Università di Pisa

Dipartimento di Informatica

Technical Report : TR-96-35

Sistema di protezione per il Dipartimento di Informatica

Vincenzo Ambriola, Claudio Telmon

October 25, 1996

ADDR: Corso Italia 40,56125 Pisa,Italy. TEL: +39-50-887111. FAX: +39-50-887226

Sistema di Protezione per il Dipartimento di Informatica technical report

Vincenzo Ambriola - Claudio Telmon
Dipartimento di Informatica
Università di Pisa

Maggio 1996

Sommario

In questo lavoro si descrive il progetto del sistema di protezione per il sistema informatico del Dipartimento di Informatica. Nella progettazione si è tenuto conto delle peculiarità di questo tipo di organizzazioni di ricerca. Si tratta di organizzazioni tradizionalmente aperte, il cui principale interesse consiste nella disponibilità delle risorse più che nella riservatezza dei dati trattati. Il progetto ha quindi come principale obiettivo la protezione di alcune risorse essenziali dalle quali è possibile ripristinare uno stato corretto sui principali sistemi del Dipartimento. Fa eccezione la sottorete amministrativa, per la quale devono essere garantite anche la riservatezza e l'integrità dei dati. Il progetto, completato nell'aprile 1996, è in fase avanzata di realizzazione.

1 Introduzione

La protezione di una rete connessa a Internet presuppone la valutazione e la definizione delle risorse da proteggere, del loro valore, delle funzionalità che la rete deve offrire agli utenti e degli attacchi ai quali la rete può essere sottoposta. Da una valutazione anche economica di questi fattori nasce la scelta della protezione più adatta.

Nella maggior parte dei sistemi di protezione attualmente realizzati, questa valutazione ha portato a ritenere valide alcune ipotesi:

- la riservatezza e l'integrità dei dati e delle risorse sono requisiti in generale più importanti della disponibilità delle risorse stesse; un esempio classico di questo approccio sono i criteri TCSEC, nei quali la riservatezza dei dati è il requisito fondamentale; spesso la disponibilità di Internet, vista come risorsa, è il requisito meno importante; l'approccio tipico è che nelle condizioni in cui non è sufficientemente sicuro accedere a Internet, l'accesso viene semplicemente impedito;

- è possibile imporre agli utenti della rete sia l'uso che possono fare di Internet e delle risorse in generale, sia il software da utilizzare sulle macchine che si intendono proteggere.

Queste ipotesi portano, di solito, a dividere le reti in due parti: la rete della quale si può garantire una protezione adeguata e la rete per la quale non si è in grado di garantire una sufficiente integrità e riservatezza dei dati. Mentre la prima viene protetta e ai suoi utenti si impongono norme più o meno restrittive sull'uso delle risorse, la seconda è quasi abbandonata a se stessa, o non viene connessa a Internet.

In molte organizzazioni di ricerca non profit (Non Profit Research Organization, in seguito NPRO), queste ipotesi non sono valide, per vari motivi:

- la riservatezza è uno dei requisiti meno importanti, in quanto la maggior parte delle attività di queste istituzioni è pubblica; il requisito più importante è la disponibilità delle risorse;
- Internet, vista come risorsa, è ormai indispensabile; l'idea di rinunciarvi in funzione di una maggior sicurezza è improponibile;
- la possibilità da parte degli amministratori della rete di imporre dei vincoli sull'uso delle risorse da parte dei ricercatori è molto limitata;
- gli utenti legittimi della rete sono fonte di buona parte dei problemi; un caso tipico sono gli studenti all'interno delle Università; le sanzioni sono un deterrente, ma di solito o non sono abbastanza severe, o non possono essere comminate.

In questo documento descriviamo innanzitutto le peculiarità delle NPRO dal punto di vista della sicurezza. Segue una panoramica delle tecniche attualmente disponibili per la protezione di una rete connessa a Internet. Esaminiamo poi l'uso di queste tecniche per la protezione della rete di una NPRO e, in particolare, il progetto del sistema di protezione per la rete del Dipartimento di Informatica dell'Università di Pisa. Infine esaminiamo gli aspetti da affrontare nella definizione di una politica di sicurezza, nonché la politica di sicurezza proposta per il Dipartimento di Informatica.

2 Protezione della rete di una NPRO

In questo contesto con "Non Profit Research Organization" indichiamo organizzazioni il cui scopo è la ricerca scientifica senza scopo di lucro, tipicamente per pubblica utilità. Esempi sono le Università e il C.N.R. Non consideriamo organizzazioni con esigenze particolari di sicurezza, quali ad esempio istituti che svolgono ricerche a fini militari.

2.1 Utenza

L'utenza della rete di una NPRO può essere divisa in quattro gruppi:

- ricercatori la cui attività riguarda direttamente Internet: questi ricercatori hanno la necessità di un accesso a Internet poco vincolato;
- ricercatori per i quali Internet è esclusivamente uno strumento: adottano strumenti standard per accedere a Internet, ma non si possono fare assunzioni sul software che usano sulle proprie macchine;
- altro personale dell'NPRO, come ad esempio il personale amministrativo: per questi è possibile imporre vincoli sull'uso della rete in funzione delle esigenze di sicurezza;
- personale esterno: rientrano in una delle precedenti categorie, con in più la necessità frequente di accedere alla rete locale dall'esterno e la difficoltà di comminare sanzioni quando necessario.

Inoltre, sia nelle università che in altre NPRO, utenti della rete sono anche studenti, che sono frequentemente fonte di problemi.

2.2 Utilizzo della rete da parte dell'utenza

Gli utenti della rete di una NPRO vogliono comunicare liberamente con gli altri utenti di Internet. Mentre in un'organizzazione commerciale gli obiettivi dell'azienda definiscono con chi e con quali modalità è lecito scambiare informazioni, nell'ambiente NPRO questa scelta è fatta in base alle necessità dei singoli progetti, gestiti autonomamente dai gruppi di ricerca. Inoltre è fondamentale condividere e scambiare le proprie conoscenze con altri ricercatori che hanno interessi comuni. Questo fa sì che non sia possibile definire a priori con chi avverranno le comunicazioni sulla rete. Non è possibile imporre metodi di autenticazione non standard, o sistemi di protezione che richiedano l'utilizzo di strumenti particolari per l'accesso alla rete.

Un'altra esigenza molto forte è quella di utilizzare gli strumenti più idonei alle proprie attività, sia in termini di accesso ai servizi offerti da Internet, sia di software installato sulle macchine. Non è proponibile, ad esempio, impedire l'utilizzo di determinati strumenti che l'utente ritiene necessari, per il solo fatto che le caratteristiche di sicurezza degli strumenti non sono state valutate. Si utilizzano così strumenti notoriamente insicuri, o utilizzati in modo palesemente insicuro.

Infine, nell'ambito di collaborazioni con enti esterni alcuni utenti accedono alle risorse locali da punti imprecisati di Internet, sulle cui caratteristiche di sicurezza non si hanno garanzie.

2.3 Esigenze di sicurezza

Le esigenze di sicurezza, per contro, sono limitate. La maggior parte dell'attività svolta all'interno di una NPRO è pubblica. Le esigenze, in termini di riservatezza sono ridotte. Fa eccezione la posta elettronica, per la quale è richiesta una ragionevole protezione. I progetti di collaborazione con enti esterni che richiedono la riservatezza di parte dei dati non sono abbastanza numerosi da poter imporre delle misure restrittive a tutti gli utenti in funzione delle esigenze di questi progetti.

Un'altra eccezione è il tentativo da parte di ricercatori di accedere al risultato del lavoro di altri, allo scopo di farsene attribuire indebitamente il merito. Ancora una volta, questo pericolo non giustifica misure restrittive per l'intera rete.

Anche le esigenze in termini di integrità dei dati sono limitate. Se vengono eseguiti backup regolari, si corre solo il rischio della perdita dell'attività di pochi giorni. Per quanto possa essere spiacevole questo evento, neppure questo giustifica, per ammissione di molti utenti, misure restrittive sull'uso delle risorse. Da questo punto di vista è più interessante riuscire a rilevare quanto prima possibile eventuali modifiche.

L'esigenza che gli utenti sentono maggiormente è invece la disponibilità continua delle risorse. Gli utenti sono sensibili agli attacchi di *denial of service*, o ad attacchi che danneggiano la configurazione delle macchine, nonché ad attacchi che comportano lunghi tempi di ripristino, ad esempio per riesaminare l'intera configurazione della macchina.

2.4 Esigenze degli amministratori della rete

Gli ammministratori della rete devono fornire i servizi di rete in modo efficiente e continuo. La disponibilità delle risorse è anche per loro l'esigenza principale, insieme alla riduzione dell'onerosità, in termini di tempo e di risorse, del ripristino da eventuali attacchi. Nella realizzazione di un sistema di protezione è necessario considerare inoltre il costo, in termini di tempo e risorse, che gli amministratori della rete sostengono per la normale gestione delle protezioni.

2.5 Tipologie di attacco frequenti

La rete di una NPRO è soggetta ad attacchi frequenti. Gli attacchi più comuni, almeno in Italia, sono poco sofisticati. Nella maggior parte dei casi sono ad opera di studenti universitari che utilizzano strumenti facilmente reperibili su Internet per raccogliere password, o che inviano messaggi di posta elettronica falsificando il mittente. Altri attacchi sfruttano difetti di configurazione delle macchine o di gestione delle *home directory* da parte degli utenti. Non sono ancora diffusi attacchi più sofisticati, anche se in questo ambiente un attaccante preparato può nascondere facilmente le proprie attività. Questa situazione è destinata a cambiare: in Italia la complessità degli attacchi è ancora bassa, ma si allineerà con quella di altri paesi in cui l'uso di Internet, particolarmente dal punto di vista commerciale, è più diffuso. Inoltre, l'introduzione di misure di sicurezza per le NPRO costringe gli attaccanti a utilizzare tecniche più evolute.

3 Protezione di una rete connessa a Internet

Questa sezione presenta le principali tipologie di difesa disponibili per fronteggiare gli attacchi a una sottorete connessa a Internet. La scelta del tipo di difesa è subordinata alla definizione di una politica di sicurezza che stabilisca il tipo e il valore delle risorse da proteggere, come definito nella sezione successiva. Esaminiamo in particolare le categorie di attacchi alle quali ci si può opporre efficacemente, e quali problemi presenta la messa in opera delle difese. Da questo punto di vista, oltre alle difficoltà tecniche, è particolarmente interessante esaminare le restrizioni che la difesa impone ai servizi offerti o utilizzati su Internet.

Per quanto riguarda la gestione della sicurezza di sottoreti da attacchi esterni, è importante individuare i punti di accesso alle sottoreti: i *router*, i *modem*, eventuali cavi di rete che transitino per ambienti non controllati. È infatti attraverso il traffico proveniente da queste connessioni che la rete può essere attaccata.

3.1 Protezioni a livello di sistema

Un primo approccio consiste nella protezione dei singoli sistemi. Essendo questi ultimi gli oggetti degli attacchi, una scelta può essere quella di concentrare su di essi la protezione. I passi da compiere per rendere sicuro un sistema generico sono:

- configurare correttamente il sistema; deve essere verificata l'assenza di errori di configurazione; le procedure di gestione del sistema devono essere definite e rispettate in modo da rendere l'introduzione di difetti un evento improbabile;
- mantenere aggiornata la configurazione del sistema, in particolare per quanto riguarda le nuove versioni del software installato;
- installare i *patch* di sicurezza per il software installato; i *patch* sono distribuiti dalle case produttrici e la loro disponibilità è pubblicizzata su Internet mediante apposite *mailing list*.
- eliminare i servizi di rete non utilizzati, per non offrire inutilmente dei punti di attacco dall'esterno;
- utilizzare meccanismi di *logging* delle operazioni significative dal punto di vista della sicurezza e, in particolare, degli accessi ai servizi di rete e delle operazioni effettuate;

- introdurre meccanismi di selezione delle entità di rete autorizzate a utilizzare i servizi; in particolare possono essere usati i *TCP Wrapper* [13], che hanno il compito di selezionare queste entità in base al nodo mittente; essi inoltre offrono funzionalità di *logging* più estese di quelle dei servizi che proteggono;
- utilizzare meccanismi di autenticazione delle entità che utilizzano i servizi di rete.

Per quanto riguarda l'autenticazione, i servizi possono essere divisi in due categorie: servizi disponibili a utenti selezionati e servizi pubblici.

I primi devono utilizzare delle forme di autenticazione adeguatamente robuste, fino eventualmente ad arrivare alla crittografia dell'intera sessione.

I secondi, quelli pubblici, devono utilizzare dei meccanismi di autenticazione compatibili con il protocollo standard previsto per il servizio. Per i servizi pubblici, o "anonimi" (ad esempio ftp anonimo) non è definito e autorizzato a priori un insieme ristretto di utenti. È però possibile utilizzare tecniche di autenticazione o metodi alternativi, generalmente deboli ma comunque utili, per verificare l'identità degli utenti. Esempi possono essere il *reverse DNS lookup*, l'uso del servizio *ident* o l'uso di autenticazioni basate su chiavi pubbliche certificate, utilizzate ad esempio con SSL [5] per la connessione fra client e server WWW.

Il vantaggio principale della protezione a livello di sistema è che, da molti punti di vista, le modifiche ai sistemi e alla sottorete sono relativamente poche. Molte di esse sono ragionevoli anche senza la connessione a Internet, in quanto fanno parte della corretta gestione di un sistema.

Gli svantaggi sono molteplici. Innanzitutto, questo approccio richiede un atteggiamento difensivo dei singoli sistemi nei confronti di tutti quelli che li circondano. Questo comporta dei meccanismi di autenticazione robusti e conseguentemente scomodi e complessi, anche nei confronti degli altri calcolatori della stessa sottorete. In particolare, numerosi servizi intrinsecamente insicuri, quali ad esempio le *r-utility* e NFS [12], non sono utilizzabili. Oltre a questo, le potenziali vulnerabilità della sottorete crescono con il numero dei sistemi connessi. Nonostante tutte le precauzioni, infatti, errori di configurazione o nel software possono comunque essere presenti.

La gestione della sicurezza è difficilmente centralizzabile, a meno che non si centralizzi l'amministrazione di tutti i sistemi. La presenza di amministratori locali fa sì che ad essi competa necessariamente la gestione di almeno alcuni aspetti della sicurezza dei loro sistemi (come minimo la corretta configurazione). Lo stesso vale per il monitoraggio dei sistemi. Bisogna infine sottolineare che questo approccio dipende strettamente dalle funzionalità offerte dai sistemi operativi utilizzati: se questi non permettono di limitare le attività degli utenti, difficilmente si può proteggere efficacemente il sistema.

3.2 Uso dei Firewall

Un approccio alternativo alla protezione dei singoli sistemi consiste nella difesa di un'intera sottorete. Si tratta di interporre tra la rete locale e Internet un sistema, il *firewall* [3], che ha il compito di gestire in modo sicuro il traffico tra le due reti; in particolare gestisce la selezione degli utenti ammessi dalla rete geografica e dei servizi offerti, l'autenticazione delle entità coinvolte in una connessione e il *logging* degli eventi significativi per la sicurezza della sottorete. Queste funzionalità possono essere offerte in modo più o meno completo e sicuro, in base alla sicurezza richiesta e alle funzionalità offerte dai sistemi della sottorete.

Un firewall può essere utilizzato per separare due o più reti, siano esse locali, geografiche o di entrambi i tipi. I vantaggi dell'uso dei firewall sono molteplici e derivano dall'introduzione di un punto di centralizzazione nella gestione della sicurezza. I vantaggi principali sono:

- definizione di funzionalità di autenticazione aggiuntive, per l'accesso all'intera sottorete o per l'uso di specifici sistemi o servizi;
- presenza, fra le due reti, di un sistema appositamente configurato e gestito per la sicurezza; le difese di questo sistema sono più robuste rispetto a quelle di un sistema generico; è possibile assegnare al firewall amministratori particolarmente preparati, o eventualmente specializzati in questo tipo di sistemi, o affidare la gestione a fornitori esterni del servizio; questa scelta rende meno grave la presenza sulla rete locale di macchine gestite da personale impreparato, problema particolarmente sentito in ambienti in cui è diffuso l'uso di *workstation* e *personal computer* gestiti dall'utente;
- esistenza di una separazione netta e riconoscibile tra la rete locale e la rete geografica, che permette di avere ambienti diversi fra le due e in particolare di avere un ambiente più collaborativo sulla rete locale; sulla rete interna è così possibile utilizzare protocolli che altrimenti sarebbero troppo rischiosi;
- il firewall è un sistema dedicato alla sicurezza; la sua configurazione è ottimizzata per questo scopo, senza servizi aggiuntivi o utenti, a parte quelli necessari per la manutenzione; la gestione è più semplice e più semplice è anche l'individuazione di variazioni nei file o nella configurazione;
- in caso di un attacco al quale, per qualche motivo, non si è in grado di opporsi, almeno temporaneamente, c'è sempre la possibilità di bloccare il traffico verso i servizi oggetto di attacco, pur mantenendo funzionanti sia la rete protetta, sia eventuali funzionalità minime non soggette all'attacco (ad esempio la posta elettronica).

L'installazione del firewall su un punto di centralizzazione già presente nella topologia della rete, ovvero la connessione fra due reti, rende trascurabile l'impatto sulle prestazioni delle due reti.

Le difese di un firewall possono comunque essere superate: un ambiente insicuro sulla rete difesa (d'ora in poi rete interna, in contrapposizione alla rete esterna che è quella dalla quale provengono gli attacchi) può esporre a gravi rischi in caso di attacco con successo al firewall. Si devono anche tenere in considerazione le necessità dei sistemi e dei loro utenti in termini di servizi offerti e richiesti dalla rete esterna: più l'accesso ai servizi è vincolato attraverso il firewall, minore è la fruibilità della connessione, sia in termini di servizi disponibili, sia in termini di facilità d'uso. Questo è particolarmente vero su Internet, una rete caratterizzata dall'offerta di servizi pubblici scarsamente modificabili in termini di protocollo e di interfaccia d'uso.

Infine, questo approccio non protegge la rete interna da attacchi che utilizzano accessi alternativi, come ad esempio un modem connesso a una macchina interna.

Esaminiamo adesso, in ordine crescente di complessità e di sicurezza, varie categorie di firewall.

3.3 Firewall a livello rete

Si tratta essenzialmente di protezioni realizzate tramite *router*. Il *router* è collocato nel punto di connessione fra due reti, dove si trova per gestire il traffico fra le due reti: è un candidato ideale per essere utilizzato come firewall. A questo scopo vengono utilizzate delle tabelle di filtraggio, definibili sulla maggior parte dei *router*. Queste tabelle, benché agiscano sui singoli pacchetti a livello rete (IP/ICMP su Internet), sono in grado di riconoscere il protocollo di livello trasporto (TCP/UDP su Internet) e di filtrare i pacchetti in base ad esso. I filtraggi sono definiti in termini di pacchetti ammessi o scartati secondo diversi parametri:

- Interfaccia di ingresso sul *router*
- Interfaccia di uscita dal *router*
- Indirizzo IP del mittente
- Indirizzo IP del destinatario
- Tipo di protocollo (ICMP, TCP, UDP)
- Tipo di pacchetto (Redirect, Host unreachable, ecc.) nel caso di pacchetti ICMP
- Porta mittente, nel caso di pacchetti UDP o TCP
- Porta destinatario, nel caso di pacchetti UDP o TCP
- Presenza del flag ACK, nel caso di pacchetti TCP

Per evitare gli attacchi descritti recentemente [1] è necessario scartare alcuni pacchetti IP frammentati il cui *offset* non soddisfa determinati requisiti. È un insieme piuttosto ampio di parametri, che seleziona le coppie (sistema, servizio) autorizzate a comunicare fra loro.

Il vantaggi di questo tipo di firewall sono:

- nessun costo aggiuntivo in termini di apparecchiature, perché il *router* è già presente;

- assoluta trasparenza delle regole di filtraggio, ovvero nessuna differenza di comportamento dei servizi dei quali è ammesso l'uso;
- stabilità delle prestazioni della connessione, a meno di regole particolarmente complesse.

I limiti e i difetti di questo schema sono però numerosi. Vediamo i principali:

- Le regole di filtraggio sono un meccanismo rigido e di difficile verifica. In particolare, le regole sono scandite nell'ordine in cui sono scritte. Non appena il pacchetto soddisfa una regola, la regola viene applicata e il pacchetto viene scartato o inoltrato. È necessario prestare molta attenzione alla struttura e all'ordinamento delle regole, tenendo presente che in tabelle complesse gli errori sono comuni.
- Non è prevista alcuna forma di autenticazione. Un servizio con un'autenticazione debole non migliora con la presenza del *router*.
- La selezione viene fatta in base agli indirizzi IP, in generale inaffidabili: non si è realmente in grado di distinguere fra diversi indirizzi della rete esterna.
- La selezione viene fatta in base ai sistemi e non in base ai singoli utenti. Questo tipo di selezione può facilmente risultare a grana troppo grossa per una rete con necessità di sicurezza.
- L'accesso ai sistemi interni è diretto: una volta che una connessione è stata accettata, i pacchetti arrivano direttamente alle porte dei sistemi destinatari, dove sono possibili molti tipi di attacco, ad esempio quelli basati sugli errori dei processi che gestiscono i servizi o sugli errori di configurazione.
- Alcuni servizi sono gestiti male con questo schema. In particolare, tutti i servizi non associati a una porta prefissata, come ad esempio quelli il cui indirizzo viene fornito da *portmapper*. Un caso difficile da trattare è il servizio FTP, in quanto la connessione dati è normalmente iniziata dal server verso una porta scelta dal client; connessioni FTP verso l'esterno richiedono di lasciare passare connessioni verso l'interno, originate dalla porta 20 ma destinate a una porta arbitraria. L'opzione PASV del protocollo FTP, che risolve questo problema, non sempre è supportata.
- Modifiche nella scelta delle coppie (indirizzo, porta) ammesse, sia in ingresso che in uscita, comportano la modifica delle tabelle del *router*. Questa necessità aumenta enormemente la possibilità di errori.
- I servizi che utilizzano il protocollo UDP sono di difficile gestione, in quanto il protocollo è *datagram* e non permette, ad esempio, di riconoscere le richieste provenienti dall'esterno (non autorizzate) dalle risposte a precedenti richieste dall'interno (autorizzate). Recentemente questo problema è stato affrontato dai firewall *stateful*, che ricordano le caratteristiche dei pacchetti UDP in uscita e abilitano, per un tempo limitato, l'ingresso dei corrispondenti pacchetti di risposta.

La difesa offerta da questo tipo di firewall può quindi essere estremamente lacunosa, a seconda del numero e del tipo di servizi offerti sulla sottorete interna.

3.4 Proxy generici

Si tratta di un tipo di firewall che si colloca a livello trasporto. In questo caso tra la rete interna e la rete esterna si interpone un sistema, tipicamente Unix, che accetta le connessioni utilizzando dei processi detti *proxy*. Questi processi, uno per ogni servizio accettato, effettuano alcune verifiche e, se la connessione risulta autorizzata, aprono a loro volta una connessione con il vero destinatario. Da questo momento fino alla chiusura della sessione, i *proxy* trasferiscono dati da una connessione all'altra. In letteratura i firewall che usano questo meccanismo sono chiamati "Firewall a livello di circuito".

Utilizzando questo metodo, è possibile svolgere controlli aggiuntivi rispetto a quanto offerto dal firewall basato sul *router*.

È possibile aggiungere un'autenticazione all'inizio della sessione. L'autenticazione può essere basata sull'utente, invece che sull'indirizzo, con due vantaggi:

- si può scegliere un protocollo di autenticazione robusto, anziché utilizzare gli indirizzi IP;
- si svincola l'utente dalla necessità di connettersi da una macchina specifica. Questa possibilità è particolarmente utile quando un utente della rete interna è in viaggio e deve connettersi al proprio sistema. In tal caso infatti non è prevedibile l'indirizzo IP dal quale viene iniziato il collegamento.

Bisogna però notare che può essere complesso inserire un'autenticazione aggiuntiva in una connessione aperta da un'applicazione che non prevede questa possibilità. Inoltre, poiché il servizio è mediato dal sistema, gli attacchi a livello più basso del livello trasporto (ridirezione di pacchetti, uso di pacchetti frammentati, *IP spoofing*) possono essere lanciati solo contro il firewall. Si suppone naturalmente che quest'ultimo sia configurato e gestito in modo da essere in grado di resistere. Si tratta comunque sempre di gestire attacchi su un unico sistema appositamente configurato, anziché su tutti i potenziali bersagli interni.

Dal punto di vista della configurazione poi, ogni servizio può essere gestito isolatamente, mediante tabelle o schemi in cui i diritti sono descritti in termini di utenti o connessioni e non di pacchetti. In tal modo la gestione è molto semplificata, riducendo la probabilità di errori.

Con questa tecnica è infine in parte possibile gestire anche servizi UDP, in quanto il *proxy* può conservare l'informazione relativa all'invio di una richiesta e all'attesa di una risposta. È altresì vero che un attacco portato fra l'invio della richiesta e la ricezione della risposta riuscirebbe probabilmente a passare. Inoltre non sarebbe possibile gestire servizi che restituiscono un numero arbitrario di pacchetti, in quanto il *proxy* non avrebbe l'informazione necessaria per riconoscere la fine della serie di pacchetti di risposta e chiudere l'accesso.

Con questo schema si perde però la maggior parte dei vantaggi del firewall basato sui *router*.

È necessario installare un sistema aggiuntivo, con un aumento dei costi della connessione. Nella maggior parte dei casi, il costo maggiore non è quello dell'hardware, bensì quello del software o più spesso ancora quello legato alle competenze necessarie per la sua corretta installazione, nonché il costo di gestione.

Le prestazioni della connessione possono essere degradate dalla necessità di gestire le connessioni con un hardware non specializzato, e a un livello più alto dell'abituale: tipicamente, al livello applicazione di un sistema Unix. Il dimensionamento del sistema che ospita il firewall diventa, in questo caso, critico. La gestione di linee veloci (attualmente alcune decine di Mbps) può essere impraticabile con questa tecnica.

Se si usa un meccanismo di autenticazione aggiuntivo sul firewall, è probabile che questo non sia previsto dal protocollo del servizio e che la presenza del firewall non sia più trasparente.

A seconda della tecnica con cui è realizzato il meccanismo di *proxy* può non essere più trasparente nemmeno l'indirizzamento: può essere necessario indirizzare le proprie connessioni al *proxy*, cioè al firewall, e poi fornire l'indirizzo del vero destinatario. La tecnica può essere implementata sia modificando i client delle applicazioni [9], con le difficoltà che ne conseguono, sia costruendo gli indirizzi in modo particolare, modificando il comportamento dell'utente. Ad esempio, invece dell'indirizzo *servizio@host* potrebbe essere necessario indicare *servizio@firewall* e poi *servizio@host*. La modifica del comportamento dell'utente non è necessariamente più semplice della modifica dei client delle applicazioni. Alcuni firewall di recente realizzazione, detti "trasparenti", superano questo problema, purché il firewall stesso sia configurato come *gateway* per le macchine interne. La realizzazione di questo tipo di firewall richiede modifiche estese della parte del sistema che gestisce il traffico di rete (in una macchina Unix, si tratta del nucleo del sistema operativo).

Anche con questa tecnica, numerosi tipi di attacco non sono in alcun modo contrastati: gli attacchi al protocollo dei servizi, quelli ai difetti di configurazione e agli errori del codice dei programmi che implementano i servizi si collocano a un livello più alto del livello trasporto e sono trasmessi come semplici dati dai *proxy* generici.

3.5 Proxy specifici

Molti limiti del meccanismo appena descritto derivano dalla mancanza da parte dei *proxy* di conoscenze sintattiche e semantiche dei protocolli dei servizi di cui gestiscono le connessioni. È ragionevole sostituire i *proxy* generici con *proxy* specifici per i singoli servizi. I firewall che usano questo meccanismo sono chiamati "Firewall a livello applicazione". Questo modello offre vari vantaggi.

È possibile verificare la correttezza sintattica e, in parte, semantica dei protocolli. Mentre la verifica sintattica può essere approfondita, i controlli semantici sono limitati da due fattori: le prestazioni e, soprattutto, la complessità del codice necessario per i controlli. Una complessità eccessiva del codice può infatti introdurre più errori e difetti di quanti ve ne fossero nell'implementazione originale del servizio.

È inoltre possibile utilizzare meccanismi di autenticazione diversi per servizi diversi, in modo da ridurre l'impatto sul protocollo del servizio. È inoltre più facile gestire gruppi di utenti diversi per servizi diversi, o adottare politiche diverse per i servizi pubblici rispetto a quelle utilizzate per i servizi critici.

Data la conoscenza sintattica e semantica dei protocolli, è possibile trattare anche protocolli senza connessione, come ad esempio i servizi basati su UDP.

I *proxy* specifici possono essere utilizzati anche per compiti di controllo non strettamente legati alla sicurezza. Ad esempio possono essere utilizzati per attività di *logging* o *accounting* o per limitare la banda disponibile per determinate applicazioni.

È possibile infine limitare l'uso di un servizio. Un esempio significativo è l'inclusione di *applet* Java in documenti HTML. Gli *applet* sono al momento considerati un problema per la sicurezza delle reti protette da firewall. Invece di basare la sicurezza della rete sulla disabilitazione delle funzionalità Java in ogni singolo client installato, è possibile impedire il trasferimento degli *applet* attraverso il proxy.

Gli svantaggi di questo approccio, rispetto al precedente, sono più di carattere gestionale che di sicurezza.

Le prestazioni sono, in generale, peggiori. Si tratta infatti di applicazioni notevolmente più complesse, che esaminano nel dettaglio i dati in transito, invece di trasmetterli semplicemente. È necessario dimensionare correttamente il sistema utilizzato come firewall.

L'assenza di un *proxy* specifico per un servizio implica l'impossibilità di usare il servizio. Non è infatti ragionevole utilizzare meccanismi di sicurezza più robusti per un servizio e più deboli per un altro, a parità di pericolosità. Vale in questo caso il principio: "Una catena è robusta quanto il suo anello più debole". Lo stesso problema si presenta con le nuove versioni di un protocollo, o con servizi in rapida evoluzione, quale ad esempio HTTP [7].

I *proxy* specifici, se correttamente realizzati, contrastano la maggior parte dei tipi di attacchi ai servizi, sempre supponendo che il firewall sia a sua volta correttamente realizzato, configurato e gestito. Questa condizione è tutt'altro che facile da verificare e nella pratica i firewall possono presentare difetti di configurazione che ne limitano l'efficacia. Questa situazione è forse ancora più pericolosa dell'assenza del firewall, in quanto crea una sensazione di sicurezza che porta a ridurre le difese sulla rete interna. Un attacco che riuscisse ad approfittare del difetto del firewall troverebbe un ambiente ancora più indifeso.

Uno dei motivi per cui un firewall è meno robusto di quanto potrebbe, è l'esigenza di trovare un compromesso tra i requisiti di sicurezza e la comodità e fruibilità dei servizi di rete. Questa esigenza non deve portare a far passare dal firewall servizi troppo insicuri. È comunque importante che questo equilibrio sia definito e stabilito prima della progettazione e installazione del firewall, per evitare in seguito modifiche arbitrarie e dall'effetto imprevedibile. Questo e altri aspetti sono affrontati nella definizione della politica di sicurezza. Anche con un firewall a livello applicazione realizzato in modo corretto rimangono alcuni gravi problemi.

- Errori nel codice dei processi che gestiscono i servizi permettono attacchi che sfruttano messaggi assolutamente corretti dal punto di vista sintattico e semantico. Questi messaggi possono superare senza difficoltà le difese del firewall.
- Lo stesso vale per i difetti di configurazione della macchina interna su cui è fornito il servizio: un uso corretto del sistema potrebbe sfruttare dei diritti eccessivi per attaccare il sistema. Questo problema è comune nel caso di server FTP e WWW.
- In alcuni casi può essere troppo rischioso concedere agli amministratori del firewall il controllo degli accessi alla sottorete. A seconda del valore dei dati da proteggere, si può temere che essi stessi riducano la sicurezza del sistema; è lo stesso problema che si presenta quando si consegna a singole persone la combinazione di una cassaforte contenente materiale di grande valore.

3.6 Firewall a più livelli

Alcuni dei problemi rimasti insoluti con l'introduzione dei firewall a livello applicazione possono essere affrontati utilizzando più sistemi in serie sulla stessa connessione. Non si tratta di ripetere più volte la stessa configurazione, per non ripetere gli eventuali errori o difetti. Si tratta invece di utilizzare una configurazione in cui i vari sistemi si integrano per formare un unico firewall più robusto.

Le configurazioni possibili sono numerose. Una delle più diffuse è detta *screened subnet*, descritta in figura 1. Uno dei concetti utilizzati in questa configurazione è quello della cosidetta DMZ, "*DeMilitarized Zone*", termine piuttosto criticato con cui si indica una sottorete connessa in un punto intermedio delle difese della rete privata. Le macchine nella DMZ non si trovano nè al di fuori delle difese, dove potrebbero essere attaccate con grande facilità, nè all'interno, dove potrebbero risultare troppo pericolose, ad esempio perché offrono servizi pubblici. Se la DMZ è realizzata con la dovuta cura, si possono proteggere effettivamente i servizi pubblici senza mettere eccessivamente a repentaglio la sicurezza della rete interna. Verso la parte più interna del firewall non passerebbero più connessioni per servizi pubblici, ma solo connessioni per servizi autenticati in modo adeguato.

Un'altra possibilità offerta dai firewall a più livelli consiste nell'affidare a diversi amministratori la gestione di diversi sottosistemi, rendendone necessaria

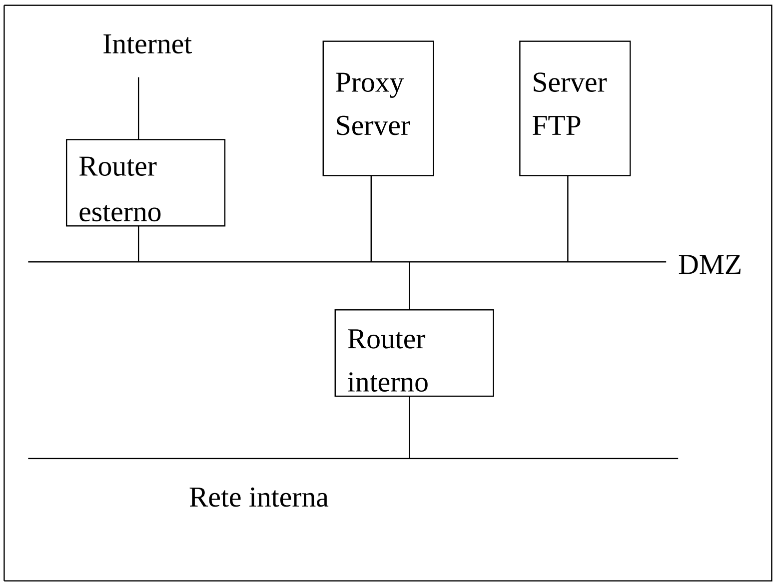

Figura 1. Schema di screened subnet

la coazione per superare il firewall. Questo uso è analogo alla necessità di più chiavi, affidate a persone diverse, per aprire la porta di una cassaforte.

3.7 Correttezza della realizzazione di un firewall

Dato che il firewall deve proteggere l'intera sottorete, è evidente l'importanza di realizzarlo e configurarlo in modo corretto. L'unico scopo del firewall è gestire in modo sicuro il traffico tra le due reti e questa caratteristica può essere sfruttata per utilizzare sistemi operativi con funzionalità ridotte e con vincoli aggiuntivi sull'attività degli utenti; in un firewall, queste limitazioni sono un vantaggio.

L'approccio più diffuso consiste nella realizzazione di sistemi quanto più semplici possibile. In particolare, si dà molto peso all'eliminazione di tutti i processi eseguiti con diritti di superutente, quando questi diritti non sono assolutamente necessari, nonché alla sostituzione o eliminazione di applicazioni che offrono funzionalità non indispensabili. Inoltre, i programmi con diritti di superutente o che offrono servizi all'esterno sono posti in un ambiente circoscritto e quanto possibile ridotto, ad esempio mediante l'uso della funzione *chroot* dei sistemi Unix.

Un approccio diverso consiste nell'utilizzo di un sistema operativo appositamente realizzato per operare in ambienti con elevate esigenze di sicurezza. Ad esempio, si usano tecniche quali Multi Level Security o Domain Type Enforcement [14].

Tuttavia, la complessità introdotta da questo approccio può favorire l'introduzione di errori nell'implementazione dei meccanismi di controllo. Firewall che

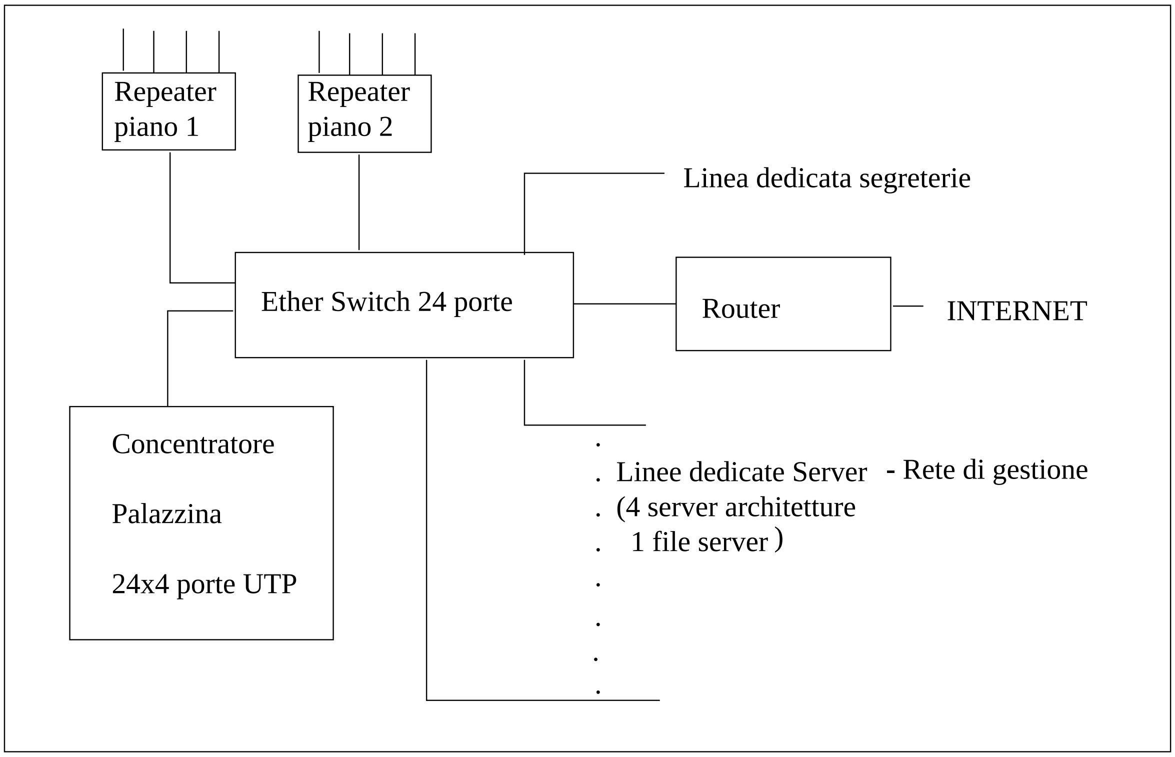

Figura 2. Schema della rete dipartimentale

fanno uso di queste tecniche sono disponibili da poco tempo, e non sono disponibili dati sulla loro reale efficacia.

Esiste infine il problema del test dell'installazione. Ogni firewall viene installato in un ambiente diverso e la sua configurazione deve essere adattata per il singolo caso: nasce la necessità di verificarne la correttezza. La richiesta in questo senso è grande, ma non sono attualmente disponibili strumenti di uso generale.

4 La rete del Dipartimento di Informatica

Il Dipartimento di Informatica dell'Università di Pisa è un caso tipico di NPRO. In questa sezione se ne descrivono le caratteristiche.

4.1 Topologia

La rete del Dipartimento di Informatica sta subendo alcune modifiche dovute alla ristrutturazione di un'ala dell'edificio e all'introduzione di uno switch Ethernet e di un fileserver. La topologia prevista al termine dei lavori è descritta in figura 2. Dal punto di vista funzionale si individuano in particolare:

- una sottorete amministrativa, formata dai segmenti ai quali sono connesse le macchine della segreteria amministrativa e della segreteria didattica;
- una sottorete di gestione, alla quale sono connesse le macchine dei sistemisti e quelle che forniscono i servizi per la gestione della rete;
- una sottorete per i servizi critici, composta dalle macchine che offrono servizi la cui compromissione è particolarmente grave dal punto di vista della sicurezza (NIS, DNS e distribuzione delle configurazioni).

Il router, i repeater, i server principali e le macchine dei sistemisti sono nello stesso locale, con l'eccezione dei repeater del primo e secondo piano, e i segmenti associati alle diverse sottoreti sono per la maggior parte ben riconoscibili.

Alla rete sono connesse macchine molto eterogenee, la cui classificazione completa esula dalle finalità di questo documento. Le architetture relative alle sottoreti amministrativa e di gestione sono:

- Sottorete amministrativa: collega personal computer con architettura Apple Macintosh o DOS/Windows.
- Sottorete di gestione: collega workstation Unix con architettura SUNOS, Solaris, Linux e AIX. È prevista la possibilità di utilizzare altre architetture per le attività di sviluppo e di configurazione dei pacchetti da rendere disponibili alle altre macchine del Dipartimento.

4.2 Servizi

I servizi pubblici, intendendo con questo i servizi offerti a utenti esterni al Dipartimento, sono i seguenti:

- Servizio WWW; gli utenti della rete possono gestire un proprio spazio all'interno del servizio; lo spazio utenti è gestito attraverso il servizio NFS; gli utenti del Dipartimento non accedono alla macchina WWW per aggiornare il loro spazio.
- Servizio FTP; gli utenti della rete possono gestire un proprio spazio all'interno del servizio. A questo scopo agli utenti vengono assegnate proprie directory, delle quali perciò gli utenti possono modificare i diritti, o all'interno delle quali possono essere create sottodirectory con diritti diversi.
- Servizio DNS per la gestione del dominio locale.
- Servizio di posta elettronica (SMTP). La gestione del servizio è centralizzata.
- Servizio finger, centralizzato.
- Un caso particolare di servizio "offerto all'esterno" è la gestione degli account, svolta con un'apposita procedura dal dominio cli.di.unipi.it; questa necessità è motivata dalla gestione centralizzata degli account della rete dipartimentale e del Centro di Calcolo Didattico.

Altri servizi sono disponibili in modo distribuito sulle singole macchine della rete, in modo variabile a seconda dell'architettura e della configurazione:

- Servizio talk, disponibile sulla maggior parte delle macchine Unix.
- Servizio X Windows, disponibile sulla maggior parte delle macchine Unix.

I servizi locali sono quelli destinati ai soli utenti della rete dipartimentale:

- Servizio NIS per la gestione dell'autenticazione e degli account.
- Servizio NFS per la condivisione di file system fra macchine. In particolare, buona parte dei file "di sistema" per le diverse architetture Unix e delle applicazioni più comuni è gestito con questo servizio.
- Servizio per la gestione dei backup, centralizzato, realizzato attraverso il package Amanda.
- Servizio per la gestione della posta elettronica. La ricezione dei messaggi non è fatta localmente sulle singole macchine: gli utenti accedono ai propri messaggi montando tramite NFS l'apposito file system. I sistemi che non sfruttano questa opzione, ad esempio le macchine Macintosh, usano il servizio POP.
- Servizio di stampa distribuito: gli utenti possono utilizzare una qualsiasi stampante del Dipartimento, in funzione della comodità e della qualità di stampa.
- Servizio di aggiornamento delle configurazioni locali, eseguito tramite rdist.
- Un indirizzo di posta elettronica al quale rivolgersi per interazioni con i sistemisti.

Su alcune macchine sono poi offerti altri servizi, principalmente attraverso l'RPC portmapper.

4.3 Gestione

La gestione della rete è centralizzata, e in particolare la gestione dei servizi di rete e degli accessi. Non è permessa la creazione di account locali sulle macchine in rete.

La configurazione delle macchine è, per quanto possibile, centralizzata. Le configurazioni base, nonché le applicazioni più comuni, sono distribuite tramite NFS. Gli altri aspetti della gestione delle macchine sono affidati ai responsabili delle singole macchine.

La gestione delle macchine è affidata a responsabili nominati dai gestori dei singoli progetti. Nel momento in cui le macchine sono connesse alla rete del Dipartimento però, devono essere accettate alcune norme e alcuni principi. Particolarmente rilevanti sono:

- la gestione centralizzata degli account, che comprende anche la durata e il rinnovo;

- l'offerta di servizi in rete, che deve essere autorizzata e concordata con l'amministrazione della rete;
- l'utilizzo della rete per soli scopi di ricerca; questo anche in conseguenza del fatto che la connessione a Internet è fatta tramite il GARR, che a sua volta impone le stesse limitazioni.

Per il resto, i vincoli imposti agli utenti da politiche di gestione sono molto limitati e riguardano principalmente azioni che possono ridurre la disponibilità di servizi per altri utenti. In pratica, non essendo attualmente in corso alcun tipo di sperimentazione sui protocolli di rete fino al livello 4 (trasporto), la possibilità di interferire con altri utenti è limitata al livello dei servizi. Per quanto riguarda la sicurezza, le uniche norme esplicite riguardano il divieto di eseguire azioni manifestamente ostili, nonché l'obbligo di mantenere personale l'uso dell'account, obbligo che si concretizza nella segretezza della password. Non ci sono vincoli sull'uso di file .rhosts, a parte la cessione esplicita dei diritti ad altri utenti, e neppure per quanto riguarda i diritti su file e directory. L'utenza ha una notevole libertà nell'uso delle risorse, come d'abitudine in queste strutture.

La manutenzione dell'hardware è effettuata da ditte esterne. La manutenzione del software è invece effettuata dal personale interno, almeno per quanto riguarda i sistemi interessanti dal punto di vista della sicurezza.

4.4 Requisiti di sicurezza

Si sono individuate le diverse esigenze di sicurezza delle quattro sottoreti:

- Sottorete amministrativa. Su queste macchine è richiesta una sicurezza elevata, in quanto conservano dati dell'amministrazione del Dipartimento, la cui modifica può causare notevoli disagi o danni, nonché dati personali la cui protezione è o sarà richiesta dalle normative in materia di protezione delle banche dati.
- Sottorete per i servizi critici. Queste macchine richiedono una buona protezione, in quanto la loro compromissione influenza potenzialmente l'intera sottorete e rende complesso il ripristino di uno stato corretto dopo un attacco.
- Sottorete di gestione e sviluppo. Le esigenze di sicurezza sono analoghe a quelle della rete dei servizi critici, ma con l'ulteriore necessità di operare agevolmente sulla totalità della rete dipartimentale.
- Altre macchine. Per le altre macchine non sono richieste protezioni dal punto di vista della riservatezza, a parte la posta elettronica. L'interesse maggiore è per la disponibilità delle risorse e la possibilità di ristabilire rapidamente uno stato corretto dei dati e delle risorse stesse; per quanto riguarda i dati si è ritenuto sufficiente il servizio di backup esistente; questa scelta lascia vulnerabili le macchine per le quali questo servizio non viene fornito ma, secondo le statistiche disponibili sugli attacchi in rete, per queste

macchine è comunque più probabile la perdita dei dati per errori degli utenti o guasti dei sistemi: se il servizio dump non è ritenuto necessario per questi eventi, non lo è neppure per la gestione degli attacchi. Unica eccezione possono essere i server di alcuni servizi, come ad esempio il mailserver, del quale può essere maggiormente curata la sicurezza a livello di singolo sistema.

Uno degli obiettivi principali dell'attuale gestione della rete è la tolleranza ai guasti. L'introduzione di sistemi di protezione deve quindi evitare, per quanto possibile, l'introduzione di punti critici da questo punto di vista. I meccanismi di protezione in progetto hanno lo scopo di rendere più agevole e veloce il recupero dell'operatività in caso di incidenti di sicurezza. Sarebbe in qualche modo contrario a questi obiettivi rendere più difficile l'attività dei gestori della rete. L'introduzione dei meccanismi di protezione non deve rendere eccessivamente onerosa o macchinosa la gestione della rete rispetto alla situazione attuale. Unica eccezione sono le macchine della sottorete amministrativa, per la quale invece lo scopo principale è una buona protezione dei dati e per la quale è ammissibile una gestione meno agevole.

4.5 Servizi utilizzati

È utile individuare i servizi utilizzati sulle sottreti amministrativa e di gestione, in quanto devono essere gestiti correttamente dal sistema di protezione.

Sottorete amministrativa I servizi effettivamente necessari e utilizzati sono la posta elettronica, attraverso il servizio POP, il servizio FTP e il servizio HTTP. Attualmente viene utilizzato anche il sistema di filesystem distribuito, ma la sostituzione di questa funzionalità con il solo FTP non presenta difficoltà.

Sottorete per la gestione Sono utilizzati numerosi servizi. Tra essi, telnet, FTP, WWW (HTTP/gopher/FTP) hanno caratteristiche di sicurezza note che possono essere affrontate con gli strumenti tipici per essi. Un esame particolare è invece richiesto per gli altri servizi.

- NFS: è un servizio estremamente insicuro. L'uso di NFS per importare/esportare file system deve essere bloccato. L'uso del mirror rende inutile questa possibilità.
- X Windows: è un servizio insicuro e rischioso, a causa della cattiva autenticazione e della possibilità, avuto accesso al server, di interferire con la gestione dello schermo, della tastiera e del mouse. Il servizio è però indispensabile per i sistemisti: senza di esso la gestione della rete diventa più scomoda, lenta e macchinosa, in contrasto con l'obiettivo di ottenere, grazie alla maggiore sicurezza di parte della rete, un migliore servizio per la rete dipartimentale nel complesso. Il servizio deve essere offerto, cercando di

renderlo quanto più sicuro possibile. Anche per questo, però, la sottorete di gestione non può essere considerata del tutto sicura.

- Servizio Amanda per la gestione dei backup. È un servizio in fase di beta-test, le cui caratteristiche dal punto di vista della sicurezza non sono ancora ben note. Alcune caratteristiche, come ad esempio l'uso di pacchetti UDP, lo rendono di difficile gestione dal punto di vista dell'attraversamento dei firewall. Poiché è utilizzato per eseguire il backup di macchine insicure, ci si preoccupa principalmente di impedire che attraverso questo servizio possa essere compromessa la sicurezza della sottorete di gestione, più che di garantire l'autenticità e la correttezza dei dati registrati. Questo comporta un'accorta configurazione del servizio e un attento esame delle procedure per il suo utilizzo.
- Accesso via modem dall'esterno. Questa attività è normale per gli amministratori della rete. Sono quindi forniti uno o più modem su una delle macchine della sottorete di gestione con meccanismi di autenticazione robusti. Il rischio di manipolazione della connessione telefonica è considerato trascurabile in questo contesto.

5 Architettura del sistema di protezione

Nella realizzazione del sistema di protezione per la rete di una NPRO, quale è la rete dipartimentale, si devono considerare le esigenze specifiche di queste organizzazioni, per individuare quali delle tecniche descritte possono essere utilizzate in modo efficace. Esaminiamo alcune soluzioni possibili, descrivendo poi quella proposta.

I problemi legati a un approccio basato sulla protezione dei singoli sistemi sono evidenti in una rete NPRO. In particolare, la difficoltà nel controllare la gestione e l'utilizzo delle singole risorse fa sì che questa soluzione sia impraticabile. È tuttavia la soluzione più diffusa all'interno delle NPRO: chi ha esigenze di sicurezza le gestisce isolatamente, spesso al prezzo di un isolamento quasi totale dal resto della rete e di Internet.

Un firewall fra la rete locale e Internet è la soluzione più sicura per quanto riguarda il controllo degli accessi da Internet. In una NPRO però, i difetti di questa soluzione sono evidenti:

- è difficile offrire una vera protezione alla rete senza imporre agli utenti forti restrizioni sull'uso di programmi e sul controllo degli accessi concessi a utenti esterni;
- si riduce fortemente la disponibilità della risorsa Internet;
- una parte dei problemi sono causati da utenti interni; per questo problema questa protezione è del tutto inutile.

Abbiamo così deciso di considerare un approccio diverso, che offra una sicurezza minore dal punto di vista della riservatezza e dell'integrità, ma che garantisca un'elevata disponibilità delle risorse. In particolare, vogliamo ridurre al minimo i tempi di ripristino dopo un incidente. In più, parti della rete che richiedono un livello di sicurezza maggiore devono essere protette con misure più efficaci dal punto di vista della privacy e dell'integrità. Un esempio di questa esigenza sono le macchine dell'amministrazione.

L'obiettivo del sistema di protezione proposto è difendere alcune risorse essenziali, dalle quali ripristinare rapidamente e con facilità uno stato corretto degli altri sistemi della rete. Queste risorse sono la sottorete per la gestione e una macchina, chiamata "macchina delle configurazioni", sulla quale vengono conservate delle versioni corrette e aggiornate dei file necessari per il corretto funzionamento delle macchine della rete dipartimentale: sistema operativo, file di configurazione e pacchetti software.

Queste risorse sono separate dal resto della rete da un firewall, che le protegge sia dall'esterno che da eventuali macchine compromesse sulla rete locale. Un fileserver, posto all'esterno del firewall, viene utilizzato per distribuire il package e i file di sistema delle macchine gestite dagli amministratori. Il fileserver viene gestito e aggiornato dalle macchine poste dietro il firewall, utilizzando connessioni sicure.

Delle risorse protette dal firewall è garantita l'integrità, che permette di avere sempre a disposizione dati corretti da trasmettere al fileserver.

Sulla rete non protetta dal firewall è previsto un sistema per il monitoraggio del traffico, con lo scopo di individuare traffico sospetto o chiaramente ostile.

Anche la sottorete amministrativa è protetta da tutte le altre sottoreti, sempre sfruttando il firewall.

Con questo approccio, la rete della NPRO resta aperta a un gran numero di attacchi. Solo occasionalmente il sistema di monitoraggio sarà in grado di prevenirli, mentre più frequentemente dovrebbe essere in grado di rilevarli. Non essendovi risorse di grande valore sulla rete, una volta individuato un attacco in corso la politica non prevede necessariamente il blocco immediato e il successivo ripristino della situazione corretta. Si potrà invece passare a uno stato in cui il monitoraggio della rete è più attento e mirato, per individuare le tecniche e gli strumenti utilizzati dall'attaccante e, se possibile, localizzare l'attaccante stesso, collaborando con i gestori dei siti da cui provengono gli attacchi e se necessario con le autorità di pubblica sicurezza. Una volta raccolte le informazioni interessanti, anche per stabilire come agire per evitare il ripetersi dello stesso tipo di attacco, si potrà bloccare l'attacco stesso e ripristinare una situazione corretta.

5.1 Efficacia del sistema

È necessario innanzitutto sottolineare che questo approccio garantisce comunque un'adeguata protezione per risorse che la richiedano esplicitamente: eventuali progetti che richiedano protezione dal punto di vista dell'integrità e della riservatezza possono essere posti a loro volta su una sottorete protetta dal firewall. In questo caso, però, avendo richiesto esplicitamente una protezione, gli utenti di questa sottorete sono tenuti a rispettare tutti i vincoli necessari per garantire la sicurezza delle loro risorse.

Per quanto riguarda le macchine senza esigenze particolari, se non la disponibilità delle risorse, si prevedono misure di protezione che non interferiscano con l'utilizzo normale della rete (filtraggi sul router, corretta configurazione delle macchine e dei servizi) e un monitoraggio che individui le attività anomale.

Il monitoraggio individua gli attacchi più comuni e pericolosi, per stabilire quali aspetti della sicurezza della rete è urgente migliorare. Questi miglioramenti sono effettuati senza modificare la struttura generale del sistema di protezione. È possibile che la necessità di alcuni miglioramenti si riveli immediata; un esempio può essere l'uso di password ripetibili. Qualora si decidesse di eliminarle, la storia degli attacchi riusciti basati su questo problema può aiutare nell'affrontare un passo così drastico.

La rete per la gestione si trova in una situazione intermedia; è protetta, ma l'elevata interazione con la rete non protetta e il possibile utilizzo di servizi insicuri, o la cui sicurezza non è stata accertata, non ne esclude la compromissione in caso di attacchi sofisticati. Questo giustifica la necessità di proteggere ulteriormente la macchina sulla quale sono conservate le configurazioni. È vero che le configurazioni possono essere aggiornate, e quindi compromesse, dalla rete di gestione. Questo passaggio permette di accedere però solo a un ambiente limitato. La configurazione della macchina stessa non può essere modificata, e quindi non ne possono essere ridotte le funzionalità di logging. È possibile stabilire quale dei suoi backup può essere utilizzato senza rischio.

Il rapido ripristino di uno stato corretto sulle macchine della rete del NPRO evidenzia il ruolo essenziale della macchina delle configurazioni e del fileserver. Il fileserver è una macchina esposta, ma la sua configurazione può essere ripristinata rapidamente dalla macchina protetta. Dal fileserver è poi possibile ripristinare in modo altrettanto veloce la configurazione delle altre macchine della rete, il vero obiettivo del sistema di protezione.

5.2 Implementazione dello schema proposto

Lo schema concettuale che si intende realizzare è indicato in figura 3. È una configurazione con diversi livelli di sicurezza per le diverse sottoreti. Per quanto riguarda la sottorete di gestione/sviluppo, è essenzialmente una configurazione con "*dual homed bastion host*", ovvero un sistema connesso a due sottoreti che gestisce il traffico mediante proxy, non permettendo il passaggio diretto di pacchetti a livello rete. Per quanto riguarda invece i sistemi posti dietro il router interno (rete amministrativa e macchina delle configurazioni), è un firewall di tipo "*screened subnet*", in cui il bastion host non è semplicemente connesso alla rete intermedia, ma opera su di essa come un dual homed bastion host (vedi sopra). Questo schema è indicato spesso come "*belt and suspenders*".

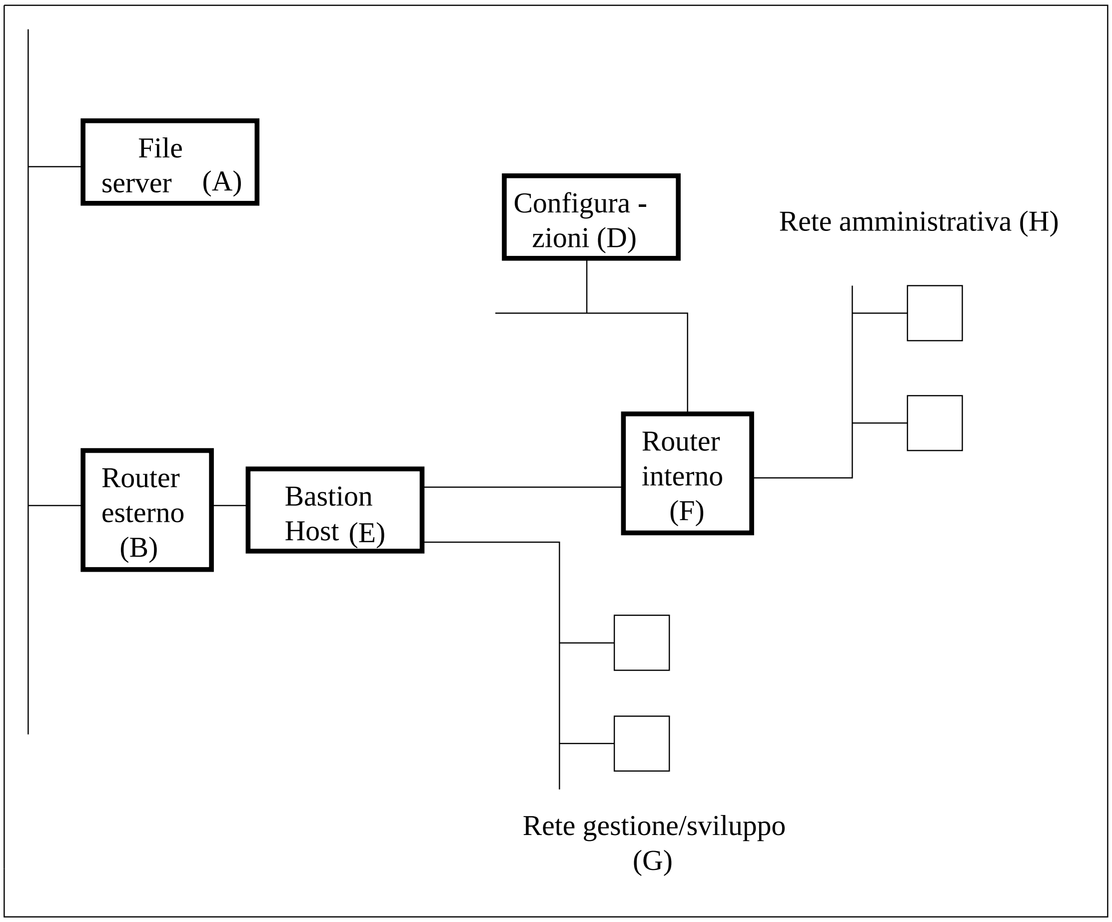

Figura 3. Schema concettuale del sistema di protezione

In pratica il router esterno è integrato con il bastion host, in quanto ha principalmente lo scopo di proteggere il bastion host dalla falsificazione di indirizzi IP e questo può essere ottenuto con strumenti software. Questa scelta ha anche il vantaggio che, dal punto di vista della sottorete amministrativa e della macchina delle configurazioni, la sottorete di gestione e sviluppo si può considerare completamente al di fuori del firewall e quindi le protezioni anche nei confronti di questa possono essere uguali a quelle nei confronti di Internet.

Questa configurazione comporta l'utilizzo di indirizzi di rete diversi per le varie sottoreti. Per le sottoreti protette si utilizzano indirizzi non annunciati, come indicato nell'RFC1597. La configurazione del DNS deve permettere la risoluzione degli indirizzi esterni da parte delle macchine interne, mentre gli indirizzi interni non devono essere visibili all'esterno. Esaminiamo ora singolarmente le varie componenti del firewall e, in seguito, le caratteristiche delle sottoreti protette.

Router Esterno Il router esterno garantisce che il traffico proveniente dalla rete dipartimentale e da Internet (d'ora in poi "dall'esterno") non abbia indirizzo mittente uguale a quello di una delle macchine interne. Le macchine interne, infatti, sono autorizzate a svolgere operazioni diverse rispetto a quelle esterne e la falsificazione dell'indirizzo mittente permette in alcuni casi di impersonare una delle macchine interne. Per ottenere questa protezione, il router seleziona i pacchetti che lo possono attraversare in base all'indirizzo mittente e all'interfaccia di provenienza: se un pacchetto proveniente dall'interfaccia esterna ha indirizzo mittente interno, si tratta chiaramente di un tentativo di falsificazione. Poiché l'operazione è semplice e poco onerosa, non si è ritenuto necessario un router dedicato allo scopo. Si è scelto invece di utilizzare un prodotto software, come ad esempio IPFirewall, da installare sul bastion host, che esamina i pacchetti in ingresso prima di passarne il contenuto ai vari servizi e proxy. È fondamentale però che il prodotto sia in grado di esaminare non solo i pacchetti che devono proseguire verso altre interfacce, ma anche e soprattutto quelli destinati all'host locale, distinguendoli in base all'interfaccia di provenienza.

Bastion Host È la componente più complessa di tutto il firewall. Esso deve mediare e verificare tutto il traffico che lo attraversa. Grazie all'uso del software di filtraggio (router esterno), il bastion host può assumere che gli indirizzi IP di provenienza dei pacchetti siano corretti, almeno per quanto riguarda indirizzi IP di sottoreti protette: dovrà bloccare tutte le comunicazioni da e per servizi e/o host non esplicitamente autorizzati. Il traffico sarà possibile solo mediante l'utilizzo di proxy, mentre l'attraversamento diretto del sistema da parte di pacchetti IP dovrà essere bloccato. Le connessioni ammesse sono solo quelle qui descritte.

- Dalla rete esterna per la gestione degli account. Queste connessioni sono verso la macchina delle configurazioni, provenienti dalla macchina del Centro di Calcolo Didattico appositamente autorizzata e adeguatamente autenticate e crittografate. A questo scopo si utilizza il package ssh.
- Dalla rete di gestione e sviluppo, verso l'esterno e verso la macchina delle configurazioni. Le connessioni verso la macchina delle configurazioni sono adeguatamente autenticate e hanno il solo scopo di permettere l'aggiornamento delle configurazioni, in un ambiente ristretto simile a quello previsto per la gestione degli account. Le connessioni verso l'esterno servono per le normali attività di gestione della rete dipartimentale e sono svolte attraverso proxy, quando possibile specifici per i singoli servizi utilizzati. In particolare, sono utilizzati i proxy specifici del Firewall Toolkit realizzato dalla TIS Inc., mentre per i proxy generici può essere utilizzato il package SOCKS V.5. Le connessioni per la gestione del fileserver sono crittografate e autenticate, per proteggere l'accesso alle funzionalità più critiche del server. Anche in questo caso si utilizza il package ssh.
- Dalla macchina delle configurazioni verso il fileserver esterno, in modo da aggiornarne il database, utilizzando il package ssh.

- Dalla rete amministrativa solo verso il bastion host, che fa da POP server per la posta elettronica, e verso i server FTP e HTTP del Dipartimento per gestire l'aggiornamento e la pubblicazione di documenti. Un'alternativa all'installazione del server POP sul bastion host è l'uso di un proxy generico per portare le connessioni dalla rete amministrativa al server dipartimentale.

Dove si usa il package ssh, quest'ultimo può essere utilizzato anche come proxy, oppure potrà essere utilizzato un proxy generico come ad esempio quello del TIS toolkit. I file di log del bastion host sono mantenuti sia sul bastion host che su una macchina della rete di gestione. Si tratta di una soluzione non ottimale, in quanto l'eventuale compromissione del bastion host rende immediata la compromissione della rete di gestione. Soluzioni più sofisticate, come l'impiego di una macchina connessa via linea seriale o l'impiego di supporti di registrazione WORM, non sembrano economicamente proponibili per questo progetto. Per la realizzazione del bastion host deve essere utilizzato un sistema Unix al cui kernel possano essere fatte le modifiche necessarie, come l'installazione del software di filtraggio. Dovendo essere un sistema particolarmente robusto è consigliabile l'utilizzo di FreeBSD, mentre l'utilizzo di un sistema Linux è sconsigliato. La maggior parte possibile del filesystem deve essere configurata in sola lettura a livello hardware. A questo scopo possono essere utilizzati dischi rigidi con uno switch per disabilitare la scrittura o anche, per piccole quantità di dati, floppy disk.

Router interno Data la complessità della configurazione del bastion host e la sua diretta esposizione agli attacchi, è prevedibile che occasionalmente, magari in seguito alla scoperta di nuovi difetti del software o di nuove forme di attacco, il bastion host sia compromesso. Senza il router interno questo evento comporterebbe l'immediato libero accesso alla rete amministrativa e alla macchina delle configurazioni. Lo stesso accadrebbe se il bastion host non fosse direttamente compromesso, ma fosse attraversato da un traffico non autorizzato, anche se magari limitato. Lo scopo del router interno è far sì che anche in queste occasioni le reti protette conservino una ragionevole difesa. Il router infatti permetterà comunque solo il traffico autorizzato, e in particolare:

- verso la macchina delle configurazioni, solo il traffico verso i servizi fortemente autenticati previsti per la gestione degli account e delle configurazioni;
- verso la rete amministrativa, solo il traffico verso i client per FTP, HTTP e la posta elettronica, quando questi attivano una connessione dall'interno. Non sarà possibile aprire connessioni dall'esterno verso le macchine dell'amministrazione. Per questo motivo, sarà necessario utilizzare l'opzione "passive" per il client FTP.

Questa limitazione sarà ottenuta utilizzando i meccanismi di filtraggio del router.

È molto probabile che l'ipotetico attaccante, nel tentativo di capire quale traffico può passare, invii dei pacchetti non autorizzati, la cui ricezione da parte del router interno causa l'immediata segnalazione di un'intrusione in corso, permettendone una rilevazione tempestiva.

Rete amministrativa La gestione della rete amministrativa nella configurazione indicata presuppone che la rete si trovi su un unico segmento, da connettere al router interno. Attualmente le due segreterie, didattica e amministrativa, si trovano su due segmenti separati, corrispondenti a due rami diversi connessi ai repeater delle rispettive ali del primo piano. È necessario realizzare il cablaggio che le connetta, attraversando l'atrio del primo piano. Per la rete amministrativa sono previsti i seguenti servizi:

- posta elettronica, mediante il POP server installato sul bastion host;
- FTP in uscita per l'aggiornamento e la pubblicazione di documenti sui server pubblici del Dipartimento, mediante il proxy FTP del bastion host;
- HTTP in uscita per l'esame del server dipartimentale.

I client POP utilizzati sulle macchine di questa sottorete devono essere configurati in modo da non eseguire automaticamente comandi MIME contenuti in messaggi o documenti, e sui client HTTP le funzionalità Java e Javascript devono essere disattivate. Quale misura aggiuntiva si può effettuare un filtraggio di questi linguaggi sul bastion host. Questa scelta implica l'utilizzo di un proxy specifico, come quello del TIS toolkit.

Macchina delle configurazioni Questa macchina Unix dovrà accettare in ingresso solo connessioni fortemente autenticate e in ambienti limitati per la gestione delle configurazioni e degli account. La protezione è ottenuta con ssh, mentre la limitazione dell'ambiente si ottiene, fra l'altro, limitando il file system accedibile con l'utilizzo della funzionalità Unix chroot. Deve poi aggiornare, con procedure automatizzate appositamente realizzate e mediante servizi protetti con ssh, il fileserver esterno e le eventuali configurazioni locali di altre macchine della rete dipartimentale. Deve essere inoltre gestito il logging di eventi significativi per la sicurezza della macchina, come tentativi di connessione a porte non autorizzate o autenticazioni fallite. In alcuni eventi particolarmente gravi, può essere previsto lo shutdown automatico della macchina, a meno che questo evento non sia tempestivamente impedito da console. Questa procedura non comporta gravi disservizi alla rete, almeno una volta raggiunta una configurazione stabile. La stessa macchina può inoltre fare da server per l'attività di logging e di allarme del router interno. Bisogna notare che non è sicuro inviare questa informazione alla rete di gestione, se non a titolo informativo, in quanto nel caso in cui si presentino problemi di sicurezza a questo livello è molto probabile che la rete di gestione sia a sua volta già compromessa.

Rete di gestione e sviluppo È quella che presenta le esigenze più varie e di difficile gestione. A causa dell'inevitabile minor sicurezza che ciò comporta, questa rete non si trova dietro al router interno, in modo che una sua compromissione non pregiudichi la sicurezza delle altre sottoreti. I servizi in uscita che si prevede di fornire sono sotto elencati.

- Servizi FTP e telnet, attraverso i proxy specifici del TIS Toolkit.
- Servizi HTTP, gopher e FTP quando utilizzato nell'ambito di WWW. Per questi servizi non sarà utilizzato un proxy specifico, in quanto la rapida evoluzione di questo ambiente fa sì che sia difficile e oneroso mantenere aggiornato il proxy. Si prevede invece l'utilizzo di proxy generici, in particolare SOCKS. Questo implica l'utilizzo di client in grado di gestire il protocollo SOCKS, come ad esempio il client Netscape. L'utilizzo di client Netscape è subordinato alla disabilitazione delle funzionalità Java e Javascript.
- Posta elettronica, gestita installando sul bastion host i programmi smap e smapd del TIS Toolkit.
- Connessioni autenticate verso la macchina delle configurazioni, utilizzando ssh.
- Servizio Amanda per la gestione dei backup. È fornito mediante proxy generici, eseguendo il client in un ambiente limitato, ad esempio con chroot. Purtroppo sembra difficile stabilire l'approccio migliore per questo servizio senza effettuare prima una sperimentazione "sul campo", particolarmente per quanto riguarda la configurazione dei proxy e tenendo conto del fatto che utilizza anche il protocollo UDP, la cui gestione sicura è particolarmente difficile.

In entrata si prevede di avere il servizio X Windows, ovvero la connessione di client esterni a server interni. Questo servizio è stato esplicitamente richiesto dal personale che si occupa della gestione della rete dipartimentale. Anche se questo servizio è insicuro, si ritiene che l'utilizzo di un proxy specifico ne riduca notevolmente la pericolosità, specialmente tenendo conto della probabilità di un attacco verso questo obiettivo.

Per quanto riguarda la connessione via modem, la soluzione più semplice e sicura è l'installazione di una o due schede modem su una delle macchine della rete, evitando l'accesso da macchine esterne. Per l'autenticazione deve essere utilizzato un meccanismo robusto. L'accesso è permesso solo da macchine con sicurezza paragonabile a quella della rete di gestione.

Fileserver Questa macchina è il punto da cui i package gestiti dagli amministratori della rete sono distribuiti alle altre macchine della rete dipartimentale, tramite NFS. Questa parte del file system è esportata in sola lettura. Ciò non impedisce, se necessario, di esportare in lettura e scrittura altre parti del file system, sulle quali si trovino file gestiti da utenti della rete dipartimentale. Questi file non devono però essere utilizzati nelle attività di gestione del fileserver. In caso di compromissione di una macchina della rete dipartimentale, la sua configurazione corretta può essere immediatamente ripristinata dal fileserver tramite rdist, mentre la correttezza dei pacchetti software è garantita dal fatto che l'esportazione è fatta in sola lettura. I dati locali possono essere recuperati invece solo fino allo stato in cui erano al momento dell'ultimo backup. Durante la fase di sviluppo e di aggiornamento, gli amministratori della rete possono avere la necessità di modificare direttamente i dati sul fileserver, anziché sulla macchina delle configurazioni. Questa operazione è possibile utilizzando canali autenticati e protetti fra le macchine della rete di gestione e il fileserver. Al termine delle modifiche, le versioni finali sono archiviate sulla macchina delle configurazioni, che provvede a riallineare le versioni sul fileserver.

Altre considerazioni. Tutti i componenti del sistema di protezione devono eseguire un logging delle attività significative dal punto di vista della sicurezza. Il risultato di questa attività deve essere esaminato regolarmente per rilevare i tentativi di violazione. Per rendere più agevole questo compito possono essere utilizzati degli strumenti che presentino i dati in un modo utilizzabile efficacemente dall'addetto a questo compito.

Si deve inoltre considerare che, per quanto quest'ultima attività possa essere semplificata con vari strumenti di analisi disponibili, si tratta comunque di un'attività che richiede un impegno non trascurabile.

La possibilità di connettersi alla macchina delle configurazioni da un sistema del Centro di Calcolo Didattico presuppone un'adeguata protezione di questo sistema. Inoltre può essere utile configurare il router che connette la rete dipartimentale a Internet in modo da filtrare il traffico evidentemente legato a un attacco, come ad esempio pacchetti con l'indirizzo mittente chiaramente falsificato o alcuni tipi di pacchetti ICMP.

5.3 Sistema di monitoraggio

L'architettura descritta permette di ripristinare rapidamente lo stato corretto delle risorse dipartimentali danneggiate in seguito a un'intrusione. È però auspicabile che le intrusioni possano avvenire quanto più raramente possibile e che possano comunque essere individuate prima che possano causare qualche danno. Dato che non è prevista la protezione della rete dipartimentale dal punto di vista dell'integrità e della riservatezza, si è optato per la realizzazione di un sistema di monitoraggio del traffico che permetta di rilevare eventuali attività anomale che possano far sospettare un attacco in corso. In più, l'integrità dei singoli sistemi gestiti dagli amministratori della rete deve essere periodicamente verificata con strumenti quali Tripwire.

Monitoraggio del traffico È diviso in due parti: una totalmente automatica, con lo scopo di rilevare il traffico anomalo e potenzialmente pericoloso e un'altra, attivabile in caso di necessità, che permetta di ispezionare il traffico. Lo scopo di questa seconda parte è da una parte scoprire se il traffico è effettivamente pericoloso, dall'altra controllare le attività dell'attaccante, per tentare di individuare il sito di provenienza dell'attacco, le tecniche adottate, nonché gli eventuali danni provocati sul sistema oggetto dell'attacco.

La parte automatica del sistema sarà composta da un packet sniffer installato su una macchina connessa alla rete dipartimentale. Questa macchina deve essere abbastanza sicura da evitare che il sistema di monitoraggio sia disabilitato con facilità, e sufficientemente scarica da permettere il funzionamento dello sniffer, che comporta un certo carico e che rischierebbe altrimenti di perdere parte del traffico. Ai pacchetti raccolti dallo sniffer sono applicate delle regole di filtraggio per scartare il traffico evidentemente locale. I pacchetti rimasti sono poi esaminati da alcune procedure che estraggono le informazioni interessanti e le memorizzano per l'esame da parte del personale addetto. Nel caso in cui venga rilevato del traffico chiaramente pericoloso, questo può essere segnalato immediatamente ai gestori della rete. Uno sniffer adatto a questo scopo è Tcpdump. Il riconoscimento del traffico pericoloso migliorerà man mano che lo strumento viene utilizzato, anche in funzione dell'uso effettivo della rete dipartimentale. Le regole di filtraggio e analisi devono poter essere modificate con facilità.

La parte di ispezione in tempo reale del traffico deve invece permettere di selezionare e registrare intere sessioni. Per alcuni tipi di traffico, come ad esempio le sessioni telnet, FTP e rlogin, deve essere possibile esaminare direttamente la sessione visualizzandone i dati nel modo più simile possibile a come risultano visualizzati all'attaccante. A questo scopo sembra molto adatto il package LIE, realizzato al Politecnico di Torino. L'accesso a questo strumento e ai dati raccolti deve essere attentamente controllato, per evitarne l'abuso e garantire agli utenti della rete la riservatezza delle comunicazioni. Le modalità di utilizzo di questo strumento devono essere definite nella politica di sicurezza.

Controllo dell'integrità dei sistemi Di tutti i sottosistemi componenti il sistema di protezione deve essere periodicamente verificata l'integrità. È auspicabile l'estensione di questa procedura a quante più macchine possibile, e in particolare a quelle gestite dagli amministratori della rete. Uno strumento adatto a questo scopo, per macchine Unix, è il programma Tripwire, che utilizza checksum crittografate per individuare variazioni nel contenuto dei file system. Sul bastion host, la cui configurazione non deve subire variazioni se non in situazioni eccezionali, la verifica copre l'intero file system, mentre sulle altre macchine copre solo i file di sistema. Per quanto riguarda le rimanenti parti dei file system, si utilizzano periodicamente procedure per la rilevazione di file potenzialmente pericolosi, come ad esempio file con diritti eccessivi o posseduti dall'utente sbagliato. A questo scopo possono essere utilizzati strumenti come Cops o Tiger. Sia i programmi che i dati raccolti devono essere protetti dalla modifica. Dove possibile, si devono installare file system in sola lettura, come ad esempio floppy disk con scrittura disabilitata.

5.4 Fasi per la realizzazione e installazione

La realizzazione di un sistema di protezione per un ambiente in cui la connessione a Internet è già presente e ampiamente sfruttata comporta la necessità di non interferire eccessivamente con l'utilizzo della rete durante l'installazione delle varie parti del sistema stesso. In particolare, è auspicabile che il corretto funzionamento delle varie parti del sistema sia verificato prima dell'installazione vera e propria, per non rischiare di bloccare completamente le attività sulla rete. È necessario altresì evitare che il sistema di protezione possa essere manomesso da utenti di Internet prima ancora di essere completamente realizzato. Per questi motivi la realizzazione e l'installazione delle varie parti del sistema di protezione devono avvenire secondo le seguenti fasi:

1. - installazione del router; questo permette di realizzare immediatamente la topologia di rete desiderata, e in particolare il posizionamento delle segreterie su un unico segmento ethernet, dietro al router; il router stesso può effettuare un logging di eventuali connessioni che non riguardano i servizi previsti nel presente progetto, permettendo così di scoprire se sono utilizzati altri servizi oltre a quelli individuati; la rete di gestione è a sua volta connessa al router, per gli stessi motivi; in questa fase, tuttavia, non viene bloccato alcun tipo di traffico;
   - aggiornamento del software delle segreterie, per utilizzare i soli servizi previsti, cioè FTP, WWW e POP;
   - preparazione fuori linea della macchina delle configurazioni; in particolare devono essere eseguiti fuori linea la configurazione, l'aggiornamento del software con i patch di sicurezza, l'installazione del tool ssh e la preparazione degli ambienti ristretti in cui eseguire l'aggiornamento;
   - preparazione fuori linea del bastion host; in particolare, preparazione del kernel, del software per il filtraggio e dei proxy; configurazione dei proxy e del servizio di posta;
   - installazione del tool ssh sul fileserver;
   - installazione delle schede modem sulla macchina interna scelta.
2. - installazione del bastion host sulla rete di gestione; il traffico della rete di gestione e della rete amministrativa viene man mano configurato in modo da passare per il bastion host; in questo modo, qualora sorgano problemi con i proxy, il traffico può essere semplicemente riconfigurato per non utilizzare il bastion host; alla fine di questa operazione, il router deve vedere solo traffico fra il bastion host e l'esterno e fra il bastion host e la rete amministrativa; in questa fase il software di filtraggio sul bastion host è necessariamente disabilitato;

- installazione sulla rete di gestione della macchina delle configurazioni; realizzazione e verifica delle procedure per l'aggiornamento delle configurazioni e del fileserver.

3. - realizzazione della topologia definitiva, con il bastion host interposto fra il router e la rete dipartimentale;
   - attivazione dei filtri sul bastion host e sul router;
   - verifica della correttezza della configurazione delle macchine coinvolte (fileserver, macchine della rete di gestione, bastion host e macchina delle configurazione); installazione dei patch di sicurezza e attivazione del tool Tripwire per individuare eventuali variazioni;
   - realizzazione degli strumenti per la gestione e l'analisi dei log del bastion host e del router.
4. il sistema di protezione a questo punto è in grado di funzionare; rimane da realizzare il sistema di monitoraggio della rete dipartimentale; questa fase consiste nella realizzazione e installazione degli strumenti di base, in quanto il monitoraggio della rete comporta una continua modifica e aggiornamento degli strumenti stessi; in questa stessa fase si provvederà a verificare, per quanto possibile, la configurazione degli host principali della rete dipartimentale, e in particolare di quelli che offrono servizi all'esterno.

È importante inoltre che le attività di preparazione, configurazione e gestione del firewall, del router e della macchina delle configurazioni siano eseguite solo da console, o in un ambiente adeguatamente protetto.

6 Politiche di Sicurezza

Una politica di sicurezza è una precondizione necessaria per stabilire misure di difesa efficaci [6]. In essa sono definiti i parametri essenziali per la scelta del tipo di difesa, quali ad esempio le risorse da proteggere, il loro valore, i servizi necessari, le procedure da adottare per la gestione.

Gli aspetti affrontati dalla politica di sicurezza sono divisi in tre gruppi:

1. analisi del rischio;
2. aspetti normativi;
3. aspetti gestionali.

Esaminiamo a grandi linee questi tre gruppi. In molti casi è difficile dare indicazioni generali, in quanto questo aspetto della sicurezza è particolarmente dipendente dalle peculiarità dei diversi siti.

6.1 Analisi del rischio

Per realizzare una buona difesa bisogna innanzitutto definire cosa si vuole proteggere e da quali pericoli.

A seconda del sito in esame, una parte più o meno grande delle risorse può essere considerata di valore. Inoltre, a seconda del tipo e del valore delle risorse, sono possibili diversi tipi di attacco.

Sia la difesa che l'attacco di un sistema hanno dei costi. Di questi costi è necessario tenere conto per stabilire misure di sicurezza che da una parte non superino il valore dei dati da proteggere, dall'altra contrastino efficacemente i possibili attacchi.

I costi della difesa sono dovuti a numerosi fattori:

- risorse hardware dedicate
- software utilizzato
- costo della progettazione e dell'installazione dei sistemi di sicurezza
- personale dedicato
- riduzione della produttività (dovuta ai vincoli imposti dalla sicurezza)
- costo della manutenzione e ridefinizione della politica di sicurezza.

I costi degli attacchi sono invece:

- risorse hardware dedicate
- tempo uomo per la messa a punto dell'attacco (ad esempio la realizzazione di programmi specifici)
- tempo uomo per la realizzazione dell'attacco
- conseguenze dell'eventuale identificazione e cattura (in funzione della probabilità di essere catturati).

Questi costi, particolarmente per quanto riguarda gli attacchi, possono essere divisi fra più bersagli. Ad esempio, il costo della realizzazione di un programma può diventare trascurabile, se utilizzando quel programma è possibile attaccare un numero elevato di sistemi. Gli investimenti nella difesa e nell'attacco sono limitati dal valore delle risorse che si vogliono rispettivamente proteggere o sottrarre. In generale, è diverso il danno costituito dalla sottrazione delle risorse, rispetto a non averle avute affatto. Nel primo caso le proprie attività si basano sulla disponibilità delle risorse e il danno causato dalla loro sottrazione è maggiore.

Queste valutazioni devono essere mantenute aggiornate, perché le variazioni nell'ambiente possono variare costi e valori.

Anche la sicurezza di un sito varia con il tempo, in conseguenza del miglioramento delle tecnologie e con le variazioni dell'ambiente. I cambiamenti possono modificare, in generale, sia le possibilità di difesa che quelle di attacco. Per esempio, la disponibilità dei primi firewall ha favorito solo la difesa, mentre il miglioramento delle prestazioni delle reti e dei computer ha favorito entrambi; l'aumento del numero di utenti di Internet e la loro diversa preparazione hanno probabilmente favorito più gli attaccanti che i difensori.

Per stabilire le difese da adottare è necessario definire, oltre alle risorse da proteggere e al loro valore, anche le funzionalità che il sistema deve offrire. Sarebbe infatti facile proteggere i dati semplicemente non connettendo il sistema in rete; questa soluzione però impedirebbe l'uso dei servizi necessari.

È necessario distinguere fra servizi indispensabili e servizi facoltativi o desiderabili, in quanto l'impossibilità di difendere un sito a causa di un servizio facoltativo porta all'eliminazione del servizio, mentre se la causa è un servizio indispensabile, è necessario riesaminare l'opportunità della connessione in rete dei sistemi su cui sono conservati i dati critici, o addirittura di tutto il sito.

Infine, in alcuni siti, come istituti bancari e organizzazioni militari, alcuni dati sono considerati di valore illimitato sia per gli attaccanti che per i difensori.

6.2 Aspetti normativi

Per regolamentare l'uso delle risorse significative per la sicurezza del sistema è necessario definire vari aspetti della politica di sicurezza.

Entità che avalla la politica di sicurezza Questa entità deve avere l'autorità necessaria per imporre la politica di sicurezza a tutti coloro che la devono rispettare. La politica deve essere definita congiuntamente da chi ha l'autorità e gli strumenti per imporla e chi ha le conoscenze tecniche per renderla efficace per la difesa.

La definizione di questa entità è essenziale: le norme per l'uso delle risorse non devono essere definite solo dal personale tecnico che si occupa della loro gestione, per evitare che siano messe in discussione da personale più autorevole. In qualche caso può essere necessaria l'approvazione di più entità, ciascuna competente per un diverso aspetto o per un diverso settore dell'organizzazione. Questo è particolarmente vero per quanto riguarda la definizione delle sanzioni.

Entità che verifica il rispetto della politica di sicurezza Questa entità verifica effettivamente che le norme stabilite dalla politica di sicurezza siano rispettate. Si tratta di personale tecnico, delegato dall'entità che ha definito o avallato la politica. La delega può riguardare la sola attività di verifica, oppure anche l'autorità necessaria per applicare eventuali sanzioni.

Entità esterne coinvolte nella gestione della sicurezza Devono essere identificate sia le entità esterne coinvolte nella gestione ordinaria della sicurezza del sistema, sia quelle coinvolte nella gestione degli incidenti; devono essere chiari i loro compiti, i loro diritti e i loro doveri. Anche questi aspetti devono essere concordati con le suddette entità ed eventualmente formalizzati, ad esempio con un contratto di assistenza. È opportuno contattare preventivamente le entità esterne da coinvolgere nella gestione di incidenti, per non affrontare i rischi dell'improvvisazione durante un incidente.

Norme per l'uso, l'amministrazione e la manutenzione delle risorse Devono essere definiti numerosi aspetti.

- Norme sugli usi ammessi per le risorse; le norme devono essere definite in modo non ambiguo e comprensibile agli utenti, per evitare l'insorgere di problemi nel riconoscimento delle violazioni; vanno considerati tutti i casi particolari, quali ad esempio gli utenti con privilegi speciali, in modo che queste situazioni non siano trattate al di fuori della politica, generando situazioni di difficile gestione in caso di incidenti.
- Chi ha l'autorità di autorizzare l'accesso alle risorse, e con quali vincoli; devono essere chiare le politiche di condivisione o divulgazione di password; deve essere definita la politica per la selezione di password non banali, per la loro distribuzione agli utenti, nonché per l'utilizzo di altri strumenti per l'autenticazione (schede, smart card o altro).
- Regole per la gestione dei diritti di superutente e degli altri privilegi: chi ha i vari diritti, per quali scopi e con quali limiti li può utilizzare.
- Procedure per l'individuazione e la gestione di informazioni di valore: se un utente conserva informazioni di valore in una directory modificabile da tutti, può essere difficile stabilire di chi sia la responsabilità di un eventuale danno.
- Politiche di *accounting* e di *logging* delle attività.
- Limiti alle risorse utilizzabili, come ad esempio al tipo di traffico permesso sulla rete; deve essere stabilito se è vietato utilizzare determinati programmi o servizi, sia sulla rete locale che da questa su altre reti; in alcuni casi il semplice possesso di determinati programmi può costituire una violazione.
- Gestione di diritti e licenze sul software, nonché la politica nei confronti dell'uso di software pirata o della diffusione, volontaria o involontaria, di virus, *worm* e *trojan horse*.

Diritti degli utenti Devono essere definiti i diritti degli utenti, per evitare che possano essere violati. Un caso importante è la privacy delle comunicazioni e dei dati: deve essere chiaro se e con quali vincoli gli amministratori dei sistemi sono autorizzati a esaminare i dati o i messaggi degli utenti. Se queste operazioni non fossero ammesse, devono essere evitate anche nelle procedure di prevenzione e gestione degli attacchi. Particolarmente nella definizione di questi aspetti, è importante tenere conto delle leggi esistenti. Non è tuttavia legittimo aspettarsi il rispetto delle leggi da parte degli utenti anonimi provenienti da Internet, in quanto questi possono agire da paesi con usi e normative diversi.

Deve essere chiaro se gli utenti hanno diritto di accedere ai propri dati e alle proprie risorse, o se l'accesso può essere loro negato per motivi di sicurezza.

Pubblicazione e accettazione della politica La politica di sicurezza deve essere resa nota agli interessati, comprendendo sia coloro che gestiscono i controlli e le risorse, sia coloro il cui comportamento è vincolato. Questi possono essere gli utenti abituali del sistema, ma possono comprendere anche gli utenti dei servizi offerti in rete. È difficile infatti aspettarsi un comportamento conforme alla politica di sicurezza da utenti che non ne conoscono le caratteristiche, a parte quanto definito dalle leggi vigenti. Per questo motivo a volte può essere necessario inserire delle schermate informative all'inizio delle sessioni.

Può essere necessario richiedere agli utenti l'accettazione esplicita della politica di sicurezza, ad esempio mediante la sottoscrizione di un apposito modulo: non sempre infatti chi gestisce il servizio ha l'autorità di imporre dei vincoli all'utente.

È importante che la politica di sicurezza sia realistica, e in particolare che possa ragionevolmente essere fatta rispettare. È importante anche che gli utenti capiscano i motivi per cui vengono imposte le norme e le procedure: se non educati, gli utenti considerano la politica di sicurezza come una serie di vincoli imposti senza motivo, aumentando così la probabilità di violazioni.

Responsabilità È necessario chiarire in modo inequivocabile chi è responsabile di eventuali violazioni: in alcuni casi la responsabilità è personale, in altri può essere di un'organizzazione di cui la persona fisica presente è un semplice rappresentante. Se un attacco è stato favorito dal comportamento incompetente di un amministratore, questi può essere correo. In tal caso questa eventualità deve essere chiarita nella definizione dei compiti dell'amministratore, che potrebbe ritenere la sicurezza un aspetto trascurabile della gestione del sistema, o un compito non di sua competenza.

Può poi essere necessario descrivere, se non definire, le responsabilità del sito e dei suoi utenti per quanto riguarda eventuali attacchi ad altri sistemi connessi.

Devono essere definiti i responsabili della gestione dei vari aspetti della sicurezza, in modo che esistano riferimenti precisi ai quali riportare eventuali problemi, o a cui chiedere suggerimenti sul corretto comportamento.

Sanzioni Le sanzioni, per quanto possibile, devono essere definite all'interno della politica di sicurezza. Questa scelta ha numerosi vantaggi rispetto all'alternativa di deciderle all'atto della violazione:

1. la scelta delle sanzioni può essere fatta con maggiore oculatezza, evitando così stime errate della gravità delle violazioni, o punizioni dovute all'emozione del momento;
2. l'entità delle sanzioni può scoraggiare i potenziali violatori, che altrimenti potrebbero non essere consapevoli della gravità delle proprie azioni;
3. si possono evitare con più facilità differenze di trattamento fra violatori della stessa norma.

Devono essere chiariti i casi in cui si ricorre all'autorità giudiziaria, quelli in cui si prevedono sanzioni di tipo amministrativo, ed eventuali altri casi. Si deve fare attenzione a che le sanzioni e le norme definite non siano in contrasto con alcuna legge, o con norme di fonte più autorevole. È importante notare come in generale sia difficile definire le azioni illegali in un sistema informatico. Spesso sono definite in termini di "scopo delle azioni" e di "intenzioni", in quanto la stessa operazione può essere corretta in un contesto e scorretta in un altro. Si pensi ad esempio all'uso di strumenti per la verifica dell'integrità di un sistema.

6.3 Aspetti gestionali

Per garantire il rispetto delle norme definite nella politica di sicurezza, è necessario definire le procedure per la gestione della sicurezza del sistema. Altre procedure devono essere definite per la corretta gestione degli incidenti.

Procedure per l'applicazione delle norme Le norme definite nella sezione precedente devono essere tradotte in procedure per la loro gestione. Si devono definire le procedure per:

- l'aggiornamento della politica di sicurezza;
- il mantenimento dei contatti con le entità coinvolte nella gestione della sicurezza;
- la distribuzione, la manutenzione e la revoca dei diritti di accesso alle risorse;
- la scelta delle password;
- la distribuzione e l'uso dei privilegi, come l'uso di account di superutente;
- la gestione delle informazioni di valore;
- la gestione della configurazione delle macchine;
- la gestione dei *backup*;
- l'aggiornamento del software e dell'hardware;
- l'aggiornamento sulle scoperte di difetti nel software e sulle relative correzioni;
- la gestione del traffico da e per l'esterno;
- l'introduzione di dati e di software nel sistema;
- la pubblicazione della politica di sicurezza;
- l'accettazione della politica di sicurezza;
- la distribuzione delle responsabilità e dei compiti, nonché la pubblicazione di questi assegnamenti, affinché sia chiaro a chi rivolgersi in caso di necessità;
- la gestione delle interazioni con altri siti: diritti di accesso, uso dei servizi, eccetera;

- la rilevazione di violazioni alla politica, anche quando non portano a una violazione della sicurezza del sistema;
- la comminazione di sanzioni.

Queste procedure devono essere dettagliate, in modo da poter essere seguite in modo preciso, per riconoscere eventuali violazioni alle procedure stesse.

La correttezza e il rispetto delle procedure di controllo devono essere a loro volta verificabili: l'inefficacia di una procedura può causare l'abbandono delle norme il cui rispetto doveva verificare.

Monitoraggio del sistema Devono essere definite le procedure per il monitoraggio della rete, dei sistemi e del sistema di protezione. Queste comprendono:

- l'uso di strumenti per la verifica della correttezza della configurazione;
- le procedure per la verifica del corretto comportamento degli utenti; se è previsto il monitoraggio delle operazioni effettuate dagli utenti, o l'esame dei loro dati privati, le procedure devono rispettare le norme sulla privacy degli utenti; è opportuno notificare agli utenti l'esistenza di procedure e controlli;
- le tecniche da adottare per individuare eventuali attacchi, come ad esempio la gestione dei messaggi di errore; spesso questi messaggi sono registrati ma non esaminati;
- l'utilizzo delle funzionalità di *logging* del sistema, nonché l'esame e la gestione dei file generati.

Gestione di sospetti attacchi Nella maggior parte dei casi, da anomalie del sistema o dai messaggi di errore non si può dedurre immediatamente se è in corso un attacco, specialmente se a notare le anomalie sono degli utenti. È necessario avere delle procedure per gestire questi eventi, in modo da riconoscere gli attacchi reali e prendere contromisure, senza però causare inutili interruzioni nei servizi nel caso di semplici errori. La gestione di questa fase è molto importante, perché il fallimento nell'individuazione di un attacco in corso impedisce l'attivazione delle apposite procedure di difesa. Devono essere definite delle procedure per gestire i seguenti punti:

- notifica di anomalie da parte degli utenti; questo è il punto più importante: gli utenti devono sapere a chi rivolgersi, e come; devono essere rassicurati sul fatto che il loro problema venga gestito, poiché se l'utente non ottiene risposte alle sue comunicazioni, non è stimolato a farne altre in futuro;
- variazioni nelle procedure di monitoraggio e di esame della configurazione; esame più attento dei file di log, aumento del *logging*, verifica più approfondita della configurazione del sistema, esame dei *backup* e confronto con i dati attuali, monitoraggio delle attività di utenti sospetti;

- contatti preliminari con gli enti da coinvolgere in caso di riconoscimento di un attacco: da quel momento in poi, infatti, le azioni devono essere svolte con tempestività, e la mancanza di accordi può portare all'impossibilità di collaborare con enti esterni;
- protezione di risorse di valore: per quanto possa non essere necessario interrompere i servizi di rete, il valore di alcune classi di dati può richiederne la rimozione dalla rete fino al chiarimento della situazione e alla valutazione dell'effettivo pericolo;
- procedure da attivare qualora la situazione precipitasse improvvisamente; devono essere definite con precisione le circostanze di attivazione di queste procedure.

Gestione degli attacchi I problemi legati all'improvvisazione nella gestione degli attacchi sono stati citati nella sezione precedente; poiché gli effetti di azioni improvvisate o errate sono più gravi, è ancora più importante avere già stabilito le procedure da adottare. A seconda del tipo di attacco, si possono scegliere tre politiche:

- non prendere particolari provvedimenti; questa scelta ha senso qualora l'attacco risulti debole, o le difese siano ritenute adeguate; vi sono siti che, per vari motivi, sono attaccati con grande frequenza, ma nella maggior parte dei casi con attacchi già noti e insufficienti per le difese presenti: se questi siti dovessero reagire ogni volta, si otterrebbe una forma molto particolare di *denial of service*; ciò non significa che questi attacchi non debbano essere monitorati, nel caso dovessero diventare più pericolosi;
- individuare l'attaccante e raccogliere prove; questo comporta lasciare una certa libertà d'azione all'attaccante stesso, mettendo in potenziale pericolo le risorse che si vogliono proteggere; questa scelta non ha senso qualora non si voglia o non si possa poi perseguire l'attaccante;
- difendere le risorse; questa scelta porta a interrompere i servizi sotto attacco, fino a che non si ritenga di essere in grado di affrontare la situazione con sicurezza, ad esempio dopo aver rimosso le risorse di valore dalla rete.

La scelta tra queste tre politiche deve essere in parte definita nella politica di sicurezza, ma in parte può essere fatta caso per caso in base al tipo di attacco.

Un'attenzione particolare va rivolta alle relazioni pubbliche: per molte organizzazioni, quali ad esempio gli istituti di credito, il danno all'immagine dovuto alla divulgazione di informazioni su un attacco riuscito può essere superiore a quello causato dall'attacco stesso, che magari è stato respinto, o che ha acceduto a dati di poco valore. Deve essere chiaro come gestire le relazioni con l'informazione pubblica, e in particolare deve essere stabilito chi ha il compito di fornire informazioni: gli altri, probabilmente, non saranno autorizzati a comunicare alcunché.

Procedure di ripristino A meno che non si sia catturato l'attaccante, può essere difficile stabilire la fine dell'attacco e il ripristino delle difese a uno stato normale. Da una parte, un'azione troppo avventata può permettere all'attaccante di avere successo; dall'altra, una situazione di allerta, con i servizi limitati e il personale impegnato a seguire l'attacco, porta a perdite di produttività anche considerevoli. Inoltre, va considerato che i responsabili della sicurezza si trovano notevolmente sotto pressione in queste situazioni: da una parte c'è l'utenza che insiste per riavere la disponibilità delle risorse, dall'altra ci sono le responsabilità in caso di un ripristino avventato.

È soprattutto nella fase di ripristino che si deve organizzare il materiale raccolto durante l'attacco: file di log, strumenti lasciati dall'attaccante, informazioni e schemi di nuovi tipi di attacchi, punti deboli delle proprie difese. È opportuno avere delle procedure per gestire questo materiale, in modo che non vada perso e se ne possa trarre profitto. Le informazioni raccolte possono essere utili anche ad altri siti soggetti allo stesso tipo di attacco, magari a opera della stessa persona.

7 Politica di Sicurezza proposta per la rete dipartimentale

Questa sezione non rappresenta di per sè la definizione della politica di sicurezza per la rete dipartimentale. Questa operazione deve infatti essere svolta dall'autorità competente. Si è però cercato di dare indicazioni quanto più dettagliate e complete possibile. Per alcune parti si tratta solo di linee guida; parte della politica di sicurezza potrà infatti essere completamente definita solo in seguito alla realizzazione del sistema di protezione (procedure per l'analisi dei file di log, gestione dei diritti, ecc.). Almeno in linea di massima, gli aspetti normativi devono essere definiti, in accordo con il Direttore del CDC, prima di iniziare la realizzazione del sistema di protezione, per evitare che risultino poi delle incongruenze fra la politica che si vuole realizzare e le funzionalità del sistema di protezione. La parte di politica di sicurezza riguardante la definizione delle risorse da proteggere e il tipo di rischi dai quali devono essere protette non sono riportate, ma sono deducibili dalle sezioni precedenti del documento. Sono descritti invece gli aspetti normativi e quelli gestionali.

7.1 Aspetti normativi

Entità che avalla la politica di sicurezza La politica di sicurezza sarà avallata dal Direttore del Centro di Calcolo. Questa entità ha l'autorità necessaria e sufficiente per imporre norme sull'uso della rete dipartimentale, nonché per decidere le sanzioni in caso di violazioni. Nei casi in cui il Direttore del CDC abbia l'autorità di intervenire sull'uso delle risorse, ma non di comminare sanzioni, sarà necessario l'avallo di un'autorità più alta. Questi casi devono essere riconosciuti e gestiti al momento della definizione delle possibili sanzioni (vedi seguito).

Entità che verifica il rispetto della politica di sicurezza (nel seguito RRPS) Questo compito può essere assunto dal sistemista che si occuperà del monitoraggio della rete e dell'esame dei log del sistema di protezione. Eventuali indizi di violazioni devono essere riportati infatti proprio da questi strumenti. Per assumere questo compito il RRPS deve aver ben compreso il funzionamento del sistema di protezione.

Il Direttore del CDC deve stabilire se, in caso di violazioni provate o sospette e nel solo caso in cui ulteriori indagini siano utili, il RRPS può o meno effettuare indagini senza il preventivo consenso del Direttore del CDC. Devono essere indicati casi particolari, come:

- segnalazioni o richieste da siti esterni;
- classi particolari di utenti, come docenti o studenti;
- situazioni di urgenza, come attività sospetta in corso;
- risorse particolari sulle quali non sono permesse indagini senza il consenso dell'interessato o del Direttore del CDC, come:
  - posta elettronica
  - documenti conservati nella home directory di utenti (esclusi i file di sistema).

Deve essere chiaro, al momento dell'incarico, quali responsabilità comporta questo ruolo, particolarmente per quanto riguarda gli eventuali danni provocati da imperizia dell'incaricato.

Entità esterne coinvolte nella gestione della sicurezza Dato il tipo di istituzione non è necessario mantenere contatti permanenti con entità esterne, se non con il centro SERRA per coordinare le attività con le altre reti dell'Università. In caso di necessità può essere contattato, ad esempio, il CERT-IT, per chiedere le indicazioni necessarie per individuare altre entità la cui collaborazione può essere utile o necessaria.

Norme per l'uso, l'amministrazione e la manutenzione delle risorse Per quanto concerne il sistema di protezione, sono interessanti i seguenti aspetti:

- Rete Amministrativa: possono essere utilizzati i servizi di posta elettronica, WWW e il servizio FTP solo in uscita, con le limitazioni già indicate. Le macchine connesse in rete possono essere utilizzate solo dal personale addetto, o da altre persone esplicitamente autorizzate dal Direttore del CDC. L'installazione di software e la modifica della configurazione delle macchine possono essere effettuate solo dopo che il RRPS ha valutato le implicazioni dal punto di vista della sicurezza e ha dato un parere positivo. Queste operazioni possono essere effettuate solo da persone sulla cui adeguatezza al compito il RRPS abbia dato un parere positivo.

- Rete per la Gestione: sulla sottorete possono essere utilizzati tutti i servizi per i quali vi sia necessità, previa autorizzazione del RRPS. Fanno eccezione:
  - i servizi tramite i quali è possibile la generazione o la ricezione di traffico che attraversi il firewall; in questi casi possono essere utilizzati solo i servizi per i quali è esplicitamente prevista la gestione nella documentazione del firewall, secondo le modalità indicate; per questi servizi devono essere utilizzati programmi la cui adeguatezza sia stata positivamente valutata dal RRPS, anche per quanto riguarda la configurazione. Il RRPS si deve attenere a quanto indicato nella documentazione del sistema di protezione;
  - la macchina per la gestione delle configurazioni; questa macchina puó essere utilizzata solo per gli scopi e secondo le modalità indicate nella documentazione del sistema di protezione;
  - parti della sottorete esplicitamente dedicate al sistema di protezione (ad esempio il firewall); queste macchine possono essere utilizzate solo per gli scopi e secondo le modalità indicati nella documentazione del sistema di protezione.

  L'uso di questa sottorete è limitato al personale dedicato all'amministrazione della rete dipartimentale, previa autorizzazione del Direttore del CDC. Eventuali eccezioni devono essere anch'esse autorizzate dal Direttore del CDC, che indica anche la durata dell'autorizzazione e le risorse di cui è autorizzato l'uso. L'autorizzazione è subordinata all'accettazione della politica di sicurezza.

- Restante rete dipartimentale: in aggiunta a eventuali norme già emanate, si aggiungono le seguenti:
  - non è permesso utilizzare o tentare di utilizzare macchine dedicate al sistema di protezione, e in particolare il firewall, se non mediante un uso corretto dei servizi indicati come disponibili al pubblico nella documentazione del sistema di protezione (es. la posta elettronica);
  - non è permesso tentare di superare il sistema di protezione per accedere in modo anche legittimo a macchine da esso protette;
  - non è permesso tentare di acquisire maggiori diritti di quelli concessi dagli amministratori delle macchine o della rete, o permettere ad altri di acquisirli;
  - l'uso delle risorse da parte di utenti che si connettano da Internet deve essere limitato ai casi in cui il permesso viene esplicitamente concesso; in particolare, nei file .rhosts degli utenti devono essere indicate coppie host - utente, senza l'uso di caratteri jolly. Queste concessioni

devono essere comunicate al RRPS, affinché questi possa riconoscere le connessioni autorizzate da quelle non autorizzate;

– non è permesso tentare di acquisire diritti non esplicitamente concessi su macchine anche non appartenenti alla rete dipartimentale, utilizzando a questo scopo macchine della rete dipartimentale, o connessioni alla rete dipartimentale (ad esempio attraverso modem).

Gli utenti devono essere istruiti su come proteggere i propri dati e le proprie home directory. Le istruzioni possono essere parte di un documento sul server WWW del dipartimento o sulla mailing list dipartimento.

Diritti degli utenti Il direttore del CDC deve chiarire quali sono i diritti degli utenti, particolarmente per quanto riguarda la privacy, sia nei confronti degli altri utenti, sia nei confronti dei gestori della rete o dei servizi di rete. In particolare deve essere stabilito se possono essere letti, cancellati o modificati:

- i file di configurazione contenuti nella directory dell'utente (.login, .rhosts, ecc.);
- i file conservati nella directory dell'utente, per i quali l'utente stesso abbia configurato i permessi in modo che le operazioni sopra indicate siano possibili, ma non abbia concesso esplicitamente l'autorizzazione a farlo;
- i file per i quali l'utente abbia configurato i permessi in modo che le operazioni non siano possibili (in questo caso sono necessari diritti di superutente);
- file dell'utente temporaneamente gestiti dai servizi di rete (es. posta elettronica);
- comunicazioni dell'utente (es. sniffing);
- file contenenti informazioni sull'utente, ma controllati dai gestori dei sistemi o della rete (es. file di password).

Possono essere definite delle eccezioni per casi particolari, quali:

- normale amministrazione della rete;
- normale monitoraggio della rete;
- indagini su violazioni della politica di sicurezza in cui l'utente sia coinvolto;
- indagini su violazioni della politica di sicurezza in cui il coinvolgimento dell'utente non sia accertato;
- indagini su violazioni in cui l'utente non è coinvolto, ma lo è il suo account.

Per alcune di queste eccezioni può essere richiesta l'autorizzazione dell'utente. La definizione di questa parte della politica di sicurezza deve tener conto della normativa vigente in termini di riservatezza dei dati e delle comunicazioni.

Pubblicazione e accettazione della politica La politica di sicurezza deve essere pubblicata, ad esempio sul server WWW. Agli utenti deve essere richiesto di sottoscrivere, almeno per presa visione, gli articoli che li riguardano. I servizi pubblici ai quali si può accedere da Internet o via modem devono mostrare un messaggio di avvertimento sui vincoli riguardanti l'uso e sulle sanzioni in caso di violazione. Agli utenti deve essere fornita un'indicazione su come contattare il RRPS per chiarimenti o notifiche di problemi di sicurezza (ad esempio l'indirizzo di e-mail help).

Responsabilità Dato il tipo di istituzione, le responsabilità sono personali per qualsiasi violazione. Anche questo aspetto deve essere pubblicato e sottoscritto dagli utenti.

Sanzioni Il Direttore del CDC deve stabilire dei limiti minimi e massimi per le sanzioni, distinguendo diversi casi come:

- violazioni dovute a ignoranza di aspetti tecnici e che non hanno lo scopo o l'effetto palese di procurare danno o di acquisire o concedere privilegi non legittimi;
- violazioni che non hanno uno scopo evidente di procurare danno o di acquisire o concedere privilegi non legittimi;
- violazioni che mirano a procurare danno o a utilizzare in modo illegittimo i servizi, compresa, ad esempio, l'impersonazione di altri utenti nell'invio di messaggi di posta elettronica; in questi casi possono essere distinte violazioni di diversa gravità;
- violazioni che provocano danni agli utenti locali, o che richiedano il ripristino dello stato corretto delle risorse;
- violazioni che mirano ad attaccare altre reti o sistemi al di fuori della rete dipartimentale.

Possono essere considerati aggravanti, ad esempio:

- la recidività;
- lo sfruttamento di ruoli privilegiati;
- l'utilizzo di strumenti appositamente realizzati o installati (fattore che indica una forte premeditazione e determinazione).

Deve essere indicato esplicitamente in quali casi e secondo quali modalità è previsto il ricorso all'autorità giudiziaria. In caso di danneggiamento degli utenti, sia della rete dipartimentale che esterni, può essere chiesto il loro parere sul ricorso all'autorità giudiziaria, anche nei casi in cui questa azione non sarebbe prevista. Naturalmente, le sanzioni scelte devono essere effettivamente applicate nei confronti dei potenziali trasgressori. Può risultare necessario prevedere sanzioni diverse in funzione dei diversi ruoli degli utenti.

7.2 Aspetti Gestionali

Procedure per l'applicazione delle norme Devono essere definite le procedure per la messa in atto e la manutenzione della politica di sicurezza.

Aggiornamento della politica di sicurezza L'aggiornamento è proposto quando necessario dal RRPS al Direttore del CDC, per migliorare la politica o per adattarla a cambiamenti dell'architettura o della gestione della rete. Il personale di gestione della rete può a sua volta proporre modifiche, che sono presentate al Direttore del CDC insieme al parere del RRPS.

Gestione dei diritti di accesso alle risorse Queste procedure devono essere in grado di gestire in modo esplicito casi particolari e permessi temporanei, per poter chiarire sempre se un'azione è stata o meno autorizzata. Deve essere posta particolare attenzione alla rimozione dei diritti e degli account non più necessari.

Scelta delle password Devono essere date agli utenti sufficienti indicazioni sulla scelta di password quanto più possibile robuste, compatibilmente con le difficoltà di memorizzazione delle stesse.

Gestione dei privilegi Privilegi particolari, quali ad esempio l'accesso ad account di superutente, devono essere concessi solo in caso di necessità, per gli usi e la durata strettamente necessari, che devono essere esplicitamente indicati all'atto dell'autorizzazione. Deve essere indicato in quali casi e con quali limiti questi privilegi possono essere concessi dagli amministratori delle singole macchine, dagli amministratori della rete, dal RRPS, o dal Direttore del CDC.

Deve essere possibile gestire casi particolari, eventualmente dietro autorizzazione esplicita del Direttore del CDC. La mancata gestione di casi particolari è un tipico caso in cui la politica di sicurezza e i sistemi di protezione sono violati dagli stessi amministratori, rendendo poi difficile la gestione degli incidenti.

Deve essere posta particolare attenzione a privilegi che permettano di superare o manomettere il sistema di protezione. Questi privilegi non devono essere concessi se non in caso di necessità neppure ai gestori della rete dipartimentale e devono essere revocati appena possibile. Ciò evita anche che la compromissione di account privilegiati porti automaticamente al superamento del sistema di protezione.

Gestione della configurazione delle macchine La configurazione delle macchine deve essere affidata esplicitamente a uno o più gestori. Su alcune macchine, quale parte del sistema di protezione, possono essere installati strumenti per il rilevamento di modifiche alla configurazione. Il gestore deve essere in grado di riconoscere, in generale, se le modifiche alla configurazione sono state eseguite da lui o da altri.

La configurazione delle macchine esplicitamente dedicate al sistema di protezione non deve essere modificata se non per correggere malfunzionamenti o per adattarne le funzionalità a modifiche dell'architettura o alla topologia della rete, o per adattarla a variazioni della politica di sicurezza. Queste operazioni devono essere affidate dal RRPS a una persona qualificata, che acquisisca i diritti necessari secondo le modalità indicate nel punto precedente, e solo per il tempo necessario.

Gestione dei backup L'archiviazione di dati contenenti informazioni riservate, in particolare quelle la cui riservatezza è rilevante per il corretto funzionamento del sistema di protezione, deve essere effettuata garantendo il perdurare della protezione dei dati, anche con adeguate misure di sicurezza fisica.

Aggiornamento sui difetti del sistema di sicurezza Il RRPS deve mantenersi aggiornato sulla scoperta di difetti del software o di tipologie di attacco che possono ridurre o annullare le difese offerte dal sistema di protezione e deve avviare le procedure necessarie per correggere questi difetti.

Distribuzione dei compiti . Il RRPS può delegare parte dei suoi compiti a personale qualificato, previa autorizzazione del Direttore del CDC. In questi casi deve essere chiaro anche se e in quale misura sono delegati i corrispondenti privilegi e responsabilità. In caso di cambiamento del Direttore del CDC o del RRPS, i nuovi incaricati devono nuovamente esaminare, eventualmente modificare e sottoscrivere la politica di sicurezza. Attività impreviste o non indicate nella politica di sicurezza devono essere gestite dal Direttore del CDC, salvo esplicita delega.

Verifica delle procedure Le procedure definite nella politica di sicurezza devono essere verificate periodicamente, per accertarne la validità e l'adeguatezza alle necessità della rete Dipartimentale. Durante la verifica si deve tenere conto delle indicazioni fornite dagli utenti o dagli amministratori della rete.

Monitoraggio Il RRPS deve verificare che gli strumenti per il monitoraggio della rete dipartimentale e del sistema di protezione siano utilizzati come indicato nella documentazione del sistema di protezione. Il Direttore del CDC o il RRPS possono definire procedure aggiuntive, anche di uso occasionale, purché nel rispetto della politica di sicurezza e delle norme vigenti.

Gestione di sospetti attacchi Deve innanzitutto essere chiara la politica del Dipartimento in termini di risposta agli attacchi. In particolare deve essere definito se e in quali casi si vuole procedere al blocco immediato dell'attacco e in quali casi si vuole invece lasciare libertà d'azione al potenziale attaccante, per individuare con quali tecniche e strumenti è portato l'attacco e possibilmente scoprire l'identità reale dell'attaccante. Devono essere definite le procedure, da utilizzare in caso di sospetto attacco, per:

- registrare le attività svolte durante la gestione dell'incidente, per fornire materiale valido in caso di ricorso all'autorità giudiziaria, nonché per ricostruire le fasi dell'incidente per una successiva analisi e verifica della validità delle misure di protezione;
- aumentare l'attività di logging e conservare le registrazioni dei dati per una successiva analisi;
- interrompere attività che potrebbero facilitare la compromissione di sottoreti o sistemi critici, come ad esempio le connessioni dalla sottorete amministrativa;
- verificare in modo più approfondito la correttezza della configurazione delle macchine; in questo stato, l'individuazione di anomalie non porta necessariamente alla loro correzione: nel caso in cui si sia deciso di lasciare agire l'intrusore, le anomalie potrebbero essere semplicemente registrate e esaminate;
- informare il RRPS, il Direttore del CDC, o altre entità coinvolte nella gestione degli incidenti;
- riconoscere quando passare dalla gestione di un sospetto attacco alla gestione di un attacco in corso.

Gestione di un attacco in corso Gli aspetti da coprire in caso di attacco in corso sono gli stessi di quelli di un sospetto attacco. In più, può essere necessario:

- stabilire o concordare le modalità di gestione di attività al di fuori del normale orario di lavoro;
- stabilire le modalità per contattare amministratori di reti esterne, coinvolti nell'attacco o nella gestione dell'attacco; lo stesso dicasi per gruppi di supporto quali CERT e simili e per le autorità di pubblica sicurezza;
- stabilire quando e come passare dal monitoraggio all'azione, e secondo quali modalità.

Procedure di ripristino La gestione del ripristino di uno stato corretto é divisa in tre fasi:

Riconoscimento della fine dell'attacco È, in generale, un evento difficile da definire. È il Direttore del CDC, sentito il parere del RRPS, a dichiarare concluso l'attacco.

Ripristino dello stato corretto della rete Utilizzando i backup e il materiale raccolto durante il monitoraggio dell'attacco, si ripristina lo stato corretto della rete. In più, si provvede alla correzione dei difetti del sistema di protezione individuati durante l'attacco. Al termine di questa fase, il Direttore del CDC può dichiarare concluso l'incidente e la rete e le procedure possono tornare allo stato normale.

Analisi successiva Si procede nel seguito all'analisi dei dati raccolti durante l'incidente, per ricavarne:

- ulteriori informazioni su difetti del sistema di protezione, o su nuove metodologie di attacco;
- informazioni di vario tipo (tecnico, culturale, ecc.) sulle attività e le motivazioni degli attaccanti;
- informazioni su altri siti violati dall'attaccante, per avvertirli del problema;
- in caso di necessità, una raccolta organica di prove a carico dell'attaccante.

8 Conclusioni

La progettazione di un sistema di protezione presuppone la comprensione delle esigenze di sicurezza del sito da proteggere. Il progetto descritto è una valida soluzione per le esigenze del Dipartimento di Informatica, tipico esempio di NPRO. Questa soluzione permette inoltre un facile adattamento sia a un aumento delle esigenze di riservatezza e integrità delle risorse, sia alla gestione di singoli progetti con elevate esigenze di sicurezza. La maggiore complessità di realizzazione rispetto ad altre soluzioni è controbilanciata da una maggiore facilità di gestione prevista. La progettazione del sistema di protezione, iniziata nel febbraio 1996, è stata conclusa nell'aprile dello stesso anno. La realizzazione è stata ritardata da alcune modifiche alla rete dipartimentale rese necessarie dalla ristrutturazione di un'ala del Dipartimento stesso. Il fileserver è stato installato e la realizzazione del sistema di protezione è prevista entro la fine del 1996.

Bibliografia

[1] CERT. *Computer Emergency Response Team.* http://cert.org.

[2] Chapman, D. B., and Zwicky, E. D. *Building Internet Firewalls.* O'-Reilly Associates, Inc., 1995.

[3] Cheswick, B., and Bellovin, S. *Firewalls and Internet Security: Repelling The Wily Hacker.* Addison Wesley Publishing Company, 1994.

[4] Garfinkel, S., and Spafford, G. *Practical Unix Security.* O'Reilly Associates, Inc., 1991.

[5] Hickman, K. E. B. *The SSL Protocol.* Mosaic Communications Corp., 1994.

[6] Holbrook, P., and Reynolds, J. *Site Security Handbook.* Request for Comments: 1244, 1991.

[7] IETF. *Active IETF Working Groups: HTTP Charter.* http://www.ietf.cnri.reston.va.us/html.charters/http-charter.html.

[8] Inc., T. *Firewall Toolkit.* http://www.tis.com/docs/products/fwtk.

[9] Lee, Y. *Four easy steps to SOCKSify (most of) your favorite network programs.* ftp://ftp.nec.com/ pub/security/socks.cstc/ How_to_SOCKSify, 1992.

[10] Schneier, B. *Applied Criptography.* John Wiley & Sons, Inc., 1994.

[11] SSH. *Secure Shell.* http://www.cs.hut.fi/ssh.

[12] Stern, H. *Managing NFS and NIS.* O'Reilly Associates, Inc., 1991.

[13] Venema, W. *TCP Wrapper: network monitoring, access control, and booby traps.* ftp://ftp.win.tue.nl/pub/security/tcp_wrappers.txt.Z, 1992.

[14] Walker, K. M. A Domain Type Enforcement UNIX Prototype. In *Proceedings of the Fifth USENIX UNIX Security Symposium* (1995), pp. 127–140.