PROCEDURE DI SICUREZZA

INSTALLAZIONE E HARDENING DA EFFETTUARE SU SERVER E DISPOSITIVI DI RETE DELLA FONDAZIONE

Release 1.0

07 Maggio 2010

Cambiamenti rispetto all'ultima release

- Si tratta della prima emissione

Introduzione

La fase di installazione del sistema operativo e più in generale di una macchina riveste un'importanza cruciale nell'intero processo di protezione dei dati e dei servizi poiché durante questa fase devono essere prese delle decisioni che possono influire in maniera decisiva sulla sicurezza dell'intero sistema informativo. La messa in sicurezza di una macchina server o di un dispositivo permette di:

- proteggere i dati critici contenuti nella maniera più idonea possibile,
- garantire un maggiore livello di servizio, disponibilità ed affidabilità,
- rendere più performanti i servizi erogati dalla macchina,
- ottenere un maggiore controllo e governo della macchina e degli accessi,
- avere meno problematiche gestionali sulla macchina.

La blindatura specifica per ogni macchina e per ogni servizio installato costituisce la base della sicurezza dell'intero sistema informativo e, come è noto, ogni anello della catena della sicurezza va preso in considerazione per innalzare il livello globale di protezione.

Finalità

L'attività di hardening consiste nel configurare una macchina (server, switch, router, firewall, altro dispositivo di rete o di sicurezza) in modo tale che sia il più difficile possibile da espugnare e prevede principalmente di agire sulla configurazione di sistema, servizi, applicazioni, utenze e privilegi. Tale operazione è tipicamente complementare ai sistemi di log auditing e ad una corretta politica di mantenimento della macchina stessa.

La presente procedura ha come scopo principale quello di fornire una serie di linee guida da seguire attentamente durante il processo di installazione, configurazione e messa in produzione di una macchina server o di un dispositivo di rete.

Ambito di applicabilità

Verranno di seguito elencate le linee guida e i passi organizzativi, tecnici e pratici che l'esperienza insegna possano aiutare a rendere più sicura una macchina o un dispositivo. Tali indicazioni dovranno essere seguite scrupolosamente sia dal personale interno che dal personale esterno alla Fondazione nel momento della configurazione e messa in produzione di:

- una macchina server,
- una macchina o un dispositivo di sicurezza,
- un dispositivo di rete.

I paragrafi che seguono sono suddivisi per argomenti (hardware, file system, servizi, applicazioni, utenze, gestione) e il titolo assegnato ad ognuno di essi fa parte di due categorie:

1. linee guida generali: direttive legate a qualsiasi tipologia di installazione si stia facendo e quindi di carattere generale,
2. linee guida specifiche: direttive legate strettamente ad una tipologia di ambiente o di dispositivo e che di conseguenza non vanno considerate per le altre tipologie.

NOTE IMPORTANTI

Questo documento è soltanto una guida contenente la descrizione di una serie di impostazioni il cui utilizzo è raccomandato per migliorare la sicurezza di una macchina o di un dispositivo; non vuole e non è destinato a sostituire le politiche e le linee guida (best practices) di sicurezza ben strutturate e raccomandate dal produttore del sistema operativo. Per cui chiunque utilizzi tale procedura deve considerare come maggiormente prioritarie e recenti le specifiche e le linee guida del sistema operativo e dei vari vendor.

Qualora la macchina o il dispositivo oggetto dell'hardening non fosse installata da zero ma esistesse già in produzione, è fortemente sconsigliato applicare le impostazioni descritte nel presente documento senza prima averle applicate e verificate con successo in un ambiente di test non operativo.

Linee guida generali: modalità di installazione

L1. Nell'installazione della macchina e del sistema operativo occorre attenersi scrupolosamente alle best practices più recenti fornite dal produttore dell'hardware e del sistema operativo. Ad avvenuta installazione occorrerà rendere noto formalmente (attraverso la redazione della scheda indicata nell'allegato 1 del presente documento) all'U.O. Sistemi Informativi ed Informatici le linee guida di riferimento utilizzate e i passi di hardening eseguiti.

L2. La scheda di cui al punto L1 si deve consegnare all'U.O. Sistemi Informativi ed Informatici unitamente a quella relativa alle specifiche principali della macchina installata (caratteristiche hardware, periferiche, sistema operativo, versioni, software installato, indirizzi IP, eventuali rotte, altre configurazioni particolari…). Tale scheda si trova nell'allegato 2 del presente documento.

L3. Salvo casi motivati e formalmente descritti nella scheda di cui all'allegato 1, qualsiasi server deve essere configurato in modo da risultare parte del dominio Windows della Fondazione.

L4. Non deve mai essere installato un server con funzionalità di dominio o di active directory: l'unico dominio approvato è quello dell'U.O. Sistemi Informativi ed Informatici Fondazione (Appendice 1).

L5. Non collegare la macchina alla rete se non sono stati preventivamente installati tutti gli aggiornamenti, le service pack, le patch e le hot fix più recenti, fatta eccezione per eventuali incompatibilità conosciute.

Linee guida generali : impostazioni hardware

L6. Salvo casi motivati e formalmente descritti nella scheda di cui all'allegato 1, è proibito installare un server o un dispositivo in locali non adibiti a CED dall'U.O. Sistemi Informativi ed Informatici Fondazione. Questo per poter garantire i seguenti sottopunti:

a. L'accesso al locale dove risiede la macchina che si vuole proteggere deve essere limitato e controllato.
b. E' fondamentale prevedere un sistema di climatizzazione per mantenere una temperatura adeguata nell'ambiente in cui va posizionata la macchina.
c. Occorre evitare eventuali danni fisici volontari o involontari posizionando la macchina in rack chiusi e con adeguati accorgimenti nella gestione e protezione dei cavi, sia di rete che elettrici.
d. Qualora il servizio erogato dalla macchina fosse reputato critico, è necessario utilizzare gruppi di continuità o gruppi elettrogeni, per consentire di continuare ad erogare elettricità anche in caso di problemi alla linea principale.
e. Il locale che ospiterà la macchina dovrà essere dotato di un adeguato e testato piano anti-incendio.

L7. Occorre impostare una password a protezione del BIOS della macchina come indicato nella *Politica di gestione delle password* della Fondazione. Tale password andrà conservata in cassaforte ed acceduta solo in casi di estrema e motivata necessità. Tale password verrà indicata nella scheda di installazione consegnata a fine lavori.

L8. E' necessario modificare la sequenza di boot predefinita, disabilitando il boot da floppy, da cdrom, da USB, da rete o da qualunque dispositivo che non sia quello di avvio predefinito.

L9. In caso di macchine linux o unix, occorre intervenire sul file di configurazione del bootloader, in maniera tale che quest'ultimo chieda l'inserimento di una password solo se si cerca di passare qualche parametro al kernel (nel caso di LILO si tratta di impostare l'opzione *Restricted* nel file */etc/lilo.conf*). Tale password, specificata nello stesso file, sarà la stessa di quella utilizzata per la modifica del BIOS. E' ovvio che tale file sia accessibile dal solo utente root. Tale impostazione dovrà essere indicata nella scheda di installazione consegnata a fine lavori.

L10. Sempre relativamente al bootloader delle macchine linux e unix, potrebbe essere una buona idea anche prevedere due differenti "etichette". Una per il normale avvio del server, ed una seconda per eventuali operazioni di manutenzione, avviando il sistema con un determinato runlevel (ad esempio 4) dove sono stati disattivati tutti i servizi non necessari.

L11. E' consigliato disabilitare il riavvio del sistema da tastiera tramite la combinazione dei tasti CTRL+ALT+CANC.

L12. In caso di installazione di macchine critiche, è necessario avere i dischi configurati in RAID 1 o in RAID5, a maggiore garanzia di protezione e disponibilità di dati e servizi.

L13. I driver delle varie periferiche hardware devono essere certificati per la piattaforma su cui sono stati installati e a completamento dell'attività vanno consegnati su supporto magnetico all'U.O. Sistemi Informativi ed Informatici.

L14. In caso di installazione di macchine critiche, è necessario avere l'alimentazione e le schede di rete ridondate.

L15. Qualora la macchina fosse collegata a NAS/SAN, deve essere impostata un'apposita VLAN e il loro accesso deve essere configurato sul relativo firewall (i dettagli tecnici necessari a tale operazione possono essere richiesti all'U.O. Sistemi Informativi ed Informatici).

L16. **SOLO ed esclusivamente** per i server installati nell'ambito del sistema di **virtualizzazione vmware** messo a disposizione dalla Fondazione ci si deve attenere alle seguenti disposizioni:

   a. tutte le macchine virtuali devono avere installato l'ultima versione di VMware Tools specifica del sistema operativo (il file di installazione verrà messo a disposizione dall'U.O. Sistemi Informativi ed Informatici),
   b. compilare debitamente il modulo richiesto dall'UOSII per la configurazione del firewall a protezione dei sistemi virtuali,
   c. per i sistemi windows, disabilitare il servizio "Ora di Windows" e impostare la sincronizzazione del server con l'host fisico nei VmWare Tools,
   d. per i sistemi linux, disabilitare la sincronizzazione del clock nei VmWare Tools ed impostare il server NTP della Fondazione nel sistema operativo,
   e. per i sistemi windows, consentire l'accesso remoto anche all'utente "administrator",
   f. per tutto quanto non contemplato valgono le indicazioni relative ai server fisici a cui si riferisce tutta la presente procedura.

Linee guida generali: file system

L17. Non consentire agli utenti il montaggio delle unità rimovibili quali cdrom, dischetti e pendrive.

L18. Evitare che vengano montate unità rimovibili automaticamente durante la fase di boot.

L19. L'utilizzo delle quote disco consente di limitare lo spazio che un utente o un gruppo di utenti può avere sulla macchina. Ai fini della sicurezza, imporre dei limiti è sicuramente utile, ad esempio per impedire che un utente possa riempire tutto lo spazio assegnato. Le quote impostate andranno indicate nella scheda di installazione consegnata a fine lavori.

L20. Verificare che non vi siano cartelle, programmi o file scrivibili da tutti gli utenti ad eccezione delle aree di scrittura temporanea.

L21. L'unico protocollo di rete aziendale "riconosciuto" è il tcp/ip v.4, per cui tutti gli altri protocolli devono essere disabilitati (novell ipx/spx, tcp/ip v.6, netbios over tcp/ip, …).

Linee guida specifiche: file system in ambienti Linux e Unix

In aggiunta alle linee guida per il file system sopra elencate, si devono seguire le seguenti indicazioni inerenti nello specifico gli ambienti Linux o Unix:

L22. Per non rischiare di incorrere in perdita di dati a seguito di assenza di corrente o di spegnimento brutale della macchina, il filesystem scelto deve essere di tipo journaled.

L23. Porre le directory scrivibili pubblicamente, come ad esempio */tmp* o */var/tmp* in partizioni separate dal resto del sistema. Lo stesso discorso vale per le directory */home* e */usr* e per le directory che contengono i log come ad esempio */var/log*. Il partizionamento effettuato andrà indicato nella scheda di installazione consegnata a fine lavori (Allegato 2).

L24. Impedire l'esecuzione di programmi e script su alcune cartelle, tramite ad esempio l'opzione noexec. Questo vale certamente per directory condivise in rete e per le unità rimovibili quali dischi floppy, cdrom e pendrive.

L25. Impedire l'uso dei bit SUID/SGID nelle directory dove sono presenti i diversi eseguibili. Se esiste la reale necessità di eseguire un programma con permessi particolari è meglio utilizzare il comando *sudo*. Tale reale necessità, richiesta formalmente, è obbligatorio che venga approvata dall'U.O. Sistemi Informativi ed Informatici.

L26. Disabilitare il bit SUID a tutti quegli eseguibili che non devono essere lanciati dagli utenti attraverso la linea di comando, come ad esempio */bin/login*, *usr/bin/chsh*, */usr/bin/newgrp*, */usr/bin/gpasswd*, *mount* ed *umount*.

L27. Consentire la registrazione del tempo di accesso ad un file, ad esempio evitare l'utilizzo dell'opzione *noatime*.

L28. Utilizzare le ACL per gestire permessi e privilegi eccezionali, evitando di essere laschi nei permessi associati a gruppi.

L29. Installare *sudo* e configurare opportunamente il relativo file */etc/sudoers* per consentire e distribuire capillarmente le operazioni amministrative ad utenti amministrativi ma non root.

Linee guida specifiche: file system in ambienti Windows

In aggiunta alle linee guida per il file system sopra elencate, si devono seguire le seguenti indicazioni inerenti nello specifico gli ambienti Windows:

L30. Nel limite del possibile, occorre suddividere lo spazio disco in tre partizioni: la prima dedicata al sistema operativo, la seconda agli applicativi e la terza ai dati degli applicativi e degli utenti. Il partizionamento effettuato andrà indicato nella scheda di installazione consegnata a fine lavori (Allegato 2).

L31. Per poter usufruire delle caratteristiche di sicurezza, efficienza e compressione dei dati fornite da Windows bisogna creare tutte le partizioni utilizzando esclusivamente il file system NTFS.

L32. Subito dopo l'installazione è opportuno azzerare i privilegi esistenti per tutte le partizioni logiche di tutti i dischi in modo da rimuovere ogni occorrenza del gruppo Everyone.

L33. Rimuovere *Everyone*, *All Users* e *Authenticated Users* dalla root del sistema. Cambiare i permessi di *%SystemRoot%\repair* e impostare che solo *Administrators* e *Systems* vi hanno accesso (full access).

L34. Da registry, disabilitare *AutoRun* per i driver CD-ROM.

L35. Proteggere le chiavi di registro relative al servizio SNMP (se lasciato running): impostare l'accesso in modo "*Administrators – Full Control*" e "*System – Full Control*".

L36. Se non in contrasto con quanto installato sulla macchina, si consiglia di proteggere le seguenti chiavi impostando l'accesso a "*Administrators and System - Full Control*", "*Authenticated Users – Read*".

a. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
b. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
c. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
d. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall
e. HKEY_LOCAL_MACHINE\Software\Microsoft\DrWatson (lasciare inalterati i permessi del Terminal Server User, se esistono)
f. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg

L37. Controllare che solo *administrators* and *backup operators* siano abilitati all'accesso ai registry.

L38. Nelle *Local Security Policy*, abilitare il flag "Network security: Do not store LAN Manager hash value on next password change".

Linee guida specifiche: sistema operativo Windows

L39. Qualora il server fosse posizionato sul confine fra il mondo esterno e il mondo interno alla Fondazione, occorre evitare che si trovi esposto ad una serie di debolezze intrinseche del protocollo NetBios su TCP/IP (nonché di SMB/CIFS), disabilitando tali protocolli esclusivamente sul lato pubblico delle connessioni.

Linee guida generali: servizi

La configurazione dei servizi è una fase molto importante ed in quanto tale dovrebbe essere posta in essere tenendo bene a mente due principi fondamentali:

L40. Eseguire un numero di servizi minimo assolutamente indispensabile per il corretto funzionamento del server e disabilitare tutti gli altri: questa pratica oltre ad avere un impatto positivo sia sulle risorse che sugli oneri di amministrazione riduce drasticamente le probabilità di trovarsi in presenza di un servizio che cela al suo interno una grave vulnerabilità.

L41. Tra i servizi precedentemente individuati eseguire automaticamente all'avvio soltanto quelli che effettivamente lo richiedono ed impostare invece tutti gli altri in modo da essere lanciati manualmente.

L42. I servizi non devono avviarsi o essere eseguiti come utente root o administrator.

L43. Eseguire ciascun servizio con il minimo dei privilegi necessari per il suo corretto funzionamento onde evitare il tipo di inconvenienti prima citati.

L44. Mantenere una lista aggiornata e periodicamente verificata in merito ai servizi attivi ed eseguiti automaticamente all'avvio (ovvero aggiornare la scheda tecnica di installazione di cui l'allegato 2 ad ogni variazione e consegnarla all'U.O. Sistemi Informativi ed Informatici).

Linee guida generali: applicativi

L45. Mantenere una lista aggiornata e periodicamente verificata in merito a cosa è installato sulla macchina e quali programmi sono attivi (ovvero aggiornare la scheda tecnica di installazione di cui l'allegato 2 ad ogni variazione e consegnarla all'U.O. Sistemi Informativi ed Informatici).

L46. Disabilitare o meglio disinstallare i programmi non utilizzati.

L47. Verificare periodicamente che tutti i file di configurazione siano corretti e conformi alle politiche.

L48. Verificare che i programmi abbiano i permessi necessari per il loro funzionamento e non oltre.

L49. I programmi non devono avviarsi o essere eseguiti come utente root o administrator.

L50. Verificare che le cartelle in cui risiedono i programmi, i file di configurazione dei programmi stessi ed i file di configurazione negli account degli utenti abbiano le protezioni corrette.

L51. Occorre essere certi che non sia possibile accedere ad applicazioni sia da locale che da remoto senza password o con le password di default inserite dal vendor, come ad esempio snmp, l'accesso a database, interfacce web di gestione etc…

Linee guida generali: utenze

L52. Disabilitare account e gruppi inutili.

L53. Impostare una password di amministrazione (administrator o root) molto lunga e complessa secondo quanto definito nella *Politica di gestione delle password* della Fondazione ed affidarla alla custodia dell'U.O. Sistemi Informativi ed Informatici. Prima di effettuare tale passo occorre definire gli utenti locali con i loro associati e minimi poteri di amministrazione.

L54. Solo l'U.O. Sistemi Informativi ed Informatici della Fondazione può, in casi eccezionali, adoperare la password di amministrazione prendendola dalla cassaforte e cambiandola prima di rimetterla in busta chiusa al suo interno.

L55. Tutti gli account amministrativi interni ed esterni devono essere nominali e ad essi devono essere associati i privilegi minimi affinché possano eseguire esclusivamente il lavoro a loro affidato.

L56. Raggruppare gli utenti in gruppi in base alle attività che ciascuno di essi deve compiere ed assegnare al gruppo di appartenenza soltanto i privilegi minimi indispensabili.

L57. Gli account associati a servizi o all'interno di batch o script devono avere un'utenza specifica a loro associata e con privilegi minimi per poter svolgere la propria funzione. In nessun caso un servizio deve partire con account administrator o root.

L58. Con la sola eccezione delle macchine virtuali (punto L16), è necessario impedire l'accesso all'utente root o administrator da remoto, ma permetterlo solo da console o da un altro utente della macchina (se necessario creare un utente da utilizzare per accedere alla macchina da remoto).

Linee guida generali: log, auditing e gestione

L59. Devono essere conservati localmente alla macchina i log generati per almeno sei mesi, specialmente quelli relativi alla sicurezza. Deve essere effettuata una rotazione dei log tale per cui al termine del periodo definito avvenga la sovrascrittura di quelli più vecchi con quelli nuovi.

L60. I log, oltre che localmente, devono essere spediti ad un server centrale della Fondazione. Questo comporta l'installazione, sulle macchine critiche e sulle macchine che contengono dati sensibili, di un client Symantec per la spedizione dei log a norma di legge. I dettagli tecnici per poter effettuare le operazioni possono essere richiesti all'U.O. Sistemi Informativi ed Informatici (Appendice 1).

L61. Impostare il client NTP per sincronizzare la macchina con l'NTP Server della Fondazione i cui riferimenti possono essere richiesti all'U.O. Sistemi Informativi ed Informatici (Appendice 1).

L62. Occorre fornire alla Fondazione i file e le cartelle da sottoporre a backup per quanto riguarda la configurazione e le funzionalità del sistema.

L63. L'amministrazione della macchina deve essere effettuata mediante strumenti sicuri che garantiscano la cifratura del canale trasmissivo fra la postazione richiedente e la macchina (ad esempio *SSH* e non *TELNET*).

L64. Se possibile, prevedere l'utilizzo di un sistema di verifica dell'integrità del file system, per poter verificare eventuali modifiche di file e cartelle.

L65. Mantenere la macchina aggiornata con i più recenti upgrade e patch di sicurezza, e utilizzarla esclusivamente per lo scopo ad essa associato. Qualora taluni aggiornamenti non fossero possibili occorre comunicare formalmente all'U.O. Sistemi Informativi ed Informatici mediante la scheda tecnica di installazione di cui all'allegato 2:

   a. la descrizione dell'aggiornamento non possibile,
   b. la motivazione che non permette l'aggiornamento,
   c. l'eventuale work-around o consiglio che viene proposto per limitare al massimo il rischio.

L66. Su tutte le macchine deve essere installato il client antivirus della Fondazione. Nella scheda di installazione della macchina, il fornitore deve indicare le eventuali cartelle da escludere sia dalla protezione real-time sia dalla full scan settimanale in modo da non pregiudicare l'esecuzione dell'applicativo installato. Il fornitore deve anche indicare un giorno e un orario idoneo per pianificare la scansione settimanale.

L67. Non utilizzare mai la macchina come postazione di lavoro o di navigazione.

L68. Per tutte le macchine linux-unix e per tutte le macchine windows non inserite in dominio, occorre impostare le seguenti politiche di logging:

   a. Eventi di logon e logoff alla macchina (tutti, ovvero da console, locali, remoti): sia il successo che il fallimento

b. Eventi legati alla gestione degli account: sia il successo che il fallimento
c. Cambiamenti alle politiche di audit e di sicurezza: sia il successo che il fallimento
d. Eventi legati all'utilizzo di privilegi: solo il fallimento
e. Eventi di stop e start della macchina: sia il successo che il fallimento

L69. Verificare periodicamente che le password utilizzate rispettino le politiche di sicurezza definite e che nessun utente abbia accesso alla macchina senza una password.

L70. Appena completata l'installazione dell'apparato o della macchina occorre effettuare una scansione di sicurezza con idoneo strumento. Il report di tale attività va consegnato all'U.O. Sistemi Informativi ed Informatici. L'operazione di scansione va eseguita periodicamente e ad ogni variazione sensibile della configurazione, ovvero a seguito di importanti aggiornamenti oppure dopo nuove installazioni.

Linee guida specifiche: switches e routers

L71. Conservare la password in maniera sicura e non facilmente ricavabile (assolutamente non in chiaro), ad esempio utilizzando un hash MD5. Se possibile utilizzare l'autenticazione via Radius.

L72. Inserire un banner all'accesso per rendere evidente che si tratta di un'area ristretta e riservata ed aggiungendo la parte che acconsente il tracciamento della sessione[1].

L73. Impostare correttamente il protocollo NTP (sia ora che time zone) per sincronizzare i router con l'NTP Server della Fondazione i cui riferimenti possono essere richiesti all'U.O. Sistemi Informativi ed Informatici (Appendice 1).

L74. Configurare la conservazione dei log per almeno un mese con sovrascrittura automatica degli eventi vecchi una volta giunti alla fine della finestra temporale scelta. Qualora il dispositivo in questione abbia scarse possibilità di spazio, è accettabile una conservazione di almeno una settimana.

L75. Impostare come syslog server l'indirizzo IP della macchina della Fondazione predisposta a tale scopo, i cui dati tecnici possono essere richiesti all'U.O. Sistemi Informativi ed Informatici (Appendice 1).

L76. Se possibile, si consiglia di abilitare il timestamp sui log e disabilitare la traduzione dei nomi DNS nei log.

L77. Effettuare il tuning della CPU per garantire il tempo minimo per i processi vitali.

L78. Disabilitare tutti quei servizi non necessari al corretto funzionamento dell'apparato.

L79. Disabilitare i servizi di *telnet* e *tftp* e gestire l'apparato esclusivamente attraverso *SSH*.

L80. E' bene restringere solo a determinati IP l'accesso via rete all'apparato attraverso le ACL. Richiedere all'U.O. Sistemi Informativi ed Informatici le eventuali ulteriori ACL da impostare.

[1] Un esempio potrebbe essere il seguente: "This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials."

L81. Impostare l'SNMP in modo tale da limitare gli attacchi, ad esempio restringendo tramite ACL le macchine abilitate alla gestione e scegliendo communities non facilmente intuibili. Richiedere all'U.O. Sistemi Informativi ed Informatici l'eventuale presenza di un server SNMP a cui collegarsi (Appendice 1).

L82. Effettuare almeno mensilmente una copia di backup della configurazione dell'apparato. Lasciando inalterata la periodicità mensile, occorre effettuare una copia di backup anche a seguito di una qualsiasi variazione della configurazione stessa.

Linee guida specifiche: ulteriori azioni previste per i routers

L83. Nell'ottica di effettuare un miglioramento dello stack IP del router, è consigliabile abilitare l'algoritmo di *Nangle* per la gestione del controllo della congestione (RFC 896), limitare il tempo di timeout dei pacchetti *Syn*.

L84. Configurare il router nel pieno rispetto degli standard RFC 1323 (TCP Extensions for High Performance) e RFC 2018 (TCP Selective Acknowledgment Options).

L85. Alcuni broadcast effettuati in UDP vengono ruotati di default. E' necessario capire se qualcuno di questi sia realmente utilizzato, ad esempio per il DHCP, ed abilitare solo quello corrispondente. Disabilitare quindi tutti i broadcast UDP ad eccezione di quelli utilizzati.

L86. Secondo quanto reso disponibile dalla tecnologia utilizzata, configurare l'apparato in maniera tale che sia protetto da *denial of service* o *smurf attack*.

L87. Consentire solamente i seguenti tipi di ICMP: echo, *echo-reply*, *unreachable*, *time-exceeded*, *ttl-exceeded* e *packet-too-big*. Consentire i redirect solo se effettivamente necessario rispetto alla topologia di rete; negare tutti i rimanenti.

L88. Se non necessaria, disabilitare la funzionalità di *proxy-arp* da tutte le interfacce.

ALLEGATO 1

ADERENZA ALLE LINEE GUIDA DELLA PROCEDURA

(da consegnare all'U.O. Sistemi Informativi ed Informatici ad avvenuta installazione, dopo averla compilata ed allegata alla scheda di installazione di cui all'allegato 2)

Elenco Best Practices e Linee guida utilizzate per piattaforma, database e applicativi

Linea Guida	Effettuata (SI/NO)	Motivazione (in caso di NO)
L1		
L2		
L3		
L4		
L5		
L6		
L7		
L8		
L9		
L10		
L11		
L12		
L13		
L14		
L15		
L16		
L17		
L18		
L19		
L20		
L21		
L22		

L23		
L24		
L25		
L26		
L27		
L28		
L29		
L30		
L31		
L32		
L33		
L34		
L35		
L36		
L37		
L38		
L39		
L40		
L41		
L42		
L43		
L44		
L45		
L46		
L47		
L48		
L49		
L50		
L51		
L52		
L53		
L54		
L55		
L56		
L57		

L58		
L59		
L60		
L61		
L62		
L63		
L64		
L65		
L66		
L67		
L68		
L69		
L70		
L71		
L72		
L73		
L74		
L75		
L76		
L77		
L78		
L79		
L80		
L81		
L82		
L83		
L84		
L85		
L86		
L87		
L88		

ALLEGATO 2

SCHEDA TECNICA DI INSTALLAZIONE

Installazione	
Data di consegna	
Tipologia (dispositivo, server, firewall…)	
Funzione principale a cui il server/dispositivo è adibito	
Piattaforma e versione	
Nome macchina	
Password di accesso al BIOS	

Dischi interni	
Nome della partizione	Dimensionamento
Tipologia RAID	

Dischi esterni	
Tipologia Storage (NAS/SAN)	
Dimensionamento	
Tipologia RAID	

Rete	
Indirizzo/i IP e subnetmask	
Default gateway	
Eventuali rotte statiche	
Appartenenza a VLAN	

Servizi	
Elenco servizi che partono automaticamente (con indicato fra parentesi con che account)	

Applicativi installati		
Nome dell'applicativo	Scopo	Versione

Utenze locali (utente, servizi, batch, script…)			
username	descrizione	password (da non indicare se riferita a utente)	quota (da non indicare se riferita a utente)
Administrator o root	amministrazione		

Scansione	
Data della scansione	
Strumento utilizzato	
Elenco porte aperte	

Aggiornamenti e patch	
Patch	Motivazione della non avvenuta installazione

Backup (lista file e cartelle da sottoporre a backup)

APPENDICE 1

DETTAGLI TECNICI DELLA FONDAZIONE

Antivirus server	Symantec Endpoint Protection 11 (172.31.233.208)
NTP Server	Router Cisco (172.31.230.94 e 172.31.230.95)
Syslog server	Kiwi Syslog Deamon (172.31.233.194)
SNMP server	SNMPC (172.31.233.194 e 172.31.233.169 e 10.9.230.103)
Centralizzazione	Symantec Security Information Manager (172.31.234.7)
Dominio Microsoft	Windows 2003 (2000server.omm)