Computersicher vor was? Und vor wem?

Ein paar Gedanken aus unserem Workshop beim RH-Seminar 2022

Wer beim Seminar der Roten Hilfe 2022 dabei war, mag sich an unseren etwas wolkig mit „Computersicherheit“ überschriebenen Workshop erinnern. Darin haben wir zunächst einmal die einschlägigen Fragen der Anwesenden gesammelt und im Anschluss versucht, diese Fragen so gut wie möglich zu beantworten. Es hat sich ergeben, dass wir dabei einen gemeinamen Hintergrund der Antworten abgesteckt haben, der, so hoffen wir, auch als Artikel interessant ist.

Im aktivistischen Umgang mit EDV mischt sich recht regelmäßig großer Eifer in der Abwehr ziemlich unplausibler Angriffe mit grobem Leichtsinn an anderen Stellen. Beispiele für ersteres wären zum Beispiel Programme, die Anfang der 2000er Jahre Text mit niedrigem Kontrast und Störpatterns anzeigten, um TEMPEST-Angriffe abzuwehren, also (gerade bei Röhrenmonitoren auch wirklich sehr erfolgversprechende) Versuche, Bildschirminhalte aus der Ferne mit einer Antenne auszulesen. Heute ist das verbreitetste Beispiel vielleicht die Sorge, die deutsche Polizei könne Mobiltelefone als Wanzen einsetzen (vgl. RHZ 3/2008; zumindest an diesem Teil hat sich nicht viel geändert).

Grober Leichtsinn hingegen ist das Hinterlassen von Spuren, für die die Polizei Programme gekauft hat oder die sie aufgrund ihrer Gewalt über Betreiberfirmen leicht bekommen kann: Telefon-Verbindungsdaten, riesige Mail-Inboxen oder -Archive, unverschlüsseltes Zeug auf beschlagnahmegefährdeten Festplatten oder gar „in der Cloud“, Server-Logs mit echten IP-Adressen und so fort.

Tatsächlich ist es aussichtslos, sich gegen jeden möglichen Angriff auf EDV absichern zu wollen, jedenfalls, wenn mensch politisch tätig sein und nicht nur Geheimdienst spielen will. Daher muss mensch überlegen, was die eigenen und fremden Rechner aushalten sollen und dann sehen, wie das mit den Möglichkeiten der Menschen zusammengeht, denn immerhin sollen die Leute den Krempel ja benutzen. Die tollste, „sicherste“, selbst offenste Technologie hilft nicht, wenn die, die sie nutzen sollen, am Ende genervt auf die bequemen kommerziellen Schnüffeldienste ausweichen.

Bedenkt bei all dem auch, dass fast alle Menschen einen *viel* besseren Instinkt dafür haben, wie ein verantwortlicher Umgang mit Daten aussieht, wenn sie physisch vorhanden sind, also etwa auf Papier oder zumindest auf einem USB-Stick. Insofern: Mensch sollte einen guten Grund haben, Daten auf einen Computer zu packen, und einen noch besseren, Daten statt auf konkreter und greifbarer Hardware auf irgendwelchen abstrakt erscheinenden Computern anderer Leute (genau: das ist diese „Cloud“) zu speichern.

Auf dieser Basis könnt ihr euch Gedanken machen über die Szenarien für Angriffe, die diese Daten abziehen wollen könnten, und dann überlegen, welchen davon ihr realistisch begegnen könnt, bei welchen ihr vielleicht die Folgen etwas abmildern könnt – und bei welchen nur die Abwägung bleibt, ob ihr es lasst oder halt doch erhebliche Risiken eingeht.

Die folgenden vier Angriffs-Kategorien können helfen, eigene Praktiken zu reflektieren.

Sie haben dein Passwort

Szenario: Nazis oder Bullen machen das gmx-Konto auf und lesen darin die Mails. Also: das muss kein Mail-Konto sein, das stimmt genauso für dropbox oder die meisten Chatplattformen (jedenfalls die, die Gesprächsverläufe auf ihren Servern halten) oder generell Daten auf Servern von Dritten, die nur durch eine Zugangskennung und nicht durch separate Verschlüsselung unter eurer eigenen Kontrolle geschützt sind.

Gegen sowas hilft z.B. PGP bei Mails, weil immerhin schon mal nicht mehr die Inhalte gelesen werden können. Vor allem hilft aber, Daten auf Maschinen anderer Leute besonders rasch zu löschen. Löschen, „ge-

sunden Menschenverstand“ anwenden, ist übrigens ganz generell die wichtigste Datenschutzmaßnahme, weit vor total raffinierten Technics („technische und organisatorische Maßnahmen“ im Datenschutz-Jargon). Ihr schneidet (hoffentlich) eure Gespräche im wirklichen Leben nicht mit. Tut das auch für eure Chats nicht. Nur, weil es einfach ist, ist es noch lange keine gute Idee.

Und wenn ihr doch Archive von Mails, Schriftstücken, Bildern oder was immer anlegt, tut es wenigstens so, dass ihr den Speicher anfassen könnt und nach Möglichkeit so, dass Rechner (ja, dazu gehören natürlich auch Mobiltelefone), an denen der Speicher hängt, nicht ständig aus dem Internet erreichbar sind. Natürlich ist es bequem, auf die gleichen Daten vom Desktop, einem Notebook und einem Mobiltelefon aus zugreifen zu können. Aber je einfacher das ist, desto einfacher haben es auch Nazis und/oder Bullen. Und desto mehr Zeit haben sie.

Hausdurchsuchung!

Szenario: Die Polizei kommt und schleppt die EDV (per Hausdurchsuchung oder auch einfach nur das Telefon bei Gewahrsamnahme) in die Asservatenkammer. Das ist dann nur noch ärgerlich (weil: Elektrik weg) und keine Katastrophe mehr, wenn die lokalen Massenspeicher verschlüsselt sind. Allerdings kennt das die Polizei inzwischen auch, und sie versucht dann und wann mit einigen Tricks, an laufende Maschinen mit entschlüsselten Massenspeichern zu kommen. Gegen sowas wiederum helfen mehrere verschlüsselte Container für verschiedene Anwendungen. Und natürlich: Geräte ausschalten, wenn sie nicht benötigt werden.

Solche verschlüsselten Container sind Stücke auf dem Massenspeicher, in denen ein Programm Daten verschlüsselt verwaltet und diese dem Betriebssystem als eine Sammlung von Dateien (also einen Verzeichnisbaum) präsentiert. Mit anderen Worten: Wenn ihr Daten aus so einem Container braucht, startet ihr ein Programm, gebt ein Passwort ein und bekommt dann etwas wie ein neues Verzeichnis (oder „Laufwerk“, wenn ihr noch Windows habt) in eurem Computer. Was ihr dortrein speichert, ist physisch – also auf dem Speicher – verschlüsselt. Wenn ihr fertig seid, könnt ihr die Daten wieder aushängen, und sie sind auch für Blitz-Hausdurchsuchungen (oder Staats- und Verschlüsselungstrojaner, siehe unten) nicht zugänglich.

In RHZ 4/2018 haben wir von encfs erzählt, was – für geeigenete Bedeutungen von „leicht“ – sehr leicht feingliedrige Plattenverschlüsselung erlaubt; so könntet ihr z.B. euer Mail-Archiv entschlüsselt halten, während ihr Mails lest, während eure Flugblätter verschlüsselt blieben, und beides verschlüsselt, während ihr mit personenbezogenen Daten Dritter, etwa für euren Job, arbeitet. Etwas konventioneller (und kryptographisch korrekter) ist das auf vielen Plattformen verfügbare veracrypt[1].

Die meisten Mobiltelefone lassen sich heute recht leicht verschlüsseln, und die Verfahren sind im Prinzip durchaus sicher, modulo den Schwierigkeiten, etwas wie Passwörter einzutouchen. Lasst euch zur Heilung dessen nicht zu Biometrie (Fingerabdrücke, Gesichtserkennung o.ä.) verführen: im Zweifel kontrolliert die Polizei euren Körper *viel* leichter als eure Gedanken.

Allerdings bestimmen bei Smartphones am Ende Apple bzw. Google, was auf den Geräten passiert, auch wenn sie das aus kommerziellen Gründen gegenwärtig noch nicht regelmäßig nutzen, um für die Staatsgewalt Daten abzuziehen. Außerdem speichert die durchschnittliche App heute praktisch keine Daten mehr auf dem Telefon selbst und schiebt sie stattdessen zu den Leuten, die Software, Dienste oder halt euch verkaufen. Grundregel: Wenn so eine App Daten „mit anderen Geräten teilen“ kann, sind diese Daten schon irgendwo im Netz, so dass eure Telefonverschlüsselung wahrscheinlich nicht mehr wirkt.

Lawful Interception

Szenario: Abhören auf der Leitung (in Wirklichkeit: beim Telekommunikations-Unternehmen). Das geht für normale Telefonie und SMS natürlich immer noch so einfach wie früher. Für Computerkram dagegen ist das inzwischen ernsthaft schwierig. HTTPS und anderes SSL-gekapseltes ist im Großen und Ganzen sicher gegen passives Abhören. Das ist auch der Hintergrund für die Sucht der „Bedarfsträger“ nach dem Staatstrojaner: sie wollen die Daten abschnorcheln, bevor sie in die Transportverschlüsselung kommen, sofern sie nicht einfach zu den Betreiber_innen der Server gehen können. Selbst dann ist für sie bei Ende-zu-Ende-verschlüsselter Kommunikation (wie sie einige der verbreiteten kommerziellen Plattformen in einigen Modi anbieten, und ebenso bei e-Mail mit PGP) oft nichts zu holen.

Häufig nicht (hinreichend) zu verschleiern sind dabei Verkehrsdaten, also Information darüber, wer wann

mit wem kommuniziert hat. Ganz klassisch kann mensch hier durch Nutzung von Tor abhelfen; Tails macht das per Voreinstellung. Tor macht es für *alle* Beteiligten glaubhaft schwierig, eure Klicks nachzuverfolgen, auch wenn es natürlich nicht magisch Mail-Adressen oder Chat-Identitäten verschwinden lässt. Doch Vorsicht! Auf den wenigen Übergängen zwischen anonymen Tor-Netz und dem Rest des Internets hören garantiert staatliche Stellen mit. Wenn ihr also unverschlüsselte Verbindungen habt (z.B. http oder unverschlüsseltes Messaging), dann werden die auf jeden Fall mitgelesen werden, wenn sie das Tor-Netzwerk verlassen. Mehr dazu in get connected von RHZ 4/07 und 2/08 (alt, aber immer noch zutreffend).

Zum „passiv" beim Abhören oben: Solange ihr euch nicht per Protokoll Gedanken machen müsst, wem die Schlüssel eigentlich gehören (also insbesondere bei https), ist die Transportverschlüsselung anfällig gegen Man-in-the-Middle-Angriffe, bei denen euch jemand „aktiv" einen Schüssel für, sagen wir, riseup.net unterschiebt, der in Wirklichkeit sein_ihr eigener ist und dann zwischen euch und riseup sitzt und mitliest. Während sowas in Firmennetzen unter dem Vorwand des „Virenscannens" leider durchaus üblich ist, findet es staatlicherseits nach unserer Kenntnis nicht regelmäßig statt, und es würde wohl auffallen, wenn das verbreitete Praxis wäre: gefälschte Schlüssel dieser Art aus anderen Ländern sind jedenfalls schon öfter mal aufgeflogen.

Der Staatstrojaner

Szenario: Der Staat (oder Leute, die mit Erpressung ihren Lebensunterhalt verdienen wollen) lässt in eurer EDV Programme laufen, die Daten von der Platte oder aus Kommunikationsprogrammen abziehen oder die Verschlüsselung stören. Sich gegen sowas „sicher" zu wehren ist sehr schwierig. Andererseits: Staatstrojaner-Einsatz ist immer noch selten (~100/Jahr bundesweit), und sein *erfolgreicher* Einsatz ist noch seltener. Selbst wacklige EDV geht nicht einfach auf (äußeren) Knopfdruck auf – auch nicht für Erpressungstrojaner.

Zumindest beim alten Digitask-Trojaner (~2010) gelangen Angriffe regelmäßig nur, wenn die Staatsgewalt (Zoll z.B.) die Geräte in der Hand hatte. Die Vorstellung, dass sich da Mitarbeiter_innen der Innenministerien hinsetzen und Rechner durch „Hacking" und unveröffentlichte Sicherheitslücken aufbrechen, ist eher autoritäres Wunschdenken der Gegenseite. Allerdings: Die meisten einschlägigen Gesetze erlauben, dass Bullen in Wohnungen gehen, um Staatstrojaner zu installieren.

Diesen Vorteil haben die Betreiber_innen privater Erpressungstrojaner nicht. Fieserweise sind die längst über das lokale Verschlüsseln hinausgewachsen und lassen ihre Software inzwischen auch mal Daten ins Netz schieben. Statt Geld für Entschlüsselung fordern diese Leute dann Lösegeld für die Unterlassung der Veröffentlichung. Guckt mal auf eure Inbox und überlegt, wie doof das in eurem Fall wäre. Die große Gruselvorstellung in so einem Szenario wäre, wenn sich so beispielsweise Unterstützungsanträge mit allem drum und dran in „der Cloud" wiederfänden...

Wer es Staats- und anderen Trojanern schwer machen will, muss zumindest mal die Software auf dem Rechner halbwegs aktuell halten. Meistens sind die Vektoren hier ganz platt Makros in Office-Dateien u.ä., die per Mail kommen. Angegriffen wird ganz besonders Combo aus Outlook, Office und Active Directory („Windows-Ökosystem"). Gerade die Beschaffenheit und Standardkonfiguration der Office-Programme ist hier grausam. Stellt *zumindest* mal Makros ab und pflaumt Leute an, die euch Dateien schicken, die von diesen abhängen.

In zweiter Linie kommen Trojanerangriffe über Webseiten, die mensch per Link in Mails oder auf Twitter besuchen soll („Herzlichen Glückwunsch, sie haben x Euro gewonnen"). Diese Seiten versuchen dann, Lücken in der Javascript-Maschinerie von Web-Browsern auszunutzen. Aktuelle Browser und vor allem Javascript-Blocker sind hier viel wert. Das Internet sieht übrigens ohne Javascript auch viel weniger hässlich aus.

Fazit

So sehr mensch jetzt Angriffsszenarien aus- und überdenken möchte, zentral bleibt: Wichtiger als Technik ist Menschenverstand. Daten, die gar nicht gespeichert sind, sind gegen alle denkbaren Angriffsszenarien unterhalb von Telepathie sicher.

Datenschutzgruppe der Roten Hilfe HD/MA

Kontakt und Artikel-Archiv: https://datenschmutz.de

PGP Fingerprint: 4FD3 B3EE 7FCE 9FFD EC75 CAF9 4847 5F52 5C0C 5DB1

[1] https://www.veracrypt.fr