Claudia Fischer

Digitale Angriffe im Büro

Tipps für alle, die beruflich Geheimnisse wahren müssen

digitalcourage

KURZ&MÜNDIG

Art d'Ameublement

Band 9

KOSTENFREI

Einordnung

Wir arbeiten mit Menschen zusammen, die digital angegriffen werden oder wurden. Dabei geht es nicht um Beschimpfungen in sozialen Medien, sondern um direkte Attacken auf ihre Computer, Smartphones, Büroräume, Mailaccounts etc.

Diese Angriffe kommen von Täterinnen und Tätern, die es gezielt auf die Integrität von Berufsgruppen abgesehen haben, die mit sensiblen Informationen arbeiten: Anwältinnen, Ärzte, Pastorinnen usw. Ihnen und ihren Klientinnen und Klienten wollen wir mit dieser Broschüre helfen und ihnen zeigen, worauf sie achten müssen.

Motto:

„Ich habe keine Angst, bin aber professionell und aufmerksam."

Impressum

1. Auflage 05-21, Art d'Ameublement, cc-by 4.0, ISBN 978-3934636-37-8

Autorin: Claudia Fischer, verstandenwerden.de

Redaktion: Katrin Schwahlen, katrinschwahlen.de

Layout: Isabel Wienold, iwi-design.de

Bildlizenzen: S. 14 Gilles Lambert on unsplash; S. 15 public domain;
S. 30 Noa Laurin cc by 4.0; S. 31 Fabian Kurz cc-by 4.0
Alle weiteren Bilder: iwi-design.de, Isabel Wienold cc-by 4.0

Was ist ein digitaler Angriff?

Digitale Angriffe haben unterschiedliche Gesichter. Vielleicht denken Sie zuerst an „Hacking", dass also jemand versucht, z. B. Ihre Passwörter zu knacken und auf Ihre Geräte und Accounts zuzugreifen. Wie Sie sich davor schützen können, zeigen wir Ihnen ab ► Seite 26.

Digitale Angriffe bleiben häufig nicht digital, sondern haben physische Auswirkungen: Zum Beispiel, wenn jemand Kameras oder Mikrofone in Ihren Räumen versteckt oder kontrolliert [► S. 10] oder wenn jemand Sie verfolgt, weil er über digitale Wege weiß, wo Sie sich befinden [► S. 15].

Diese Broschüre kann Ihnen nur ein paar grundsätzliche Hinweise geben. Wenn Sie sicher sind, digital angegriffen worden zu sein, reicht das nicht. Dann brauchen Sie eine professionelle IT-Sicherheitsberatung! [► S. 25]

Sind Angriffe und Überwachung das gleiche?

Nein. Überwachung betrifft alle Menschen, nicht nur Sie persönlich. Überwachung gibt es von staatlicher Seite [z.B. durch Geheimdienste und Polizei] und von kommerziellen Firmen wie Facebook, Google und Amazon, die Persönlichkeitsprofile anlegen und vermarkten. Um Überwachung geht es in dieser Broschüre nicht.

Wer wird angegriffen?

Die meisten Menschen kennen digitale Angriffe nur aus Spionage-Thrillern. Aber für manche, insbesondere in bestimmten Berufen, sind sie Realität.

- **Die Ärztin**, die in einer Klinik Opfer von Menschenhandel gesund pflegt, bekommt Ausdrucke ihrer internen dienstlichen E-Mails per Post mit der Drohung „Wir wissen, was Du tust! Lass Deine Finger aus unseren Angelegenheiten!“
- **Der Anwalt**, der sich für politische Gefangene einsetzt, entdeckt eine versteckte Kamera in seinem Besprechungszimmer.
- **Journalistinnen** entdecken an Redaktionscomputern einen Keylogger, einen kleinen Zusatz-Stecker, der alle Tastatureingaben, Texte und Passwörter aufzeichnet.
- Einer **Psychotherapeutin**, die einen Sekten-Aussteiger therapiert, fallen immer wieder die gleichen dunklen Autos auf, wenn sie Termine mit ihren Kindern wahrnimmt. Offensichtlich weiß jemand laufend, wo ihre Kinder sind, und will die Therapeutin einschüchtern.

Alle diese Beispiele sind so passiert.

Solche Angriffe erschüttern das Urvertrauen und gefährden die Angegriffenen und ihre Kontaktpersonen. Gehen wir der Sache auf den Grund!

Was ist eigentlich passiert?

Versuchen Sie, Klarheit zu bekommen, womit Sie es zu tun haben.

Beispiel: Eine versteckte Kamera in Ihrem Besprechungszimmer ist ein physischer Angriff auf einen beruflichen Raum, eine objektive Bedrohung. Jemand hatte Zugang zu Ihren Räumen – aber wer kann das gewesen sein? Und wohin gehen die Bilder dieser Kamera?

☒ Hardware	☐ Software
☐ PC/Laptop	☐ Handy/Smartphone/ Tablet
Keins davon	
☐ Subjektive Bedrohung	☒ Objektive Bedrohung
☐ Externer Angriff ?	☐ „Inside-Job“ Besucher.innen/Kollegium
siehe Seite 20	
☒ Berufliche Geräte/ Räume/Accounts	☐ Private Geräte/ Räume/Accounts

Merkzettel:

Je mehr Fakten Sie über einen Angriff sammeln und dokumentieren, desto weniger Paranoia entsteht.

Und:

Je genauer Sie Ihren Angriff beschreiben können, desto besser können Fachleute Ihnen helfen!

Ist das schon Paranoia?

Ein digitaler Angriff, der gezielt auf Ihre Geräte oder Räume abzielt, ist aufwändig und fast immer illegal. Wer das tut, geht ein hohes Risiko ein. Wenn Sie einen Verdacht haben, angegriffen worden zu sein, stellen sich folgende Fragen:

? Sind Sie sich sicher, dass Sie digital angegriffen wurden? Haben Sie einen definitiven Beweis [z. B. eine versteckte Kamera entdeckt] oder kann es auch eine andere Antwort geben [z.B. kann jemand Informationen im Internet oder von Bekannten bekommen haben]?

? Wenn Sie sicher sind: Wie groß ist das Risiko, das jemand eingehen muss, um diese Aktion zu vollziehen?

? Was ist das mögliche Ziel der Aktion? Will jemand Informationen abgreifen? Oder Sie einschüchtern? Ihre Arbeit verhindern? Sie erpressen oder zum Schweigen bringen? Oder Ihre Daten benutzen, um jemand anderen zum Schweigen zu bringen?

? Wie groß ist das Interesse, das diese Person mit dieser Aktion verfolgt? Wer könnte dieses Interesse haben? Könnte es jemand aus Ihrem Umfeld sein? [▸ Seite 20]

? Wie groß ist das Risiko, dabei entdeckt zu werden?

Tipp: Suchen Sie sich eine Vertrauensperson, die Ihnen bei der Einschätzung hilft.

Wie realistisch ist ein Angriff?

Fragen Sie sich auch:

Lohnt es sich für die angreifende Person, so einen Aufwand zu betreiben, oder ist das Vorgehen unplausibel?

Wenn es beispielsweise darum geht, dass Sie als Journalistin eine bestimmte Recherche beenden sollen, gibt es ein hohes Entdeckungsrisiko, wenn jemand Ihr Auto sabotiert. Viel weniger aufwändig ist es, Ihnen deutlich zu machen, dass man weiß, wo Ihre Eltern wohnen. Ihr Umfeld zu bedrohen, ist dabei viel effektiver, als allein Sie selbst unter Druck zu setzen.

Faustregel: Wenn Sie Zweifel haben, ob es sich wirklich um einen Angriff handelt, gehen Sie lieber von einem Zufall aus.

Wenn Sie verfolgt werden oder sich jemand wiederholt in Ihrer Nähe zeigt, bitten Sie die Polizei, eine Personenfeststellung durchzuführen. Dann sind die Begegnungen dokumentiert und der Angreifer merkt, dass Sie sich wehren werden. Wie Sie am besten mit der Polizei kommunizieren, erklären wir auf Seite 29.

Welche Daten sind für Täter.innen interessant?

- **Standortdaten**
- **Zugriff auf Kamera und Mikrofon**
- **Kontaktdaten, Telefon-/Adressbücher**
- **Metadaten:** Mit wem haben Sie wann und wie oft Kontakt?
- **Kalenderdaten,** insbesondere wenn sie mit Ortsangaben und Adressbüchern verknüpft sind
- **Vertrauliche Kommunikationsinhalte** [Mails mitlesen, Gespräche abhören oder sogar mitschneiden]

Am sichersten sind Daten, die nicht entstehen. Nicht alle Apps, die Standortdaten abfragen, brauchen diese auch wirklich. Geben Sie diese Berechtigung im Smartphone nur frei, wenn Sie sie dringend brauchen. Die Bahn-App z. B. muss nicht dauernd wissen, an welchem Bahnhof Sie stehen; diese Info können Sie auch schnell per Hand auswählen.

Verknüpfen Sie Kalenderdaten nur dann mit Adressbuch und Co, wenn Sie diese Funktionen wirklich nutzen. Besonders sensibel sind Fitness-Apps: Ist das nicht meistens Spielerei? Soll Ihre Laufstrecke in fremde Hände geraten? Wer greift auf diese Daten zu? Lassen Sie sich nicht verführen! Datensparsamkeit ist eine Tugend!

Mehr zu Smartphones: ▸ ab Seite 14

Der digitale Giftschrank
Angriffe und Gegenmittel

Angriffe auf PC-Eingaben und Datenverkehr

Schützen Sie die Daten auf Ihrem Computer so gut wie möglich. Tipps zur Verschlüsselung von Festplatten und Sticks finden Sie auf ► S. 25. Auch per E-Mail sollten Sie so oft wie möglich verschlüsselt kommunizieren [► S 24].

Angriffe können allerdings auch schon vor der Verschlüsselung passieren, zum Beispiel zwischen Tastatur und Computer. Suchen Sie ab und zu Ihr Büro nach unbekannter Hardware ab – und schrauben Sie Ihren Computer auch ruhig mal auf. Machen Sie Fotos für spätere Vergleiche.

Was könnten Sie finden?

Keylogger oder Keygrabber [links] werden zwischen Computer und Tastatur gesteckt und nehmen jeden einzelnen Tastendruck auf. Auch Passwörter.

Über sternförmige Zwischenstecker [rechts] kann der Datenverkehr über Kabel-Netzwerke ausgeforscht werden: Von oben nach unten fließt Ihr Datenstrom, rechts und links stöpseln sich die ein, die mitlesen wollen.

Versteckte Kameras

Kameras sind inzwischen so winzig, dass es wirklich schwer ist, sie zu entdecken. Falls Sie neugierig sind: Suchen Sie mal im Internet nach „Kamera Damentoilette“. Sie werden auf unzählige Fälle von Spannern stoßen, die Frauen beim ‚Pipimachen‘ filmen. Die Kameras stecken in Schrauben, Toilettenrollen, Astlöchern, Schlüssellöchern, Lampen, Ladesteckern, nahezu überall.

Finden Sie die Kamera in dieser Armbanduhr?

Oder bei diesem Alexa-Wecker?

Auflösung nächste Seite.

Was können Sie tun?

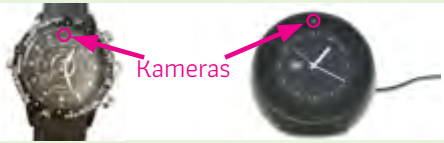
- Wenn Sie wollen, dass Ihr Besuch keine technischen Geräte mit in den Raum bringt, richten Sie einen abschließbaren Schrank dafür ein, zu dem Ihr Besuch die Schlüssel bekommt. Nur dann können beide Seiten sicher sein, dass niemand die Geräte manipuliert.

- Kleben Sie Kameras an Ihren Laptops, Handys, Tablets etc. standardmäßig ab, wenn Sie sie nicht brauchen.

- Suchen Sie aktiv nach eingebauten Kameras und meiden Sie Geräte, die Kameras enthalten.

- Es gibt Kamera-Suchgeräte für wenig Geld im Internet zu kaufen. Manche Apps bieten an, nach Sendefrequenzen von Kameras zu suchen. Wir haben damit allerdings bislang noch nie eine Kamera gefunden. Das meiste ist Nepp.

Auflösung von Seite 11:



Versteckte Mikrofone

Die klassischen Wanzen aus dem Spionage-Film gibt es immer noch. Dafür muss der Angreifer Ihre Räume betreten, um die Wanzen gut zu verstecken. Dabei ist das Entdeckungsrisiko am höchsten. Außerdem brauchen Wanzen eine Stromversorgung – Smartphones sind deshalb heute der viel einfachere Weg. [▸ nächste Seite]

In-Ohr-Wanzen sind kaum sichtbar und sehen aus wie ein Hörgerät. Wenn Ihr Besuch so etwas trägt, kann jemand z.B. im Nebenraum mithören. Die Reichweite ist nicht sehr groß. Der Ton kann aber auch von einem Gerät in der Jackentasche mitgeschnitten werden.

Merke:

Meiden Sie „Alexa“, Uhren, Fernbedienungen und andere „smarte“ Geräte, die per Stimme bedient werden. Denn die müssen permanent auf Empfang sein, um zu merken, wann sie angesprochen werden. Auch wenn es praktisch scheint – Finger weg!

Das Smartphone
Wanze und Freund

Welche Daten waren nochmal interessant?

Blättern Sie zurück auf Seite 8.
Fällt Ihnen etwas auf?

Genau, alle diese Daten tragen Sie in einem Gerät bei sich: Ihrem Smartphone. Und gleichzeitig die Daten Ihrer Familie, Ihrer Klient.innen, Ihr Online-Banking, Ihre Browserverläufe und Fitness-Daten. Deshalb müssen Sie die Funktionen Ihres Smartphones gut kennen, regelmäßig prüfen und Ihr Gerät gut vor Zugriffen schützen.

Standortdaten übers Smartphone

Standort-Apps: Viele Apps zeigen den Standort Ihres Handys an: Navigations-Apps, Fitness- und Jogging-Apps, „Finde mein Smartphone“-Apps, „Finden Sie Ihre Kinder“-Apps und viele mehr. ► Seite 8 und 16

„Stille SMS“ oder „seltsame Anrufe“: Wenn es nur einmal klingelt, hat sich vielleicht jemand verwählt. Vielleicht hat aber auch jemand Ihr Handy angepingt, um darüber Ihren Standort lokalisieren zu können. Eine „Stille SMS“ werden Sie gar nicht bemerken, aber Ihr Handy wird angeregt zu senden und damit seinen Standort preiszugeben. Bausätze für sogenannte IMSI-Catcher, die auch von Polizei und Geheimdiensten eingesetzt werden, um Gespräche abzuhören und Handy-Standorte zu bestimmen, gibt es schon für wenige hundert Euro.

Funkzellenabfragen: Im Normalbetrieb hat Ihr Handy meist Kontakt zu mehreren Telefon-Sendemasten. Darüber lässt sich Ihr Standort errechnen – in der Stadt genauer als auf dem Land, wo es weniger Sendemasten gibt. Mit dem neuen 5G-Standard wird das noch viel genauer, weil es mehr Sendemasten gibt.

Checkliste für die Smartphone-Sicherheit

- Stellen Sie eine komplizierte Code-Nummern-Sperre ein und achten Sie darauf, dass Sie bei der Eingabe nicht beobachtet werden. Meiden Sie Wisch-Gesten, Face-ID und Fingerabdruck.

- Prüfen Sie regelmäßig, welche der installierten Apps Sie wirklich brauchen. Unbekannte Apps könnten ein Hinweis sein, dass Ihr Smartphone angegriffen wurde. [► Seite 18]

- Prüfen Sie, welche Apps auf Telefonbuch, Mikrofon, Kamera und Standortdaten zugreifen. Deaktivieren Sie diesen Zugriff so oft wie möglich. Vorsicht: Nach manchen Updates wird der Zugriff automatisch wieder aktiviert. Kontrollieren Sie deshalb regelmäßig.

- Schalten Sie Bluetooth ab, wenn Sie es nicht nutzen. Es ist nicht sicher gegen Angriffe von außen.

- Wenn Sie sich unterwegs schützen oder Handys Ihrer Besucher.innen abschirmen wollen [► Seite 12], kappen Sie jede Funkverbindung mit einer Schutzhülle [z. B. von 🔗shop.digitalcourage.de]. Schalten Sie aber vorher Ihr Handy aus, denn sonst will es eine Verbindung herstellen und saugt Ihren Akku leer.

- Um auf Nummer Sicher zu gehen, reicht es nicht, den Flugmodus einzustellen,. Denn das GPS funktioniert trotzdem noch und auch Tonaufzeichnungen sind weiterhin möglich. Sie können abgerufen werden, sobald der Flugmodus wieder aus ist.

- Ohne Strom ist Ihr Handy wirklich lahmgelegt. Entfernen Sie deshalb in heiklen Situationen den Akku.

Moderner Mythos: Das Smartphone im Kühlschrank

Hartnäckig hält sich die Behauptung, im Kühlschrank wäre ein Smartphone sicher gegen Angriffe von außen. Der Kühlschrank sei ein Faradayscher Käfig, der Funkkontakte unterbindet. Das können Sie ganz einfach testen: Legen Sie Ihr Handy in den Kühlschrank und rufen Sie es an. Es klingelt? Dann hat die Abschirmung gegen Funksignale wohl nicht funktioniert. ☺

Was im Kühlschrank funktioniert: Mikro oder Kamera können Ihre Gespräche und Räume nicht mehr bespitzeln. Das bewirken aber auch unsere anderen Hinweise: Nehmen Sie den Akku heraus, verbannen Sie das Handy aus dem Raum [► Seite 12] oder wickeln Sie es in eine dicke Decke.

Fazit: Alles, was Sie von einem Smartphone im Kühlschrank erwarten können, ist ein kalter Akku. 🤡

Spy-Apps
(Spionage-Programme)

Die schlechte Nachricht ist: Es gibt sie wirklich. Programme fürs Smartphone (und den PC), mit denen sich quasi alles darauf kontrollieren lässt. Man kann alles sehen, was damit passiert, und es sogar fernsteuern. Solche Apps lassen sich auf dem Smartphone verstecken und kosten auch nicht viel.

Die gute Nachricht ist: Um so eine App zu installieren, muss man das Zielgerät in den Händen halten. Aus der Ferne kann man so etwas (bisher) noch nicht installieren. Deshalb kommen Spy-Apps erheblich seltener vor als die völlig berechtigte Angst vor ihnen.

Eine Spy-App auf einem Gerät zu finden ist sehr schwer. Ein Zeichen könnte sein, wenn plötzlich der Datenverbrauch enorm steigt oder der Akku sich schnell entleert. Aber das ist nicht eindeutig: Es könnte auch damit zu tun haben, dass der Akku alt wird und kaputt geht. Oder man hat eine andere App installiert, die viel Strom oder Daten verbraucht.

Manche Spy-Apps werden von Virenscanner-Apps oder von Google Play Protect entdeckt. Doch auch das hat seine Nachteile. Denn nicht jede App, die sich „Virenscanner“ nennt, ist auch tatsächlich ein Virenscanner. Und Google Play Protect setzt voraus, dass man Google nutzen möchte.

Auf einem iPhone kann man keine Apps verstecken. Eine Spy-App kann sich aber auch hier tarnen, indem sie sich einen harmlosen Namen gibt, wie „Wi-Fi“.

Wer tut sowas?
Umgang mit „Inside-Jobs“?

Wir kommen an diesen unangenehmen Fragen nicht vorbei: Wer versteckt Spionagegeräte in Ihren Räumen? Einbrecher? Wer schmuggelt Spy-Apps auf Ihr Handy? Geheimdienste?

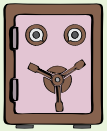
Die Erfahrung zeigt leider, dass es nicht selten „Inside-Jobs“ sind. „Spione“, die sich ganz legal in Ihren Räumen aufhalten und denen Sie vertrauen.

- Bei der Zeitungsredaktion [taz] war es ein Journalisten-Kollege, der mit Keyloggern [▸ Seite 10] Tastatureingaben mitgeschnitten hat.
- Anwälte aufgepasst: Vielleicht trägt Ihr Mandant die Armbanduhr mit Kamera? [▸ Seite 11]
- Ärztinnen, die von Menschenhandel betroffene Frauen behandeln, sollten sich fragen, ob ihre Patientinnen vielleicht erpresst werden, um möglichst viele Informationen aus der Praxis mitzubringen.
- Und klassisch: Bezahlen Sie Ihre Putzkraft gut genug, dass sie nicht anfällig für ein paar Euro nebenbei ist?

Nochmal: Es geht hier nicht um Paranoia! Es geht um Ihre Berufsgeheimnisse. Wenn Sie in sensiblen Bereichen arbeiten, sollten Sie sich diesen Fragen stellen. Das sind Sie auch Ihren Mandantinnen und Kunden schuldig, deren Geheimnisse Sie schützen müssen.

Deshalb ein paar Grundregeln:

- Lassen Sie Besuch in sensiblen Räumen nur kurz oder besser gar nicht alleine. Schon gar nicht, wenn sich dort technische Geräte befinden.
- Richten Sie ein Passwort ein, mit dem nur Sie Ihren Computer freischalten können, wenn er im Ruhezustand ist. Und verlassen Sie den Rechner nie, ohne diese Sperre aktiv einzuschalten [Tastenkombination bei Windows: Windows-Taste + L, Tastenkombination bei Mac: [Ctrl] + [Shift] + [Eject ⏏]].
- Passen Sie auf, dass niemand Sie bei der Eingabe Ihres Sperrcodes ins Smartphone beobachten kann [▸ S. 16]. Auch nicht mit einer Kamera.
- Trauen Sie Ihrem Bauchgefühl – wenn Ihnen etwas komisch vorkommt, protokollieren Sie Ihren Eindruck und überlegen Sie, was Sie tun können. Sprechen Sie mit einer Vertrauensperson, suchen Sie sich Rat.
- Vielleicht ist dies ein guter Moment, um das vollgeräumte Regal komplett aus- und wieder einzuräumen? Danach ist alles wanzenfrei und wieder gut sortiert.



Motto: Better safe than sorry!

[Früher hieß das: „Vorsicht ist die Mutter der Porzellankiste.“ – aber wer hat heute schon noch Porzellankisten? ☺]

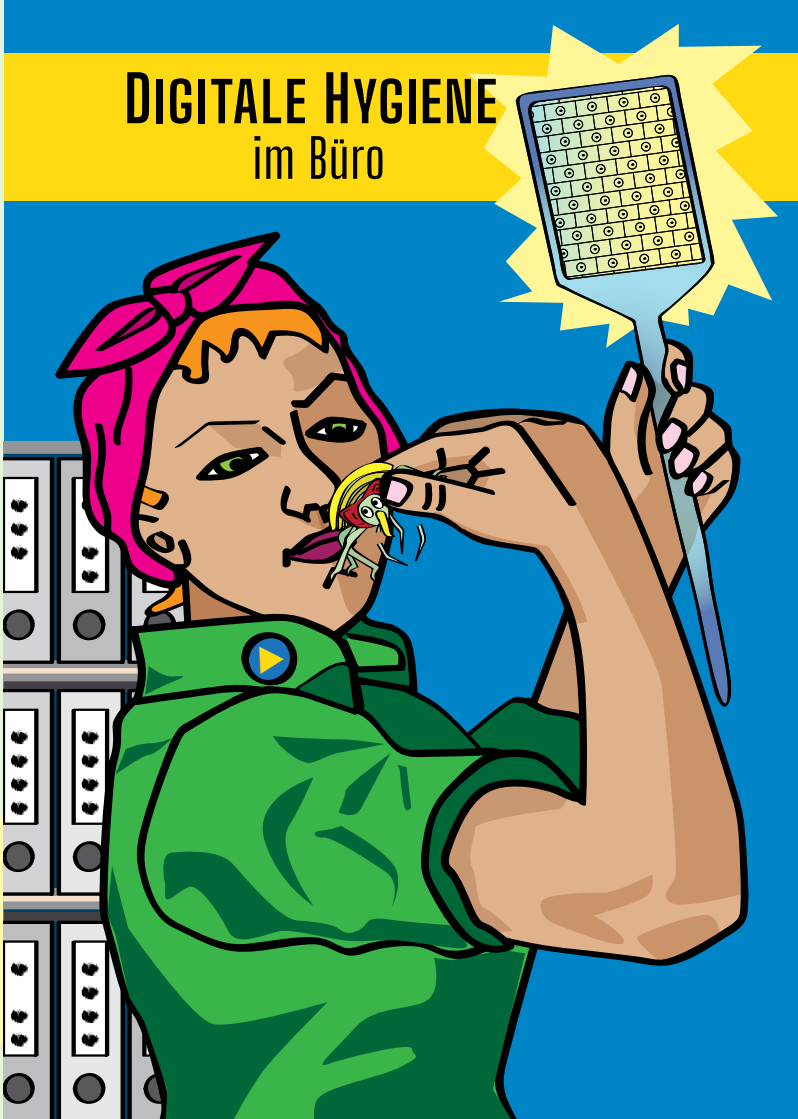
Beweissicherung beim Smartphone

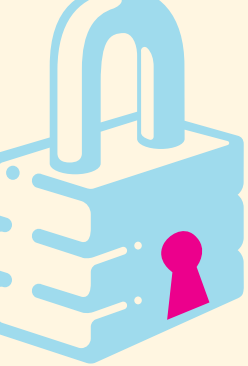
Wissen Sie, wie Sie mit Ihrem Smartphone einen Screenshot (Bildschirmfoto) machen? Das sollten Sie so schnell wie möglich können, denn wenn seltsame Dinge anzeigt werden, haben Sie oft wenig Zeit.

Optimal ist, wenn auf dem Bild **Datum, Uhrzeit** und die **aktive App** erkennbar sind.

Sichern Sie diesen Screenshot so schnell wie möglich – zum Beispiel, indem Sie ihn zur Aufbewahrung an Vertrauenspersonen senden. Es könnte auch jemand ein Foto von Ihnen und Ihrem Handy-Display machen und später die Authentizität bezeugen.

Mit der „NoStalk“-App des Weißen Rings kann man Beweise vom Smartphone direkt hochladen und sichern. Die App wurde in Zusammenarbeit mit der Polizei entwickelt. Leider lassen nicht alle Gerichte diese Daten als Beweise zu. Sie gelten aber zumindest als „schwächere Anscheinsbeweise“.





Sichere E-Mails

Beherrschen und beachten Sie die Grundregeln für sicheren E-Mail-Verkehr? Öffnen Sie Anhänge und Links mit Bedacht. Trick: Fahren Sie mit der Maus über einen Link, ohne zu klicken. Meist wird dann unten links angezeigt, wohin dieser Link führt.

Halten Sie Computer, Smartphone, Programme und Apps immer aktuell. Bei Windows-Rechnern sind Firewall und Virenscanner schon eingebaut – Bitte einschalten!

Nutzen Sie einen sicheren E-Mail-Anbieter? posteo.de und mailbox.org verschlüsseln zu vielen anderen Anbietern automatisch. Der Service kostet wenig und ist das Geld wert!

Verschlüsseln Sie E-Mails? Eigene, aktive Verschlüsselung sollte für sensible Berufe Standard sein. Nutzen Sie OpenPGP oder pEp. Ja, das bedeutet anfangs Aufwand, aber man gewöhnt sich erstaunlich schnell daran.

Auf dem Smartphone ist E-Mail-Verschlüsselung leider noch unkomfortabel, aber die Technik entwickelt sich weiter. Bleiben Sie dran!

Verschlüsseln Sie Ihre Datenträger

Ob Computer, Stick oder mobile Festplatte: Mit der Software Veracrypt können Sie Datenträger sicher verschlüsseln. So kommt niemand an Ihre Daten, auch kein Dieb.

Achten Sie auf Aktualisierungen! Bislang haben wir die Software Truecrypt empfohlen. Diese wurde nicht mehr weiter entwickelt, sondern von Veracrypt abgelöst.

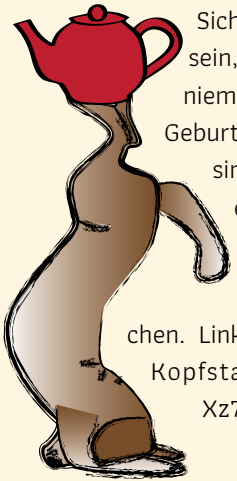
Also: Wenn Sie IT-Nachrichten nicht laufend verfolgen, setzen Sie sich mindestens zweimal im Jahr einen Termin dafür. Gibt es inzwischen etwas Besseres auf dem Markt? Gab es Sicherheitslücken? Haben Sie automatische Updates aktiviert? Ist alles auf dem neuesten Stand?

Hilfe finden

Gut wäre natürlich, Sie hätten jemanden, der Sie bei der IT-Sicherheit unterstützt. Aber leider ist so jemand schwer zu finden. Wer sich auskennt, wird von großen Firmen "vom Markt gepflückt". Es gibt keine hilfreichen Dachverbände oder Gütesiegel.

Tipp: Hören Sie auf Empfehlungen und greifen Sie zum Telefon. Erklären Sie Ihre Sicherheitsbedürfnisse. Machen Sie sich ein Bild, ob die Person zu Ihnen passt. Falls Sie bereits angegriffen wurden: Suchen Sie nach "IT-Forensik" oder "Computer-Forensik".

Wählen Sie sichere Passwörter



Sichere Passwörter sollten lang/komplex sein, nirgendwo doppelt verwendet und mit niemandem geteilt werden. Namen oder Geburtstage von Haustieren oder den Liebsten sind verboten. Die können viel zu leicht erraten werden.

Am besten wählen Sie vier Wörter und trennen diese mit einem Sonderzeichen. Links sehen Sie z. B. Hund.Teekanne.rot.Kopfstand – das ist sicherer und leichter als Xz7Qm9?HnqrY*

Nur Sie selbst sollten Ihre eigenen Passwörter kennen. Legen Sie Ihre Log-ins in Websites und Mailkonten selbst an, teilen Sie die Passwörter niemandem mit und nutzen Sie eine Passwort-Verwaltung, z. B. KeePassXC.

Vorsicht bei der Funktion „Passwort vergessen?“ Prüfen Sie regelmäßig, welche Mailadressen und Handynummern in Ihren Kundenkonten hinterlegt sind. Wer sich hier böswillig einträgt, kann Ihre Accounts kontrollieren!

Einfach mal anders machen:
Digitale Life-Hacks

Ein einfacher Trick, Angreifer zu verwirren und nicht komplett durchleuchtbar zu sein, ist, wenn Sie regelmäßig bewusste **Medien-Brüche und Stolpersteine** einbauen. Beispielsweise:

- Wenn Ihnen eine E-Mail komisch vorkommt, greifen Sie zum Telefonhörer und fragen Sie nach. [Medienbruch Mail → Telefon]
- Wenn Sie eine komische Nachricht [Mail, SMS, …] bekommen, stellen Sie erst eine Rückfrage, bevor Sie mit einer Antwort etwas preisgeben. [Stolperstein]
- Schicken Sie einen Link per Mail und übermitteln Sie das Passwort erst beim nächsten persönlichen Treffen. [Medienbruch, niemals Link und Passwort über den gleichen Kanal]

Löschen Sie **Accounts**, wenn Sie sie nicht mehr brauchen.

Füttern Sie Ihr **Adressbuch** auf dem Smartphone nicht mit den echten Namen gefährdeter Kontaktpersonen. Verwenden Sie Spitznamen, die nur Sie kennen. Viele Apps greifen nämlich auf Ihr Adressbuch zu. Seien Sie datensparsam: Adressen nur, wenn es nötig ist, Geburtstage von Ihren Kontakten gehören gar nicht ins Mobilgerät. Je weniger sensible Daten Sie miteinander verknüpfen, desto besser.

Digitale Unabhängigkeit

- Übernehmen Sie Verantwortung für Ihre Geräte und Passwörter. Wenn Sie von der IT-Abteilung Ihres Arbeitgebers abhängen, melden Sie besonderen Schutzbedarf an und suchen Sie das Gespräch.
- Schützen Sie Ihr Netzwerk im Büro und lassen Sie keine Fremden ins WLAN. Alternativ können Sie einen Gastzugang anbieten (viele Router können das).
- Trennen Sie dienstliche und private Geräte.
- Verzichten Sie auf die Internet-Giganten wie Facebook, Amazon, Google, Dropbox, Zoom, Mailanbieter wie GMX und web.de sowie Smart Home-Geräte wie Alexa. Auf 🔗digitalcourage.de/digitale-selbstverteidigung finden Sie für fast alle Dienste sichere Alternativen.
- Nehmen Sie Ihr Bauchgefühl ernst. Wenn Ihnen etwas komisch vorkommt, schauen Sie genau hin und suchen Sie jemanden, der/die den Verdacht mit Ihnen prüft.

Und was ist mit Messengern? WhatsApp und sowas?

WhatsApp geht gar nicht, das gehört zu Facebook, und die lesen alles mit.

Gibt es bessere Messenger?

Ja, viele. Welcher zu Dir passt, findest Du auf 🔗digitalcourage.de/Messenger heraus.

Und wenn alles schief geht …

Auch darüber müssen wir reden. Wenn Sie ein Spionage-Tool in Ihrem Büro gefunden haben, wenn Sie jemanden aus Ihrem Umfeld ertappt haben, wenn Daten abgeflossen sind – was dann?

Bewahren Sie Ruhe! Atmen Sie durch, behalten Sie einen klaren Kopf. Überlegen Sie, wer Ihnen helfen kann. Alleine sind Sie womöglich überfordert und machen Fehler.

Anzeige erstatten oder nicht? **Es kommt darauf an. Wie eindeutig können Sie Ihren Angriff nachweisen? Gefährden Sie Ihre Klientinnen oder Mandanten mit einer Anzeige? Wie können Sie diese schützen?**

Gehen Sie nur in Begleitung **(mit Anwältin oder Beratungsstelle) zur Polizei. Machen Sie einen Termin aus, dann können Sie etwas sicherer sein, einer kompetenten Person gegenüber zu sitzen.**

Heuern Sie Fachleute an! Sie haben Ihren Job, sind Anwalt, Medizinerin oder Journalist. Sie können nicht auch noch IT-Spezialistin sein, denn das ist ein Vollzeitjob. Investieren Sie rechtzeitig Zeit und Geld in Ihre IT-Sicherheit, bevor etwas passiert.

Die Autorin

Claudia Fischer ist freie Journalistin und Diplom-Medienpädagogin. Sie beschäftigt sich journalistisch seit 20 Jahren mit organisierter sexualisierter Gewalt und noch etwas länger mit Grundrechten und Digitalisierung.

Claudia Fischer schreibt für Print und Online, hat viele Jahre TV- und Radio-Erfahrung und hält Workshops und Vorträge. Für Digitalcourage arbeitet sie bei den BigBrotherAwards mit, ist Redakteurin des Jahrbuchs und für die Reihe „kurz und mündig“.

Kontakt: verstandenwerden.de,
claudia.fischer@digitalcourage.de

Die KURZ&MÜNDIG-Reihe wird herausgegeben von:

digitalcourage e.V. engagiert sich seit 1987 für Grundrechte, Datenschutz und eine lebenswerte Welt im digitalen Zeitalter. Wir sind technikaffin, doch wir wehren uns dagegen, dass unsere Demokratie „verdatet und verkauft“ wird. Seit 2000 verleihen wir die BigBrotherAwards. Digitalcourage ist gemeinnützig, finanziert sich durch Spenden und lebt von viel freiwilliger Arbeit.

Mehr zu unserer Arbeit finden Sie auf
digitalcourage.de **und** bigbrotherawards.de

Weitere Informationen zum Thema dieser Broschüre finden Sie in anderen Heften aus dieser Reihe:

Stalking, Hass, Kontrolle
Digitale Gewalt erkennen und beenden, k&m Band 6

Faire Websites
Handbuch für erfolgreiche Macherinnen und Macher, k&m Band 1

In der KURZ&MÜNDIG-Reihe sind bisher erschienen:

01 Digitale Mündigkeit
02 Datenschutzrechte in Schulen durchsetzen
03 Faire Websites
04 Leitlinien für digitale Bildung in Schulen
05 Uploadfilter
06 Stalking, Hass, Kontrolle
07 Homeoffice
08 Digitale Bildungsangebote selbst erstellen
09 Digitale Angriffe im Büro

Dieses KURZ&MÜNDIG-Minibuch ist auch als komfortables interaktives PDF erhältlich. Es kostet nur 5,00 Euro und ist wie alle KURZ&MÜNDIG-Ausgaben (auch als Printversion) erhältlich unter: digitalcourage.de/kum

Versteckte Kameras im Besprechungszimmer,
Keylogger am Computer,
Spionage-Apps auf dem Smartphone.

Anwälte, Ärztinnen, Journalisten, Beratungsstellen, Pastoren und Menschen, die die Geheimnisse anderer wahren müssen, finden in diesem Heft konkrete Tipps und Hinweise, was technisch möglich ist und wie Sie sich schützen können und sollten.

BETTER SAFE THAN SORRY!

Digitalcourage e.V.
Marktstraße 18 | 33602 Bielefeld
mail@digitalcourage.de | digitalcourage.de
T: +49 521 1639 1639

9 783934 636378 >
5,00 Euro
4,00 SFR
ISBN 978-3934636-37-8

digitalcourage
k&m009 Digitale Angriffe