De l’espionnage électronique politicier et des moyens de s’en protéger

Sommaire

Chapitre 1. Principes

1. 1. La technologie de l'information dans le quotidien politique

Le quotidien politique a été transformé considérablement par la technologie d'information. Des dates de réunions sont convenues par mail ou par SMS, des informations sont rapidement recherchées dans des sites d'Internet etc. qu'il s'agisse du PC, de l'Internet ou de la téléphonie mobile, chaque outil procure des possibilités qui peuvent et doivent être utilisées dans la résistance révolutionnaire. Toutefois, la sécurité ne doit pas être oubliée. Elle ne doit pas paralyser non plus. Nous allons devoir nous adapter à la situation actuelle et à la contre-révolution par notre mode de travail en utilisant ces moyens techniques.

C'est à la fois la possibilité donné par un outil et la situation objective qui doivent diriger l'usage de cet outil. Nous devons donc perfectionner nos connaissances sur les possibilités objectives de la contre-révolution, pour que nous trouvons un mode d'emploi approprié des outils à notre disposition.

1. 2. Proportionnalité

Dans l'utilisation d'ordinateurs, de téléphones portables etc. il va de soi qu'une sécurité à 100% n'existe pas. Ce pourquoi il s'agit de trouver un chemin qui se situe entre la sécurité absolue et notre capacité d'agir. La complexité des situations des différents groupes et des différents pays ne permet pas d'établir des directives générale. Une analyse de risques est donc toujours de mise pour pouvoir réagir par les bonnes mesures.

Exemple : L'Internet est un outil puissant pour notre travail, mais n'est pratiquement pas contrôlable par nous. Ce pourquoi nous devons tout entreprendre pour que des informations n'arrivent que chez le destinataire. De l'autre côté nous devons pas permettre l'abandon de l'Internet par peur ou par ignorance. C'est un média qui a trop de valeur pour qu'on puisse s'en passer.

Par conséquent : Analyse de risque · Jugement de ce qu'on peut envoyer par Internet ou ce qu'on peut enregistrer sur le disque dur et ce qu'on ne peut pas faire · Contre-mesures.

1. 3. Analyse de risque

Dans une analyse de risque, il s'agit toujours d'une situation objective. Il n'y a pas de place pour des dispositions subjectives comme la peur ou les tendances offensives. L'analyse de risque doit être faite par des spécialistes, tout en incluant des non-spécialistes. Nous entendons le terme "spécialistes" non pas dans le sens de techniciens hautement qualifiés, mais bien dans le sens de camarades qui peuvent objectivement juger la situation en ayant recours à des spécialistes de l'informatique, de l'Internet ou de la téléphonie.

Exemple de l'établissement d'une analyse de risque :
· Intensité de la lutte des classes
· Force et importance de notre structure
· Interventions et types d'interventions de notre structure
· Qui a quelles connaissances et possibilités ?
· Connaissances techniques de toutes/tous les camarades
· Possibilités objectives de la contre-révolution
· Dans quelle mesure nos spécialistes sont-elles/ils formé(e)s ?
· Avec quelle rapidité pouvons-nous réagir à une menace ?

Cette énumération est largement incomplète, mais elle montre dans quelle direction peut aller une telle analyse.
L'analyse des réponses à ces questions donne une image de la situation de menace par rapport à notre structure et par là des possibilités de protection de la structure. Il ne faut pas oublier que la protection est une nécessité basique. L'analyse doit également comporter une estimation du " qui peut écouter ou lire un message par quel moyen " ? Les conséquences immédiates se distinguent par rapport à la situation, c'est-à-dire selon que l'espionnage se déroule sur une base de pur service de renseignements ou si des forces de répression sont directement inclues.

1. 4. Les mots de passe

Le choix du mot de passe est très crucial. En effet, des mots de passe trop simples sont identifiés rapidement, tandis qu'il n'est pas facile de retenir un mot de passe compliqué. Il ne sert à rien de choisir un mot de passe compliqué que l'on doit ensuite noter quelque part pour ne pas l'oublier. Par ailleurs, des mots de passe qui sont des citations de livres etc. doivent aussi être considérés comme des mots de passe simples. En principe, les mots de passe doivent comporter 25 signes au minimum, doivent comporter des caractères majuscules et minuscules, ainsi que des chiffres et des caractères spéciaux. Pour retenir le mot de passe, un moyen mnémotechnique peut aider.
Exemple : "*consciEnce_dE_la_sociEté!6e*"
Ici, nous devons par exemple retenir que le texte comporte 6 e, dont les premiers de chaque mot en majuscule.

1. 5. Formation

La formation est un moment central dans une structure, que ce soit de nature philosophique, économique ou technique. L'apprentissage amène la sécurité. Beaucoup de camarades ne sont pas conscients des dangers mais aussi des possibilités des nouvelles techniques. De ce fait, certaines formations sont indispensables. L'ignorance peut nuire à la sécurité d'une structure, tout comme elle peut paralyser les activités d'une structure. Une organisation doit décider ce qu'elle exige des camarades actifs dans une structure définie. Ainsi, les exigences sont différentes qu'il s'agisse d'une communication du Comité central ou d'une communication sur la date de la vente d'un journal. Les exigences sont donc à définir clairement.
Le choix des thèmes à apprendre dépend de l'analyse de risque. Néanmoins il y a des connaissances de base que tous devraient avoir, par exemple :

· Comment chiffrer mes informations sur un disque dur ?
· Comment chiffrer des mails ?
· Comment supprime-je correctement des documents ?
· Comment rendre anonyme ma visite sur Internet ?

Des formations techniques nécessitent beaucoup de temps et sont difficiles à organiser. Ceci est lié au fait que les camarades sont parfois très décalés par rapport aux moyens techniques. Les uns utilisent encore des machines à écrire, tandis que les autres disposent des dernières jouets techniques. Le but d'une formation doit être telle que toutes/tous les camarades connaissent les problèmes éventuelles ainsi que les solutions, qu'ils doivent pouvoir appliquer.

Chapitre 2. Téléphone fixe et téléphone portable

2. 1. Téléphones fixes

On suppose que le risque des téléphones fixes est largement connu aujourd'hui. Ce pourquoi nous voulons nous contenter de les décrire en grandes lignes… Lorsqu'on téléphone, on peut toujours supposer que les forces de la contre-révolution puissent écouter. Qu'il s'agisse d'un raccordement analogique traditionnel ou de l'ISDN. D'ailleurs, il est possible d'espionner une pièce par un microphone qui peut être placé dans le téléphone.

2. 1. 1. Téléfax

Le téléfax est aussi facilement espionnable.

2. 1. 2. Modem analogique ou ISDN

Il y a eu des essais d'écouter une pièce par le moyen d'un microphone dans un modem. Ces essais ont partiellement eu du succès. Nous pouvons en tirer la conclusion que ni le téléphone ni le fax procurent la sécurité, et ils ne peuvent être sécurisés par nous. Il est donc de mise de retirer la prise du téléphone, du fax ou du modem lors d'une réunion.

2. 2. Téléphones portables

2. 3. L'interception

Un téléphone portable peut être intercepté tout comme les télépho-

nes fixes traditionnels. Il en est de même pour les SMS et les MMS. Ces informations passent par la société téléphonique et peuvent y être observées ou enregistrées aisément.

2. 4. Profil de mouvement

Ce qui est nouveau, c'est qu'il est maintenant possible de surveiller la localisation d'un GSM. Dans les endroits avec de nombreuses cellules, par exemple dans les villes, les mouvements d'un GSM peuvent être observés de manière assez exacte.

2. 4. 1. Saut de cellules

Une cellule est une ou plusieurs antennes qui transmettent les informations du téléphone portable, par exemple lors d'une communication, vers la société téléphonique. Par là, la société téléphonique peut voir quel GSM se trouve dans une certaine cellule. Dès qu'une communication s'établit, que ce soit par appel ou par SMS, le téléphone portable se raccorde à l'antenne assurant la meilleure réception. Si nous sommes en mouvement, nous laissons donc une trace et permettons de voir dans quelle direction nous nous dirigeons. Pour cette raison, il est inutile de nous diriger vers une réunion clandestine et d'éteindre notre GSM une fois que nous sommes arrivés. Si votre téléphone portable est surveillé, dès que vous écrivez un SMS, que vous appelez quelqu'un ou que vous recevez un SMS ping (on y reviendra), on peut voir où vous vous trouvez. Même s'il n'est pas possible d'écouter un GSM qui est éteint et qui se trouve à une réunion, il est important de savoir que, si des GSM surveillés se rencontrent dans un même endroit à une même heure, cet endroit ne doit plus être choisi comme lieu de rencontre après.

2. 5. SMS ping

Le SMS ping est une technique qui est utilisée pour localiser un GSM. La société téléphonique envoie un signal au téléphone, assez similaire à un SMS. Par là, une communication est établie qui permet à nouveau d'observer dans quelle cellule se trouve le GSM. Après ce bref moment, la communication est terminée. Le SMS ping

est donc quelque chose par lequel une communication est établie avec le téléphone portable sans que cela puisse se voir sur l'écran du téléphone.

2. 6. N° IMSI etc.

Un téléphone portable communique par différents numéros avec le service téléphonique et les cellules. Nous connaissons les numéros d'appel. Cependant, à côté de ce numéro, chaque téléphone a un numéro. Ce numéro est appelé n°IMSI. Grâce à ce numéro, le téléphone est toujours identifiable, même dans le cas du changement de la carte SIM.

2. 7. Pour être certain...

Pour être certain qu'un téléphone portable n'émet plus de signaux, il est conseillé de retirer la batterie du téléphone. En faisant ceci, on peut être rassuré que le GSM soit éteint et en plus, les changements techniques qui ont peut-être été introduits ne peuvent pas fonctionner sans électricité. Cependant il faut être vigilant. Certains fabricants ont annoncé de vouloir mettre sur le marché des GSM qui peuvent fonctionner pendant un certain temps grâce à une deuxième batterie intégrée (pour effectuer des appels d'urgence etc.). Si possible il vaut donc mieux de déposer le GSM quelque part et de le reprendre après la réunion.

2. 8. IMSI Catcher

Le IMSI Catcher est un outil que les flics peuvent installer dans le coffre de leurs voitures. Il stimule la cellule d'une société téléphonique, mais avec un peu plus de puissance. Par ce fait, les téléphones portables ne se connectent pas à la cellule officielle mais à ce IMSI Catcher. Par ce moyen, les flics peuvent découvrir avec quel GSM on téléphone et prendre connaissance des numéros IMSI et IMEI. Désormais l'utilisation du GSM de quelqu'un d'autre est inutile.
De plus, par le moyen du IMSI Catcher il est possible d'intercepter directement la communication à partir de la voiture. Les dernières versions connues de cet engin n'ont permis que la communication à partir du téléphone. Pas les appels vers le téléphone. Ceci va probablement changer rapidement.
Le désavantage le plus grand pour les flics est que, s'ils utilisent cet

outil, ils doivent mener une filature. Ils doivent donc rester proche du GSM ciblé pour ne pas perdre le contact.

Chapitre 3. Ordinateur et accessoires

3. 1. "Supprimer" ("Delete")

"Supprimer" n'est pas anéantir. La fonction "supprimer" sur un PC est comparable avec une poubelle. Le document n'est plus visible directement. Cependant un document supprimé peut être rétabli et réutilisé facilement. La comparaison entre un document et une poubelle n'est techniquement pas très pertinente, mais elle aide pour décrire le problème. Au contraire d'un document dans une poubelle, un document passé dans le broyeur de papier est difficilement réutilisable. En ce qui concerne le PC, cela s'apprête encore différemment. Le document n'est pas détruit mais autre chose est inscrit plusieurs fois (généralement entre 32 et 35 fois) sur l'espace qu'il occupe sur le disque dur. La récupération du document est ainsi exclue. Une chose qui va avec cette suppression du document est qu'il faut faire la même opération de "surscription" sur l'espace libre du disque dur. Généralement, un système procède automatiquement à la copie du document pour prévenir la perte. Ces copies ne sont pas visibles et se suppriment régulièrement automatiquement. Mais pour être certain que toutes ces copies soient vraiment "surscrit" il faut utiliser l'espace libre sur le disque dur pour autre chose. En effet, s'il y a encore de l'espace libre sur le disque dur, celui-ci est souvent utilisé automatiquement par le système pour y conserver ces copies qui ont été automatiquement faites puis supprimées par le système. Donc supprimées mais pas disparues.
Le système de gestion de fichiers est important également. Si l'on utilise Windows, on ne doit surtout pas utiliser NTFS mais FAT32. Si l'on utilise un système Linux, il faut utiliser Ext 2 et surtout pas Ext 3 ou ReiserFS. Généralement dit, il ne faut pas utiliser de Journaling-Filesystem. (Les informations par rapport à cela se trouvent dans les descriptions des systèmes de gestion de fichiers)

3. 1. 1. Système d'exploitation

Sous Windows
Eraser
Avec Eraser, des documents et registres sont supprimés de manière sûre. L'espace libre est "surscrit". On peut régler ce programme en sorte que la suppression se fasse par exemple tous les jours à 23 h. Avec les réglages "par défaut", les documents, registres et l'espace libre sur le disque dur sont "surscrits" 35 fois.
URL : http://sourceforge.net/projects/eraser

Sous Linux/Unix/MacOS X
Shred
Avec ceci, on peut supprimer et "surscrire" des documents. Cela fait partie des installations standard de Linux.
Secure delete
Ceci est un programme avec lequel on peut supprimer des documents, des registres, le Memory et le Swap. De plus, on peut remplir l'espace vide du disque dur avec ce programme.

3. 2. Codage du disque dur

Le codage du disque dur ou d'une partie du disque dur (ou d'une clé USB) est très important. Crypter les documents qui sont envoyés, graver les documents imprimés, etc. ne sert à rien compte tenu du fait que les forces de répression peuvent confisquer l'ordinateur et lire tout document qui s'y trouve. Pour éviter cela, on dispose de différents outils :

Sous Windows
PGP Disk
Avec ce programme il est possible de créer des compartiments sécurisés ("containers") dans lesquels on peut déposer des documents. Le container ne peut pas être ouvert sans un mot de passe.
Disc Crypt
C'est également un programme pour la création de container dans

lesquels on peut déposer des documents. Ces deux programmes sont commerciaux et doivent donc être achetés, si l'on ne veut pas les télécharger quelque part.

Sous Linux
Loop AES
Avec ceci on peut également établir des containers que l'on peut coder. On peut aussi coder le disque dur intégralement. Dans ce cas, il faut un mot de passe pour démarrer l'ordinateur.
Crypt Loop
Crypt Loop est directement conçu pour le Linux Kernel.

3. 3. Codage de la circulation sur l'Internet

Quand nous allons sur un site Internet ou quand nous téléchargeons quelque chose, ceci peut être observé facilement. En effet, nous laissons une véritable trace derrière nous qui dénonce ce qui nous intéresse. Nous sommes par exemple allés de notre quotidien en ligne vers le site du Secours Rouge International et ensuite vers le site de notre organisation, et nous nous avons été intéressés par telle ou telle page. Ces traces peuvent cependant être cachées. Pour ceci, nous avons besoin d'un nouvel outil. Actuellement on peut utiliser JAP ou TOR. Avec ce programme, notre trace est mélangée avec la trace d'autres utilisateurs d'Internet et ne peut dès lors plus être reconstituée. JAP existe pour tous les système d'exploitation présents sur le marché et son utilisation est très facile. TOR existe également pour tous les système d'exploitation.

3. 4. Cryptage des mails

La poste électronique est comparable à une carte postale. Si quelqu'un peut accéder à la carte, il peut la lire directement. Par conséquent, tous les mails devraient être codés. Les programmes de notre sélection sont PGP ou GnuPG. Le cryptage est basé sur un processus appelé "Public-key" ("clé publique"). Toute personne ou organisation dispose d'une clé privée et d'une clé publique. La clé publique est communiquée à tous ceux avec lesquels on veut avoir

une communication. La clé privée ne doit pas tomber dans de mauvaises mains. Elle est le garant de la sécurité du cryptage.
· Disquette, USB
· un autre ordinateur
Si la clé est envoyée, il faut absolument contrôler le fingerprint par téléphone ou lors d'un rendez-vous. Le fingerprint est un signe, une chaîne de chiffres et de caractères qui peut être vérifiée et ne pas être falsifié dans une clé. Pourquoi tout cela ? (Man in the Middle Attack)

3. 5. *Live System*

Les *Live systems* sont spécialement efficaces pour des travaux qui ne doivent pas être enregistrés dans un PC, comme par exemple des explications. Le fonctionnement est très simple. Ce sont des programmes qui sont démarrés par un CD. Un texte ou n'importe quoi d'autre peut être écrit. Ensuite, le travail peut être imprimé et le PC peut être éteint. Comme le disque dur n'a pas été impliqué dans le processus, les informations ne s'y trouvent pas. Avec un tel système on peut évidemment aussi utiliser une clé USB ou une disquette pour enregistrer des informations et pour les déposer autre part. Attention : un tel système ne se prête pas à l'utilisation anonyme de l'Internet.

3.6. Accès aux programmes

Nous proposons de préparer sur le site du Secours rouge International une page web qui donnera accès aux différents programmes (PGP et GnuPG, PGPDisc, JAP, Eraser). Ceci va nous permettre de réagir aux défauts qui pourraient éventuellement se trouver dans des anciennes versions.
Site: www.rhi-sri.org/tools/UID:rhi-sriPW:pw4tools!

Commission pour un Secours Rouge International
Secrétariat international
Postfach 1121, CH - 8026 Zurich