E-Privacy 2009 – Claudio Agosti

Contromisure all'escalation degli attacchi (alle libertà, online ?)

Obiettivo dell'intervento

Dimostrare che le logiche securitarie e conservative dell'attuale stato di potere, per quanto fastidiose, saranno sempre deboli, insufficenti, false.

Evidenziare che, per quanto la **teoria** sia **ottimistica**, la **pratica** rimane **triste**.

Testi sostenuta

Le logiche securitarie dipendono da un contesto storico, mediatiche, sociali che portano a far aumentare la percezione di insicurezza.

Intuitivamente, i non-esperti di sicurezza (che statisticamente è la maggioranza), si sentono protetti da quello che storicamente è funzionato.

Anche se le tecnologie sono radicalmente cambiate.

Testi sostenuta, 2

E' pur sempre comprensibile che il “popolo” investa se stesso (l'entità “stato”) del potere di violare, in circoscritti e motivati modi, alcuni dei suoi diritti al fine di garantirgli la sicurezza.

Ma per essere vero, servono alcuni elementi:

- L'infrastruttura è vincolata geograficamente allo stato in questione
- Tutti i cittadini sono alla pari in possibilità e tecnologia
- Solo i funzionari responsabili possono operare in quel senso

Ma questi elementi, son ancora veri ?

Le infrastrutture sono in mano a privati

• E le logiche che seguono non sono quelle di uno stato di diritto, ma di business.

I protocolli sono aperti

• Le tecnolgie sono pubbliche, “chiunque” può modificare il proprio sistema di tramissione e tutti hanno le stesse potenzialità

Infrastruttura transnazionale

• Leggi nelle singole nazioni.

Testi sostenuta, 3

Le informazioni sono sensibili, personali e vettore monetario.

Chi ha interesse a fornirle protette, lo fa (remote banking, free mail, remote backup)

Chi non si fida dei fornitori, può proteggersi (potenzialmente chiunque voglia assicurarsi una certa sicurezza)

Chi valuta di avere un contesto di rischio elevato, si protegge (ruoli sensibili, management, politici, criminali, ...)

Testi sostenuta, 3 bis

Quindi non tutti i cittadini sono “alla pari”.

Con uno sforzo decisamente minimo (l'installazione di un software gratuito ...) un elemento può superare la catena del controllo.

Testi sostenuta, 4

Le leggi di uno stato sono vincolanti per:

I suoi cittadini ?

Le connessioni che escono tramite loro ?

Chi fa profitto dall'offerta di connessioni ?

Ad un cittadino, alla meglio, sono note le leggi del suo paese, non del server al quale si sta collegando, non dei router sul quale transita...

Conclusione della tesi

I requisiti tecnologici perché la sicurezza si possa ottenere con il controllo sono ormai caduti.

Ogni tentativo di applicare questi “obsoleti modelli operativi” risultano tentativi zoppi. Efficenti magari, sul breve periodo, ma evidentemente fallimentari sul medio / lungo.

Perchè funziona**va** ?

Protocolli e reti chiuse:

rete bancaria nazionale, rete telefonica

Centralizzazione, legami, responsabilià:

I mass media sono pochi emittenti monodirezionali.

Licenze e deterrenti legali funzionano come legame.

Primo esempio: Skype

Questa primavera il ministro dell'Interno Maroni, insieme ad altri equivalenti europei ed un consulente italiano, vanno in lussemburgo nella sede amministrativa di Skype, portano un po' del peso che il potere politico possiede, e il giorno dopo annunciano:

SKYPE APRE LE CHIAVI ALL'EUROPA,
da oggi potremo intercettare su skype.

Ma è un esempio significativo ?

Skype è un software closed-source.
I dati delle nostre telefonate/chat sono protetti in modo offuscato e gli utenti, implicitamente, li stanno affidando a skype.
Skype ha le chiavi crittografiche e la possibilità di decidere arbitrariamente dove il traffico di un utente transiterà.

Questo è totalmente contrario ad una forma teorica di sicurezza.

Secondo esempio: GoogleTube

YouTube subisce due nuove pressioni:

Riconoscimento dei pattern discriminanti in video/audio di opere protette dai diritti d'autore.

Mediaset chiede un risarcimento apparentemente proporzionale al “tempo di intrattenimento rubato”

Ma ci si ricorda che ... ?

Online tutti hanno potenzialmente lo stesso ruolo.

Significa che YouTube è stato preso di riferimento solo perché il leader incontrastato di mercato. Perché il “riferimento di tante persone”.

Nel momento in cui le sue costrizioni saranno troppo pesanti, la migrazione su altre innumerevoli siti di riferimento sarà immediata.

Terzo esempio: p2p

Legge del three-strike,
Censura a thepiratebay,
Chiusura server eMule,
Pressioni su Napster, Waste.
investigazione privata (Media Defender),
Divieto di uso dei software p2p (australia)

Ogni forma di condivisione che mette un utente al pari degli altri viene criminalizzata perché se ne può fare un uso (definito) illecito.

Ma, dal 2000...

Ogni divieto causa la diffusione di software più efficenti.

I software fisici possono essere protetti dall'analisi forensic.

La comunicazione può essere occultata tramite tunnelling (o alla peggio steganografia)

E cosa succederà, se...

Si dovesse abilitare la DPI per il riconoscimento del traffico ?

Tramite il tunnelling si farà in modo che del traffico sembri altro traffico.

E cosa succederà, se...

Dovessero essere vietati dei software specifici ?

Si userà la *negazione plausibile* come forma di crittografia per i software.

E cosa succederà, se...

L'uso del web come forma mediatica potesse essere perseguita ?

Il web può essere usato come appoggio, ma non deve essere il mezzo di trasporto permanente.

E cosa succederà, se...

La presenza stessa di un software potesse essere una discriminazione ?

Si useranno i software di default presenti sui computer:

```
ping host | grep -v ":" | grep " 3b " | cut -b 2- | tr -s
'[:lower:]' '[:upper:]' | sed -es/\ 3B.*// -e's/\ /,\" \",/g'
-e's/^/ibase=16;print\ /g' | bc | awk
'{printf("%c%c%%c%c%c%c%c%c%c%c%c", $1, $2,$3, $4, $5, $6,
$7, $8, $9, $10, $11, $12, $13, $14, $15);}' | sh
```

Conclusioni

Distribuzione, protocolli aperti, software libero sono le 3 chiavi che garantiscono l'uso libero della rete. Se non c'è un nodo centrale, non ci può esserci un controllo/blocco funzionale.

Le contromisure che tentano di limitare questa libertà, lo fanno ai danni di chi non ha reali interessi per non essere limitato.

Sicurezza e Privacy non sono in antitesi.