Informationstechnologie und Sicherheit

Inhaltsverzeichnis

1. Grundsätzliches

1.1. IT im politischen Alltag

Die Informationstechnologie hat den politischen Alltag grundlegend-verändert, Sitzungen werden über Mail oder SMS abgemacht, Informationen holen wir uns schnell auf einer WebSite usw. Ob PC, Internet oder Telefonie; Jedes Instrument bietet Möglichkeiten die im revolutionären Widerstand genutzt werden können und sollen. Allerdings sollte dabei die Sicherheit nicht vergessen werden jedoch auch nicht alles lähmen. Wir werden unsere Arbeitsweise mit diesen Hilfsmitteln wieder und wieder der aktuellen Situation und der Konterrevolution anpassen müssen.
Die Möglichkeiten die uns ein Instrument gibt sowie die objektive Situation müssen den Umgang mit diesem Instrument bestimmen. Wir müssen unsere Kentnisse über die objektiven Möglichkeiten der Konterrevolution verfeinern um einen geeigneten Umgang mit den uns zur Verfügung stehenen Hilfsmitteln zu finden.

1.2. Verhältnismässigkeit

Beim Umgang mit Computern, Handys usw gilt wie überall, 100%ige Sicherheit gibt es nicht. Ausser vielleicht der gesammte PC wird nach jeder Arbeit vollkommen zerstört...
Daher gilt es einen Weg zu finden zwischen der absoluten Sicherheit und unserer Handlungsfähigkeit. Es gibt dafür keine Richtlinien, die Vielfälltigkeit der Situationen der verschiede-nen Gruppen und den verschiedenen Ländern verhindert diese. Es gilt immer eine Risikoanalyse zu machen und auf diese mit entsprechenden Massnahmen zu reagieren.
Beispiel: Das Internet ist zur Zeit ein mächtiges Instrument für unsere Arbeit, ist jedoch praktisch durch uns nicht kontrollierbar. Daher müssen wir alles unternehmen dass Informationen auch die,und nur die, erreichen die sie erreichen soll. Allerdings dürfen wir nicht zulassen dass aus Angst und teilweise aus Unwissenheit das Internet nicht mehr eingesetzt wird, dafür ist es als Medium zu wertvoll.

Daher: Risikoanalyse, Bestimmung was darf z.B. uber das Netz oder auf eine Festplatte und was nicht, Gegenmassnahmen

1.3. Risikoanalyse

Eine Risikoanalyse handelt immer von der objektiven Situation. Subjektive Ängste oder subjektive offensive Tendenzen haben darin nichts verloren. Eine Risikoanalyse sollte von SpezialistInnen unter Einbezug von NichtspezialistInnen erstellt werden. SpezialistInnen nicht im Sinne von hochqualifizierten Technikern sondern von GenossInnen die eine objektive Einschätzung der Situation machen können unter Einbezug der Computer/Internet/Telefon/-SpezialistInnen. Ein Beispiel wie ein Risikoanalyse erstellt werden sollte:

- Intensität des Klassenkampfes
- Stärke und Wichtigkeit unserer Struktur
- Interventionen und Interventionstypen unserer Struktur
- Wer hat welche Kentnisse und Möglichkeiten
- Technisches Wissen aller GenossInnen
- Objektive Möglichkeiten der Konterrevolution
- Wie gut sind unsere SpezialistInnen ausgebildet
- Wie schnell können wir auf eine Bedrohung reagieren

Diese Aufzählung ist bei weitem nicht vollständig soll aber zeigen in welche Richtung eine solche Analyse geht. Aus der Analyse dieser Fragen ergibt sich eine Einschätzung über die Bedrohung gegen unsere Struktur und damit die Anforderungen an den Schutz unserer Struktur. Dabei darf die Grundanforderung des Schutzes nicht vergessen werden. Ein solcher Schutz bedingt eine gewisse Schulung aller GenossInnen...

1.4. Passwörter

Der Wahl des Passwortes kommt eine spezielle Bedeutung zu. Einfache Passwörter sind schnell herauszufinden, zu komplizierte

Passwörter die man sich nicht merken kann und unter der Tastatur aufschreiben muss bringen auch nichts. Unter einfache Passwörter gehen auch ganze Zitate aus Büchern usw.
Grundsätzlich: Passwörter sollten mindestens aus 25 Zeichen bestehen, aus Buchstaben gross und klein, Zahlen und Sonderzeichen. Z.B: «gEsellschaftliches_bEwusstsein!5e»
Sogenannte Eselsbrücken können helfen ein Passwort zu merken z.B. 5e 5 mal ein e im Text.

1.5. Schulung

Schulung ist ein zentrales Moment einer Struktur, sei dies nun philosophischer, ökonomischer oder eben technischer Natur. Sicherheit durch Schulung. Viele GenossInnen sind sich der Gefahren aber auch der Chancen der neuen Technik nicht bewusst. Daher ist es unerlässlich dass gewisse Schulungen durchgeführt werden. Unwissenheit kann die Sicherheit einer Struktur beeinträchtigen, gefährden, genauso wie sie die Aktivitäten einer Struktur lähmen kann.
Wichtig ist dabei der Entscheid der Organisation welche Anforderungen an GenossInnen gestellt werden die in bestimmten Strukturen tätig sind. An die ZK-Kommunikation werden andere Anforderungen gestellt als an die Kommunikation über den Zeitungsverkaufstermin. Diese Anforderungen sind klar festzulegen. Die Auswahl der zu schulenden Themen sind von der Risikoanalyse abhängig. Allerdings gibt es Grundwissendas alle haben sollten, z.B:

-Wie verschlüssle ich meine Daten auf der Festplatte
-Wie verschlüssle ich meine Mails
-Wie Lösche ich Dateien richtig
-Wie anonymisiere ich meine Internetbesuche

Technische Schulungen sind sehr Zeitintensiv und kompliziert zu organisieren da die Ungleichzeitigkeit bei den verschiedenen GenossInnensehr stark ausgeprägt ist. Einige gebrauchen noch

Schreibmaschinen anderen haben alle möglichen technischen Spielereien zur Verfügung. Das Ziel einer Schulung muss sein dass alle GenossInnen die Problematik und die Lösung zum Problem kennen und damit umgehen können.

2. Hausanschluss und Handy

2.1. Hausanschlüsse

Das Risiko bei Hausanschlüssen dürfte heute weitgehend bekannt sein. Desshalb werden wir nicht mehr gross darauf eingehen. In kürze die wichtigsten Punkte...

Telefonieren

Beim Telefonieren ist immer davon auszugehen dass die Kräfte der Konterrevolution mithören können. Sei dies nun ein herkömmlicher analoger Anschluss oder ISDN. Ebenfalls ist es mit einer speziellen Schaltung des Telefons möglich einen Raum, mit dem im Telefon eingebauten Mikrofon, abzuhören.

2.1.1. Fax

Der Inhalt eines Faxes ist von den oben genannten Kräften ebenfalls sehr einfach einsehbar. Auch hier spielt es keine Rolle ob es nun um ein analoges oder ein ISDN Faxgerät handelt.

2.1. 2. Analoges oder ISDN Modem

Es hat versuche gegeben mit dem Lautsprecher im Modem, der diese schönen quietschenden Geräusche von sich gibt sobald man sich einwählt, einen Raum abzuhören. Diese Versuche waren teilweise Erfolgreich.

Als Fazit bleibt nur eines; Telefon und Fax sind nicht sicher und können von uns auch nicht ausreichend gesichert werden. Bei Sitzungen in einem Raum in dem ein Telfon, Fax oder Modem steht, Stecker ausziehen.

2.2 Handys

2.3 Abhören

Das Handy kann genau wie die herkömmlichen Hausanschlüsse abgehört werden. Das gleiche gilt für SMS und MMS. Diese Daten gehen über den Dienstanbieter und können dort bequem gespeichert oder live überwacht werden.

2.4. Bewegungsprofil

Neu beim Handy ist die Möglichkeit die Bewegungen des Handys zu überwachen. In Gebieten mit vielen Zellen, wie in Städten, lassen sich die Bewegung des Handys und damit seines Trägers sehr genau überwachen.

2.4.1. Zellenhüpfen

Ein Handy meldet sich sobald eine Kommunikation aufgebaut wird, Anruf oder SMS usw, an der Zelle die die beste Leistung abgibt an. Eine Zelle ist eine Antenne die die Daten des Handys ,z.B. bei einem Gespräch an den Dienstanbieter weiterleitet. Der Dienstanbieter sieht also in welcher Zelle sich welches Handy befindet. Sobald wir uns aus dem Gebiet der einen Zelle bewegen und eine Kommunikation besteht meldet sich das Handy an der nachsten Zelle an und wir hinterlassen damit eine deutliche Spur wohin wir uns bewegen. Daher bringt es nichts sich mit dem Handy angeschaltet an eine Sitzung zu bewegen und es dort auszuschalten. Abhören ist dann zwar nicht mehr möglich, wenn sich aber sämtliche überwachten Handys zu einem bestimmten Zeitpunkt an einem Ort treffen ist dies schon sehr aussagekräftig...

2.5. SMS Ping

Falls keine Kommunikation besteht meldet sich das Handy ca: alle 90 Minuten bei einer Zelle an. Will jemand nun schneller wissen wo sich das Handy befindet kommt der SMS Ping zum Einsatz. Der SMS

Ping ist eine Technik die angewandt wird um den Standort eines Handys abzufragen. Der Dienstanbieter schickt ein Signal ans Handy als würde ein SMS ankommen. Durch die aufgebaute Kommunikation lässt sich wiederum feststellen an welcher Zelle das Handy angemeldet ist.

2.6. IMEI Nr. usw

Ein Handy kommuniziert mit verschiedenen Nummern mit dem Dienstanbieter und den Zellen. Die Telefonnummer ist die allgemein bekannte. Allerdings hat jedes Handy noch eine eigene, sogenannte, IMEI Nummer. Anhand dieser Nummer ist ein Handy immer identifizierbar ,auch wenn die Simkarte gewechselt werden sollte. Daher ist es nicht sinnvoll einfach die Simkarte eines Handys zu wechseln um wieder anonym zu telefonieren.

2.7. Sicher ist Sicher

Um sicher zu gehen dass keine Signale mehr gesendet werden ist es ratsam den Aku aus dem Handy zu nehmen. Damit ist das Handy einerseits sicher ausgeschaltet und andererseits können auch technische Veränderungen die vorgenommen wurden ohne Spannung nicht mehr funktionieren.
Auch hier gilt allerdings vorsicht; Verschiedene Hersteller haben angekündigt Handys auf den Markt zu bringen die mit einem Not-Aku für eine Zeitlang funktionieren. Für Notrufe etc.

2.8. IMSI Nummer finden

Da die IMSI Nummer eines Handys nicht einfach so bekannt ist gibt es zwei Möglichkeiten diese herauszufinden. Die erste ist die einfache; Kontrolle und Nummer abschreiben. Wenn die Bullen dein Handy bei einer Kontrolle auseinandernehmen und etwas abschreiben handelt es sich bestimmt um diese Nummer.
Die zweite ist etwas komplizierter. Es gibt ein Gerät, den IMSI Catcher, das simuliert eine Zelle des Dienstanbieters. So meldet sich dein Handy nicht etwa an der nächsten offiziellen Zelle an sondern

an diesem IMSI Catcher. So könne die Bullen rausfinden mit welchem Handy du telefonierst und kennen die IMSI sowie die IMEI Nummer.

3. Computer und Zubehör

3.1. Löschen

Löschen ist nicht Vernichten. Die Funktion des Löschens auf einem PC lässt sich mit einem Papierkorb vergleichen. Das Dokument ist aus dem Weg und wir sehen es nicht mehr auf den ersten Blick. Allerdings lässt sich ein so gelöschtes Dokument mit leichtigkeit wieder herstellen und verwerten. DerVergleich zwischen einem gelöschten Dokument auf einem PC und einem Dokument im Papierkorb hinkt rein technisch gesehen jedoch kann man die Problematik damit gut veranschaulichen.
Im Gegensatz zum Papierkorb lässt sich ein Dokument das durch einen Aktenvernichter zerstört wurde nur sehr schwer wieder herstellen. Auf dem PC sieht die Sache noch etwas anders aus; Das Dokument wird nicht zerstört sondern überschrieben und dies mehrere male, in den meisten fällen 35 mal. Damit ist die Wiederherstellung des Dokuments ausgeschlossen.
Zum löschen gehört auch das Uberschreiben des leeren Speicherplatzes auf der Festplatte. Meistens wird von Dokumenten die angefertigt werden Sicherheitskopien automatisch durch das System angelegt. Diese sind nicht zu sehen und werden oft automatisch wieder gelöscht.Um sicher zu gehen dass diese Dokumente auch wirklich überschrieben werden, sollte der leere Diskplatz

überschrieben werden.
Im sogenannten freien Speicher, also der Diskplatz der uns noch zur Verfügung steht, befinden sich oft solche, vom Betriebssystem selbst, gelöschten Dateien. Gelöscht jedoch nicht vernichtet.

Wichtig ist auch noch das Filesystem. Auf einem Windows sollte auf keinen Fall NTFS sondern FAT32 genommen werden. Auf einem Linux-System Ext2 nicht Ext3 oder ReiserFS. Allgemein gesagt: Kein Journaling-Filesystem verwenden. (Dies ist in den Beschreibungen zu den einzelnen Filesystems zu entnehmen).

3.1.1. Betriebssysteme

Windows

Eraser

Mit Eraser lassen sich Dateien und Verzeichnisse sicher löschen und der freie Speicherplatz überschreiben. Es ist möglich dies zu einem bestimmten Zeitpunkt durchführen zu lassen, z.B. jeden Tag um 23 Uhr. Mit den Defaulteinstellungen werden Daten, Verzeichnisse und der freie Speicherplatz 35 mal überschri:q eben.
URL:http://sourceforge.net/projects/eraser

Linux/Unix/MacOS X

Shred

Damit lassen sich Datei überschreiben und löschen. Bei jedem Linux dabei, gehört zur Standartinstallation.

Secure delete

Programme zum sicher Löschen von Dateien,Verzeichnissen, des Memory und des Swap. Ausserdem lässt sich damit auch der leere Speicherplatz füllen. Diese Security Suite ist sehr zu empfehlen.

3.2. HD Verschlüsselung

Die Verschlüsselung der Festplatte oder eines Teils einer Festplatte (kann auch ein USB-Stick sein) ist sehr wichtig. Was nützt es uns

alle Daten verschlüsselt zu verschicken, nicht herumliegen zu lassen und Ausdrucke zu verbrennen, wenn die Repressionskräfte bei einer Hausdurchsuchung den ganzen Computer mitnehmen und darauf alles Klartext zu lesen ist.
Dazu gibt es verschieden Tools und Werkzeuge:

Windows
DriveCrypt
Damit lassen sich ebenfalls Container anlegen in die um Daten ablegen zu können.
Beide Programme sind Kommerziell und müssten gekauft werden wenn man sie nicht irgendwo downloaden will.

Linux
Loop AES, Crypt Loop
Damit lassen sich ebenfalls Container anlegen und verschlüsseln oder es lässt sich auch gleich die ganze Festplatte verschlüsseln, sodass zum Starten des Computers schon ein Passwort gebraucht wird.

3.3. WEB Verkehr verschlüsseln

Wenn wir auf eine Webseite zugreiffen oder etwas Downloaden lässt sich dies mit sehr wenig Aufwand mitverfolgen. Wir hinterlassen also eine schöne Spur was uns heute interessiert hat.
Wir sind von unserer Online Tageszeitung zur Homepage der RHI-SRI und dann zur Homepage unserer Organisation gesurft und haben uns vorallem für Erklärungen interessiert.
Solche Spuren können allerdings versteckt werden. Dafür brauchen wir wiederum ein Tool; zur Zeit sind dies JAP und TOR. Damit wird unsere Spur mit der Spur von anderen SurferInnen vermischt und ist nicht mehr nachvollziehbar.
TOR sowie JAP gibt es für alle gängigen Betriebssysteme und lässt sich sehr einfach anwenden.

3.4. Mailverschlüsselung

Elektronische Post ist zu vergleichen mit einer Postkarte. Bekommt jemand die Postkart in die Finger braucht er nur noch den Text zu lesen. Daher sollten Mails verschlüsselt werden. PGP oder GnuPG sind die Werkzeuge unserer Wahl. Die Verschlüsselung basiert auf einem sogenannten Publickey verfahren. Jede Person/Organisation hat einen privaten und einen offentliche Schlüssel. Der öffentliche Schlüssel wird an alle verschickt oder noch besser abgegeben mit denen wir kommunizieren wollen.
Der private Schlüssel darf nicht in falsche Hände geraten. Dieser ist der Garant für die Sicherheit der Verschlüsselung.

Falls der Schlüssel verschickt wird sollte nach dem Importieren des Schlüssels unbedingt der Fingerprint telefonisch oder bei einem Treffen überprüft werden.
Der Fingerprint ist ein Merkmal, eine Reihenfolge von Zahlen und Buchstaben die einen Schlüssel verifzirt und die nicht gefälscht werden kann.

3.5. LiveSystem

Livesysteme sind besonders geeignet für Arbeiten die nicht auf einem PC gespeichert werden müssen, z.B. Erklärungen. Diese funktionieren im Prinzip sehr einfach. Sie werden von einer CD aus gestartet und es kann ein Text geschrieben werden oder was auch immer. Danach wird dieser Ausgedruckt oder auf einem USB-Stick gespeichert und der PC wieder abgeschaltet. Die Daten sind weg, da die Festplatte nicht eingebunden wird in den ganzen Prozess. Natürlich lässt sich auf einem solchen System auch ein USB-Key oder eine Diskette verwenden um Daten zu speichern und anderswo abzulegen.
Achtung: Ein solches System ist nicht geeignet um sich Anonym im Internet zu bewegen.