Allgemeines

E-Mails (oft auch nur Mails genannt) werden auch als „elektronischer Brief“ bezeichnet und dienen zur Übertragung von Nachrichten. Früher waren sie auf reinen Text beschränkt. Durch eine Erweiterung (MIME – Multipurpose Internet Mail Extensions) können auch Dateien in E-Mails versendet werden. Da E-Mails ursprünglich nur für Text gedacht waren, werden die Daten vor dem Versand entsprechend angepasst. Dabei vergrößert sich die Dateigröße und dies kann zu Problemen führen, wenn der Anbieter von SenderIn oder EmpfängerIn Beschränkungen für die Größe der E-Mails hat, was meistens der Fall ist. Im Allgemeinen tritt dies nicht auf. Falls eine Mail aus Speicherplatzgründen nicht übermittelt wurde, wird mensch jedoch darüber benachrichtigt.
Wenn mensch nun eine E-Mail schreibt, wird diese an den Mailserver des eigenen E-Mailanbieters geschickt. Dort wird die E-Mail entweder direkt zugestellt, wenn der/die EmpfängerIn seine/ ihre E-Mailadresse bei demselben Anbieter hat, oder der Mailserver schickt es an einen anderen Mailserver. Bei dem nächsten Mailserver geschieht nun das Gleiche, bis ein Mailserver erreicht wird, bei dem es den/ die EmpfängerIn gibt und die Nachricht zugestellt wird.

E-Mails sind wie Postkarten

Die Gefahr ist nun, dass die E-Mails, die einfach Textdateien sind, von jedem dieser Mailserver kopiert oder verändert werden können. Das heißt es kann alles verändert werden, also z.B. der Absender oder der Inhalt der Nachricht. Außerdem können Kopien der Mails angefertigt werden, die gespeichert und ausgewertet werden können. Die Auswertung nach bestimmten Begriffen ist seit 1998 üblich. Wer genaueres wissen will hier ein Artikel aus dem besagtem Jahr:
„Bei CovertAction Quarterly kann man nähere Hinweise zum System und zur Arbeitsweise des ECHELON-Systems (siehe auch die Newstickermeldung vom 9.1.) finden, dass den Geheimdiensten von fünf Ländern – USA, Großbritannien, Australien, Kanada und Neuseeland – erlaubt, weltweit die meisten Telefongespräche, E-Mails, Fax- und Telefaxsendungen abzufangen und automatisch über das Programm ‚Dictionary‘ nach bestimmten Begriffen zu durchforschen. (…) Abgehört wird jede Kommunikation, die über die internationalen Telekommunikationssatelliten (Intelsats) und einige weitere Satelliten geht, aber auch Informationen, die durch die auf dem Meeresboden verlegten Kabel fließen, können belauscht werden.“
Quelle: http://www.heise.de/tp/r4/artikel/1/1403/1.html
Natürlich werden die Überwachungs- und Repressionsorgane diese Technik seit 1998 weiterhin präzisiert und optimiert haben. Mensch kann damit rechnen, dass jede E-Mail durchsucht und der gesamte E-Mailverkehr von staatlicher Seite überwacht wird. Aber auch für politische Gegner*innen ist es bei weitem nicht unmöglich Mails mitzulesen. Rein technisch ist das Überwachen eines E-Mail-Kontos sehr einfach und mit geringen Kosten verbunden.

Gegenmaßnahmen

Um dies zu verhindern, kann mensch die Nachrichten verschlüsseln und signieren. Dabei wird der „Betreff“, also die Überschrift, die mensch einer Mail gibt, um dem/ der EmpfängerIn einen Anhaltspunkt über den Inhalt der E-Mail zu geben, nicht verschlüsselt. Also sollte mensch nichts in den „Betreff“ schreiben, was einen Hinweis auf den Inhalt der E-Mail gibt. Die Verschlüsselung führt nun dazu, dass niemand außer dem/ der EmpfängerIn den Inhalt der Nachricht lesen kann (Zumindest ist der Aufwand sehr hoch, aber mit sehr viel Aufwand und äußerst viel Zeit ist jede Verschlüsselung entschlüsselbar, im Allgemeinen ist das relativ unwahrscheinlich). Das Signieren dient dazu, sicher zu stellen, dass die Nachricht nicht verändert wurde und von dem Absender ist, der angeben ist. Es ist auch möglich Nachrichten nur zu signieren. Dann kann jeder die Nachricht lesen, aber Veränderungen am Text können festgestellt werden.

Verschlüsselung mit PGP und GnuPGP

Bei der Verschlüsselung mit PGP / GnuPG wird ein asymmetrisches Verfahren eingesetzt, das bedeutet, dass für das Verschlüsseln und das Entschlüsseln ein unterschiedlicher Schlüssel verwendet wird. Aus diesem Grund erzeugt mensch sich nach der Installation der Software ein Schlüsselpaar, das aus einem privaten und einem öffentlichen Schlüssel (beides Dateien) besteht. Den öffentlichen Schlüssel muss mensch an alle Leute weitergeben, die einem verschlüsselte Nachrichten zusenden wollen. Mensch kann also sobald mensch den öffentlichen Schlüssel besitzt, dem/ der BesitzerIn des privaten Schlüssels verschlüsselte Nachrichten schicken. Der/ die EmpfängerIn kann diese Nachricht mit seinem/ ihren privaten Schlüssel entschlüsseln. Wenn beide Kommunikationspartner*innen den öffentlichen Schlüssel der jeweils anderen Person besitzen ist eine komplett verschlüsselte Kommunikation möglich.
Eine Mail kann mit dem persönlichen Schlüssel des Versenders / der Versenderin signiert werden. Der/die EmpfägerIn stellt dann durch den öffentlichen Schlüssel des/der VersenderIn fest, ob die Mail verändert wurde. Eine Signierung bietet keinerlei Schutz vor einem Mitlesen von E-Mails sonder zeigt nur ob etwas am Inhalt verändert wurde. Einen effektiven Schutz vor Mitleser*innen bietet nur die Verschlüsselung.

Anleitungen:

Eine Anleitung zur Installation von GnuPG findet sich z.B. hier
Eine Anleitung für die Verwendung von GnuPG in Thunderbird (E-Mail-Programme) unter Windows findet sich z.B. hier
Es ist wesentlich komfortabler E-Mail-Verschlüsselung in einem Mailprogramm zu verwenden. Da sich durch die genannten Mailprogramme (Thunderbird & Seamonkey) zudem auch noch viel Zeit sparen lässt, weil z.B. Mails automatisch abgerufen und in Ordner einsortiert werden können, sind die kostenlos nutzbaren Programme nur zu empfehlen. Viele weitere Sicherheitseinstellungen lassen sich hier zudem leichter und komfortabler vornehmen als beim Abrufen der Mails über die Homepage des Mailanbieters.

Schwachstellen der Verschlüsselung

Natürlich haben auch diese Verschlüsslungen Schwachstellen. Es gibt einen Zeitpunkt bei dem definitiv die komplette Verschlüsselung gefährdet ist und das ist die Übertragung des ersten öffentlichen Schlüssels. Da die Mail mit dem Schlüssel noch für andere lesbar ist, kann diese auch abgefangen werden. Es kann sich also eine dritte Person einklinken, die dann an dem/ der KommunikationspartnerIn wiederum einen eigenen Schlüssel schickt. So kann sich gänzlich unbemerkt von den beiden Kommunikationspartner*innen eine weitere Person dazwischen geschaltet haben, die die Mails einfach nur durchreicht. Darum ist es wichtig, dass der erste öffentliche Schlüssel auf einem sicheren Weg weitergegeben wird. Das kann durch die Übergabe eines Speichermediums (USB-Stick, Diskette, CD…), das den öffentlichen Schlüssel enthält, erfolgen. Nachteil hierbei ist, dass ein Treffen stattfinden muss, was teilweise sehr schwierig ist. Ein weiterer Weg ist die Übertragung des Schlüssels über einen bereits verschlüsselten Kommunikationsweg. Das kann beispielsweise so funktionieren: Anna möchte gerne mit Tim verschlüsselte E-Mails schreiben, da Tim aber aus einer anderen Stadt kommt ist ein Treffen nicht möglich. Aber Anna hat bereits eine verschlüsselte Mailverbindung zu Ali der wiederum den öffentlichen Schlüssel von Tim besitzt. Über diese bereits verschlüsselte Verbindung kann der öffentliche Schlüssel von Tim sicher übertragen werden. Anna schreibt dann einfach eine Mail an Tim, an die sie ihren öffentlichen Schlüssel anhängt und die mit Tims öffentlichen Schlüssel verschlüsselt wird. Und schon können auch Anna und Tim sicher miteinander kommunizieren.
Der private Schlüssel sollte immer mit einem Passwort versehen sein, da er sonst, falls er in falsche

Hände gelangt, sehr leicht missbraucht werden kann. Jeder der euren privaten Schlüssel besitzt kann sämtliche für diesen Schlüssel verschlüsselten Mails entschlüsseln und lesen. Falls ihr den Schlüssel zusätzlich mit einem Passwort gesichert habt, muss das auch noch bekannt sein, damit euer Schlüssel missbraucht werden kann. Also nie einen Schlüssel ohne Passwort erstellen.
Das Passwort selbst sollte möglichst beliebig sein, Groß- und Kleinschreibung sowie Sonderzeichen enthalten. Passwörter die beispielsweise in Wörterbüchern stehen werden schnell geknackt, dass gestaltet sich bei willkürlich zusammengestellten Zeichensätzen schon schwieriger. Um euch einen Überblick darüber zu geben was gute und schlechte Passwörter sind, haben wir ein paar Positiv- und Negativbeispiele zusammengestellt. Verwendet aber keinesfalls unsere Beispielpasswörter.

Ganz schlechte Passwörter sehen in etwa so aus:

- alletierefrei
- vegan
- polizeigewalt
- rebelle

Und hier ein paar Beispiele für gute Passwörter:

- dü?&9Uyp
- !cd39z6G7(<+
- /?%§mdcoDESCE&()/

Bei einem korrekt zusammengestellten Passwort sollten 12 Zeichen ausreichen. Je mehr ihr verwendet desto sicherer wird das Ganze natürlich. Bei zu ausgefallenen Sonderzeichen kann es auch passieren, dass diese auf manchen Tastaturen fehlen, was aber unwahrscheinlich ist.
Viele E-Mail-Programme, Webbrowser oder ähnliches bieten die Möglichkeit Passwörter zu speichern. Diese gespeicherten Passwörter sind auslesbar. Zwar ist ein gespeichertes Passwort besser als gar keins, dennoch stellt es ein Sicherheitsrisiko dar. Der einzig sichere Speicher ist euer eigener Kopf. Also Passwörter am besten auswendig lernen. Nach 10-mal eintippen könnt ihr es eh schon ;-)

Andere mehr oder weniger schlimme Sachen bei E-Mails

Kabellose Netzwerke (W-LAN):

Grundsätzlich ist zu sagen, dass ein kabelloses Netzwerk immer verschlüsselt sein sollte, da ansonsten Dritte die Möglichkeit nutzen könnten über euren Zugang, ins Internet zu gelangen. Problematisch hierbei ist, dass nicht der/ die SurferIn selbst sondern die Person auf deren Namen der Internetanschluss registriert ist für das verantwortlich ist was von diesem Anschluss aus im Internet gemacht wird und dass kann teuer werden wenn beispielsweise Musik oder ähnliches illegal heruntergeladen wird. Ganz von der Haftung abgesehen, stellt ein unverschlüsseltes, kabelloses Netzwerk auch ein Sicherheitsrisiko für die sich in diesem Netzwerk befindenden Rechner dar. Dritte können sich einklinken und die übertragenen Daten mitlesen oder sogar auf alle sich auf dem Rechner befindenden Daten zugreifen. Dadurch können nicht nur E-Mails mitgelesen werden.
Bei einem verschlüsselten WLAN ist dieses Einklinken nur Personen möglich, denen der Schlüssel bekannt ist. Was aber auch problematisch werden kann, da beispielsweise in Hotels alle Personen die das WLAN nutzen auch über den Schlüssel verfügen. Daher stellen auch verschlüsselte Netzwerke zu denen Personen Zugriff haben, die einem nicht vertraut sind, ein Sicherheitsrisiko dar.

Beim Abrufen von E-Mails:

Hierbei sollte darauf geachtet werden, dass die Verbindung zum Mailanbieter verschlüsselt ist, da ansonsten der Nutzername, das dazugehörige Passwort und die Nachrichten im Klartext übertragen werden. Dies ist vor allem bei WLANs problematisch, da jedeR, der/ die sich im diesem WLAN befindet, diese Daten mitlesen und aufzeichnen kann. Bei E-Mail-Programmen kann mensch die verschlüsselte Verbindung (in der Regel) in den Einstellungen für die Benutzerkonten festlegen. Dort steht normalerweise SSL (Secure Sockets Layer) oder TLS (Transport Layer Security) zur Verfügung. Nicht alle Anbieter von E-Mail-Adressen bieten beide Möglichkeiten an, aber normalerweise wird mindestens eine dieser Optionen angeboten. Mensch kann das einfach einstellen und ausprobieren, ob eine Verbindung zu Stande kommt, oder ob mensch eine Fehlermeldung erhält. Diese Einstellung kann mensch in der Regel für das Senden und Empfangen einzeln einstellen, also muss mensch dies an zwei Stellen einrichten. Bei der Abfrage der Mails über eine „Web-Oberfläche“, also in einem Browser (z.B. Mozilla Firefox, Internet Explorer, …), wird in der Regel nur das Anmelden über eine verschlüsselte Verbindung erledigt und die Nachrichten werden unverschlüsselt übertragen. Dies ist bei kostenlosen E-Mail-Adressen üblich und eine verschlüsselte Übertragung ist bei den Anbietern als kostenpflichtiger Dienst verfügbar. Meistens ist eine komplett verschlüsselte und zudem kostenlose Übertragung also nur per Mailprogramm erreichbar.

E-Mails an fremden Rechnern:

Allgemein gilt E-Mails an fremden Rechnern zu kontrollieren ist ein Sicherheitsrisiko. Das gilt besonders für Computer an Arbeitsstätten, „Bildungs“-einrichtungen, Internetcafés oder Vergleichbarem. Oftmals laufen Aufzeichnung- und Überwachungsprogramme im Hintergrund mit, der komplette Datenverkehr kann überwacht, jede Tasteneingabe und jeder Mausklick registriert werden und dass ganz ohne dass das für den/die NutzerIn bemerkbar wäre. Ein Passwort zu einem E-Mailkonto, das an solch einem Rechner eingetippt wurde, findet sich eindeutig lesbar in den Protokollen der Programme wieder, genauso wie eingehende und ausgehende E-Mails. Es ist sogar möglich live dabei zuzusehen, was sich denn auf dem Bildschirm so alles abspielt. Bei nicht vertrauenswürdigen Rechnern gilt: Macht nur das was euch unbedenklich erscheint. Es ist kein Problem sich nach Backrezepten zu erkundigen aber sobald besagte Rezepte per E-Mail verschickt werden entstehen Sicherheitsrisiken. Gleiches gilt überall wo Passwörter eingegeben werden müssen.

Mailprogramm interne Suchfunktionen:

Teilweise bieten Mail-Programme die Möglichkeit innerhalb des Programms die Nachrichten zu durchsuchen. Dabei erfolgt üblicherweise eine Indexierung der Nachrichten, d.h. zumindest Teile der Nachrichten werden in einer Index-Datei abgespeichert, damit schneller Suchergebnisse geliefert werden können. Dadurch könnte es vorkommen, dass bei verschlüsselten Nachrichten die vom Nutzer entschlüsselte Variante in der Index-Datei lesbar wird. Ob das in der Realität zutrifft, ist schwierig zu beurteilen, da mensch sich genau ansehen müsste, wir die Programme wirklich arbeiten, aber wenn mensch ganz sicher gehen will, besteht die Möglichkeit das Indexieren der Nachrichten in den Einstellungen zu deaktivieren.

HTML-Mails:

HTML ist eine Sprache mit der aufwändigere grafische Darstellungen möglich sind. HTML kann auch in E-Mails eingesetzt werden damit diese schöner gestaltet werden können. Allgemein wird von der Darstellung von HTML-Mails abgeraten, da es immer wieder vorkommt, dass durch Fehler, die

durch das Darstellen solcher Nachrichten entstehen, Sicherheitslücken in den Programmen ausgenutzt werden können. Die Darstellung von HTML-Mails kann mensch in der Regel in den Optionen für die Darstellung von Nachrichten abschalten. Bei HTML-Mails handelt es sich oft um sogenannten Spam. Für die normale Kommunikation zwischen Personen sind keine HTML-Mails notwendig.

Viren:

werden in der Regel als Anhang verschickt. Oft werden auch Absenderadressen von Freunden oder Bekannten verwendet, da sich Viren auch selbst per E-Mail verschicken können. Sobald sie einen Computer infiziert haben, verschicken sie sich selbst an alle gespeicherten Mailadressen weiter. Bei Viren handelt es sich um Programme, die meistens an der Endung .exe oder .com erkennbar sind. Achtung nicht auf die angezeigten Icons verlassen, da diese bei Viren meist nicht stimmig sind. Falls du also eine ausführende Datei von einem Freund oder Bekannten erhältst, obwohl du sie nicht von ihm erwartest solltest du diese in keinem Fall öffnen, sondern zuvor kurz mit der jeweiligen Person Rücksprache halten ob er/ sie dir diese auch zugesandt hat. Es kann sich lohnen.

Spam:

ist in der Regel eigentlich harmlos, da es sich nur um Werbung handelt. Auch diese treten relativ häufig in Form von HTML-Mails auf. Viele Mailanbieter haben einen Spam-Filter, der Werbemails aus dem normalen Mailverkehr herausfiltert um den Nutzer nicht durch Werbung unnötig zu belasten. Falls E-Mails verschwinden, kann es sich lohnen den Spamfilter zu kontrollieren ob die Nachrichten hier nicht durchgelassen werden.

Hoaxes:

sind mit Kettenbriefen vergleichbar. Es ist immer ein Aufruf enthalten die Mail an andere weiter zu versenden. Hoaxes sollten getrost ignoriert werden. Oft handelt es sich dabei um Warnungen vor angeblichen Viren oder Ähnlichem. Einen Nutzwert haben Hoaxes jedoch nicht. Eine Sammlung von Hoaxes findet ihr unter http://hoax-info.tubit.tu-berlin.de/hoax/

Nachladen von Bildern

Ein weiterer Punkt ist das Nachladen von Bildern aus E-Mails. Dabei werden Bilder in E-Mails eingebettet, die nicht in der E-Mail mitgeschickt werden, sondern aus dem Internet nachgeladen werden. Immer wenn das Bild nachgeladen wird, kann z.B. gesehen werden wann die E-Mail gelesen wird. Verhindern lässt sich dieses Nachladen meist in den Einstellungen oder Optionen eures Mailprogramms oder der Benutzeroberfläche eures Mailanbieters.

Eindeutige Verlinkungen:

In dem Zusammenhang passt auch, dass es üblich ist, eindeutige Links zu verwenden, die in Nachrichten (z.B. Newsletter) angegeben werden. Das heißt der Link zu weiterführenden Informationen existiert so nur einmal. Wenn nun jemand auf diesen Link klickt, kann daraus geschlossen werden, dass zum einen diese Person mit der zugehörigen E-Mailadresse überhaupt existiert und diese auch für sich nutzt, und zum anderen, dass sich die Person für ein bestimmtes Thema interessiert. Mit den gewonnen Informationen werden eventuell entsprechende Werbemaßnahmen individuell angepasst. So kann immer zum jeweiligen Zeitpunkt festgestellt werden, ob die Nachrichten gelesen werden und eine weitere Einschätzung der betroffenen Person erfolgen. Falls ihr Links von Leuten bekommt, denen ihr nicht vertraut / die ihr nicht kennt, empfiehlt es sich die entsprechende Seite über eine Suchmaschine aufzusuchen.

Phishing

Mit Phishing wird versucht Bankdaten zu stehlen. Dabei wird in der Nachricht meist angegeben, dass es nötig wäre, die Bankdaten aufgrund eines Problems zu bestätigen, um weiterhin Online-Banking betreiben zu können. Innerhalb dieser Nachricht führt ein Link zu einer Webseite, die der echten Webseite des Onlinebankings absolut oder nahezu identisch aussieht, auf der die geforderten Daten dann eingegeben werden sollen. Auf E-Mails die einem dazu auffordern Bankdaten anzugeben sollte mensch nicht reagieren. Keine seriöse Bank würde derlei Sachen über eine E-Mail klären.

Das wichtigste zum Schluss:

Zweck ist es nur die uns bekannten Probleme für politisch aktive Menschen im Zusammenhang mit E-Mails aufzuzeigen. Es sollte jedeR selbst entscheiden in wie weit er/ sie Gegenmaßnahmen ergreift. Wir wollen aber dazu anregen nicht all zu leichtfertig mit dem Thema umzugehen. Gerade Aktivist*innen werden oftmals stärker überwacht als politisch nicht Engagierte und dass kann teilweise über Jahre hinweg geschehen ohne dass es bemerkt wird. Wer es also den Gegenspielern all zu leicht macht einen Einblick in unsere Strukturen zu bekommen, der gefährdet nicht nur sich selbst sondern ganz konkret alle Menschen mit denen kommuniziert wurde. Im schlimmsten Fall wird es sogar ermöglicht ganze Politgruppen zu zerschlagen und die Arbeit von Jahren zunichte zu machen.