.

Datenlecks vermeiden

Um zu verhindern, dass Passwörter, Fotos und andere sensible Daten versehentlich verraten werden, gibt es noch weitere Maßnahmen, die umgesetzt werden können. Hierzu gehört das Löschen gemeinsamer Accounts mit der gewaltausübenden Person in den sozialen Netzwerken sowie von Accounts, die nicht mehr genutzt werden. So verschwinden alte Bilder und Passwörter aus dem Internet. Wichtig ist hierbei darauf zu achten, dass die Konten tatsächlich geschlossen und nicht nur deaktiviert werden, sonst können diese schnell wieder mit allen Informationen und Fotos hergestellt werden. Manchmal sind dazu extra Anfragen bei den Betreiber*innen nötig.

Besondere Vorsicht ist geboten, wenn unaufgefordert E-Mails kommen, mit denen Passwörter von Accounts zurückgesetzt werden können. Wenn es sich um eine echte E-Mail des Online-Dienstes handelt und das Passwort zuvor selbst geändert wurde, ist dies ein Hinweis dafür, dass noch jemand anderes eingeloggt war, der gerade erfolgreich ausgesperrt wurde. Möglich ist auch, dass jemand anderes versucht das Passwort zu ändern, um der Klientin den Zugang zu einem Dienst zu versperren. Um dies zu verhindern, ist ein E-Mail-Konto ohne fremden Zugriff essenziell wichtig für Betroffene von digitaler Gewalt. In diesem Fall sollte man sich noch einmal vergewissern, dass das Passwort lang genug und sicher ist und nicht in fremde Hände gelangt ist. Sinnvoll ist auch ein Screenshot der E-Mail zur Beweissicherung.

Mehr technisches Wissen erfordert das sogenannte Phishing, eine Wortkreation aus dem Englischen (dt. Passwort fischen). Dazu werden Lock-E-Mails mit der Aufforderung geschickt einen Link anzuklicken, der auf eine gefälschte Webseite führt. Werden dort Zugangsdaten eingegeben, können diese ausgelesen und ohne Einverständnis weiterverwendet werden. Statt verdächtige Links zu öffnen, ist es ratsam den Mauszeiger auf den Link zu platzieren und einen Augenblick zu warten, dann wird die eigentliche Linkadresse in der Vorschau angezeigt. Oft werden beim Phishing auch Anhänge mitgeschickt, um deren Öffnung gebeten wird. Von verdächtigen E-Mails sollte zur Beweissicherung nur ein Screenshot gemacht werden, um sie anschließend komplett zu löschen. Inzwischen versteckt sich Schadsoftware[7] nicht nur in Dateien, die auf »EXE« enden, sondern auch in Office-Dateien, wobei sich diese nur verraten, weil zur Installation eine Fehlermeldung angezeigt wird, die sich beim Nachprüfen als gefälscht erweist, also keine offizielle Fehlermeldung von Office ist. Aus der Beratungspraxis ist bekannt, dass Gewalttäter vermeintlich wichtig erscheinende E-Mail-Anhänge für Behördentermine bzw. Sorgerechtsangelegenheiten an die (Ex-)Partnerin versenden, um Schadsoftware mitzuschicken. Um E-Mail-Angriffe schneller zu erkennen und abzuwehren, ist es hilfreich, Spam konsequent zu markieren und Spamfilter einzusetzen. Eine weitere Maßnahme ist das Abbestellen von Newslettern.

Sicherheitseinstellungen in sozialen Netzwerken

Facebook[8] ist – laut eigener Angaben – das beliebteste Soziale Netzwerk in Deutschland. Nach viel Kritik aufgrund fragwürdiger Datenschutzpraktiken bietet die Firma heute einige sinnvolle Sicherheits- und Privatsphäre-Einstellungen für seine Nutzer*innen. Unter *https://facebook.com/safety/tools* werden Empfehlungen und Erklärvideos zur Verfügung gestellt, um das eigene Profil sicherer zu gestalten. Es wird auf Möglichkeiten wie sichere Passwörter, Anmeldewarnungen, die angesprochene zweistufige Authentifizierung, abmelden, gehackte Konten, Beiträge posten, Profilgestaltung, Markierung auf Fotos, Markierungsüberprüfung, Chroniküberprüfung, sein

7 Siehe hierzu die Ausführungen zu »Rechner sichern« im weiteren Verlauf dieses Artikels.

8 Das National Network To End Domestic Violence (NNEDV) hat einen umfangreichen Leitfaden für Betroffene von häuslicher und digitaler Gewalt für die Privatsphäre- und Sicherheitseinstellungen auf Facebook veröffentlicht (vgl. NNEDV 2014).

Publikum (»Freunde«) kennen, entfreunden und blockieren von Freund*innen eingegangen. Die Seite bietet aufschlussreiche Informationen für Betroffene digitaler Gewalt und steht in verschiedenen Sprachen zur Verfügung. Grundsätzlich lässt sich festhalten, dass die Privatsphäre- und Sicherheitseinstellungen von Facebook bei einer Erstanmeldung sehr offen gehalten sind. Immer wenn neue Nutzungsbedingungen von sozialen Netzwerken wie Facebook erscheinen oder Updates erfolgen, sollten nochmals alle Sicherheitseinstellungen überprüft werden. Es kann sein, dass neue Funktionen hinzugekommen sind, die eine gewaltbetroffene Frau gefährden könnten, oder dass vorgenommene Einstellungen rückgängig gemacht worden sind.

Unter »Einstellungen« auf Facebook und »Sicherheit und Login« lassen sich wichtige Funktionen für Betroffene von digitaler Gewalt konfigurieren:

- »Wähle Freunde, die du kontaktieren kannst, wenn du dich ausgesperrt hast« – Diese Funktion soll es Facebook-Nutzer*innen leichter machen sich einzuloggen, wenn sie ihr Passwort vergessen haben, indem die eingetragenen »Freunde« die Anfrage über einen Code verifizieren. Hier ist es wichtig zu überprüfen, ob eine gewaltausübende Person eingetragen ist. Wenn dies der Fall ist, sollte die Person sofort aus der Funktion gelöscht werden. Danach sollten die Passwörter so schnell wie möglich geändert werden und die Zwei-Faktor-Authentifizierung aktiviert werden. Die Passwörter können unter »Passwörter ändern« und »Verwende die Zweistufige Authentifizierung« geändert werden.
- »Wo bist du gerade angemeldet?« – Unter dieser Funktion lässt sich einsehen, wo und mit welchem Gerät das Facebook-Profil angemeldet ist. So kann eingesehen werden, ob sich eine unbefugte Person Zugang zu dem Profil verschafft hat. Manchmal handelt es sich auch um ältere Anmeldungen, bei denen man sich selbst nicht ausgeloggt hat. Über die drei Punkte neben jeder Angabe und »Das bist nicht Du?« gibt es ggf. noch weitere Informationen. Außerdem gibt es dort den Button zum »Abmelden«. Im Zweifelsfall kann man sich auch »Von allen Sitzungen abmelden«. Hat jemand Fremdes Zugriff, sollten so schnell wie möglich die Passwörter geändert und eine Zwei-Faktor-Authentifizierung aktiviert werden.
- »Anmeldewarnungen bei Logins über unbekannte Geräte erhalten« – Die Aktivierung dieser Funktion ist für gewaltbetroffene Frauen sinnvoll, denn sie verschickt eine Benachrichtigung (per E-Mail oder SMS) mit einem Warnhinweis, wenn eine unbefugte Person versucht, sich

von einem anderen Internetbrowser oder Gerät als gewöhnlich in dem Benutzer*innenkonto anzumelden.
- Unter »Einstellungen« und in den »Privatsphäre-Einstellungen« sollte beachtet werden, dass alle möglichen Funktionen auf »Freunde« statt auf »Öffentlich« gestellt sind, damit nicht alle geteilten Informationen und Bilder für die gesamte Internetöffentlichkeit und möglicherweise die gewaltausübende Person einsehbar sind und somit eine Gefahr für die Sicherheit der betroffenen Person darstellen.
- Unter »Einstellungen« und »Deine Facebook-Informationen« können alle Informationen und Daten per E-Mail abgerufen werden. Diese Datensammlung enthält u.a. alle Nachrichten (teilweise auch gelöschte) sowie alle Posts und Fotos. Diese Funktion eignet sich hervorragend als Mittel zur Sicherung von Beweisen, die über Facebook eingegangen sind.

Achtung: In der Beratung sollte geklärt werden, mit wem die betroffene Frau und ihre Kinder in den sozialen Netzwerken »befreundet« sind und ob diese »Freundschaften« sie gefährden können. Wichtig ist hierbei zu klären, ob die Facebook »Freunde« tatsächlich Freund*innen aus ihrem realen Leben sind, oder ob es sich um Personen handelt, die Kontakt mit der gewaltausübenden Person haben. Wenn das Facebook-Profil gehackt wurde, kann dies unter *www.facebook.com/hacked* gemeldet werden. Das Profil kann vorübergehend gesperrt bzw. ein neues Passwort vergeben werden.

Außerdem hat sich in der Beratung gezeigt, dass gewaltausübende Personen und/oder deren Freund*innen gefälschte Profile erstellen, in denen sie vorgeben die betroffene Frau zu sein. Sie nutzen das Profil, um Gerüchte zu streuen, intimes Bildmaterial zu veröffentlichen oder die Frau zu diffamieren. Für die Meldung eines Fake-Profils benötigt die meldende Person einen Facebook-Account, um das gefälschte Profil abzurufen. Dort muss auf das Titelbild geklickt werden, dann unter »Support erhalten« oder »Profil melden«, »Nachahmung« oder »gefälschtes Profil« auswählen. Facebook prüft nach eigenen Angaben zeitnah, ob das Profil gegen die Facebook »Gemeinschaftsstandards« verstößt. Sollte keine Reaktion folgen bzw. die Meldung abgelehnt werden, sollte ein*e Anwält*in hinzugezogen werden.

Die hier vorgestellten Tipps und Hinweise wurden exemplarisch für Facebook erläutert; sie gelten ebenso für andere soziale Netzwerke, obwohl sich die Einstellungsmöglichkeiten im Detail meist unterscheiden.

Messenger sicher nutzen

Ein weiterer Dienst von Facebook ist der beliebte Messenger WhatsApp, der sicherheitstechnisch inzwischen auch angezogen hat. In den Privatsphäre-Einstellungen lässt sich zum Beispiel begrenzen, wer das Profilfoto sehen kann und ob man ungefragt zu Gruppen hinzugefügt werden kann. Weiterhin lassen sich dort Telefonnummern sperren, sodass diese keinen Kontakt mehr aufnehmen können. Dieser Vorgang muss für jeden einzelnen Messengerdienst sowie SMS und normale Anrufe wiederholt werden. Empfehlenswerte Alternativ-Messenger sind »Threema« und »Signal«, die mit Gruppenchats und Sprachnachrichten einen ähnlichen Funktionsumfang aufweisen. In Threema lässt sich sogar die eigene Telefonnummer verbergen.

Die Vorschau von Messenger-Nachrichten auf dem Startbildschirm kann auf gesperrten Smartphones sensible Details verraten. Daher ist es sinnvoll diese Einstellung zu verändern, damit z.B. eine möglichst wenig aussagekräftige Meldung wie »1 neue Nachricht« angezeigt wird. Es ist sinnvoll dies auch bei allen Apps zu minimieren oder diese sogar ganz auszuschalten.

Rechner absichern

Viren, Würmer, Trojaner und andere sogenannte Malware (dt. schadhafte Software) können großen Schaden in Geräten anrichten und zu Datenverlust führen. Erfahrungsgemäß werden diese oft über zweifelhafte E-Mail-Anhänge verschickt. Werden diese unabsichtlich geöffnet, kann die Schadsoftware im Hintergrund der Geräte agieren. Eine gewaltausübende Person kann so Macht über die betroffene Frau erlangen, indem sie Geräte durch den Virenbefall unbrauchbar werden lässt.

Unter Windows 8 und Windows 10 ist der eingebaute »Windows Defender« inzwischen eine gute Abwehr gegen unerwünschte Downloads. Auch Mac-Rechner brauchen kaum ein zusätzliches Anti-Virus-Programm. Wer dennoch zusätzlichen Schutz wünscht, wird bei »Bitdefender«, »Kaspersky« oder »Norton« fündig, die jeweils direkt beim Hersteller heruntergeladen werden sollten und kostenpflichtige Abos erfordern. Leider kursieren im Internet auch Programme, die Anti-Virenschutz nur vorgaukeln und selbst Malware sind. Kostenlose Virenscanner gibt es von »Avast« und »AVG« – die einem bei der Installation leider noch andere Software aufdrängen, derzeit z.B. den Browser »Google Chrome«. Dessen Installation kann durch das Entfernen eines Häkchens aktiv verhindert werden.

Eine schnelle Kontrollmöglichkeit bietet der Blick auf aktuell laufende Programme. Auf Windows-Rechnern sind die in der Leiste unten rechts, beim Mac oben rechts zu finden. Dort befinden sich in der Regel Programme beispielsweise zum Antivirenschutz, zur Monitoreinstellung, zur Drucker- oder Scannereinstellung, zur Desktop- oder Googlesuche, zur Kamerafunktion, zum Batteriestatus oder für Bildimporte. Es gibt jedoch Programme wie z.B. »Refog« oder »BestKeylogger«, die alle Tastatureingaben wie Texte und Passwörter protokollieren (sogenannte Keylogger) und dann meist über das Internet direkt weitersenden. Weiterhin gibt es Programme, die den kompletten Bildschirm auf einen anderen Rechner übertragen (z.B. »VNC«, »Teamviewer«). Sollte sich in der Leiste ein unbekanntes Programm befinden, kann der Name ermittelt werden, indem die Maus draufgehalten wird. Informationen über die Programme finden sich im Internet. Gibt es eine mitlesende Person, kann das Programm mit der rechten Maustaste beendet werden.

Wichtig ist vor allem, die jeweils aktuellen Updates zu laden, sowohl der Betriebssysteme von Rechner und Mobilgeräten, wie auch der installierten Software. Komfortablerweise bieten viele Programme inzwischen eine automatische Update-Funktion an. Meist werden die Updates des Betriebssystems nachts durchgeführt, wenn das Smartphone gerade geladen wird oder der Rechner abends nicht heruntergefahren wurde. Anwendungsprogramme wie Bildbearbeitungssoftware bitten das Update beim Schließen des Programms zu installieren und stören so deutlich weniger als früher.

Im Internet surfen ohne Beobachtung

Durch das Einsehen des Seitenverlaufs des Browsers (»Internet Explorer/Edge«, »Google Chrome«, »Mozilla Firefox« oder »Safari«) werden genaue Informationen zum Surfverhalten sichtbar. Dort ist beispielsweise zu sehen, welche Internetseiten besucht und nach welchen Suchbegriffen (z.B. Frauenberatungsstelle) gesucht wurde. Der Verlauf kann zwar gelöscht werden, noch effektiver ist es jedoch, von vornherein – zumindest bei gemeinsam genutzten Geräten – den privaten Modus zu nutzen und die Speicherung des Verlaufs zu verhindern. Dies funktioniert auf Computern und Smartphones. Dazu wird ein neues Fenster im Internet-Browser als private Sitzung geöffnet. Im Internet Explorer und Edge heißt es »InPrivate-Modus«, für Chrome »Inkognito-Modus«, für Firefox »Neues Privates Fenster« und für Safari »privates Fenster«. Allerdings werden die Informationen erst gelöscht, wenn das Fenster bzw. der genutzte Tab geschlossen werden.

Der private Modus hat noch weitere Vorteile: Der Browser löscht die gesetzten Cookies, mit denen viele Seiten ihre Besucher*innen tracken – also verfolgen sowie Eingaben, die er sonst für die Autovervollständigung von Formularen und ähnlichem speichern würde. Über »Einstellungen« und »Sicherheit« sind die auf einem Rechner gesetzten Cookies einsehbar. Ein vorhandener Cookie ist kein Beweis für den Besuch einer Seite – durch das Einbinden von Werbung, Videos und SocialMedia-Inhalten werden heute oft zahlreiche, unterschiedliche Cookies gespeichert, ohne die Seiten selbst aufgerufen zu haben. Der private Modus ist leider kein Garant dafür, dass die Person komplett anonym im Internet unterwegs ist. Sobald man sich bei Online-Diensten einloggt, speichern die dahinterstehenden Firmen den Besuch. Auch bei Facebook sind Nutzer*innen trotz des privaten Modus für Facebook-Freund*innen dennoch erkennbar online, solange die Sichtbarkeit nicht in den Facebook-Einstellungen geändert wurde. Für zusätzliche Sicherheit ist es notwendig, sich vor dem Schließen des Tabs aus genutzten Diensten auszuloggen. Eventuell getätigte Einkäufe werden von Online-Shops ganz normal bearbeitet und heruntergeladene Dateien bleiben ebenfalls auf dem Rechner.

Beweismaterial und Kontakt mit Seitenbetreiber*innen

Die Beweissicherung bei digitaler Gewalt ist sehr wichtig und kann sehr umfangreich sein.[9] Im Falle von übergriffigem und gewalttätigem Verhalten empfiehlt es sich ein Tagebuch zu führen. Dort sollte alles erfasst werden zu Art, Umfang und Häufigkeit von Vorfällen. Hilfreich ist das Notieren möglicher Zeug*innen, aber auch die psychischen oder physischen Reaktionen der Angriffe bei der betroffenen Person. Zu den dokumentierbaren Übergriffen zählen Nachrichten und Drohungen, Fake-Profile in sozialen Netzwerken und anderen Plattformen, unerlaubt verbreitete Bilder sowie unerlaubt bearbeitete Bilder, unerwünscht installierte Programme und weitere ungewöhnliche Vorfälle. Jede Handlung sollte mit Beweismaterial gestützt werden. Je nachdem, wo und wie ein Übergriff passiert ist, bieten sich unterschiedliche Vorgehensweisen an. Eine einfache Sofortmaßnahme sind Screenshots, die zunächst im Vollbildformat und ohne Bearbeitung abgespeichert werden sollten, damit z.B. das Datum erkennbar ist. Viele

9 Für weitere Informationen siehe bff: Bundesverband Frauenberatungsstellen und Frauennotrufe (Hg.) (o.J.): »Wie dokumentiere ich?«. https://aktiv-gegen-digitale-gewalt.de/de/wie-dokumentiere-ich-richtig.html [Zugriff: 2.7.2020].

Programme benennen die Dateien automatisch mit einem Datums- und Zeitstempel. Es ist sinnvoll diesen bestehen zu lassen und nur ggf. mit einem Hinweis auf den Inhalt wie »Twitter-Nachricht mit Bildmontage« zu ergänzen, um die Datei später besser auffinden zu können. Um persönliche Informationen bei der Weitergabe zu schützen, sollte eine Kopie angelegt und eventuell erkennbare Infos in der Kopie unkenntlich gemacht werden.

Die Organisation Weißer Ring bietet mit »NO STALK« eine App für Android-Smartphones und iPhones an, um Foto-, Video- oder Sprachaufnahmen zu sichern. Die App richtet sich vor allem an Betroffene von Online-Stalking und bietet ihnen die Möglichkeit, Vorfälle wie in einem Tagebuch zu beschreiben. Die Daten werden in einem Rechenzentrum in Deutschland gespeichert und laut Weißem Ring vor Gericht anerkannt. Zu finden ist die App auf *www.nostalk.de* und in den gängigen App Stores.

Ob Facebook-Profile, Kommentare auf Facebook oder einzelne Tweets auf Twitter – oft sind Inhalte auf Webseiten und sozialen Netzwerken über *einen spezifischen Link* (URL) zu finden, wie etwa https://twitter.com/bff_gegenGewalt/status/1207997598419881988. Um etwa diesen Tweet zu sichern, muss dieser Link in einem Browser geöffnet werden, um dann im dessen Menü »Seite speichern unter…« die »komplette Seite« abzuspeichern. Außerdem sollte ein Screenshot gemacht werden, bei dem der komplette Link (sofern möglich) gut sichtbar ist. Das ist wichtig, falls der Inhalt des Posts nicht mehr abrufbar ist, wenn der Post von dem*der Urheber*in gelöscht wird.

In Messengern empfangene Sprachnachrichten können für weitere Verwendung exportiert werden. Die Android-Version von WhatsApp speichert die Nachrichten selbstständig im Dateimanager des Smartphones ab. Auf iPhones muss jede Sprachnachricht einzeln abgespeichert werden. Dazu drückt man lange auf die Nachricht, um zur Option »Weiterleiten« zu kommen. Über das Teilen-Icon kann die Nachricht auf dem Telefon oder einem externen Cloud-Dienst wie Dropbox gespeichert werden. Auch hier besteht der Dateiname aus Datum und Zeit der Aufnahme und sollte höchstens um einen aussagekräftigen Hinweis am Ende ergänzt werden.

Bei E-Mails empfiehlt es sich, diese mit einem E-Mail-Programm wie »Thunderbird«, »Outlook« oder »Apple Mail« abzurufen und zu sichern. Wichtig ist die Speicherung im Dateiformat .eml, das den »Mail Header« umfasst. Der Mail-Header bietet der Polizei wichtige Meta-Daten für die Strafermittlung, etwa über die verwendeten E-Mail-Server. Je nach Programm muss beim Speichern »Reine Datei der E-Mail«, »Outlook-Nachrichtenformat – Unicode« oder »Mail-Dateien« ausgewählt werden. Auch hier bieten sich

Datum und Hinweis auf den Inhalt als Dateiname an. Webmail-Oberflächen bieten manchmal ebenfalls einen eml-Download an, aber nicht immer; das GMX-Webmail speichert E-Mails nur als html-Dateien ohne Mail-Header. Die Header können im Web-Interface (Webansicht) separat angeschaut und dann als Textdatei extra gespeichert werden. Um sie einzusehen, muss meist auf »Header«, »Kopfzeile« oder »Original anzeigen« geklickt werden. Wird eine E-Mail weitergeleitet, entsteht übrigens ein neuer Mail-Header, der nur noch die Weiterleitung beinhaltet.

Viele Online-Dienste bieten Möglichkeiten, die Aktivitäten des eigenen Kontos zu exportieren. Dies kann nützlich sein, wenn die gewaltausübende Person Zugriff hatte und zum Beispiel Nachrichten darüber verschickt hat. So kann aus den Twitter-Einstellungen ein Archiv der eigenen Daten heruntergeladen werden; Google bietet unter *takeout.google.com* gleich verschiedene Archivformate für eine Sicherung an. Auch der Browserverlauf eignet sich zur Beweissicherung, wenn etwa der Browser genutzt wurde, obwohl die betroffene Person gar nicht zu Hause war. Hier ist es wichtig Screenshots inklusive des Datums zu machen, ohne die angezeigten Webseiten erneut aufzurufen oder anzuklicken, da die Seite sonst aus dem Verlauf vergangener Tage ans obere Ende ins »Jetzt« rutscht. Je nachdem, ob und wie Sie eine Anzeige erstatten wollen, können Beweise wie Screenshots und E-Mails, inklusive des Headers, neben der digitalen Sicherung ausgedruckt und analog abgelegt werden. Für das weitere Vorgehen und etwaige Nachfragen sollten die digitalen »Originale« sicher aufbewahrt werden.

Digitale Beweismaterialien können als Hinweise zu einer Anzeige über die Online-Wache der Polizei in fast allen Bundesländern unter *https://online-strafanzeige.de* vermerkt, jedoch nicht hochgeladen werden. Die Beweise sollten nicht an andere Personen weitergeleitet werden, um Manipulationen auszuschließen, ausgenommen sind natürlich Rechtsanwält*innen oder Beratungsstellen. Wenn die Beweise gesichert sind, sollte unverzüglich gemeinsam mit der betroffenen Person Kontakt mit den Seitenbetreiber*innen aufgenommen werden, um unerwünschte Informationen wie Posts, Fotos, Nachrichten, Daten oder Fake-Profile von Internetseiten oder in sozialen Netzwerken löschen zu lassen. Schließlich können personenbezogene Daten aus der Google-Suche oberflächlich gelöscht werden. Google bietet dazu ein Antragsformular unter: *https://google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf.* Falls die Kontaktaufnahme mit den Seitenbetreiber*innen keinen Erfolg hat, sollte ein*e Anwält*in hinzugezogen werden.

Geräte zurücksetzen oder neu installieren

Für einen digitalen Neuanfang können elektronische Geräte meist auf die Werkseinstellungen zurückgesetzt oder sogar das Betriebssystem neu installiert werden. Sowohl für das Smartphone als auch für Computer, Laptop und Tablets gilt dabei, dass zunächst alle persönlichen Daten extern gesichert werden müssen. Bei der Neu-Installation oder dem Zurücksetzen werden die installierten Programme und gespeicherten Daten gelöscht. Letztere sind danach nur in Ausnahmefällen mit spezieller Software wiederherzustellen. Für gängige Smartphones ist es möglich, unter »Einstellungen«, unter »Allgemein« oder »Allgemein verwalten« das Telefon in die Werkseinstellungen zurückzusetzen.

Im Internet finden sich Anleitungen, wie Computer oder Laptops ohne große IT-Kenntnisse neu aufgesetzt werden können. Unter Windows 10 geht dies inzwischen aus den »Einstellungen« heraus. Unter »Updates und Sicherheit« muss die »Wiederherstellung« ausgewählt werden. Dabei gibt es die Möglichkeit, die eigenen Dateien zu erhalten oder wirklich alles zu entfernen. Am sichersten ist es, die Dateien vorher gezielt zu sichern und anschließend alles zu löschen. Eine Neueingabe des Lizenzschlüssels ist bei diesem Vorgehen normalerweise nicht nötig. Bei älteren Windows-Versionen oder der Neu-Installation von Windows 10 ist eine Installations-DVD oder ein USB-Stick mit einer Installationsdatei nötig. Am einfachsten geht es, wenn ein Zugriff auf eine mitgelieferte Installations-DVD und den Lizenzschlüssel (auch »Product Key« genannt) gewährleistet ist. Dann sollte der Rechner das System von der DVD starten und das Betriebssystem direkt neu installiert werden. Wer den eigenen Lizenzschlüssel nicht kennt, muss diesen vor der Neuinstallation auslesen – auch dazu gibt es Gratis-Programme und Anleitungen im Netz. Oft ist er auf einem Aufkleber auf dem Rechner oder im mitgelieferten Benutzerhandbuch zu finden. Gibt es keine Installations-DVD, kann ein USB-Stick mit mindestens vier GB Speicher als Installations-Stick genutzt werden. Microsoft bietet dafür die »Windows USB/DVD-Download Tools« auf *https://microsoft.com/de-de/download/details.aspx?id=56485* an. Die deutsche Sprachversion ist mit de-DE gekennzeichnet. Neben dem Tool muss noch die passende Windows-Version als Datenträgerabbild bzw. ISO-Datei von https://microsoft.com/de-de/software-download/ heruntergeladen werden. Die ISO-Datei wird über das USB/DVD-Download Tool auf den Stick geladen, der nun ein »bootfähiger USB-Stick« ist, von dem aus die Installation startet. Dafür wird er beim Rechnerneustart als

»1st Boot Device« festgelegt. Bei einer Neuinstallation wird der USB-Stick allerdings automatisch wieder formatiert. Soll damit ein weiterer Laptop zurückgesetzt werden, muss das Prozedere von vorn begonnen werden. Mit dem USB/DVD-Download Tool kann alternativ eine Installations-DVD gebrannt werden. Computerzeitschriften bieten auch regelmäßig Notfall-Windows-DVDs an, die Heften beiliegen oder deren Inhalt aus dem Internet geladen werden kann, um bootfähige USB-Sticks zu erstellen.

Mac-Rechner lassen sich seit OS X Lion (10.7) direkt zurücksetzen. Dafür ist nur eine Internetverbindung nötig. Kann die bisherige Apple-ID weiterverwendet werden, müssen während eines Neustarts des Rechners die Tasten CMD und R gleichzeitig gedrückt werden. In den macOS-Dienstprogrammen kann die Option »macOS erneut installieren« gewählt werden. Für den Fall, dass künftig eine neue Apple-ID genutzt werden soll, muss die alte Apple-ID vor der Neu-Installation aus iTunes, iCloud und iMessage abgemeldet werden. Wurde die Festplatte in Partitionen (verschiedene Laufwerke) unterteilt, muss nach dem Neustart in den macOS-Dienstprogrammen zunächst das Festplattendienstprogramm ausgewählt werden. Hier können die Partitionen gelöscht werden. Schließlich kann auch die gesamte Festplatte gelöscht werden, bevor das System neu installiert wird. Dabei werden alle Daten so überschrieben, dass sie nicht mehr zu retten sind.

Ausblick

Aus der Beratung bei digitaler Gewalt ist bekannt, dass ein frühzeitiges, systematisches und schnelles Vorgehen zentral für den Schutz und die Handlungsfähigkeit von Betroffenen ist, um weitere Angriffe zu unterbinden bzw. bestehende Gefährdungen wie veröffentlichte Nacktbilder oder eine veröffentlichte Adresse für die betroffene Person abzuwenden. Die Bearbeitung dieser Gewaltform ist für die Berater*innen besonders zeitintensiv und bindet personelle Ressourcen, die in ambulanten Fachberatungsstellen oft noch unzureichend finanziert sind. Ebenso verfügen nicht alle Beratungsstellen über die fachliche Expertise für eine solche Beratung.

Nach Ansätzen der feministischen parteilichen Beratung ist es kontraproduktiv, Betroffenen digitaler Gewalt die Schuld zuzuweisen. Zum einen tun dies Betroffene oft genügend selbst, zum anderen findet hier eine Täter-Opfer Umkehr statt – ein Phänomen, das bei Gewalt gegen Frauen immer auftaucht. Wie bei allen Gewaltformen müssen auch bei digitaler Gewalt Be-

troffene ernstgenommen werden, sodass sie nach dem Kontrollverlust durch digitale Gewalt wieder in Handlungsfähigkeit gelangen können.

Neben der Wiedererlangung der Kontrolle gilt es, Betroffene über die grundlegenden Sicherheitsprinzipien ihrer digitalen Geräte aufzuklären, Beweise zu sichern, das physische und psychische Wohlbefinden zu schützen und die digitale Medienkompetenz zu stärken. Ein weiteres Ziel feministischer Intervention in diesem Bereich ist es, den gesellschaftlichen Diskurs über digitale Gewalt voranzutreiben, damit die Strafverfolgungsbehörden, Sozialen Netzwerke, Pornoplattformen und Spionage-Software-Firmen digitale Gewalt ächten und schnell auf sie reagieren.

Literatur

bff: Bundesverband Frauenberatungsstellen und Frauennotrufe (Hg.) (o.J.): »Wie dokumentiere ich?«. https://aktiv-gegen-digitale-gewalt.de/de/wie-dokumentiere-ich-richtig.html [Zugriff: 2.7.2020].

Bleich, Holger (2018): »Alptraum Handy-Wanze: Smartphone-Spionage-Apps als Stalker-Werkzeuge«, in: c't, Nr. 18, S. 76. https://heise.de/select/ct/2018/18/1535416499320900 [Zugriff: 5.1.2020].

Coalition Against Stalkerware (Hg.) (o.J.): »The State of Stalkerware in 2019«. https://media.kasperskydaily.com/wp-content/uploads/sites/92/2019/11/18053214/Kaspersky_Coalition_The-state-of-stalkerware-in-2019_ENG_fin.pdf [Zugriff: 5.5.2020].

Gierow, Hauke (2019): »Spionage-Apps: Schutz vor Überwachung ist möglich«. https://mobilsicher.de/ratgeber/spionage-apps-schutz-vor-partner-spyware-ist-moeglich#9 [Zugriff: 28.10.2019].

klicksafe/Institut für Digitale Ethik (IDE) der Hochschule der Medien Stuttgart (Hg.) (2018): »Neu bei klicksafe: Digital Safety Compass«. https://klicksafe.de/service/aktuelles/news/detail/neu-bei-klicksafe-digital-safety-compass/ [Zugriff: 1.3.2020].

NNEDV (National Network To End Domestic Violence) (Hg.) (2014): »Privacy and Safety on Facebook: A Guide for Survivors«. https://nnedv.org/mdocs-posts/privacy-safety-on-facebook-a-guide-for-survivors/ [Zugriff: 2.7.2020].