ÍNDEX

Versió	Redactat / revisat per	Data publicació	Descripció
1.0.	CTTI – Qualitat i Seguretat	28/09/2006	Versió inicial
2.0	Jordi Casas – Oficina de Seguretat	01/03/2007	Revisió aplicació OpenSSH i actualització de versions de programari

Estàndard signat digitalment pel:

Generalitat de Catalunya

Centre de Telecomunicacions i Tecnologies de la Informacio
Estàndard aprovat
Barcelona
2007.03.13 13:28:52 +01'00'

RESPONSABLE DEL DOCUMENT: Oficina de Seguretat - CTTI

1. OBJECTIU I MOTIVACIÓ

L'objectiu d'aquest document és oferir recomanacions en l'ús d'eines per a realitzar comunicacions segures en el nus corporatiu i en els sistemes d'informació dels Serveis TIC Centrals de Caràcter Continuat de la Generalitat de Catalunya gestionats pel CTTI (d'ara endavant "*Serveis TIC Centrals*").

Aquesta manual inclou algunes recomanacions de xifrat i comunicacions segures per a les tasques més habituals que requereixen de l'ús dels sistemes d'informació dels *Serveis TIC Centrals*.

2. ÀMBIT I VIGÈNCIA

Aquest manual va dirigit a tota persona, departament, organisme o empresa contractista que faci ús del nus corporatiu, i en particular a tota persona que utilitzi eines d'administració remota (consoles de text i gràfiques) i eines de transferència remota de fitxers.

Aquest manual romandrà vigent fins la propera versió revisada del mateix.

3. DESCRIPCIÓ

3.1. Eines gràfiques d'administració remota

El següent recull ofereix detalls de configuració d'algunes de les eines gràfiques d'administració remota de sistemes més utilitzades. Aquestes eines, configurades de forma correcta, ofereixen tots els controls i compleixen totes les normes de seguretat per a la realització de les tasques d'administració.

Els següents aspectes s'han de tenir en compte en la configuració d'aquests programaris:

- Xifrar la sessió (màxim)
- Xifrar el logon (màxim)
- Limitar les connexions només des de les IP que han d'administrar els equips
- Limitar el nombre i el temps dels intents de logon per cada connexió
- Limitar el temps d'inactivitat i el temps de connexió
- Forçar el log off en finalitzar la sessió

TERMINAL SERVER/REMOTE DESKTOP

Aquesta és la solució propietària de Microsoft per a l'administració remota d'equips. Utilitza el protocol RDP (Remote Desktop Protocol), que a partir de la versió RDP 5.0 ofereix els requisits mínims de seguretat exigibles.

RDP és el protocol utilitzat per els programes *Terminal Services Advanced Client* (TSAC)*, Terminal Server Client, Remote Desktop* (Escriptori Remot) i *Remote Assistance* (Assistència Remota). La versió 5.0 és la utilitzada per el client TSAC per les últimes versions de Windows 2000 i per els clients i sistemes operatius posteriors.

També algunes eines de programari lliure que es troben per a sistemes Linux, com rdesktop (http://www.rdesktop.org/) i tsclient (http://www.gnomepro.com/tsclient/), ofereixen suport per a connectar amb servidors RDP.

PCANYWHERE

És un dels programaris comercials més estesos. Les versions a partir de la 11.5 (l'actual és la 12.0) i posteriors ofereixen els requisits desitjables de seguretat, com el xifrat de les comunicacions i l'autenticació Windows.

El programari té suport per als següents Sistemes Operatius:

- Windows® XP Home/XP Pro/2000 Pro/2000 Server/2003 Server (Host, Remote & Gateway);
- Windows NT® 4/Me/98 (Host & Remote only);
- Windows XP Pro x64/2003 Server x64 (Host & Gateway only).

Suporta els següents tipus d'autenticació:

- Contra Active Directory (W2000)

- Contra LDAP
- Autentificació NT (W2000 i NT)

Més informació a: http://www.symantec.com/home_homeoffice/products/remote_pc_fax/pca12/index.html

DAMEWARE

Una altra alternativa són els programaris desenvolupats per DameWare (NT Utilities i Mini Remote Control). Les versions a partir de la 4.9 (l'actual és la 5.5) i posteriors ofereixen els requisits desitjables de seguretat.

El programari té suport per versions de Windows a partir de NT 4.0 SP1 i superiors.

Més informació a: http://www.dameware.com/

VNC

Existeixen en el mercat moltes solucions diferents que utilitzen VNC com a eina d'administració remota, per a sistemes Windows, UNIX i MacOS. Gran part d'aquestes solucions tenen suport per als requisits de seguretat que s'han de complir, com ara xifrat de la sessió, autentificació segura, etc.

Aquesta solució és una bona alternativa als programaris comercials per administració remota d'equips Windows; també és una bona alternativa a les X-Windows per a Linux, que no disposa del nivell de seguretat adequat.

Per a versions de programes VNC que no ofereixin les opcions de xifrat de comunicacions requerides existeix la possibilitat d'utilitzar un túnel segur mitjançant SSH. Aquesta possibilitat existeix també per a les X-Windows. En el *punt 3.4* es poden trobar alguns consells sobre la manera de crear aquests túnels.

NOTA: Existeix una vulnerabilitat crítica en el programari RealVNC que permet realitzar obtenir l'accés a un sistema sense necessitat de contrasenya. S'han publicat noves versions que solucionen aquesta vulnerabilitat:

- Free Edition versió 4.1.2.
- Personal Edition/Enterprise Edition versió 4.2.3.

3.2. Programari de consola d'administració remota Secure Shell (SSH)

Consoles remotes d'administració: part servidor

Es recomana per simplicitat, fiabilitat i compatibilitat l'ús de Secure Shell (SSH) per a l'administració per consola remota. OpenSSH (www.openssh.com) és la opció més robusta i estesa com a servidor SSH i es distribueix sota llicència lliure BSD. Les principals característiques són:

- Suport per a la majoria de les plataformes
- Suport per a totes les versions del protocol SSH
- Xifrat 3DES, Blowfish, AES i Arcfour
- Capacitat de fer Port Forwarding (redirigir ports) cap a un túnel segur per a protocols com X-Windows, FTP, Telnet 3270, VNC insegur, etc.
- Autentificació robusta i compressió de dades
- Suport per a client i servidor SFTP. Cal tenir en compte que aquesta funcionalitat no permet aplicar chroot ("engabiat") dels usuaris. En cas de requerir-se aquesta funcionalitat, cal utilitzar altres productes (veure punt 3.3).

A continuació s'enumeren algunes de les solucions més utilitzades com a servidor de Secure Shell (SSH) per a diferents plataformes:

- OpenSSH (multiplataforma, llicència lliure BSD): http://www.openssh.com
- Pragma FortressSSH (Windows, comercial): http://www.pragmasys.com/Fortress/
- FreeSSHd (Windows, gratuït): http://www.freesshd.com
- WeOnlyDo wodSSHServer (ActiveX Component, comercial): http://www.weonlydo.com/index.asp?showform=SSHServer
- SSH Tectia Server (multiplataforma, comercial): http://www.ssh.com

- BitVise WinSSHD (Windows, comercial): http://www.bitvise.com/winsshd.html

Un llistat amb altres programaris es pot trobar en el lloc web http://freessh.org/ .

Consoles remotes d'administració: part client

Per la connexió via SSH existeix un gran nombre de clients per a la majoria de les plataformes. Alguns dels més estesos són:

- Putty (http://www.chiark.greenend.org.uk/~sgtatham/putty/) Llicència lliure MIT
- SSH Client (http://www.ssh.com/support/downloads/secureshellwks/non-commercial.html) Producte comercial, però la versió 3.2 es continua oferint de forma gratuïta.
- Comanda *ssh* (generalment ja instal·lada des de l'inici en les distribucions UNIX)
- MacSSH (www.macssh.com) Programa lliure per a MacOS
- BlueZone (http://www.seagullsoftware.com/products/bluezone/terminal-emulation.html) Comercial

Un llistat amb altres programaris es pot trobar en el lloc web http://freessh.org/ .

3.3. Programari de transferència segura de fitxers SCP i SFTP

Transferència remota de fitxers: part servidor

Es recomana l'ús de SFTP o SCP per a la transferència segura de fitxers.

A continuació s'enumera algunes de les solucions més utilitzades com a servidor de Secure Copy (SCP) i Secure FTP (SFTP):

- SSH Tectia Server (Multiplataforma, comercial): http://www.ssh.com
- HP-UX Secure Shell (HP-UX, gratuït): http://h20293.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=T1471AA
- GlobalScape Secure FTP Server (Windows, comercial): http://www.globalscape.com/gsftps/secure_ftp_server.asp
- Pragma FortressSSH (Windows, comercial): http://www.pragmasys.com/Fortress/
- FreeFTPd (Windows, gratuït): http://www.freeftpd.com
- BitVise WinSSHD (Windows, comercial): http://www.bitvise.com/winsshd.html
- Platypus Secure FTP Server (multiplataforma, gratuït): http://www.jscape.com/platypus/index.html
- FileZilla Server (Windows, gratuït): http://filezilla.sourceforge.net

Un llistat amb altres programaris es pot trobar en el lloc web http://freessh.org/ .

Transferència remota de fitxers: part client

Un gran nombre de clients FTP ofereixen suport per a SFTP i/o SCP; també existeix un gran nombre de programes específics per a SFTP i SCP, molts d'ells gratuïts. Alguns d'ells són:

- WinSCP (http://winscp.net/eng/docs/lang:es) Gratuït
- FileZilla (http://filezilla.sourceforge.net/) Llicència lliure GPL
- GlobalScape CuteFTP (http://www.cuteftp.com/cuteftp/) Comercial
- Comandes *sftp* i *scp* (generalment ja instal·lades des de l'inici en les distribucions UNIX)
- SSH Client (http://www.ssh.com/support/downloads/secureshellwks/non-commercial.html) Producte comercial, però la versió 3.2 es continua oferint de forma gratuïta.
- PSFTP (http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html) Llicència lliure MIT, client SFTP en línia de comandes
- PSCP (http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html) Llicència lliure MIT, client SCP en línia de comandes
- SecureFX (http://www.vandyke.com/products/securefx/index.html) Comercial
- WS_FTP (http://www.ipswitch.com/products/ws_ftp/index.asp) Comercial
- BlueZone (http://www.seagullsoftware.com/products/bluezone/secure-ftp.html) Comercial
- Glub Tech Secure FTP (http://www.glub.com/products/secureftp/) Gratuït, multiplataforma.

Un llistat amb altres programaris es pot trobar en el lloc web http://freessh.org/ .

3.4. Altres recomanacions i solucions de xifrat de comunicacions

Transferència segura de pàgines web amb Macromedia/Adobe Dreamweaver
Les versions de Dreamweaver a partir de la MX-2004 i posteriors (la versió actual és la 8.0) tenen suport directe de SFTP per a la càrrega de fitxers si es selecciona l'opció en la configuració del programari.

Per a versions anteriors, es pot fer la càrrega de forma segura sense necessitat de programes SFTP externs a través de l'ús de un programa de consola remota SSH. Una guia detallada de com fer-ho es pot trobar en l'enllaç http://www.adobe.com/cfusion/knowledgebase/index.cfm?id=tn_16126 (Windows) i http://www.adobe.com/cfusion/knowledgebase/index.cfm?id=tn_16143 (MacOS)

Superposició d'una capa SSL a un servidor FTP
Alguns programes com el *Glub Tech Secure FTP Wrapper* (http://www.glub.com/products/ftpswrap/) ofereixen la possibilitat de superposar una capa de xifrat SSL a qualsevol servidor FTP sense suport per a xifrat.

Aquest programari té suport per a qualsevol sistema Windows, MacOS i UNIX amb JAVA.

Creació de túnels SSH per a protocols insegurs
Una altra solució per a xifrar les comunicacions amb un servidor FTP insegur és la creació d'un túnel SSH. De fet, es pot utilitzar aquesta tècnica per a xifrar les comunicacions de qualsevol protocol que sigui insegur. L'únic requisit és disposar d'un servidor i un client SSH amb la capacitat de fer túnels (port-forwarding), com la majoria dels programaris SSH disponibles.

La tècnica consisteix en redirigir tot el tràfic d'un port local al costat del client per SSH cap al servidor SSH en l'altre extrem. Un cop allà el tràfic es redirigirà al port insegur local pertinent. Per a fer la comunicació, el client connectarà al port local del costat client escollit.

Les dues solucions següents fan referència a dos casos concrets de túnels SSH.

Creació d'un túnel SSH per a VNC
Per a les versions de programaris VNC que no tenen suport per al xifrat de les dades es pot utilitzar la tècnica dels túnels SSH. En el següent enllaç es pot consultar una guia explicativa de la tècnica: http://www.vanemery.com/Linux/VNC/vnc-over-ssh.html

Creació d'un túnel SSH per a X-Windows
Una de les solucions més esteses per a l'administració remota d'equips Linux és l'ús de les X-Windows de forma remota. En el següent enllaç (http://www.vanemery.com/Linux/XoverSSH/X-over-SSH2.html) es mostra una guia de com crear un túnel per a xifrar el tràfic X-Windows i preservar la confidencialitat de les dades enviades.

Nota: l'ús de X-Windows de forma remota té un consum d'ample de banda molt elevat, fins i tot utilitzant tècniques de compressió, fet que s'ha de tenir en compte i que converteix la solució en un mal sistema per a ser empleat en l'entorn corporatiu. És per aquest motiu que no ha de ser usat a menys que no hi hagi cap altra alternativa.

4. DIVULGACIÓ

El CTTI publicarà aquest manual a la seva intranet.

L'Oficina de Seguretat serà responsable de la distribució d'aquest manual en l'entorn de *Serveis TIC Centrals*.

5. GLOSSARI DE TERMES

Serveis TIC Centrals: Serveis TIC Centrals de Caràcter Continuat de la Generalitat de Catalunya, gestionats pel Centre de Telecomunicacions i Tecnologies de la Informació (CTTI).

6. PARAULES CLAU

Protocols, xifrar, administració, transferència de fitxers, accés, consola remota, comunicacions segures.

7. HISTÒRIC

Versió 1.0

Dates d'inici de cada fase:

Detecció de necessitat	*Fase de treball*	*Fase de discussió*	*Fase d'aprovació*	*Fase de difusió*	*Fase de suport*
04/2006	08/05/2006	04/09/2006	26/9/2006	28/9/2006	1/1/2007

Equip de treball: Qualitat i Seguretat: Silvia Garre, Josep Mangas, Oficina Seguretat (Indra)
Equip de discussió: CTTI – Innovació i Tecnologia: Emili Platel (+ equip arquitectura d'IiT), Joan Pérez, Enric Martínez i resta equip Enginyeria).
Òrgan aprovador: Comitè de Direcció del CTTI
Equip de suport: Oficina Seguretat

Donat el caràcter tècnic d'aquest manual i per a agilitzar-ne el seu manteniment, les futures revisions no passaran pel Comitè de Direcció del CTTI per a la seva aprovació.

Versió 2.0

Revisió de les versions actuals del programari que s'indica.
Notificació vulnerabilitat de seguretat crítica pel programari VNC.
Eliminació del programari OpenSSH com a servidor FTP, degut a què no presenta suport d'engabiat (chroot) d'usuaris.