Consiglio Nazionale delle Ricerche

Componente di Sicurezza del TIX e della Infrastruttura di RTRT - Indicazioni tecniche per le fasi di progettazione e gestione

M.C. Buzzi, F. Dianda, E. Prati, L. Rossi, M. Sommani

IIT TR-07/2003

Technical Report

Luglio 2003

Istituto di Informatica e Telematica

Sommario

1. Introduzione

1.1 Premessa

In data 1 ottobre 2002 è stata stipulata una convenzione tra Regione Toscana ed Istituto di Informatica e Telematica del C.N.R. per la consulenza specialistica a supporto della realizzazione di attività inerenti il Tuscany Internet eXchange (T.I.X.). Tra i diversi punti oggetto della consulenza è stato previsto il supporto alla progettazione ed al mantenimento della componente di sicurezza del TIX e della infrastruttura della Rete Telematica della Regione Toscana (RTRT).

Questo documento ha l'obiettivo di produrre una prima analisi del grado di sicurezza del TIX cosí come indicato nella progettazione, e di determinare eventuali spazi di intervento per accrescerne la qualità, cercando ove possibile di indicare strategie e metodologie applicabili. L'analisi del grado di sicurezza del TIX è condotta relativamente agli aspetti strategici e gestionali in conformità a quanto previsto dalla legislazione vigente in materia di sicurezza fisica e logica.

Partendo dalla descrizione dei dispositivi di sicurezza previsti dalla normativa nazionale quindi, il documento prende in esame la situazione del TIX indicando cosa debba essere definito e fornendo suggerimenti su come implementarlo (cap.2). Analizzando poi la progettazione del sistema di sicurezza del TIX, vengono messi in evidenza possibili fonti di rischio ed aspetti della documentazione che andrebbero maggiormente dettagliati o specificati, cercando di fornire informazioni sulle possibili misure (meccanismi, strumenti od accorgimenti) utilizzabili per aumentare la sicurezza fisica (cap. 3) e logica (cap. 4) del sistema.

1.2 Documenti di riferimento

Non essendo allo stato attuale il TIX ancora operativo, è stato necessario basare l'analisi su quanto indicato nelle policies di sicurezza di Regione Toscana e

nella documentazione finora fornita dal Raggruppamento Temporaneo d'Impresa (RTI) Telecom-Getronics-Brain Technology, assegnatario della gestione del TIX. Manca nella documentazione presa in esame un vero e proprio Piano della Sicurezza del TIX, previsto dal bando ma non ancora prodotto dal RTI.

I documenti presi in esame per effettuare l'analisi sono stati:

[1] Offerta Tecnica per la realizzazione del TIX – 9 Novembre 2001

[2] Piano di Lavoro TIX – Tuscany Internet eXchange – 3 Febbraio 2003

[3] Bando di Gara TIX – luglio 2001

[4] Politiche di Sicurezza di Regione Toscana – 15 Dicembre 1999.

1.3 Glossario

1.3.1 ACRONIMI E SIGLE

- *ARP:* Address Resolution Protocol
- *ASP:* Application Service Provider
- *HTTP*: HyperText Tranfer Protocol
- *MAC*: Media Access Control
- *ICT*: Information and Communication Technology
- *ISP*: Internet Service Provider
- *IXP*: Internet eXchange Point
- *NSA*: National Security Agency
- *NTP:* Network Time Protocol
- *RT*: Regione Toscana
- *RTRT*: Rete Telematica Regione Toscana
- *RTI*: Raggruppamento Temporaneo di Imprese
- *SMTP:* Simple Mail Transmission Protocol
- *SNMP:* Simple Network Management Protocol
- *SSH:* Secure Shell
- *SSL:* Secure Socket Layer
- *TIX*: Tuscany Internet eXchange, IXP per la Pubblica Amministrazione Toscana
- *VLAN:* Virtual LAN.

1.3.2 DEFINIZIONI

- *MAC address*: Indirizzo a 48 bit per individuare univocamente ogni scheda Ethernet;

- *MAC Flood*: forma di attacco informatico volta a saturare le capacità di memorizzazione di uno switch L2;
- *Defaceament*: forma di attacco informatico volto alla sostituzione, alterazione, o distruzione di un sito web o di parte di esso;
- *PIX*: abbreviazione di Private Internet eXchange Firewall, tecnologia di protezione mediante firewall sviluppata da Cisco Systems;
- *DMZ*: De-Militarized Zone, porzione di rete separata dal resto tramite strumenti di filtraggio (firewall, router, ecc.) con lo scopo di isolare;
- *Autonomous Systems*: insieme di reti sotto lo stesso dominio o politica di routing;
- *BGP*: Border Gateway Protocol, protocollo di routing di tipo “distance vector” per lo scambio di informazioni circa la raggiungibilità di reti tra e fra Autonomous Systems;
- *NAP*: Neutral Access Point, punto di scambio del traffico IP;
- *VPN:* Virtual Private Network, insieme di tecnologie in grado di stabilire tunnel cifrati o in chiaro per trasmettere dati attraverso una rete pubblica;
- *IPsec*: protocollo per la creazione di un tunnel cifrato a livello IP, in grado quindi di cifrare tutto il traffico in uscita da un nodo;
- *IDS*: Intrusion Detection System, dispositivo in grado di rivelare e segnalare comportamenti “anomali” in un segmento di rete o su un particolare host;
- *Switch*: dispositivo di rete in grado di instradare traffico tra segmenti di rete, con la sigla L2 (layer 2) si indicano dispositivi in grado di lavorare a livello Data Link, con L3 (layer 3) si indicano dispositivi in grado di lavorare a livello Network;
- *IP-MAC Spoofing*: forma di attacco informatico volto ad falsificare un indirizzo mittente in una comunicazione.

2. Gestione della sicurezza

Ai sensi della Direttiva del Presidente del Consiglio dei Ministri del 16 Gennaio 2002, Dipartimento per l'Innovazione e le Tecnologie [5], del relativo Allegato 2 [6], Capitolo 2, e del Decreto Interministeriale "Istituzione del Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni" [7], l'Amministrazione è tenuta a disporre un sistema di gestione della sicurezza che tenga conto di strategie e risorse specifiche. Sul modello della struttura ministeriale, le organizzazioni non ministeriali (nella fattispecie la Regione Toscana) individuano nel soggetto avente rappresentanza legale il vertice nel funzionigramma che si fa carico della sicurezza dei sistemi informatici e delle telecomunicazioni. Egli è coadiuvato da consiglieri, responsabili e un comitato della sicurezza ICT. In virtù della realizzazione della struttura dei responsabili, è fatto obbligo che essi approntino una serie di dispositivi, di seguito elencati.

2.1 Carta della Sicurezza

È obbligatorio redigere e approvare una Carta della Sicurezza che definisca le politiche di sicurezza, le strategie ed il modello amministrativo. Questo compito spetta alla Pubblica Amministrazione e quindi a Regione Toscana. La Carta della Sicurezza fa da radice per l'indirizzo delle politiche di sicurezza, ragion per cui va approntata prima degli altri dispositivi che invece sono stilati sulla base di quanto contenuto nei documenti che stanno loro a monte.

2.2 Politiche Generali della Sicurezza

Sono le direttive per lo sviluppo, la gestione e il controllo e la verifica delle misure di sicurezza; devono essere elaborate da Regione Toscana nel rispetto della Carta della Sicurezza e modificate in base ai cambiamenti di scenario.

Il documento relativo alle Politiche Generali di Sicurezza ha una corrispondenza nei contenuti all'attuale "Politiche per la Sicurezza Informatica e Telematica della

Regione Toscana" [4], con la differenza che la nuova versione dovrebbe risultare conforme alla Carta della Sicurezza, definita gerarchicamente a un livello superiore.

La rilevanza del TIX come infrastruttura strategica nazionale rende urgente l'adeguamento a tali disposizioni, in modo che la definizione dei dispositivi permetta al Gestore Esterno (definito in [6] come il fornitore di servizi che opera sotto il controllo del responsabile dei sistemi informativi, il quale pianifica gli interventi e la committenza delle attività da affidare all'esterno) di approntare nello specifico gli altri dispositivi previsti dal medesimo allegato ed elencati di seguito. Il Gestore Esterno nello specifico è individuato nel gestore del TIX e quindi nel RTI assegnatario del contratto di gestione per 5 anni.

2.3 Politiche Specifiche (Norme)

Il gestore deve emettere normative per l'organizzazione, il personale ed i sistemi, aggiornandole tempestivamente in base alle esigenze in modo conforme a quanto previsto da Regione Toscana tramite le Politiche Generali della Sicurezza.

2.4 Specifiche Procedure

Il gestore deve farsi carico della gestione delle System Security, della Network Security, della continuità del servizio e della gestione operativa, cosí come del ciclo di vita del software, della gestione di incidenti, del controllo e monitoraggio del sistema di sicurezza e della sicurezza del personale.

2.5 Gestione della fase transiente

Il bando del TIX [3] richiedeva che unitamente all'Offerta Tecnica [1] fosse approntato un Piano della Sicurezza, non ancora realizzato. Il gestore quindi è tenuto sia per contratto che per legge ad approntare i dispositivi sopra indicati. Il Piano dovrà essere adeguato quanto prima alle indicazioni di Regione Toscana relative alla pianificazione delle attività in materia di sicurezza, e da quanto indicato nella Carta della Sicurezza (§ 2.1) e nelle Politiche Generali della Sicurezza (§ 2.2).

Si ricorda inoltre che ai sensi del Decreto Legislativo 318 del 28 Luglio 1999 è inoltre fatto obbligo da parte del gestore di nominare un responsabile della tutela dei dati personali (Art.2).

Dato che la realizzazione del TIX è in corso d'opera, nell'intervallo di tempo che occorre per la realizzazione dell'intero sistema di controllo è necessario garantire comunque un elevato standard di sicurezza; sono quindi da prevedersi due fasi di adeguamento delle politiche della sicurezza allo standard richiesto dai ministeri, che prevedano uno sviluppo parallelo delle politiche ed un successivo adeguamento per renderle congruenti. Infatti nonostante l'approccio più lineare sia quello di produrre la documentazione in modo sequenziale partendo dalla Carta di Sicurezza, l'urgenza della definizione e dell'applicazione di policies di sicurezza presso il TIX obbliga a svolgere le fasi in parallelo cercando di renderle consistenti con un eventuale aggiustamento a posteriori. Le due fasi da prevedersi sono quindi:

1) Sviluppo parallelo delle politiche:
    - Redazione della Carta della Sicurezza da parte di RT e adeguamento delle Politiche Generali della Sicurezza già esistenti alla Carta della Sicurezza
    - Redazione delle Politiche Specifiche della Sicurezza e delle procedure per il TIX da parte del RTI, in conformità con le attuali Politiche della Sicurezza di RT.

2) Strutturazione organica delle politiche:
    - Adeguamento delle Politiche Specifiche della Sicurezza e delle Specifiche Procedure da parte del RTI ai documenti di livello superiore di RT.

Adottare una procedura di questo tipo comporta i seguenti vantaggi:

- permette a RT di approntare senza urgenza immediata le proprie politiche
- permette al TIX di godere del necessario livello di sicurezza fin dal momento dell'attivazione.
- rende consistenti tra loro in ogni parte le documentazioni approntate da RT e dal gestore.

Nel seguito saranno evidenziati alcuni aspetti relativi alla sicurezza fisica (cap. 3) e logica (cap. 4) non sufficientemente dettagliati nell'Offerta Tecnica [1] sui quali porre particolare attenzione, indicando possibili accorgimenti tecnici applicabili.

3. Sicurezza fisica: accessibilità degli apparati e controllo degli accessi ai locali

3.1 Gruppo di continuità

In riferimento a quanto contemplato dal paragrafo 1.2.1 dell'offerta [1], è previsto un gruppo di continuità che garantisca 15 minuti di autonomia al sistema in caso di black-out; oltre a ciò è previsto un gruppo elettrogeno diesel di autonomia pari a 5 ore per rifornimento. Nell'Offerta [1] non risulta essere descritto il procedimento di attivazione che implica il subentro del secondo meccanismo in sostituzione del primo. Non è specificato inoltre quale tipo di apparati include la stima di autonomia di 5 ore. Oltre a ciò occorrerebbe definire una procedura di controllo periodico dello stato di manutenzione dell'apparato che garantisca la sua entrata in funzione all'occorrenza.

Non è specificato inoltre se l'apparato in questione coincide con quello già in dotazione di Brain Technology o se si tratti di uno apposito dedicato al TIX. Nel primo caso occorre verificare che si tratti di un impianto dimensionato in modo adeguato per fornire la potenza aggiuntiva richiesta dalla fornitura della corrente elettrica al TIX.

3.2 Accesso ai locali

Le misure di sicurezza adottate per controllare l'accesso ai locali, presentate nei paragrafi 1.1.2 e 1.1.3 dell'Offerta [1], richiedono la definizione di alcuni elementi importanti. I locali presso cui è ospitato il TIX sono di proprietà di Brain Technology quindi per la sorveglianza esterna si suppone che siano utilizzate le misure attualmente in uso; di tali misure non esiste però alcun riferimento dettagliato. Risulta pertanto difficile valutare cosa si intenda con il termine "accesso controllato" indicato nel paragrafo 1.1.2 dell'Offerta [1].

Questa mancanza è facilmente superabile tramite la presentazione, da parte del gestore, di un documento che presenti in dettaglio:

- Strumenti utilizzati per la sorveglianza dei locali (servizio di guardia, videosorveglianza, ecc.) e loro modalità di erogazione (24h, sala di controllo remota presidiata, ecc.)
- Meccanismi per l'accesso ai locali (badge magnetici, telecomandi, ecc.)
- Orario di accesso ai locali
- Meccanismo di separazione tra i locali destinati al TIX (primo e secondo piano) e quelli di Brain (citato genericamente nell'Offerta Tecnica [1] come misura di ulteriore selezione degli accessi)
- Procedure di segnalazione di eventi anomali o catastrofici:
  - Strumenti di comunicazione utilizzabili in caso di emergenza: è necessario prevedere almeno un meccanismo primario ed uno secondario il più possibile indipendenti dai locali e dal TIX stesso (es: evitare linee telefoniche fisse e comunicazioni tramite reti IP annunciate al TIX)
  - Soggetti cui notificare tali eventi (es.: forze dell'ordine).

Si consiglia inoltre di stabilire una policy di accesso rigorosa per l'accesso alla sala macchine, in particolare:

- Orario di accesso
- Necessità di un meccanismo per autenticazione per l'operatore che chiede l'accesso
- Necessità di operare comunque sotto la supervisione o il controllo di un operatore del TIX (in particolare per quanto riguarda fornitori terzi, come menzionato a pag. 15 dell'Offerta Tecnica [1]).

4. Sicurezza logica

I sistemi del TIX devono essere resistenti alla penetrazione da parte di soggetti esterni. La sicurezza dell'accesso alle informazioni e del controllo del sistema è garantita tramite quattro azioni:

1. Progettazione dell'architettura della rete e configurazione logica degli apparati
2. Sicurezza e livelli di servizio in caso di mancato funzionamento del TIX
3. Strumenti per il controllo dell'integrità, della disponibilità e dell'accesso all'informazione
4. Feedback tramite vulnerability assessement.

4.1 Progettazione dell'architettura della rete e configurazione logica degli apparati

4.1.1 SEPARAZIONE FISICA E LOGICA NELLA RETE

I paragrafi indicati nel seguito si riferiscono tutti all'Offerta Tecnica del RTI [1].

La progettazione della rete, schematizzata tramite la figura 3.3 e descritta nel paragrafo 3.2, consiste nel separare la rete in tre zone, esterna (Internet), demilitarizzata (zona servizi) e militarizzata (rete interna) tramite 2 firewall in "cascata". Questo schema obbliga ad accedere alla rete interna passando dalla zona demilitarizzata e quindi il traffico è soggetto alle politiche di sicurezza dei 2 firewall.

L'ultima versione del piano di lavoro [2] consta di un cluster di due PIX 525 che serve allo stesso modo sia i servizi esterni che quelli interni, mentre la versione precedente prevedeva due coppie di firewall in serie per isolare con diversi gradi di sicurezza le porzioni di rete. La soluzione attuale, permettendo una separazione tra le VLAN della rete RTRT, rappresenta una valida soluzione per la separazione a livello logico del traffico di rete per scopi di gestione e controllo. Si osservi che, a causa della natura broadcast del traffico ethernet, la soluzione precedente basata

sulla separazione fisica avrebbe consentito una limitazione più marcata tra le sottoreti.

4.1.2 SICUREZZA DEI SINGOLI APPARATI

Diventa di fondamentale importanza garantire la sicurezza degli apparati di rete ed in particolare quelli su cui sono configurate le VLAN e il relativo routing. E' necessario perció adottare misure di sicurezza che restringano l'accesso ai soli manager dei dispositivi di rete, che limitino gli accessi alle sole "macchine" designate alle funzioni di management, e che prevedano la registrazione con indicazione temporale ed esito di tutti i tentativi di accesso.

Il sistema di autenticazione e le politiche di definizione dei profili utente con la gestione dei diritti associati sono un punto chiave da progettare e gestire con particolare attenzione; per rafforzare la politica di sicurezza del TIX dovrebbero avvalersi di un ulteriore strumento ovvero di sistemi di cifratura. E' doveroso sottolineare però che una gestione incompleta o disorganica del sistema di autenticazione potrebbe agevolare un ipotetico aggressore, mettendolo in condizioni di sfruttare gli strumenti di cifratura per " nascondere" le proprie attività

Nell'ottica di ridurre la vulnerabilità dei dispositivi di rete, è raccomandata l'adozione di meccanismi robusti quali protocolli (es. SSHv2, SNMPv3), strumenti (es. liste di accesso) ed accorgimenti, come ad esempio quelli sulle configurazioni dei routers e switch, così come suggerito anche dalla NSA nel documento "Router Security Configuration Guide" [8].

Risulta interessante prendere in considerazione, vista la presenza di due Switch Cisco Catalyst 4506 nella parte NAP del TIX e della suite di monitoraggio Cisco Works2000, la possibilità di implementare un sistema di sicurezza in cui ci sia un mapping statico tra il MAC address dell'interfaccia del router dell'ISP presso il NAP e la porta degli switch su cui si attesta, garantendo così l'identità della periferica collegata senza aggravi dal punto di vista del management della rete. Adottando questa politica di sicurezza sugli switchs, gli ipotetici aggressori non potranno portare attacchi del tipo Mac Flood e Mac Spoofing per guadagnare

accesso allo switch o ascoltare il traffico di un particolare host. Non è comunque possibile, configurando un mappaggio statico tra MAC address e porta dello switch, vanificare attacchi di tipo ARP Spoofing, questo perchè l'ARP Spoofing consiste nell'invalidamento della ARP cache sulla macchina bersaglio dell'attacco. Se si dovesse verificare un attacco di questo tipo, ci sarebbe un'esposizione ad azioni di dirottamento delle sessioni.

La presenza di un NTP server che sincronizzi i device di rete e i syslog server, permetterebbe di identificare cronologicamente gli eventi, e di fornire anche maggiore granularità nella gestione degli accessi alle risorse, ove necessario.

È da ritenersi comunque che la separazione tra VLAN non dovrebbe essere considerata una soluzione sostituiva all'utilizzo di strumenti di cifratura del traffico (es: SSL). La modalitá di accesso ai servizi inoltre dovrebbe prevedere l'utilizzo di tali strumenti indipendentemente dal percorso dal quale giunga la richiesta.

4.1.3 PACKET FILTERING DEL CISCO 4006

Occorre sincerarsi che il router di frontiera Cisco 4006 L3 tra TIX e RTRT svolga una funzione di packet filtering, pena una maggiore mole di lavoro da parte della coppia di PIX e di conseguenza una maggiore importanza degli apparati stessi. In questo caso, il principio che può essere utilizzato per valutare l'efficienza e l'importanza di un firewall è il "paradosso della protezione perimetrale" che può essere così sintetizzato: il valore di un firewall è direttamente proporzionale al numero di macchine a lui connesso, ma la sua efficacia è inversamente proporzionale a tale numero. In questo caso occorre valutare il grado di protezione richiesto sui servizi poiché potrebbe essere consigliabile fare parziale uso delle funzionalità di firewall del Cisco 4006 L3.

4.1.4 RIDONDANZA DEL CISCO 4006

Il Cisco 4006 non è ridondato e questo fa da single failure point, cioè in caso di malfunzionamento dell'apparato, gli ISP attestati al TIX non raggiungerebbero la RTRT direttamente via 4006 ma sarebbero costretti a passare su Internet.

Occorre valutare se il router che annuncia RTRT sul TIX può mancare di ridondanza al pari degli altri, dal momento che RTRT detiene i principali servizi e quindi riveste un ruolo di primaria importanza. La mancata ridondanza di questo nodo potrebbe inficiare tutte le altre ridondanze previste nella LAN TIX e LAN RTRT.

4.1.5 INTRUSION DETECTION SYSTEMS

Il sistema è coadiuvato da un Intrusion Detection Systems (IDS) che incrementa la sicurezza del sistema, che dal piano di lavoro risulta servire tutta la LAN RTRT. La presenza nell'Offerta Tecnica [1] di un IDS Cisco 4235 rappresenta un elemento ulteriore di protezione perimetrale; tale tipo di apparati risulta ampiamente diffuso, anche se esistono dibattiti aperti su quale tipo di attacchi essi siano effettivamente in grado rilevare. Dalla documentazione [2] risulta che l'apparato in questione è connesso agli switch Cisco 6506, da cui si desume che è utilizzato per monitorare comportamenti anomali in corso nelle sei VLAN. Questa configurazione potrebbe non risultare molto efficace a causa del numero di macchine ospitate nella varie sottoreti, e dall'elevato utilizzo di connessioni cifrate. È opportuno verificare che il dispositivo previsto (operante nella migliore delle ipotesi per un traffico di 100Mbps senza packet-loss) sia adeguato alla mole di traffico prevista sulla rete; in caso contrario esso non risulterebbe di particolare utilità e converrebbe restringere la sua azione alla porzione di rete dedicata ai servizi.

Si tiene a far presente che gli IDS sono utili strumenti, ma la soluzione migliore rimane sempre la presenza di personale che conoscendo la rete su cui lavora, possa discriminare tra attività "sospette" o "normali comportamenti della rete" e che periodicamente sfogli i log prodotti dai firewalls, dai routers, e delle altre periferiche importanti (vedi § 4.4.2). A partire dal momento di utilizzo del NAP infatti sarebbe necessario monitorare il sistema tramite una registrazione sicura degli eventi a carico del gestore ed una fase successiva di log-auditing, non prevista nell'offerta ma richiesta dalla normativa di riferimento (sezione 1 di [6]: "Separazione dei compiti" relativa a chi effettua il monitoraggio degli indicatori di performance, sicurezza/rischio, e chi lo verifica) e da far svolgere ad un soggetto

differente dal Gestore. Sarebbe opportuno definire tra le attività del personale del TIX anche quelle di lettura dei Log.

4.2 Sicurezza e livello di servizio in caso di mancato funzionamento del TIX

4.2.1 ACCORGIMENTI NELLA CONFIGURAZIONE DEL ROUTING

Occorre prevedere una gestione delle situazioni di temporanea mancata erogazione del servizio da parte del TIX. Il protocollo BGP permette ai punti terminali di una connessione di continuare a comunicare anche in tali casi, ma occorre specificare le modalità in cui questo avviene. Ad esempio, occorre stabilire quale policy adottare nel caso in cui una VPN IPSEC tra due utenti richieda la cifratura. E' necessario definire una politica di instradamento e di accesso ai dati qualora il servizio del TIX non sia in atto. Il livello di servizio dovrebbe essere il medesimo, per cui occorre configurare il sistema in modo tale da permettere a una sessione di stabilirsi e a un servizio di svolgersi solo in presenza delle medesime richieste; occorre quindi fare in modo che le politiche di sicurezza siano coerenti con quelle adottate in regime di normale servizio del TIX.

E' inoltre auspicabile applicare alcune pratiche di sicurezza correntemente utilizzate in Internet:

- come consigliato dall'RFC 1918 [9] è necessario esercitare un controllo sullo Spazio di Indirizzamento Privato, applicando liste di accesso per le classi private in modo da permettere l'instradamento di pacchetti provenienti da questi IP solo sulle interfaccie dove espressamente richiesto E' inoltre opportuno verificare l'assenza di route che potrebbero far uscire dalla rete "Interna" del traffico di reti "private" verso l'esterno;
- è necessario configurare le liste di accesso sulle interfaccie dei routers in modo tale che siano in linea con quanto consigliato nell'RCF2827 [10], ovvero che accettino pacchetti in uscita solo dagli indirizzi IP appartenenti alle reti logiche configurate sulle rispettive interfaccie. Ciò permette di vanificare il tentativo di IP spoofing proveniente da hosts interni, utile a generare attacchi di tipo Denial of Service;

- è necessario configurare le liste di accesso sulle interfaccie esterne dei routers in modo tale che non siano accettati pacchetti con indirizzi IP appartenenti a reti interne.

4.3 Strumenti per il controllo dell'integrità della disponibiltà e dell'accesso all'informazione

La gestione della sicurezza logica comporta la formulazione di una politica di sicurezza organica basata sull'analisi rigorosa dell'ambiente circostante per determinare un livello di sicurezza, o più esattamente un livello di esposizione al rischio: in pratica la definizione dei livelli di confidenzialità, integrità e disponibilità dell'informazione da mantenere, con l'adozione di appositi strumenti, durante tutto il ciclo di funzionamento.

Nel caso del TIX, questa politica deve tener conto delle due diverse entità che lo compongono: la parte NAP, punto nevralgico delle comunicazioni tra gli afferenti, e la parte ASP, punto nevralgico di servizi offerti dalla rete RTRT.

Nei paragrafi precedenti sono stati delineati alcuni strumenti di base per la gestione della parte NAP; in questo paragrafo si presentano alcuni punti aspetti da prendere in considerazione per il mantenimento dei livelli suddetti per la parte ASP. Gestire la sicurezza della parte ASP vuol dire affrontare le problematiche di sicurezza dei servizi ospitabili nelle VLAN che la compongono: a differenza delle parte NAP, in questa parte di rete del TIX possono essere ospitati apparati e macchine di natura diversa, il cui funzionamento può essere sensibile ad una classe di minacce particolari (es: un server HTTP è soggetto a minacce diverse rispetto ad un server SMTP, banalmente un defaceament è diverso dallo spam). Visti i recenti trend in fatto di attacchi informatici inoltre non basta limitarsi ai soli aspetti della network security, dal momento che essa prende in esame le problematiche dei soli livelli di comunicazione.

Nella componente ASP del TIX sono presenti un elevato numero di sistemi la cui sicurezza ha riflessi significativi non solo per il governo della regione ma anche su quello del paese, e sui quali quindi dovrebbe essere posta particolare attenzione: ad esempio le macchine in collegamento con i Ministeri risultano

importanti sia a causa dell'elevato valore delle informazioni in esse contenute sia perché potenzialmente sensibili ai sensi della legge 675/96.

L'utilizzo di un firewall (il cluster di PIX525), sulla parte front end (quella tra NAP e gli switch Catalyst 6506), è da considerarsi una misura minima di sicurezza, ma non sufficiente per proteggere i sistemi della rete RTRT: in particolare manca una policy da implementare sul firewall in relazione al traffico proveniente e/o diretto da/verso esso. La definizione di quest'ultima è un punto da chiarire nel Piano di Lavoro [2]: tale policy è quella in uso in RT ([2], pag.25), ma vista la molteplicità degli afferenti alla rete RTRT è consigliabile delineare la modalità di estensione di tale documento, sia per ciò che riguarda i servizi, sia per ciò che riguarda le tipologie di utente, in modo che il gestore sia in grado di approntare le necessarie configurazioni. In particolare, per quanto riguarda la parte ASP, non è possibile valutare in modo esaustivo il livello di rischio cui i sistemi ospitati possono essere soggetti, non essendo presenti alcune informazioni discriminanti quali:

- Servizi offerti ospitati nella parte ASP
- Profilo degli utenti che possono accedere a tali servizi
- Eventuali metodi di autenticazione degli accessi e/o degli utenti (es: SSL, VPN ecc.)
- Procedure per l'audit delle informazioni di log registrate dagli apparati
- Procedure per il disaster recovery
- Procedure per il backup dei dati con particolare attenzione alla fase di recovery.

Particolare attenzione dovrebbe essere rivolta a quelli che statisticamente sono gli aspetti più sensibili, che vengono presentati in dettaglio nel seguito.

4.3.1 POSTA ELETTRONICA

Visto il loro vasto utilizzo, i sistemi di posta elettronica hanno un ruolo cruciale nelle comunicazioni interne ed esterne; è opinione diffusa nel mondo della ricerca che tali sistemi saranno sempre più oggetto di attacchi e di fenomeni di abuso quali lo spam. Si consiglia di approntare il prima possibile una serie di misure

tecniche volte a limitare la frequenza di tali eventi, utilizzando liste di controllo e installando antivirus sui server di posta elettronica.

4.3.2 CONTROLLO DEGLI ACCESSI

Nell'ambito di una corretta gestione della sicurezza è necessario stabilire un meccanismo di controllo degli accessi degli utenti alle informazioni presenti sui sistemi della rete RTRT. In particolare, dovrebbero essere rimossi tutti quei meccanismi deboli (es. password in chiaro) o basati su protocolli insicuri (es: netbios, nfs) a favore di meccanismi robusti (ssh, ssl, uso di certificato digitale e firma digitale).

4.3.3 GESTIONE DEGLI AGGIORNAMENTI E CICLO DI VITA DEL SOFTWARE

La scoperta di bugs nei software è da considerarsi una situazione ordinaria, pertanto è necessario stabilire una serie di comportamenti da attuare per limitare il livello di esposizione a tale minacce, come ad esempio le procedure per l'aggiornamento dei software in questione (manuale, automatica, ecc.) e la verifica preventiva dell'efficacia dell'aggiornamento proposto. Un caso particolare di software la cui efficacia è influenzata dalla frequenza degli aggiornamenti è costituito dagli antivirus: il loro costante aggiornamento è da considerararsi misura necessaria da associare al loro corretto posizionamento nell'architettura di rete (es: controllo delle mail in entrata).

4.3.4 GESTIONE DEI CODICI DI ACCESSO E SENSIBILIZZAZIONE A LORO CORRETTO UTILIZZO

La gestione delle password è uno degli elementi più critici in una politica di sicurezza; se da un lato è necessario imporre vincoli sulla loro non banalità (inibizione di date di nascita, nomi di persona, ecc.), dall'altro è necessario che l'utente sia in grado di ricordarle con il minor sforzo possibile altrimenti sarà costretto ad annotarle su supporti inadeguati. Gli inconvenienti derivanti da tali comportamenti possono essere mitigati con l'utilizzo di appositi supporti crittografici (smartcard, token, ecc.) o biometrici, introducendo però un fattore di costo non indifferente. Una volta definite le norme per uso e conservazione corretti

dei codici di accesso è opportuno sensibilizzare gli utenti ad applicarle, spiegando anche i rischi derivanti da una loro violazione.

4.4 Misure e strumenti per l'analisi dello stato di funzionamento del TIX

4.4.1 VULNERABILITY ASSESSMENT

Nel paragrafo 3.7 dell'Offerta Tecnica [1] viene presentato il servizio di vulnerability assessment (VA) dei sistemi appartenenti alla rete RTRT da erogarsi, previa autorizzazione, da parte del gestore del TIX

Tale modalità è da considerarsi un caso particolare: infatti, questo genere di operazioni viene commissionato direttamente dal proprietario dei sistemi ad aziende o laboratori specializzati, senza l'intermediazione del gestore.

E' doveroso ricordare che esiste una dibattito assai acceso sull'efficacia di questo tipo di controlli, sia per quanto riguarda la metodologia più significativa di svolgimento, sia sul significato da attribuire ai risultati ottenuti. Per quanto riguarda la metodologia si è soliti distinguere i test:

- Automatici: i risultati sono prodotti quasi esclusivamente dell'esecuzione di software specifici
- Manuali: i risultati sono il prodotto delle abilità di un singolo o di un gruppo di specialisti che possono anche avvalersi di strumenti automatici.

Da un lato si sostiene che l'esclusivo utilizzo di software automatici per l'analisi delle vulnerabilità porta ad ottenere dei risultati poco significativi a causa dell'elevato numero di "falsi positivi", dall'altro si fa notare come siano veramente pochi i professionisti con l'esperienza e la preparazione necessaria per eseguire tali operazioni.

Indipendentemente dalla metodologia adottata per un vulnerability assessment è quindi necessario analizzare con molta cura i risultati ottenuti, in quanto possono essere perturbati dall'efficacia dello strumento nel primo caso, dalla preparazione del singolo nel secondo.

Per queste ragioni molto spesso la metodologia adottata è un compromesso tra le due: a svolgere i test sono specialisti del settore con provate referenze che si

avvalgono di strumenti automatici di cui analizzano successivamente in maniera critica i risultati ottenuti.

Pertanto il vulnerability assessment da eseguire sulla rete RTRT dovrebbe seguire tale modalità, attraverso una serie di passi così schematizzabili:

1. Individuazione di una classe di minaccie da testare (questa operazione è necessaria vista la mancanza di un modello unico di sicurezza)
2. Selezione di un gruppo di specialisti indipendenti dal gestore
3. Selezione degli obiettivi su cui svolgere il test
4. Indicazione dei tempi di inizio e di fine del test
5. Individuazione degli strumenti (software ed altro) con cui svolgere il test
6. Ottenimento delle autorizzazioni necessarie e notifica alle strutture interessate delle informazioni del punto 4.
7. Auditing dei risultati in base alle politiche di sicurezza della rete RTRT.

Analizzando l'offerta tecnica [1], si nota che ad effettuare tali operazioni dovrebbe essere l'RTI esclusivamente tramite strumenti automatici, non precisando chi eseguirà il test effettivamente nè quali esperienze specifiche abbia in materia. Non si trovano inoltre accenni alla necessità di accordarsi tra RTI e RT circa le minacce di cui valutare il grado di esposizione: la mancanza di questa fase può influenzare in maniera decisiva la successiva fase di analisi dei risultati ottenuti.

È da notare inoltre che i quattrocento indirizzi pubblici indicati al paragrafo 3.7.3 di [1] corrispondono ad un tasso di test dello 0,06 % se rapportato alla disponibilità di indirizzi pubblici della rete RTRT, senza considerare gli eventuali indirizzi privati "mascherati". E' quindi necessario trovare un metodo più rigoroso per quantificare il numero di test da effettuare in modo da poter considerare attendibili i risultati ottenuti.

L'attività di vulnerability assessment non può essere considerata sostitutiva di quelle di analisi del rischio e di auditing, che devono essere necessariamente eseguite prima della piena operatività della rete telematica regionale estesa agli operatori privati (ISP) accreditati.

Inoltre è previsto un servizio in più, dietro compenso aggiuntivo, per il VA da denial of service. Posto che il sistema deve essere configurato in modo tale da prevenire in attacco di tale tipo, questo servizio dovrebbe essere incluso e concertato con RT in base alle esigenze di funzionamento del sistema.

Resta il fatto che è universalmente riconosciuto il principio “chi esegue non verifica” anche a livello legislativo, per cui è necessario che il gestore si rivolga a un soggetto esterno per effettuare questo tipo di controllo.

4.4.2 LOG ED AUDIT

Una politica di sicurezza non può considerarsi completa senza una periodica attività di revisione dello stato del sistema; in questa fase la proprietà da garantire è la tracciabilità, ovvero la facoltà di associare un azione o un evento all’utente o al processo che lo ho creato o richiesto. Le informazioni di base da cui partire per un'attività di questo genere sono i file di log, che dovrebbero registrare in modo quanto più accurato possibile gli eventi che si verificano nel funzionamento del TIX. Analizzare il contenuto di questi files non è un’attività banale: spesso infatti può risultare difficile correlare le informazioni memorizzate ad un evento anomalo o ad un attacco. Per queste ragioni, questa attività dovrebbe essere svolta da personale esperto, in possesso di un certo bagaglio di esperienza su questo specifico aspetto, che periodicamente se non quotidianamente analizzi in modo accurato gli eventi segnalati.

Le informazioni registrate sono l’unica prova di cosa è accaduto e cosa stà accadendo nel funzionamento del TIX, pertanto è necessario approntare opportune misure per la loro corretta conservazione, in particolare, alcuni fattori critici su cui porre particolare attenzione sono:

- Scelta di un opportuno “metodo” di conservazione: evitare di conservare i file su apparati di “prima linea”, piuttosto valutare l’eventualità di un sistema di log centralizzato, in cui i dati vengano inviati ad una macchina designata per tale scopo, a cui accedere eventualmente soltanto da console

- Scelta dell'adeguato supporto di memorizzazione e di backup: i tipi di supporti scelti devono essere in grado di rimanere integri per il periodo di conservazione stabilito
- Scelta di un meccanismo "robusto" di controllo degli accessi sia per i file sia per copie di backup.

Può risultare utile l'uso di particolari tool di segnalazione automatica di eventi; tali programmi, previsti nel piano di lavoro, se configurati correttamente possono essere di aiuto per inviare una segnalazione tempestiva di una particolare situazione; in questo caso, come nel caso dell'analsi dei log, è compito dell'operatore che riceverà tale messaggio valutarne l'attendibilità, discernendo eventuali falsi positivi.

Se i log registrano cosa è accaduto e cosa stà accadendo, la fase di audit in un certo senso può scoprire cosa accadrà, o cosa potrebbe accadere: per audit si intende generalmente quel processo che, utilizzando le informazioni di log, cerca di apportare eventuali correttivi alla politica di sicurezza in uso, inserendo o modificando alcune norme. Come tale, questa fase è meno tecnica e più organizzativa, ma è l'unica in grado di migliorare il piano organizzativo messo in atto. In un certo senso, la fase di audit può essere pensata come un bilancio consuntivo delle attività del TIX in materia di sicurezza informatica, dove RTI e RTRT si incontrano per analizzarne il funzionamento, per capirne la situazione attuale, e per delineare scelte ed obiettivi futuri.

5. Bibliografia/riferimenti

[1] Offerta Tecnica per la realizzazione del TIX – 9 Novembre 2001

[2] Piano di Lavoro TIX – Tuscany Internet eXchange – 3 Febbraio 2003

[3] Bando di Gara TIX – luglio 2001

[4] Politiche di Sicurezza di Regione Toscana – 15 Dicembre 1999

[5] Direttiva del Presidente del Consiglio dei Ministri del 16 Gennaio 2002, Dipartimento per l'Innovazione e le Tecnologie http://www.innovazione.gov.it/ita/intervento/normativa/allegati/direttiva_sicurezza.pdf

[6] Direttiva del Presidente del Consiglio dei Ministri del 16 Gennaio 2002, Dipartimento per l'Innovazione e le Tecnologie - Allegato 2 http://www.innovazione.gov.it/ita/intervento/normativa/allegati/direttiva_sicurezza_all2.pdf

[7] Decreto Interministeriale "Istituzione del Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni" - Luglio 2002 http://www.innovazione.gov.it/ita/intervento/normativa/allegati/dm_240702.pdf

[8] Router Security Configuration Guide http://nsa2.www.conxion.com/cisco/guides/cis-2.pdf

[9] RFC 1918 "Address Allocation for Private Internet" http://www.ietf.org/rfc/rfc1918.txt?number=1918

[10] RFC 2827 "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing" http://www.ietf.org/rfc/rfc2827.txt?number=2827