



**FORTIFICACIÓ D'ENTORNS
WINDOWS 2003 SERVER**

Índex

3 . . . Qui fem aquesta guia

4 . . . Llicència d'ús

5 . . . Introducció

5 . . . Audiència

5 . . . Abast

5 . . . Aspectes legals i normatius

7 . . . Descripció general

7 . . . Una visió general de l'arquitectura

8 . . . Amenaces presents en l'ús d'aquesta tecnologia

8 . . . Errors de configuració

9 . . . Accés no autoritzat

9 . . . Elevació de privilegis

9 . . . Infecció per malware

10 . . . Denegació de servei

10 . . . Pèrdua o robatori d'informació

11 . . . Recomanacions

11 . . . Recomanacions per prevenir errors de configuració

13 . . . Recomanacions per prevenir l'accés no autoritzat

13 . . . Recomanacions per prevenir l'escalada de privilegis

14 . . . Recomanacions per prevenir la infecció per Malware

14 . . . Recomanacions a l'hora de prevenir la pèrdua de disponibilitat del servei

14 . . . Recomanacions per prevenir la pèrdua o robatori d'informació

16 . . . Conclusions

17 . . . Glossari de termes

18 . . . Referències i enllaços web

18 . . . Eines

Qui fem aquesta guia

El Centre de Seguretat de la Informació de Catalunya, CESICAT, és l'organisme executor del Pla nacional d'impuls de la seguretat TIC aprovat pel govern de la Generalitat de Catalunya el 17 de març de 2009. La missió d'aquest pla és la de garantir una Societat de la Informació Segura Catalana per a tots. Amb aquesta finalitat, es crea el CESICAT com a eina per a la generació d'un teixit empresarial català d'aplicacions i serveis de seguretat TIC que sigui referent nacional i internacional.

La forma jurídica del CESICAT és la de "fundació del sector públic de l'administració de la Generalitat".

Amb l'objectiu de proporcionar unes bones pràctiques i uns coneixements mínims en seguretat de la informació, el CESICAT ofereix com a servei preventiu un conjunt de guies de seguretat adreçades a ciutadans, empreses, administracions públiques i universitats.

www.cesicat.cat

El Pla nacional d'impuls de la seguretat TIC a Catalunya s'estructura al voltant de quatre objectius estratègics principals que seran desenvolupats pel CESICAT:

- Executar l'estratègia nacional de seguretat TIC establerta pel Govern de la Generalitat de Catalunya
- Donar suport a la protecció de les infraestructures crítiques TIC nacionals
- Promocionar un teixit empresarial català sòlid en seguretat TIC
- Incrementar la confiança i protecció de la ciutadania catalana en la societat de la informació.

El contingut de la present guia és titularitat de la Fundació Centre de Seguretat de la Informació de Catalunya i resta subjecta a la llicència de Creative Commons BY-NC-ND. L'autoria de l'obra es reconeixerà mitjançant la inclusió de la següent menció:



Obra titularitat de la Fundació Centre de Seguretat de la Informació de Catalunya.


Llicenciada sota la llicència CC BY-NC-ND.

La present guia es publica sense cap garantia específica sobre el contingut.





L'esmentada llicència té les següents particularitats:


Vostè és lliure de:

 Copiar, distribuir i comunicar públicament la obra.

Sota les condicions següents:

 **Reconeixement:** S'ha de reconèixer l'autoria de la obra de la manera especificada per l'autor o el llicenciador (en tot cas no de manera que suggereixi que gaudeix del seu suport o que dona suport a la seva obra).

 **No comercial:** No es pot emprar aquesta obra per a finalitats comercials o promocionals.

 **Sense obres derivades:** No es pot alterar, transformar o generar una obra derivada a partir d'aquesta obra.

Respecte d'aquesta llicència caldrà tenir en compte el següent:

■ **Modificació:** Qualsevol de les condicions de la present llicència podrà ser modificada si vostè disposa de permisos del titular dels drets.

■ **Altres drets:** En cap cas els següents drets restaran afectats per la present llicència:.

■ Els drets del titular sobre els logotips, marques o qualsevol altre element de propietat intel·lectual o industrial inclòs a les guies. Es permet tan sols l'ús d'aquests elements per a exercir els drets reconeguts a la llicència.

■ Els drets morals de l'autor.

■ Els drets que altres persones poden tenir sobre el contingut o respecte de com s'empra la obra, tals com drets de publicitat o de privacitat.

Avis: En reutilitzar o distribuir la obra, cal que s'esmentin clarament els termes de la llicència d'aquesta obra.

El text complet de la llicència pot ser consultat a <http://creativecommons.org/licenses/by-nc-nd/3.0/es/legalcode.ca>.

Introducció

Audiència

Aquesta guia està adreçada als administradors i responsables de sistemes d'Universitats i Centres de Recerca, Administracions públiques catalanes i PIME que utilitzen equips basats en Microsoft Windows 2003 Server a la seva xarxa.

Donada la naturalesa de les recomanacions i la metodologia emprada per a l'anàlisi, administradors d'altres sistemes operatius diferents poden aprofitar les idees expressades en aquest document i adaptar-les al seu entorn.

De la mateixa manera, qualsevol organització que tingui previst implantar un sistema de Gestió per a la Seguretat de la Informació trobarà interessant i útil el conjunt de bones pràctiques recollides en aquesta guia.

Abast

La finalitat d'aquest document és assolir unes bones pràctiques en seguretat de la informació aplicades a l'administració de servidors Windows 2003 Server. Aquests dispositius estan subjectes a diverses amenaces que poden posar en perill la productivitat i la imatge de les organitzacions.

Aspectes legals i normatius

La present guia s'ha elaborat tenint en compte les recomanacions provinents de l'estàndard internacional ISO 27002, que queden recollides als controls següents:

- 11.4.4 Protecció dels ports de configuració i diagnòstic remot.
- 11.5.1 Processos de connexió segurs.
- 11.5.3 Sistema de gestió de les contrasenyes.
- 11.6.1 Restricció d'accés a la informació.
- 12.5.3 Restriccions en els canvis als paquets de programari.

Descripció general

Una visió general de l'arquitectura

Windows 2003 Server és un sistema operatiu de la família Windows de Microsoft, utilitzat a moltes organitzacions i empreses com a base per construir i oferir els serveis més importants de la xarxa corporativa, ja sigui de manera centralitzada o distribuïda. Els serveis més comuns suportats per aquesta tecnologia són els següents:

- **Servidor d'aplicacions:** funcionalitat que permet gestionar i aglutinar l'accés a dades per part de les aplicacions. D'aquesta manera se centralitza i disminueix la complexitat el desenvolupament de programari.
- **Servidor d'arxius:** funcionalitat que habilita un espai al servidor on emmagatzemar els fitxers dels usuaris per tal que hi puguin accedir des de diferents punts de la xarxa, bé amb el seu equip, bé mitjançant un altre equip d'usuari. La centralització d'informació dels usuaris fora del seu equip també en facilita la conservació al llarg del temps mitjançant la realització de còpies de seguretat.
- **Servidor web:** Windows 2003 Server disposa d'un servei web per publicar pàgines web a Internet.
- **Servidor d'impressió:** el servidor d'impressió centralitza i gestiona les peticions d'impressió provinents dels diferents equips d'usuari cap a les impressores que es troben en xarxa.

■ **Servidor d'accés remot i autenticació (IAS, VPN, RADIUS):** funcionalitat que habilita l'ús de diferents protocols d'accés remot utilitzats pels usuaris que accedeixen remotament als diferents recursos de la xarxa interna, després de superar amb èxit el procés d'autenticació cap al sistema intern.

■ **Servidor de certificació:** autoritat de certificació incorporada al Windows 2003 Server per tal que les organitzacions puguin construir les seves pròpies infraestructures de clau pública (PKI o Public Key Infrastructure) i, així, utilitzar una infraestructura de xifrat i signatura digital basada en cadenes de confiança.

■ **Controlador de domini (Active Directory):**

■ Servei d'administració i gestió centralitzada de xarxes Windows. Aquest servei habilita l'autenticació en xarxa, l'accés als diferents recursos i la gestió centralitzada de còpies de seguretat, entre d'altres.

■ En funció de la mida de la xarxa interna, les organitzacions en poden tenir prou amb un únic servidor, ■ poden requerir-ne més d'un i que es comuniquin entre ells, existint un controlador primari, mentre que la resta funcionen com a controladors secundaris.

■ **Servidors d'infraestructura (DNS, DHCP, WINS):** es tracta de serveis utilitzats de manera transparent pels equips d'usuari i servidors per navegar tant per la xarxa interna com externa, així com per a la compartició d'informació dins la xarxa interna.

■ **Encaminament de les comunicacions:** servei de Windows 2003 Server per a la gestió de les comunicacions mitjançant rutes definides manual o dinàmicament, per accedir a serveis interns i externs.

El fet de tenir tantes funcionalitats en un mateix producte no només n'augmenta la importància i versatilitat i en disminueix el cost, també augmenta el volum d'amenaques a què es troba subjecte l'actiu o actius on està instal·lat, pel fet de centralitzar tants serveis crítics per a una entitat en un únic o diversos dispositius (si existeixen servidors primaris i secundaris). Si aquestes amenaces no es gestionen correctament, poden acabar materialitzant riscos que causin impactes importants, ja siguin econòmics, legals, en la imatge de l'organització o en la seva operativa. Per tal de mitigar aquests riscos, als següents apartats d'aquesta guia es posaran de manifest les principals amenaces associades amb aquesta tecnologia, així com les recomanacions que cal tenir presents per reduir aquestes amenaces.

Amenaces presents en l'ús d'aquesta tecnologia

Errors de configuració

Segons Gartner[1], la probabilitat d'una incidència als nostres sistemes depèn fonamentalment dels errors humans en les configuracions (40%) i de la fiabilitat de les nostres aplicacions (40%).

Un sistema Windows 2003 Server, donada la seva condició de sistema operatiu i servidor d'aplicacions, presenta

un perfil favorable per a l'aparició d'errors de configuració i/o vulnerabilitats que poden comprometre el sistema.

D'una banda, tenim que un sistema operatiu és un conjunt de codi força llarg i complex, que requereix d'un manteniment periòdic per part del fabricant, ja sigui per optimitzar-lo o per resoldre funcionaments anòmals detectats durant la vigència del producte.

D'altra banda, tot el seguit d'aplicacions que poden integrar-s'hi afegixen més complexitat a l'administració i el manteniment del servidor i, si no es fa amb cura, poden minvar la fiabilitat del sistema.

Aquest sistema operatiu està orientat a equips servidors i permet dur a terme una instal·lació per defecte. És important recordar que les configuracions de fàbrica tant de sistema operatiu com d'aplicacions no es poden considerar segures.

Accés no autoritzat

Els servidors Windows 2003 Server són la base sobre la qual una organització construeix la xarxa Windows interna. Per tant, aquests servidors es converteixen en actius crítics per a l'organització, ja que, sense ells, els usuaris de la xarxa no podrien operar normalment amb els seus equips informàtics.

Un dels principals riscos als quals es troba subjecte tot servidor important d'una organització és el fet que algú vulgui accedir-hi, tot i no estar autoritzat.

Si a l'organització s'utilitzen contrasenyes febles, és a dir, contrasenyes construïdes amb pocs caràcters o basades en paraules que podem trobar en diccionaris (amb independència de l'idioma utilitzat) es facilita que puguin ser descobertes i utilitzades per tercers que vulguin accedir al sistema. El mateix succeeix si utilitzem sèries lògiques i comuns per construir la contrasenya, com per exemple, abcdefg, 12345678, abc123, etc.

Intercanviar contrasenyes robustes mitjançant canals de comunicació no segurs també en facilita el descobriment. Per exemple, si utilitzem serveis d'administració que utilitzen comunicacions no xifrades, com pot ser obrir sessions FTP o Telnet, en lloc d'utilitzar els seus homònims xifrats (SFTP i SSH, respectivament), o bé utilitzar formularis d'autenticació web sense mecanismes de xifrat (utilitzar HTTP en comptes d'HTTPS).

Elevació de privilegis

Un cop es disposa d'unes credencials vàlides d'accés al sistema, un usuari amb accés al servidor Windows 2003 Server pot intentar elevar els seus privilegis originals per tal d'aconseguir comprometre la seguretat de l'entorn. Amb un perfil amb més privilegis que els originals, l'atacant pot arribar a fer-se amb el control del servidor i de tota la informació que conté, o utilitzar-lo de trampolí per tal de comprometre altres sistemes connectats a la xarxa interna de l'organització.

Infecció per codi maliciós

La infecció per codi maliciós (malware) en entorns Windows és un dels principals problemes de seguretat al món actual. Segons SANS[2], la prioritat número 1 en

seguretat és fer front a l'entrada als sistemes de cucs, virus i altres tipus de codi maliciós que permeten prendre el control del sistema infectat.

Un equip infectat pot ser utilitzat per dur a terme atacs contra tercers, perjudicant així la imatge i el bon nom de l'organització. Per exemple, pot ser utilitzat per infectar altres equips i enviar correu brossa. Segons Symantec[3], el 40% del SPAM (correu brossa) prové d'equips que han estat infectats.

El robatori de dades i credencials, sobretot bancàries, ha estat un dels principals objectius dels creadors de codi maliciós. Altres virus, per exemple, provoquen un mal funcionament del sistema, degradant el servei o tornant-lo impossible de gestionar.

Totes aquestes amenaces poden conjugar-se al mateix temps, sobretot si el codi maliciós que infecta el nostre servidor el posa sota el control d'una xarxa criminal, i convertir el nostre equip en un Zombie que farà el que li ordenin: robar dades i credencials, llançar atacs, enviar correu brossa o infectar altres equips.

Denegació de servei

Una denegació de servei consisteix a col·lapsar un sistema o servidor per tal que deixi de funcionar normalment. Un cop materialitzada la denegació del servei, per poder recuperar l'actiu afectat, o cal reiniciar el servei o serveis de la màquina hagin estat afectats, o, en el pitjor dels casos, reiniciar el servidor completament.

quest tipus d'amenaça té especial rellevància en un actiu Windows 2003 Server, doncs pot suposar la pèrdua temporal dels serveis de xarxa utilitzats pels usuaris corporatius i, per tant, la pèrdua de productivitat.

La materialització de l'amenaça pot provenir de múltiples peticions de connexió que es llancen contra el servidor, de manera que aquest va reservant memòria per atendre cada connexió. Si el nombre de peticions és suficientment gran, el servidor es col·lapsarà per manca de memòria i provocarà la caiguda del servei. Col·lapsar l'espai del disc o consumir tot el temps de la CPU són altres conseqüències d'una caiguda del servei.

Pèrdua o robatori d'informació

Les amenaces exposades als punts anteriors també poden arribar a ocasionar una pèrdua o robatori d'informació del sistema afectat.

Tot sistema d'informació té una finalitat. És la peça d'un engranatge corporatiu que compleix amb uns objectius concrets, doncs forma part d'un o més serveis que l'organització proporciona, ja siguin interns (comptabilitat, facturació, cartera de clients, etc.), o per als seus clients (dates d'entrega de material, nombre de paquets, saldos bancaris, etc.). Aquests serveis tenen associat el tractament i/o emmagatzematge d'informació. Si aquesta informació resulta malmesa i és important per a l'organització, serà imprescindible poder recuperar-la en un estat igual o similar a aquell en què es trobava just abans que es materialitzés l'amenaça que ha afectat aquesta informació.

El fet de no poder recuperar-la pot repercutir negativament en les finances i la imatge de l'organització, principalment.

Recomanacions

Aquest seguit d'amenaques, si es materialitzen al llarg del temps, en major o menor mesura, tindran efectes perjudicials per a l'organització a la qual pertanyen. Per tal d'evitar que això succeeixi, o minimitzar-ne l'efecte si és que l'amenaça no pot evitar-se totalment, a continuació es proporcionen tot un conjunt de recomanacions dirigides als responsables i administradors de sistemes Windows 2003.

Recomanacions per prevenir errors de configuració

És durant la instal·lació i configuració dels sistemes i dels seus serveis quan poden aparèixer les primeres amenaces. Per aquest motiu, la persona responsable de la instal·lació i posada en servei d'un servidor Windows 2003 Server ha de tenir en compte les recomanacions següents:

- Formatar els discs durs de l'actiu amb un sistema de fitxers que proporcioni la màxima funcionalitat i versatilitat a les solucions que s'hi instal·laran. Per al cas d'un Windows 2003 Server es recomana utilitzar el sistema NTFS.
- No instal·lar programari o paquets disponibles amb el propi sistema operatiu que no es tingui previst d'utilitzar en breu. Cada programa o servei que s'activa en un actiu, obre nous ports cap a la comunitat que són susceptibles de ser utilitzats per a un atac. Per exemple, cal desactivar el servei de NetBIOS si no s'ha d'utilitzar, o si el nostre servidor no s'ha d'utilitzar per publicar pàgines web, no cal instal·lar aquesta funcionalitat.

- No instal·lar programari o paquets de tercers que provenen de fonts no confiables en actius crítics com un Servidor Windows 2003 Server.
- Personalitzar les configuracions per defecte, principalment cal:
 - Deshabilitar els comptes d'accés de convidat, així com d'altres comptes d'accés que es configuren automàticament durant la instal·lació dels diferents mòduls del producte i que no han de ser utilitzats.
 - Canviar la contrasenya per una de personalitzada en aquells comptes d'accés que es configuren automàticament durant la instal·lació dels diferents mòduls del producte i que està previst que s'utilitzin internament.
 - Personalitzar els missatges de benvinguda dels diferents serveis actius al servidor que mostren tant el servei de què es tracta, com la versió, per tal que no siguin fàcilment identificables per un tercer que intenti accedir al servei.
- Aplicar les actualitzacions i els paquets d'esmenes (Service Packs) del fabricant per tal de corregir les vulnerabilitats existents en l'actiu abans de posar-lo en funcionament dins l'organització.

S'ha de tenir molta cura de mantenir els sistemes actualitzats. Microsoft publica contínuament actualitzacions i paquets d'esmenes per corregir vulnerabilitats. Per tant, tot i que s'hagi tingut en compte aquesta recomanació abans de posar l'actiu en servei, cal seguir aplicant aquests paquets periòdicament durant la vida activa del dispositiu. Per fer-ho efectiu, s'hauran de provar en un entorn de proves abans de fer-los efectius en un entorn

de producció, per tal d'evitar caigudes de servei per incompatibilitats entre les modificacions i els serveis actius al dispositiu afectat.

Per identificar i habilitar/deshabilitar els serveis del sistema cal anar a la següent ubicació de l'editor d'objectes de directiva de grup: Configuración de equipo\Configuración de Windows\Configuración de seguridad\Servicios del sistema\.

A l'hora de crear configuracions a nivell de grup (GPO o Group Policy Object) perquè puguin ser aplicades simultàniament a un grup de servidors, cal fer-ho a l'Active Directory. D'aquesta manera s'assegura que la configuració s'aplicarà homogèniament a la xarxa i no en funció d'un únic servidor. Aquesta recomanació és especialment interessant a l'hora d'aplicar polítiques de contrasenya als usuaris de la xarxa.

A més a més, **Microsoft disposa d'una guia [4]** per configurar aspectes relacionats amb la seguretat a Windows 2003 i **es recomana que les organitzacions segueixin aquestes configuracions.**

Microsoft també disposa d'un programari per crear les línies bàsiques de configuració de seguretat del sistema i ajudar a exportar aquesta configuració a la resta d'equips: Microsoft Security Compliance Manager per a Windows Server 2003 Security Baseline.

Al mateix temps, comptem amb eines que ajuden a analitzar l'estat de la seguretat dels sistemes Windows, com

l'eina Microsoft Baseline Security Analyzer (MBSA) de Microsoft, o l'eina Open Vulnerability and Assessment Language (OVAL) de MITRE.

Recomanacions per prevenir l'accés no autoritzat

En primer lloc, cal implementar una **política de contrasenyes coherent i robusta**, preservar la privacitat de les contrasenyes i controlar-ne la vigència. La guia publicada pel CESICAT -Guia per gestionar les contrasenyes^[5]-és una bona referència en aquest sentit, però no es tracta d'una guia de màxims. És a dir, en funció de la importància que tingui l'actiu Windows 2003 Server per a l'organització on es troba, es pot implementar una política encara més estricta que la recomanada a la guia esmentada anteriorment.

En segon lloc, caldrà protegir els processos d'autenticació en xarxa, com per exemple:

- Si es disposa d'intranets o formularis a pàgines web que requereixen autenticació, aquesta ha de realitzar-se sobre **HTTPS**. HTTPS transporta la informació xifrada, mentre que HTTP la transporta en clar.
- Si volem xifrar el procés d'autenticació al servei d'accés remot, s'haurà d'utilitzar **SSH** i no pas Telnet.

Recomanacions per prevenir l'escalada de privilegis

Unes bones pràctiques en seguretat de la informació recomanen que els usuaris tinguin accés estrictament a aquells recursos tecnològics, comunicacions i informació que realment necessitin per exercir les seves

funcions professionals. Aquest accés, però, haurà de limitar-se també al principi d'atorgar els mínims privilegis a cada usuari per tal que aquestes funcions i operativa siguin viables.

Partint de la necessitat de garantir aquest principi, s'ha de definir, **gestionar i administrar de manera correcta** els comptes amb **privilegis d'administrador**, eliminar tots els usuaris que no siguin necessaris del sistema i donar als altres els privilegis que siguin estrictament necessaris en cada cas perquè puguin desenvolupar les seves tasques correctament.

Com ja s'ha comentat prèviament, és imprescindible comptar amb una **bona política de contrasenyes** per garantir la robustesa del nostre sistema enfront dels atacs. En aquest sentit, l'administrador ha de garantir que **l'arxiu de contrasenyes estigui xifrat de manera irreversible**, per garantir que ningú pugui recuperar la informació i obtenir credencials vàlides.

Encara que el fitxer de contrasenyes estigui xifrat, com que els usuaris no tenen cap necessitat d'accedir-hi, s'ha de garantir que **només l'administrador hi tingui accés**.

Les configuracions a nivell de grup (GPO o Group Policy Object), com ja s'ha explicat al punt 6.1, poden ajudar en la **gestió coherent de les configuracions dels nostres servidors**.

Recomanacions per prevenir la infecció per codi maliciós

L'administrador, abans de posar el sistema a producció, ha d'assegurar-se de tenir instal·lades i actualitzades proteccions contra codi maliciós, com són el programari antivirus i el sistema de prevenció d'intrusions (HIPS o Host-Based Intrusion Prevention System), per poder prevenir i reaccionar a temps enfront comportaments anòmals del sistema que puguin estar relacionats amb la presència de codi maliciós.

D'altra banda, els perfils encarregats del manteniment del sistema hauran d'aplicar unes bones pràctiques en seguretat de la informació:

- No executar al sistema programari no autoritzat per l'organització.
- No executar al sistema programari provinent de fonts no segures.
- Tenir el control sobre el que veiem al nostre sistema, mitjançant l'activació a la configuració de carpetes de les opcions per veure tant l'extensió dels arxius, com les carpetes i els fitxers ocults.

També és important que els administradors tinguin presents les recomanacions recollides al punt 6.1 d'aquesta guia, ja que també contribuiran a minvar les possibilitats que el sistema es vegi afectat per aquesta amenaça.

Recomanacions a l'hora de prevenir la pèrdua de disponibilitat del servei

Microsoft recomana una configuració específica per als sistemes Windows 2003 Server, amb l'objectiu de prevenir una denegació de servei provinent de la xarxa. Aquesta configuració ha d'aplicar-se a la ruta següent del fitxer de registre de la màquina:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters.
```

L'administrador haurà d'assegurar-se de fer primer els canvis en servidors d'entorns de preproducció amb l'objectiu de comprovar l'estabilitat dels sistemes, abans de fer efectius els canvis en l'entorn de producció.

Paral·lelament, i per evitar problemes derivats d'una manca de capacitat dels recursos físics del sistema, caldrà aplicar quotes definides de memòria i disc per a usuaris i processos, de manera que no puguin consumir tota la memòria i/o el disc del sistema i provocar una denegació de servei involuntària.

Recomanacions per prevenir la pèrdua o robatori d'informació

Per tal de protegir la informació d'errors del sistema, atacs o accessos indeguts, es proposen les recomanacions següents:

- Configurar el sistema per utilitzar particions NTFS i separar les particions de dades d'usuari de les aplicacions que s'instal·laran i del sistema operatiu. Així s'aconseguirà limitar l'accés no autoritzat a les dades i que un error del sistema corrompi la totalitat de la informació.

- S'haurà de fer un ús adequat dels usuaris, els grups, les propietats dels fitxers i els permisos dels usuaris i grups sobre els fitxers i/o les aplicacions, per tal de mantenir la confidencialitat i integritat de les dades. Com ja s'ha comentat anteriorment, sempre caldrà mantenir el principi de mínims privilegis.
- Els canals de comunicació per on viatgi informació confidencial corporativa i/o credencials d'accés hauran d'estar xifrats i la robustesa del sistema de xifrat s'haurà d'escollir d'acord amb la importància de la informació que cal protegir.
- Aplicar regularment les actualitzacions i paquets d'esmenes que publiquen els diferents fabricants de programari periòdicament.
- Establir una Política de Còpies de Seguretat[6] per a la informació corporativa d'acord amb els diferents nivells de criticitat de la informació.
- Establir una Política de Recuperació de la Informació[6] per tal de garantir la correcta recuperació de la informació perduda, així com el correcte estat i manteniment de les còpies de seguretat i els suports físics utilitzats.

Conclusions

La seguretat en un entorn Windows 2003 té múltiples vessants, es poden activar múltiples serveis, es poden obtenir moltes funcionalitats i també s'està exposat a moltes amenaces diverses.

Hem vist com el nostre sistema pot veure's afectat per una mala configuració que el posi en perill i com les principals solucions passen per tenir **el sistema actualitzat amb els últims paquets d'esmenes**, disposar d'un servidor net **només amb les aplicacions i els usuaris necessaris** i amb **configuracions personalitzades**, en lloc de configuracions de fàbrica.

S'ha demostrat que la **gestió de les contrasenyes** i la **protecció dels sistemes d'autenticació** tenen una importància clau en la lluita contra l'amenaça de l'accés no autoritzat i hem pogut comprendre com unes bones pràctiques basades en el **principi de mínims privilegis** poden ajudar a prevenir el risc associat a l'elevació de drets d'un usuari al sistema.

No hem d'oblidar, però, que el codi maliciós s'ha convertit en un perill important per als sistemes Windows. En aquest sentit, hem vist que cal disposar d'un **sistema contra codi maliciós** actualitzat i d'un **sistema de prevenció d'intrusions** (HIPS o Host-Based Intrusion Prevention System) per detectar comportaments anòmals al sistema, així com **no instal·lar aplicacions de fonts desconegudes o no confiables**.

Hem analitzat també com **configurar un Windows 2003 Server** seguint les indicacions de Microsoft per

mitigar els atacs de denegació de servei, uns dels més comuns que poden arribar des de la xarxa.

Finalment, hem vist que podem comptar amb una **política de còpies de seguretat** per poder recuperar la informació en cas de pèrdua i que ens podem ajudar d'una **partició intel·ligent** del sistema de fitxers.

Només resta animar els administradors de sistemes Windows 2003 Server perquè posin en pràctica aquestes recomanacions i s'esforcin per fer cada esglaó d'aquesta cadena més fort dia a dia.

Glossari de termes

Active Directory: sistema centralitzat i estandarditzat que automatitza la gestió de la informació en xarxa d'usuaris, la seguretat i els recursos distribuïts, i proporciona interacció amb altres directoris.

DHCP: Dynamic Host Configuration Protocol. Servei que assigna dinàmicament adreces IP als equips que ho sol·liciten. Evita que s'hagin d'assignar manualment les adreces als equips.

NTP: Network Time Protocol. Protocol utilitzat per sincronitzar els rellotges dels equips d'una xarxa.

SP: Service Pack. Actualitzacions de programari que distribueix Microsoft per solucionar vulnerabilitats detectades al programari del sistema operatiu.

WINS: Windows Internet Naming Service. Servei que associa el nom lògic de les estacions de treball amb l'adreça IP associada.

Zombie: estat en què cau un ordinador infectat per determinats codis maliciosos, de manera transparent per a l'usuari, i que el col·loca sota les ordres d'una xarxa criminal.

Referències i enllaços web

S'han utilitzat com a referència en l'elaboració d'aquesta guia:

GE-GUI10-02 Guia protecció entorns Windows 2003, del Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya (CTTI).

[5] **Guia per gestionar les contrasenyes, CESICAT**, febrer de 2010.

[PDF] <http://www.cesicat.cat>

[6] **Guia de còpies de seguretat, CESICAT**, febrer de 2010.

[PDF] <http://www.cesicat.cat>

A la web s'hi pot trobar informació rellevant, relacionada amb la matèria desenvolupada en aquesta guia:

[1] High Availability Q&A: Failures, Standards and Metrics, Gartner, juliol de 1998

<http://www.gartner.com/webletter/ibmglobal/edition2/article5/article5.html>

[2] The Top Cyber Security Risks, SANS Institute, setembre de 2009

<http://www.sans.org/top-cyber-security-risks/>

[3] Introduction to botnets, Symantec, maig de 2008

http://www.symantec.com/business/playerdetail.jsp?cid=state_of_spam_botnets&sg=business&type=videos&lg=en&ct=us&fp=y

[4] Windows 2003 Security Guide, Microsoft, desembre de 2005

<http://technet.microsoft.com/es-es/library/dd162275.aspx>

Eines

Microsoft Baseline Security Analyzer

Eina que ajuda les organitzacions a determinar el seu estat de seguretat segons les recomanacions de seguretat de Microsoft i ofereix orientació sobre solucions específiques.

<http://technet.microsoft.com/es-es/security/cc184924.aspx>

Microsoft Security Compliance Manager per a Windows Server 2003 Security Baseline

Eina que permet gestionar i desenvolupar la línia de base de seguretat dels entorns Windows 2003, així com personalitzar-la, exportar-la entre equips i proporcionar tot un conjunt de directrius de seguretat.

<http://technet.microsoft.com/en-us/library/cc163140.aspx>

OSVAL

Eina que consulta la configuració del sistema i permet que les organitzacions comprovin fàcilment la seguretat dels seus sistemes, com ara configuracions segures, actualitzacions i paquets d'esmenes o vulnerabilitats.

<http://oval.mitre.org/repository>



Centre de Seguretat de la
Informació de Catalunya

www.cesicat.cat