Sullo spionaggio elettronico poliziesco e sui metodi per proteggersene

Riassunto

Capitolo 1 : Principi
1.1. La tecnologia dell'infomazione nel quotidiano politico
1.2. Proporzionalità
1.3. Analisi di rischio
1.4. Le pass-words
1.5. Formazione
Capitolo 2 Telefonia fissa e portabile
2.1. Telefoni fissi
2.1.1. Telefax
2.1.2. Modem analogico o ISDN
2.2. Telefoni portabili
2.3. L'intercettazione
2.4. Profilo di movimento
2.4.1. Salto delle celle
2.5. SMS ping
2.6. N. IMSI, ecc
2.7. Per essere sicuri...
2.8. IMSI Catcher
Capitolo 3 Computer ed accessori
3.1. Sopprimere ("Delete")
3.1.1. Sistema d'impiego
3.2. Codificazione del disco duro
3.3. Codificare la circolazione su Internet
3.4. Criptaggio dei mails
3.5. Live System
3. 6. Accesso ai programmi

Capitolo 1 : Principi

1.1. La tecnologia dell'infomazione nel quotidiano politico

Il quotidiano politico è stato considerevolmente trasformato dalla tecnologia dell'informazione.
Si stabiliscono date di riunione per mail o SMS, informazioni sono ricercate rapidamente via Internet, ecc. Che si tratti del PC, dell'Internet o della telefonia mobile, ogni mezzo procura possibilità che possono e debbono essere utilizzate nella resistenza rivoluzionaria.
La sicurezza non va dimenticata. Non deve neppure diventare ragione di paralisi.
Dobbiamo adattarci alla situazione attuale, alla contro-rivoluzione, nel nostro modo di lavorare, utilizzando questi mezzi tecnici.
Sono, allo stesso tempo, le possibilità offerte da uno strumento e la situazione oggettiva a dover dirigere l'utilizzo di questo strumento. Dobbiamo dunque prfezionare le nostre conoscenze sulle possibilità oggettive della contro-rivoluzione, alfine di trovare un modod'impiego appropriato degli strumenti a nostra disposizione.

1.2. Proporzionalità

Nell'utilizzo di computer, telefoni portabili, ecc, va da sé che una sicurezza a 100% non c'è.
Si tratta di trovare un metodo che si situa tra la sicurezza assoluta e la nostra capacità di agire.
La complessità di situazioni, di differenti gruppi e differenti paesi, non consente di stabilire delle direttive generali. Un'analisi dei rischi è dunque sempre doverosa, per poter reagire con misure adeguate.
Esempio :
Internet è uno strumento potente per il nostro lavoro, ma è

praticamente incontrollabile da parte nostra. Ragion per cui dobbiamo mettere tutto in opera affinchè delle informazioni non giungano che al loro destinatario. Da un altro lato, non dobbiamo permetterci l'abbandono di Intarnet per paura, o per ignoranza. E' un media troppo importante, da non poter negligere.
Di conseguenza : Analisi dei rischi. Valutazione di cio' che si puo' inviare per Internet, o che si puo' registrare sul disco duro, e di cio' che non si puo' fare. Contro-misure.

1.3. Analisi di rischio

In un'analisi di rischio, i tratta semre di una situazione oggettiva. Non vi è posto per disposizioni soggettive come la paura o le tendenze offensive. L'analisi di rischo deve essere compiuta da specalisti, includendovi dei non-specialisti. Intendiamo il termine "specialisti" non già nel senso di tecnici altamente qualificati, ma ben nel senso di compagni in grado di valutare la situazione facendo ricorso a degli specialsti dell'informatica, dell'Internet o della telefonia.

Esempio di definizione di un'analisi di rischio :
- Intensità dlla lotta di classe
- Forza ed importanza della nostra struttura
- Interventi e tipi d'intervento della nostra struttura
- Chi ha conoscenze e possibilità ?
- Conoscenze tecniche di tutte/i i compagni
- Possibilità oggettive della contro-rivoluzione
- Rispetto a quali misure sono formate/i i nostri specialisti ?
- Con quale rapidità possiamo reagire ad una minaccia ?

Questa enumerazione è largamente incompleta, ma essa mostra in che direzione puo' andare una tale analisi. L'analisi delle risposte a queste questioni dà un'immagine della situazione di minaccia rispetto alla nostra struttura, e percio' delle possibilità di protezione della struttura. Non bisogna dimenticare che la proteyione è una necessità di base. L'analisi deve

egualmente comportare un'estimazione sul "chi puo' leggere o ascoltare un messaggio, e con quale mezzo?"
Le conseguenze immediate sono diverse per rapporto alla situazione, a seconda cioè che lo spionaggio si svolga sulla base di puro servizio d'informazioni, o che vi siano coinvolte direttamente delle forze di repressione.

1.4. Le pass-words

La scelta della parola è cruciale. In effetti, dei pass-words troppo semplici sono rapidamente identificati, mentre non è facile memorizzare una pass-word complicata. Non serve a niente scegliere una pass-word complicata che si debba poi notare da qualche parte, per non dimenticarla. Peraltro, pass-words come citazioni di libri, ecc, devono pure essere considerate come semplici. In principio, le pass-words devono comportare 25 segni minimo ; devono comportare caratteri minuscoli e maiuscoli, così come cifre e caratter speciali.
Per riternere la pass-word, un metodo mnemonico puo' aiutare. Per esempio : *"cosciEnze _dElle-sociEtà!5e"*
Qui, per esempio, dobbiamo ritenere che il testo comporta 5 e, di cui le prime di ogni parola in maiuscolo.

1.5. Formazione

La formazione è un momento centrale in una struttura, che sia di natura filosofica, economica o tecnica. L'apprendimento porta alla sicurezza. Molti compagni non sono coscienti dei pericoli, ma neppure delle possibilità delle nuove tecnologie. Di fatto, certe formazioni sono indispensabili. L'ignoranza puo' nuocere alla sicurezza di una struttura, tanto come puo' paralizzare le sue attività. Un'organizzazione deve decidere cio' che esige dai compagni attivi in una determinata struttura. Così le esigenze sono diverse, che si tratti d'una comunicazione di comitato centrale o che si tratti d'una comunicazione sulla data di vendita d'un giornale. Le

esigenze vanno precisamente definite.
La scelta dei temi da apprendere dipende dall'analisi di rischio. Tuttavia vi sono delle conoscenze che tutti dovrebbero avere. Per esempio :
- Come cifrare le mie informazioni su un disco duro ?
- Come cifrare dei mails ?
- Come distruggo correttamente dei documenti ?
- Come rendere anonime le mie visite su Internet ?
Delle formazioni tecniche necessitano molto tempo e sono difficil da organizzare. Cio' tiene al fatto che i/le compagni/e sono talvolta molto distaccati rispetto ai mezzi tecnici. Gli uni utilizzano ancora delle macchine da scrivere, mentre gli altri dispongono dei più recenti gadget tecnici. Scopo di una formazione deve essere tale che tutte/i i compagni conoscano i problemi eventuali, così come le soluzioni. Soluzioni che siano poi in grado di poter applicare.

Capitolo 2 Telefonia fissa e portabile

2.1. Telefoni fissi

Si suppone che il rischio legato ai telefoni fissi sia oggi ampiamente conosciuto. Percio' ci accontenteremo di descriverlo a grandi linee.
Quando si telefona, si puo' sempre supporre che le forze della contro-rivoluzione siano all'ascolto. Che si tratti di un raccordo analogico tradizionale o dell' ISDN. D'altronde è possibile spiare una stanza con un microfono piazzabile nel telefono

2.1.1. Telefax

Le telefax è egualmente spiabile, con facilità

2.1.2. Modem analogico o ISDN

Si sono avuti tentativi di acolto di una stanza, attraverso n

microfono piazzato in un modem.
Tentativi parzialmente riusciti. Possiamo trarne la conclusione che né il telefono, né il fax danno sicurezza, e che non possono essere sicurizzati da parte nostra. E' dunque doveroso staccare prese del telefono, di fax o di modem, durante una riunione.

2.2. Telefoni portabili

2.3. L'intercettazione

Un telefono portabile puo' essere intercettato esattamente come un telefono fisso tradizionale. Lo stesso dicasi per gli SMS, e gli MMS. Queste informazioni transitano per la società telefonica, dove possono essere osservati e registrati facilmente.

2.4. Profilo di movimento

Cio' che è nuovo è il fatto che ora è possibile sorvegliare la localizzazione d'un GSM. Nelle zone con numerose celle, per esempio nelle città, i movimenti d'un GSM possono essere osservati in modo sufficientemente esatto.

2.4.1. Salto delle celle

Una cella consiste in una o più antenne che trasmettono le informazioni del telefono portabile, per esempio nel corso di una comunicazione, verso la società telefonica. A partire da questa, la società telefonica puo' vedere quale GSM si trova in una certa cella. Dall'avvio di una comunicazione, che sia per chiamata o per SMS, il telefono portabile si raccorda all'antenna che gli assicura la migliore ricezione. Se siamo in movimento, dunque, noi lasciamo traccia e permettiamo di vedere in quale direzione ci stiamo dirigendo. Percio' è assurdo di andare ad una riunione clandestina e di spegnere il nostro GSM una volta arrivati. Se il vostro telefono porta-

bile è sorvegliato, dal momento che voi scrivete un SMS, o che chiamate qualcuno, o che ricevete un SMS-ping (ci ritorneremo), si puo' vedere dove voi vi troviate. Pure se non è possibile d'ascoltare un GSM spento, e che si trova in riunione, è importante sapere che, se dei GSM sorvegliati si incontrano alla stessa ora, allo stesso posto, questo non dovrà più essere scelto come luogo di riunione successiva.

2.5. SMS ping

Il SMS-ping è una tecnica utilizzata per localizzare un GSM. La società telefonica invia un segnale al telefono, simile ad un SMS. Attraverso questo, una comunicazione viene stabilita, permettente di osservare in quale cella si trova il GSM. Dopo questo breve contatto, la comunicazione è interrotta. Il SMS-ping è dunque un segnale attraverso il quale una comunicazione viene stabilita con il telefono portabile, senza che cio' si possa vedere sullo schermo del telefono.

2.6. N. IMSI, ecc

Un telefono portabile comunica, via diversi numeri, con i servizi telefonici e le celle. Noi conosciamo i numeri di chiamata. Pertanto, a lato di questo numero, ogni telefono possiede un numero. Questo numero è denominato IMSI. Grazie a questo numero, il telefono è semre identificabile, pure nel caso di cambiamento della carta SIM.

2.7. Per essere sicuri...

Per essere sicuri che un telefono prtabile non emetta più segnali, è consigliabile di rimuovere la batteria del telefono. Cio' facendo, si puo' ssere rassicurati che il GSM sia spento e, in più, le modificazioni tecniche che possono essere state introdotte non potranno funzionae senza elettricità. Tuttavia bisogna essere vigilanti. Alcuni fabbricanti hanno annunciato l'introduzione sul mercato di GSM capaci di funzionare, per un certo tempo, grazie ad una seconda batteria integrata (per effettuare chiamate d'urgenza, ecc). Se possibile, è tanto meglio lasciare il GSM da qualche parte e riprenderlo dopo la riunione.

2.8. IMSI Catcher

Il IMSI Catcher è uno strumento che gli sbirri possono installare nel cofano delle vetture. Esso sollecita la cella d'una

società telefonica, ma con maggiore potenza. Percio' i telefoni portabili non si connettono alla cella ufficiale, ma a questo IMSI Catcher. Per questa via, gli sbirri possono scoprire con quale GSM si telefona, e prendere conoscenza dei numeri IMSI e IMEI. Ormai l'utilizzo del GSM di qualcun altro è così inutile.
Di più, per mezzo dell'IMSI Catcher è possibile intercettare direttamente la comunicazione a partire dalla vettura. Le ultime versioni conosciute di questo apparecchio non permettono che la comunicazione a partire dal telefono. Non le chiamate verso il telefono. Cio' va a cambiare rapidamente, probabilmente.
Lo svantaggio per gli sbirri è che, per utilizzare questo strumento, devono fare pedinamento. Devono restare prossimi al GSM sorvegliato, per non perdere il contatto.

Capitolo 3 Computer ed accessori

3.1. Sopprimere ("Delete")

"Sopprimere" non è distruggere. La funzione "sopprimere" in un PC è paragonabile ad una pattumiera. Il documento non è più visibile direttamente. Ma un documento soppresso puo' essere ristabilito e riutilizzato facilmente. Il paragone tra un documento soppresso ed una pattumiera non è tecnicamente molto pertinente, ma aiuta a descrivere il problema. Contrariamente ad un documento gettato in pattumiera, un documento passato al macero è difficilmente riutilizzabile. Per cio' che concerne il PC, questo si presenta differentemente.
Il documento non è distrutto, ma altre cose vi sono sovrascritte diverse volte (generalmente tra 32 e 35 volte), nello spazio occupato dal disco duro. Il recupero del documento è a quel punto impossibile. Un'operazione che va con questa

distruzione del documento è che bisogna fare la stessa operazione di "sovrascrizione" sullo spazio libero del disco duro. Generalmente, un sistema procede automaticamente alla copia del documento, per prevenirne la perdita. Queste copie non sono visibili, e si sopprimono regolarmente, automaticamente. Ma per essere sicuri che tutte queste copie siano veramente "sovrascritte", va utilizzato lo spazio libero sul disco duro per altra cosa. In effetti, se vi è ancora dello spazio libero sul disco duro, questo è sovente utilizzato automaticamente dal sistema per conservarvi queste copie che sono state prodotte automaticamente, poi soppresse dal sistema. Dunque soppresse, ma non scomparse.
Il sistema di gestione degli archivi è egualmente importante. Se si utilizza Windows, non si deve assolutamente utilizzare NTFS, ma FAT32. Se si utilizza Linux, si deve usare Ext 2 e assolutamente non Ext 3 o ReiserFS. In generale, non si deve utilizzare Journaling-Filesystem
(Le informazioni per rapporto a cio' si trovano nelle descrizioni dei sistemi di gestione degli archivi).

3.1.1. Sistema d'impiego

Con Windows
Eraser
Con Eraser, documenti e registri sono soppressi in maniera sicura. Lo spazio libero viene "sovrascritto". Si puo' regolare questo programma di modo che la soppressione si faccia, per esempio, tutti i giorni alle ore 23. Con il reglaggio "per difetto", documenti, registri, e lo spazio libero sul disco duro sono "sovrascritti" 35 volte.
URL : http://sourceforge.net/projects/eraser

Con Linux/Unix/MacOS X
Shred
Con queso programma, si possono sopprimere e "sovrascriv-

ere" dei documenti. Esso fa parte delle installazioni standard di Linux.
Secure delete
Queto è un programma con cui si puo' sopprimere documenti, registri, Memory e il Swap.
Di più, si puo' riempie lo spazio vuoto del disco duro con questo programma.

3.2. Codificazione del disco duro

La codificazione del disco duro, o di una sua parte (o di una chiave USB), è molto importante.
Criptare i documenti inviati, registrare i documenti stampati, ecc, non serve a nulla conto tenuto del fatto che le forze di repressione possono confiscare il computer e leggervi ogni documento. Per evitare cio', si dispone di vari strumenti :

Con Windows
PGP Disk
Con questo programma è possibile crear dei compartiment securizzati ("containers"), nei quali depositare dei documenti. Il container non puo' essere aperto senza pass-word.
Disc Crypt
E' egualmente un programma per la creazione di container, nei quali depositare documenti.
Questi due programmi sono commercializzati e debbono dunque essere acquistati, se non si vuole telecaricarli da qualche parte.

Con Linux
Loop AES
Con questo , pure, si possono costituire dei container codificabili. Si puo' anche codificare il disco duro, integralmente. In questo caso ci vuole una pass-word per avviare il computer.
Crypt Loop
Crypt Loop è direttamente concepito per il Linux Kernel.

3.3. Codificare la circolazione su Internet

Quando si va su un sito Internet, o quando si telecarica qualcosa, cio' puo' essere osservato facilmente. In effetti noi lasciamo una vera traccia dietro di noi, denunciante cio' che ci interessa. Per esempio, durante la giornata siamo andati sul sito del occorso Rosso Internazionale ed in seguito sul sito della nostra organizzazione ; e noi ci siamo interessati a questa o quella pagina. Queste tracce, pertanto, possono essere nascoste. Per fare questo, abbiamo bisogno di un nuovo strumento. Attualmente si puo' utilizzare JAP o TOR.
Con questo programma, la nostra traccia è mischiata a quella di altri utilizzatori d'Internet e non puo' più essere ricostituita. JAP esiste per turri i sistemi d'impiego presenti sul mercao, ed il suo utilizzo è molto semplice. TOR esiste egualmente per tutti i sistemi d'impiego.

3.4. Criptaggio dei mails

La posta elettronica è paragonabile ad una carta postale. Se qualcuno puo' accedere alla carta, puo' leggerla direttamente. Per cui, tutte le mails dovrebbero essere codificate. I programmi della ostra selezione sono PGP o GnuPG. Il criptaggio è basato su un processo denominato "Public- key" (chiave pubblica). Ogni persona od organizzazione dispone d'una chiave privata e di una chiave pubblica. La chiave pubblica è trasmessa a tutti quelli con cui si vuol essere in comunicazione. La chiave privata non deve cadere in mani sbagliate. Essa è la garante della sicurezza del criptaggio.
- Dischetta, USB
- Un altro computer

Se la chiave è inviata, bisogna assolutamente controllare il fingerprint per telefono o nel corso di un incontro. Il fingerprint è un segno, una catena di cifre e caratteri, che puo' eseere verificata e non puo' essere falsificatain una chiave.
Perché tutto cio' ? Man in the Middle Attack

3.5. *Live System*

I Live Systems sono specialmente efficaci per dei lavori che non devono essere registrati su un PC, come per esempio delle spiegazioni. Il funzionamento è molto semplice. Sono programmi avviati da un CD. Un testo, o altra cosa, puo' essere scritto. In sguito, il lavoro puo' eseere impresso ed il PC spento. Essendo che il disco duro non è stato implicato nel processo, le informazioni non vi si trovano. Con un tale sistema si puo' anche utilizzare, evidentemente, una chiave USB o una dischetta, per registrare delle informazioni e per depositarle altrove.
Attenzione : un tale sistema non si presta all'utilizzo anonimo di Internet.

3.6. Accesso ao programmi

Proponiamo di preparare sul sito del Soccorso Rosso Internazionale una pagina web che darà accesso ai diversi programmi (PGP e GnuPG, PGPDisc, JAP, Eraser). Questo ci permetterà di ovviare ai difetti che potrebbero eventualmente trovarsi nelle versioni precedenti.
Sito: www.rhi-sri.org/tools/UID:rhi-sriPW:pw4tools!

Commissione per un SRI
(Segretariato internazional)
Postfach 1121, CH - 8026 Zurigo