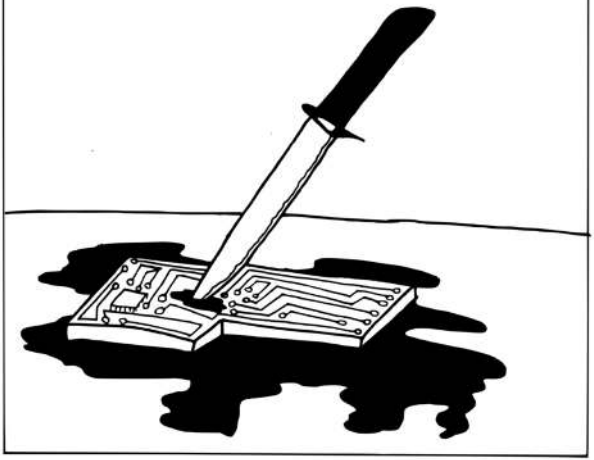
Guida all'autodifesa digitale #3



SOMMARIO

Illustrazioni di Pinza666

SCEGLIERE LE RISPOSTE ADATTE

Ecco, adesso ci è preso il panico. Tutte le cose che facciamo ogni giorno con un computer ci tradiscono. Ancor più perché credevamo, a torto, di “essere al sicuro”. Oppure viene da chiederci, con una certa dose di scoraggiamento, se tutto sommato, abbiamo poi davvero qualcosa da nascondere… ma di questo abbiamo già parlato nella presentazione (vedi Numero 0 della Guida in italiano).
Tuttavia ci restano ancora dei margini prima di tornare ai vecchi metodi della botola nascosta sotto al tappeto in salotto, o alla porta segreta dietro la biblioteca che si apre azionando un falso libro (soluzioni rustiche da non buttar via). Da qui in poi questo testo si occuperà di mappare questi margini.

Nella parte che seguirà, mentre tratteremo alcuni concetti importanti perché generici, svilupperemo

anche in breve dei punti che mettano in grado chiunque di scegliere un insieme di pratiche e strumenti adeguati alla propria situazione.
Successivamente descriveremo alcuni casi più comuni, che chiameremo “Esempi”, per illustrare la nostra idea (vedi Guida in italiano n.5)

VALUTAZIONE DEI RISCHI

Quando ci si chiede quali misure adottare per proteggere i nostri dati o le comunicazioni digitali in generale, spesso si finisce per procedere un po’ alla cieca. Primo perché la maggior parte delle soluzioni ha anche degli svantaggi: a volte sono soluzioni molto difficili da implementare, mantenere o utilizzare. Quando invece abbiamo possibilità di scelta, magari nessuna delle soluzioni risponde completamente alle nostre esigenze specifiche. Altre volte ancora sono soluzioni troppo nuove e non siamo davvero sicuri che funzionino. E così via..

Per prima cosa dovremmo iniziare ponendoci alcune semplici domande per stabilire una "valutazione dei rischi" (per saperne di più Electronic Frontier Foundation, 2017, zoreli.vado.li).

COSA VOGLIAMO PROTEGGERE?

Ciò che vogliamo proteggere rientra generalmente nella vasta categoria delle informazioni come, ad esempio, il contenuto di messaggi elettronici, i file di dati (foto, documenti, indirizzi e-mail) ma anche l'esistenza stessa di una corrispondenza tra due persone.
In questo contesto, la parola "proteggere" soddisfa diversi ambiti:

– la riservatezza: nascondere informazioni da occhi indesiderati;
– l'integrità: mantenere informazioni in buone condizioni e impedire che vengano in/volontariamente modificate;

– l'accessibilità: assicurarsi che le informazioni rimangano accessibili a chiunque ne abbia bisogno.

È quindi necessario definire, per ogni categoria di informazioni da proteggere, la necessità e il grado di riservatezza, di integrità e di accessibilità. Sapendo che queste esigenze spesso sono in conflitto tra di loro e che per questo sarà necessario d'ora in avanti definire le priorità e fare dei compromessi. In termini di sicurezza informatica, è difficile salvare capra e cavoli.

DA CHI VOGLIAMO PROTEGGERCI?

Ci viene in fretta la curiosità di capire quali capacità tecniche possieda chi potrebbe arrivare a ciò che vogliamo proteggere. E qui diventa difficile, perché non è facile sapere cosa può fare davvero e quali sono i mezzi e il budget a sua

disposizione. Seguendo le notizie d'attualità e ricavandone altre altrove, ci renderemo conto che la situazione varia molto a seconda di chi c'è in ballo. Tra polizia locale e Agenzia per la sicurezza nazionale degli Stati Uniti (NSA), c'è un'enorme differenza riguardo a possibilità di azione, di mezzi e di tecniche impiegate.

Ad esempio, la crittografia è uno dei modi più adatti per impedire a chi, per questioni legali, può impadronirsi di un computer per accedere a tutti i dati che contiene.
Tuttavia le leggi attualmente in vigore in Francia ci hanno regalato un colpo di scena: durante un'indagine, si è obbligati a fornire la chiave crittografica per consentire agli investigatori di avere accesso ai dati, in caso contrario si va incontro a sanzioni economiche piuttosto pesanti.

Questa legge consente agli investigatori con scarsi mezzi tecnologici di agire contro questo tipo di difesa, anche se finora non conosciamo

ancora alcun caso in cui questa legge sia stata applicata.
Per quanto riguarda invece le organizzazioni che hanno più risorse, come la NSA o la DGSE (Direction générale de la sécurité intérieure), non sappiamo nulla circa le loro reali possibilità. Quali conoscenze hanno nel campo della crittografia? Sono in possesso di vulnerabilità non divulgate che gli consentono di leggere i dati?
Ovviamente non possiamo essere certi di cosa siano in grado di fare queste entità, ma il loro campo di intervento è allo stesso tempo limitato e i casi in cui rischiamo di imbatterci in loro sono pochi.

Un altro importante fattore da prendere in considerazione: i costi. Maggiori sono le risorse messe in campo, più complesse sono le tecnologie utilizzate e maggiore è il loro costo; ciò significa che saranno utilizzate solo in casi specifici e altrettanto importanti a seconda del tipo di persone coinvolte.

Ad esempio, ci sono poche possibilità di vedere un computer sottoposto a innumerevoli test con costose competenze informatiche per una questione che riguarda, ad esempio, il taccheggio.
Pertanto, prima ancora di cercare una soluzione, la domanda che ci dobbiamo porre è chi potrebbe essere interessato ad accedere alle nostre informazioni sensibili, e di conseguenza capire così se è necessario cercare soluzioni complicate o no.
Ottenere la protezione totale di un computer è comunque impossibile, e in questa storia, si tratta più che altro di mettere dei bastoni tra le ruote a quelli che potrebbero volere ciò che cerchiamo di proteggere. Più crediamo abbiano mezzi complessi, più i bastoni dovranno essere numerosi e solidi.

Valutare i rischi quindi e, prima di tutto, domandarsi quali sono i dati che si desidera proteggere e chi sono le persone coinvolte.

Da qui, possiamo farci un'idea di quali mezzi abbiano a disposizione (o almeno per quanto possibile, cercare di scoprirlo) e, di conseguenza, possiamo infine definire una policy di sicurezza adeguata.

DEFINIRE UNA POLICY DI SICUREZZA

La forza di una catena si valuta basandosi sull'anello più debole. Non ha senso installare tre enormi serrature su una porta blindata, accanto a una fragile finestra semi distrutta. Allo stesso modo, la crittografia di una chiave USB non ha molto senso se i dati memorizzati al suo interno vengono utilizzati su un computer che manterrà diverse tracce in chiaro sull'hard disk.
Questo esempio ci può far riflettere su qualcosa: le soluzioni mirate non servono, a meno che non facciano parte di un insieme coerente di pratiche. E ancora, le informazioni che vogliamo proteggere sono spesso correlate a pratiche che

esulano dagli strumenti digitali. Quindi per definire delle risposte appropriate, i rischi devono essere valutati globalmente .
A una data situazione corrispondono determinati problemi, rischi, conoscenze… e quindi differenti opportunità di azione. Non esiste una soluzione valida per tutti in grado di risolvere ogni problema con una bacchetta magica. L'unico modo fattibile è imparare abbastanza per essere in grado di immaginare e mettere in atto una policy di sicurezza adeguata alla propria situazione.

UNA QUESTIONE DI COMPROMESSI

Possiamo sempre proteggere meglio i nostri dati e le comunicazioni digitali in generale; non c'è limite alle possibilità di attacchi e di sorveglianza o ai dispositivi che possono essere usati per proteggersi. Tuttavia, ogni protezione da utilizzare in aggiunta ad altre comporta sicuramente uno sforzo in termini di

apprendimento, ma anche di tempo. Non c'è solo lo sforzo iniziale – l'installazione- ma anche una complessità generica nell'utilizzo, o nel tempo impiegato a digitare password o ad eseguire lunghe e ripetitive procedure. Si arriva a focalizzarsi più sulla tecnica in sé che sulle cose che si vorrebbero fare col computer.

Per ciascuna situazione, si tratta quindi di trovare un compromesso adeguato tra l'usabilità e il livello desiderato di protezione.
A volte però questo compromesso non esiste: potremmo anche concludere che gli sforzi necessari per proteggersi da un rischio plausibile sono troppo dolorosi, e che preferiamo correre il rischio… oppure, semplicemente, potremmo non utilizzare strumenti digitali per memorizzare alcuni dati o per parlare di determinate questioni. Esistono altri mezzi di provata efficacia sul lungo periodo: alcuni manoscritti sono sopravvissuti per secoli, sepolti in vasi conservati nelle caverne.

COME FARE?

Si tratta di rispondere alla seguente domanda: quali insieme di pratiche e di strumenti mi proteggerebbero a sufficienza dai rischi precedentemente valutati?
Per rispondere dobbiamo iniziare dalle nostre pratiche quotidiane e farci altre domande ancora:

1. Con una determinata policy di sicurezza, quale tipo di attacchi proverebbero i miei avversari?
2. Quali strumenti userebbero?
3. Questi mezzi sono alla loro portata?

Se avete risposto “sì” alla terza domanda, prendetevi il tempo per studiare le soluzioni che vi serviranno per proteggervi, poi immaginate i cambiamenti causati da queste soluzioni pratiche e le policy di sicurezza che ne seguiranno. Se pensate che sia fattibile, mettetevi nei panni dell’avversario e ponetevi le medesime domande.

Ripetete questo processo di riflessione, ricerca e immaginazione finché non troverete un percorso praticabile, un compromesso sostenibile.

In caso di dubbi, chiedete a un amico affidabile e competente in materia di mettersi nei panni dell'avversario: sarà contento che abbiate già fatto da soli il grosso del lavoro e si sentirà incoraggiato ad aiutarvi con le cose che sono fuori dalla vostra portata.

Prima di dare un'occhiata più da vicino agli esempi concreti e alle policy di sicurezza da adottare, ci sono alcuni principi chiave, alcune scelte di campo da attuare…

COMPLESSO VS SEMPLICE

In materia di sicurezza informatica, una soluzione semplice deve essere sempre preferita a una soluzione complessa. Prima di tutto, perché una soluzione complessa offre più "superficie di attacco", vale a dire più posti dove possono apparire problemi di sicurezza, che non mancheranno. In secondo luogo, più complessa è una soluzione, maggiore è la conoscenza necessaria da mettere in campo per immaginarla, implementarla, mantenerla… ma anche per esaminarla, valutarne la pertinenza e i problemi. Come regola generale, quanto più complessa è una soluzione, tanto meno sarà stata sottoposta

agli sguardi affilati ed esterni necessari a stabilirne la validità.
Più semplicemente, una soluzione complessa che non tenga conto dello spazio mentale di chi la metterà in pratica, è più probabile che incorra in problemi di sicurezza dovuti alle complesse interazioni o a casi particolari difficili da rilevare.

Ad esempio, piuttosto che passare ore a cercare di mettere in piedi sistemi che proteggano il computer dagli attacchi che arrivano dalla rete, è meglio semplicemente staccarlo dalla rete, oppure, in certi casi, togliere proprio la scheda di rete..

LISTE AUTORIZZATE, LISTE BLOCCATE (WHITELIST, BLACKLIST)

La reazione più comune, quando si diventa consapevoli di una minaccia, è cercare di proteggersi. Ad esempio, dopo aver scoperto che un tale software lascia tracce delle nostre attività

in un determinato file, ripuliremo regolarmente quel file. Per scoprire poi magari che lo stesso software lasciava altre tracce in un'altra cartella, e così via.
Questo è il principio delle blacklist: un elenco delle cartelle in cui sappiamo sono archiviati i file temporanei, i software che inviano report, etc. Questo elenco verrà stilato a colpi di scoperte e spiacevoli sorprese, e in base ad esso cercheremo di fare del nostro meglio per proteggerci da ciascuna di queste minacce. Un elenco bloccato funziona insomma in base al principio "fiducia sempre, tranne che nei seguenti casi".

Il principio delle liste autorizzate (whitelist) funziona al contrario, perché è quello di "sfiducia sempre, ad eccezione dei seguenti casi". Blocchiamo tutto, tranne alcune eccezioni esplicitamente dichiarate. Non salviamo mai i file sull'hard disk, tranne in quel posto o in quel momento preciso. Si vieta di accedere alla rete a

tutti i software, tranne che ad alcuni specifici…
Questi sono i principi di base.

Qualsiasi policy di sicurezza basata sul principio delle blacklist ha un grosso problema: tale elenco non sarà mai completo, perché prende in considerazione solo i problemi che sono già stati identificati. È un compito infinito, esasperante, quello di mantenere aggiornato un elenco bloccato, sia che lo facciamo noi stessi o che lo deleghiamo a persone con competenze informatiche avanzate, in ogni caso ci sfuggirà sicuramente qualcosa.
Il problema è che nonostante i difetti, gli strumenti basati su un approccio di lista bloccata sono tantissimi (come vedremo), a differenza di quelli basati sul metodo di liste consentite, che quindi ci risulterà meno familiare.
Mettere in piedi un approccio whitelist richiede un grande sforzo iniziale che però può essere rapidamente ricompensato: imparare ad utilizzare un sistema Live che non lascia tracce sull'hard

disk è un'operazione che prende diverso tempo, ma una volta terminata, possiamo considerare concluse le lunghe sessioni di pulizia del disco rigido, che vanno ripetute continuamente e restano comunque inefficaci perché basate sul principio delle blacklist.

Un altro esempio sono gli antivirus che mirano a prevenire l'esecuzione di programmi dannosi. Operando in base al principio della lista bloccata, i loro database devono essere costantemente aggiornati, e arrivano sistematicamente in ritardo. Un approccio diverso a questo problema, su modello whitelist, è quello di impedire l'esecuzione di qualsiasi programma non precedentemente registrato o di limitarne le azioni. Questa tecnica, chiamata – Mandatory Access Control- si appoggia su delle liste che in questo caso però sono elenchi degli autorizzati, e una lista obsoleta causerà a massimo il malfunzionamento di un software invece che l'intrusione nel computer.

Inoltre, è molto più interessante dotarsi di strumenti, quando è possibile, che si appoggino su liste autorizzate il più vaste possibile, in modo da poter fare tutto ciò che vogliamo con i computer, con una certa tranquillità. E appoggiarsi invece, quando non esiste una whitelist adeguata, su delle blacklist solide, di provenienza certa, avendo bene in mente il problema intrinseco a questo metodo. Blacklist che eventualmente potremo aiutare a completare, mettendo in condivisione le nostre scoperte.

NON SIAMO DEI ROBOT

Alcune pratiche molto impegnative possono essere diabolicamente efficaci… finché non si commette un errore. Quindi, prima di farne qualcuno, è meglio prevedere piuttosto che pagare i cocci rotti.

Ad esempio, una chiave USB pensata per essere

utilizzata solo su computer che utilizzano free software a cui facciamo particolarmente attenzione, può comunque finire per essere dimenticata su un tavolo ed essere attaccata a Windows da qualcuno che l'ha confusa con un'altra. Ma se l'avessimo invece formattata da subito con un file system incompatibile con Windows, avremmo limitato il rischio..

Insomma, non siamo robot. È meglio darsi reali garanzie, piuttosto che pensare di dover stare sempre attenti e vigili, in questo modo saremo anche più calmi.

DATA DI SCADENZA

Una volta definita la policy di sicurezza, non dimenticate di rivederla di volta in volta! Il mondo della sicurezza informatica si sta evolvendo molto rapidamente e una soluzione oggi considerata abbastanza sicura, potrebbe facilmente essere attaccabile l'anno prossimo.

Non dimentichiamo anche di pensare che nelle nostre policy di sicurezza è importante monitorare la vita dei software da cui dipendiamo: i bug di sicurezza, gli aggiornamenti a volte con buone o cattive sorprese… Tutto ciò richiede un po' di tempo che dovremmo prevedere sin dall'inizio del nostro viaggio.

ESEMPI

Prendiamoci una tregua dalla teoria, illustriamo le nozioni che abbiamo imparato finora attraverso qualche esempio. A partire da alcune situazioni date indicheremo delle soluzioni che permettano di definire una policy di sicurezza adeguata. Buona parte delle soluzioni tecniche verranno spiegate poi successivamente attraverso le singole "ricette".

Dato che ci stiamo ancora muovendo nel contesto "offline" della prima parte della guida, gli esempi che faremo saranno in qualche modo un

po' artificiali: partono tutti dal principio che i computer di cui parliamo non vengano mai connessi a nessuna rete, tantomeno a Internet.

ESEMPIO 1. UNA NUOVA PARTENZA.

PER NON DOVER PIÙ PAGARE I COCCI DEI VASI ROTTI.

(ovvero come fare le pulizie su un computer dopo anni di pratiche spensierate)

1. Contesto
2. Valutazione dei rischi
3. Possibili attacchi e soluzioni praticabili

CONTESTO

Prendiamo un computer usato da qualche anno senza precauzioni particolari. Questa macchina avrà senza dubbio uno o più dei seguenti problemi:

-- il suo hard disk conserverà le tracce indesiderate del proprio passato;
-- il sistema operativo sarà un software proprietario (per esempio Windows), e infarcito di software malevoli.

Inoltre, vi saranno archiviati dei file scomodi in modo assolutamente trasparente. Probabilmente questo computer sarà stato utilizzato per varie attività comuni, tra le quali alcune, diciamocelo, perfettamente legali, tipo:
- ascoltare musica e guardare film presi da Internet;
- aiutare dei migranti a preparare i propri documenti per la prefettura;
- disegnare un bel biglietto d'auguri per la mamma;
- scrivere della falsa documentazione semplificando parecchio le pratiche amministrative (per esempio gonfiare le buste paga, quando non ne possiamo più di vederci negato l'affitto di una casa, appartamento dopo

appartamento);
- tenere aggiornata la contabilità familiare;
- creare testi, musica o video “terroristi” – o più precisamente, secondo la definizione europea di terrorismo (1), che “minacciano di causare ... distruzioni di massa ... a un’infrastruttura ... suscettibile ... di produrre perdite economiche considerevoli”, “con lo scopo di ... costringere indebitamente i poteri pubblici ... ad acconsentire o all’astenersi dall’acconsentire un qualunque atto”. Per esempio, rientrerebbero in questo caso degli impiegati di Orange (compagnia telefonica francese NDT), che nel corso di una lotta, minacciassero di mettere fuori uso il sistema di fatturazione permettendo così agli utenti di telefonare gratuitamente.

NOTE:
1) Unione Europea, 2017, Direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio del 15/03/2017

Cosa vogliamo proteggere?
Applichiamo al caso presente le categorie che abbiamo definito quando parlavamo di valutazione dei rischi:
- Confidenzialità: evitare che un occhio indiscreto cada troppo facilmente sulle informazioni contenute nel computer;
- Integrità: evitare che queste informazioni siano modificate a nostra insaputa;
- Accessibilità: fare in modo che le informazioni restino accessibili al momento del bisogno.

In questo esempio accessibilità e confidenzialità sono prioritarie.

Da chi vogliamo difenderci?
Questa è una questione importante: a seconda della risposta che diamo, la policy adeguata può variare completamente.

Gesto generoso, conseguenze giudiziarie.

Il computer potrebbe essere oggetto di una perquisizione. Per esempio: vostro figlio ha generosamente regalato un grammo di fumo a un amico che era al verde e che, dopo essersi fatto beccare, ha raccontato alla polizia dove l'ha preso. Di conseguenza vostro figlio viene penalmente considerato un trafficante di stupefacenti. Di qui la perquisizione.
In questo genere di situazioni, anche il vostro computer molto probabilmente verrà esaminato dalla polizia, mettendo così in pericolo l'obiettivo della confidenzialità. La gamma dei mezzi che verranno probabilmente impiegati va dalla Gendarmeria di Saint-Tropez, che accenderà il computer e cliccherà dappertutto, al perito giudiziario che esaminerà da molto più vicino l'hard disk. In compenso è improbabile che in questa situazione vengano utilizzati dei mezzi extra-legali, normalmente nelle mani dei Servizi e dei militari.

Furto.

Il computer potrebbe essere rubato durante un furto. Al contrario della polizia, i ladri non sanno molto che farsene dei vostri piccoli segreti.. e non vi denunceranno. Alla peggio potrebbero ricattarvi per recuperare i dati. E d'altra parte è improbabile che mettano in campo grandi mezzi per trovarli all'interno dell'hard disk.

Definire una policy di sicurezza. Ovvero..

POSSIBILI ATTACCHI E SOLUZIONI PRATICABILI

Adesso fatevi le domande di prima, mettendovi dalla parte dell'avversario.

Primo stadio: quando per vedere basta aprire gli occhi.

Tipo d'attacco più praticabile: montare l'hard disk su un altro computer, esaminarne il contenuto e

trovare tutti i vostri piccoli segreti.
Strumenti necessari: un altro computer, di cui il poliziotto di Saint-Tropez si servirà per trovare il più grande tra i vostri segreti; un perito giudiziario saprà invece anche ritrovare i file che voi credevate di aver cancellato; Nostradamus ne dedurrà la data di germinazione delle vostre semine.
Credibilità dell'attacco: alta.

Adesso adattiamo di conseguenza le vostre pratiche. Contro questo tipo di attacco cifrare l'hard disk è la risposta ovvia: installare e utilizzare un sistema cifrato è ormai relativamente semplice.

I passi per arrivarci saranno dunque:
Lanciare un sistema live per effettuare le operazioni che seguiranno in un contesto relativamente sicuro; salvaguardare temporaneamente, su un disco esterno o una penna USB cifrati, i file che devono sopravvivere

alla grande pulizia; espellere/smontare e staccare questo supporto di archiviazione esterno; cancellare “davvero” l’interno hard disk del computer. Installare un sistema operativo libero, precisando al programma di installazione di cifrare l’hard disk, compresa la memoria virtuale (swap). Copiare sul nuovo sistema i dati precedentemente salvaguardati. Fare il possibile per eliminare i file dal supporto esterno in modo “sicuro”, in modo da poter poi… Cancellare il contenuto dei file che si trovano sul supporto di backup temporaneo, che potrà eventualmente poi servire di nuovo.
In seguito, di tanto in tanto, fare in modo che i dati cancellati senza precauzioni particolari non siano recuperabili in seguito. Si dovrà anche assicurarsi di aggiornare il sistema regolarmente, per poter parare i “buchi di sicurezza” che potrebbero essere sfruttati dai software malevoli.

Per effettuare questi passi, nei prossimi capitoli vi forniremo le ricette giuste:

- cifrare un disco esterno o una penna USB;
- utilizzare un sistema live;
- archiviare dei dati;
- cancellare “davvero”;
- installare un sistema cifrato;
- mantenere aggiornato un sistema.

Se questa strada ci sembra praticabile, poniamoci di nuovo le stesse domande.

Secondo stadio: il cassetto del comodino non è cifrato

Tipo di attacco: una copia dei file che cerchiamo di proteggere potrebbe essere anche nella stanza accanto, nel terzo cassetto del comodino, su carta o su una penna USB.
Strumenti necessari: perquisizione, furto, o altre visite impreviste.
Credibiltà dell’attacco: alta, è esattamente da questo tipo di situazioni che cerchiamo di proteggerci in queste pagine.

Ancora una volta, dobbiamo renderci conto che una policy di sicurezza deve essere pensata nell'insieme. Senza un minimo di coerenza nelle pratiche, non serve a niente incaponirsi a usare password lunghe come un giorno senza pane. (espressione francese per indicare quanto il tempo passi lentamente senza cibo, in italiano si direbbe diversamente, ma l'espressione ci piaceva :) NDT)

E' quindi tempo di mettere in ordine le carte nel comodino e di ripulire tutte le penne USB, i CD e i DVD che contengono dati che ormai abbiamo deciso di cifrare:
archiviare su un supporto cifrato i dati da conservare; per le penne USB e gli hard disk esterni: cancellarne "davvero" il contenuto; per i CD e i DVD: distruggerli e sbarazzarsi dei residui; decidere cosa fare dei dati precedentemente salvati: copiarli sull'hard disk appena cifrato o archiviarli.

Terzo stadio: la legge come mezzo di coercizione

Tipo di attacco: la polizia ha il diritto di esigere che gli venga dato accesso alle informazioni cifrate, come abbiamo spiegato nel capitolo dedicato alla crittografia.
Strumenti necessari: una sufficiente perseveranza nelle indagini per applicare questa legge.
Credibilità dell'attacco: di nuovo, basta che la polizia pensi di poter trovare degli elementi di prova sul computer, ed esserne talmente convinta da volersi spingersi fin qua. Nell'esempio delle indagini che partivano dal grammo di fumo, è poco probabile, ma non impossibile.

Se la polizia arriva a esigere l'accesso ai dati cifrati, in pratica ci si dovrà porre la seguente domanda: le informazioni contenute nel computer mi faranno correre più rischi rispetto a quelli derivanti da un rifiuto di consegnare la password?

Insomma dipende da come ce la sentiamo. Cedere, in questa situazione, non rimette in discussione l'importanza della cifratura dell'hard disk: permette almeno di sapere cosa è stato rivelato, quando e a chi.

Detto ciò, può essere bene organizzarsi per vivere in modo meno critico una situazione come questa: il nuovo obiettivo potrebbe essere quello di avere un hard disk sufficientemente "pulito" in modo che non sia una catastrofe dover cedere di fronte alla legge, o nel caso in cui il sistema crittografico venga compromesso.

Come primo passo, spesso è possibile fare un compromesso riguardo all'accessibilità, almeno per i file che riguardano dei progetti finiti a cui non si ha bisogno di accedere spesso. Ne parleremo più avanti, riguardo all'esempio sull'archiviazione.

Successivamente, c'è tutta la questione della compartimentazione; anche se è effettivamente possibile aumentare globalmente il livello di sicurezza dell'insieme delle attività praticate.. questo potrebbe rivelarsi troppo faticoso.

Conviene quindi definire meglio i singoli bisogni, in termini di confidenzialità, delle diverse attività che svolgiamo. E a partire da questo, tirare le fila e decidere quali sono più "sensibili" delle altre e quali hanno bisogno di un trattamento di favore.

Il prossimo esempio studierà questi trattamenti di favore, ma abbiate pazienza, finiamo prima di parlare di questo caso.

Quarto stadio: in rete

Tutto quando detto finora vale per un computer disconnesso dalla rete. Nel momento in cui si connette, ci sono tutta una serie di altri attacchi immaginabili. Li studieremo nella seconda parte

della Guida (e nelle prossime puntate della sua traduzione italiana NDT).

Oltre ai problemi che abbiamo visto fin qui, rimangono ancora molti altri attacchi che possono minare la policy di sicurezza che avevamo definito.

Tipo di attacco: una falla nel sistema di cifratura

Come spiegato precedentemente, ogni sistema di sicurezza può rischiare di venire compromesso. Se l'algoritmo di cifratura usato viene violato, questa notizia farà probabilmente il giro del mondo, tutti lo sapranno e sarà possibile reagire.

Ma se quello ad essere compromesso è il modo in cui viene impiegato dentro al kernel Linux, non lo leggerete sul giornale ed è molto probabile che soltanto gli specialisti di sicurezza informatica ne saranno al corrente.
A meno che non abbiate modo di conoscere uno

di questi strani esseri, un modo di tenersi al corrente è quello di iscriversi alla mailing-list degli annunci di sicurezza di Debian (1). Le email ricevute da quel giro sono scritte in inglese, ma contengono l'indirizzo della pagina in cui si può trovarne la traduzione in altre lingue. La difficoltà poi è quella di riuscire a interpretarle..

Detto questo, anche se il sistema di cifratura fosse stato compromesso, bisogna comunque che anche gli avversari lo sappiano.. il poliziotto di Saint-Tropez non ne saprà niente, ma magari un perito giudiziario si.

Inoltre, entrando nel campo della fantascienza, ricordiamo che è difficile sapere in anticipo cosa hanno in mano, in materia, militari e agenzie governative come l'NSA.

NOTE:
1) Debian-security-announce:
https://lists.debian.org/debian-security-announce/

Tipo di attacco : cold boot attack

Abbiamo descritto il cold boot attack nel capitolo dedicato alle tracce che lasciamo in giro (vedi Guida in italiano #1 NDT)
Credibilità dell'attacco: per quello che ne sappiamo noi, questo attacco non è mai stato utilizzato dalle autorità, almeno in modo pubblico. La sua credibilità è quindi debole.

Può sembrare superfluo proteggersi contro questo attacco nella situazione che abbiamo descritto finora, ma è sempre meglio prendere da subito delle buone abitudini, piuttosto che avere brutte sorprese tra qualche anno. Quali abitudini? Eccone qualcuna che rende un po' più difficile questo attacco:
spegnere il computer quando non lo si usa; prevedere la possibilità di staccare la corrente facilmente e rapidamente: interruttori delle ciabatte accessibili facilmente, rimuovere la batteria del portatile quando è attaccato alla

corrente (in modo che basti staccare il cavo per spegnerlo); rendere più lungo e difficile l'accesso all'alloggiamento che contiene la RAM, per esempio incollandolo o saldandolo.

Tipo di attacco: occhi e videosorveglianza

Con il sistema di cifratura che ci siamo immaginati nel primo passo, la riservatezza dei dati confida sul fatto che la password venga mantenuta segreta. Se viene digitata davanti a una videocamera di sorveglianza, un avversario che abbia accesso a questa videocamera o alle sue eventuali registrazioni potrà scoprirla e poi usarla sul computer per avere accesso ai dati. Ancora più semplicemente, uno sguardo attento, dentro un bar, potrebbe cogliere la vostra password mentre la digitate.

Mettere in atto questo tipo di attacco necessita di tenere sotto sorveglianza le persone che utilizzano quel computer, fino a quando una di

loro digiterà la password all'interno del luogo sbagliato. Questa operazione può comportare diverso tempo ed è costosa.
Nell'esempio che stiamo studiando, un attacco così sarebbe pura fantascienza; attualmente sono poche le organizzazioni che possono mettere in campo mezzi così specifici, tranne che i diversi servizi speciali: anti-terrorismo, spionaggio industriale…

Per premunirsi da un tale attacco, conviene:
scegliere una password lunga, che rende molto complicato che un osservatore umano la memorizzi "al volo"; guardarsi intorno alla ricerca di eventuali occhi (umani o elettronici) indesiderabili, prima di digitare la propria password; nascondere la propria tastiera con l'aiuto dello schermo, nel caso di un portatile, o con un telo (1) (mantello, asciugamano…).

NOTE:
1) Nel film Citizen Four, si vede Edward Snowden

che si copre con una coperta mentre sta digitando la propria password.

Tipo d'attacco: la partizione non cifrata e il firmware

Come abbiamo già spiegato nel dettaglio, un sistema "cifrato" non lo è interamente: il piccolo software che all'avvio del computer ci chiede la password per decifrare il resto dei dati è, a sua volta, contenuto in chiaro sulla parte del disco che si chiama /boot. Un attaccante che ha accesso al computer può agevolmente, nel giro di qualche minuto, modificare questo software e installarci sopra un keylogger in grado di salvarsi la password e poi farsela inviare in rete o venire a prendersela più tardi.

Se questo attacco viene progettato per tempo, l'avversario potrà in seguito decifrare l'hard disk quando avrà di fronte il computer, durante una perquisizione, per esempio.

I mezzi impiegati in questo attacco sono, tutto sommato, abbastanza limitati: di base non occorre essere Superman per avere accesso per qualche minuto alla stanza dove risiede il computer.

Ciò nonostante, nel caso descritto in questo esempio, si tratterebbe ancora di pura fantascienza. Talvolta però la realtà ha la tendenza a superare la finzione..

Una protezione contro questo attacco è quella di tenere i programmi di avvio, tra cui questa piccola directory non cifrata (/boot), su un supporto esterno, ad esempio una penna USB, che verrà conservata permanentemente in un luogo più sicuro del computer. In questo caso ciò che va protetto non è la riservatezza di questi dati, ma la loro integrità. Questa prassi esige un buon numero di competenze e di rigore; non la approfondiremo in questa guida.
Queste pratiche alzano il livello, ma c'è un però:

una volta ottenuto l'accesso fisico al computer, se /boot non è accessibile né quindi modificabile, è comunque possibile effettuare lo stesso tipo di attacco sul firmware della macchina. E' leggermente più difficile, perché come farlo dipende dal modello di computer usato, ma è fattibile. Non conosciamo in questo caso nessun modo praticabile di proteggersi.

Tipo d'attacco: i software malevoli

Nelle puntate precedenti abbiamo capito che dei software installati a nostra insaputa su un computer possono rubare i nostri dati. In questo caso, un simile software è capace di trasmettere la chiave di cifratura dell'hard disk a un avversario… che così otterrà, grazie a questa chiave, l'accesso ai dati cifrati, quando avrà poi accesso fisico al computer.
Installare un software malevolo sul sistema Debian, di cui parliamo qui, richiede delle competenze di più alto livello rispetto agli attacchi

studiati finora, e anche più preparazione. Un attacco del genere, almeno nel caso della situazione di cui parliamo, è di nuovo fantascienza. In altre situazioni, bisognerà dare prova di una estrema prudenza riguardo alla provenienza dei dati e dei software che immettiamo nel computer, in particolare quando siamo connessi a Internet.. caso di cui, lo ricordiamo, non stiamo parlando in questa prima parte della guida.

Quando abbiamo parlato dell'installazione dei software abbiamo lanciato qualche consiglio utile sul come installare programmi in modo corretto. Più avanti, quando ci dedicheremo alla rete e a Internet in particolare, entreremo meglio nel dettaglio.

TIpo d'attacco: il brute force

Attaccare un sistema crittografico con il brute force, cioè cercare la password provando una per

una tutte le combinazioni possibili, è il più semplice, il più stupido e il più lento dei metodi. Ma quando non si possono mettere in atto altri tipi di attacco…

Per decifrare in questo modo un hard disk cifrato ci vuole moltissimo tempo (molti anni) e/o un'enormità di soldi e di competenze specifiche… se la password è solida.

Quello che possiamo dire, è che a priori, se un'organizzazione è disposta a investire tutte queste risorse per avere accesso ai vostri dati, preferirà di gran lunga mettere in atto uno degli altri attacchi elencati fin qui, meno costosi e altrettanto efficaci. Primo tra tutti quello di chiedere direttamente la password alla persona stessa, in modo più o meno cordiale..

Nel prossimo numero:
Ancora esempi: Lavorare su un documento sensibile - Archiviare un progetto finito...

Quello che avete tra le mani è il quarto numero della traduzione a puntate della Guide d'autodéfence numerique.
L'edizione originale integrale (in francese) è leggibile online e scaricabile liberamente qui:
http://guide.boum.org
Trovate invece le puntate precedenti della traduzione in italiano qui:
http://numerique.noblogs.org